Δημήτριος Α. Βάρσος

ΘΕΜΕΛΙΩΔΕΙΣ ΕΝΝΟΙΕΣ ΤΩΝ ΜΑΘΗΜΑΤΙΚΩΝ

ΚΑΛΛΙΠΟΣ ανοικτές ακαδημαϊκές εκδόσεις

Φωτογραφία εξωφύλλου: “lafabriquedesplis” από τον Thomas Renaud.
Άδεια: Free to use under the Unsplash License
https://unsplash.com
Φωτογραφία οπισθοφύλλου: “Το όρος Βαρδούσια” από τον Δημήτριο Βάρσο.

ΘΕΜΕΛΙΩΔΕΙΣ ΕΝΝΟΙΕΣ ΤΩΝ ΜΑΘΗΜΑΤΙΚΩΝ

Θεμελιώδεις Έννοιες των Μαθηματικών

Δημήτριος Βάρσος
Μαθηματικός
ΕΚΠΑ

ΚΑΛΛΙΠΟΣ
ΑΝΟΙΚΤΕΣ ΑΚΑΔΗΜΑΪΚΕΣ ΕΚΔΟΣΕΙΣ
www.kallipos.gr

Τίτλος πρωτοτύπου: «*Θεμελιώδεις έννοιες των μαθηματικών*»

Συντελεστές έκδοσης

Γλωσσική επιμέλεια:	Δημήτριος Καλλιάρας
Γραφιστική επιμέλεια:	Βασίλης Πασχάλης
Τεχνική επεξεργασία:	Βασίλης Πασχάλης

ΚΑΛΛΙΠΟΣ

Εθνικό Μετσόβιο Πολυτεχνείο

Ηρώων Πολυτεχνείου 9

15780 Ζωγράφου

www.kallipos.gr

Βιβλιογραφική αναφορά:	Βάρσος, Δ., (2023). *Θεμελιώδεις έννοιες των μαθηματικών*. [Προπτυχιακό εγχειρίδιο]. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις
Διαθέσιμο στο:	http://dx.doi.org/10.57713/kallipos-206
ISBN:	**978-618-5726-79-9**

Στην Δήμητρα, τον Αθανάσιο

και την Σταματίνα

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΕΥΧΑΡΙΣΤΙΕΣ

Η επιτυχής συγγραφή ενός διδακτικού βιβλίου, πέραν του συγγραφέως, εξαρτάται και από πολλούς άλλους παράγοντες.

Οι παράγοντες αυτοί, τις περισσότερες φορές, είναι αφανείς για τον αναγνώστη. Αυτό δεν σημαίνει ότι είναι και ασήμαντοι.

Κατά την πολύχρονη διδασκαλία μου σε φοιτητές του Τμήματος Μαθηματικών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, το υλικό του βιβλίου, κατά μέρη, έχει δοκιμαστεί διαχρονικά στην τάξη. Οι παρατηρήσεις, οι υποδείξεις ακόμη και οι απορίες από ορεξάτους φοιτητές με φρέσκα μυαλά ήταν πολύτιμες για την διάρθρωση και παρουσίαση της ύλης στην τελική της μορφή.

Τους ευχαριστώ θερμά.

Δύο όμως πρόσωπα συνέβαλαν ουσιαστικά στην υλοποίηση του όλου εγχειρήματος. Πρόκειται για τους συνεργάτες κ. Βασίλειο Πασχάλη, διδάκτορα Λογικής και κ. Ιωάννη Ανδρή, πτυχιούχο Μαθηματικών και κάτοχο μεταπτυχιακού τίτλου σπουδών.

Ο κ. Πασχάλης, ως υπεύθυνος Τεχνικής Επεξεργασίας, δεν περιορίστηκε μόνο στην επεξεργασία του αρχικού κειμένου. Παράλληλα μελετούσε το κείμενο και εντόπισε και *Μαθηματικές αβλεψίες* προφυλάσσοντάς με από ατοπήματα.

Ο κ. Ανδρής, ο πρώτος ο οποίος είχε πρόσβαση στο ολοκληρωμένο κείμενο, το "ξεσκόνισε" εξονυχιστικά εκπλήσσοντάς με με το πλήθος των αβλεψιών που εντόπισε.

Πέραν της ευσυνειδησίας που επέδειξαν, ασχολήθηκαν ερασιτεχνικά[1] και με μεράκι[2] με το έργο, με αποτέλεσμα την όσο το δυνατόν αρτιότερη ποιοτική και τεχνική αναβάθμιση του αρχικού κειμένου.

Οι όποιες ευχαριστίες από την θέση αυτή είναι ανεπαρκείς για να εκφράσουν το μέγεθος της προσφοράς τους.

[1] Ερασιτέχνης: Εκ του "έραμαι την τέχνη" και όχι με την κακόσημη έννοια της καθημερινότητας.

[2] Μεράκι: Μη μετρήσιμη έννοια, ανεκτίμητη αξία.

ΠΡΟΛΟΓΟΣ

Εδώ και μερικές δεκαετίες έχει διαπιστωθεί ότι το "χάσμα", που υπάρχει μεταξύ της Μέσης και της Ανώτατης/Ανώτερης Εκπαίδευσης, αντί να συρρικνώνεται, αμβλύνεται και βαθύνεται. Ειδικά στην Μαθηματική Παιδεία, η κατάσταση είναι απογοητευτική[3]. Σχεδόν σε όλα τα Τμήματα Μαθηματικών, στα Ελληνικά Πανεπιστήμια, γίνονται προσπάθειες "γεφύρωσης" του χάσματος για μια ομαλή ένταξη των νεοεισερχομένων φοιτητών στα αντίστοιχα προγράμματα σπουδών. Οι προσπάθειες αυτές εστιάζονται στην εισαγωγή και διδασκαλία προπαρασκευαστικών μαθημάτων με τίτλο (ή παρεμφερή) "Θεμέλια των Μαθηματικών". Για την υποστήριξη αυτών των μαθημάτων, έχουν γραφεί πολλές σημειώσεις, οι οποίες κυκλοφορούν σε έντυπη ή ηλεκτρονική μορφή. Οι περισσότερες όμως είναι αποσπασματικές και εστιάζονται σε συγκεκριμένες περιοχές των Μαθηματικών. Επίσης, σε συγγράμματα Απειροστικού Λογισμού, ή Γραμμικής Άλγεβρας παρατίθενται εισαγωγικά κεφάλαια, εστιασμένα στο τι έπεται. Ελάχιστα (καθ' όσον γνωρίζουμε) είναι τα συγγράμματα, τα οποία έχουν γραφεί αποκλειστικά για τον σκοπό αυτόν[4].

Το μεγάλο πρόβλημα εντοπίζεται στο ότι οι νεοεισερχόμενοι φοιτητές δεν έχουν διδαχθεί/εξασκηθεί στην "πειθαρχία" σκέψης και έκφρασης (προφορικής και γραπτής). Δεδομένου δε, ότι έχουν έλθει επιφανειακά σε επαφή με την έννοια της απόδειξης/τεκμηρίωσης, αντιμετωπίζουν μεγάλο πρόβλημα στην "άρθρωση" επιχειρημάτων.

Το *ανά χείρας σύγγραμμα*, ως κύριο σκοπό έχει να συμβάλει στην άρση των προβλημάτων, που αντιμετωπίζουν οι πρωτοετείς φοιτητές στα Ελληνικά Πανεπιστήμια, οι οποίοι σκοπεύουν να σπουδάσουν τα Μαθηματικά.

Πριν αναφερθούμε στην δομή του βιβλίου, ας αναφερθούμε σε μερικές γενικές αρχές, οι οποίες χαρακτηρίζουν την σπουδή των Μαθηματικών.

Ένας, ο οποίος σκοπεύει να ασχοληθεί με την μελέτη των Μαθηματικών, πρέπει σιγά-σιγά να μάθει να χρησιμοποιεί την Μαθηματική σκέψη για επαλήθευση Μαθηματικών ισχυρισμών (Θεωρημάτων), να ανακαλύπτει (Μαθηματικές) αλήθειες... και

[3] Αν και έχουμε γνώμη για, τουλάχιστον μερικά, από τα αίτια, τα οποία οδήγησαν στην κατάσταση αυτή, δεν ενδείκνυται, ούτε προτιθέμεθα να ανοίξουμε συζήτηση, μέσω του προλόγου ενός βιβλίου.

[4] Τουναντίον, η ξενόγλωσση βιβλιογραφία, στον τομέα αυτόν, είναι πλούσια και αξιόλογη.

να "δημιουργεί" στα Μαθηματικά[5]. Έτσι προετοιμάζεται να σκέφτεται κριτικά και διερευνητικά, να κατανοεί αποδείξεις και να γράφει τις δικές του αποδείξεις.

Ένας τρόπος, για να επιτευχθούν αυτά, είναι να χρησιμοποιήσουμε τα ίδια τα Μαθηματικά. Ίσως ακούγεται οξύμωρο, αλλά αυτή είναι η πραγματικότητα. Δηλαδή να χρησιμοποιούμε Μαθηματικές γνώσεις, τις οποίες (ή μάλλον νομίζουμε ότι) γνωρίζουμε, για να μάθουμε να κατανοούμε και να επιχειρηματολογούμε[6]. Οι προαπαιτούμενες γνώσεις είναι ελάχιστες. Επαναφέροντας αυτές τις γνώσεις στο προσκήνιο, προχωράμε σιγά-σιγά εντοπίζοντας κενά στην κατανόησή τους, ακόμη και λάθη ως προς τον τρόπο, με τον οποίο (νομίζαμε ότι) τις είχαμε κατανοήσει. Θα διαπιστώσουμε ότι το να σκεφτόμαστε "Μαθηματικώ τω τρόπω" είναι διαφορετικό από τον τρόπο σκέψης σε άλλα επιστημονικά πεδία.

Η μελέτη των Μαθηματικών δεν είναι μια απλή ανάγνωση *"στον καναπέ"*. Είναι μια δυναμική διαδικασία, η οποία απαιτεί ενεργητικότητα και συνεχή χρήση "μολυβιού και χαρτιού". Πρέπει να είμαστε σε εγρήγορση ελέγχοντας και επαληθεύοντας τους ισχυρισμούς του συγγραφέα. Η κατανόηση δεν επιτυγχάνεται, όσες φορές και αν παρακολουθήσουμε εμπνευσμένους και χαρισματικούς δασκάλους. Μην περιμένουμε *"βρεγμένο το παξιμάδι"*. Επίσης, πρέπει να έχουμε μια ευελιξία στην μελέτη μας. Ποτέ δεν εστιαζόμαστε σε μόνο μια πηγή (βιβλίο ή οτιδήποτε άλλο). Ο περιορισμός σε ένα σύγγραμμα, όσο καλό και να είναι, *εγκλωβίζει* τον αναγνώστη.

Εδώ θα πρέπει να επισημάνουμε ότι ανάλογα με το επίπεδο, όχι τόσο των γνώσεων, αλλά της Μαθηματικής ωριμότητας του αναγνώστη, είναι σημαντική η επιλογή του κατάλληλου βιβλίου. Κάθε βιβλίο (συνήθως) απευθύνεται σε συγκεκριμένο κοινό και με συγκεκριμένο σκοπό. Αυτό δεν σημαίνει ότι δεν μπορούμε ταυτόχρονα να εναλλασσόμεθα σε διαφορετικά επίπεδα κατά την μελέτη μας. Επίσης, η μελέτη (κυρίως στα Μαθηματικά) παρουσιάζει παλινδρομήσεις. Δηλαδή, μπορεί κάπου να συναντήσουμε ένα εμπόδιο, το οποίο φαντάζει ανυπέρβλητο. Θα μπορούσαμε να το παρακάμψουμε προσωρινά (αλλά όχι να το ξεχάσουμε), να προχωρήσουμε και να επανέλθουμε. Τις περισσότερες φορές θα διαπιστώσουμε ότι είμαστε ωριμότεροι στην αντιμετώπιση του συγκεκριμένου προβλήματος.

Σκοπός της μελέτης στα Μαθηματικά δεν είναι μόνο η απόκτηση γνώσεων, αλλά και η ανάπτυξη της ικανότητας να γράφουμε Μαθηματικά. Σε άλλα επιστημονικά πεδία, π.χ. στην Φυσική και Χημεία, υπάρχουν τα εργαστήρια, όπου οι σπουδάζοντες αποκτούν την απαιτουμένη εμπειρία. Για έναν, που σπουδάζει τα Μαθηματικα, ο "εργαστηριακός" εξοπλισμός αποτελείται από την βιβλιοθήκη του,... τα μολύβια του και τα άγραφα χαρτιά του.... Το αποτέλεσμα των "πειραματισμών" του είναι... στοίβες από μουτζουρωμένα/τσαλακωμένα χαρτιά και... (ίσως) κάποιες καθαρογραμμένες σελίδες[7]. Εδώ συνειδητοποιούμε την μεγάλη διαφορά μεταξύ του κατανοώ κάτι, το οποίο μελετώ, του απαντώ σε ένα ερώτημα (λύνω ένα πρόβλημα) και του παρουσιάζω (προφορικά ή γραπτά) κατανοητά την απάντηση ενός προβλήματος.

Όπως προείπαμε, το βιβλίο αυτό απευθύνεται σε νεοεισερχόμενους φοιτητές σε Τμήματα Μαθηματικών σε Ελληνικά πανεπιστήμια. Αυτό δεν σημαίνει ότι δεν μπο-

[5]Προς αποφυγή συγχύσης. Άλλο είναι η παραγωγή νέας Μαθηματικής γνώσης και άλλο η Μαθηματική δημιουργία. Ένας νέος, ο οποίος κατορθώνει να λύσει μια δύσκολη (άγνωστη γι' αυτόν) άσκηση, τηρουμένων των αναλογιών, δεν διαφέρει πολύ από έναν ερευνητή, ο οποίος "παράγει" Μαθηματική γνώση.

[6]Ενας, ο οποίος αρχίζει να μαθαίνει ένα μουσικό όργανο δεν χρειάζεται να μάθει πρώτα θεωρητική μουσική και μετά να ξεκινήσει να παίζει. Χρησιμοποιεί τις νότες για να... σπουδάσει τις νότες.

[7]Don't just read it; fight it! Ask your own questions, look for your own examples, discover your own proofs. – Paul Halmos (1916–2006)

ρεί να φανεί χρήσιμο σε οποιονδήποτε θέλει να ξεκινήσει να ασχολείται με την μελέτη των Μαθηματικών. Για τον λόγο αυτόν έχει δομηθεί, ώστε να προσφέρεται και για αυτοδιδασκαλία.

Το βιβλίο χωρίζεται σε επτά Κεφάλαια και ένα Παράρτημα (με τρία υπο-παραρτήματα). Έγινε προσπάθεια ούτως ώστε τα κεφάλαια, αλλά και οι επιμέρους παράγραφοι, να είναι όσον το δυνατόν ανεξάρτητα, για να εξασφαλίζεται η σχετική ευελιξία, ως προς την σειρά, τόσον κατά τη διάρκεια της διδασκαλίας στην τάξη (ανάλογα με τις ανάγκες του ακροατηρίου), όσον και κατά την αυτοδιδασκαλία (ανάλογα με τα ενδιαφέροντα του αναγνώστη).

Στο πρώτο κεφάλαιο επιχειρείται μια εισαγωγή στην θεμελιώδη έννοια του συνόλου. Όπως είναι φυσικό, δεν είναι δυνατόν, στο επίπεδο αυτό, να επιχειρηθεί μια αξιωματική θεμελίωση των συνόλων[8]. Εδώ, στηριζόμενοι στην όποια διαισθητική εικόνα που έχει κάποιος για τα σύνολα, γίνεται προσπάθεια να διαλευκανθούν ορισμένες έννοιες. Εντοπίζονται κάποιες παρανοήσεις, τις οποίες μπορεί να έχει κάποιος σε αυτό το στάδιο των σπουδών του και επισημαίνονται αδιέξοδα[9], στα οποία οδηγούμαστε, λόγω της μη αυστηρής θεμελίωσης των συνόλων.

Κατόπιν παρουσιάζονται οι έννοιες του υποσυνόλου, της τομής, της ένωσης, του συμπληρώματος συνόλων.

Επίσης, γίνεται αναφορά στο δυναμοσύνολο ενός συνόλου και στην έννοια της διαμέρισης ενός συνόλου. Τέλος, παρουσιάζεται η έννοια του διατεταγμένου ζεύγους και το καρτεσιανό γινόμενο συνόλων.

Στο δεύτερο κεφάλαιο παρουσιάζεται η έννοια της Μαθηματικής Πρότασης, σε αντιδιαστολή με την έννοια της πρότασης στην καθημερινότητά μας. Γίνεται αναφορά στην "κατασκευή" νέων Προτάσεων από άλλες Προτάσεις και γίνεται προσπάθεια να διαλευκανθεί, περισσότερο μέσω παραδειγμάτων, η έννοια της συνεπαγωγής Προτάσεων. Οι πίνακες αληθείας στο σημείο αυτό είναι πολύ κατατοπιστικοί. Εδώ δεν μπορούμε να επεκταθούμε περισσότερο προς την περιοχή της Μαθηματικής Λογικής. Μια τέτοια προσπάθεια, στο επίπεδο αυτό, θα ήταν ατελέσφορη.

Το τρίτο κεφάλαιο είναι αφιερωμένο στην έννοια της Μαθηματικής απόδειξης. Όπως προείπαμε, οι περισσότεροι πρωτοετείς φοιτητές δεν έχουν σαφή αίσθηση του τι σημαίνει επιχειρηματολογώ/αποδεικνύω στα Μαθηματικά. Στην αρχή δίνεται προσοχή στην κατανόηση ορισμών και διευκρινίζεται τι σημαίνει αξίωμα και τι σημαίνει Θεώρημα/Πρόταση. Κατόπιν παρουσιάζεται ο τρόπος, με τον οποίο κατανοούμε τις αποδείξεις (τις οποίες έχουν γράψει άλλοι) και στο τέλος παρουσιάζονται μέθοδοι/τεχνικές, ώστε να κάνουμε αποδείξεις και να τις παρουσιάζουμε.

Αν δεν υπήρχε η έννοια της σχέσης μεταξύ συνόλων, τα σύνολα θα παρέμεναν απλώς... *συλλογές αντικειμένων*.

Στο τέταρτο κεφάλαιο παρουσιάζονται οι σχέσεις συνόλων και μελετώνται οι σχέσεις διάταξης και ισοδυναμίας. Έχοντας αναφέρει την έννοια της διαμέρισης στο πρώτο κεφάλαιο, εδώ βλέπουμε ότι οι έννοιες διαμέριση συνόλου και σχέση ισο-

[8]Εδώ πρέπει να επισημάνουμε ότι, ενώ σε επόμενα Κεφάλαια γίνεται αναφορά στο ***Αξίωμα της Επιλογής***, εδώ (σκόπιμα) δεν αναφέρεται.

[9]Εδώ αναφερόμαστε στο παράδοξο του Russell, το οποίο, πάλι, (σκόπιμα) δεν κατονομάζεται.

Κατά την γνώμη μας, οι αναφορές του τύπου *ZFC set theory* ή *Russell's paradox*, χωρίς την δυνατότητα ή την πρόθεση, να επεκταθούμε περισσότερο, δεν προσφέρουν, πέραν του εντυπωσιασμού, κάτι.

δυναμίας σε ένα σύνολο είναι αλληλένδετες (αποτελούν τις "δύο όψεις του ιδίου νομίσματος").

Μια από τις σημαντικότερες έννοιες στα Μαθηματικά είναι η έννοια της απεικόνισης/συνάρτησης[10]. Εδώ γίνεται μια συστηματική μελέτη των απεικονίσεων. Πέραν των εννοιών, που παρουσιάζονται, γίνεται προσπάθεια να αρθούν παρανοήσεις και λάθος θεωρήσεις ως προς την έννοια της απεικόνισης.

Μια σημαντική κατηγορία απεικονίσεων είναι οι πράξεις συνόλων.

Οι πράξεις συνόλων είναι αυτές, οι οποίες προσδίδουν δομή σε ένα σύνολο και, όπως προείπαμε, τα σύνολα δεν είναι απλώς συλλογές αντικειμένων.

Στο πέμπτο κεφάλαιο μελετώνται πράξεις συνόλων, οι οποίες πληρούν ορισμένες χαρακτηριστικές ιδιότητες και δίνονται οι ορισμοί της ομάδας, του δακτυλίου και του σώματος. Δίνονται πολλά παραδείγματα από γνωστές ομάδες και δακτυλίους και παρουσιάζονται οι βασικές ιδιότητές τους. Αποδεικνύεται ένα από τα βασικότερα θεωρήματα (το Θεώρημα του Lagrange) στην θεωρία Ομάδων, αλλά και γενικότερα στα Μαθηματικά. Εδώ βλέπουμε πόσο σημαντική είναι η έννοια της σχέσεως ισοδυναμίας και πώς, σε "πρώιμο" στάδιο, μπορούν να παρουσιαστούν τόσο "βαθιά" θεωρήματα.

Στο σημείο αυτό δεν επεκτεινόμεθα περισσότερο, παραπέμποντας τον αναγνώστη στο τρίτο Παράρτημα, όπου συνεχίζουμε μια περαιτέρω παρουσίαση των ομάδων και των δακτυλίων.

Ο πλέον οικείος δακτύλιος είναι ο δακτύλιος των ακεραίων. Μάλιστα δε οι ιδιότητές του φαντάζουν ως κάτι, το οποίο είναι αυταπόδεικτο και δεν χρήζουν αποδείξεως.

Το έκτο κεφάλαιο είναι αφιερωμένο στην αυστηρή παρουσίαση του δακτυλίου των ακεραίων αριθμών και του σώματος των ρητών αριθμών. Έχοντας ως αφετηρία τους φυσικούς αριθμούς, οι οποίοι μελετώνται στο πρώτο Παράρτημα, ορίζονται, μέσω μιας σχέσης ισοδυναμίας, οι ακέραιοι αριθμοί. Οπότε, οι γνωστές πράξεις της πρόσθεσης και του πολλαπλασιασμού ορίζονται, όλες οι γνωστές ιδιότητες αποδεικνύονται και το σύνολο των ακεραίων αποκτά την δομή μεταθετικού δακτυλίου με μονάδα. Στον δακτύλιο των ακεραίων ορίζεται και μια σχέση ολικής διάταξης, η οποία είναι "συμβιβαστή" με την πρόσθεση και τον πολλαπλασιασμό. Αυτό μας δίνει την δυνατότητα να ορίσουμε την έννοια της διαιρετότητας στους ακεραίους αριθμούς (ο Ευκλείδειος αλγόριθμος). Χωρίς να επεκταθούμε περισσότερο, φθάνουμε σε ένα σημείο, από το οποίο θα μπορούσε να ξεκινά ένα πρώτο μάθημα Θεωρίας αριθμών.

Οι ρητοί αριθμοί ορίζονται, πάλι, μέσω μιας σχέσης ισοδυναμίας στους ακεραίους αριθμούς. Οπότε, οι γνωστές πράξεις της πρόσθεσης και του πολλαπλασιασμού ορίζονται, καθώς και η διάταξη στους ρητούς αριθμούς. Όλες οι ιδιότητές τους αποδεικνύονται και το σύνολο των ρητών αριθμών αποκτά την δομή σώματος.

Η "επέκταση" από τον δακτύλιο των ακεραίων στο σώμα των ρητών αριθμών γίνεται κατά "φυσικό" τρόπο, ώστε οι ακέραιοι, ως δομή δακτυλίου, να εμφυτεύονται στο σώμα των ρητών αριθμών.

Πέραν της διαφοράς, αλγεβρικής φύσεως, μεταξύ ακεραίων και ρητών αριθμών (κάθε μη μηδενικός ρητός αριθμός έχει αντίστροφο ως προς τον πολλαπλασιασμό), επισημαίνεται μια σημαντική δομική διαφορά. Κάθε κάτω φραγμένο υποσύνολο των ακεραίων αριθμών έχει ελάχιστο στοιχείο, κάτι που δεν ισχύει, εν γένει, στους ρητούς αριθμούς.

[10]Όπως διευκρινίζεται, όταν δίνεται ο σχετικός ορισμός, οι δύο λέξεις απεικόνιση-συνάρτηση έχουν την ίδια Μαθηματική σημασία. Εδώ θα χρησιμοποιούμε, σχεδόν πάντοτε, τον όρο απεικόνιση.

Το πλέον, φαινομενικά, οικείο σώμα είναι το σώμα των πραγματικών αριθμών. Από τις πρώτες τάξεις του Λυκείου οι μαθητές έρχονται σε επαφή με τους πραγματικούς αριθμούς (τετραγωνικές ρίζες ακεραίων, μελέτη πραγματικών συναρτήσεων κ.λ.π.). Μάλιστα, κατά την γνώμη μας, η υπερβολική αυτή ενασχόληση με τους πραγματικούς αριθμούς (υποβαθμίζοντας-αγνοώντας άλλες περιοχές των Μαθηματικών) μόνο στρέβλωση επιφέρει.

Στο έβδομο κεφάλαιο γίνεται μια προσπάθεια αυστηρής θεμελίωσης των πραγματικών αριθμών.

Υπάρχουν πολλοί τρόποι ορισμού των πραγματικών αριθμών. Εδώ προτιμούμε έναν τρόπο, ο οποίος, κατά την γνώμη μας, "ρέει φυσιολογικότερα". Ακολουθώντας την "ροή" Φυσικοί αριθμοί → Ακέραιοι αριθμοί → Ρητοί αριθμοί, επεκτείνουμε τους ρητούς αριθμούς στους πραγματικούς αριθμούς. Εδώ το "άλμα" είναι τεράστιο και για να επιτευχθεί χρειάστηκε να επινοηθούν οι τομές Dedekind (κατάλληλα υποσύνολα των ρητών αριθμών).

Ο ορισμός των τομών Dedekind, αν και φαντάζει τεχνικός, κοιτάζοντάς τον εκ των υστέρων, είναι φυσιολογικός.

Στο σύνολο όλων των τομών Dedekind (αυτό που μετέπειτα αποτελεί το σύνολο των πραγματικών αριθμών) ορίζονται οι πράξεις της πρόσθεσης και του πολλαπλασιασμού καθώς και μια ολική διάταξη. Με τις πράξεις αυτές, το σύνολο των πραγματικών αριθμών αποκτά την δομή ενός (διατεταγμένου) σώματος.

Εδώ δίνουμε όλες τις αποδείξεις, οι οποίες, αν και τεχνικές, θεωρούνται αναγκαίες.

Επισημαίνουμε την θεμελιώδη διαφορά ρητών και πραγματικών αριθμών (αρχή της πληρότητας) καθώς και ορισμένες χαρακτηριστικές ιδιότητες των πραγματικών αριθμών.

Δεν επεκτεινόμεθα περισσότερο, δεδομένου ότι έχουμε φτάσει στο κατώφλι του Απειροστικού Λογισμού.

Στο δεύτερο μέρος του κεφαλαίου αυτού παρουσιάζονται οι μιγαδικοί αριθμοί.

Στην αρχή αναφέρονται ορισμένοι από τους λόγους, που οδήγησαν στην επινόηση της φανταστικής μονάδας.

Κατόπιν ορίζονται οι μιγαδικοί αριθμοί, οι πράξεις της πρόσθεσης και του πολλαπλασιασμού και αποδεικνύεται ότι το σύνολο των μιγαδικών αριθμών αποτελεί σώμα. Γίνεται η γεωμετρική αναπαράσταση των μιγαδικών αριθμών, τόσο με καρτεσιανές, όσο και με πολικές συντεταγμένες και μελετώνται οι n-οστές ρίζες της μονάδας.

Στο τέλος, εντελώς ανορθόδοξα, διότι λείπει στο σχετικό υπόβαθρο, παρατίθεται η έκφραση των μιγαδικών αριθμών σε εκθετική μορφή. Ο λόγος αυτής της παράθεσης είναι καθαρά λειτουργικός, δεδομένου ότι οι φοιτητές, από νωρίς, καλούνται να "χρησιμοποιήσουν" τους μιγαδικούς αριθμούς σε διάφορες άλλες περιοχές των Μαθηματικών, καθώς και σε άλλες επιστημονικές περιοχές.

Το βιβλίο ολοκληρώνεται με τρία Παραρτήματα.

Τα Παραρτήματα αυτά αποτελούν αναπόσπαστο μέρος του βιβλίου και ο χαρακτηρισμός ως Παραρτήματα έγινε, όπως αναφέρθηκε και στην αρχή, χάριν ευελιξίας τόσον κατά την διδασκαλία, όσον και την αυτοδιδασκαλία.

Στο πρώτο Παράρτημα γίνεται η θεμελίωση των Φυσικών αριθμών κατά Peano. Ορίζονται οι πράξεις της πρόσθεσης και του πολλαπλασιασμού και αποδεικνύονται οι γνωστές ιδιότητες των Φυσικών αριθμών.

Παρουσιάζεται η αρχή του ελαχίστου και αποδεικνύεται η ισοδυναμία μεταξύ της Μαθηματικής επαγωγής και της αρχής του ελαχίστου.

Στο τρίτο κεφάλαιο αναφέρεται η αρχή της Μαθηματικής επαγωγής απλώς ως μια τεχνική απόδειξης. Εδώ γίνεται μια συστηματική παρουσίαση σε αντιδιαστολή με την αναδρομή.

Για κατανόηση της διαφοράς των δύο εννοιών (επαγωγή, αναδρομή), στο τέλος γίνεται μια σύντομη αναφορά στις ακολουθίες με εφαρμογή σε δύο αναδρομικές ακολουθίες, τις ακολουθίες Fibonacci και Lucas.

Τις έννοιες του πεπερασμένου πλήθους αντικειμένων και απείρου πλήθους αντικειμένων τις χρησιμοποιούμε συνεχώς, ακόμη και στην καθημερινότητά μας, στηριζόμενοι στην διαίσθησή μας. Εδώ, μέχρι τώρα, τις χρησιμοποιούσαμε (χωρίς ιδιαίτερα προβλήματα) πάλι διαισθητικά.

Στο δεύτερο Παράρτημα επισημαίνονται προβλήματα, τα οποία προκύπτουν από την μη σαφή διάκριση μεταξύ των εννοιών "πλήθος" στοιχείων ενός συνόλου και "μέγεθος" ενός συνόλου και επιχειρείται μια μελέτη της πληθικότητας συνόλων.

Για την μελέτη καίριο ρόλο διαδραματίζουν οι απεινονίσεις μεταξύ συνόλων.

Ορίζεται η ισοπληθικότητα μεταξύ δύο συνόλων και γίνεται διάκριση μεταξύ πεπερασμένων και απείρων συνόλων.

Επίσης, γίνεται διάκριση μεταξύ αριθμησίμων και μη αριθμησίμων συνόλων.

Για τα πεπερασμένα σύνολα παρουσιάζεται η "αρχή του περιστεριώνα" και για τα άπειρα σύνολα το Θεώρημα των Cantor-Schroeder-Bernstein.

Αποδεικνύουμε ότι το σύνολο των ρητών αριθμών είναι αριθμήσιμο, ενώ το σύνολο των πραγματικών αριθμών είναι υπεραριθμήσιμο και γίνεται αναφορά στην "υπόθεση του συνεχούς".

Το τρίτο Παράρτημα αποτελεί συνέχεια του πέμπτου κεφαλαίου, όπου εντρυφούμε περισσότερο στις ομάδες και στους δακτυλίους παρουσιάζοντας περισσότερες κατηγορίες ομάδων και δακτυλίων. Όπως είναι οι κυκλικές ομάδες, οι ομάδες ισομετριών, οι δακτύλιοι ακεραίων $mod\, m$ και οι δακτύλιοι πολυωνύμων. Τέλος, παρουσιάζεται η έννοια του ομομορφισμού μεταξύ αλγεβρικών δομών, όπου γίνεται μια προσπάθεια να συνειδητοποιήσουμε την έννοια του ισομορφισμού και το τι σημαίνει δύο (αλγεβρικές) δομές, από αλγεβρικής υφής, να είναι *"ίδιες"*.

Φυσικά το πεδίο είναι ανεξάντλητο και εδώ επιχειρείται μια πρώτη, αλλά αναγκαία, επαφή με την περιοχή αυτή των Μαθηματικών.

Σε όλη την έκταση του βιβλίου, μετά την παρουσίαση μιας έννοιας και της σχετικής συζήτησης, παρατίθενται πολλά παραδείγματα και στο τέλος κάθε παραγράφου πολλές ασκήσεις, των οποίων το επίπεδο δυσκολίας ποικίλλει. Εδώ πρέπει να επισημάνουμε ότι πολλές αποδείξεις θεωρημάτων, προτάσεων κ.λ.π. παραλείπονται και ο αναγνώστης παραπέμπεται σε αντίστοιχες ασκήσεις. Πιστεύουμε ότι οτιδήποτε, κατά την γνώμη μας, είναι δυνατόν να αντιμετωπιστεί ως άσκηση, στηριζόμενοι στα προηγούμενα, να προτείνεται ως άσκηση[11].

Μάλιστα, ορισμένες ασκήσεις τίθενται "προκλητικά" σε σημείο, όπου φαντάζουν απρόσιτες, ενώ, αν παρουσιάζονταν σε επομένη ενότητα, ίσως να φάνταζαν τετριμμένες.

Πέραν των προτεινομένων ασκήσεων, το κείμενο είναι *διανθισμένο* με εκφράσεις του τύπου *...εύκολα βλέπουμε ότι...*, *...δεν είναι δύσκολο να αποδείξουμε ότι...*, *η*

[11] Δεν μπορούμε να καταλάβουμε την εμμονή ορισμένων *δασκάλων*, οι οποίοι παραθέτουν ορισμένα θεωρήματα (χωρίς απόδειξη) και *σπεύδουν* να λύσουν (στρυφνές) ασκήσεις ως εφαρμογή των θεωρημάτων.

απόδειξη αφήνεται ως άσκηση…, *προφανώς (;)*, όπως επίσης και πολλά *γιατί;* Κατά τη γνώμη μας, τα σημεία αυτά αποτελούν τις πλέον σημαντικές, για την κατανόηση, ασκήσεις και για τον λόγο αυτόν συνιστάται να δίνονται τέτοιου είδους ερεθίσματα τόσον κατά τη διδασκαλία στην τάξη όσον και κατά την ιδίαν μελέτη.

Όπως έχουμε επισημάνει, κατά την διάρκεια της μελέτης ενός αντικειμένου ο περιορισμός σε ένα μόνο σύγγραμμα (όσο καλό και να είναι αυτό) *εγκλωβίζει* τον αναγνώστη. Στο τέλος κάθε κεφαλαίου παρατίθεται μια ενδεικτική βιβλιογραφία. Εκτός από τα συγγράμματα, στα οποία παραπέμπεται ο αναγνώστης σε συγκεκριμένα σημεία του κειμένου, περιλαμβάνονται και άλλα, κατά τη γνώμη μας, ενδιαφέροντα συγγράμματα. Με τον τρόπο αυτόν ο ενδιαφερόμενος αναγνώστης *απεγκλωβίζεται* και οδηγείται σε περαιτέρω μελέτη.

Τέλος, επειδή το καλύτερο βιβλίο είναι …αυτό που δεν γράφτηκε…, το βιβλίο αυτό σίγουρα περιέχει λάθη και επιδέχεται βελτιώσεων. Θα θέλαμε να πιστεύουμε ότι τα τυπογραφικ'α λάθη είναι λίγα, τα γραματοικά και ωρθογραφεικά λιγότερα, ελάχιστα συντακτικά λάθη τα εκφραστικά. Κάθε διόρθωση που προέρχεται από καλοπροαίρετη (έστω αυστηρή) κριτική είναι ευπρόσδεκτη και οι ευχαριστίες προκαταβάλλονται….

Οκτώβριος 2022

ΚΕΦΑΛΑΙΟ 1

ΣΥΝΟΛΑ

1.1 Η έννοια του συνόλου

Η έννοια του *συνόλου* αποτελεί θεμελιώδη και ταυτόχρονα πρωταρχική έννοια στα Μαθηματικά και για τον λόγο αυτόν είναι δύσκολο να δοθεί ένας (αυστηρός) ορισμός, ιδίως όταν ξεκινάμε για πρώτη φορά να μελετάμε τα Μαθηματικά.

Στα επόμενα θα προσπαθήσουμε, στηριζόμενοι περισσότερο στην διαίσθηση και στην φαντασία μας, να δώσουμε έναν ορισμό του συνόλου, ο οποίος, αν και όχι αυστηρός, είναι *ικανοποιητικός*, ώστε να προχωρήσουμε με τις λιγότερες δυνατόν δυσκολίες.

1.1.1 Ορισμοί - Βασικές έννοιες

Ένας "αφελής" ορισμός της έννοιας του συνόλου είναι ο εξής:

Ορισμός 1.1.1. Σύνολο είναι μια "καλά–ορισμένη" συλλογή (διακεκριμένων) αντικειμένων.

Αμέσως βλέπουμε ότι εγείρονται ερωτήματα του τύπου:
Τι σημαίνει "καλά ορισμένη συλλογή";
Τι σημαίνει "αντικείμενο";
Πότε δύο αντικείμενα είναι διακεκριμένα;
Τι σημαίνει ένα αντικείμενο ανήκει σε μια συλλογή;
Εδώ την έννοια του αντικειμένου θα την αντιλαμβανόμεθα απλώς ως ένα "πρωταρχικό άτομο" χωρίς την ανάγκη περαιτέρω ορισμού[1].

Τα αντικείμενα, στο εξής, θα αναφέρονται με το όνομά τους. Επομένως, λέγοντας

[1] Δεν πρέπει να γίνεται σύγχυση με την έννοια του *αντικειμένου* στην καθημερινότητα, όπου εκεί τα αντικείμενα τα θεωρούμε ως κάτι το απτό.

ότι ένα αντικείμενο συμβολίζεται με x ή ότι το x είναι ένα αντικείμενο, θα εννοούμε ότι x είναι το όνομα του εν λόγω αντικειμένου.

Επίσης, θα χρησιμοποιούμε τον όρο της ισότητας δύο αντικειμένων με την συνήθη έννοια ότι πρόκειται περί του ιδίου αντικειμένου. Η ισότητα μεταξύ δύο αντικειμένων x και y συμβολίζεται με $x = y$ και σημαίνει ότι x και y είναι διαφορετικά ονόματα του "ιδίου" αντικειμένου. Η άρνηση του $x = y$ δηλώνεται με $x \neq y$. Εδώ τονίζουμε ότι για δύο αντικείμενα θα έχουμε είτε $x = y$ είτε $x \neq y$.

Έχοντας τώρα υπόψιν την έννοια του αντικειμένου και της ισότητας αντικειμένων, θα μπορούσαμε να προσπαθήσουμε να ορίσουμε την έννοια του συνόλου "ως μια *δραστηριότητα* συγκέντρωσης αντικειμένων σε μια 'ολότητα'". Αλλά πάλι αμέσως διαπιστώνουμε ότι ένας τέτοιος ορισμός, όχι μόνο δεν είναι ικανοποιητικός, αλλά οδηγεί και σε παραδοξότητες.

Αργότερα θα επανέλθουμε σε παράδοξα, τα οποία προκύπτουν από την μη δυνατότητα, σε αυτό το επίπεδο, να ορίσουμε αξιωματικά τα σύνολα.

Εγκαταλείποντας την προσπάθεια να ορίσουμε τα σύνολα αυστηρά, παραμένουμε στον ορισμό 1.1.1, οπότε παραμένει αναπάντητη και η έννοια "ένα αντικείμενο ανήκει σε ένα σύνολο" και αρκούμαστε στην διαίσθηση και την φαντασία μας.

Συνήθως τα σύνολα θα τα συμβολίζουμε με ένα κεφαλαίο γράμμα του Ελληνικού ή Λατινικού αλφαβήτου.

Αν ένα αντικείμενο x ανήκει σε ένα σύνολο A, τότε συμβολίζουμε $x \in A$ και το ότι το x δεν ανήκει στο A δηλώνεται με $x \notin A$. Συνεπώς, δοθέντος ενός αντικειμένου x και ενός συνόλου A, είτε $x \in A$ είτε $x \notin A$.

Τα αντικείμενα, που ανήκουν σε ένα σύνολο, ονομάζονται **στοιχεία** του συνόλου και οι εκφράσεις: $x \in A$, το x ανήκει στο σύνολο A, το x είναι στοιχείο του συνόλου A, το σύνολο A περιέχει το στοιχείο x, είναι (Μαθηματικά) ισοδύναμες εκφράσεις.

Αν και η έννοια του συνόλου δεν έχει ορισθεί, τα σύνολα, αυτά καθ' εαυτά, θα μπορούσαν να θεωρηθούν αντικείμενα, οπότε έχουμε σύνολα των οποίων στοιχεία είναι άλλα σύνολα[2].

Ένας συνήθης τρόπος "περιγραφής" ενός συνόλου είναι η χρήση 'άγκιστρων'. Για παράδειγμα, έχουμε το σύνολο $A = \{\alpha, \beta, \gamma\}$, του οποίου τα στοιχεία είναι τα γράμματα α, β, γ και μόνο αυτά.

Προσοχή! Ο τρόπος αυτός περιγραφής ενός συνόλου δεν είναι μοναδικός και, το κυριότερο, τις περισσότερες φορές είναι αναποτελεσματικός. Αργότερα θα επανέλθουμε στον τρόπο "παράστασης" ενός συνόλου, δεδομένου ότι δεν έχουμε ορίσει τα σύνολα αυστηρά.

Παρατήρηση 1.1.2. Πρέπει να τονισθεί ότι άλλη η σημασία της έκφρασης το x *είναι στοιχείο του συνόλου* A και άλλη η σημασία της έκφρασης x *είναι μέρος του συνόλου* A. Αργότερα, όταν θα εισαχθεί η έννοια του υποσυνόλου, θα δούμε την διαφορά μεταξύ του *ανήκειν* και του *μέρους*. Εδώ αρκούμαστε στο διαισθητικό. Η έννοια του μέρους είναι μεταβατική. Αν το A είναι μέρος του B και το B είναι μέρος του C, τότε το A είναι μέρος του C. Ενώ, αν ένα στοιχείο $a \in A$ και το $A \in X$ (το σύνολο A είναι στοιχείο ενός άλλου συνόλου X), **δεν** έπεται ότι το στοιχείο $a \in X$.

Έχοντας πάντα υπόψιν ότι η έννοια "σύνολο" και η έννοια "ένα αντικείμενο ανήκει σε ένα σύνολο", εδώ δεν ορίζονται αξιωματικά, μπορούμε να δεχθούμε ορισμένα αξιώματα.

Το πρώτο αξίωμα που δεχόμαστε είναι το εξής:

[2] Εδώ προκύπτει ένα παράδοξο. *Θα μπορούσε ένα σύνολο να περιέχει τον εαυτό του; Με άλλα λόγια, υπάρχει σύνολο, του οποίου ένα από τα στοιχεία του να είναι το ίδιο το σύνολο;*

Υπάρχει τουλάχιστον ένα σύνολο.
(Αξίωμα της ύπαρξης).

Ένα άλλο αξίωμα, το οποίο μας επιτρέπει να *διαχειριστούμε* την (μη ορισθείσα) έννοια του *ανήκειν* και την έννοια της *ισότητας* είναι το:

Ένα σύνολο προσδιορίζεται επακριβώς από τα στοιχεία του.
(Αξίωμα της έκτασης).

Δύο σύνολα A και B είναι ίσα ($A = B$) αν το A περιέχει κάθε στοιχείο του B και το B περιέχει κάθε στοιχείο του A.
Ισοδύναμα:
$A = B$, *αν: Για κάθε* x, $x \in A$, *αν και μόνο αν* $x \in B$.

Επειδή η έννοια του *ανήκειν* και η έννοια του *συνόλου* δεν έχουν ορισθεί αυστηρά, απαιτείται προσοχή στην επίκληση του προηγουμένου αξιώματος.

Θεωρούμε το εξής "μοντέλο": Κάθε θετικός ακέραιος n αποτελεί ένα σύνολο, του οποίου τα στοιχεία είναι όλοι οι (ακέραιοι) διαιρέτες του n και μόνο αυτοί. Τότε, για τον θετικό ακέραιο 6 έχουμε ότι τα στοιχεία του είναι οι ακέραιοι αριθμοί ± 1, ± 2, ± 3, ± 6.

Ας θεωρήσουμε τώρα το εξής "μοντέλο": Κάθε ακέραιος r αποτελεί ένα σύνολο, του οποίου τα στοιχεία είναι όλοι οι (ακέραιοι) διαιρέτες του r και μόνο αυτοί. Τότε, και για τους δύο (διαφορετικούς) ακεραίους 6 και -6 έχουμε ότι τα στοιχεία τους είναι οι ακέραιοι αριθμοί ± 1, ± 2, ± 3, ± 6. Οπότε, σύμφωνα με το Αξίωμα της έκτασης θα έπρεπε να έχουμε $6 = -6$, κάτι που, με την *εμπειρία* μας, δεν ισχύει.

Η αντίφαση, που προκύπτει, έγκειται στην, μη αυστηρά, προσδιορισμένη *συμπεριφορά* του συμβόλου $\in$.

Παρατήρηση 1.1.3. Εδώ χρησιμοποιούμε τις έννοιες του ακεραίου, του διαιρέτη ενός ακεραίου κ.λ.π., χωρίς καν να έχουν ορισθεί, αλλά στηριζόμενοι στην *εμπειρία* μας. Αυτό δεν πρέπει να μας εμποδίζει να επικαλούμαστε παραδείγματα και έννοιες, με τις οποίες υπάρχει ένας βαθμός εξοικείωσης, χωρίς να είναι αυστηρά ορισμένες.

Αυτό θα συμβαίνει συχνά στο εξής, όπου θα επικαλούμαστε παραδείγματα από τους φυσικούς, ακεραίους, ρητούς, πραγματικούς και μιγαδικούς αριθμούς χωρίς να αποτελεί πρόβλημα η πρωθύστερη επίκλησή τους[3].

Θα δούμε τώρα μια ισοδύναμη έκφραση του αξιώματος της έκτασης.

Θεώρημα 1.1.4. *Έστω A και B δύο σύνολα. Υποθέτουμε ότι για όλα τα x, με $x \notin A$, έπεται ότι $x \notin B$ και για όλα τα x, με $x \notin B$, έπεται ότι $x \notin A$. Τότε $A = B$.*

Απόδειξη. Έστω $x \in A$, τότε έχουμε ότι $x \in B$. Πράγματι, αν $x \notin B$, από την αρχική μας υπόθεση, θα έχουμε $x \notin A$, άτοπο.

Υποθέτουμε ότι έχουμε ένα στοιχείο $x \in B$, τότε, αναγκαστικά, $x \in A$, διότι αν $x \notin A$, από την αρχική μας υπόθεση, θα έχουμε $x \notin B$, άτοπο. Συνεπώς, από το αξίωμα της έκτασης έχουμε $A = B$ ό.έ.δ.

Τα προηγούμενα αξιώματα δεν μας εγγυώνται ότι για κάθε αντικείμενο, έστω a, υπάρχει σύνολο, το οποίο να περιέχει ως στοιχείο (μόνο) αυτό το αντικείμενο. Επομένως χρειαζόμαστε το εξής:

[3] Ας κάνουμε τον παραλληλισμό. Ας υποθέσουμε ότι το "αντικείμενο" μελέτης μας είναι η γλώσσα μας. Για την μελέτη του (μελέτη της γλώσσας) χρησιμοποιούμε το ίδιο "αντικείμενο" (την γλώσσα) για να το μελετήσουμε.

> ***Για κάθε αντικείμενο**, **έστω** a **υπάρχει σύνολο**, **το οποίο περιέχει ως στοιχείο (μόνο) το** a, **δηλαδή το** $\{a\} = \{x \mid x = a\}$.*
> (Αξίωμα του μονοσυνόλου).

Μια πρώτη συνέπεια του αξιώματος αυτού, σε συνδυασμό με το αξίωμα της έκτασης, είναι η εξής: Για κάθε αντικείμενο, έστω a υπάρχει (μοναδικό) σύνολο, το οποίο περιέχει ως στοιχείο (μόνο) το a, δηλαδή το $\{a\}$.

Πράγματι, από τα προηγούμενα έχουμε ότι $\{a\} = \{a, a\}$.

Εξ αυτού έπεται ότι σε ένα σύνολο τα στοιχεία του είναι διακεκριμένα (γιατί;).

***Η έννοια του υποσυνόλου**, **το κενό σύνολο**.*

Έχοντας αποδεχθεί τα δύο προηγούμενα αξιώματα, μπορούμε να προχωρήσουμε και να ορίσουμε την έννοια του υποσυνόλου ενός συνόλου.

Ορισμός 1.1.5. Έστω A και B δύο σύνολα. Το B θα ονομάζεται **υποσύνολο** του A και θα συμβολίζεται $B \subseteq A$ αν κάθε στοιχείο του B είναι στοιχείο του A.

Συμβολικά θα μπορούσαμε να εκφράσουμε την έννοια του υποσυνόλου ως εξής:

$$B \subseteq A, \text{ αν και μόνο αν } x \in B \implies x \in A.$$

Η άρνηση της ιδιότητας του υποσυνόλου δηλώνεται με τον συμβολισμό $B \nsubseteq A$. Ισοδύναμες εκφράσεις της έννοιας του υποσυνόλου είναι οι εξής:

> Το σύνολο B περιέχεται (ως υποσύνολο) στο σύνολο A ή
> το σύνολο A περιέχει (ως υποσύνολο) το σύνολο B ή
> το σύνολο A είναι υπερσύνολο του συνόλου B, συμβολικά $A \supseteq B$).

Μια πρώτη συνέπεια της έννοιας του υποσυνόλου είναι το εξής θεώρημα:

Θεώρημα 1.1.6. *Δύο σύνολα A και B είναι ίσα αν και μόνο αν το A είναι υποσύνολο του B και το B είναι υποσύνολο του A.*

Απόδειξη. Υποθέτουμε ότι το σύνολο A είναι υποσύνολο του B και το σύνολο B είναι υποσύνολο του A.

Έστω $x \in A$, από την υπόθεση και τον ορισμό του υποσυνόλου, έπεται ότι $x \in B$. Παρομοίως, για $x \in B$, έπεται ότι $x \in A$. Δηλαδή ικανοποιείται ο ορισμός ισότητας συνόλων (το αξίωμα της έκτασης).

Προφανώς, αν $A = B$, τότε $A \subseteq B$ και $B \subseteq A$. ό.έ.δ.

Πόρισμα 1.1.7.

i. Για κάθε σύνολο A ισχύει $A \subseteq A$.

ii. Έστω A, B, C τρία σύνολα. Υποθέτουμε ότι $A \subseteq B$ και $B \subseteq C$. Τότε ισχύει ότι $A \subseteq C$.

Απόδειξη. Η απόδειξη είναι προφανής και αφήνεται ως άσκηση. ό.έ.δ.

Το προηγούμενο θεώρημα θα αποτελεί στο εξής μια μέθοδο/τακτική στον έλεγχο της ισότητας δύο συνόλων.

Όταν ένα σύνολο B είναι υποσύνολο ενός συνόλου A, αλλά διαφορετικό του A, δηλαδή $B \subseteq A$ και $B \neq A$, τότε το B ονομάζεται **γνήσιο** υποσύνολο του A και συνήθως συμβολίζεται με $B \subset A$ ή $B \subsetneq A$.

Επανερχόμαστε τώρα στην Παρατήρηση 1.1.2 στην διάκριση μεταξύ των εννοιών του "ανήκειν" (συμβολικά $\in$), η οποία, όπως έχουμε διευκρινίσει, είναι πρωταρχική έννοια και του "περιέχεσθαι" (συμβολικά $\subseteq$), η οποία ορίζεται (Ορισμός 1.1.5). Ας δώσουμε ένα παράδειγμα.

Έστω το σύνολο $A = \{1, 2, 3, B\}$. Τα στοιχεία του συνόλου αυτού είναι οι φυσικοί αριθμοί $1, 2, 3$ και το B, όπου B είναι το σύνολο $B = \{1, 2\}$ (δεν ξεχνάμε ότι επιτρέπεται στοιχεία ενός συνόλου να είναι άλλα σύνολα). Τότε βλέπουμε ότι το $B \in A$ (ως στοιχείο), αλλά, επειδή μερικά από τα στοιχεία του σύνολου A είναι και οι αριθμοί $1, 2$, το σύνολο $\Gamma = \{1, 2\}$ αποτελεί υποσύνολο του συνόλου A ($\Gamma \subseteq A$). Τι παρατηρούμε; $B = \Gamma$ (το αξίωμα της έκτασης), δηλαδή το σύνολο Β έχει "διττό" ρόλο ως προς το σύνολο A, μια φορά ως στοιχείο του και μια φορά ως υποσύνολό του. Αυτό δεν πρέπει να μας δημιουργεί σύγχυση.

Όταν έχουμε ένα σύνολο, έστω A, το πρόβλημα που προκύπτει είναι το πώς προσδιορίζουμε (όλα) τα υποσύνολά του και εάν τα υποσύνολα αυτά "σχηματίζουν" ένα (άλλο) σύνολο. Προς το παρόν αναβάλλουμε την απάντηση στο πρόβλημα αυτό.

Ας επικεντρωθούμε σε έναν τρόπο σχηματισμού υποσυνόλων συνόλων. Στην αρχή δύο παραδείγματα.

i. Έστω A το σύνολο των φυσικών ακεραίων, οι οποίοι είναι μικρότεροι ή ίσοι του 20. Δηλαδή
$$A = \{1, 2, 3, \dots, 20\}.$$
Από τα στοιχεία του συνόλου A επιλέγουμε (μόνο) τους περιττούς αριθμούς και σχηματίζουμε το υποσύνολο
$$B = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19\}.$$
Τα στοιχεία του υποσυνόλου B ικανοποιούν μια χαρακτηριστική ιδιότητα: "Είναι στοιχεία του συνόλου A **και** είναι περιττοί αριθμοί".

ii. Έστω C το σύνολο όλων των κατοίκων του πλανήτη, μια δεδομένη χρονική στιγμή. Από τα στοιχεία του συνόλου C επιλέγουμε (μόνο) τους κατοίκους, οι οποίοι έχουν γεννηθεί κατά την διάρκεια του έτους 1955 και σχηματίζουμε το υποσύνολο
$$D = \{ \text{ οι κάτοικοι του πλανήτη, οι οποίοι έχουν γεννηθεί κατά το έτος 1955 } \}.$$
Τα στοιχεία του υποσυνόλου D ικανοποιούν την χαρακτηριστική ιδιότητα: "Είναι στοιχεία του συνόλου C **και** έχουν γεννηθεί κατά το έτος 1955".

Και στα δύο παραδείγματα είναι εμφανές ότι για τον σχηματισμό των υποσυνόλων "επιλέξαμε" κάποια στοιχεία, τα οποία ικανοποιούν μια "εξειδικευμένη" ιδιότητα.

Ας προσπαθήσουμε να γενικεύσουμε.

Ένα υποσύνολο προσδιορίζεται από την ιδιότητα των στοιχείων.
(Αξίωμα του προσδιορισμού).

Έστω ένα σύνολο A και p μια "πρόταση/ισχυρισμός". Για ένα $x \in A$, με $p(x)$ θα εννοούμε ότι το στοιχείο x "ικανοποιεί" την πρόταση p. Υπάρχει (μοναδικό) υποσύνολο B, του οποίου τα στοιχεία είναι ακριβώς τα στοιχεία x του συνόλου A, για τα οποία η πρόταση $p(x)$ είναι αληθής. Συνήθως το (μοναδικό) αυτό υποσύνολο το παριστάνουμε ως εξής:
$$B = \{x \in A \mid p(x)\}.$$
Επομένως στο πρώτο παράδειγμα θα γράφαμε $B = \{x \in A \mid x \text{ περιττός } \}$

Σχόλιο 1.1.8. Το σύνολο A, στο πρώτο παράδειγμα, θα μπορούσε να θεωρηθεί και αυτό υποσύνολο του συνόλου όλων των φυσικών αριθμών $\mathbb{N}$, οι οποίοι ικανοποιούν την ιδιότητα $p(x)$: ο x είναι φυσικός αριθμός μικρότερος ή ίσος του 20. Δηλαδή

$$A = \{ x \in \mathbb{N} \mid x \leq 20 \}.$$

Παρατηρήσεις 1.1.9. Εδώ δεν δίνουμε ακριβή ορισμό του τι σημαίνει "πρόταση" και του τι σημαίνει μια πρόταση είναι "αληθής", αρκούμαστε στην εμπειρία μας και στην διαίσθησή μας. Στο επόμενο κεφάλαιο θα εντρυφήσουμε περισσότερο επ' αυτού.

Απλώς επισημαίνουμε ότι δεν ορίζουν υποσύνολα όλες οι "προτάσεις". Επίσης, έχει μεγάλη σημασία ως προς ποιο σύνολο αναφερόμαστε. Για παράδειγμα: Ας πάρουμε την πρόταση $q(x)$: "Ο x είναι κοντός". Αν γράψουμε $\{ x \in A \mid q(x) \}$, όπου A είναι το σύνολο στο πρώτο, από τα αμέσως προηγούμενα, παραδείγματα, τότε **δεν** ορίζεται υποσύνολο.

Επίσης, για την ίδια πρόταση $q(x)$: "Ο x είναι κοντός", αν γράψουμε $\{ x \in C \mid q(x) \}$, όπου C είναι το σύνολο στο δεύτερο παράδειγμα, τότε πάλι **δεν** ορίζεται υποσύνολο, διότι δεν έχουμε προσδιορίσει (με σαφήνεια) του τι σημαίνει "κοντός".

Θα θέλαμε να επισημάνουμε ότι ορισμένες φορές, όταν έχουμε ένα σύνολο, τα στοιχεία του ενδέχεται να μην ικανοποιούν κάποια "ορατή" κοινή ιδιότητα. Για παράδειγμα: Τα στοιχεία του συνόλου $\{ 3, 52, 1216, 91 \}$ δεν πληρούν κάποια χαρακτηριστική ιδιότητα (εκτός του ότι είναι αριθμοί). Η μόνη "ιδιότητα", την οποία εμείς προσδώσαμε, είναι ότι αποφασίσαμε να τα θεωρήσουμε, στη σκέψη μας, ως μια ολότητα, δηλαδή ένα σύνολο.

Παράδειγμα 1.1.10. Τα σύνολα

$$A = \{ z \mid \text{ο } z \text{ είναι πραγματικός αριθμός,} \\ \text{που ικανοποιεί την εξίσωση } x^2 - 3x + 2 = 0 \}$$

και

$$B = \{ n \mid \text{ο } n \text{ είναι φυσικός αριθμός μικρότερος του } 3 \},$$

αν και "περιγράφονται" διαφορετικά, είναι ίσα.

Όταν αναφερόμαστε στο κενό σύνολο, συνήθως χρησιμοποιούμε την έκφραση:

> *Κάνουμε την παραδοχή ότι υπάρχει ένα σύνολο, το οποίο δεν περιέχει στοιχεία.*

Τώρα είμαστε σε θέση να αποδείξουμε την ύπαρξη (και μοναδικότητα) του κενού συνόλου (αρκετές παραδοχές έχουμε κάνει άλλωστε).

Έστω A ένα (οποιοδήποτε) σύνολο και έστω η πρόταση $p(x) : x \neq x$, λαμβάνουμε το υποσύνολο

$$\varnothing = \{ x \in A \mid x \neq x \}.$$

Το σύνολο $\varnothing$ δεν περιέχει στοιχεία. Πράγματι, αν υποθέσουμε ότι υπάρχει $x \in \varnothing$, τότε το στοιχείο αυτό θα έχει τις ιδιότητες: $x \in A$ και $x \neq x$. Η αρχική μας παραδοχή όμως είναι ότι δύο αντικείμενα είτε είναι ίσα είτε είναι διαφορετικά (βλέπε σελ. 2) επομένως $x \notin \varnothing$ για όλα τα στοιχεία του συνόλου A. Το αξίωμα της έκτασης μας εξασφαλίζει ότι δεν έχει σημασία ποιο σύνολο A επιλέξαμε, άρα το σύνολο $\varnothing$ υπάρχει και είναι μοναδικό.

Άρα έχει προηγηθεί η απόδειξη του εξής θεωρήματος:

Θεώρημα 1.1.11. *Υπάρχει μοναδικό σύνολο, το οποίο δεν περιέχει στοιχεία.*

Ορισμός 1.1.12. Το μοναδικό σύνολο $\varnothing$ θα ονομάζεται το **κενό** σύνολο και θα συμβολίζεται και ως $\{\ \}$.

Κάθε σύνολο, το οποίο δεν είναι το κενό σύνολο, θα ονομάζεται **μη κενό** σύνολο.

Προφανώς (γιατί;) το μόνο υποσύνολο του κενού συνόλου είναι μόνο το ίδιο το κενό σύνολο.

Πρόταση 1.1.13. *Το κενό σύνολο είναι το μόνο σύνολο, το οποίο είναι υποσύνολο κάθε συνόλου. Δηλαδή:*

i. $\varnothing \subseteq A$, *για κάθε σύνολο* A.

ii. Αν B *είναι ένα σύνολο ώστε* $B \subseteq A$ *για κάθε σύνολο* A, *τότε* $B = \varnothing$.

Απόδειξη. Ο πρώτος ισχυρισμός απορρέει από τον τρόπο ορισμού του κενού συνόλου[4].

Για τον δεύτερο ισχυρισμό. Αν το σύνολο B είναι υποσύνολο κάθε συνόλου, θα είναι και υποσύνολο του κενού συνόλου ($B \subseteq \varnothing$). Αλλά από τον πρώτο ισχυρισμό έχουμε $\varnothing \subseteq B$. Τέλος. ό.έ.δ.

Στην υποσημείωση της σελίδας 2 είχαμε θέσει το ερώτημα:

> Θα μπορούσε ένα σύνολο να περιέχει τον εαυτό του;

Ένα *παρεμφερές* ερώτημα είναι το εξής:

> Υπάρχει σύνολο, το οποίο να περιέχει τα "πάντα";

(Εδώ η έκφραση "τα πάντα" δεν ορίζεται αυστηρά, αλλά μας αρκεί αυτό που διαισθανόμαστε και θα μπορούσε να αντικατασταθεί με την έκφραση "το σύμπαν").

Πριν προχωρήσουμε στην απάντηση του δευτέρου ερωτήματος, μπορείτε να δείτε πώς 'συνδέονται' τα δύο αυτά ερωτήματα;

Θεώρημα 1.1.14. *Δοθέντος ενός συνόλου* A *υπάρχει αντικείμενο, έστω* B, *το οποίο δεν ανήκει στο σύνολο* A ($B \notin A$).

Απόδειξη. Θεωρούμε την πρόταση

$$p(x)\text{: Το } x \text{ είναι ένα σύνολο και το } x \notin x.$$

Από το αξίωμα του προσδιορισμού έχουμε το εξής υποσύνολο του A,

$$B = \{\, x \in A \mid p(x) \,\}.$$

Θα αποδείξουμε ότι το αντικείμενο B δεν ανήκει στο σύνολο A.

Ας υποθέσουμε ότι $B \in A$. Για το αντικείμενο B έχουμε δύο (μόνο) δύο επιλογές. Είτε $B \in B$ είτε $B \notin B$.

Υποθέτουμε ότι ισχύει η πρώτη επιλογή ($B \in B$). Επίσης, έχουμε υποθέσει ότι $B \in A$. Αυτό, από τον ορισμό του συνόλου B, σημαίνει ότι $B \notin B$, αντίφαση.

Υποθέτουμε ότι ισχύει η δεύτερη επιλογή ($B \notin B$). Επίσης, έχουμε υποθέσει ότι $B \in A$. Συνεπώς, (πάλι) από τον ορισμό του συνόλου B έχουμε ότι $B \in B$, αντίφαση.

Τελικά και για τις δύο επιλογές έχουμε ότι η υπόθεση $B \in A$ είναι εσφαλμένη. Άρα $B \notin A$. ό.έ.δ.

[4] Ισοδυνάμως θα μπορούσαμε να επιχειρηματολογήσουμε ως εξής: Η πρόταση $x \in \varnothing$ είναι πάντα λανθασμένη. Συνεπώς, η συνεπαγωγή $x \in \varnothing \implies x \in A$, για κάθε σύνολο A είναι πάντα αληθής, αλλά ακόμη δεν έχουμε μιλήσει για (λογικές) συνεπαγωγές.

Πόρισμα 1.1.15. *Δοθέντος ενός συνόλου A, υπάρχει σύνολο B έτσι ώστε $B \notin A$.*

Απόδειξη. Στο προηγούμενο θεώρημα το αντικείμενο που κατασκευάσαμε και δεν ανήκει στο σύνολο A είναι σύνολο. ό.έ.δ.

Μια σημαντική συνέπεια των προηγουμένων είναι ότι απαντήσαμε αρνητικά στα προηγούμενα ερωτήματα. Ήτοι:

> Δεν υπάρχει σύνολο, το οποίο να περιέχει το σύμπαν. Όλα τα σύνολα δεν αποτελούν σύνολο.

Επειδή όλα τα σύνολα δεν αποτελούν σύνολο, όταν έχουμε μια "συλλογή" συνόλων, η οποία (δεν γνωρίζουμε) ότι αποτελεί σύνολο, χρησιμοποιούμε τον όρο **οικογένεια** συνόλων ή **κλάση** συνόλων.

Σχόλιο 1.1.16. Επισημαίνεται ότι σε πολλά εγχειρίδια Θεωρίας Συνόλων επιχειρείται μια διαφορετική προσέγγιση.

Αντί του αξιώματος του προσδιορισμού, με το οποίο οδηγούμαστε στην απόδειξη της ύπαρξης του κενού συνόλου, θεωρούμε το αξίωμα: Υπάρχει σύνολο, το οποίο περιέχει "τα πάντα". Με αυτό το αξίωμα πάλι οδηγούμαστε στην απόδειξη της ύπαρξης του κενού συνόλου.

Χωρίς να επεκταθούμε περισσότερο, τελικά, χωρίς μεγάλες διαφορές, και οι δύο "εκδοχές" παρουσίασης οδηγούν στα ίδια αποτελέσματα.

1.1.2 Η ένωση και η τομή συνόλων

Υποθέτουμε ότι έχουμε δύο σύνολα A και B και ενδιαφερόμαστε να "κατασκευάσουμε" (αν υπάρχει) ένα άλλο σύνολο, το οποίο να περιέχει, ως υποσύνολα, τα A και B και να είναι το "μικρότερο", ως προς την σχέση του περιέχεσθαι με αυτήν την ιδιότητα.

Υποθέτουμε ότι και τα δύο σύνολα A και B περιέχονται σε ένα άλλο σύνολο, έστω Ω. Το υποσύνολο

$$\{ x \in \Omega \mid x \in A, \text{ ή } x \in B \},$$

το οποίο ορίζεται καλά από το αξίωμα του προσδιορισμού, πληροί τις απαιτούμενες συνθήκες. Πράγματι, αν υπάρχει ένα άλλο σύνολο, έστω S, το οποίο περιέχει τα A και B, τότε ορίζεται το υποσύνολο

$$\{ x \in S \mid x \in A, \text{ ή } x \in B \}.$$

Τα σύνολα

$$\{ x \in \Omega \mid x \in A \text{ ή } x \in B \} \text{ και } \{ x \in S \mid x \in A \text{ ή } x \in B \}$$

είναι ίσα (γιατί;). Επομένως το σύνολο που αναζητούσαμε δεν εξαρτάται από την επιλογή των (υπερ)συνόλων Ω και S. Συνεπώς, μπορούμε να γράφουμε για το σύνολο αυτό

$$\{ x \mid x \in A, \text{ ή } x \in B \}.$$

Μάλιστα δε ισχύει ότι:

$$\text{Αν } A, B \subseteq C, \text{ τότε } \{ x \mid x \in A \text{ ή } x \in B \} \subseteq C.$$

Υπ' αυτήν την έννοια το σύνολο αυτό είναι το μικρότερο σύνολο που περιέχει ως υποσύνολα τα σύνολα A και B.

Όλα αυτά ισχύουν υπό την προϋπόθεση ότι υπάρχει σύνολο, το οποίο να περιέχει τα δοθέντα σύνολα A και B. Για δύο όμως τυχαία σύνολα δεν είμαστε βέβαιοι ότι πάντα υπάρχει ένα σύνολο, το οποίο τα περιέχει. Δεν ξεχνάμε ότι δεν υπάρχει σύνολο, το οποίο να περιέχει τα πάντα. Επομένως είμαστε αναγκασμένοι να αποδεχθούμε ένα ακόμη αξίωμα.

> ***Δοθέντων δύο συνόλων*** A ***και*** B, ***υπάρχει ένα σύνολο***, ***το οποίο περιέχει τα*** A ***και*** B.
> (Αξίωμα του εγκλεισμού).

Μετά την παραδοχή του αξιώματος αυτού, όλα τα προηγούμενα είναι εφαρμόσιμα και οδηγούμαστε στον εξής ορισμό:

Ορισμός 1.1.17. Η **ένωση** δύο συνόλων A και B είναι το σύνολο

$$A \cup B = \{x \mid x \in A, \text{ ή } x \in B\}.$$

Θεώρημα 1.1.18. *Δοθέντων τριών συνόλων* A, B, C *ισχύουν τα εξής:*

1. $A \cup A = A$.
2. $A \cup B = B \cup A$ *(Η μεταθετικότητα της ένωσης).*
3. $A \subseteq A \cup B$ *και* $B \subseteq A \cup B$.
4. *Έστω* $A \subseteq C$ *και* $B \subseteq C$, *τότε* $A \cup B \subseteq C$.
5. $A \cup (B \cup C) = (A \cup B) \cup C$ *(Η προσεταιριστικότητα της ένωσης).*
6. $A \cup \varnothing = A$.

Απόδειξη. Η απόδειξη όλων των ισχυρισμών είναι εύκολη και αφήνεται ως άσκηση.

Εδώ θα αποδείξουμε μόνο την προσεταιριστικότητα της ένωσης.

Έστω $x \in A \cup (B \cup C)$, τότε $x \in A$ ή $x \in B \cup C$.

Υποθέτουμε ότι $x \in A$, τότε από το (3) έχουμε $x \in A \subseteq A \cup B \subseteq (A \cup B) \cup C$.

Υποθέτουμε ότι $x \in B \cup C$, τότε $x \in B$ ή $x \in C$. Αν $x \in B$, τότε, από το (3), έχουμε $x \in A \cup B$ και συνεπώς, πάλι από το (3), $x \in (A \cup B) \cup C$. Αν $x \in C$, από το (3), έχουμε ότι $x \in (A \cup B) \cup C$.

Άρα σε όλες τις περιπτώσεις, με την υπόθεση ότι $x \in A \cup (B \cup C)$, αποδεικνύουμε ότι $x \in (A \cup B) \cup C$. Δηλαδή $A \cup (B \cup C) \subseteq (A \cup B) \cup C$.

Όμοια αποδεικνύεται ότι $(A \cup B) \cup C \subseteq A \cup (B \cup C)$.

Άρα, από το Θεώρημα 1.1.6 έπεται το αποτέλεσμα. ό.έ.δ.

Το (4) του προηγουμένου θεωρήματος απαντά στον αρχικό προβληματισμό μας.

> "Η ένωση δύο συνόλων είναι το *μικρότερο*, ως προς την σχέση του εγκλεισμού, σύνολο το οποίο περιέχει και τα δύο σύνολα."

Μετά την απόδειξη της ισότητας $A \cup (B \cup C) = (A \cup B) \cup C$, μπορούμε, αδιακρίτως, να γράφουμε

$$A \cup (B \cup C) = (A \cup B) \cup C = A \cup B \cup C$$

και, επαναληπτικά[5], να επιτυγχάνουμε την ένωση περισσοτέρων των τριών συνόλων. Δηλαδή

$$A_1 \cup A_2 \cup \cdots \cup A_{n-1} \cup A_n = (A_1 \cup A_2 \cup \cdots \cup A_{n-1}) \cup A_n.$$

Για συντομία έχει επικρατήσει ο συμβολισμός

$$\bigcup_{i=1}^{n} A_i.$$

Πρόταση 1.1.19. *Έστω A, B, C, D σύνολα με $A \subseteq C$ και $B \subseteq D$. Τότε $A \cup B \subseteq C \cup D$.*

Απόδειξη. Άσκηση.

Πρόταση 1.1.20. *Έστω A, B δύο σύνολα. Τότε ισχύει $A \subseteq B$ αν και μόνο $A \cup B = B$.*

Απόδειξη. Άσκηση.

Έχοντας το αξίωμα του εγκλεισμού (σελ. 9) για δύο σύνολα, είδαμε ότι μπορούμε να ορίσουμε την ένωση δύο συνόλων και, επαναληπτικά, την ένωση πεπερασμένου το πλήθος συνόλων.

Όταν όμως έχουμε άπειρο το πλήθος σύνολα, τότε δεν μπορούμε να επικαλεσθούμε την επαναληπτικότητα και να ορίσουμε την ένωσή τους. Επομένως είμαστε αναγκασμένοι να αποδεχθούμε ένα αξίωμα:

Έστω $\mathcal{A}$ ένα σύνολο, του οποίου τα στοιχεία είναι σύνολα. Το σύνολο

$$\bigcup(\mathcal{A}) = \{ x \mid x \in B \textbf{ για κάποιο } B \in \mathcal{A} \}$$

υπάρχει και ονομάζεται η συνολοθεωρητική ένωση των στοιχείων του $\mathcal{A}$. (Αξίωμα της ένωσης).

Επ' αυτού του αξιώματος θα επανέλθουμε αργότερα.

Παρατήρηση 1.1.21. Δεν έχουμε ορίσει, αυστηρά, τι σημαίνει άπειρο το πλήθος ή πεπερασμένο το πλήθος. Προς το παρόν αρκούμαστε στην διαίσθησή μας και την φαντασία μας.

Το μόνο, που μπορούμε να αναφέρουμε εδώ, είναι ότι πρόκειται για ένα αξίωμα, το οποίο, όπως θα δούμε αργότερα, μας επιτρέπει να κάνουμε σαφή διαχωρισμό μεταξύ της έννοιας του "πεπερασμένου" και του "απείρου".

Για κάθε σύνολο X πάντα ορίζεται το σύνολο $X \cup \{X\}$, το οποίο θα το συμβολίζουμε

$$\sigma(X) = X \cup \{X\}.$$

Το πρώτο που παρατηρούμε είναι η διττή ιδιότητα του συνόλου X ως προς το σύνολο $\sigma(X) = X \cup \{X\}$. Δηλαδή,

$$X \in \sigma(X) = X \cup \{X\} \text{ και } X \subseteq \sigma(X) = X \cup \{X\}.$$

[5]Εδώ χρησιμοποιούμε τον όρο "επαναληπτικά" διαισθητικά. Αργότερα, όταν μιλήσουμε για επαγωγή και αναδρομή (ιδέ Παράρτημα Α), ο όρος "επαναληπτικά" θα αποκτήσει *Μαθηματική υπόσταση*.

Επίσης, παρατηρούμε ότι την ιδιότητα αυτή την έχει και το σύνολο $\sigma(X) = X \cup \{X\}$, ως προς το σύνολο

$$\sigma(X \cup \{X\}) = \sigma(\sigma(X)) = (X \cup \{X\}) \cup \{X \cup \{X\}\}.$$

Οπότε, μπορούμε να επαναλαμβάνουμε την ανωτέρω διαδικασία "αενάως".

Η έκφραση *...επαναλαμβάνουμε την ανωτέρω διαδικασία "αενάως"*[6], δεν μπορεί να ερμηνευθεί αυστηρά, για τον λόγο αυτόν αποδεχόμεθα το εξής αξίωμα:

Υπάρχει ένα σύνολο E ***με τις ιδιότητες:***

- $\varnothing \in E$.
- ***Αν*** $a \in E$, ***τότε*** $\sigma(a) = a \cup \{a\} \in E$.

(Αξίωμα του απείρου).

Ένα σύνολο που ικανοποιεί το αξίωμα αυτό θα ονομάζεται **επαγωγικό** σύνολο. Το στοιχείο $\sigma(a)$ θα ονομάζεται το **επόμενο** του a. Επ' αυτών, όπως προείπαμε, θα επανέλθουμε αργότερα.

Η δυϊκή έννοια της ένωσης συνόλων είναι η έννοια της τομής συνόλων.

Έστω A και B δύο σύνολα. Από το αξίωμα του προσδιορισμού τα στοιχεία του συνόλου A, τα οποία είναι και στοιχεία του συνόλου B, ορίζουν ένα υποσύνολο του συνόλου A, δηλαδή το σύνολο $\{x \in A \mid x \in B\}$. Όμοια ορίζεται ένα υποσύνολο του συνόλου B, του οποίου τα στοιχεία είναι και στοιχεία του συνόλου A, δηλαδή το σύνολο $\{x \in B \mid x \in A\}$.

Από το αξίωμα της έκτασης έπεται εύκολα (γιατί;) ότι

$$\{x \in A \mid x \in B\} = \{x \in B \mid x \in A\}.$$

Το σύνολο αυτό, το οποίο αποτελείται από όλα τα στοιχεία, τα οποία ανήκουν ταυτόχρονα και στο σύνολο A και στο σύνολο B, είναι το σύνολο $\{x \mid x \in A \text{ και } x \in B\}$.

Ορισμός 1.1.22. Δοθέντων δύο συνόλων A και B το σύνολο

$$A \cap B = \{x \mid x \in A \text{ και } x \in B\}$$

θα ονομάζεται **τομή** των A και B.

Πριν προχωρήσουμε μια παρατήρηση.

Παρατήρηση 1.1.23. Στην περίπτωση της ένωσης συνόλων, τα μέχρι τότε αξιώματα δεν "επαρκούσαν" και υποθέσαμε ένα (ακόμη) αξίωμα (το αξίωμα του εγκλεισμού). Στην περίπτωση της τομής συνόλων δεν χρειάζεται να υποθέσουμε ένα επιπλέον αξίωμα.

Επίσης, θα θέλαμε να επισημάνουμε την εντελώς διαφορετική σημασία που αποκτά η χρήση της λέξης "και" στην τομή και στην ένωση συνόλων. Ένα αντικείμενο ανήκει στην τομή $A \cap B$, αν ανήκει στο A **και** στο B. Το σύνολο, το οποίο αποτελείται από τα στοιχεία του A **και** από τα στοιχεία του B είναι η ένωση $A \cup B$.

Πρόταση 1.1.24. *Έστω* A, B, C *σύνολα με* $C \subseteq A$ *και* $C \subseteq B$, *τότε* $C \subseteq A \cap B$.

[6] *αενάως* σημαίνει επ' άπειρον.

Απόδειξη. Για κάθε $x \in C$ έχουμε $x \in C \subseteq A$, δηλαδή $x \in A$. Όμοια από την σχέση $x \in C \subseteq B$ έχουμε ότι $x \in B$. Συνεπώς, για κάθε $x \in C$ έχουμε ότι $x \in A$ και $x \in B$, άρα $x \in A \cap B$. ό.έ.δ.

Θεώρημα 1.1.25. *Δοθέντων τριών συνόλων A, B, C ισχύουν τα εξής:*

1. $A \cap A = A$.
2. $A \cap B = B \cap A$ *(Η μεταθετικότητα της τομής).*
3. $A \cap B \subseteq A$ *και* $A \cap B \subseteq B$.
4. *Έστω* $C \subseteq A$ *και* $C \subseteq B$, *τότε* $C \subseteq A \cap B$.
5. $A \cap (B \cap C) = (A \cap B) \cap C$ *(Η προσεταιριστικότητα της τομής).*
6. $A \cap \varnothing = \varnothing$.

Το θεώρημα αυτό αποτελεί την "δυϊκή έκφραση" του Θεωρήματος 1.1.18, το οποίο αναφέρεται στην ένωση συνόλων.

Απόδειξη. Η απόδειξη είναι "παράλληλη" της απόδειξης του Θεωρήματος 1.1.18 και αφήνεται ως άσκηση. ό.έ.δ.

Το (4) του προηγουμένου θεωρήματος θα μπορούσε να αναδιατυπωθεί ως εξής:

> "Η τομή δύο συνόλων είναι το *μεγαλύτερο*, ως προς την σχέση του εγκλεισμού, σύνολο, το οποίο περιέχεται και στα δύο σύνολα."

Όπως στην περίπτωση της προσεταιριστικότητας της ένωσης, έτσι και στην προσεταιριστικότητα της τομής μπορούμε, αδιακρίτως, να γράφουμε

$$A \cap (B \cap C) = (A \cap B) \cap C = A \cap B \cap C$$

και, επαναληπτικά, να επιτυγχάνουμε την τομή περισσοτέρων των τριών συνόλων. Δηλαδή

$$A_1 \cap A_2 \cap \cdots \cap A_{n-1} \cap A_n = (A_1 \cap A_2 \cap \cdots \cap A_{n-1}) \cap A_n.$$

Για συντομία έχει επικρατήσει ο συμβολισμός

$$\bigcap_{i=1}^{n} A_i.$$

Πρόταση 1.1.26. *Έστω A, B, C, D σύνολα με $A \subseteq C$ και $B \subseteq D$. Τότε $A \cap B \subseteq C \cap D$.*

Απόδειξη. Άσκηση.

Πρόταση 1.1.27. *Έστω A, B δύο σύνολα. Τότε ισχύει $A \subseteq B$ αν και μόνο $A \cap B = A$.*

Απόδειξη. Άσκηση.

Όπως είδαμε, μπορούμε να ορίσουμε, επαναληπτικά, την τομή περισσοτέρων των δύο συνόλων. Όταν όμως έχουμε άπειρο το πλήθος σύνολα, τότε δεν μπορούμε να επικαλεσθούμε την επαναληπτικότητα και να ορίσουμε την τομή τους. Επομένως είμαστε αναγκασμένοι να αποδεχθούμε (όπως και στην περίπτωση της ένωσης) ένα αξίωμα:

Έστω $\mathcal{A}$ ένα (μη κενό) σύνολο, του οποίου τα στοιχεία είναι σύνολα. Το σύνολο

$$\bigcap(\mathcal{A}) = \{ x \mid x \in B \text{ για όλα τα } B \in \mathcal{A} \}$$

υπάρχει και ονομάζεται η συνολοθεωρητική τομή των στοιχείων του $\mathcal{A}$. (Αξίωμα της τομής).

Ένας άλλος σημαντικός συσχετισμός μεταξύ συνόλων είναι ο εξής:

Ορισμός 1.1.28. Δύο σύνολα A και B θα ονομάζονται **ξένα** μεταξύ τους αν $A \cap B = \varnothing$[7].

Μπορούμε να επεκτείνουμε αυτήν την έννοια σε περισσότερα των δύο συνόλων. Έστω A, B, C τρία σύνολα, τα σύνολα αυτά θα λέγονται ξένα μεταξύ τους, αν δεν υπάρχει αντικείμενο, το οποίο να ανήκει σε περισσότερα του ενός σύνολα. Αυτό σημαίνει ότι $A \cap B = A \cap C = B \cap C = \varnothing$.

Προσοχή! Η συνθήκη $A \cap B \cap C = \varnothing$ είναι ασθενέστερη, διότι σημαίνει ότι δεν υπάρχει αντικείμενο, το οποίο να ανήκει και στα τρία σύνολα, αλλά δεν αποκλείει την περίπτωση να υπάρχει αντικείμενο, το οποίο να ανήκει σε δύο από τα τρία σύνολα.

Προς αποφυγή σύγχυσης, έχει επικρατήσει, όταν έχουμε περισσότερα των δύο σύνολων, να λέμε ότι τα σύνολα είναι *ανά δύο* ξένα μεταξύ τους.

Η τομή και η ένωση δύο συνόλων *συνδέονται* μεταξύ τους με τον "νόμο του επιμερισμού".

Θεώρημα 1.1.29. *Δοθέντων τριών συνόλων A, B, C ισχύει.*

i. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

ii. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Απόδειξη. i. Έστω $x \in A \cap (B \cup C)$. Αυτό σημαίνει ότι $x \in A$ και $x \in B \cup C$, δηλαδή $x \in A$ και $x \in B$ ή $x \in C$. Αν $x \in B$, τότε $x \in A \cap B$. Αν $x \in C$, τότε $x \in A \cap C$. Οπότε, οποιαδήποτε περίπτωση και αν ισχύει, έχουμε $x \in (A \cap B) \cup (A \cap C)$. Συνεπώς, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Αντίστροφα, έστω $x \in (A \cap B) \cup (A \cap C)$. Αυτό σημαίνει ότι $x \in A \cap B$ ή $x \in A \cap C$. Αν $x \in A \cap B$, τότε $x \in A$ και $x \in B$. Αν $x \in A \cap C$, τότε $x \in A$ και $x \in C$. Οπότε, οποιαδήποτε περίπτωση και αν ισχύει, έχουμε ότι $x \in A$ και $x \in B$ ή $x \in C$. Συνεπώς, $x \in A \cap (B \cup C)$, δηλαδή $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. Τελικά $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Όμοια αποδεικνύεται η δεύτερη περίπτωση ότι $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ και αφήνεται ως άσκηση. ό.έ.δ.

Οικογένειες συνόλων - Δείκτες σε σύνολα.

Προηγουμένως είχαμε ορίσει (αξιωματικά) την ένωση και την τομή απείρου, το πλήθος συνόλων (ιδέ σελίδες 10 και 13). Εκεί είχαμε σύνολα των οποίων τα στοιχεία είναι σύνολα. Στην σελίδα 8 είχαμε αναφέρει τις οικογένειες/συλλογές συνόλων, οι οποίες δεν αποτελούν κατ' ανάγκη σύνολα. Προς αποφυγήν σύγχυσης, στο εξής ένα σύνολο, του οποίου τα στοιχεία είναι σύνολα, θα ονομάζεται **οικογένεια** συνόλων και τα στοιχεία της θα ονομάζονται μέλη της οικογένειας.

Ορισμένες φορές, όταν έχουμε μια οικογένεια συνόλων τα μέλη της τα "αριθμούμε".

[7] Πολλές φορές αναφέρεται, λανθασμένα, ότι δύο ξένα σύνολα *δεν έχουν τομή*. Δεν ξεχνάμε ότι η τομή δύο συνόλων πάντα ορίζεται.

Τι σημαίνει "αριθμούμε";
Ας δώσουμε στην αρχή ορισμένα παραδείγματα.

i. Έστω η οικογένεια συνόλων $\mathcal{A} = \{A, B, C, D\}$. Τότε μπορούμε να θέσουμε

$$A_1 = A, A_2 = B, A_3 = C, A_4 = D$$

και να έχουμε την (ίδια) οικογένεια $\mathcal{A} = \{A_1, A_2, A_3, A_4\}$.

ii. Έστω τα σύνολα $\{0, 1, 2\}, \{1, 2, 3\}, \{2, 3, 4\}, \{3, 4, 5\}$. Τα σύνολα αυτά τα αριθμούμε

$$B_1 = \{0, 1, 2\}, B_2 = \{1, 2, 3\}, B_3 = \{2, 3, 4\}, B_4 = \{3, 4, 5\}$$

και έχουμε την οικογένεια συνόλων $\mathcal{B} = \{B_1, B_2, B_3, B_4\}$.

iii. Για κάθε φυσικό αριθμό n, έστω τα σύνολα $A_n = \{n-1, n, n+1\}$, οπότε έχουμε την οικογένεια συνόλων $\mathcal{A} = \{A_1, A_2, \dots, A_n, \dots\}$.

iv. Για κάθε πραγματικό αριθμό a, έστω τα σύνολα $C_a = \{a-1, a, a+1\}$, οπότε έχουμε την οικογένεια συνόλων $\mathcal{C} = \{C_a, : a \in \mathbb{R}\}$.

Στα δύο πρώτα παραδείγματα έχουμε το σύνολο $\Lambda = \{1, 2, 3, 4\}$ και σε κάθε στοιχείο του αντιστοιχούμε ένα μέλος της οικογένειας.

Στο τρίτο παράδειγμα έχουμε το σύνολο $\mathbb{N}$ και σε κάθε στοιχείο του αντιστοιχούμε ένα μέλος της οικογένειας.

Στο τέταρτο παράδειγμα έχουμε το σύνολο των πραγματικών αριθμών $\mathbb{R}$ και σε κάθε στοιχείο του αντιστοιχούμε ένα μέλος της οικογένειας.

Στα τρία πρώτα παραδείγματα αριθμούμε τα μέλη της οικογένειας, όπως (διαισθητικά) γνωρίζουμε. Στο τέταρτο παράδειγμα η "αρίθμηση" γίνεται με την βοήθεια του συνόλου των πραγματικών αριθμών.

Μπορούμε τώρα να γενικεύσουμε. Έστω Λ ένα μη κενό σύνολο. Υποθέτουμε ότι για κάθε $a \in \Lambda$ υπάρχει (μόνο) ένα σύνολο A_a. Η οικογένεια των συνόλων

$$\mathcal{A} = \{A_a \mid a \in \Lambda\}$$

ονομάζεται μια οικογένεια **δεικνυόμενη** από το σύνολο Λ, το οποίο θα ονομάζεται **σύνολο δεικτών**. Στην περίπτωση αυτήν η οικογένεια θα συμβολίζεται και ως

$$(A_a)_{a\in\Lambda}{}^{8}.$$

Προφανώς το κενό σύνολο αποτελεί μια οικογένεια, την κενή οικογένεια. Στο εξής όλες οι οικογένειες συνόλων θα θεωρούνται μη κενές, εκτός και αν αυτό επισημαίνεται.

Αν έχουμε μια δεικνυόμενη οικογένεια συνόλων $(A_a)_{a\in\Lambda}$ με σύνολο δεικτών ένα σύνολο της μορφής $\Lambda = \{1, 2, \dots, n\}$ ή $\Lambda = \mathbb{N}$, τότε για την ένωση και την τομή των μελών της θα χρησιμοποιούμε, κατά περίπτωση, τους εξής συμβολισμούς:

$$\bigcup_{i=1}^{n} \mathrm{A}_i, \bigcup_{i=1}^{\infty} \mathrm{A}_i = \bigcup_{i\in\mathbb{N}} \mathrm{A}_i.$$

$$\bigcap_{i=1}^{n} \mathrm{A}_i, \bigcap_{i=1}^{\infty} \mathrm{A}_i = \bigcap_{i\in\mathbb{N}} \mathrm{A}_i.$$

[8] Τις περισσότερες φορές, η παράθεση του $(A_a)_{a\in\Lambda}$, και μόνο, δηλώνει ποια είναι η (δεικνυόμενη) οικογένεια και ποιο είναι το σύνολο δεικτών.

Παραδείγματα 1.1.30.

1. Έστω $\Lambda = \{1, 2, 3, 4\}$. Για $n \in \Lambda$ ορίζουμε

$$A_n = \{2n + 6, 16 - 2n\}.$$

Παρατηρούμε ότι

$$A_1 = \{8, 14\}, \quad A_2 = \{10, 12\}, \quad A_3 = \{12, 10\}, \quad A_4 = \{14, 8\}.$$

Δηλαδή $A_1 = A_4$ και $A_2 = A_3$.

2. Έστω $\Lambda = \mathbb{R}$, για κάθε $x \in \Lambda$ ορίζουμε τα σύνολα $A_x = \{0, x^2, x^4\}$. Παρατηρούμε ότι $\mathrm{A}_{-1} = \mathrm{A}_1$.

Δηλαδή, και στα δύο παραδείγματα, σε δύο διαφορετικούς δείκτες αντιστοιχεί το ίδιο σύνολο. Αυτό δεν απαγορεύεται.

Ας δούμε μερικά ακόμη παραδείγματα.

Παραδείγματα 1.1.31.

1. Έστω η οικογένεια συνόλων $A_i = \{-i, 0, i\}$, $i \in \mathbb{N}$. Είναι εύκολο να δούμε ότι

$$\bigcup_{i=1}^{\infty} \mathrm{A}_i = \mathbb{Z} \text{ και } \bigcap_{i=1}^{\infty} \mathrm{A}_i = \{0\}.$$

(Να κάνετε μια λεπτομερή αιτιολόγηση, γιατί πράγματι ισχύουν αυτές οι ισότητες συνόλων).

2. Για κάθε θετικό πραγματικό αριθμό ορίζουμε A_a να είναι το διάστημα $(-1, a]$, δηλαδή $A_a = \{x \in R \mid -1 < x \leq a\}$. Είναι εύκολο να δούμε ότι

$$\bigcup_{a \in \mathbb{R}^+} \mathrm{A}_a = (-1, \infty) = \{x \in \mathbb{R} \mid -1 < x\}$$

και

$$\bigcap_{a \in \mathbb{R}^+} \mathrm{A}_a = (-1, 0] = \{x \in \mathbb{R} \mid -1 < x \leq 0\}.$$

(Να κάνετε μια λεπτομερή αιτιολόγηση, γιατί πράγματι ισχύουν αυτές οι ισότητες συνόλων).

Θεώρημα 1.1.32. *Έστω Λ ένα μη κενό σύνολο, $\mathcal{A} = \{A_a \mid a \in \Lambda\}$ μια οικογένεια συνόλων με σύνολο δεικτών το Λ και B ένα σύνολο. Τότε ισχύουν:*

i. *Για κάθε $\beta \in \Lambda$, $\bigcap_{a \in \Lambda} A_a \subseteq A_\beta$.*

ii. *Για κάθε $\beta \in \Lambda$, $A_\beta \subseteq \bigcup_{a \in \Lambda} A_a$.*

iii. $B \cap (\bigcup_{a \in \Lambda} A_a) = \bigcup_{a \in \Lambda} (B \cap A_a)$.

iv. $B \cup (\bigcap_{a \in \Lambda} A_a) = \bigcap_{a \in \Lambda} (B \cup A_a)$.

Απόδειξη. Το *i.* και *ii.* απορρέουν από τον Ορισμό της τομής και της ένωσης συνόλων αντίστοιχα.

Το *iii.* και *iv.* είναι ο "νόμος του επιμερισμού" και έχει αποδειχθεί για τρία σύνολα στο Θεώρημα 1.1.29.

Η απόδειξη είναι ακριβώς η ίδια και στην περίπτωση μιας οικογένειας συνόλων. Να την επαναλάβετε εδώ με κάθε λεπτομέρεια. ό.έ.δ.

Συμπληρώματα συνόλων - Διαφορά συνόλων.

Ας ξεκινήσουμε με δύο παραδείγματα.

1. Έστω X το σύνολο όλων των θετικών ακεραίων, δηλαδή $X = \{1, 2, 3, 4, \dots\}$, A το σύνολο όλων των θετικών ακεραίων, οι οποίοι είναι άρτιοι, δηλαδή $A = \{2, 4, 6, \dots\}$ και B το σύνολο όλων των θετικών ακεραίων, οι οποίοι είναι περιττοί, δηλαδή $B = \{3, 5, 7, \dots\}$. Προφανώς[9] το σύνολο B θα μπορούσε να περιγραφεί ως εξής: $B = \{x \in X \mid x \notin A\}$.

2. Έστω $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ και $B = \{5, 6, 7, 8, 9, 10, 11, 12\}$. Αναζητούμε το υποσύνολο του A, το οποίο αποτελείται από τα στοιχεία, τα οποία δεν ανήκουν στο σύνολο B. Προφανώς το σύνολο αυτό είναι το σύνολο
$$\{x \in A \mid x \notin B\} = \{1, 2, 3, 4\}.$$

Στα δύο παραδείγματα έχουμε δύο σύνολα και αναζητούμε ένα τρίτο σύνολο, το οποίο περιέχει στοιχεία από το ένα σύνολο, **τα οποία** δεν ανήκουν στο άλλο σύνολο. Υπάρχει όμως μια διαφορά. Στο πρώτο παράδειγμα, το ένα από τα δυο δοθέντα σύνολα είναι υποσύνολο του άλλου συνόλου ($A \subseteq X$), ενώ στο δεύτερο παράδειγμα κανένα από τα δύο σύνολα δεν είναι υποσύνολο του άλλου ($A \nsubseteq B$ και $B \nsubseteq A$).

Ορισμός 1.1.33. Έστω X ένα σύνολο και A ένα υποσύνολό του. Το (απόλυτο) **συμπλήρωμα** του A, ως προς το X, είναι το σύνολο
$$A^c_X = \{x \in X \mid x \notin A\}.$$

Ορισμός 1.1.34. Έστω A και B δύο σύνολα. Το (σχετικό) **συμπλήρωμα** ή **διαφορά** του B, ως προς το A είναι το σύνολο
$$A \setminus B = \{x \in A \mid x \notin B\}.$$

Πριν προχωρήσουμε, ας κάνουμε μερικές παρατηρήσεις ως προς την ορολογία και την "σχέση" των δύο ορισμών.

Στον πρώτο ορισμό έχουμε ένα σύνολο X και ένα υποσύνολό του A. Το υπερσύνολο X, ως προς το οποίο λαμβάνουμε το συμπλήρωμα του A, συνήθως ονομάζεται **σύνολο αναφοράς** και, όταν δεν υπάρχει πρόβλημα για ποιο σύνολο πρόκειται, αντί του συμβολισμού A^c_X απλώς γράφουμε A^c.

Ας πάμε στον δεύτερο ορισμό. Εδώ έχουμε δύο σύνολα A και B, τα οποία δεν είναι, κατ' ανάγκη, το ένα υποσύνολο του άλλου. Σύμφωνα με τον δεύτερο ορισμό έχουμε:
$$A \setminus B = \{x \in A \mid x \notin B\}.$$

Ας θεωρήσουμε τώρα το σύνολο A ως σύνολο αναφοράς και ας πάρουμε το συμπλήρωμα του υποσυνόλου του $A \cap B$, ως προς τον πρώτο ορισμό. Τότε έχουμε
$$(A \cap B)^c_A = \{x \in A \mid x \notin A \cap B\}.$$
Είναι εύκολο να δούμε (γιατί;) ότι
$$A \setminus B = (A \cap B)^c_A.$$
Συνεπώς, η διάκριση σε απόλυτο και σχετικό συμπλήρωμα είναι "τεχνική" και στο εξής θα μπορούμε να αναφερόμαστε απλώς στο συμπλήρωμα ενός συνόλου ως προς κάποιο άλλο.

[9] Εδώ θεωρούμε προφανές, εξ εμπειρίας, το καθόλου (προς το παρόν) προφανές, ότι ένας θετικός ακέραιος είναι είτε άρτιος είτε περιττός.

Ορισμός 1.1.35. Έστω A και B δύο σύνολα. Ως **συμμετρική διαφορά** των A και B ορίζουμε το σύνολο

$$A \triangle B = (A \setminus B) \cup (B \setminus A).$$

(Ορισμένες φορές, αντί του συμβολισμού $A \triangle B$, χρησιμοποιούμε τον συμβολισμό $A \oplus B$).

Πρόταση 1.1.36. *Έστω E ένα σύνολο και $A \subseteq E$. Τότε ισχύει ότι*

$$A \cap (E \setminus \mathrm{A}) = \varnothing \text{ και } A \cup (E \setminus \mathrm{A}) = E.$$

Απόδειξη. Έστω $x \in A \cap (E \setminus \mathrm{A})$. Αυτό σημαίνει ότι $x \in A$ και $x \notin A$. Δεν ξεχνάμε όμως την παραδοχή: Ένα αντικείμενο είτε ανήκει σε ένα σύνολο είτε δεν ανήκει (σελ. 2), άρα $A \cap (E \setminus \mathrm{A}) = \varnothing$.

Προφανώς $A \cup (E \setminus \mathrm{A}) \subseteq E$.

Έστω $x \in E$. Έχουμε (πάλι από την ίδια παραδοχή) ότι, είτε $x \in A$ είτε $x \notin A$. Στην δεύτερη περίπτωση έχουμε ότι $x \in E \setminus A$. Άρα $x \in A \cup (E \setminus \mathrm{A})$. ό.έ.δ.

Πρόταση 1.1.37. *Δοθέντων δύο συνόλων A και B ισχύει ότι:*

1. $A \setminus A = \varnothing$.
2. $A \setminus \varnothing = A$.
3. $\varnothing \setminus A = \varnothing$.
4. $B \setminus A = \varnothing$, *αν και μόνο αν* $B \subseteq A$.
5. $(A \setminus B) \cap (B \setminus A) = \varnothing$.
6. $A \cap (B \setminus A) = \varnothing$.

Απόδειξη.

1. Έστω $x \in A \setminus A$, τότε από τον ορισμό της διαφοράς έχουμε ότι $x \in A$ και $x \notin A$. Δεν ξεχνάμε όμως την παραδοχή: Ένα αντικείμενο είτε ανήκει σε ένα σύνολο είτε δεν ανήκει, άρα $A \setminus A \subseteq \varnothing$.

2. Εξ ορισμού της διαφοράς συνόλων έχουμε $A \setminus \varnothing \subseteq A$.

   Έστω $x \in A$, πάντα έχουμε ότι $x \notin \varnothing$. Συνεπώς, πάλι από τον ορισμό της διαφοράς συνόλων, έχουμε ότι $x \in A \setminus \varnothing$, δηλαδή $A \subseteq A \setminus \varnothing$.

3. Από τον ορισμό της διαφοράς συνόλων έχουμε ότι $\varnothing \setminus A \subseteq \varnothing$.

   Αλλά πάντα έχουμε ότι $\varnothing \subseteq \varnothing \setminus A$.

4. Υποθέτουμε ότι

   $B \setminus A = \varnothing$. Έστω $x \in B$, υποθέτουμε ότι $x \notin A$, τότε $x \in B \setminus A = \varnothing$, άτοπο, άρα αναγκαστικά $x \in A$, δηλαδή $B \subseteq A$.

   Αντίστροφα, υποθέτουμε ότι $B \subseteq A$. Αν υπάρχει $x \in B \setminus A$, τότε από τον ορισμό της διαφοράς συνόλων έχουμε ότι $x \notin A$, άτοπο.

5. Έστω $x \in (A \setminus B) \cap (B \setminus A)$. Από τον ορισμό της τομής και της διαφοράς συνόλων έχουμε $x \in A \setminus B$ και $x \in B \setminus A$. Από την πρώτη σχέση έχουμε ότι $x \in A$ και $x \notin B$. Ταυτόχρονα από την δεύτερη σχέση έχουμε $x \in B$ και $x \notin A$, Δηλαδή, $x \in A \setminus A = \varnothing$.

6. Όπως προηγουμένως, από τον ορισμό της τομής και της διαφοράς συνόλων έχουμε $x \in A \cap (B \setminus A)$ αν και μόνο αν $x \in A$ και $x \in B \setminus A$. Από την δεύτερη σχέση έχουμε ότι $x \notin A$, δηλαδή $x \in A \setminus A = \varnothing$. ό.έ.δ.

Πρόταση 1.1.38. *Έστω E ένα σύνολο και A, B δύο υποσύνολά του, τότε ισχύει ότι:*

i. $E \setminus (E \setminus \mathrm{A}) = \mathrm{A}$.

ii. $A \subseteq B$ *αν και μόνο αν* $E \setminus B \subseteq E \setminus A$.

Απόδειξη. i. Έστω $x \in E \setminus (E \setminus \mathrm{A})$, τότε $x \in E$ και $x \notin E \setminus \mathrm{A}$. Από την Πρόταση 1.1.36 έχουμε ότι $E = A \cup (E \setminus \mathrm{A})$, συνεπώς, αφού $x \notin \mathrm{E} \setminus \mathrm{A}$, έχουμε ότι $x \in A$.

Αντίστροφα, υποθέτουμε ότι $x \in A$. Τότε, πάλι από την Πρόταση 1.1.36 έχουμε ότι $x \notin E \setminus \mathrm{A}$. Αυτό σημαίνει ότι $x \in E \setminus (E \setminus \mathrm{A})$.

ii. Υποθέτουμε ότι $A \subseteq B$. Έστω $x \in E \setminus B$, δηλαδή $x \notin B$, συνεπώς $x \notin A$ (αφού $A \subseteq B$). Άρα $x \in E \setminus A$.

Υποθέτουμε ότι $E \setminus B \subseteq E \setminus A$. Έστω $x \in A$, τότε, από την Πρόταση 1.1.36, έπεται ότι $x \notin E \setminus A$, δηλαδή $x \notin E \setminus B$, Οπότε, πάλι από την Πρόταση 1.1.36, έχουμε ότι $x \in B$. Τέλος. ό.έ.δ.

Πρόταση 1.1.39. *(Ο νόμος του Morgan ως προς τα συμπληρώματα συνόλων).*
Έστω E ένα σύνολο και A, B δύο υποσύνολά του, τότε ισχύει ότι:

i. $\mathrm{E} \setminus (A \cap B) = (E \setminus A) \cup (E \setminus B)$.

ii. $E \setminus (A \cup B) = (E \setminus A) \cap (E \setminus B)$.

Απόδειξη. i. Έστω $x \in E \setminus (A \cap B)$. Αυτό σημαίνει ότι $x \notin A \cap B$. Από την σχέση αυτή έχουμε ότι $x \notin A$ ή $x \notin B$. Αν $x \notin A$, τότε από την Πρόταση 1.1.36, έχουμε $x \in E \setminus A$. Αν $x \notin B$, τότε έχουμε $x \in E \setminus \mathrm{B}$. Άρα $x \in E \setminus A$ ή $x \in E \setminus \mathrm{B}$. Δηλαδή $E \setminus (A \cap B) \subseteq (E \setminus A) \cup (E \setminus B)$.

Έστω $x \in (E \setminus A) \cup (E \setminus B)$, τότε $x \notin A$ ή $x \notin B$. Αν $x \notin A$, τότε $x \in E \setminus A \subseteq E \setminus (A \cap B)$ (αφού ισχύει το *ii*) της προηγουμένης πρότασης). Όμοια, αν $x \notin B$, έπεται ότι $x \in E \setminus (A \cap B)$. Άρα $(E \setminus A) \cup (E \setminus B) \subseteq E \setminus (A \cap B)$.

ii. Θέτουμε στην θέση του συνόλου A το σύνολο $E \setminus A$ και στην θέση του συνόλου B το σύνολο $E \setminus B$, εφαρμόζουμε το *i*) λαμβάνοντας υπόψιν ότι ισχύει το *i*) της προηγουμένης πρότασης. Οπότε, έπεται το ζητούμενο. (Να συμπληρωθούν οι τεχνικές λεπτομέρειες από τον αναγνώστη). ό.έ.δ.

Σχόλιο 1.1.40. Στις προηγούμενες προτάσεις, όπου είχαμε $A, B \subseteq E$, θα μπορούσαμε να χρησιμοποιήσουμε τον συμβολισμό του συμπληρώματος (ως προς σύνολο αναφοράς το E) και να έχουμε, για παράδειγμα, τον νόμο του Morgan εκφρασμένον ως εξής:

i. $(A \cap B)^c = A^c \cup B^c$.

ii. $(A \cup B)^c = A^c \cap B^c$.

Παρατήρηση 1.1.41. Στην απόδειξη της προηγουμένης πρότασης, αν παρατηρήσουμε με προσοχή, πουθενά δεν χρησιμοποιούμε ότι τα σύνολα A και B είναι υποσύνολα ενός (κοινού) συνόλου E. Επομένως, μπορούμε να γενικεύσουμε τον νόμο του Morgan.

Πρόταση 1.1.42. *Έστω τρία σύνολα A, B, C. Τότε ισχύει ότι:*

i. $C \setminus (A \cap B) = (C \setminus A) \cup C \setminus B)$.

ii. $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$.

Απόδειξη. Η απόδειξη είναι ακριβώς η ίδια με την προηγουμένη. Απλώς να την επαναλάβετε. ό.έ.δ.

Έχοντας υπόψιν τα προηγούμενα (ιδέ και το σχόλιο μετά τους Ορισμούς 1.1.33 και 1.1.34), μπορούμε να έχουμε τις δύο "εκδοχές" του νόμου του Morgan στην πλέον γενική μορφή.

Θεώρημα 1.1.43. *Έστω Λ ένα μη κενό σύνολο, $\mathcal{A} = \{A_a \mid a \in \Lambda\}$ μια οικογένεια συνόλων με σύνολο δεικτών το Λ και B ένα σύνολο. Τότε ισχύουν:*

i. $(\bigcap_{a\in\Lambda} A_a)^c = \bigcup_{a\in\Lambda} A_a^c$.

ii. $(\bigcup_{a\in\Lambda} A_a)^c = \bigcap_{a\in\Lambda} A_a^c$.

iii. $B \setminus (\bigcup_{a\in\Lambda} A_a) = \bigcap_{a\in\Lambda} (B \setminus A_a)$.

iv. $B \setminus (\bigcap_{a\in\Lambda} A_a) = \bigcup_{a\in\Lambda} (B \setminus A_a)$.

Απόδειξη. Η απόδειξη, μετά τα προηγηθέντα, είναι πλέον προφανής. Απλώς να την επαναλάβετε. ό.έ.δ.

1.1.3 Ασκήσεις

Πρόβλημα 1: Θεωρούμε τον γηραιότερο Μαθηματικό μεταξύ των σκακιστών και τον γηραιότερο σκακιστή μεταξύ των Μαθηματικών. Πρόκειται για το ίδιο πρόσωπο;

Πρόβλημα 2: Το ένα δέκατο των Μαθηματικών είναι σκακιστές, ενώ το ένα έκτο των σκακιστών είναι Μαθηματικοί. Ποιοι είναι οι περισσότεροι, οι Μαθηματικοί ή οι σκακιστές;

Συμβολισμός: Έστω a, b δύο πραγματικοί αριθμοί με $a \leq b$, Τότε θα συμβολίζουμε

$$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\} \text{ και } (a, b) = \{x \in \mathbb{R} \mid a < x < b\}^{10}.$$

1. Δείξτε ότι $A \subseteq B$, αν και μόνο αν $A \cap B = A$, αν και μόνο αν $A \cup B = B$, αν και μόνο αν $A \setminus B = \emptyset$.

2. Δίνονται τα σύνολα

$$A = \{1, 2, 3, 4, 5, 6\}, \quad B = \{4, 5, 6, 7, 8, 9\}, \quad C = \{2, 4, 6, 8\},$$
$$D = \{1, 4, 5\}, \quad E = \{5, 6\}, \quad F = \{4, 6\}$$

και ένα σύνολο X, το οποίο ικανοποιεί τις συνθήκες: $X \subseteq A$, $X \subseteq B$ και $X \nsubseteq C$. Ποιο από τα σύνολα A, B, C, D, E, F είναι το σύνολο X;

[10] Πρόκειται για τα "γνωστά" κλειστά και ανοικτά διαστήματα πραγματικών αριθμών.

3. Ποιο από τα σύνολα

$$\{x \mid \text{ο } x \text{ είναι περιττός ακέραιος και } x^2 = 2\},$$
$$\{x \mid \text{ο } x \text{ είναι ακέραιος και } x + 8 = 8\},$$
$$\{x \mid \text{ο } x \text{ είναι θετικός ακέραιος και } x < 1\}$$

είναι το κενό σύνολο;

4. Δίνονται τα σύνολα $A = \{(x, x^2) \in \mathbb{R}^2\}$ και $B = \{(x, x+2) \in \mathbb{R}^2\}$.

Να υπολογίσετε τα σύνολα $A \cup B$, $A \cap B$ και $A \setminus B$.

Μπορείτε να "αναπαραστήσετε γραφικά" τα σύνολα αυτά στο επίπεδο;

5. Δίνονται τα σύνολα A, B, C. Να δείξετε ότι:

(α) $A \setminus B = (A \cup B) \setminus B = A \setminus (A \cap B)$.

(β) $A \cap B = A \setminus (A \setminus B)$.

(γ) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.

(δ) $A \triangle B = (A \cup B) \setminus (A \cap B)$.

(Σε πολλά εγχειρίδια δίνεται αυτός ως ορισμός της συμμετρικής διαφοράς, αντί του Ορισμού 1.1.35).

6. Δείξτε ότι $A = B$, αν και μόνο αν $A \triangle B = \varnothing$.

7. Δείξτε ότι $A \triangle (B \triangle C) = (A \triangle B) \triangle C$.

(Η προσεταιριστικότητα της συμμετρικής διαφοράς).

8. Δείξτε ότι $(A_1 \cap A_2) \triangle (B_1 \cap B_2) = (A_1 \triangle B_1) \cup (A_2 \triangle B_1) \cup (A_1 \triangle B_2) \cup (A_2 \triangle B_2)$.

9. Δείξτε ότι $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

10. Στην Πρόταση 1.1.39 είχαμε δει ότι η διαφορά συνόλων επιμερίζεται ως προς την τομή και την ένωση. Ισχύει το αντίστροφο; Δηλαδή η τομή και η ένωση επιμερίζονται ως προς την διαφορά συνόλων; Συγκεκριμένα εξετάστε αν ισχύουν οι σχέσεις

$$A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C).$$
$$A \cup (B \setminus C) = (A \cup B) \setminus (A \cup C).$$

11. Δίνονται τα σύνολα $A = \{a, b, c, d\}$, $B = \{d, e, f\}$, $C = \{1, 2, 3\}$.

Να υπολογίσετε τα σύνολα $(A \setminus B) \cup (B \setminus A)$ και $(A \cap C) \cup (A \setminus C)$.

12. Να δώσετε έναν άλλο τρόπο "περιγραφής" των εξής συνόλων:

$$A = \{x \in \mathbb{R} \mid x^2 = 1\},$$
$$B = \{x \in \mathbb{Z} \mid x > -2 \text{ και } x \leq 3\},$$
$$C = \{r \in \mathbb{N} \text{ και } r^2 - 5r + 6 = 0\}.$$

13. Θεωρούμε τα σύνολα

$$A = \{x \in \mathbb{Z} \mid \ x = 2(y-2), \text{ όπου } y \in \mathbb{Z}\}$$

και

$$B = \{x \in \mathbb{Z} \mid \ x = 2z, \text{ όπου } z \in \mathbb{Z}\}.$$

Εξετάστε αν $A = B$.

14. Να υπολογίσετε τα σύνολα $\bigcap_{n\in\mathbb{N}}[-1/n, 1/n]$ και $\bigcup_{n\in\mathbb{N}}[-1/n, 1/n]$.

15. Να υπολογίσετε τα σύνολα $\bigcap_{n\in\mathbb{N}}[n, n+1]$ και $\bigcup_{n\in\mathbb{N}}[n, n+1]$.

16. Έστω A και B δύο υποσύνολα του συνόλου E. Δείξτε ότι:

(α) $A \setminus B = A \cap B^c$.
(β) $(A \setminus B)^c = A^c \cup B$.
(γ) $B \setminus (B \setminus A) = A \Leftrightarrow A \subseteq B$.

17. Έστω $A_1, A_2 \ldots, A_n$ και B υποσύνολα του συνόλου E. Δείξτε ότι:

$$B \setminus \left(\bigcap_{i=1}^{n} A_i\right) = \bigcup_{i=1}^{n} (B \setminus A_i) \qquad \text{και} \qquad B \setminus \left(\bigcup_{i=1}^{n} A_i\right) = \bigcap_{i=1}^{n} (B \setminus A_i)$$

είναι το θεώρημα 1.1.43.

18. Ποιες από τις ακόλουθες σχέσεις είναι αληθείς:

$\varnothing \in \{\varnothing\}$.

$\varnothing \subseteq \{\varnothing\}$.

19. Να ολοκληρώσετε, με κάθε λεπτομέρεια, την απόδειξη του Θεωρήματος 1.1.18.

20. Να αποδείξετε, με κάθε λεπτομέρεια, τις Προτάσεις 1.1.19 και 1.1.20.

21. Να αποδείξετε, με κάθε λεπτομέρεια, το Θεώρημα 1.1.25.

22. Στο αξίωμα της τομής (σελ. 13) είχαμε υποθέσει ότι στην τομή μετέχει τουλάχιστον ένα σύνολο. Θα μπορούσαμε να ορίσουμε την $\cap(\varnothing)$;

(Προσοχή! Έχουμε αποδεχθεί ότι δεν υπάρχει σύνολο, το οποίο να περιέχει "τα πάντα").

1.1.4 Το δυναμοσύνολο ενός συνόλου

Στην μελέτη ενός συνόλου, συνήθως, μας ενδιαφέρει να έχουμε μια "εικόνα" των υποσυνόλων του ως "ολότητα". Το πρώτο που μας ενδιαφέρει είναι, αν αυτή η ολότητα αποτελεί σύνολο. Στην περίπτωση ενός συνόλου με πεπερασμένο το πλήθος στοιχεία είναι αρκετό το αξίωμα του εγκλεισμού (σελ. 9), για να δούμε ότι όλα τα υποσύνολα ενός συνόλου με πεπερασμένο το πλήθος στοιχεία αποτελούν ένα σύνολο. Στην περίπτωση ενός τυχαίου συνόλου είμαστε αναγκασμένοι να το δεχθούμε ως αξίωμα.

***Έστω** A **ένα σύνολο. Η "ολότητα" των υποσυνόλων του αποτελεί σύνολο, το οποίο θα συμβολίζουμε με** $\mathcal{P}(A)$ **και θα ονομάζεται δυναμοσύνολο του συνόλου** A.*
(Αξίωμα του δυναμοσυνόλου).

Προφανώς, για κάθε σύνολο A, ισχύει $\varnothing, A \in \mathcal{P}(A)$. Παράλληλα $\varnothing \subseteq \mathcal{P}(A)$, ενώ γενικά $A \not\subseteq \mathcal{P}(A)$.

Προφανώς

$$\begin{aligned}\mathcal{P}\{\varnothing\} &= \varnothing.\\ \mathcal{P}(\{a\}) &= \{\varnothing, \{a\}\}.\\ \mathcal{P}(\{a, b\}) &= \{\varnothing, \{a\}, \{b\}, \{a, b\}\}.\end{aligned}$$

Γενικά είναι δύσκολο (αλλά όχι ακατόρθωτο) να προσδιορίσουμε τα υποσύνολα ενός συνόλου με πεπερασμένο το πλήθος στοιχεία. Γνωρίζουμε όμως πόσα είναι.

Πρόταση 1.1.44. *Το πλήθος των υποσυνόλων ενός συνόλου A, το οποίο έχει n το πλήθος στοιχεία, ισούται με 2^n.*

Εδώ θα δώσουμε μια πρώτη απόδειξη αυτού του αποτελέσματος, η οποία "*πάσχει*" δεδομένου ότι είναι περισσότερο διαισθητική, παρά "φορμαλιστική". Αργότερα θα επανέλθουμε δίνοντας περισσότερες της μίας αποδείξεις.

Απόδειξη. Για να σχηματίσουμε ένα υποσύνολο του συνόλου A, πρέπει να μπορούμε να αποφανθούμε αν ένα στοιχείο του A ανήκει ή δεν ανήκει στο υποσύνολο αυτό. Επομένως, έχουμε δύο επιλογές:

- Ένα στοιχείο ανήκει στο υποσύνολο.
- Ένα στοιχείο δεν ανήκει στο υποσύνολο.

Επειδή έχουμε n το πλήθος στοιχεία και για κάθε στοιχείο υπάρχουν 2 επιλογές, έχουμε ότι υπάρχουν $\underbrace{2 \times 2 \times \cdots \times 2}_{n} = 2^n$ το πλήθος υποσύνολα.

Εδώ δεν πρέπει να ξεχνάμε την Πρόταση 1.1.36. ό.έ.δ.

Παρατήρηση 1.1.45. Το δυναμοσύνολο ενός συνόλου A, από τον ορισμό του, είναι μια οικογένεια συνόλων, της οποίας μέλη είναι τα υποσύνολα του συνόλου A. Επομένως, ορίζεται η τομή και η ένωση οσωνδήποτε υποσυνόλων του A. Ιδέ το αξίωμα της ένωσης (σελ. 11) και το αξίωμα της τομής (σελ. 13).

Στην συγκεκριμένη περίπτωση, όπου όλα τα σύνολα είναι υποσύνολα του ιδίου συνόλου A, μπορούμε να ορίσουμε την ένωση και την τομή οσωνδήποτε υποσυνόλων του, αποφεύγοντας την χρήση αυτών των αξιωμάτων, χρησιμοποιώντας (μόνο) το αξίωμα του προσδιορισμού και το αξίωμα του δυναμοσυνόλου.

Πράγματι, έστω $\mathcal{A} \subseteq \mathcal{P}(A)$, τότε το σύνολο

$$\bigcup_{B \in \mathcal{A}} B = \{x \in A \mid \ x \in B \text{ για κάποιο } B \in \mathcal{A}\}$$

υπάρχει, από το αξίωμα του προσδιορισμού και είναι η ένωση των στοιχείων του συνόλου $\mathcal{A}$.

Όμοια έχουμε την τομή

$$\bigcap_{B\in\mathcal{A}} B = \{\, x \in A \mid \ x \in B \text{ για όλα τα } B \in \mathcal{A} \,\}$$

των στοιχείων του συνόλου $\mathcal{A}$.

Προφανώς (γιατί;) $\bigcup_{B\in\mathcal{P}(A)} B = A$ και $\bigcap_{B\in\mathcal{P}(A)} B = \emptyset$.

Πρόταση 1.1.46. *Δοθέντων δύο συνόλων A και B, ισχύει ότι*

$$A \subseteq B \text{ αν και μόνο αν } \mathcal{P}(A) \subseteq \mathcal{P}(B).$$

Απόδειξη. Έστω $A \subseteq B$ και $C \in \mathcal{P}(A)$, δηλαδή $C \subseteq A$, τότε $C \subseteq B$, δηλαδή $C \in \mathcal{P}(B)$.

Αντίστροφα, υποθέτουμε ότι $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Έστω $a \in A$, τότε $\{a\} \in \mathcal{P}(A) \subseteq \mathcal{P}(B)$, δηλαδή $\{a\} \subseteq B$, το οποίο σημαίνει ότι $a \in B$. ό.έ.δ.

Πρόταση 1.1.47. *Δοθέντων δύο συνόλων A και B, ισχύει ότι:*

$$\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B).$$
$$\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B).$$

Απόδειξη. Έστω $C \in \mathcal{P}(A \cap B)$, δηλαδή $C \subseteq A \cap B$. Αυτό σημαίνει ότι $C \subseteq A$ και $C \subseteq B$. Συνεπώς

$$C \in \mathcal{P}(A) \cap \mathcal{P}(B).$$

Αντίστροφα, έστω $C \in \mathcal{P}(A) \cap \mathcal{P}(B)$. Τότε $C \in \mathcal{P}(A)$ και $C \in \mathcal{P}(B)$, δηλαδή $C \subseteq A$ και $C \subseteq B$. Άρα $C \subseteq A \cap B$, επομένως $C \in \mathcal{P}(A \cap B)$.

Έστω $C \in \mathcal{P}(A) \cup \mathcal{P}(B)$, τότε $C \subseteq A \subseteq A \cup B$ ή $C \subseteq B \subseteq A \cup B$. Επομένως, πάντα

$$C \in \mathcal{P}(A \cup B).$$ ό.έ.δ.

Παρατήρηση 1.1.48. Στην προηγούμενη πρόταση έχουμε αποδείξει

$$\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B),$$

αλλά δεν αποδείξαμε την αντίστροφη σχέση εγκλεισμού, κάτι που αποδείξαμε στην περίπτωση της τομής συνόλων.

Μπορείτε να αποδείξετε (δίνοντας ένα αντιπαράδειγμα) ότι δεν ισχύει η αντίστροφη σχέση εγκλεισμού;

Μπορείτε να δώσετε συνθήκη ώστε να ισχύει η αντίστροφη σχέση εγκλεισμού;

Μια πολύ σημαντική έννοια στα σύνολα και γενικότερα σε όλα τα Μαθηματικά είναι η έννοια της διαμέρισης ενός συνόλου.

Ορισμός 1.1.49. Έστω ένα σύνολο A. Ένα υποσύνολο $\mathcal{D} \subseteq \mathcal{P}(A)$ θα ονομάζεται **διαμέριση** του συνόλου A, αν ισχύουν τα ακόλουθα:

- $\emptyset \notin \mathcal{D}$.
- $\bigcup_{B\in\mathcal{D}} B = A$.
- $B \cap C = \emptyset$, για δύο διαφορετικά $B, C \in \mathcal{D}$.

Δηλαδή το υποσύνολο $\mathcal{D} \subseteq \mathcal{P}(A)$ αποτελεί διαμέριση του συνόλου A, αν και μόνο αν τα στοιχεία του είναι μη κενά και κάθε στοιχείο του A ανήκει σε ακριβώς ένα από τα στοιχεία του $\mathcal{D}$.

Προφανώς, από τον ορισμό, για το κενό σύνολο δεν υπάρχει διαμέριση. Επίσης, τα

$$\mathcal{D}_1 = \{A\} \text{ και } \mathcal{D}_2 = \{\{x\} \mid \text{για όλα τα } x \in A\}$$

αποτελούν διαμερίσεις του (μη κενού) συνόλου A.

Ένα ενδιαφέρον πρόβλημα είναι το εξής:

> Δοθέντος ενός συνόλου, είναι δυνατόν να προσδιορίσουμε όλες τις διαμερίσεις του;

Επ' αυτού θα επανέλθουμε αργότερα.

Παραδείγματα 1.1.50.

i. Όλες οι διαμερίσεις του συνόλου $A = \{a, b, c\}$ είναι οι εξής:

$$\mathcal{D}_1 = \{\{a, b, c\}\}, \quad \mathcal{D}_2 = \{\{a\}, \{b\}, \{c\}\}, \quad \mathcal{D}_3 = \{\{a, b\}, \{c\}\},$$
$$\mathcal{D}_4 = \{\{a, c\}, \{b\}\}, \quad \mathcal{D}_5 = \{\{b, c\}, \{a\}\}.$$

ii. Έστω $\mathbb{Z} = \{\cdots, -3, -2, -1, 0, +1, +2, +3, \cdots\}$ το σύνολο των ακεραίων αριθμών και τα εξής υποσύνολά του.

$$A = \{r \in \mathbb{Z} \mid r \text{ άρτιος}\}, \quad \mathrm{B} = \{r \in \mathbb{Z} \mid r \text{ περιττός}\},$$
$$C = \{r \in \mathbb{Z} \mid r \text{ αρνητικός}\}, \quad D = \{r \in \mathbb{Z} \mid r \text{ θετικός}\}.$$

Δύο διαμερίσεις του συνόλου $\mathbb{Z}$ είναι οι εξής:

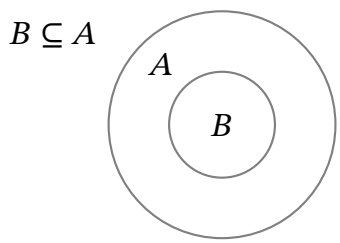
$$\mathcal{D}_1 = \{\mathrm{A}, B\}, \quad \mathcal{D}_2 = \{C, D, \{0\}\}.$$

Διαγράμματα του Venn.

Ένας παραστατικός τρόπος παρουσίασης των συνόλων, ο οποίος, αν και εποπτικός και χωρίς αποδείξεις, είναι πολύ χρήσιμος στην κατανόηση των σχετικών εννοιών, όπως είναι η έννοια του υποσυνόλου, της τομής, της ένωσης και της διαφοράς συνόλων.

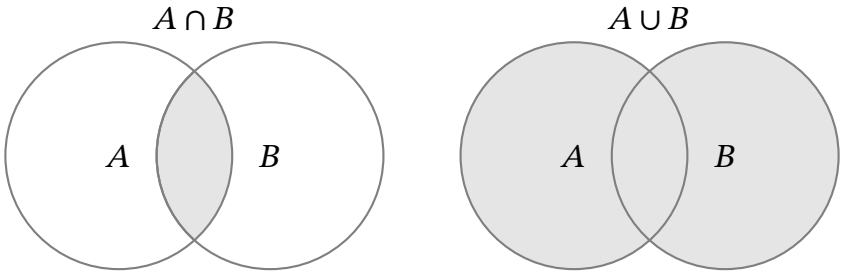
Η ιδέα είναι απλή, παριστάνουμε ένα σύνολο με ένα τμήμα του επιπέδου περικλειόμενου από μια απλή κλειστή γραμμή, συνήθως έναν κύκλο.

Στο σχήμα 1.1 παρουσιάζεται εποπτικά η έννοια του συνόλου και του υποσυνόλου.

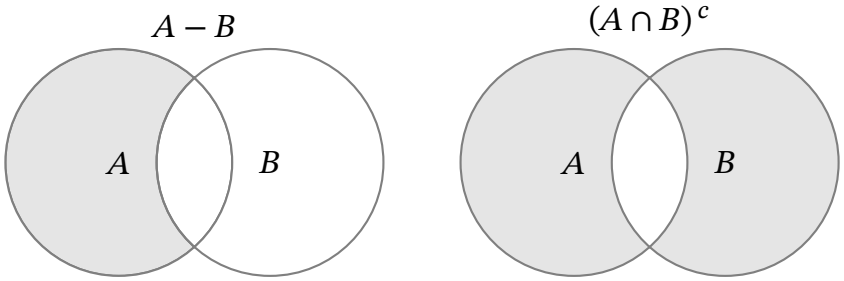


Σχήμα 1.1: *Διάγραμμα Venn υποσυνόλου.*

Στο σχήμα 1.2 παρουσιάζεται εποπτικά η έννοια της ένωσης και της τομής δύο συνόλων.



Σχήμα 1.2: *Διαγράμματα Venn ένωσης και τομής.*

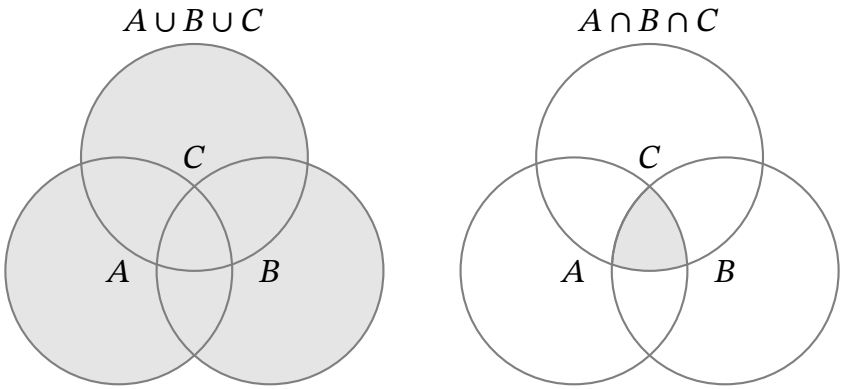


Σχήμα 1.3: *Διαγράμματα Venn διαφοράς και συμπληρώματος τομής.*

Στο σχήμα 1.3 παρουσιάζεται εποπτικά η έννοια της συνολοθεωρητικής διαφοράς $A - B$ δύο συνόλων. Επίσης, παρουσιάζεται και η έννοια του συμπληρώματος της τομής δύο συνόλων $(A \cap B)^c$ που είναι γνωστή και ως αποκλειστική διάζευξη δηλαδή

$$A \text{ ή } B \text{ αλλά όχι } (A \text{ και } B).$$

Στο σχήμα 1.4 παρουσιάζεται εποπτικά η έννοια της ένωσης και της τομής τριών συνόλων.



Σχήμα 1.4: *Διαγράμματα Venn ένωσης και τομής.*

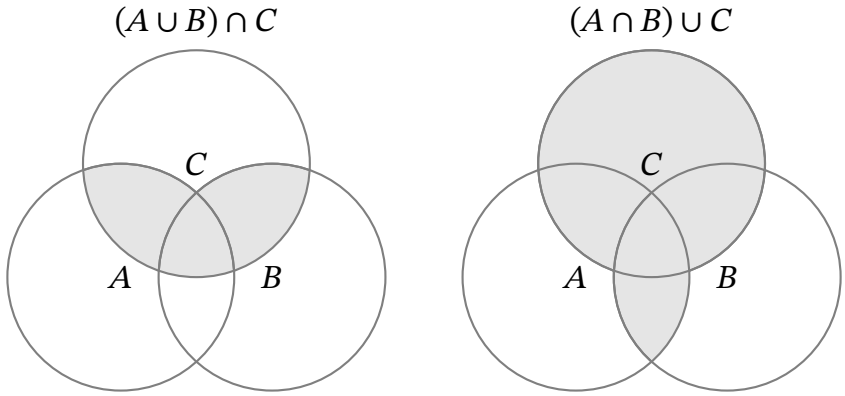
Στο σχήμα 1.5 εμφανίζεται γραμμοσκιασμένη η τομή μίας ένωσης συνόλων με τρίτο σύνολο, δηλαδή το σύνολο

$$(A \cup B) \cap C.$$

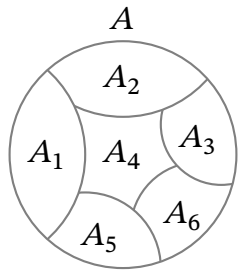
Επίσης, εμφανίζεται γραμμοσκιασμένη και η ένωση της τομής δύο συνόλων με τρίτο σύνολο, δηλαδή το σύνολο

$$(A \cap B) \cup C.$$

Το σχήμα 1.6 αποτελεί παράδειγμα διαμέρισης συνόλου με την χρήση διαγραμμάτων του Venn.



Σχήμα 1.5: *Διαγράμματα Venn.*



Σχήμα 1.6: *Διαμέριση συνόλου.*

1.1.5 Ασκήσεις

1. Δίνονται τα σύνολα $A = \{a, b, c\}$ και $B = \{c, d\}$.
   Να υπολογίσετε τα σύνολα

$$\mathcal{P}(A \cap B),\ \mathcal{P}(A) \cap \mathcal{P}(B),$$
$$\mathcal{P}(A) \cup \mathcal{P}(B),\ \mathcal{P}(A \cup B),$$
$$\mathcal{P}(A \setminus B),\ \mathcal{P}(A) \setminus \mathcal{P}(B).$$

2. Δίνεται ένα σύνολο A με 3 το πλήθος στοιχεία.
   Να υπολογίσετε το πλήθος των στοιχείων του συνόλου $\mathcal{P}(\mathcal{P}(A))$.

3. Να υπολογίσετε το δυναμοσύνολο $\mathcal{P}(\{\emptyset, \{1, 2\}\})$.

4. Να υπολογίσετε το δυναμοσύνολο $\mathcal{P}(\mathcal{P}(\{2\}))$.

5. Να υπολογίσετε το σύνολο $\mathcal{P}(\{\{a, b\}\}, \{c\})$.

6. Να υπολογίσετε τα σύνολα

$$\{X \in \mathcal{P}(\{1, 2, 3\}) : |X| \leq 1\}.$$
$$\{X \subseteq \mathcal{P}(\{1, 2, 3\}) : |X| \leq 1\}.$$
$$\{X \in \mathcal{P}(\{1, 2, 3\}) : 2 \in X\}.$$

7. Να βρείτε όλες τις διαμερίσεις των συνόλων $A = \{1, 2, 3, 4\}$ και $B = \{a, b, c, d\}$.
   Τι παρατηρείτε;

8. Να προσδιορίσετε (τουλάχιστον) τρεις διαμερίσεις του συνόλου των ακεραίων αριθμών.

9. Έστω A, B, C τρία σύνολα. Χρησιμοποιώντας διαγράμματα Venn να επαληθεύσετε τις ισότητες

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \text{ και } A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

(Ιδέ Θεώρημα 1.1.29).

10. Έστω A, $B \subseteq E$. Έχοντας ως σύνολο αναφοράς το σύνολο E, με την βοήθεια των διαγραμμάτων του Venn, να επαληθεύσετε τον νόμο του Morgan

(i) $(A \cap B)^c = A^c \cup B^c$.

(ii) $(A \cup B)^c = A^c \cap B^c$.

(Ιδέ Πρόταση 1.1.39).

1.1.6 Διατεταγμένα ζεύγη - Καρτεσιανά γινόμενα συνόλων

Στην σελίδα 4 είχαμε δει την ύπαρξη μονοσυνόλων. Με την βοήθεια της έννοιας της ένωσης συνόλων μπορούμε να προχωρήσουμε στην έννοια του μη διατεταγμένου ζεύγους και κατόπιν στην έννοια του διατεταγμένου ζεύγους.

Έστω a, b δύο αντικείμενα, τότε ορίζεται η ένωση

$$\{a\} \cup \{b\} = \{a, b\}$$

και το σύνολο $\{a, b\}$ ονομάζεται το ζεύγος των αντικειμένων a και b. Δεδομένου δε ότι

$$\{a\} \cup \{b\} = \{b\} \cup \{a\} = \{a, b\} = \{b, a\},$$

έχουμε ένα **μη** διατεταγμένο ζεύγος.

Η διαδικασία αυτή θα μπορούσε να επαναληφθεί και να επιτύχουμε (μη διατεταγμένες) τριάδες ως εξής:

$$\{a, b, c\} = \{a, b\} \cup \{c\}$$

και ούτω καθ' εξής να επιτύχουμε n-άδες ως

$$\{a_1, a_2, \ldots, a_{n-1}, a_n\} = \{a_1, a_2, \ldots, a_{n-1}\} \cup \{a_n\}.$$

Ορισμένες φορές όμως είναι αναγκαίο να προκαθορίσουμε την διάταξη των στοιχείων a και b, τα οποία εμφανίζονται στο ζεύγος $\{a, b\}$. Επικαλούμενοι την εμπειρία μας, για παράδειγμα, το σημείο του επιπέδου με συντεταγμένες (1, 2) είναι διαφορετικό από το σημείο με συντεταγμένες (2, 1).

Διαισθητικά θα μπορούσαμε να ορίσουμε το διατεταγμένο ζεύγος δύο αντικειμένων ως:

> *Διατεταγμένο ζεύγος δύο στοιχείων a και b είναι ένα σύνολο $\{a, b\}$, όπου έχουμε* ***προκαθορίσει*** *την σειρά εμφάνισης/αναγραφής των στοιχείων του.*

Όπως βλέπουμε, ένας τέτοιος "ορισμός" δημιουργεί παρερμηνείες. Για παράδειγμα, τι σημαίνει "σειρά εμφάνισης"; Τι σημαίνει δύο διατεταγμένα ζεύγη είναι ίσα; Το αξίωμα της έκτασης μας εξασφαλίζει πότε τα σύνολα (μη διατεταγμένα ζεύγη) $\{a, b\}$ είναι $\{c, d, \}$ ίσα. Με τον προηγούμενο "ορισμό" του διατεταγμένου ζεύγους δεν μπορεί να μας εξασφαλίσει πότε δύο διατεταγμένα ζεύγη είναι ίσα.

Εδώ δεν χρειάζεται να αποδεχθούμε ένα νέο αξίωμα. Αρκεί να διατυπώσουμε έναν "καλό ορισμό".

Ορισμός 1.1.51. [11]

Έστω τα αντικείμενα a και b. Το σύνολο $(a, b) = \{\{a\}, \{a, b\}\}$ θα ονομάζεται το **διατεταγμένο ζεύγος** των a και b. Το a θα ονομάζεται η πρώτη συντεταγμένη του ζεύγους και το b η δεύτερη συντεταγμένη.

Θεώρημα 1.1.52. *Δύο ζεύγη (a, b) και (c, d) είναι ίσα αν και μόνο αν $a = c$ και $b = d$.*

Απόδειξη. Υποθέτουμε ότι $a = c$ και $b = d$. Τότε προφανώς $\{a\} = \{c\}$ και $\{a, b\} = \{c, d\}$ συνεπώς

$$(a, b) = \{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\} = (c, d).$$

Αντίστροφα, υποθέτουμε ότι

$$(a, b) = \{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\} = (c, d).$$

Από το αξίωμα ισότητας συνόλων (αξίωμα έκτασης) έχουμε ότι $\{a\} = \{c\}$ ή $\{a\} = \{c, d\}$.

Υποθέτουμε ότι $\{a\} = \{c\}$, τότε, επειδή, στην περίπτωση αυτή, αναγκαστικά θα έχουμε $\{a, b\} = \{c, d\}$, έπεται ότι $b = d$ και τέλος.

Υποθέτουμε ότι $\{a\} = \{c, d\}$, τότε θα έχουμε $a = c = d$. Αλλά, επειδή στην περίπτωση αυτή θα έχουμε αναγκαστικά ότι $\{a, b\} = \{c\}$, έπεται ότι $a = b = c$. Δηλαδή τελικά $a = b = c = d$ και τέλος. ό.έ.δ.

Επαναληπτικά μπορούμε να ορίσουμε την διατεταγμένη τριάδα ως εξής:

> Έστω a, b, c τρία αντικείμενα. Τότε ορίζεται η διατεταγμένη τριάδα ως εξής:
> $$(a, b, c) = ((a, b), c).$$

Πρόταση 1.1.53. *Δύο διατεταγμένες τριάδες (a, b, c) και (d, e, f) είναι ίσες αν και μόνο αν $a = d$, $b = e$, $c = f$.*

Απόδειξη. Η απόδειξη αποτελεί εφαρμογή του προηγουμένου θεωρήματος και αφήνεται ως άσκηση. ό.έ.δ.

Με συνεχείς επαναλήψεις μπορούμε να ορίσουμε την διατεταγμένη n-άδα

$$(a_1, a_2, \ldots, a_{n-1}, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n) \text{ για } n \geq 3.$$

Παρατήρηση 1.1.54. Πρέπει να είμαστε προσεκτικοί στον ορισμό της διατεταγμένης τριάδας και γενικότερα της διατεταγμένης n-άδας. **Δεν** ισχύει ότι

$$((a, b), c) = (a, (b, c)) \text{ (γιατί;)}.$$

Πολλοί θέτουν $(a, b, c) = (a, (b, c))$, αλλά το τηρούν στα επόμενα.

[11] Ο ορισμός αυτός εδόθη από τον Πολωνό Μαθηματικό K. Kuratowski (1896-1980). Υπάρχουν και άλλοι "καλοί ορισμοί" του διατεταγμένου ζεύγους.

Καρτεσιανά γινόμενα.

Έχοντας ορίσει την έννοια του διατεταγμένου ζεύγους, μπορούμε να ορίσουμε το καρτεσιανό γινόμενο δύο συνόλων.

Ορισμός 1.1.55. Δοθέντων των συνόλων A και B, το σύνολο όλων των διατεταγμένων ζευγών (a, b), όπου $a \in A$ και $b \in B$ θα ονομάζεται **καρτεσιανό** γινόμενο των συνόλων A και B[12].

Πριν προχωρήσουμε θα θέλαμε να παρατηρήσουμε ότι **δεν** είναι προφανές ότι η "ολότητα" των διατεταγμένων ζευγών (a, b), όπου $a \in A$ και $b \in B$, αποτελεί σύνολο. Σε πολλά εγχειρίδια αυτό θεωρείται προφανές. Σε άλλα τίθεται ως ένα (επιπλέον) αξίωμα.

Θα αποδείξουμε ότι, με τα μέχρι τούδε αξιώματα, πράγματι το καρτεσιανό γινόμενο δύο συνόλων υπάρχει ως σύνολο.

Έστω A και B δύο σύνολα. Λαμβάνουμε το δυναμοσύνολο της ένωσής τους $\mathcal{P}(A \cup B)$. Κατόπιν λαμβάνουμε το δυναμοσύνολο αυτού του δυναμοσυνόλου, δηλαδή το $\mathcal{P}(\mathcal{P}(A \cup B))$. Θεωρούμε το διατεταγμένο ζεύγος $(a, b) = \{\{a\}, \{a, b\}\}$, όπου $a \in A$ και $b \in B$. Τα σύνολα $\{a\}, \{a, b\}$ ανήκουν στο $\mathcal{P}(A \cup B)$ (είναι στοιχεία του), επομένως το σύνολο $(a, b) = \{\{a\}, \{a, b\}\}$ είναι στοιχείο του $\mathcal{P}(\mathcal{P}(A \cup B))$. Συνεπώς, από το αξίωμα του προσδιορισμού μπορούμε να κατασκευάσουμε το σύνολο

$$\{x \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid x = (a, b) \text{ για } a \in A \text{ και } b \in B\}.$$

Το σύνολο αυτό είναι το μόνο που αποτελείται από όλα τα διατεταγμένα ζεύγη (a, b) με $a \in A$, $b \in B$ (αξίωμα της έκτασης). Το σύνολο αυτό θα το συμβολίζουμε ως

$$A \times B = \{x = (a, b) \text{ για } a \in A \text{ και } b \in B\}.$$

Πρόταση 1.1.56. *Ο προηγούμενος ορισμός είναι "καλός".*

Απόδειξη. Η απόδειξη έχει προηγηθεί. ό.έ.δ.

Προφανώς, εάν τουλάχιστον ένα από τα σύνολα A και B είναι το κενό σύνολο, τότε το καρτεσιανό τους γινόμενο είναι το κενό σύνολο. Δηλαδή

$$A \times \varnothing = \varnothing \times B = \varnothing$$

Επίσης, γενικά ισχύει ότι $A \times B \neq B \times A$.

Ερώτημα: Σε ποίες περιπτώσεις ισχύει ότι $A \times B = B \times A$;

Ορισμένες φορές το καρτεσιανό γινόμενο $A \times A$ συμβολίζεται ως A^2. Επίσης, επαναληπτικά μπορούμε να ορίσουμε το καρτεσιανό γινόμενο

$$A^n = (A^{n-1}) \times A) \text{ για } n \geq 3.$$

Πρόταση 1.1.57. *Έστω A, B, C τρία σύνολα. Τότε ισχύει:*

i. $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

ii. $(A \cap B) \times C = (A \times C) \cap (B \times C)$.

[12] Ο ορισμός παραπέμπει στην γνωστή μας αναπαράσταση των σημείων ενός επιπέδου με Καρτεσιανές συντεταγμένες (διατεταγμένα ζεύγη πραγματικών αριθμών).

iii. $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$.

Απόδειξη.

i. Έστω $(x, y) \in (A \cup B) \times C$. Αυτό σημαίνει ότι $x \in A \cup B$ και $y \in C$. Δηλαδή $(x \in A$ ή $x \in B)$ και $y \in C$. Συνεπώς, $(x \in A$ και $y \in C)$ ή $(x \in B$ και $y \in C)$. Επομένως, $(x, y) \in A \times C$ ή $(x, y) \in B \times C$. Άρα αποδείξαμε ότι

$$(A \cup B) \times C \subseteq (A \times C) \cup (B \times C).$$

Έστω τώρα $(x, y) \in (A \times C) \cup (B \times C)$. Αυτό σημαίνει ότι $(x, y) \in A \times C$ ή $(x, y) \in B \times C$. Δηλαδή, $(x \in A$ ή $x \in B)$ και $y \in C$. Συνεπώς, $x \in A \cup B$ και $y \in C$. Επομένως, $(x, y) \in (A \cup B) \times C$. Άρα αποδείξαμε ότι

$$(A \times C) \cup (B \times C) \subseteq (A \cup B) \times C.$$

Τέλος.

ii. Η απόδειξη είναι παρόμοια με το i. και αφήνεται ως άσκηση.

iii. Έστω $(x, y) \in (A \setminus B) \times C$. Αυτό σημαίνει ότι $x \in A \setminus B$ και $y \in C$. Δηλαδή $x \in A$, άλλα $x \notin B$ (βλέπε Ορισμός 1.1.5). Συνεπώς, $(x, y) \in A \times C$, αλλά $(x, y) \notin B \times C$. Άρα $(x, y) \in (A \times C) \setminus (B \times C)$. Δηλαδή αποδείξαμε ότι $(A \setminus B) \times C \subseteq (A \times C) \setminus (B \times C)$.

Έστω τώρα $(x, y) \in (A \times C) \setminus (B \times C)$. Αυτό σημαίνει ότι $(x, y) \in A \times C$, αλλά $(x, y) \notin B \times C$. Δηλαδή, $x \in A$, αλλά $x \notin B$ και $y \in C$. Συνεπώς, $x \in A \setminus B$ και $y \in C$. Άρα $(x, y) \in (A \setminus B) \times C$. Επομένως, αποδείξαμε ότι

$$(A \times C) \setminus (B \times C) \subseteq (A \setminus B) \times C.$$

Τέλος. ό.έ.δ.

Πρόταση 1.1.58. *Έστω $\mathcal{A} = \{A_a \mid a \in \Lambda\}$ μια οικογένεια συνόλων με το σύνολο δεικτών Λ μη κενό και B ένα σύνολο. Τότε ισχύει ότι:*

i. $B \times (\bigcup_{a \in \Lambda} A_a) = \bigcup_{a \in \Lambda} (B \times A_a)$.

ii. $B \times (\bigcap_{a \in \Lambda} A_a) = \bigcap_{a \in \Lambda} (B \times A_a)$.

Απόδειξη. Η πρόταση αυτή αποτελεί γενίκευση των *i.* και *ii.* της προηγουμένης πρότασης. Απλώς να την επαναλάβετε. ό.έ.δ.

Παράδειγμα 1.1.59. Έστω $I = [0, 2] = \{x \in \mathbb{R} \mid 0 \leq x \leq 2\}$. Θεωρούμε το I ως σύνολο δεικτών και κατασκευάζουμε την εξής οικογένεια συνόλων:

$$A_a = \{(x, a) \mid x \in \mathbb{R} \ : \ 1 \leq x \leq 2\}, \text{ για } a \in I.$$

Θέλουμε να υπολογίσουμε την ένωση $\bigcup_{a \in I} A_a$.

Παρατηρούμε ότι $A_a = [1, 2] \times \{a\}$ (γιατί;).
Συνεπώς

$$\bigcup_{a \in I} A_a = \bigcup_{a \in I} ([1, 2] \times \{a\}).$$

Από την προηγουμένη πρόταση έπεται ότι

$$\bigcup_{a \in I} ([1, 2] \times \{a\}) = [1, 2] \times (\bigcup_{a \in I} \{a\}) = [1, 2] \times I = [1, 2] \times [0, 2].$$

Όμοια μπορούμε να δούμε ότι $\bigcap_{a \in I} A_a = \varnothing$ (γιατί;)

1.1.7 Ασκήσεις

1. Δίνονται τα σύνολα $A = \{a, b, c, d\}$, $B = \{d, e, f\}$, $C = \{1, 2, 3\}$.
   Να υπολογίσετε τα σύνολα $(A \cap B) \times C$ και $(A \times C) \cap (B \times C)$.

2. Έστω A, B, C τρία σύνολα με $C \neq \emptyset$. Υποθέτουμε ότι $A \times C = B \times C$. Δείξτε ότι $A = B$. (Είναι αναγκαία η συνθήκη $C \neq \emptyset$;)

3. Έστω A, B, C τρία σύνολα. Είναι οι ισότητες
   $$(A \times C) \cap (B \times D) = (A \cap B) \times (C \cap D)$$
   και
   $$(A \times C) \cup (B \times D) = (A \cup B) \times (C \cup D)$$
   σωστές; Δώστε απόδειξη ή αντιπαράδειγμα.

4. Ένα σύνολο A έχει n το πλήθος στοιχεία και ένα σύνολο B έχει m το πλήθος στοιχεία. Να δείξετε ότι το σύνολο $A \times B$ έχει $n \cdot m$ το πλήθος στοιχεία.

5. Να υπολογίσετε τα σύνολα
   $$\mathcal{P}(\{a, b\} \times \{c\}), \qquad \mathcal{P}(\{a, b\}) \times \mathcal{P}(\{c\}), \qquad \mathcal{P}(\{a, b\}) \times \mathcal{P}(\{0, 1\}).$$

6. Έστω δύο σύνολα A και B. Υποθέτουμε ότι το A έχει 3 στοιχεία και το B έχει 2 στοιχεία. Να υπολογίσετε το πλήθος των στοιχείων καθ' ενός από τα σύνολα
   $$\mathcal{P}(A \times B), \qquad \mathcal{P}(A) \times \mathcal{P}(B).$$
   Να γενικεύσετε, όταν το σύνολο A έχει n το πλήθος στοιχεία και το σύνολο B έχει m το πλήθος στοιχεία.

7. Δίνονται οι "ισότητες":
   $$(\mathbb{R} \times \mathbb{Z}) \cap (\mathbb{Z} \times \mathbb{R}) = \mathbb{Z} \times \mathbb{Z},$$
   $$(\mathbb{R} \times \mathbb{Z}) \cup (\mathbb{Z} \times \mathbb{R}) = \mathbb{R} \times \mathbb{R},$$
   $$(\mathbb{R} \setminus \mathbb{Z}) \times \mathbb{N} = (\mathbb{R} \times \mathbb{N}) \setminus (\mathbb{Z} \times \mathbb{N}).$$
   Εξετάστε ποιες είναι σωστές και ποιες λάθος. Δικαιολογήστε την απάντησή σας.

8. Να υπολογίσετε τα σύνολα $\bigcup_{n \in \mathbb{N}} (\mathbb{R} \times [n, n+1])$ και $\bigcap_{n \in \mathbb{N}} (\mathbb{R} \times [n, n+1])$.

9. Να υπολογίσετε τα σύνολα $\bigcup_{x \in [0,1]} ([x, 1] \times [0, x^2])$ και $\bigcap_{x \in [0,1]} ([x, 1] \times [0, x^2])$.

10. Μπορείτε να "φανταστείτε" ποιο είναι το δυναμοσύνολο του συνόλου των σημείων του επιπέδου; Δηλαδή το $\mathcal{P}(\mathbb{R} \times \mathbb{R})$.
    (Η σελίδα που έχετε μπροστά σας είναι ένα στοιχείο του συνόλου $\mathcal{P}(\mathbb{R} \times \mathbb{R})$!).

Βιβλιογραφία

[1] E.D. Bloch. *Proofs and Fundamentals: A first course in Abstract Mathematics*. Second Edition, Springer, 2011. ISBN: 978-14-4197-126-5.

[2] J. Cummings. *Proofs: A Long-Form Mathematics Textbook*. Independently published, 2021. ISBN: 979-85-9526-597-3.

[3] Herbert B. Enderton. *Elements of Set Theory*. Academic Press, 1977. ISBN: 978-01-2238-440-0.

[4] D. Goldrei. *Classic Set Theory: For Guided Independent Study*. Chapman Hall CRC Press, 1996. ISBN: 978-04-1260-610-6.

[5] K. Hrbacek-T. Jech. *Introduction to Set Theory*. Third Edition. Marcel Dekker Inc., 1999. ISBN: 08-2477-915-0.

[6] P. Halmos. *Naive Set Theory*. Springer, 1974. ISBN: 978-03-8790-104-6.

[7] K. Houston. *How to Think Like a Mathematician*. Cambridge University Press, 2009. ISBN: 978-05-2189-546-0.

[8] Steven G. Krantz. *The Elements of Advanced Mathematics*. Fouth Edition. Textbooks in mathematics. CRC Press Taylor and Francis Group, 2018. ISBN: 978-11-3850-631-2.

[9] M. Liebeck. *A Concise Introduction to Pure Mathematics*. Third Edition. Chapman Hall CRC Press, 2011. ISBN: 978-14-3983-598-2.

[10] Bernd S. W. Schröder. *Fundamentals of Mathematics: An Introduction to Proofs, Logic, Sets and Numbers*. First Edition. Wiley, 2010. ISBN: 978-04-7055-138-7.

[11] C. Schumacher. *Chapter Zero: Fundamental Notions of Abstract Mathematics*. Second Edition. Addison-Wesley, 2001. ISBN: 02-0143-724-4.

[12] I. Stewart & D. Tall. *The Foundations of Mathematics*. Second Edition. Second Edition, Oxford University Press, 2015.

[13] Αντώνης Τσολομύτης. *Σύνολα και αριθμοί*. Leader Books, 2004. ISBN: 978-96-0790-147-7.

ΚΕΦΑΛΑΙΟ 2

ΠΡΟΤΑΣΙΑΚΟΣ ΛΟΓΙΣΜΟΣ

2.1 Η έννοια της Μαθηματικής Πρότασης

Στην καθημερινότητά μας για την επικοινωνία μας, γραπτώς ή προφορικώς, χρησιμοποιούμε "προτάσεις" και "ισχυρισμούς". Μάλιστα δε, μερικές φορές, οι προτάσεις αυτές και οι ισχυρισμοί, είναι "αληθείς" και μερικές φορές "ψευδείς". Επίσης, ορισμένες φορές, πρόκειται για απλές προτάσεις και ισχυρισμούς, υπάρχουν όμως περιπτώσεις, όπου οι προτάσεις και οι ισχυρισμοί είναι σύνθετοι. Δεν αποκλείονται όμως και περιπτώσεις, όπου οι προτάσεις και οι ισχυρισμοί να είναι "ακατάληπτοι" (δεν έχουν νόημα).

Στα Μαθηματικά η έννοια της Πρότασης–Ισχυρισμού είναι πρωταρχική έννοια και μια προσπάθεια για έναν αυστηρό ορισμό χωρίς "αυτοεπικλήσεις" και "αυτοαναφορές" οδηγεί σε φιλοσοφικές αναζητήσεις. Επομένως, πρέπει να *συμφωνήσουμε* τι σημαίνει πρόταση στα Μαθηματικά, τι σημαίνει συνδυασμός προτάσεων, τι σημαίνει επίκληση κάποιων προτάσεων για τον σχηματισμό άλλων προτάσεων.

Μέχρι τώρα έχουμε χρησιμοποιήσει προτάσεις και ισχυρισμούς για την απόδειξη άλλων προτάσεων και ισχυρισμών[1].

Πριν προχωρίσουμε, ας επικαλεσθούμε ένα παράδειγμα:

Στην σελίδα 6 του προηγουμένου κεφαλαίου είχαμε το εξής:

Παράδειγμα 2.1.1. Τα σύνολα

$$A = \{ z \mid \text{ο } z \text{ είναι πραγματικός αριθμός,} \\ \text{που ικανοποιεί την εξίσωση } x^2 - 3x + 2 = 0 \}$$

[1] Όπως έχουμε ήδη επισημάνει, χρησιμοποιούμε *προτάσεις* και *γνωστά* αποτελέσματα των Μαθηματικών για την μελέτη αυτών των εννοιών. Αυτό δεν είναι (απαραίτητα) "κακό" και δεν αποτελεί ανακολουθία.

και

$$B = \{\, n \mid \text{ο } n \text{ είναι φυσικός αριθμός μικρότερος του } 3 \,\},$$

αν και "περιγράφονται" διαφορετικά, είναι ίσα.

Ας προσπαθήσουμε να διακρίνουμε προτάσεις.

a. "Ο z είναι πραγματικός αριθμός" αποτελεί μια (απλή) πρόταση.

b. "Ο z είναι πραγματικός αριθμός, που ικανοποιεί την εξίσωση $x^2-3x+2=0$" αποτελεί μια άλλη (συνθετότερη) πρόταση.

c. "Ο n είναι φυσικός αριθμός μικρότερος του 3" αποτελεί μια άλλη πρόταση.

Στο παράδειγμά μας υπάρχει και μια άλλη πρόταση, ως συμπέρασμα.

"Ένας αριθμός *ικανοποιεί* την πρόταση (b), αν και μόνο αν, ικανοποιεί την πρόταση (c)".

Η τελευταία πρόταση είναι (ακόμη περισσότερο) σύνθετη και για την διαπίστωση (απόδειξη) ότι είναι αληθής πρέπει να κάνουμε μια σειρά (λογικών) συνδυασμών. Με τις, μέχρι τώρα, γνώσεις μας, βλέπουμε ότι οι μόνοι πραγματικοί αριθμοί που ικανοποιούν την εξίσωση $x^2-3x+2=0$ είναι ο 1 και ο 2. Αλλά οι μόνοι φυσικοί αριθμοί οι μικρότεροι του 3 είναι μόνο το 1 και το 2. Επομένως, διαπιστώσαμε (αποδείξαμε) ότι πράγματι και η πρόταση αυτή είναι αληθής.

Μετά από αυτά ας γίνουμε πιο συστηματικοί.

Με τον όρο (δηλωτική) **πρόταση** ή ισχυρισμό εννοούμε μια πρόταση, η οποία έχει νόημα και είναι *από μόνη της* αληθής ή ψευδής, αλλά δεν είναι και τα δύο[2].

Προσοχή! Στην αυτοαναφορά στην λέξη *πρόταση*. Αμέσως μετά θα δούμε την διαφορά μεταξύ *πρότασης* και "Πρότασης".

Παραδείγματα 2.1.2. Παραθέτουμε μερικά παραδείγματα (δηλωτικών) προτάσεων.

1. Τα Μαθηματικά είναι επιστήμη.
2. Ο Τσώρτσιλ ήταν πρωθυπουργός της Αμερικής.
3. Το 3 είναι πρώτος αριθμός.
4. Το 3 είναι μεγαλύτερος του 5.
5. Το 3 είναι μεγαλύτερος του 2 και διαιρέτης του 9.
6. Το 3 διαιρεί το 6 και το 15.
7. Αν προσθέσουμε το 3 και στα δύο μέλη της ισότητας $x-3=34$, προκύπτει ότι $x=37$.
8. Υπάρχουν άπειροι το πλήθος πρώτοι αριθμοί.

[2]Εδώ δεν αναφερόμαστε στο φιλοσοφικό ερώτημα: *Τι είναι αλήθεια;* Μία και μόνο αναφορά στο ερώτημα αυτό ανοίγει *ατραπούς και λεωφόρους*, επί των οποίων δεν σκοπεύουμε, εδώ, ούτε καν να επιχειρήσουμε να...βηματίσουμε. Απλώς δεχόμαστε, μάλλον διαισθητικά, το τι σημαίνει αληθές και τι ψευδές.

Επίσης, οι εκφράσεις του τύπου: "Είναι αληθές/ψευδές για μένα" δηλώνουν υποκειμενισμό και θα αποφεύγονται παντελώς.

9. Κάθε άρτιος ακέραιος μεγαλύτερος του τρία είναι άθροισμα δύο πρώτων αριθμών. (Η περίφημη εικασία του Goldbach).

Όλες οι προηγούμενες προτάσεις είναι (δηλωτικές) προτάσεις, διότι είναι είτε αληθείς είτε ψευδείς.

Παρατηρήσεις 2.1.3.

1. Ας σταθούμε στα δύο τελευταία παραδείγματα.

   Η Πρόταση στο προτελευταίο παράδειγμα είναι αληθής. Με τις μέχρι τώρα γνώσεις μας ενδέχεται να μην γνωρίζουμε ότι, πράγματι, είναι αληθής (θα το δούμε με την πρόοδο των σπουδών μας), αλλά, ακόμη και αν δεν το γνωρίζουμε, σίγουρα είναι είτε αληθής είτε ψευδής.

   Η Πρόταση στο τελευταίο παράδειγμα, μέχρι τώρα, κανείς δεν γνωρίζει, αν είναι αληθής ή ψευδής (πρόκειται για εικασία), αλλά σίγουρα είναι Πρόταση, διότι είναι είτε αληθής είτε ψευδής.

2. Πρέπει να επισημανθεί ότι σε όλα τα παραδείγματα ισχύει (αποκλειστικά) ένα από τα δύο είτε η Πρόταση είναι αληθής είτε είναι ψευδής αποκλειομένου του ενδεχομένου να ισχύει κάτι "ενδιάμεσα". Αυτό είναι γνωστό ως **Ο Νόμος του ενδιάμεσου αποκλεισμού**.

3. Ας δούμε την εξής "πρόταση". "Ο x είναι περιττός ακέραιος". Αν το δούμε υπό την στενή έννοια του όρου πρόταση, δεν είναι (δηλωτική) πρόταση, διότι το αληθές ή ψευδές της εξαρτάται κάθε φορά από την τιμή του x. Για παράδειγμα, αν $x = 3$, η πρόταση είναι αληθής. Ενώ, αν $x = 4$, η πρόταση είναι ψευδής. Στην περίπτωση αυτή συμφωνούμε να θεωρούμε τέτοιες προτάσεις ως (δηλωτικές) προτάσεις *υπό συνθήκη* ή ότι περιέχουν μια *μεταβλητή*. Επ' αυτού θα επανέλθουμε αργότερα.

Υπάρχουν προτάσεις, υπό την έννοια της Γραμματικής και του Συντακτικού μιας γλώσσας, οι οποίες δεν είναι (δηλωτικές) προτάσεις υπό την Μαθηματική έννοια, που θέσαμε προηγουμένως. Για να καταστεί αυτό σαφές ας δούμε μερικά παραδείγματα.

Παραδείγματα 2.1.4.

1. "Άνοιξε την πόρτα."

2. "Ο αριθμός 5 είναι έξυπνος."

3. "Γιατί ο αριθμός 5 δεν είναι σύνθετος;"

4. "Προσθέτουμε το 3 και στα δύο μέλη."

5. "Ο Ερμής του Πραξιτέλη είναι ένα όμορφο γλυπτό."

6. "Η Γη δεν είναι ο μόνος πλανήτης στο Σύμπαν, ο οποίος κατοικείται από έμβια όντα."

7. "Αυτή η πρόταση είναι ψευδής."

Οι προτάσεις αυτές δεν είναι (δηλωτικές) προτάσεις, διότι δεν είναι (σαφώς) αληθείς ή ψευδείς.

Ας δούμε το παράδειγμα "Ο Ερμής του Πραξιτέλη είναι ένα όμορφο γλυπτό." Εδώ υπεισέρχεται η υποκειμενικότητα του παρατηρητή, η οποία, προφανώς, διαφέρει από άτομο σε άτομο. Επομένως, υπάρχει ασάφεια κατά πόσον η πρόταση είναι αληθής ή ψευδής.

Ας δούμε το παράδειγμα "Η Γη δεν είναι ο μόνος πλανήτης στο Σύμπαν, ο οποίος κατοικείται από έμβια όντα." Εδώ έχουμε το εξής "πρόβλημα". Πρέπει να διευκρινιστεί, από την επιστημονική κοινότητα, τι σημαίνει "έμβιο ον". Όταν πλέον έχει δοθεί ένας σαφής και αποδεκτός ορισμός του τι σημαίνει "έμβιο ον", τότε η πρόταση αυτή καθίσταται μια (δηλωτική) πρόταση. Ασχέτως, αν γνωρίζουμε ή δεν γνωρίζουμε την ύπαρξη εμβίων όντων εκτός του πλανήτη Γη.

Το τελευταίο παράδειγμα είναι χαρακτηριστικό.

Δεχόμαστε ότι η πρόταση είναι αληθής. Τότε η πρόταση λέει ότι είναι ψευδής. Αντίφαση ως προς την παραδοχή μας.

Δεχόμαστε ότι η πρόταση είναι ψευδής. Τότε ο ισχυρισμός της πρότασης είναι αληθής. Αντίφαση ως προς την παραδοχή μας.

Τελικά, ό,τι και να δεχθούμε, καταλήγουμε σε αντίφαση, δηλαδή δεν μπορούμε να αποφανθούμε, αν είναι αληθής ή ψευδής, άρα δεν είναι (δηλωτική) πρόταση. Το πρόβλημα εδώ εντοπίζεται στο ότι η πρόταση αυτοαναφέρεται[3].

Ας συγκρίνουμε το παράδειγμα "Προσθέτουμε το 3 και στα δύο μέλη." με το παράδειγμα "Αν προσθέσουμε το 3 και στα δύο μέλη της ισότητας $x - 3 = 34$, προκύπτει ότι $x = 37$." (Παράδειγμα 2.1.2 $_7$).

Βλέπουμε ότι στο μεν πρώτο υπάρχει ασάφεια, ενώ στο δεύτερο δεν υπάρχει καμία ασάφεια ως προς την αλήθεια της πρότασης.

Από τα προηγηθέντα είναι σαφές πλέον, το τι εννοούμε με τον όρο "(δηλωτική) πρόταση"[4].

Μια (δηλωτική) Πρόταση συνήθως συμβολίζεται με κάποιο από τα γράμματα του Λατινικού αλφαβήτου (πεζό ή κεφαλαίο). Για παράδειγμα:

p : "Ο π είναι άρρητος αριθμός".
q : "Αν $x \in \mathbb{R}$, τότε $x^2 + 1 > 0$".
R : "Αν ο ακέραιος αριθμός x είναι πολλαπλάσιο του 6, τότε ο x είναι πολλαπλάσιο του 2".
S : "Αν ο ακέραιος αριθμός x είναι πολλαπλάσιο του 2, τότε ο x είναι πολλαπλάσιο του 6".

Στις Προτάσεις q, R και S εμφανίζεται *μεταβλητή* x. Παρατηρούμε ότι οι Προτάσεις q και R είναι πάντα αληθείς, ενώ η S δεν είναι πάντα αληθής ή πάντα ψευδής. Το γεγονός αυτό το έχουμε ήδη επισημάνει στην Παρατήρηση 2.1.3$_3$ και είχαμε μιλήσει για Προτάσεις "υπό συνθήκη" ή Προτάσεις με μεταβλητές[5].

Επομένως, στην περίπτωση αυτή, το αληθές ή το ψευδές της Πρότασης εξαρτάται από το x, το οποίο ανήκει πάντα σε ένα προκαθορισμένο σύνολο. Στην περίπτωση

[3] Δεν θα επεκταθούμε περισσότερο σε αυτοαναφερόμενες προτάσεις, οι οποίες οδηγούν σε "παράξενες καταστάσεις". Ο κάθε ενδιαφερόμενος μπορεί να ανατρέξει, στην αρχή, σε στοιχειώδη εγχειρίδια Μαθηματικής Λογικής και κατόπιν σε πιο προχωρημένα συγγράμματα.

[4] Στα επόμενα, όταν δεν υπάρχει σύγχυση, αντί του όρου "(δηλωτική) πρόταση", θα χρησιμοποιούμε απλά τον όρο "Πρόταση" (το Π κεφαλαίο σε αντιδιαστολή με την "πρόταση").

[5] Ορισμένοι συγγραφείς μια τέτοια Πρόταση την ονομάζουν *ανοικτή πρόταση ή κατηγόρημα*.

αυτή μια πρόταση p την συμβολίζουμε $p(x)$[6].

Ενδέχεται μια Πρόταση να εξαρτάται από περισσότερες της μίας μεταβλητής. Για παράδειγμα: Η Πρόταση

$R(x, y)$: "Ο θετικός ακέραιος y είναι το τετράγωνο του θετικού ακεραίου x".

Παρατηρούμε ότι η πρόταση είναι αληθής για $x = 2$ και $y = 4$, ενώ είναι ψευδής για $x = 3$ και $y = 6$.

Όπως βλέπουμε, υπάρχουν Προτάσεις, οι οποίες είναι προφανέστατα αληθείς ή ψευδείς. Υπάρχουν όμως Προτάσεις, των οποίων το αληθές ή ψευδές δεν είναι καθόλου προφανές και απαιτείται η ανάπτυξη *λογικών* επιχειρημάτων, όπως η επίκληση γνωστών Προτάσεων, ο συνδυασμός Προτάσεων για την δημιουργία "συνθετοτέρων" Προτάσεων ή αντίστροφα, η ανάλυση συνθέτων Προτάσεων σε απλούστερες, οι οποίες τελικά μας οδηγούν στο να αποφανθούμε αν μια Πρόταση είναι αληθής ή ψευδής.

Δεν θα ήταν (κατά την γνώμη μας) μεγάλη υπερβολή, αν ισχυριστούμε ότι σκοπός της Μαθηματικής Επιστήμης είναι, ξεκινώντας από παραδοχές (αξιώματα), η κατασκευή, η ανάλυση, η σύνθεση και η "απόδειξη" Προτάσεων.

Στο επόμενο κεφάλαιο θα αναφερθούμε σε τεχνικές ανάλυσης, σύνθεσης και απόδειξης Προτάσεων. Είναι αυτό που συνήθως αναφέρεται ως "Μέθοδοι Απόδειξης".

Προς το παρόν αρκούμαστε απλώς να παραθέσουμε τρεις "εμβληματικές" Προτάσεις.

P: "Αν a, b είναι τα μήκη των κάθετων πλευρών ενός ορθογωνίου τριγώνου και c το μήκος της υποτείνουσας, τότε ισχύει $a^2 + b^2 = c^2$".
F: "Για όλους τους φυσικούς αριθμούς a, b, c, n με $n > 2$ ισχύει $a^n + b^n \neq c^n$".
G: "Κάθε άρτιος ακέραιος μεγαλύτερος του τρία είναι άθροισμα δύο πρώτων αριθμών".

Η Πρόταση P είναι το Πυθαγόρειο Θεώρημα, το οποίο αποδίδεται στον Πυθαγόρα (570 π.Χ. - 495 π.Χ.). Για την απόδειξη του Θεωρήματος αυτού (Η αλήθεια της Πρότασης P) υπάρχουν πάρα πολλές αποδείξεις (ίσως οι περισσότερες που υπάρχουν για την απόδειξη μιας συγκεκριμένης Πρότασης).

Η Πρόταση F είναι το (γνωστό;) Τελευταίο Θεώρημα του Fermat, το οποίο προτάθηκε, ως ισχυρισμός, το 1637 από τον ερασιτέχνη Μαθηματικό Pier de Fermat. Αμέτρητες (ανεπιτυχείς) προσπάθειες έγιναν για να αποδειχθεί η αλήθεια της Πρότασης αυτής. Το 1995 τελικά ο Andrew Wiles (με ουσιαστική συμβολή του μαθητή του Richard Taylor) κατόρθωσε να δώσει μια ολοκληρωμένη απόδειξη[7].

Η Πρόταση G (έχει ήδη προαναφερθεί) είναι η γνωστή "Εικασία του Goldbach", η οποία έχει προταθεί, ως ισχυρισμός, από τον Γερμανό Μαθηματικό Christian Goldbach το 1792 και η οποία, παρ' όλες τις προσπάθειες, παραμένει μέχρι σήμερα αναπάντητη, και, όπως τόσες άλλες "προκλητικές" εικασίες, "τροφοδοτούν" την έρευνα στα Μαθηματικά.

---

[6] Αργότερα, όταν μιλήσουμε για ποσοδείκτες, θα δούμε πώς οι ανοικτές Προτάσεις *μετασχηματίζονται* σε (δηλωτικές) Προτάσεις.

[7] Εδώ καταδεικνύεται ότι η προσπάθεια για την απόδειξη της αλήθειας μιας Πρότασης έγινε η αφορμή για την ανάπτυξη ολόκληρων περιοχών των Μαθηματικών. Επομένως, εγείρονται ερωτήματα (με φιλοσοφικές προεκτάσεις). Δηλαδή, κατά πόσον είναι σημαντικότερη η απόδειξη του ισχυρισμού ως αποτέλεσμα ή η απόδειξη αυτή καθ' εαυτή με τις όποιες μετέπειτα "συνέπειές της".

2.1.1 Προτάσεις, οι οποίες "προέρχονται" από άλλες Προτάσεις

Όπως έχουμε ήδη αναφέρει, θα μπορούσαμε να κατασκευάσουμε Προτάσεις αναλύοντας ή συνθέτοντας άλλες, των οποίων η αλήθεια εξαρτάται από τις "εμπλεκόμενες" Προτάσεις.

Η άρνηση Προτάσεων.

Ας ξεκινήσουμε με το εξής παράδειγμα: Έχουμε την πρόταση

p : "Ο αριθμός 2 είναι άρτιος" (η οποία, προφανώς, είναι αληθής).

Σχηματίζουμε την πρόταση

"*Δεν είναι αληθές ότι* ο αριθμός 2 είναι άρτιος" (η οποία, προφανώς, είναι ψευδής).

Γενικά, όταν έχουμε μια πρόταση p, τότε μπορούμε να σχηματίσουμε μια άλλη πρόταση:

"*Δεν είναι αληθές ότι ισχύει η* p".

Η πρόταση αυτή αποτελεί την **άρνηση** της πρότασης p.

Στο προηγούμενο παράδειγμα, χρησιμοποιώντας την ευελιξία της γλώσσας μας, θα μπορούσαμε να διατυπώσουμε την άρνηση της πρότασης "Ο αριθμός 2 είναι άρτιος" ισοδύναμα ως εξής: "Ο αριθμός 2 δεν είναι άρτιος" ή "Είναι λάθος ότι ο αριθμός 2 είναι άρτιος". Ακόμη περισσότερο, χρησιμοποιώντας τον χαρακτηρισμό των αρτίων και περιττών αριθμών, θα μπορούσαμε να διατυπώσουμε την άρνηση της πρότασης αυτής ως εξής: "Ο αριθμός 2 είναι περιττός".

Ας δούμε ένα άλλο παράδειγμα.

Έχουμε την πρόταση "Όλοι οι θετικοί ακέραιοι είναι άρτιοι". Η άρνησή της είναι "Δεν είναι αληθές ότι όλοι οι θετικοί ακέραιοι είναι άρτιοι".

Προσοχή! Εδώ πρέπει να είμαστε προσεκτικοί και να μην παρασυρόμαστε θεωρώντας ως άρνηση την "Όλοι οι θετικοί ακέραιοι είναι περιττοί".

Ας παραβάλλουμε με το παράδειγμα: "Όλα τα σκυλιά δεν είναι υπάκουα". Η άρνηση αυτής της πρότασης **δεν** είναι η "Όλα τα σκυλιά είναι υπάκουα", **αλλά** η "Μερικά σκυλιά είναι υπάκουα"[8].

Ο επόμενος ορισμός δεν επιτρέπει παρερμηνείες.

Ορισμός 2.1.5. Η άρνηση μιας πρότασης p είναι μια πρόταση ¬ p, η οποία είναι ψευδής, όταν η p είναι αληθής.

Σχόλιο 2.1.6. Στον ορισμό χρησιμοποιήσαμε τον συμβολισμό ¬p για να δηλώσουμε την άρνηση της πρότασης p και αυτόν τον συμβολισμό θα χρησιμοποιούμε στο εξής. Σε πολλά εγχειρίδια, αντί του ¬p χρησιμοποιείται το ∼ p ή το $\bar{p}$.

Σύμφωνα με τον ορισμό, όταν η Πρόταση p είναι ψευδής, η πρόταση ¬p είναι αληθής (γιατί; δεν ξεχνάμε τον ορισμό της (δηλωτικής) πρότασης στην σελ. 34). Επομένως, η Πρόταση ¬(¬p) είναι (κατ' ουσίαν) η Πρόταση p.

Στα επόμενα θα επανέλθουμε και θα δούμε πώς επιτυγχάνεται η άρνηση συνθετοτέρων Προτάσεων.

[8] Εδώ είναι εμφανής, για άλλη μια φορά, η αναγκαιότητα για "πειθαρχία σκέψης και έκφρασης".

Σύζευξη Προτάσεων.

Ας ξεκινήσουμε με το εξής παράδειγμα:
Θεωρούμε την Πρόταση

R : "Ο αριθμός 3 είναι περιττός *και* ο αριθμός 2 είναι πρώτος".

Όπως παρατηρούμε, η Πρόταση R 'προέρχεται/σχηματίζεται/δημιουργείται' από τις Προτάσεις

P : "Ο αριθμός 3 είναι περιττός" και
Q : "Ο αριθμός 2 είναι πρώτος".

Γενικά, όταν έχουμε δύο Προτάσεις, πάντα μπορούμε με την χρήση της λέξης **και** να σχηματίσουμε μια νέα (συνθετότερη) Πρόταση. Η Πρόταση, που προκύπτει, θα ονομάζεται **σύζευξη** των δύο Προτάσεων. Στο προηγούμενο παράδειγμα έχουμε ότι

R : "P και Q".

Συμβολικά έχει επικρατήσει την λέξη "και" να την συμβολίζουμε με το σύμβολο $\wedge$, οπότε έχουμε

R : "P $\wedge$ Q".

Το αν η Πρόταση, που προκύπτει από την σύζευξη δύο άλλων Προτάσεων, είναι αληθής ή ψευδής, εξαρτάται από την αλήθεια των δύο συζευγμένων Προτάσεων.

Στο προηγούμενο παράδειγμα βλέπουμε ότι οι δύο Προτάσεις

P : "Ο αριθμός 3 είναι περιττός" και
Q : "Ο αριθμός 2 είναι πρώτος"

είναι και οι δύο αληθείς, οπότε και η πρόταση

R : "Ο αριθμός 3 είναι περιττός *και* ο αριθμός 2 είναι πρώτος"

είναι αληθής.

Αν μια από τις δύο Προτάσεις, που μετέχουν στην σύζευξη, είναι ψευδής, από την "απαίτησή" του **και** στην σύζευξη απορρέει/ συμπεραίνεται ότι η Πρόταση που προκύπτει είναι ψευδής.

Για παράδειγμα, αν αντί της Πρότασης

P : "Ο αριθμός 3 είναι περιττός"

έχουμε την Πρόταση

S : "Ο αριθμός 3 είναι άρτιος",

τότε η Πρόταση

T : "S $\wedge$ Q"

είναι ψευδής.

Συμπερασματικά: Η σύζευξη δύο Προτάσεων είναι αληθής **μόνο** στην περίπτωση, όπου **και** οι δύο Προτάσεις είναι αληθείς. Σε όλες τις άλλες περιπτώσεις είναι ψευδής.

Προφανώς, όταν έχουμε τις συζεύξεις "$P \wedge Q$" και "$Q \wedge P$" δύο Προτάσεων P και Q, (κατ' ουσίαν) πρόκειται για την ίδια Πρόταση. Υπό την έννοια ότι η "$P \wedge Q$" είναι αληθής, αν και μόνο αν η "$Q \wedge P$" είναι αληθής.

Όταν έχουμε τρεις Προτάσεις, έστω P, Q, R, τότε μπορούμε να πάρουμε την σύζευξη δύο από αυτές και μετά την σύζευξη της Πρότασης που προκύπτει με την τρίτη Πρόταση. Έχουμε τις εξής περιπτώσεις:

$$(P \wedge Q) \wedge R,\ P \wedge (Q \wedge R),\ (P \wedge R) \wedge Q.$$

Σύμφωνα με τα προηγούμενα, (κατ' ουσίαν) πρόκειται για την ίδια Πρόταση, δεδομένου ότι οι Προτάσεις αυτές είναι αληθείς, αν και μόνο αν και οι τρεις Προτάσεις P, Q, R είναι αληθείς. Οπότε, θα γράφουμε (χωρίς την χρήση παρενθέσεων)

$$P \wedge Q \wedge R.$$

Διάζευξη Προτάσεων.

Όπως με το "και" συνδέουμε δύο Προτάσεις για να σχηματίσουμε μια άλλη Πρόταση, έτσι μπορούμε να συνδέσουμε με το "ή" δύο Προτάσεις για να σχηματίσουμε μια νέα Πρόταση.

Εδώ όμως πρέπει να είμαστε προσεκτικοί, διότι η χρήση του "ή" στον *κοινό λόγο*, πολλές φορές, δημιουργεί ασάφειες.

Ας δούμε μερικά παραδείγματα:

1. Πρέπει να πληρώσετε την συνδρομή σας ή θα διαγραφείτε από τον σύλλογο.
2. Η μηχανή καταστρέφεται, όταν λειτουργεί με χαμηλή στάθμη ελαίου ή με χαμηλή στάθμη νερού.
3. Αν ο ακέραιος αριθμός m ή ο ακέραιος αριθμός n είναι άρτιος, τότε το γινόμενο $m \cdot n$ είναι άρτιος αριθμός.
4. Ο ακέραιος αριθμός n είναι περιττός ή άρτιος.

Στο πρώτο παράδειγμα δεν υπάρχει αμφιβολία ότι **μόνο** ένα από τα δύο μπορεί να συμβεί, αποκλειομένου του ενδεχομένου να συμβούν και τα δύο. Δηλαδή, να πληρωθεί η συνδρομή και να γίνει διαγραφή από τον σύλλογο.

Στο δεύτερο παράδειγμα, κανείς δεν αποκλείει, σε περίπτωση καταστροφής της μηχανής, να έχουμε (μόνο) χαμηλή στάθμη ελαίου ή (μόνο) χαμηλή στάθμη νερού ή ταυτόχρονα να έχουμε και χαμηλή στάθμη ελαίου και χαμηλή στάθμη νερού.

Στο τρίτο παράδειγμα το γινόμενο $m \cdot n$ είναι άρτιος αριθμός, αρκεί ο ένας από τους δύο παράγοντες να είναι (χωρίς να αποκλείεται να είναι και οι δύο) άρτιος αριθμός.

Στο τέταρτο παράδειγμα ο n **δεν** μπορεί ταυτόχρονα να είναι περιττός και άρτιος[9].

Επομένως, ειδικά στα Μαθηματικά, όταν χρησιμοποιούμε το "ή" για τον σχηματισμό μιας νέας Πρότασης από δύο άλλες Προτάσεις, πρέπει να κάνουμε διάκριση μεταξύ της "περιεκτικής διάζευξης" και της "αποκλειστικής διάζευξης".

Συγκεκριμμένα: Αν έχουμε δύο Προτάσεις P και Q, τότε η περιεκτική διάζευξη στον σχηματισμό μιας νέας Πρότασης σημαίνει ότι η νέα Πρόταση είναι αληθής, αρκεί μια από τις δύο Προτάσεις (χωρίς να αποκλείεται και οι δύο) να είναι αληθής.

[9] Δεν χρειάζεται, προς το παρόν να επεκταθούμε σε περισσότερα παραδείγματα. Όλοι γνωρίζουμε περιπτώσεις, όπου...καταφεύγουμε στα δικαστήρια για να ερμηνεύσει ο δικαστής την ασάφεια που δημιουργείται από την χρήση του "ή" στην νομοθεσία....

Τουναντίον, η αποκλειστική διάζευξη στον σχηματισμό μιας νέας Πρότασης σημαίνει ότι η νέα Πρόταση είναι αληθής **μόνο** στην περίπτωση όπου η μια Πρόταση είναι αληθής και η άλλη ψευδής.

Για την αποφυγή σύγχυσης, από τούδε και στο εξής, θα χρησιμοποιούμε το "ή" στην σύνδεση δύο Προτάσεων στην περίπτωση της περιεκτικής διάζευξης και το "είτε... ή..." για την σύνδεση δύο Προτάσεων στην περίπτωση της αποκλειστικής διάζευξης.

Δηλαδή "P ή Q" σημαίνει περιεκτική διάζευξη και

"είτε P ή Q" σημαίνει αποκλειστική διάζευξη.

Σχόλια 2.1.7.

- Η περιεκτική διάζευξη ορισμένες φορές ονομάζεται και *λογική διάζευξη* ή απλώς *διάζευξη*.
- Σε πολλά κείμενα, συνήθως στην καθημερινότητα, το "ή" χρησιμοποιείται για την αποκλειστική διάζευξη και για την περιεκτική διάζευξη χρησιμοποιείται το "ή/και".
- Για την περιεκτική διάζευξη χρησιμοποιείται το σύμβολο $\vee$. Δηλαδή

  αντί του "P ή Q" έχουμε το "$P \vee Q$".

- Για την αποκλειστική διάζευξη χρησιμοποιείται το σύμβολο $\underline{\vee}$ (ορισμένες φορές χρησιμοποιείται και το σύμβολο $\oplus$). Δηλαδή

  αντί του "είτε P ή Q" έχουμε "$P \,\underline{\vee}\, Q$" (ή "$P \oplus Q$").

- Ορισμένες φορές, για την αποκλειστική διάζευξη, αντί του "είτε P ή Q" χρησιμοποιούμε τις (ισοδύναμες) εκφράσεις

  "είτε P είτε Q", "P ή Q, αλλά όχι και οι δύο", "ακριβώς μια από τις P ή Q".

Όταν έχουμε τρεις Προτάσεις, έστω P, Q, R, τότε μπορούμε να πάρουμε την διάζευξη δύο εξ αυτών και μετά την διάζευξη της Πρότασης που προκύπτει με την τρίτη Πρόταση. Έχουμε τις εξής περιπτώσεις:

$$(P \vee Q) \vee R,\ P \vee (Q \vee R),\ (P \vee R) \vee Q.$$

Σύμφωνα με τα προηγούμενα, (κατ' ουσίαν) πρόκειται για την ίδια Πρόταση, δεδομένου ότι οι Προτάσεις αυτές είναι ψευδείς αν και μόνο αν και οι τρεις Προτάσεις P, Q, R είναι ψευδείς. Οπότε, θα γράφουμε (χωρίς την χρήση παρενθέσεων)

$$P \vee Q \vee R.$$

Παράδειγμα 2.1.8. Στο προηγούμενο κεφάλαιο, όπου μελετούσαμε τα σύνολα, είχαμε δει την βασική αρχή ότι ένα στοιχείο a είτε ανήκει σε ένα σύνολο A ($a \in A$) ή δεν ανήκει ($a \notin A$).

Επομένως, αν έχουμε την Πρόταση

P : "$a \in A$",

τότε η άρνησή της είναι

$\neg$P : "$a \notin A$".

Επίσης, αν έχουμε δύο σύνολα A και B και τις Προτάσεις

P : "$a \in A$", Q : "$a \in B$",

τότε προφανώς (γιατί;) η σύζευξη των δύο αυτών Προτάσεων είναι η

P $\wedge$ Q : "$a \in A \cap B$".

Όμοια, για την διάζευξη των Προτάσεων αυτών έχουμε

P $\vee$ Q : "$a \in A \cup B$".

Η αποκλειστική διάζευξη αυτών των Προτάσεων αντιστοιχεί στην συμμετρική διαφορά των δύο συνόλων. Δηλαδή,

P $\oplus$ Q : "$a \in A \oplus B$".

(Υπενθυμίζουμε ότι για την συμμετρική διαφορά των A και B ισχύει ότι

$$A \oplus B = (A \cup B) \setminus (A \cap B),$$

ιδέ Άσκηση 1.1.3$_7$, σελ. 19 στο προηγούμενο κεφάλαιο).

Πίνακες αληθείας.

Οι **πίνακες αληθείας** είναι πίνακες, τους οποίους χρησιμοποιούμε στην μελέτη των Προτάσεων. Η ιδέα είναι το πώς, παραστατικά, σε έναν πίνακα θα "κωδικοποιήσουμε" την πληροφορία για την αλήθεια μιας Πρότασης. Αν και η χρήση αυτών των πινάκων είναι περιορισμένη στην "καθημερινότητα" ενός Μαθηματικού, είναι πολύ χρήσιμη για έναν, ο οποίος βρίσκεται στην αφετηρία της μελέτης των Προτάσεων. Όπου, όταν η Πρόταση είναι αληθής, δηλώνεται ως Α και όταν η Πρόταση είναι ψευδής, δηλώνεται ως Ψ (τα Α και Ψ ονομάζονται σηνήθως ως *τιμές αληθείας* της Πρότασης).

Ο πίνακας αληθείας για την άρνηση μιας Πρότασης P είναι ο εξής:

P	$\neg$ P
Α	Ψ
Ψ	Α

Ο πίνακας αληθείας για την σύζευξη Προτάσεων είναι ο εξής:

P	Q	P $\wedge$ Q
Α	Α	Α
Α	Ψ	Ψ
Ψ	Α	Ψ
Ψ	Ψ	Ψ

Ο πίνακας αληθείας για την διάζευξη (περιεκτική και αποκλειστική) είναι ο εξής:

P	Q	$P \vee Q$	$P \underline{\vee} Q$
Α	Α	Α	Ψ
Α	Ψ	Α	Α
Ψ	Α	Α	Α
Ψ	Ψ	Ψ	Ψ

Ένας πίνακας αληθείας διαβάζεται κατά γραμμές. Για παράδειγμα, στον τελευταίο πίνακα η πρώτη γραμμή δηλώνει ότι, αν η P είναι αληθής, η Q είναι αληθής, τότε η $P \vee Q$ είναι αληθής, ενώ η $P \underline{\vee} Q$ είναι ψευδής.

Ισοδυναμία Προτάσεων.

Στα προηγούμενα χρειάστηκε να "συγκρίνουμε" δύο Προτάσεις. Για παράδειγμα, στην σελ. 38 είχαμε πει "η Πρόταση $\neg(\neg p)$ είναι (κατ' ουσίαν) η Πρόταση p".

Τώρα μπορούμε να δώσουμε τον εξής Ορισμό:

Ορισμός 2.1.9. Δύο Προτάσεις P και Q θα ονομάζονται **ισοδύναμες** αν έχουν ίδιους πίνακες αληθείας.

Για παράδειγμα, οι Προτάσεις P και $\neg(\neg P)$ είναι ισοδύναμες, όπως έχουμε ήδη επισημάνει, ενώ οι Προτάσεις $P \wedge Q$ και $P \vee Q$ δεν είναι ισοδύναμες (μια απλή σύγκριση των πινάκων αληθείας στην προηγούμενη παράγραφο αρκεί).

Υπάρχουν πολλοί τρόποι για να δηλώσουμε την ισοδυναμία δύο Προτάσεων. Συνήθως συμβολίζουμε με:

$$P \approx Q \text{ ή } P \equiv Q \text{ ή } P \Leftrightarrow Q.$$

Μπορούμε εύκολα να διαπιστώσουμε ότι πράγματι

$$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R) \text{ και } (P \vee Q) \vee R \equiv P \vee (Q \vee R).$$

Παρατηρήσεις 2.1.10.

1. Ενώ ο ορισμός της ισοδυναμίας Προτάσεων είναι απλός, ορισμένες φορές είναι ατελέσφορο να καταφεύγουμε στην κατασκευή και σύγκριση πινάκων αληθείας για να διαπιστώσουμε αν δύο Προτάσεις είναι ισοδύναμες ή όχι. Στα επόμενα θα δούμε πώς μπορούμε (με άλλους τρόπους) να διαπιστώσουμε, αν δύο Προτάσεις είναι ισοδύναμες.

2. Η έννοια της ισοδυναμίας στα Μαθηματικά είναι θεμελιώδης. Μας δίνει την δυνατότητα να "βλέπουμε" και να εξετάζουμε με διαφορετικούς τρόπους τα ίδια πράγματα. Σε επόμενο κεφάλαιο θα δούμε την έννοια της ισοδυναμίας υπό άλλο πρίσμα.

Το επόμενο παράδειγμα είναι χαρακτηριστικό.

Παράδειγμα 2.1.11. Στην προηγουμένη παράγραφο έχουμε δει τους πίνακες αληθείας για την άρνηση μιας Πρότασης και για την σύζευξη και διάζευξη Προτάσεων. Ας προσπαθήσουμε να ενοποιήσουμε αυτούς τους πίνακες.

P	Q	$\neg P$	$\neg Q$	$P \wedge Q$	$P \vee Q$	$\neg(P \wedge Q)$	$(\neg P) \vee (\neg Q)$	$\neg(P \vee Q)$	$(\neg P) \wedge (\neg Q)$
Α	Α	Ψ	Ψ	Α	Α	Ψ	Ψ	Ψ	Ψ
Α	Ψ	Ψ	Α	Ψ	Α	Α	Α	Ψ	Ψ
Ψ	Α	Α	Ψ	Ψ	Α	Α	Α	Ψ	Ψ
Ψ	Ψ	Α	Α	Ψ	Ψ	Α	Α	Α	Α

Όπως παρατηρούμε, από την έβδομη και όγδοη στήλη έπεται η ισοδυναμία

$$\neg(\mathrm{P} \wedge \mathrm{Q}) \equiv (\neg \mathrm{P}) \vee (\neg \mathrm{Q}).$$

και από την ένατη και δέκατη στήλη έπεται η ισοδυναμία

$$\neg(\mathrm{P} \vee \mathrm{Q}) \equiv (\neg \mathrm{P}) \wedge (\neg \mathrm{Q}).$$

Οι δύο αυτές ισοδυναμίες είναι γνωστές ως ο **Νόμος του Morgan**.

Παρατήρηση 2.1.12. Στο Παράδειγμα 2.1.8 είχαμε δει ότι στα σύνολα οι έννοιες του ανήκειν (δεν ανήκειν), της τομής, της ένωσης και της συμμετρικής διαφοράς αποτελούν (ειδικές) περιπτώσεις άρνησης, της σύζευξης, της διάζευξης και της αποκλειστικής διάζευξης Προτάσεων.

Με το προηγούμενο παράδειγμα βλέπουμε ότι η Πρόταση 1.1.39 (σελ. 18) αποτελεί ειδική περίπτωση του Νόμου του Morgan.

2.1.2 Ασκήσεις

1. Αποφανθείτε ποιες από τις ακόλουθες "εκφράσεις" είναι Προτάσεις και ποιες δεν είναι. Στην περίπτωση που έχουμε Προτάσεις, μπορείτε να αποφανθείτε, αν είναι αληθείς ή ψευδείς;

   (α) Κάθε πραγματικός αριθμός είναι άρτιος ακέραιος αριθμός.

   (β) Κάθε άρτιος ακέραιος αριθμός είναι πραγματικός αριθμός.

   (γ) Δίνονται τα σύνολα των πραγματικών και ακεραίων αριθμών.

   (δ) Τα σύνολα των πραγματικών και ακεραίων αριθμών αποτελούνται από γλυκά.

   (ε) Τα σύνολα των πραγματικών και ακεραίων αριθμών έχουν πεπερασμένο το πλήθος στοιχεία.

   (στ) Λέγε με Δημήτρη.

   (ζ) $(A \times B) \cap (B \times A) = (A \cap B) \times (A \cap B)$.

   (η) Ο x είτε είναι πολλαπλάσιο του 5 ή δεν είναι.

   (θ) Ο ακέραιος x είτε είναι πολλαπλάσιο του 5 ή δεν είναι.

   (ι) Υπάρχει αριθμός x, έτσι ώστε $\sin(x) = x$.

   (ια) Η ζωή είναι ωραία!

2. Να διατυπώσετε την άρνηση των εξής Προτάσεων:

   (α) Η Α είναι αληθής ή η Β είναι ψευδής.

   (β) Η Α είναι ψευδής και η Β είναι αληθής.

   (γ) Η Α είναι αληθής ή η Β είναι αληθής.

   (δ) Η Α είναι ψευδής και η Β είναι ψευδής.

3. Να εκφράσετε κάθε Πρόταση ή ανοικτή Πρόταση, υπό την μορφή

$$\mathrm{P} \vee \mathrm{Q},\ \mathrm{P} \wedge \mathrm{Q} \text{ ή } \neg\ \mathrm{P}.$$

(Βεβαιωθείτε πρώτα ποια Πρόταση θεωρείτε ως P και ποια ως Q).

(α) Ο αριθμός 27 είναι ταυτόχρονα περιττός και δύναμη του 3.

(β) Ο αριθμός x είναι μικρότερος ή ίσος του y.

(γ) Ο αριθμός x ισούται με το 0, αλλά ο y όχι.

(δ) Τουλάχιστον ένας από τους αριθμούς x και y ισούται με μηδέν.

(ε) $x \in A \setminus B, \quad x \in A \cup B, \quad A \in \{X \in \mathcal{P}(\mathbb{N}) \mid X^c \quad \text{είναι πεπερασμένο}\}$.

(στ) "Δεν ζούμε τα όνειρά μας, αλλά ζούμε τους φόβους μας".

4. Να κατασκευάσετε τους πίνακες αληθείας για τις ακόλουθες Προτάσεις:

(α) (¬ A) ή (¬ B).

(β) A ή (¬ B).

(γ) (¬ B) ή B.

(δ) (¬ B), και B.

(ε) A και (B ή C)

(στ) (A και B) ή C

(ζ) (¬ A ή B) και C

2.1.3 Η συνεπαγωγή Προτάσεων

Υπάρχει ένας ακόμη τρόπος να συνθέσουμε δύο Προτάσεις για να προκύψει μια άλλη Πρόταση.

Ας ξεκινήσουμε με ένα παράδειγμα: Θεωρούμε την Πρόταση:

R : "Αν ο ακέραιος αριθμός a είναι πολλαπλάσιο του 6, τότε ο a είναι πολλαπλάσιο του 2".

Προφανώς η Πρόταση αυτή είναι αληθής.

Ας δούμε πώς η Πρόταση αυτή αναλύεται σε (ή μάλλον, καλύτερα, συντίθεται από) δύο άλλες Προτάσεις.

Θεωρούμε τις Προτάσεις:

P : "Ο ακέραιος αριθμός a είναι πολλαπλάσιο του 6".
Q : "Ο ακέραιος αριθμός a είναι πολλαπλάσιο του 2".

Τότε έχουμε για την αρχική Πρόταση.

R : "Αν P, τότε Q".

Γενικά, όταν έχουμε δύο Προτάσεις A και B, μπορούμε να σχηματίσουμε μια νέα Πρόταση:

"Αν A, τότε B",

η οποία "διαβάζεται" και ως εξής:

"Η A συνεπάγεται την B"

και θα συμβολίζεται ως

"Α $\Longrightarrow$ Β"[10].

Η νέα Πρόταση θα ονομάζεται **συνεπαγωγή**. Μια συνεπαγωγή θα ονομάζεται και **υποθετική** Πρόταση, υπό την έννοια:

> Υποθέτουμε ότι δεχόμαστε την πρώτη Πρόταση Α. Τότε δεχόμαστε την δεύτερη Πρόταση Β.

Οι Προτάσεις Α και Β αποτελούν τα *συνθετικά* της συνεπαγωγής "Α $\Longrightarrow$ Β" (πρώτο και δεύτερο συνθετικό αντίστοιχα). Επίσης, η Πρόταση Α θα ονομάζεται **υπόθεση** ή **παραδοχή** και η Πρόταση Β θα ονομάζεται **συμπέρασμα**.

Εφόσον έχουμε την νέα Πρόταση "Αν Α, τότε Β", γεννάται το ερώτημα: Ποιες είναι οι τιμές αληθείας της; Τι σχέση έχουν οι τιμές αληθείας των Προτάσεων Α και Β με τις τιμές αληθείας της νέας Πρότασης "Αν Α, τότε Β"; Μπορούμε να κατασκευάσουμε τον πίνακα αληθείας της;

Η μόνη πρωταρχική και "απαράβατη παραδοχή" είναι ότι:

> * Η Πρόταση "Αν η Α είναι αληθής, τότε (αναγκαστικά) η Β είναι αληθής" είναι αληθής *

Πριν κατασκευάσουμε τον πίνακα αληθείας, ας δούμε την άρνηση της Πρότασης "Αν Α, τότε Β". Τι σημαίνει η άρνηση ¬("Αν Α, τότε Β");

Η προφανής απάντηση είναι ότι η "Α δεν συνεπάγεται την Β". Τι σημαίνει αυτό; Μα το ότι την στιγμή που δεχόμαστε την Πρόταση Α ταυτόχρονα δεχόμαστε ότι ισχύει η άρνηση της Β.

Ας το δούμε σε όλους τους δυνατούς συνδυασμούς για τις τιμές αληθείας της Πρότασης Α και της Πρότασης Β.

Υποθέτουμε ότι η Α είναι αληθής και η Β αληθής. Τότε, από την απαράβατη παραδοχή, έχουμε ότι η Πρόταση "Αν Α, τότε Β" είναι αληθής, άρα η άρνησή της ¬("Αν Α, τότε Β") είναι ψευδής.

Υποθέτουμε ότι η Α είναι ψευδής και η Β αληθής. Στην περίπτωση αυτή η άρνηση ¬("Αν Α, τότε Β"), δηλαδή η "Α δεν συνεπάγεται την Β", είναι ψευδής. Γιατί; θα αναρωτηθεί κάποιος. Μα, αφού η Α είναι ψευδής, η αλήθεια της Β δεν εξαρτάται από την Α. Οπότε, αφού η ¬("Αν Α, τότε Β") είναι ψευδής η αρχική Πρόταση "Αν Α, τότε Β", στην περίπτωση αυτή, είναι αληθής.

Υποθέτουμε ότι η Α είναι ψευδής και η Β ψευδής. Στην περίπτωση αυτή η άρνηση ¬("Αν Α, τότε Β"), δηλαδή η "Α δεν συνεπάγεται την Β", είναι ψευδής. Γιατί; θα αναρωτηθεί κάποιος. Μα, όπως προηγουμένως, αφού η Α είναι ψευδής, η αλήθεια της Β δεν εξαρτάται από την Α. Οπότε, αφού η ¬("Αν Α, τότε Β") είναι ψευδής, η αρχική Πρόταση "Αν Α, τότε Β", στην περίπτωση αυτή, είναι αληθής.

Υποθέτουμε ότι η Α είναι αληθής και η Β ψευδής. Στην περίπτωση αυτή η άρνηση ¬("Αν Α, τότε Β"), δηλαδή η "Α δεν συνεπάγεται την Β", είναι αληθής. Γιατί; θα αναρωτηθεί κάποιος. Αν υποθέσουμε ότι η ¬("Αν Α, τότε Β"), δηλαδή η "Α δεν συνεπάγεται την Β", είναι ψευδής, τότε θα έχουμε ότι η αρχική Πρόταση "Αν Α, τότε Β" είναι αληθής, κάτι που αντιβαίνει στην απαράβατη αρχή "Αν η Α είναι αληθής, τότε (αναγκαστικά) η Β είναι αληθής" είναι αληθής.

Από τα προηγούμενα έπεται ότι ο πίνακας αληθείας για την Πρόταση "Α $\Longrightarrow$ Β" είναι ο

[10]Το σύμβολο $\Longrightarrow$ είναι το πλέον *κακοποιημένο* σύμβολο στα Μαθηματικά, λόγω λανθασμένης και καταχρηστικής χρήσης.

A	B	A $\Longrightarrow$ B
A	A	A
A	Ψ	Ψ
Ψ	A	A
Ψ	Ψ	A

Για αποσαφήνιση των ανωτέρω μερικά ακόμη παραδείγματα:

i. "Αν η θάλασσα είναι μελάνι, τότε ο ουρανός είναι χαρτί".

Εδώ έχουμε τις Προτάσεις

A : "Η θάλασσα είναι μελάνι".

B : "Ο ουρανός είναι χαρτί".

Και την συνεπαγωγή "A $\Longrightarrow$ B".

Η συνεπαγωγή είναι αληθής, διότι η ψευδής Πρόταση A : "Η θάλασσα είναι μελάνι" **δεν** καθορίζει τι είναι ο ουρανός (εν προκειμένω τον ψευδή ισχυρισμό B : "Ο ουρανός είναι χαρτί").

Η περίπτωση αυτή αναπαριστάται στην τελευταία γραμμή του πίνακα αληθείας.

ii. "Αν βρέχει, τότε έχουμε συννεφιά".

Εδώ έχουμε τις Προτάσεις

A : "Βρέχει".

B : "Έχουμε συννεφιά".

Και την συνεπαγωγή "A $\Longrightarrow$ B".

Η συνεπαγωγή είναι αληθής.

Πράγματι, υποθέτουμε ότι η Πρόταση A : "Βρέχει" είναι αληθής, τότε (αναγκαστικά δεχόμαστε ότι) η Πρόταση B : "Έχουμε συννεφιά" είναι αληθής. Επομένως, από την απαράβατη παραδοχή, έχουμε ότι η συνεπαγωγή είναι αληθής.

Η περίπτωση αυτή αναπαριστάται στην πρώτη γραμμή του πίνακα αληθείας.

Υποθέτουμε τώρα ότι η Πρόταση A : "Βρέχει" είναι ψευδής, τότε, το αν η Πρόταση B : "Έχουμε συννεφιά" είναι αληθής ή ψευδής δεν εξαρτάται από την (ψευδή) Πρόταση A : "Βρέχει". Συνεπώς, και στην περίπτωση αυτή η συνεπαγωγή "A $\Longrightarrow$ B" είναι αληθής.

Η περίπτωση αυτή αναπαριστάται στην τρίτη και τέταρτη γραμμή του πίνακα αληθείας (ανάλογα με το αν η πρόταση B : "Έχουμε συννεφιά" είναι αληθής ή ψευδής).

iii. "Αν έχουμε συννεφιά, τότε βρέχει".

Εδώ έχουμε τις Προτάσεις

A : "Έχουμε συννεφιά".

B : "Βρέχει".

Και την συνεπαγωγή "A $\Longrightarrow$ B".

Υποθέτουμε ότι η Πρόταση Α: "Έχουμε συννεφιά" είναι αληθής. Τότε, αν η Πρόταση Β: "Βρέχει" είναι αληθής, από την απαράβατη παραδοχή έχουμε ότι η συνεπαγωγή "Α $\Longrightarrow$ Β" είναι αληθής.

Η περίπτωση αυτή αναπαριστάται στην πρώτη γραμμή του πίνακα αληθείας.

Ενδέχεται όμως η Πρόταση Β: "Βρέχει" να είναι ψευδής (κανείς δεν εγγυάται ότι βρέχει, όταν έχουμε συννεφιά). Επομένως, η συνεπαγωγή "Α $\Longrightarrow$ Β" είναι ψευδής.

Η περίπτωση αυτή αναπαριστάται στην δεύτερη γραμμή του πίνακα αληθείας.

Υποθέτουμε ότι η Πρόταση Α: "Έχουμε συννεφιά" είναι ψευδής (δηλαδή έχουμε ηλιοφάνεια), τότε η Πρόταση Β: "Βρέχει" είναι (αναγκαστικά) ψευδής. Επομένως, η συνεπαγωγή "Α $\Longrightarrow$ Β" είναι αληθής.

Η περίπτωση αυτή αναπαριστάται στην τέταρτη γραμμή του πίνακα αληθείας.

iv. Αν $-1 = 1$, τότε $1 = 1$.

Εδώ έχουμε τις Προτάσεις

Α: "$-1 = 1$".

Β: "$1 = 1$".

Και την συνεπαγωγή "Α $\Longrightarrow$ Β".

Η συνεπαγωγή είναι αληθής. Πράγματι, εδώ η Πρόταση Α: "$-1 = 1$" είναι ψευδής, αλλά, θα έλεγε κάποιος, αφού αυτήν δεχόμαστε, υψώνουμε και τα δύο μέλη στο τετράγωνο (θεωρώντας ότι για οποιουσδήποτε πραγματικούς αριθμούς x και y η συνεπαγωγή $x = y \Longrightarrow x^2 = y^2$ είναι πάντα αληθής) καταλήγουμε στην αληθή Πρόταση Β: "$1 = 1$".

Η περίπτωση αυτή αναπαριστάται στην τρίτη γραμμή του πίνακα αληθείας.

v. Αν $1 = 2$, τότε $5 = 6$.

Εδώ έχουμε τις Προτάσεις

Α: "$1 = 2$".

Β: "$5 = 6$".

Και την συνεπαγωγή "Α $\Longrightarrow$ Β".

Η συνεπαγωγή είναι αληθής. Πράγματι, εδώ η Πρόταση Α: "$1 = 2$" είναι ψευδής, αλλά, θα έλεγε κάποιος, αφού αυτήν δεχόμαστε, προσθέτουμε και στα δύο μέλη το 4 (θεωρώντας ότι για οποιουσδήποτε πραγματικούς αριθμούς x και y και r η συνεπαγωγή $x = y \Longrightarrow x + r = y + r$ είναι πάντα αληθής) καταλήγουμε στην ψευδή Πρόταση Β: "$5 = 6$".

Η περίπτωση αυτή αναπαριστάται στην τέταρτη γραμμή του πίνακα αληθείας.

vi. "Αν οι ακέραιοι x και y είναι άρτιοι, τότε ο $x + y$ είναι περιττός".

Εδώ έχουμε τις Προτάσεις

Α(x, y): "οι ακέραιοι x και y είναι άρτιοι".

Β(x, y): "Ο $x + y$ είναι περιττός".

Και την συνεπαγωγή "Α$(x, y) \Longrightarrow$ Β(x, y)".

Εδώ έχουμε Προτάσεις με μεταβλητές, οι οποίες υπό την στενή έννοια του όρου δεν είναι Προτάσεις, αλλά γίνονται Προτάσεις για συγκεκριμένες τιμές των μεταβλητών x και y (ανοικτές Προτάσεις, βλέπε την Παρατήρηση $2.1.3_3$ και την συζήτηση στην σελίδα 36).

Ας δούμε μερικές περιπτώσεις για την αλήθεια της συνεπαγωγής

$$\text{“A}(x,\, y) \Longrightarrow \text{B}(x,\, y)\text{”}$$

για συγκεκριμένες τιμές των x και y.

Αν στην θέση των x και y έχουμε δύο συγκεκριμένους άρτιους αριθμούς a και b, τότε η Πρόταση $\text{A}(a,\, b)$: “οι ακέραιοι a και b είναι άρτιοι” είναι αληθής, ενώ η Πρόταση $\text{B}(a,\, b)$: “Ο $a+b$ είναι περιττός” είναι ψευδής. Οπότε, η συνεπαγωγή “$\text{A}(a,\, b) \Longrightarrow \text{B}(a,\, b)$” είναι ψευδής.

Αν στην θέση των x και y έχουμε δύο συγκεκριμένους περιττούς αριθμούς a και b, τότε η Πρόταση $\text{A}(a,\, b)$: “οι ακέραιοι a και b είναι άρτιοι” είναι ψευδής, ενώ η Πρόταση $\text{B}(a,\, b)$: “Ο $a+b$ είναι περιττός” είναι ψευδής. Οπότε, η συνεπαγωγή “$\text{A}(a,\, b) \Longrightarrow \text{B}(a,\, b)$” είναι αληθής.

Αν στην θέση των x και y έχουμε δύο συγκεκριμένους αριθμούς a και b, με τον έναν εξ αυτών άρτιο και τον άλλο περιττό, τότε η Πρόταση $\text{A}(a,\, b)$: “οι ακέραιοι a και b είναι άρτιοι” είναι ψευδής, ενώ η Πρόταση $\text{B}(a,\, b)$: “Ο $a+b$ είναι περιττός” είναι αληθής. Οπότε, η συνεπαγωγή “$\text{A}(a,\, b) \Longrightarrow \text{B}(a,\, b)$” είναι αληθής.

Μετά και τα παραδείγματα αυτά έχει αποσαφηνιστεί γιατί ο πίνακας αληθείας για την συνεπαγωγή “$\text{A} \Longrightarrow \text{B}$” είναι ο ανωτέρω.

Παρ’ όλα ταύτα, μερικές παρατηρήσεις είναι αναγκαίες.

Παρατηρήσεις 2.1.13.

1. Στην καθημερινότητα η συνεπαγωγή “Αν A ,τότε B” παρερμηνεύεται ως “Αν η A είναι αληθής, τότε η B είναι αληθής” και θεωρείται η μόνη αληθής συνεπαγωγή. Αυτή είναι η απαράβατη παραδοχή που αναφέραμε προηγουμένως. Αλλά, όπως είδαμε, δεν είναι η μόνη περίπτωση. Η παρερμηνεία αυτή (ίσως) οφείλεται στην εξής σύγχυση: Άλλο είναι το “δέχομαι την Πρόταση P” και άλλο “η Πρόταση P είναι αληθής”.

2. Η συνεπαγωγή “$\text{A} \Longrightarrow \text{B}$” εδώ αποτελεί μια νέα Πρόταση, της οποίας αναζητούμε την τιμή αληθείας. Το σύμβολο $\Longrightarrow$ **δεν** δηλώνει ότι έχουμε μια “αποδεικτική” διαδικασία, η οποία με την υπόθεση A (μέσω λογικών επιχειρημάτων) καταλήγει στο συμπέρασμα B (πρόκειται για *κακοποίηση* του συμβόλου $\Longrightarrow$). Επομένως, η *αφελής* απορία: “Πώς είναι δυνατόν το ψευδές της Πρότασης A να συνεπάγεται την αλήθεια της Πρότασης B;” (είναι η τρίτη γραμμή στον ανωτέρω πίνακα αληθείας) δεν είναι μια....*Μαθηματική απορία*.

   Συνεπώς, το αληθές ή ψευδές της Πρότασης “Αν A ,τότε B” (όπως και κάθε Πρότασης) καθορίζεται από τον πίνακα αληθείας της....και τέλος.

3. Η αλήθεια της Πρότασης “Αν A τότε B” δεν μας λέει *τίποτε* για το αληθές ή το ψευδές των Προτάσεων A και B. Αρκεί να ανατρέξουμε στο πρώτο από τα παραδείγματα: “Αν η θάλασσα είναι μελάνι, τότε ο ουρανός είναι χαρτί”.

4. Η άρνηση της συνεπαγωγής "Αν Α τότε Β" **δεν** αποτελεί συνεπαγωγή (γιατί;).

Ας σχολιάσουμε περισσότερο την άρνηση της συνεπαγωγής "Αν Α τότε Β" επεκτείνοντας τον προηγούμενο πίνακα αληθείας.

Α	Β	$A \Longrightarrow B$	$\neg (A \Longrightarrow B)$	$A \wedge (\neg B)$
Α	Α	Α	Ψ	Ψ
Α	Ψ	Ψ	Α	Α
Ψ	Α	Α	Ψ	Ψ
Ψ	Ψ	Α	Ψ	Ψ

Τι παρατηρούμε; Η άρνηση $\neg(A \Longrightarrow B)$ είναι ισοδύναμη με την Πρόταση $A \wedge (\neg B)$.

Ισοδύναμες εκφράσεις της Πρότασης "Αν Α τότε Β".

Υπάρχουν πολλές (ισοδύναμες) εκφράσεις, με τις οποίες μπορούμε να εκφράσουμε την Πρόταση "Αν Α τότε Β".

Θα αναφέρουμε μερικές:

i. "Β, αν Α".

   Ας δούμε το παράδειγμα: "Αν $1 = 2$, τότε $5 = 6$". Είναι ακριβώς το ίδιο αν πούμε "$5 = 6$, αν $1 = 2$ ".

ii. "Β, οσάκις Α"[11]. Επομένως, περισσότερο εκφραστικά, θα μπορούσαμε να πούμε: "Δεχόμαστε την Β, κάθε φορά που δεχόμαστε την Α"

iii. "Η Α είναι ικανή συνθήκη για την Β".

   Πάλι το ίδιο παράδειγμα: "Η ισότητα $1 = 2$ είναι ικανή συνθήκη για να ισχύει η ισότητα $5 = 6$".

iv. "Η Β είναι αναγκαία συνθήκη για την Α".

   Ας δούμε το παράδειγμα: "Αν βρέχει, τότε έχουμε συννεφιά". Είναι ακριβώς το ίδιο με το να πούμε: Η "Έχουμε συννεφιά" είναι αναγκαία συνθήκη για την "Βρέχει".

v. "Α, μόνο αν Β".

Εδώ πρέπει να είμαστε πιο προσεκτικοί. Ας δούμε πρώτα το παράδειγμα: "Αν βρέχει, τότε έχουμε συννεφιά". Ας το αντικαταστήσουμε με το "Βρέχει, μόνο αν έχουμε συννεφιά". Εδώ έχουμε ότι, αν η Πρόταση "Βρέχει" είναι αληθής, τότε η Πρόταση "Έχουμε συννεφιά" είναι αληθής και συνεπώς η συνεπαγωγή "Αν βρέχει, τότε έχουμε συννεφιά" είναι αληθής. Όπως και η Πρόταση "Βρέχει, μόνο αν έχουμε συννεφιά" είναι αληθής.

Ας δούμε τώρα το παράδειγμα: "Αν έχουμε συννεφιά, τότε βρέχει ". Υποθέτουμε ότι η Πρόταση "Έχουμε συννεφιά" είναι αληθής, ενώ η Πρόταση "Βρέχει" είναι ψευδής, όποτε η συνεπαγωγή "Αν έχουμε συννεφιά, τότε βρέχει " είναι ψευδής. Ας αντικαταστήσουμε τώρα την συνεπαγωγή αυτή με την "Έχουμε συννεφιά, μόνο αν βρέχει", η οποία και αυτή είναι ψευδής.

[11] Για όσους δεν γνωρίζουν την σημασία του *οσάκις*. Σημαίνει 'κάθε φορά που'.

Για την γενική θεώρηση. Στην Πρόταση "Α, μόνο αν Β" δίνουμε την σημασία 'Η Α είναι αληθής μόνο αν η Β είναι αληθής'.

Υποθέτουμε ότι η Πρόταση "Αν Α, τότε Β" είναι αληθής.

Έχουμε δύο δυνατότητες για την Πρόταση Α.

Αν η Πρόταση Α είναι αληθής, τότε (αναγκαστικά) η Πρόταση Β είναι αληθής (δεν μπορεί να είναι ψευδής). Συνεπώς, έχουμε την αλήθεια της Πρότασης "Α, μόνο αν Β".

Αν η Πρόταση Α είναι ψευδής, τότε η Β είναι ψευδής ή αληθής (δεν ξεχνάμε ότι έχουμε υποθέσει ότι η Πρόταση "Αν Α, τότε Β" είναι αληθής). Και στις δύο περιπτώσεις έχουμε το αληθές της Πρότασης "Α, μόνο αν Β".

Αν τώρα υποθέσουμε ότι η Πρόταση "Αν Α, τότε Β" είναι ψευδής, τότε η μόνη περίπτωση που έχουμε είναι η Α αληθής και η Β ψευδής. Μα τότε πάλι η Πρόταση "Α, μόνο αν Β" είναι ψευδής.

Λεπτολογώντας περισσότερο στην συνεπαγωγή Προτάσεων.

Όπως έχουμε ήδη επισημάνει, στην καθημερινότητα, η χρήση της Ελληνικής γλώσσας, πολλές φορές, δημιουργεί ασάφειες και παρερμηνείες, οι οποίες, ορισμένες φορές, περνούν απαρατήρητες. Ενώ, ορισμένες φορές μπορεί να έχουν σοβαρές επιπτώσεις. Ας δούμε μερικά παραδείγματα.

i. "Αν βρέχει, τότε δεν θα έλθω στην προγραμματισμένη συνάντηση".

   Η Πρόταση είναι σαφής, στο τι θα συμβεί αν βρέχει, ενώ **δεν** αναφέρει τίποτε για το τι θα συμβεί αν δεν βρέχει.

   Πολλές φορές όμως, στην καθημερινότητα, αυτό εκλαμβάνεται (λανθασμένα), ότι αν δεν βρέχει, τότε σίγουρα θα έλθω στην συνάντηση.

ii. Ο καθηγητής κάνει την εξής δήλωση στον φοιτητή: "Αν δεν πάρετε προβιβάσιμο βαθμό στις εξετάσεις, τότε δεν θα κατοχυρωθεί το μάθημα ως επιτυχές".

   Η Πρόταση είναι σαφής στο τι θα συμβεί, αν ο φοιτητής δεν πάρει προβιβάσιμο βαθμό στις εξετάσεις. Ενώ, **δεν** αναφέρει τίποτε για το τι θα συμβεί αν ο φοιτητής πάρει προβιβάσιμο βαθμό στις εξετάσεις.

   Αυτή η δήλωση του καθηγητή στην "φοιτητική κοινότητα" εκλαμβάνεται (κακώς) ως:

   "Αν πάρω προβιβάσιμο βαθμό στις εξετάσεις, τότε κατοχυρώνω το μάθημα".

iii. "Αν είσαι Μαθηματικός, τότε είσαι ευφυής"[12].

   Η Πρόταση **δεν** αναφέρει τίποτε για τους μη Μαθηματικούς.

   Αυτή η Πρόταση, πέραν του ότι είναι ψευδής, ενδέχεται να εγείρει αντιδράσεις του τύπου "Δηλαδή, μόνο οι Μαθηματικοί είναι ευφυείς;"

iv. Ας παραλλάξουμε το προηγούμενο παράδειγμα αντικαθιστώντας την λέξη Μαθηματικός με την λέξη άνδρας. "Αν είσαι άνδρας, τότε είσαι ευφυής"[13].

   Η Πρόταση **δεν** αναφέρει τίποτε για τις γυναίκες.

   Εδώ οι...αντιδράσεις ενδέχεται να είναι πιο έντονες...μέχρι, αυτός που κάνει μια τέτοια δήλωση, να συρθεί στα δικαστήρια για...σεξισμό για κάτι, το οποίο **δεν** υπονοεί η Πρόταση αυτή.

[12] Προσοχή!...Να έχουμε το νού μας, η Πρόταση είναι ψευδής!

[13] Προσοχή!...Να έχουμε το νού μας, η Πρόταση είναι ψευδής!

v. "Αν ο ακέραιος αριθμός a είναι δύναμη του 2, τότε είναι άρτιος".

   Η Πρόταση **δεν** αναφέρει τίποτε για τους ακεραίους, οι οποίοι δεν είναι δύναμη του 2.

vi. "Αν ο ακέραιος αριθμός a δεν είναι δύναμη του 2, τότε ο a δεν είναι άρτιος".

   Η Πρόταση **δεν** αναφέρει τίποτε για τους ακεραίους, οι οποίοι είναι δύναμη του 2.

vii. "Αν ο ακέραιος a δεν είναι άρτιος, τότε ο αριθμός a δεν είναι δύναμη του 2".

   Η Πρόταση **δεν** αναφέρει τίποτε για τους ακεραίους, οι οποίοι είναι άρτιοι.

Από τα προηγούμενα καθίσταται αναγκαίο να δώσουμε κάποιους ορισμούς.

Ορισμοί 2.1.14. Έστω Α και Β δύο Προτάσεις και η συνεπαγωγή

"Αν Α, τότε Β" (∗).

a. Η συνεπαγωγή "Αν Β, τότε Α" θα ονομάζεται **αντίστροφη** συνεπαγωγή της (∗).

b. Η συνεπαγωγή "Αν ¬Α, τότε ¬Β" θα ονομάζεται **αντίθετη** συνεπαγωγή της (∗).

c. Η συνεπαγωγή "Αν ¬Β, τότε ¬Α" θα ονομάζεται **αντιθετοαντίστροφη** συνεπαγωγή της (∗).

Επειδή στην καθομιλουμένη, ορισμένες φορές, οι λέξεις *αντίστροφη* και *αντίθετη*, ως προς την σημασία, συγχέονται και θεωρούνται ταυτόσημες, πρέπει να επισημάνουμε την διαφορά μεταξύ της αντίθετης και της αντίστροφης συνεπαγωγής.

Στο πρώτο παράδειγμα, η αντίστροφη συνεπαγωγή της

"Αν βρέχει, τότε δεν θα έλθω στην προγραμματισμένη συνάντηση"

είναι η

"Αν δεν έλθω στην προγραμματισμένη συνάντηση, τότε θα βρέχει",

η αντίθετη είναι η

"Αν δεν βρέχει, τότε θα έλθω στην προγραμματισμένη συνάντηση".

Υποθέτουμε ότι η Πρόταση Α : "Βρέχει" είναι αληθής και η Πρόταση Β : "Δεν θα έλθω στην προγραμματισμένη συνάντηση" είναι ψευδής. Τότε η συνεπαγωγή "Αν Α, τότε Β" είναι ψευδής, αλλά η αντίστροφη "Αν Β, τότε Α" είναι αληθής (γιατί;).

Αυτό είναι αρκετό για να συμπεράνουμε το εξής γενικό

> Συμπέρασμα: Μια συνεπαγωγή **δεν** είναι (πάντα) ισοδύναμη με την αντίστροφή της.

ή με ισοδύναμη διατύπωση:

> Υπάρχουν συνεπαγωγές, οι οποίες δεν είναι ισοδύναμες με την αντίστροφή τους.

Υποθέτουμε ότι η Πρόταση Α : "Βρέχει" είναι ψευδής και η Πρόταση Β : "Δεν θα έλθω στην προγραμματισμένη συνάντηση" είναι αληθής. Τότε η συνεπαγωγή "Αν Α, τότε Β" είναι αληθής, αλλά η αντίθετη ¬ Α, τότε ¬ Β" είναι ψευδής (γιατί;).

Αυτό είναι αρκετό για να συμπεράνουμε το εξής γενικό

> Συμπέρασμα: Μια συνεπαγωγή **δεν** είναι (πάντα) ισοδύναμη με την αντίθετή της.

ή με ισοδύναμη διατύπωση:

> Υπάρχουν συνεπαγωγές, οι οποίες δεν είναι ισοδύναμες με την αντίθετή τους.

Ας δούμε τώρα την αντιθετοαντίστροφη της Πρότασης αυτής. Είναι η:

"Αν έλθω στην προγραμματισμένη συνάντηση, τότε δεν θα βρέχει".

Υποθέτουμε ότι η αρχική συνεπαγωγή "Αν βρέχει, τότε δεν θα έλθω στην προγραμματισμένη συνάντηση" είναι ψευδής. Αυτό συμβαίνει (βλέπε τον πίνακα αληθείας μιας συνεπαγωγής) μόνο στην περίπτωση, όπου η Πρόταση Α : "Βρέχει" είναι αληθής και η Πρόταση Β : "Δεν θα έλθω στην προγραμματισμένη συνάντηση" είναι ψευδής. Στην περίπτωση αυτή, η Πρόταση $\neg$ Β είναι αληθής και η Πρόταση $\neg$ Α είναι ψευδής. Οπότε, **και** η αντιθετοαντίστροφη της αρχικής συνεπαγωγής είναι και αυτή ψευδής.

Θα μπορούσαμε να εξαντλήσουμε όλες τις περιπτώσεις μία–μία για να δούμε ότι κάθε φορά που η αρχική Πρόταση "Αν βρέχει, τότε δεν θα έλθω στην προγραμματισμένη συνάντηση" είναι αληθής, τότε και η αντιθετοαντίστροφή της "Αν έλθω στην προγραμματισμένη συνάντηση, τότε δεν θα βρέχει" είναι αληθής.

Αλλά τι γίνεται αν έχουμε γενικά μια συνεπαγωγή "Αν Α, τότε Β" και την αντιθετοαντίστροφή της "Αν $\neg$ Β, τότε $\neg$ Α";

Ας δούμε τον πίνακα αληθείας για τις δύο αυτές Προτάσεις.

Α	Β	$A \Longrightarrow B$	$\neg B \Longrightarrow \neg A$
Α	Α	Α	Α
Α	Ψ	Ψ	Ψ
Ψ	Α	Α	Α
Ψ	Ψ	Α	Α

Από τον Πίνακα αυτόν και τον ορισμό της ισοδυναμίας Προτάσεων (Ορισμός 2.1.9) απορρέει η εξής σημαντική διαπίστωση:

> ***Η αντιθετοαντιστροφή μιας συνεπαγωγής είναι ισοδύναμη (ως Πρόταση) με την (αρχική) συνεπαγωγή.***[14].

Η (Λογική) ισοδυναμία Προτάσεων.

Στην Παράγραφο για την ισοδυναμία δύο Προτάσεων είχαμε θέσει τον εξής Ορισμό:

> *Δύο Προτάσεις P και Q θα ονομάζονται ισοδύναμες αν έχουν ίδιους πίνακες αληθείας.*

(Ορισμός 2.1.9).

Εδώ θα επιχειρήσουμε να δούμε την έννοια της ισοδυναμίας Προτάσεων υπό το πρίσμα της συνεπαγωγής Προτάσεων.

Ας δούμε τα εξής Παραδείγματα:

[14] Αργότερα, όταν θα μιλήσουμε για "Αποδεικτικές διαδικασίες", θα δούμε την χρησιμότητα αυτής της διαπίστωσης.

i. Έχουμε τις Προτάσεις

A : "Ο ακέραιος αριθμός a είναι δύναμη του 2" και

B : "Ο ακέραιος αριθμός a είναι άρτιος".

Λαμβάνουμε την συνεπαγωγή "Αν A, τότε B", δηλαδή την "Αν ο ακέραιος αριθμός a είναι δύναμη του 2, τότε ο a είναι άρτιος" και την αντίστροφή της

"Αν B, τότε A", δηλαδή την "Αν ο a είναι άρτιος, τότε ο ακέραιος αριθμός a είναι δύναμη του 2".

Προφανώς, στην πρώτη συνεπαγωγή, αν η πρώτη Πρόταση είναι αληθής, τότε η δεύτερη Πρόταση είναι αληθής.

Στην δεύτερη όμως συνεπαγωγή, αν η πρώτη Πρόταση είναι αληθής, δεν σημαίνει ότι η δεύτερη Πρόταση είναι αληθής.

Αυτό σημαίνει ότι η συνεπαγωγή "Αν A, τότε B" δεν είναι (Λογικά) ισοδύναμη με την αντίστροφή της "Αν B, τότε A".

ii. Έχουμε τις Προτάσεις

A : "Ο ακέραιος αριθμός a είναι άρτιος".

B : "Ο ακέραιος αριθμός a^2 είναι άρτιος".

Παίρνουμε την συνεπαγωγή "Αν A, τότε B", δηλαδή την "Αν ο ακέραιος αριθμός a είναι άρτιος, τότε ο a^2 είναι άρτιος" και την αντίστροφή της.

"Αν B, τότε A", δηλαδή την "Αν ο a^2 είναι άρτιος, τότε ο ακέραιος αριθμός a είναι άρτιος".

Προφανώς, στην πρώτη συνεπαγωγή, αν η πρώτη Πρόταση είναι αληθής, τότε η δεύτερη Πρόταση είναι αληθής.

Αλλά και στην δεύτερη συνεπαγωγή, αν η πρώτη Πρόταση είναι αληθής, τότε η δεύτερη Πρόταση είναι αληθής.

Αυτό σημαίνει ότι η συνεπαγωγή "Αν A, τότε B" είναι (Λογικά) ισοδύναμη με την αντίστροφή της "Αν B, τότε A".

Από τα προηγούμενα παραδείγματα οδηγούμαστε στον εξής ορισμό:

Ορισμός 2.1.15. Έστω οι Προτάσεις A και B. Αν οι συνεπαγωγές "A$\Longrightarrow$B" και "B$\Longrightarrow$A" είναι και οι δύο αληθείς, τότε οι Προτάσεις A και B θα ονομάζονται **(Λογικά) ισοδύναμες**.

Δύο (Λογικά) ισοδύναμες Προτάσεις A και B θα συμβολίζονται ως εξής: "A $\Longleftrightarrow$ B" και θα προφέρεται ως "A, αν και μόνο αν B".

Παρατηρήσεις 2.1.16.

1. Αν συγκρίνουμε τον Ορισμό 2.1.9 με τον αμέσως προηγούμενο ορισμό, θα δούμε ότι ο ένας αναφέρεται στους πίνακες αληθείας των Προτάσεων A και B, ενώ ο άλλος στην ταυτόχρονη αλήθεια των Προτάσεων "A$\Longrightarrow$B" και "B$\Longrightarrow$A". Φαινομενικά πρόκειται για διαφορετικούς ορισμούς, στην πραγματικότητα πρόκειται για την ίδια Μαθηματική έννοια.

   Είναι μια προκλητική άσκηση, όπου ανακεφαλαιώνοντας όλα τα προηγούμενα, μπορείτε να δείτε ότι πράγματι πρόκειται για ισοδύναμους ορισμούς.

Πράγματι, αν κατασκευάσουμε (να το κάνετε!) τον πίνακα αληθείας για τις Προτάσεις "$(\mathrm{A} \Longrightarrow \mathrm{B}) \wedge (\mathrm{B} \Longrightarrow \mathrm{A})$" και "$\mathrm{A} \Longleftrightarrow \mathrm{B}$", θα δούμε ότι είναι ισοδύναμες ως Προτάσεις, οι οποίες είναι αληθείς, αν και μόνο αν οι (αρχικές) Προτάσεις Α και Β είναι ταυτόχρονα αληθείς ή ταυτόχρονα ψευδείς, δηλαδή ισοδύναμες.

Επομένως, μπορούμε στο εξής να παραλείπουμε την παρένθεση (Λογική) και να γράφουμε απλώς "ισοδυναμία Προτάσεων".

2. Προφανώς, από τον προηγούμενο ορισμό, απορρέει ότι δύο Προτάσεις είναι ισοδύναμες ακριβώς, αν και οι δύο είναι αληθείς ή και οι δύο είναι ψευδείς (γιατί;). Δεν έχετε παρά να πάρετε την άρνηση των Προτάσεων αυτών και να χρησιμοποιήσετε την διαπίστωση ότι: Η αντιθετοαντιστροφή μιας συνεπαγωγής είναι ισοδύναμη (ως Πρόταση) με την (αρχική) συνεπαγωγή.

   Συνεπώς, η ισοδυναμία "$\mathrm{A} \Longleftrightarrow \mathrm{B}$" (ως Πρόταση) είναι αληθής όταν τουλάχιστον μια από τις Προτάσεις "$\mathrm{A} \wedge \mathrm{B}$ ή $(\neg\ \mathrm{A}) \wedge (\neg\ \mathrm{B})$" είναι αληθής. Μα αυτό δεν είναι τίποτε άλλο από την διάζευξη των δύο τελευταίων Προτάσεων.

   Στον πίνακα αληθείας που ακολουθεί, όλα αυτά διαλευκαίνονται.

A	B	$\neg$A	$\neg$B	A$\wedge$B	($\neg$A)$\wedge$($\neg$B)	(A$\wedge$B)$\vee$(($\neg$A)$\wedge$($\neg$ B))	A$\Longleftrightarrow$B
A	A	Ψ	Ψ	A	Ψ	A	A
A	Ψ	Ψ	A	Ψ	Ψ	Ψ	Ψ
Ψ	A	A	Ψ	Ψ	Ψ	Ψ	Ψ
Ψ	Ψ	A	A	Ψ	A	A	A

3. Η έκφραση "αν και μόνο αν" προφανώς απορρέει από τις ισοδύναμες εκφράσεις μιας συνεπαγωγής (βλέπε σελ. 50), καθ' ότι η συνεπαγωγή $\mathrm{A} \Longrightarrow \mathrm{B}$ ισοδυνάμως εκφράζεται ως "Α μόνο αν Β" και η συνεπαγωγή $\mathrm{B} \Longrightarrow \mathrm{A}$ ισοδυνάμως εκφράζεται ως "Α αν Β"[15].

Παράδειγμα 2.1.17. Θεωρούμε τις Προτάσεις:

Α: "Ο πραγματικός αριθμός r ικανοποιεί την εξίσωση $x^2 - 5x + 6 = 0$" και
Β: "$r = 2$ ή $r = 3$".

Η συνεπαγωγή $\mathrm{A} \Longrightarrow \mathrm{B}$ (η *μόνο αν*) είναι προφανώς αληθής. Επίσης, η συνεπαγωγή $\mathrm{A} \Longleftarrow \mathrm{B}$ (η *αν*) είναι προφανώς αληθής. Συνεπώς, η ισοδυναμία $\mathrm{A} \Longleftrightarrow \mathrm{B}$ είναι αληθής.
Θεωρούμε τώρα τις Προτάσεις:

Α: "Ο πραγματικός αριθμός r ικανοποιεί την εξίσωση $x^2 - 5x + 6 = 0$" και
Γ: "$r = 2$".

Από τα προηγούμενα συνάγεται ότι η ισοδυναμία $\mathrm{A} \Longleftrightarrow \Gamma$ είναι ψευδής. Ποια από τις δύο συνεπαγωγές $\Longleftarrow$ και $\Longrightarrow$ είναι η ψευδής; Η συνεπαγωγή $\mathrm{A} \Longleftarrow \Gamma$ (η *αν*) είναι προφανώς αληθής (γιατί;). Αλλά, η συνεπαγωγή $\mathrm{A} \Longrightarrow \Gamma$ (η *μόνο αν*) είναι ψευδής, διότι υπάρχει και το $r = 3$ (πέραν του $r = 2$), το οποίο ικανοποιεί την εξίσωση $x^2 - 5x + 6 = 0$".

[15] Πολλοί στην αρχή μπερδεύονται για το ποια συνεπαγωγή αντιστοιχεί στο "αν" και ποια στο "μόνο αν". Αν και δεν έχει σημασία, με την *τριβή* θα διαλευκανθεί σιγά–σιγά.

Ταυτολογία Προτάσεων.

Στην καθημερινότητα χρησιμοποιούμε τον όρο "ταυτολογία" για να δηλώσουμε ότι μια Πρόταση (ένας ισχυρισμός) είναι "αυταπόδεικτα"[16] αληθής και επομένως αποτελεί περιττολογία η προσπάθεια να αποδείξουμε την αλήθειά της. Επίσης, με τον όρο ταυτολογία, ορισμένες φορές, δηλώνουμε την προσπάθεια να εξηγήσουμε μια έννοια χρησιμοποιώντας την ίδια έννοια.

Ας δούμε μερικά παραδείγματα:

"Αν η άνω όψη του νομίσματος δεν είναι *γράμματα*, τότε η κάτω όψη του νομίσματος είναι *γράμματα*".

Η συνεπαγωγή αυτή είναι πάντα αληθής. Μάλιστα δε το συμπέρασμα "τότε...." *περιττεύει.*

"Τα παιδιά του Ζεβεδαίου έχουν πατέρα τον Ζεβεδαίο".
"Η Μαρία κυοφορεί, δηλαδή είναι έγκυος".
"Ο ακέραιος αριθμός a είναι άρτιος, άρα δεν είναι περιττός".

Επίσης, εδώ έχουμε μια παρόμοια κατάσταση.

Στα Μαθηματικά μια Πρόταση θα ονομάζεται **ταυτολογία** αν είναι πάντα αληθής, δηλαδή στον πίνακα αληθείας της εμφανίζεται πάντα η ένδειξη Α (αληθής)[17].

Ας προσπαθήσουμε να γίνουμε πιο σαφείς.

Έστω η Πρόταση P. Συνθέτουμε την Πρόταση R: "$P \vee (\neg\, P)$". Η Πρόταση R είναι πάντα αληθής, ανεξαρτήτως αν η P είναι αληθής ή ψευδής, δηλαδή πρόκειται για ταυτολογία.

Οι συνεπαγωγές "$(P \wedge Q) \Longrightarrow P$" και "$P \Longrightarrow (P \vee Q)$" είναι επίσης ταυτολογίες. Δεδομένου ότι είναι πάντα αληθείς, ανεξαρτήτως από τις τιμές αληθείας των (επιμέρους) Προτάσεων P και Q.

Μια Πρόταση P θα ονομάζεται **αντίφαση** αν είναι πάντα ψευδής. Ισοδύναμα, αν η άρνησή της "$\neg\, P$" είναι ταυτολογία.

Συνεπώς, από τα προηγούμενα παραδείγματα έχουμε ότι: Οι Προτάσεις

$$\begin{aligned}
\neg\,(P \vee (\neg\, P)) &\equiv (\neg\, P) \wedge (\neg(\neg\, P)) \equiv (\neg\, P) \wedge P,\\
\neg\,((P \wedge Q) \Longrightarrow P) &\equiv (P \wedge Q) \wedge (\neg\, P) \equiv P \wedge (\neg\, P),\\
\neg(P \Longrightarrow (P \vee Q)) &\equiv P \wedge (\neg(P \vee Q)) \equiv P \wedge ((\neg\, P) \wedge (\neg\, Q)) \equiv P \wedge (\neg\, P)
\end{aligned}$$

είναι όλες αντιφάσεις.

Ερώτημα: Γιατί ισχύουν οι ισοδυναμίες Προτάσεων ($\equiv$) στις ανωτέρω Προτάσεις;

Δεν έχετε παρά να ανατρέξετε στους Νόμους του Morgan (σελ. 44) και στον πίνακα αληθείας στην σελίδα 50.

Η Πρόταση "Για έναν πραγματικό αριθμό x ισχύει $x = x+1$" είναι μια αντίφαση. Η άρνησή της "Για έναν πραγματικό αριθμό x ισχύει $x \neq x+1$" είναι μια ταυτολογία.

Η έννοια της αντίφασης είναι πολύ σημαντική και, όπως θα διαπιστώσουμε αργότερα, αποτελεί ένα *ισχυρό εργαλείο* στην αποδεικτική διαδικασία.

[16] Πρέπει να είμαστε προσεκτικοί στην χρήση λέξεων, όπως "αυταπόδεικτα", "πασιφανής", "προφανής", καθότι τέτοιοι χαρακτηρισμοί ενδέχεται να εμπεριέχουν υποκειμενισμό.

[17] Προσοχή! Εδώ έχουμε μια ταυτολογία. Προσπαθούμε να εξηγήσουμε τι σημαίνει ταυτολογία, χρησιμοποιώντας ταυτολογία!....*Αυτά είναι τα "ωραία" και συνάμα "δύσκολα".*

2.1.4 Ασκήσεις

1. Χωρίς να αλλάξετε την σημασία των ακολούθων Προτάσεων να τις *μετασχηματίσετε* στην μορφή "Αν P, τότε Q" ($\mathrm{P} \Longrightarrow \mathrm{Q}$)[18].

   (Βεβαιωθείτε πρώτα ποια Πρόταση θεωρείτε ως P και ποια ως Q).

   (α) Ένας ακέραιος αριθμός διαιρείται με το 8 μόνο αν διαιρείται με το 4.

   (β) Ισχύει ότι $x^3 + 12x + 4 < 3$, αν $x^2 < 5$.

   (γ) Ένας τετραγωνικός πίνακας είναι αντιστρέψιμος δεδομένου ότι η ορίζουσά του είναι μη μηδενική.

   (δ) Σε ένα ορθογώνιο τρίγωνο, αν c είναι το μήκος της υποτείνουσας, τότε $c^2 = a^2 + b^2$, όπου a, b είναι τα μήκη των δύο άλλων πλευρών του τριγώνου.

   (ε) Για να είναι μια πραγματική συνάρτηση συνεχής, είναι αρκετό να είναι παραγωγίσιμη.

   (στ) Για να είναι μια πραγματική συνάρτηση ολοκληρώσιμη, είναι αναγκαίο να είναι συνεχής.

   (ζ) Μια πραγματική συνάρτηση είναι ολοκληρώσιμη, οσάκις είναι συνεχής.

   (η) Η διακρίνουσα ενός τριωνύμου είναι αρνητική, μόνο αν το τριώνυμο έχει μη πραγματικές ρίζες.

   (θ) "Αποτυγχάνουμε μόνο αν σταματήσουμε να προσπαθούμε" (Ray Bradbury).

   (ι) "Οσάκις το πλήθος συμφωνεί μαζί μου, αισθάνομαι ότι σφάλλω" (Oscar Wilde).

   (ια) "Γενικά ο κόσμος δέχεται γεγονότα ως αληθή μόνο αν τα γεγονότα συμφωνούν με ό,τι ήδη πιστεύει" (Andy Rooney).

2. Να γράψετε την άρνηση των κάτωθι συνεπαγωγών:

   (α) Αν $x^2 + 2x + 1 = 0$, τότε $x = -1$,

   (β) Η $x^2 + x - 2 = 0$ συνεπάγεται ότι $x = 1$ ή $x = -2$,

   (γ) Αν πετύχετε άνω του 85 τοις εκατό στις εξετάσεις, τότε θα καταταγείτε μεταξύ των αριστούχων.

3. Χωρίς να αλλάξετε την σημασία των ακολούθων Προτάσεων να τις *μετασχηματίσετε* στην μορφή "P αν και μόνο αν Q" ($\mathrm{P} \Longleftrightarrow \mathrm{Q}$).

   (α) Για να είναι ένας τετραγωνικός πίνακας αντιστρέψιμος, πρέπει και αρκεί η ορίζουσά του να είναι διάφορη του μηδενός.

   (β) Αν ένα τριώνυμο έχει πραγματικές ρίζες, τότε έχει μη αρνητική διακρίνουσα και αντίστροφα.

   (γ) Αν $xy = 0$, τότε $x = 0$ ή $y = 0$ και αντίστροφα.

[18] Ενδέχεται κάποιες από αυτές τις Προτάσεις να μην γνωρίζουμε αν είναι αληθείς ή ψευδείς. Πολύ περισσότερο, ενδέχεται να μην είναι, ούτε καν, κατανοητές από Μαθηματικής άποψης. Επίσης, ενδέχεται να μην έχουμε τις απαραίτητες Μαθηματικές γνώσεις. Αυτό **δεν** (πρέπει να) μας εμποδίζει να επιχειρήσουμε την άσκηση.

(δ) Αν ο ακέραιος αριθμός a είναι άρτιος, τότε ο $3a$ είναι άρτιος και αν ο $3a$ είναι άρτιος, τότε ο a είναι άρτιος.

(ε) "Για να *γίνει* περιπέτεια ένα περιστατικό, είναι αναγκαίο και ικανό να το διηγηθεί *κάποιος*" (Jean-Paul Sartre).

4. Να κατασκευάσετε τους πίνακες αληθείας για κάθε μία από τις επόμενες Προτάσεις:

(i) $P \vee (Q \Longrightarrow R)$,

(ii) $(Q \vee R) \Longleftrightarrow (Q \wedge R)$,

(iii) $\neg\ (P \Longrightarrow R)$,

(iv) $(P \wedge (\neg\ P)) \vee Q$,

(v) $(P \wedge (\neg\ P)) \wedge Q$,

(vi) $P \wedge (\neg\ P) \Longrightarrow Q$,

(vii) $\neg\ (P \vee Q) \vee (\neg\ P)$,

(viii) $\neg\ (\neg\ P \vee \neg\ Q)$.

5. Υποθέτουμε ότι η Πρόταση P είναι αληθής, ενώ η Πρόταση Q είναι ψευδής. Ποιες από τις ακόλουθες Προτάσεις είναι αληθείς;

(i) "$P\ \vee (\neg\ Q)$".

(ii) "$\neg(P \vee Q)$".

(iii) "$\neg Q \Longrightarrow P$".

6. Υποθέτουμε ότι η Πρόταση $((P \wedge Q) \vee R) \Longrightarrow (R \vee S)$ είναι ψευδής. Να υπολογίσετε τις τιμές αληθείας για τις Προτάσεις P, Q, R, S.

7. Υποθέτουμε ότι η Πρόταση P είναι ψευδής και ότι η Πρόταση $(R \Longrightarrow S) \Longleftrightarrow (P \wedge Q)$ είναι αληθής. Να υπολογίσετε τις τιμές αληθείας για τις Προτάσεις R και S.

(Στην άσκηση αυτή, όπως και στην προηγούμενη, ο αντίστοιχος πίνακας αληθείας ίσως σας φανεί χρήσιμος).

8. Με την χρήση πινάκων αληθείας να αποδείξετε την ισοδυναμία των Προτάσεων:

(α) "$P \wedge (Q \vee R)$" $\equiv$ "$(P \wedge Q) \vee (P \wedge R)$".
(Ο επιμερισμός του "και" ως προς το "ή").

(β) "$P \vee (Q \wedge R)$" $\equiv$ "$(P \vee Q) \wedge (P \vee R)$".
(Ο επιμερισμός του "ή" ως προς το "και").
Παραβάλλετε τα δύο προηγούμενα αποτελέσματα με τις γνωστές ιδιότητες του επιμερισμού της τομής και ένωσης στα σύνολα.

(γ) "$P \Longrightarrow Q$" $\equiv$ "$(\neg P) \vee Q$".

(δ) "$(\neg P) \Longleftrightarrow Q$" $\equiv$ "$(P \Longrightarrow \neg\ Q) \wedge (\neg Q \Longrightarrow\ P)$".

9. Αποφανθείτε αν τα ακόλουθα ζεύγη Προτάσεων αποτελούν (ή δεν αποτελούν) ισοδύναμες Προτάσεις.

(α) "$P \wedge Q$" $\leftrightsquigarrow$ "$\neg\ (\neg P \vee \neg\ Q)$".

(β) "$\mathrm{P} \vee (\mathrm{Q} \wedge \mathrm{R})$" $\leftrightsquigarrow$ "$(\mathrm{P} \vee \mathrm{Q}) \wedge \mathrm{R}$".

(γ) "$\neg\ (\mathrm{P} \Longrightarrow \mathrm{Q})$" $\leftrightsquigarrow$ "$\mathrm{P} \wedge \neg\ \mathrm{Q}$".

(δ) "$(\mathrm{P} \Longrightarrow \mathrm{Q}) \vee \mathrm{R}$" $\leftrightsquigarrow$ "$\neg\ ((\mathrm{P} \wedge \neg\ \mathrm{Q}) \wedge \neg\ \mathrm{R})$".

10. Να σχηματίσετε την αντίστροφη κάθε μιας από τις ακόλουθες Προτάσεις.

(α) "Ένας ακέραιος αριθμός είναι άρτιος ή περιττός, αλλά όχι και τα δύο".

(β) "Η εξίσωση $x^2 + 2x + 3 = 0$ δεν έχει ακέραιες λύσεις".

(γ) "Αν η ευθεία ε τέμνει την ευθεία λ, τότε τέμνει κάθε άλλη ευθεία παράλληλη προς την λ".

(δ) Αν A, B, C είναι τρία σύνολα, τότε $A \cap (B \cup C) \subseteq (A \cup B) \cap (A \cup C)$.

(ε) "Ο πρωινός καφές είναι αναγκαίος για μένα, για να είμαι ευδιάθετος όλη μέρα".

(στ) "Ο πρωινός καφές είναι αρκετός, για μένα, για να είμαι ευδιάθετος όλη μέρα".

(ζ) "Η σταματάς να μιλάς ή αποβάλλεσαι".

11. Να σχηματίσετε την αντιθετοαντίστροφη κάθε μιας από τις ακόλουθες Προτάσεις.

(i) "Αν $x = 2$, τότε ο $\sqrt{x}$ είναι άρρητος".

(ii) "Αν ο ακέραιος αριθμός a είναι πρώτος, τότε $a = 2$ ή ο a είναι περιττός".

(iii) "Αν το E είναι τετράγωνο, τότε το E είναι ορθογώνιο παραλληλόγραμμο".

(iv) "Ένας κύκλος είναι έλλειψη".

(v) "Κάθε ρόμβος είναι τετράγωνο".

12. Στην επόμενη Πρόταση να προσδιορίσετε την αντίστροφή της, την αντίθετή της και την αντιθετοαντίστροφή της.

$$\text{“}\mathrm{P} \Longrightarrow (\mathrm{Q} \Longrightarrow \mathrm{R})\text{”}.$$

13. Με την βοήθεια ενός πίνακα αληθείας να δείξετε ότι η Πρόταση

$$((\mathrm{P} \wedge \mathrm{Q}) \Longrightarrow \mathrm{R}) \Longrightarrow (\neg\ \mathrm{R} \Longrightarrow\ (\neg\ \mathrm{P} \vee \neg\ \mathrm{Q})).$$

αποτελεί ταυτολογία.

14. Αποφανθείτε αν οι ακόλουθες Προτάσεις αποτελούν ταυτολογία.

(i) "$((\mathrm{A} \Longrightarrow \mathrm{B}) \Longrightarrow \mathrm{B}) \Longrightarrow \mathrm{B}$".

(ii) "$((\mathrm{A} \Longrightarrow \mathrm{B}) \Longrightarrow \mathrm{B}) \Longrightarrow \mathrm{A}$".

(iii) "$((\mathrm{A} \Longrightarrow \mathrm{B}) \Longrightarrow \mathrm{A}) \Longrightarrow \mathrm{A}$".

(iv) "$\mathrm{A} \Longrightarrow (\mathrm{B} \Longrightarrow (\mathrm{B} \Longrightarrow \mathrm{A}))$".

(v) "$(\mathrm{A} \wedge \mathrm{B}) \Longrightarrow (\mathrm{A} \vee \mathrm{C})$".

2.1.5 Ποσοδείκτες

Σε προηγουμένη παράγραφο (σελ. 36) είχαμε δει Προτάσεις με μεταβλητές (ανοικτές Προτάσεις), όπου η αλήθεια της Πρότασης εξαρτάται από την τιμή της μεταβλητής. Για παράδειγμα: Η (ανοικτή) Πρόταση

"Ο ακέραιος αριθμός x είναι περιττός"

για κάποιες τιμές του x είναι αληθής, ενώ για κάποιες τιμές του x είναι ψευδής. Θα μπορούσαμε να μετατρέψουμε την (ανοικτή) Πρόταση σε (δηλωτική) Πρόταση θέτοντας συγκεκριμένες τιμές για το x. Ας *τροποποιήσουμε* την προηγουμένη Πρόταση. Αν γράψουμε

"Για κάθε ακέραιο αριθμό x, ο x είναι περιττός",

τότε η πρόταση αυτή είναι μια (δηλωτική) Πρόταση, η οποία προφανώς είναι ψευδής. Αν γράψουμε

"Υπάρχουν ακέραιοι αριθμοί x, οι οποίοι είναι περιττοί",

τότε η πρόταση αυτή είναι μια (δηλωτική) Πρόταση, η οποία προφανώς είναι αληθής. Οι καίριες λέξεις, οι οποίες *μετασχημάτισαν* την προηγουμένη Πρόταση είναι "Για κάθε" και "Υπάρχουν".

Ορισμός 2.1.18. Η φράση **για κάθε** αποτελεί έναν **καθολικό ποσοδείκτη**, ο οποίος για συντομία θα συμβολίζεται ως $\forall$.

Η λέξη **υπάρχει(ουν)** αποτελεί έναν **υπαρξιακό ποσοδείκτη**, ο οποίος για συντομία θα συμβολίζεται ως $\exists$.

Επομένως, στο προηγούμενο παράδειγμα θα μπορούσαμε συμβολικά να γράψουμε:

"$\forall\ x \in \mathbb{Z},$ ο x είναι περιττός" και
"$\exists\ x \in \mathbb{Z},$ έτσι ώστε ο x να είναι περιττός".

Παρατήρηση 2.1.19. Ορισμένες φορές, αντί της φράσης "για κάθε", χρησιμοποιούμε την φράση "για όλα". Προσοχή! Στην καθομιλουμένη χρησιμοποιείται και η φράση "για κάθε ένα". Η φράση αυτή στα Μαθηματικά ενδέχεται να δημιουργήσει σύγχυση δεδομένου ότι υπονοεί ότι ισχύει (ή δεν ισχύει) κάτι για κάθε ένα ξεχωριστά από τα αντικείμενα που ενδιαφερόμαστε. Συνεπώς, πρέπει να αποφεύγεται ή να χρησιμοποιείται με μεγάλη προσοχή.

Επίσης, όταν χρησιμοποιούμε την λέξη "υπάρχει(ουν)" δεν ενδιαφερόμαστε να προσδιορίσουμε αν υπάρχει ένα ή πολλά στοιχεία, τα οποία να πληρούν κάποια ιδιότητα. Τις περισσότερες φορές μας αρκεί η ύπαρξη ενός στοιχείου που να πληροί μια ιδιότητα. Επομένως, απλώς για να δώσουμε έμφαση (χωρίς να αλλάξουμε την Μαθηματική έννοια), αντί του "υπάρχει", γράφουμε "υπάρχει τουλάχιστον ένα".

Εδώ πρέπει να επισημάνουμε την αντιδιαστολή "υπάρχει το πολύ ένα" και την έκφραση "υπάρχει ακριβώς ένα". Μέσω των παραδειγμάτων που ακολουθούν, θα διευκρινισθούν πολλά σημεία.

Παραδείγματα 2.1.20.

1. (i) Για κάθε x ισχύει $x > x/2$.

   (ii) Για κάθε θετικό πραγματικό αριθμό x ισχύει $x > x/2$.

(iii) Για κάθε πραγματικό αριθμό x ισχύει $x > x/2$.

Εδώ η πρώτη πρόταση δεν έχει νόημα. Δεν είναι ούτε καν (ανοικτή) Πρόταση, διότι δεν προσδιορίζεται το σύνολο στο οποίο ανήκει η μεταβλητή x (βλέπε σελ. 36).

Η δεύτερη Πρόταση είναι μια αληθής Πρόταση, ενώ η τρίτη Πρόταση είναι μια ψευδής Πρόταση.

Επομένως, πρέπει να είμαστε προσεκτικοί στον προσδιορισμό του συνόλου στο οποίο ανήκει η μεταβλητή.

2. (α) Για κάθε ακέραιο x υπάρχει ακέραιος y, έτσι ώστε $y > x$.

   (β) Για κάθε ακέραιο x υπάρχουν ακέραιοι y, έτσι ώστε $y > x$.

   (γ) Για κάθε ακέραιο x υπάρχει τουλάχιστον ένας ακέραιος y, έτσι ώστε $y > x$.

   (δ) Για κάθε ακέραιο x υπάρχει το πολύ ένας ακέραιος y, έτσι ώστε $y > x$.

   (ε) Για κάθε ακέραιο x υπάρχει ακριβώς ένας ακέραιος y, έτσι ώστε $y > x$.

   Οι τρεις πρώτες Προτάσεις είναι αληθείς και (στην συγκεκριμένη περίπτωση) έχουν την ίδια Μαθηματική σημασία. Συμβολικά δε, παριστάνονται ως εξής:

$$\forall\, x \in \mathbb{Z}\ \exists y \in \mathbb{Z}\ :\ y > x.$$[19]

   Οι δύο τελευταίες είναι (προφανώς;) ψευδείς.

3. Στο προηγούμενο παράδειγμα, όπου είχαμε την Πρόταση:

   "Για κάθε ακέραιο x υπάρχει ακέραιος y, έτσι ώστε $y > x$"

   συμβολικά

$$\forall\, x \in \mathbb{Z}\ \exists y \in \mathbb{Z}\ :\ y > x,$$

   αν εναλλάξουμε την θέση των δύο ποσοδεικτών $\forall$ και $\exists$ θα λάβουμε την Πρόταση

$$\exists\, x \in \mathbb{Z}\ :\ \forall y \in \mathbb{Z}\ y > x.$$

   Ας αποδώσουμε την Πρόταση αυτή με λέξεις.

   "Υπάρχει ακέραιος x, έτσι ώστε να είναι μικρότερος από κάθε ακέραιο y"

   Όπως βλέπουμε, έχει αλλάξει εντελώς το νόημα της αρχικής Πρότασης (συγκεκριμένα εδώ έχουμε μια ψευδή Πρόταση). Επομένως, η θέση των ποσοδεικτών σε μια Πρόταση είναι καίριας σημασίας.

4. Ας δούμε την εξής Πρόταση: "Υπάρχουν πραγματικοί αριθμοί, οι οποίοι ικανοποιούν την εξίσωση $x^2 - 3x + 2 = 0$". Συμβολικά η Πρόταση παρίσταται ως εξής:

$$\exists r \in \mathbb{R}\ :\ r^2 - 3r + 2 = 0.$$

   Μπορούμε να αποφανθούμε αν η Πρόταση είναι αληθής ή ψευδής με πολλούς τρόπους. Ένας τρόπος είναι να λύσουμε την εξίσωση (κατά τα γνωστά) και να αποφανθούμε. Υπάρχει όμως και το (γνωστό;) κριτήριο της διακρίνουσας και

[19] Στην πρόταση αυτή, όπως και στο εξής, η διπλή τελεία ":" θα συμβολίζει την έκφραση "έτσι ώστε".

να αποφανθούμε ότι πράγματι υπάρχουν πραγματικοί αριθμοί (χωρίς να τους προσδιορίσουμε), οι οποίοι ικανοποιούν την δοθείσα εξίσωση.

Με το παράδειγμα αυτό θέλουμε να επισημάνουμε ότι, γενικά, αν έχουμε μια Πρόταση, όπου εμφανίζεται ο ποσοδείκτης $\exists$, **δεν** είναι αναγκαίο να προσδιορίσουμε συγκεκριμένες τιμές της μεταβλητής για να αποφανθούμε αν η Πρόταση είναι αληθής ή ψευδής. Αρκεί να εξασφαλίσουμε την ύπαρξη τέτοιων τιμών.

Αργότερα θα επανέλθουμε διεξοδικότερα επ' αυτού.

Γενικά, αν έχουμε μια (ανοικτή) Πρόταση $\mathrm{p}(x)$, οι συμβολισμοί

$$\forall x \in S : \mathrm{p}(x) \text{ και } \exists x \in S : \mathrm{p}(x)$$

θα μπορούσαν να θεωρηθούν ως οι εξής *διαδικασίες*:

Για τον πρώτο. Πρέπει να αποφανθούμε αν η Πρόταση $\mathrm{p}(x)$ είναι αληθής για όλα τα $x \in S$. Αρκεί ένα $x \in S$, για το οποίο η Πρόταση να μην ισχύει, οπότε ο ισχυρισμός είναι ψευδής.

Για τον δεύτερο. Αρκεί ένα $x \in S$, για το οποίο η Πρόταση να ισχύει, οπότε ο ισχυρισμός είναι αληθής.

Προσοχή! Πρόκειται για διαφορετικές Προτάσεις. Άλλη είναι η (ανοικτή) Πρόταση "$\mathrm{p}(x), x \in S$" και άλλο οι (δηλωτικές) Προτάσεις "Για κάθε $x \in S : \mathrm{p}(x)$" και "Υπάρχει $x \in S : \mathrm{p}(x)$".

Όταν μιλούσαμε για την άρνηση μιας Πρότασης (σελ. 38) είχαμε δει το εξής παράδειγμα:

Η άρνηση της Πρότασης "Όλοι οι θετικοί ακέραιοι είναι άρτιοι" είναι η "Δεν είναι αληθές ότι όλοι οι θετικοί ακέραιοι είναι άρτιοι" και όχι η "Όλοι οι θετικοί ακέραιοι δεν είναι άρτιοι (δηλαδή είναι περιττοί)".

Ας αναλύσουμε περισσότερο την άρνηση

"Δεν είναι αληθές ότι όλοι οι θετικοί ακέραιοι είναι άρτιοι".

Το ότι δεν είναι αληθές ότι όλοι οι θετικοί ακέραιοι είναι άρτιοι, σημαίνει ότι υπάρχουν θετικοί ακέραιοι, οι οποίοι δεν είναι άρτιοι. Συνεπώς, για το καθολικό "για κάθε" επιτυγχάνουμε την άρνηση χρησιμοποιώντας το υπαρξιακό "υπάρχει".

Δυϊκά, ας δούμε το εξής παράδειγμα:

"Υπάρχει ακέραιος y, ο οποίος είναι μικρότερος του 3".

Η άρνηση της Πρότασης αυτής είναι η

"Κάθε ακέραιος αριθμός είναι μεγαλύτερος ή ίσος του 3".

Γενικά, υποθέτουμε ότι η Πρόταση:

"Για κάθε $x \in S$ ισχύει η $\mathrm{p}(x)$",

τότε η άρνησή της είναι:

"Δεν είναι αληθές ότι για κάθε $x \in S$ ισχύει η $\mathrm{p}(x)$",

η οποία ισοδύναμα σημαίνει

"Υπάρχει $x \in S$ έτσι ώστε να μην ισχύει η $\mathrm{p}(x)$".

Χρησιμοποιώντας πίνακες αληθείας είναι(;) εύκολο να δούμε ότι η Πρόταση

"¬(Για κάθε x, ώστε να ισχύει η $\mathrm{p}(x)$)"

είναι ισοδύναμη με την

"Υπάρχει x, έτσι ώστε η $\mathrm{p}(x)$ να μην ισχύει".

Όπως και η Πρόταση

"¬ (Υπάρχει x, ώστε να ισχύει η $\mathrm{p}(x)$)"

είναι ισοδύναμη με την

"Για κάθε x, έχουμε ότι δεν ισχύει η $\mathrm{p}(x)$."

Παράδειγμα 2.1.21. Έστω η Πρόταση

R: "Για κάθε πραγματικό αριθμό x υπάρχει πραγματικός αριθμός y, έτσι ώστε $y^3 = x$".

Ας δούμε την άρνηση της Πρότασης αυτής,

$\neg$ R: "Υπάρχει πραγματικός αριθμός x, έτσι ώστε για κάθε πραγματικό αριθμό y να ισχύει $y^3 \neq x$".

Όπως βλέπουμε στην άρνηση Εναλλάσσονται οι ποσοδείκτες "για κάθε" και "υπάρχει". Συμβολικά θα μπορούσαμε να εκφράσουμε την Πρόταση R ως εξής:

$$\mathrm{R}: \forall\, x \in \mathbb{R},\, \exists\, y \in \mathbb{R} \;:\; y^3 = x$$

και την άρνησή της ως εξής:

$$\neg\,\mathrm{R}: \exists\, x \in \mathbb{R} \;:\; \forall\, y \in \mathbb{R}, \neg\,(y^3 = x) \equiv \exists\, x \in \mathbb{R} \;:\; \forall\, y \in \mathbb{R}, y^3 \neq x.$$

Θα τελειώσουμε την αναφορά μας στους ποσοδείκτες συνοψίζοντας στα εξής:

Ο αριθμός των ποσοδεικτών που εμφανίζονται σε μια Πρόταση, τις περισσότερες φορές, φανερώνει την *"πολυπλοκότητα"* της Πρότασης και πρέπει να εστιαζόμαστε στην κατανόηση της Πρότασης πέραν των εμφανιζομένων συμβόλων.

Αν παρατηρήσουμε τους (φορμαλιστικούς/άκαμπτους) ορισμούς του ορίου, της σύγκλισης, της συνέχειας, της παραγώγισης..., οι οποίοι εμφανίζονται νωρίς στην μελέτη της Μαθηματικής Ανάλυσης, βλέπουμε ότι εμφανίζονται πολλοί ποσοδείκτες. Μια επιφανειακή μελέτη αυτών με τάσεις μάλλον απομνημόνευσης, παρά κατανόησης, "φοβίζει" και "αποτρέπει" αυτόν που έρχεται για πρώτη φορά σε επαφή με αυτές τις έννοιες.

Ας δούμε τον ορισμό του ορίου μιας ακολουθίας.

Έστω $a_1, a_2, \ldots, a_n, \ldots$ μια ακολουθία με πραγματικούς όρους. Αν

$$\exists\, l \in \mathbb{R} \;:\; \forall\, \varepsilon > 0\, \exists n(\varepsilon) \geq 1 \;:\; \forall\, n \geq n(\varepsilon),\, -\varepsilon < a_n - l < \varepsilon,$$

το l θα ονομάζεται όριο της ακολουθίας.

Ας προσπαθήσουμε να "αποκωδικοποιήσουμε" τα εμφανιζόμενα σύμβολα.

Αν υπάρχει πραγματικός αριθμός l, έτσι ώστε για κάθε θετικό πραγματικό αριθμό ε να υπάρχει φυσικός αριθμός $n(\varepsilon)$ με την ιδιότητα: Για κάθε $n \geq n(\varepsilon)$ να ισχύει $-\varepsilon < a_n - l < \varepsilon$, τότε το l θα ονομάζεται όριο της ακολουθίας.

Ο καθένας.... κρίνει και επιλέγει τρόπο έκφρασης.

Εν κατακλείδι, η χρήση (*εξωτικών/εντυπωσιακών*) συμβόλων, όπως τα

$$\forall,\ \exists,\ \wedge,\ \vee,\ \underline{\vee},\ \Longrightarrow \ldots,$$

είναι χρήσιμη στην "συμπυκνωμένη" έκφραση Μαθηματικών εννοιών (ειδικά στην συμβολική Λογική), αλλά ορισμένες φορές, η καταχρηστική, επιπόλαιη και...για λόγους εντυπωσιασμού χρήση τους οδηγεί σε....*επώδυνες καταστάσεις*.

Στο εξής θα αποφεύγουμε την αναγραφή τέτοιων συμβόλων και αντ' αυτών θα γράφουμε την σημασία τους

"για κάθε" ($\forall$), "υπάρχει" ($\exists$), "και" ($\wedge$), "ή" ($\vee$), "είτε,... ή" ($\underline{\vee}$),
"συνεπάγεται" ($\Longrightarrow$), ...

2.1.6 Ασκήσεις

Πρόβλημα: Υπάρχει μια ρήση του Abraham Lincoln. Η ελεύθερη απόδοσή της στα Ελληνικά είναι η εξής:

> "Υπάρχουν άνθρωποι, οι οποίοι πάντοτε εξαπατώνται. Υπάρχουν στιγμές, όπου όλοι εξαπατώνται. Αλλά δεν εξαπατώνται όλοι πάντοτε."

Θα μπορούσατε να την αποδώσετε με την *γλώσσα* της συμβολικής Λογικής;

1. Να αποδώσετε με σύμβολα τις ακόλουθες Προτάσεις:

   (α) Ο αριθμός x είναι θετικός, αλλά ο αριθμός y δεν είναι θετικός.

   (β) Για κάθε πρώτο αριθμό p υπάρχει κάποιος άλλος πρώτος αριθμός q, έτσι ώστε $q > p$.

   (γ) Υπάρχει πραγματικός αριθμός r με την ιδιότητα $r + x = x$ για κάθε πραγματικό αριθμό x.

   (δ) Για κάθε ακέραιο αριθμό x, ο x είναι είτε άρτιος ή περιττός.

   (ε) Για κάθε θετικό αριθμό ε, υπάρχει ένας θετικός αριθμός δ, ώστε $\eta \mid x-a \mid < \delta$ συνεπάγεται την $\mid f(x) - f(a) \mid < \varepsilon$.

   (στ) Αν a και b είναι πραγματικοί αριθμοί με $a \neq 0$, τότε η εξίσωση $ax + b = 0$ έχει λύση.

2. Να αποδώσετε με λέξεις τις ακόλουθες Προτάσεις:

   (α) $\forall\ x \in \mathbb{R}, \exists\, n \in \mathbb{N}\ :\ x^n > 0.$

   (β) $\exists\ a \in \mathbb{R}\ :\ \forall\ x \in \mathbb{R},\ ax = x.$

   (γ) $\forall\ x \in \mathbb{Z}, \exists\, n \in \mathbb{Z}\ :\ n = x + 5.$

   (δ) $\exists\ n \in \mathbb{Z}\ :\ \forall\ x \in \mathbb{Z},\ n = x + 5.$

   (ε) $\exists\ x \in \mathbb{R}\ :\ \forall\ y \in \mathbb{R},\ x + y = 2.$

3. Να γράψετε την άρνηση των ακόλουθων Προτάσεων:

   (α) Για κάθε πρώτο αριθμό p υπάρχει κάποιος άλλος πρώτος αριθμός q, έτσι ώστε $q > p$.

   (β) Υπάρχει πραγματικός αριθμός r με την ιδιότητα $r + x = x$ για κάθε πραγματικό αριθμό x.

   (γ) Για κάθε θετικό αριθμό ε, υπάρχει ένας θετικός αριθμός δ, ώστε $\eta \mid x-a \mid < \delta$ συνεπάγεται την $\mid f(x) - f(a) \mid < \varepsilon$.

   (δ) Έστω $x, y, z \in \mathbb{N}$. Για κάθε x υπάρχει y, έτσι ώστε $x = y + z$.

   (ε) $\forall\, x \in \mathbb{R}, \exists\, n \in \mathbb{N} \;:\; x^n > 0$.

   (στ) $\exists\, a \in \mathbb{R} \;:\; \forall\, x \in \mathbb{R},\, ax = x$.

   (ζ) Όλοι οι φοιτητές Μαθηματικών εργάζονται σκληρά.

   (η) Ορισμένοι από τους φοιτητές Μαθηματικών δεν εργάζονται σκληρά.

Βιβλιογραφία

[1] E.D. Bloch. *Proofs and Fundamentals: A first course in Abstract Mathematics*. Second Edition. Springer, 2011. ISBN: 978-14-4197-126-5.

[2] K. Houston. *How to Think Like a Mathematician*. Cambridge University Press, 2009. ISBN: 978-05-2189-546-0.

[3] Steven G. Krantz. *The Elements of Advanced Mathematics*. Fourth Edition. Textbooks in mathematics. CRC Press Taylor and Francis Group, 2018. ISBN: 978-11-3850-631-2.

[4] M. Liebeck. *A Concise Introduction to Pure Mathematics*. Third Edition. Chapman Hall CRC Press, 2011. ISBN: 978-14-3983-598-2.

[5] Bernd S. W. Schröder. *Fundamentals of Mathematics: An Introduction to Proofs, Logic, Sets and Numbers*. First Edition Wiley, 2010. ISBN: 978-04-7055-138-7.

[6] C. Schumacher. *Chapter Zero: Fundamental Notions of Abstract Mathematics*. Second Edition. Addison-Wesley, 2001. ISBN: 02-0143-724-4.

[7] A. Stefanowitz. *Proofs and Mathematical Reasoning*. University of Birmingham, 2014.

[8] I. Stewart & D. Tall. *The Foundations of Mathematics*. Second Edition. Oxford University Press, 2015.

[9] T. Sundstrom. *Mathematical Reasoning, Writing and Proof*. Version 2.1, May 26, 2020.

[10] P. Suppes. *Introduction to Logic*. Dover Publications, 1999. ISBN: 978-04-8640-687-9.

ΚΕΦΑΛΑΙΟ 3

ΜΑΘΗΜΑΤΙΚΕΣ ΑΠΟΔΕΙΞΕΙΣ ΚΑΙ ΕΠΙΧΕΙΡΗΜΑΤΟΛΟΓΙΑ

3.1 Η έννοια της Απόδειξης

Στο προηγούμενο κεφάλαιο είχαμε αναφερθεί σε Προτάσεις/Ισχυρισμούς, οι οποίες είναι αληθείς και σε Προτάσεις/Ισχυρισμούς, οι οποίες είναι ψευδείς. Εκεί είχαμε προβληματιστεί κατά πόσον είναι προφανές, αν ένας ισχυρισμός είναι αληθής ή όχι. Μάλιστα δε είχαμε θέσει το ερώτημα, όταν μιλούσαμε για λογικές συνεπαγωγές, κατά πόσον μπορούμε να "χρησιμοποιήσουμε" την αλήθεια μιας Πρότασης για να αποφανθούμε για την αλήθεια μιας άλλης Πρότασης.

Πέραν αυτού, με την μέχρι τώρα πείρα μας, έχουμε σχηματίσει μια εικόνα για το τι σημαίνει "επιχειρηματολογώ" για να τεκμηριώσω/αποδείξω έναν ισχυρισμό, τόσο στην καθημερινότητά μας, όσον και στα Μαθηματικά. Δεν ξεχνάμε ότι όλοι μας έχουμε αντιμετωπίσει *Θεωρήματα - Προτάσεις* και τις *αποδείξεις* τους.

Η εικόνα, την οποία έχουμε σχηματίσει, για το τι σημαίνει απόδειξη, αλλά και για την σημασία μιας απόδειξης, ενδέχεται να είναι ασαφής, ακόμη και στρεβλή.

Εδώ θα προσπαθήσουμε να διαλευκάνουμε ορισμένα σημεία.

3.1.1 Ορισμοί και Θεωρήματα

Διαβάζοντας, κατανοώντας και διατυπώνοντας ορισμούς.

Όπως (πρέπει να) έχουμε συνειδητοποιείσει, τόσο στον προφορικό όσο και στον γραπτό λόγο πρέπει να ακριβολογούμε και να είμαστε προσεκτικοί στην σημασία, την οποία έχει η κάθε λέξη που χρησιμοποιούμε. Ιδιαίτερα, στην μελέτη των Μαθηματικών αυτό είναι ζωτικής σημασίας.

Ο κύριος σκοπός ενός ορισμού είναι ο καθένας να γνωρίζει επακριβώς την σημασία,

την οποία αποδίδουμε σε κάποιες λέξεις, οι οποίες θα χρησιμοποιούνται κατά την επιχειρηματολογία μας.

Ας δούμε ένα ακραίο παράδειγμα.

Λέει κάποιος στον συνομιλητή του: "Δεν είναι *τίμιο* αυτό που κάνεις" και απαντά ο συνομιλητής: "Μπορείς να μου πεις τι σημαίνει *τίμιο*;". Χωρίς να επεκταθούμε, αμέσως βλέπουμε ότι το πρόβλημα έγκειται στη σημασία που αποδίδουμε στην λέξη *τίμιο*.

Στα Μαθηματικά, εκτός του ότι είναι ζωτικής σημασίας το νόημα που αποδίδουμε σε μια λέξη ή μια φράση, εξίσου σημαντική είναι η ακρίβεια με την οποία αποδίδουμε αυτό το νόημα. Ένας "κρυστάλλινα" διατυπωμένος ορισμός γίνεται εύκολα αποδεκτός από την Μαθηματική κοινότητα και σε αυτόν θα αναφερόμαστε στο εξής[1].

Για παράδειγμα έχουμε τον Ορισμό:

> "Ένας ακέραιος αριθμός n ονομάζεται **άρτιος** αν υπάρχει ένας ακέραιος αριθμός r, ώστε $n = 2r$".

Η έννοια του άρτιου αριθμού αποδίδεται με μια ιδιότητα που του προσδίδουμε.

Παρατηρήσεις 3.1.1.

1. Οι λέξεις, τις οποίες χρησιμοποιούμε σε έναν ορισμό για να αποδώσουμε μια έννοια, ενίοτε δεν μας "λένε κάτι". Μάλιστα δε στον καθημερινό λόγο, τις περισσότερες φορές, σημαίνουν κάτι άλλο. Ορισμένες φορές ίσως παραπέμπουν κάπου, αυτός, που διατύπωσε για πρώτη φορά έναν ορισμό, ίσως να είχε κάποιον λόγο, που χρησιμοποίησε την συγκεκριμένη λέξη. Αυτό δεν έχει κάποια ιδιαίτερη σημασία. Άπαξ και δώσαμε στην συγκεκριμένη λέξη (ή φράση) μια συγκεκριμένη σημασία την αποδεχόμαστε και προχωρούμε.

   Στο προηγούμενο παράδειγμα δεν μας ενδιαφέρει η ετυμολογία της λέξης "άρτιος". Αργότερα θα δούμε τον ορισμό της ομάδας. Άλλη η σημασία της λέξης "ομάδα" στην καθομιλουμένη και άλλη στα Μαθηματικά.

2. Ένας ορισμός, εκτός από του ότι αποδίδει την Μαθηματική σημασία μιας λέξης, ορισμένες φορές, μας επιτρέπει να διαχωρίζουμε συγκεκριμένα αντικείμενα από ομοειδή τους. Στο παράδειγμα των αρτίων ακεραίων, έχουμε τον διαχωρισμό των ακεραίων σε άρτιους και περιττούς, καθότι μπορούμε να δώσουμε τον εξής ορισμό:

   > "Ένας ακέραιος αριθμός ονομάζεται **περιττός** αν δεν είναι άρτιος".

3. Ένας ορισμός, άπαξ και έχει διατυπωθεί, πάντα έτσι αναφέρεται. Ορισμένες φορές ενδέχεται, με την ευελιξία, που μας παρέχει η γλώσσα μας, να αναδιατυπώσουμε έναν ορισμό χωρίς να αλλάξει η αρχική Μαθηματική έννοια.

   Στο παράδειγμα των αρτίων αριθμών, θα μπορούσαμε να αναδιατυπώσουμε τον προηγούμενο ορισμό ως εξής:

   "Ένας ακέραιος αριθμός ονομάζεται άρτιος, αν είναι πολλαπλάσιο του 2".

   Προσοχή! Στις *αναδιατυπώσεις*, ενδέχεται να αλλάζουν την αρχική σημασία.

4. Όπως προείπαμε, κάθε λέξη σε έναν ορισμό έχει την σημασία της.

   Ας δούμε τον εξής ορισμό:

[1] Όπως θα έχετε καταλάβει, γίνεται μια απόπειρα να δώσουμε....έναν ορισμό του "ορισμού".

> "Ένας θετικός ακέραιος αριθμός μεγαλύτερος του 1 θα ονομάζεται πρώτος, αν οι μόνοι θετικοί διαιρέτες του είναι το 1 και ο εαυτός του."

Ορισμένες φορές, όταν κάποιος επικαλείται τον ορισμό αυτόν, παραβλέπει τον περιορισμό "μεγαλύτερος του 1". Μάλιστα δε υπάρχουν και (ακραίες) περιπτώσεις, όπου κάποιοι, επικαλούμενοι ότι το 1 έχει την ιδιότητα "οι μόνοι θετικοί διαιρέτες είναι το 1 και ο εαυτός του", θεωρούν *λάθος* την εξαίρεση του 1 από την ιδιότητα του πρώτου αριθμού.

Εδώ πρέπει να προβληματιστούμε. Γιατί το 1 εξαιρείται από τους πρώτους;

Η απάντηση δεν είναι επί του παρόντος (αργότερα θα μας δοθεί η ευκαιρία να σχολιάσουμε ποιες "ανάγκες" μας υποχρεώνουν να εξαιρέσουμε το 1 από τους πρώτους). Εδώ εστιαζόμαστε στην ακρίβεια που εμπεριέχει ένας ορισμός και στην σωστή επίκληση/αναπαραγωγή ενός ορισμού.

5. Υπάρχει περίπτωση, για την ίδια Μαθηματική έννοια, να έχουμε δύο διαφορετικούς ορισμούς, οι οποίοι ενδέχεται να προκαλούν σύγχυση για το πώς ορίζουμε κάτι. Θα προσπαθήσουμε να γίνουμε σαφείς επικαλούμενοι ένα χαρακτηριστικό παράδειγμα.

   Όλοι, ίσως, έχετε συναντήσει το σύμβολο $n!$ (διαβάζεται n παραγοντικό), όπου n είναι ένας θετικός ακέραιος μεγαλύτερος ή ίσος του 1.

   > Ορισμός 1. Έστω n ακέραιος αριθμός μεγαλύτερος ή ίσος του ένα. Ορίζουμε ως $n!$ να ισούται με το γινόμενο $1 \cdot 2 \cdot \cdots \cdot (n-1) \cdot n$. Δηλαδή
   >
   > $$n! = 1 \cdot 2 \cdot \cdots \cdot (n-1) \cdot n.$$

   Ο ορισμός αυτός αποτελεί έναν "συμβολικό" ορισμό υπό την έννοια ότι απλά ορίζει με ποιο τρόπο θα συμβολίζουμε ένα δεδομένο γινόμενο ακεραίων αριθμών. Παρ' όλα ταύτα, είναι ένας "χρήσιμος" ορισμός, ο οποίος μας διευκολύνει αφάνταστα σε πολλούς και πολύπλοκους υπολογισμούς.

   Στην πορεία όμως εμφανίζεται η ανάγκη του ορισμού του 0! (το μηδέν παραγοντικό). Εδώ "επεκτείνουμε" τον προηγούμενο ορισμό ως εξής:

   > "Έστω n ακέραιος αριθμός μεγαλύτερος ή ίσος του μηδενός. Ορίζουμε ως $n!$ να ισούται με το γινόμενο $1 \cdot 2 \cdot \cdots \cdot (n-1) \cdot n$ στην περίπτωση, όπου $n \geq 1$ και ορίζουμε $0! = 1$".

   Ας δούμε τώρα τον προηγούμενο ορισμό υπό διαφορετική γωνία.

   Έστω A ένα σύνολο με $n \geq 0$ το πλήθος στοιχεία (το σύνολο με 0 το πλήθος στοιχεία είναι το κενό σύνολο).

   > Ορισμός 2. Ορίζουμε ως $n!$ να παριστά το πλήθος των διαφορετικών τρόπων, με τους οποίους μπορούν να τοποθετηθούν τα στοιχεία του συνόλου σε μια σειρά.

   Εδώ έχουμε έναν ορισμό, που αφορά ένα πλήθος (τους διαφορετικούς τρόπους, με τους οποίους μπορούν να τοποθετηθούν τα στοιχεία του συνόλου σε μία σειρά). Όπως θα δούμε αργότερα (θα το αποδείξουμε), υπάρχουν $1 \cdot 2 \cdot \cdots \cdot$

$(n-1)\cdot n$ το πλήθος τρόποι στην περίπτωση, όπου $n \geq 1$ και μόνο ένας τρόπος στην περίπτωση, όπου έχουμε το κενό σύνολο (απλά έχουμε μια κενή παρουσίαση). Αλλά αυτό το πλήθος το έχουμε ορίσει ως $n!$. Συνεπώς, οι δύο ορισμοί "συμπίπτουν" (μόνο) ως προς τον ποιο αριθμό παριστά το σύμβολο $n!$.

Ισοδύναμοι ορισμοί - Χαρακτηρισμοί.

Ας επανέλθουμε στον ορισμό των αρτίων αριθμών.

> "Ένας ακέραιος αριθμός n ονομάζεται **άρτιος** αν υπάρχει ένας ακέραιος αριθμός r, ώστε $n = 2r$".

Η έννοια του αρτίου αριθμού αποδίδεται με μια ιδιότητα, που του προσδίδουμε. Παράλληλα είναι διατυπωμένος με τρόπο ώστε να μην αφήνει καμία αμφιβολία ότι ενδέχεται να υπάρχουν και "άλλοι" άρτιοι αριθμοί. Δηλαδή οι άρτιοι αριθμοί είναι **μόνο** αυτοί, οι οποίοι πληρούν την ιδιότητα:

> "υπάρχει ένας ακέραιος αριθμός r, ώστε $n = 2r$".

Για τον λόγο αυτόν, πολλές φορές, όταν δίνεται ένας ορισμός, χρησιμοποιείται η έκφραση "αν και μόνο αν" θέλοντας με αυτόν τον τρόπο να τονισθεί η μοναδικότητα, που προσδίδουμε στην ιδιότητα, που πληροί η υπό χαρακτηρισμό λέξη. Στο προηγούμενο παράδειγμα θα μπορούσαμε να γράψουμε:

> "Ένας ακέραιος αριθμός n ονομάζεται **άρτιος**, αν και μόνο αν υπάρχει ένας ακέραιος αριθμός r, ώστε $n = 2r$".

Η επιπλέον έκφραση "μόνο αν" στην πραγματικότητα δεν προσφέρει κάτι ουσιαστικό στην ακρίβεια του ορισμού, απλώς (υπερ)τονίζει την συγκεκριμένη ιδιότητα.

Εδώ πρέπει να είμαστε πολύ προσεκτικοί, διότι ενδέχεται να επέλθει σύγχυση[2] με την (λογική) ισοδυναμία Προτάσεων, την οποία είχαμε παρουσιάσει στο προηγούμενο κεφάλαιο. Εκεί η έκφραση "αν και μόνο αν" έχει εντελώς διαφορετική σημασία. Για τον λόγο αυτόν, στο εξής, όταν δίνουμε έναν ορισμό θα χρησιμοποιούμε (μόνο) την λέξη "αν" κρατώντας την έκφραση "αν και μόνο αν" για τους "χαρακτηρισμούς".

Ας ξεκινήσουμε με μερικά παραδείγματα.

i. Όλοι γνωρίζουμε τον τρόπο, με τον οποίο αποφαινόμαστε, αν ένας ακέραιος αριθμός είναι άρτιος ή όχι.

> "Αν το τελευταίο ψηφίο ενός ακεραίου αριθμού (στην δεκαδική του παράσταση) είναι ένα από τα 0, 2, 4, 6, 8, τότε είναι άρτιος".

Εδώ **δεν** έχουμε ορισμό. Ο ορισμός του αρτίου αριθμού έχει δοθεί προηγουμένως. Εδώ πρόκειται για μια συνεπαγωγή ("αν..., τότε"), την αλήθεια της οποίας μπορούμε (εύκολα) να διαπιστώσουμε.

Επίσης, μπορούμε να διατυπώσουμε την αντίστροφη συνεπαγωγή

> "Αν ένας ακέραιος αριθμός είναι άρτιος, τότε (στην δεκαδική του παράσταση) το τελευταίο ψηφίο του είναι ένα από τα 0, 2, 4, 6, 8",

[2] Δυστυχώς η σύγχυση αυτή δεν υπάρχει μόνο σ' αυτούς, οι οποίοι βρίσκονται στην αρχή της σπουδής των Μαθηματικών.... Μάλιστα δε, όταν χρησιμοποιείται (κακοποιημένο) το σύμβολο $\Longleftrightarrow$, η σύγχυση επιτείνεται. Για δείτε τον "*ορισμό*" "Ένας ακέραιος αριθμός n είναι άρτιος $\Longleftrightarrow$ υπάρχει ένας ακέραιος αριθμός r, ώστε $n = 2r$".

την αλήθεια της οποίας πάλι (εύκολα) μπορούμε να διαπιστώσουμε. Επομένως, έχουμε την ισοδυναμία Προτάσεων.

> "Ένας ακέραιος αριθμός είναι άρτιος, αν και μόνο αν (στην δεκαδική του παράσταση) το τελευταίο ψηφίο του είναι ένα από τα 0, 2, 4, 6, 8."

ii. Ας δούμε τον εξής ορισμό:

> "Ένας ακέραιος αριθμός n ονομάζεται πολλαπλάσιο του 3 αν υπάρχει ένας ακέραιος αριθμός r, ώστε $n = 3r$".

Ίσως να γνωρίζετε (αν δεν το γνωρίζετε δεν πειράζει) ότι, αν μας δώσουν ένα πολλαπλάσιο του 3 (στην δεκαδική του παράσταση) και πάρουμε το άθροισμα των ψηφίων του, τότε και αυτός ο αριθμός είναι πολλαπλάσιο του 3, π.χ. $56784 = 3 \cdot 18928$ και $5 + 6 + 7 + 8 + 4 = 30 = 3 \cdot 10$. Δηλαδή μπορούμε να διατυπώσουμε την εξής συνεπαγωγή:

> "Αν ένας ακέραιος αριθμός είναι πολλαπλάσιο του 3, τότε το άθροισμα των ψηφίων του είναι πολλαπλάσιο του 3".

Η συνεπαγωγή αυτή είναι αληθής. Το γιατί, είναι εύκολο να διαπιστωθεί και θα το δούμε αργότερα. (Σίγουρα δεν αρκεί το προηγούμενο παράδειγμα και όσα άλλα παραδείγματα και να κάνουμε, για να διαπιστώσουμε την αλήθεια της Πρότασης αυτής. Επ' αυτού μπορείτε να δείτε μια απόδειξη στην Άσκηση Γ.3.4$_5$).

Ας διατυπώσουμε την αντίστροφη συνεπαγωγή.

> "Αν το άθροισμα των ψηφίων ενός ακεραίου αριθμού (στην δεκαδική παράστασή του) είναι πολλαπλάσιο του 3, τότε ο αριθμός είναι πολλαπλάσιο του 3."

Για παράδειγμα, αν έχουμε τον αριθμό 56784, τότε

$$5 + 6 + 7 + 8 + 4 = 30 = 3 \cdot 10$$

και σύμφωνα με τον ισχυρισμό ο αριθμός 56784 είναι πολλαπλάσιο του 3. Η συνεπαγωγή αυτή είναι επίσης αληθής, θα το δούμε αργότερα (δεν αρκεί το παράδειγμα).

Επομένως, έχουμε την ισοδυναμία Προτάσεων.

> "Ένας ακέραιος αριθμός είναι πολλαπλάσιο του 3, αν και μόνο αν το άθροισμα των ψηφίων του (στην δεκαδική του παράσταση) είναι πολλαπλάσιο του 3".

Αρκούν αυτά τα παραδείγματα για να διαπιστώσουμε ότι υπάρχει μια ειδική και πολύ ενδιαφέρουσα κατηγορία (αληθών) ισοδυναμιών, όπου το ένα μέρος αποτελείται από έναν ορισμό και το άλλο από μια άλλη Πρόταση. Αυτού του είδους οι ισοδυναμίες θα ονομάζονται **χαρακτηρισμοί**. Παντού στα Μαθηματικά συναντούμε χαρακτηρισμούς.

Παρατηρήσεις 3.1.2.

1. Σε έναν ορισμό, όπου αποδίδουμε μια σημασία σε μια λέξη (ή φράση), μέσω μιας ιδιότητας χρησιμοποιούμε την λέξη "ονομάζεται" (ή ισοδύναμα τις λέξεις "λέγεται", "καλείται"). Ενώ, σε έναν χαρακτηρισμό την λέξη "είναι".

   Προσοχή! είναι σημαντική αυτή η επισήμανση και η διάκριση μεταξύ του "περιεχομένου" των δύο λέξεων "ονομάζεται" και "είναι".

2. Σε έναν χαρακτηρισμό, όπου έχουμε την ισοδυναμία ενός ορισμού με μια Πρόταση, θα μπορούσε κάποιος να εναλλάξει τον "ρόλο" του ορισμού με την ισοδύναμη Πρόταση.

   Για παράδειγμα: Ας συμφωνήσουμε να δώσουμε τον εξής ορισμό για τους άρτιους ακεραίους.

   > "Ένας ακέραιος αριθμός ονομάζεται άρτιος αν (στην δεκαδική του παράσταση) το τελευταίο ψηφίο του είναι ένα από τα 0, 2, 4, 6, 8".

   Άπαξ και δεχθούμε αυτόν τον ορισμό για τους άρτιους αριθμούς, τότε ο ανωτέρω χαρακτηρισμός διαφοροποιείται.

   > "Ένας ακέραιος αριθμός είναι άρτιος αν και μόνο αν είναι πολλαπλάσιο του 2".

   Εδώ φαίνεται η εναλλαγή του ρόλου των λέξεων "ονομάζεται" και "είναι". Επομένως, ορισμένες φορές, αντί για χαρακτηρισμούς, μιλάμε για **ισοδύναμους ορισμούς**. Συνεπώς, στο εξής θα επιλέγουμε (και θα αποδεχόμαστε) έναν ορισμό και οι διάφοροι χαρακτηρισμοί θα μπορούν να θεωρηθούν ότι αποτελούν ισοδύναμους ορισμούς.

   Παράδειγμα. Στην Παρατήρηση 3.1.1 $_2$ (σκόπιμα) είχαμε δώσει τον ορισμό ενός περιττού ακεραίου υπό αρνητική διατύπωση.

   > "Ένας ακέραιος αριθμός ονομάζεται **περιττός**, αν δεν είναι άρτιος".

   Ένας άλλος (μάλλον πιο οικείος) ορισμός είναι

   > "Ένας ακέραιος αριθμός n ονομάζεται **περιττός**, αν υπάρχει a ακέραιος, ώστε $n = 2a + 1$".

   Πρόκειται για ισοδύναμους ορισμούς. Μπορείτε να το διαπιστώσετε εξετάζοντας την αλήθεια της ισοδυναμίας.

   > "Ένας ακέραιος αριθμός δεν είναι άρτιος αν και μόνο αν είναι της μορφής $2a + 1$, όπου a είναι ένας ακέραιος αριθμός".

3. Ας δούμε τώρα την εξής συνεπαγωγή:

   > "Αν ο ακέραιος αριθμός n είναι πολλαπλάσιο του 4 (δηλαδή $n = 4r$ με r ακέραιο), τότε είναι άρτιος".

   Προφανώς η συνεπαγωγή αυτή είναι αληθής, όπως (πάλι προφανώς) η αντίστροφή της είναι ψευδής. Εδώ δεν πρόκειται για χαρακτηρισμό, αλλά απλώς για μια ικανή συνθήκη, όπου το δεύτερο μέρος ("τότε.....") είναι ένας ορισμός. Στην περίπτωση αυτή θα λέμε ότι έχουμε ένα **κριτήριο**.

   Ας δούμε ένα ακόμη κριτήριο.

> "Αν η απόσταση των κέντρων δύο κύκλων ισούται με το άθροισμα των ακτίνων τους, τότε οι κύκλοι εφάπτονται".

Μπορείτε να δείτε ότι πρόκειται για κριτήριο και **όχι** για χαρακτηρισμό.

(Προσπαθήστε το, δίνοντας πρώτα έναν ορισμό των εφαπτομένων κύκλων).

Θα κλείσουμε την παράγραφο με ορισμένες επισημάνσεις.

Ένας ορισμός, πέραν της ακρίβειας που πρέπει να τον διακρίνει, πρέπει να έχει "περιεχόμενο", δηλαδή να υπάρχουν "αντικείμενα", τα οποία τον ικανοποιούν ή να διακρίνει "αντικείμενα" μεταξύ άλλων "αντικειμένων". Για παράδειγμα:

> "Πλατωνικό στερεό ονομάζεται ένα κυρτό κανονικό πολύεδρο, του οποίου όλες οι έδρες είναι ίσα κανονικά πολύγωνα και όλες οι πολυεδρικές γωνίες του είναι ίσες."

Εδώ το ερώτημα είναι διπλό. Υπάρχουν Πλατωνικά στερεά και αν ναι, ποία και πόσα; Το ερώτημα έχει απαντηθεί, οπότε έχουμε έναν "καλό ορισμό".

Ας δούμε όμως και τους εξής "*ορισμούς*":

> "Ένας ακέραιος αριθμός a θα ονομάζεται σταθερός αν $a = a + 1$".

Όπως βλέπουμε, αυτός ο ορισμός είναι *κενός περιεχομένου*. Δεν υπάρχουν ακέραιοι αριθμοί που να ικανοποιούν τις απαιτήσεις του ορισμού.

> "Ένας ακέραιος αριθμός a θα ονομάζεται καθολικός αν $a = 1 \cdot a$".

Όπως βλέπουμε, αυτός ο ορισμός δεν "προσφέρει κάτι". Όλοι οι ακέραιοι ικανοποιούν αυτόν τον ορισμό.

Ένας ορισμός πρέπει να μην έρχεται σε αντίφαση με προηγούμενους ορισμούς και γνωστά αποτελέσματα. Για παράδειγμα, ας δούμε τον εξής "*ορισμό*":

> "Ένας ακέραιος αριθμός a θα ονομάζεται μηδέν αν $a = -a$".

Εδώ υπάρχει αντίφαση. Χωρίς να έχουμε έναν αυστηρό ορισμό του μηδενός (μας αρκεί αυτό που διαισθανόμαστε), η έννοια του αντιθέτου $-a$ έπεται της έννοιας του μηδενός (ουδετέρου στοιχείου ως προς την πρόσθεση). Επομένως, δεν μπορεί να χρησιμοποιηθεί για τον ορισμό του μηδενός.

Προτάσεις - Θεωρήματα.

Στο προηγούμενο κεφάλαιο είχαμε ασχοληθεί με μια κατηγορία προτάσεων, τις συνεπαγωγές. Όπου, από δύο Προτάσεις Α και Β, συνθέταμε μια νέα Πρόταση (συνεπαγωγή) "Αν Α, τότε Β" (ή "Η Α συνεπάγεται την Β" και συμβολικά "$\mathrm{A} \Longrightarrow \mathrm{B}$"). Μάλιστα δε, είχαμε ονομάσει την Πρόταση Α υπόθεση και την Πρόταση Β συμπέρασμα. Επίσης, είχαμε κατασκευάσει τον πίνακα αληθείας της, τον

Α	Β	$\mathrm{A} \Longrightarrow \mathrm{B}$
Α	Α	Α
Α	Ψ	Ψ
Ψ	Α	Α
Ψ	Ψ	Α

Όπως βλέπουμε, η αλήθεια της συνεπαγωγής "$A \Longrightarrow B$" εξαρτάται από το αληθές ή ψευδές των Προτάσεων Α και Β. Μια αληθής συνεπαγωγή "$A \Longrightarrow B$" στο εξής θα ονομάζεται **Θεώρημα**.

Πριν προχωρήσουμε, ορισμένα αναγκαία σχόλια.

Σχόλια 3.1.3.

i. Η λέξη "Θεώρημα" δεν είναι η μόνη λέξη, με την οποία αναφερόμαστε σε μια αληθή συνεπαγωγή. Άλλες λέξεις που χρησιμοποιούνται είναι οι λέξεις: **Λήμμα**, **Πόρισμα** ή απλώς **Πρόταση**. Δεν υπάρχει ένας "κανόνας", ο οποίος να υπαγορεύει πότε αναφέρονται ως Θεωρήματα και πότε διαφορετικά. Συνήθως μια αληθής συνεπαγωγή αναφέρεται ως Θεώρημα, αν πρόκειται για ένα σημαντικό Μαθηματικό αποτέλεσμα, το οποίο διέπει μια μεγάλη περιοχή των Μαθηματικών και η "συμβολή" του είναι ουσιώδης στην εξέλιξή τους.

   Μια αληθής συνεπαγωγή αναφέρεται ως Πρόταση, αν κρίνεται ότι η συμβολή της δεν είναι τόσο σημαντική όσον ενός Θεωρήματος.

   Ως Λήμμα συνήθως αναφέρεται μια αληθής συνεπαγωγή η οποία δρα "βοηθητικά" στην απόδειξη ενός Θεωρήματος ή Πρότασης.

   Τέλος, ως Πόρισμα αναφέρεται μια αληθής συνεπαγωγή, η οποία απορρέει άμεσα από ένα Θεώρημα ή Πρόταση και είναι "χρήσιμο" για περαιτέρω εφαρμογές.

   Ο ανωτέρω διαχωρισμός δεν είναι καθοριστικός, ούτε υποχρεωτικός. Εμπεριέχει και τον υποκειμενισμό των επιστημόνων Μαθηματικών. Το ίδιο Μαθηματικό αποτέλεσμα αλλού μπορεί να το συναντήσουμε ως Θεώρημα και αλλού ως Πρόταση. Επίσης, υπάρχουν Λήμματα, τα οποία έχουν καταστεί "διάσημα", καθότι στην πορεία απεδείχθησαν πιο σημαντικά, ενώ στην αρχή είχαν χρησιμοποιηθεί ως βοηθητικά.

ii. Δεδομένου ότι ένα Θεώρημα είναι μια αληθής συνεπαγωγή η διατύπωσή του είναι συνήθως της μορφής "Αν ισχύουν τα εξής....., τότε έπεται ότι ισχύει.....".

   Αυτό δεν είναι αναγκαίο. Η ευελιξία της γλώσσας μας επιτρέπει και άλλες ισοδύναμες εκφράσεις.

   Για παράδειγμα: "Οι γωνίες ενός ισοπλεύρου τριγώνου είναι ίσες."

   Πάντα όμως μπορεί να μετασχηματιστεί στην μορφή, που προαναφέραμε.

   Για το παράδειγμά μας έχουμε:

   "Αν έχουμε ένα ισόπλευρο τρίγωνο, τότε έπεται ότι οι γωνίες του είναι ίσες."

   Η διατύπωση ενός Θεωρήματος στην μορφή αυτή είναι πολύ σημαντική (ειδικά για έναν αρχάριο στην σπουδή των Μαθηματικών), όπου γίνεται σαφές ποια είναι η υπόθεση και ποιο το συμπέρασμα.

   Παρ' όλα ταύτα, υπάρχουν περιπτώσεις, όπου "δεν είναι ανάγκη" να προσπαθούμε να "προσαρμόσουμε" ένα Θεώρημα στην ανωτέρω μορφή. Για παράδειγμα:

   "Υπάρχουν άπειροι το πλήθος πρώτοι αριθμοί."

iii. Όπως προείπαμε, ένα Θεώρημα είναι μια αληθής συνεπαγωγή. Όταν έχουμε απλώς μια συνεπαγωγή, την αλήθεια της οποίας δεν γνωρίζουμε, τότε για να

καταστεί Θεώρημα πρέπει να διαπιστωθεί/εξασφαλιστεί η αλήθειά της, διαφορετικά παραμένει ένας ισχυρισμός. Αν υπάρχει η πίστη ότι μια συνεπαγωγή είναι αληθής, αλλά δεν μπορούμε να αποφανθούμε ότι είναι αληθής ή ψευδής, τότε η συνεπαγωγή αυτή αποτελεί μια **εικασία**.

Πάντα μπορούμε να κάνουμε εικασίες (στα Μαθηματικά και στη ζωή γενικότερα), αλλά οι "*καλές*" εικασίες σπανίζουν. Οι καλές εικασίες αποτελούν την "κινητήρια δύναμη" στα Μαθηματικά. Έχουμε ήδη αναφέρει την εικασία του Goldbach:

> "Κάθε άρτιος ακέραιος μεγαλύτερος του τρία είναι άθροισμα δύο πρώτων αριθμών."

Επίσης, έχουμε αναφέρει το τελευταίο Θεώρημα του Fermat:

> "Δεν υπάρχουν θετικοί ακέραιοι a, b, c, n, οι οποίοι να ικανοποιούν την ισότητα $a^n + b^n = c^n$ για $n > 2$."

Εδώ αξίζει να σημειώσουμε ότι, παρόλο που το Θεώρημα αυτό για περίπου 350 χρόνια παρέμενε μια εικασία, στην Μαθηματική Κοινότητα αναφερόταν ως Θεώρημα. Στην προσπάθεια να αποδειχθεί το Θεώρημα αυτό, απεδείχθη μια άλλη πολύ γενικότερη εικασία. Η εικασία των Taniyama–Shimura[3]. Συνεπώς, το τελευταίο Θεώρημα του Fermat, τελικά είναι Πόρισμα.

iv. Πέραν των Θεωρημάτων στα Μαθηματικά, υπάρχει η ανάγκη ύπαρξης "σημείων εκκίνησης". Συγκεκριμένα στην προσπάθειά τους οι Μαθηματικοί να θεμελιώσουν τα Μαθηματικά σε "στέρεα βάση" αναγκάστηκαν να θεωρήσουν (αυθαιρέτως) ως αληθείς Προτάσεις, επί των οποίων στηρίχτηκαν για να ξεκινήσουν την διατύπωση και απόδειξη Θεωρημάτων. Οι Προτάσεις αυτές ονομάζονται **Αξιώματα**[4].

Χαρακτηριστικά αναφέρουμε ότι η Ευκλείδεια Γεωμετρία στηρίζεται σε πέντε αξιώματα, τα οποία (απεδείχθη ότι) είναι ικανά να αποδείξουμε τα *πάντα* στην Ευκλείδεια Γεωμετρία.

Η ανάγκη να αντιμετωπίσουμε τις παραδοξότητες, που παρουσιάζονται στην μελέτη των συνόλων, οδήγησε στην "Αξιωματική θεμελίωση των συνόλων".

Επίσης, ορισμένοι ορισμοί είναι "αξιωματικοί", υπό την έννοια ότι ορίζουμε κάτι απαιτώντας να πληρούνται κάποιες ιδιότητες.

Στην πορεία θα αναφερθούμε περισσότερο στην διάκριση μεταξύ αξιωμάτων και Θεωρημάτων.

Ας επαναλάβουμε τώρα τα Παραδείγματα, που είχαμε δει στην περίπτωση, όπου μια συνεπαγωγή είναι αληθής.

i. Θεωρούμε τις προτάσεις:

A : "Ο 18 είναι πολλαπλάσιο του 6".

B : "Ο 18 είναι πολλαπλάσιο του 2".

[3] Δεν είναι δυνατόν, σε αυτό το επίπεδο, να διατυπωθεί η εικασία αυτή, καθώς και άλλες "διάσημες" εικασίες, οι οποίες τροφοδοτούν την Μαθηματική έρευνα.

[4] Εδώ μπορούμε να κάνουμε τον "παραλληλισμό". Τα αξιώματα είναι ό,τι τα Δόγματα στην (οποιαδήποτε) θρησκεία. "Αλήθειες, οι οποίες δεν χρήζουν αποδείξεως".

Η υπόθεσή μας είναι η Πρόταση Α, η οποία είναι αληθής ($18 = 6 \cdot 3$).

Το συμπέρασμά μας είναι η Πρόταση Β. Η αλήθεια της Πρότασης αυτής *απορρέει* από την Πρόταση Α ως εξής:

$$18 = 6 \cdot 3 = (2 \cdot 3) \cdot 3 = 2 \cdot (3 \cdot 3) = 2 \cdot 9.$$

Δηλαδή, αποδεχόμενοι την αλήθεια της Πρότασης Α, μέσω μιας διαδικασίας επίκλησης επιχειρημάτων, διαπιστώσαμε (αποδείξαμε) την αλήθεια της Πρότασης Β. Συνεπώς, αποφανθήκαμε ότι η συνεπαγωγή

"Ο 18 είναι πολλαπλάσιο του 6" $\Longrightarrow$ "Ο 18 είναι πολλαπλάσιο του 2"

είναι αληθής!

Η περίπτωση αυτή αναπαριστάται στην πρώτη γραμμή του πίνακα αληθείας.

ii. Αν $-1 = 1$, τότε $1 = 1$.

Εδώ έχουμε τις Προτάσεις

Α: "$-1 = 1$".

Β: "$1 = 1$".

Και την συνεπαγωγή "Α $\Longrightarrow$ Β".

Η συνεπαγωγή είναι αληθής. Πράγματι, εδώ η Πρόταση Α: "$-1 = 1$" είναι ψευδής, αλλά, θα έλεγε κάποιος, αφού αυτήν δεχόμαστε, υψώνουμε και τα δύο μέλη στο τετράγωνο (θεωρώντας ότι για οποιουσδήποτε πραγματικούς αριθμούς x και y η συνεπαγωγή $x = y \Longrightarrow x^2 = y^2$ είναι πάντα αληθής) και καταλήγουμε στην αληθή Πρόταση Β: "$1 = 1$".

Η περίπτωση αυτή αναπαριστάται στην τρίτη γραμμή του πίνακα αληθείας.

iii. Αν $1 = 2$, τότε $5 = 6$.

Εδώ έχουμε τις Προτάσεις

Α: "$1 = 2$".

Β: "$5 = 6$".

Και την συνεπαγωγή "Α $\Longrightarrow$ Β".

Η συνεπαγωγή είναι αληθής. Πράγματι, εδώ η Πρόταση Α: "$1 = 2$" είναι ψευδής, αλλά, θα έλεγε κάποιος, αφού αυτήν δεχόμαστε, προσθέτουμε και στα δύο μέλη το 4 (θεωρώντας ότι για οποιουσδήποτε πραγματικούς αριθμούς x και y και r η συνεπαγωγή $x = y \Longrightarrow x + r = y + r$ είναι πάντα αληθής) και καταλήγουμε στην ψευδή Πρόταση Β: "$5 = 6$".

Η περίπτωση αυτή αναπαριστάται στην τέταρτη γραμμή του πίνακα αληθείας.

Στα δύο τελευταία παραδείγματα, όπου η Πρόταση Α είναι ψευδής, η συνεπαγωγή "Α $\Longrightarrow$ Β" είναι πάντα αληθής και στο εξής η περίπτωση, όπου η Πρόταση Α είναι ψευδής, δεν θα μας απασχολεί.

Στην περίπτωση, όπου η Πρόταση Α είναι αληθής και η Πρόταση Β είναι ψευδής, η συνεπαγωγή "Α $\Longrightarrow$ Β" είναι πάντα ψευδής (η δεύτερη γραμμή του πίνακα αληθείας), οπότε πάλι δεν θα ασχοληθούμε με την περίπτωση αυτή.

Επομένως, ενδιαφέρον έχει η πρώτη περίπτωση, όπου έχουμε και τις δύο Προτάσεις Α και Β αληθείς. Δεν ξεχνάμε την πρωταρχική και απαράβατη παραδοχή:

> * Η Πρόταση "Αν η Α είναι αληθής, τότε (αναγκαστικά) η Β είναι αληθής" είναι αληθής *.

Άρα από τα Θεωρήματα (αληθείς συνεπαγωγές) θα μας ενδιαφέρουν και θα επικεντρωθούμε **μόνο** σε αυτά, τα οποία είναι της μορφής: "$\mathrm{A} \Longrightarrow \mathrm{B}$", όπου οι Προτάσεις Α και Β είναι αληθείς.

Διαβάζοντας, αναλύοντας και κατανοώντας Θεωρήματα.

Τα Θεωρήματα και οι αποδείξεις αποτελούν το κεντρικό σημείο στην σπουδή των Μαθηματικών. Μια μεγάλη μερίδα[5] αυτών που ασχολούνται με τα Μαθηματικά, εκλαμβάνει τα Μαθηματικά ως μια διαδικασία "χρήσιμη" στην επίλυση προβλημάτων. Για παράδειγμα: Πώς λύνουμε μια δευτεροβάθμια εξίσωση, πώς παραγωγίζουμε το γινόμενο συναρτήσεων.... Τα Θεωρήματα, και γενικότερα τα Μαθηματικά, είναι...πέραν από του να μας "εξοπλίζουν" με διαδικασίες και αλγορίθμους.

Ας δούμε ένα Παράδειγμα. Δεν υπάρχει (μέχρι τούδε) Θεώρημα, το οποίο να μας εξασφαλίζει, πώς μπορούμε να αποφανθούμε, αν ένας φυσικός αριθμός είναι πρώτος. Υπάρχει όμως το Θεώρημα:

> "Κάθε φυσικός αριθμός μεγαλύτερος του 1 αναλύεται κατά μοναδικό τρόπο σε γινόμενο πρώτων αριθμών."[6]

Δεν υπάρχει όμως Θεώρημα, το οποίο να μας εξασφαλίζει ποια είναι αυτή η ανάλυση[7]. Παρ' όλα ταύτα το Θεώρημα αυτό είναι θεμελιώδες.

Επομένως, όταν έχουμε ένα Θεώρημα δεν πρέπει να ενδιαφερόμαστε μόνο στο τι μπορούμε να κάνουμε, σε πρακτικό επίπεδο, με αυτό το Θεώρημα, αλλά το τι πράγματι σημαίνει αυτό το Θεώρημα.

Το πρώτο πράγμα, που έχουμε να κάνουμε, όταν έχουμε ένα Θεώρημα, είναι να το αναλύσουμε λέξη προς λέξη. Σε ένα καλά διατυπωμένο Θεώρημα η κάθε λέξη έχει την σημασία της. Στο προηγούμενο παράδειγμα

> "Κάθε φυσικός αριθμός μεγαλύτερος του 1 αναλύεται κατά μοναδικό τρόπο σε γινόμενο πρώτων αριθμών."

(σκόπιμα) υπάρχει μια ασάφεια. Τι σημαίνει "...κατά μοναδικό τρόπο..."; Υπάρχουν μοναδικοί πρώτοι αριθμοί των οποίων το γινόμενο μας δίνει αυτόν τον αριθμό; Η σειρά των παραγόντων έχει κάποια σημασία στην μοναδικότητα της γραφής; Όλα αυτά πρέπει να διαλευκανθούν.

Θα αναφέρουμε ένα άλλο παράδειγμα, το γνωστό(;) Θεώρημα Μέσης Τιμής του Διαφορικού Λογισμού.

> "Έστω f μια πραγματική συνάρτηση. Αν η f είναι συνεχής στο κλειστό διάστημα $[a, b]$ και παραγωγίσιμη στο ανοικτό διάστημα (a, b), τότε υπάρχει $c \in (a, b)$ έτσι ώστε $f'(c) = \frac{f(b)-f(a)}{b-a}$".

Το Θεώρημα αυτό μας εξασφαλίζει την ύπαρξη ενός στοιχείου με μια συγκεκριμένη ιδιότητα, δεν μας λέει όμως τίποτε για το πώς βρίσκουμε αυτό το σημείο. Παρ' όλα ταύτα, είναι ένα θεμελιώδες Θεώρημα.

---

[5] Δυστυχώς στην μερίδα αυτή δεν περιλαμβάνονται μόνο οι φοιτητές των Μαθηματικών.....

[6] Το θεώρημα αυτό, γνωστό ως Θεμελειώδες Θεώρημα της Αριθμητικής, εδώ το αναφέρουμε απλώς ως παράδειγμα. Αργότερα θα δούμε μια απόδειξη (ιδέ Άσκηση $3.2.11_{18}$ και Θεώρημα 6.1.35).

[7] Προς απογοήτευση αυτών, οι οποίοι προσβλέπουν μόνο στις "λογιστικές εφαρμογές" ενός τέτοιου Θεωρήματος.

Ας κάνουμε μια παρένθεση. Όπως, ίσως, το έχετε διαπιστώσει, στα Μαθηματικά (αλλά και γενικότερα) υπάρχει ένας "άτυπος πόλεμος" μεταξύ του "συγγραφέα" και του "αναγνώστη". Είναι αυτό που λέμε *επικοινωνούμε μέσω ενός άψυχου χαρτιού*. Επομένως, πρέπει, τόσο ο συγγραφέας, όσο και ο αναγνώστης να καταβάλουν κάθε δυνατή προσπάθεια, ο μεν συγγραφέας να είναι σαφής και ακριβής στην διατύπωσή του προσέχοντας κάθε λέξη που γράφει, ο δε αναγνώστης να "διυλίζει" κάθε λέξη που διαβάζει. Ειδικά στα Μαθηματικά, όπου δεν πρόκειται για ένα απλό ανάγνωσμα[8].

Ας επανέλθουμε όμως. Βρισκόμαστε στην μελέτη ενός Θεωρήματος. Σε ένα Θεώρημα, ακόμα και όταν δεν είναι διατυπωμένο στην μορφή "Αν ισχύουν τα εξής..., τότε έπεται ότι ισχύει...", πρέπει να διαλευκάνουμε ποια είναι η υπόθεση (ή το σύνολο των υποθέσεων) και ποιο το συμπέρασμα (ή τα συμπεράσματα).

Στο προηγούμενο παράδειγμα. Ας αναδιατυπώσουμε το Θεώρημα ως εξής:

> "Έστω n ένας φυσικός αριθμός μεγαλύτερος του 1. Τότε υπάρχουν μοναδικοί πρώτοι αριθμοί $p_1, p_2, \ldots, p_k$, ώστε $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$."

Τώρα είναι σαφές ποια είναι η υπόθεση και ποιο το συμπέρασμα.

Δεν είναι λίγες οι φορές, όπου "μπερδεύονται" η υπόθεση με το συμπέρασμα. Αυτό ενδέχεται να οφείλεται στην "στρυφνή" διατύπωση από τον συγγραφέα ή επιπόλαια ανάγνωση του αναγνώστη.

Ένα άλλο σημείο, το οποίο πρέπει να προσέξουμε, κατά την κατανόηση ενός Θεωρήματος είναι πόσο "ισχυρές" είναι οι υποθέσεις και τα συμπεράσματα σε ένα Θεώρημα. Ένα "καλό" Θεώρημα είναι αυτό, που έχει "ασθενή" υπόθεση και "ισχυρό" συμπέρασμα.

Εδώ τίθεται ένα άλλο ερώτημα: Με ποια κριτήρια αποφαινόμαστε περί του "ασθενούς" ή "ισχυρού"; Εδώ, επειδή υπεισέρχεται και ο υποκειμενικός παράγων, δεν υπάρχει ομοφωνία μεταξύ των Μαθηματικών. Παρ' όλα ταύτα, ας δούμε το εξής "*Θεώρημα*":

> "Έστω $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$ η ανάλυση ενός φυσικού αριθμού $n > 1$ σε γινόμενο πρώτων. Αν $k = 1$, τότε ο n είναι πρώτος."

Το "*Θεώρημα*" αυτό δεν προσφέρει τίποτε. Έχει τόσο ισχυρή υπόθεση ($k = 1$), ώστε το συμπέρασμα να είναι ασθενέστατο (ο ορισμός του πρώτου).

Ας δούμε ακόμη ένα παράδειγμα:

> "Έστω $r \in \mathbb{R}$, έτσι ώστε $r^2 + 4r + 4 = 0$, τότε $r \geq -2000$".

Εδώ έχουμε μια ισχυρή υπόθεση και ένα ασθενές συμπέρασμα. Στην πραγματικότητα έχουμε ισχυρό αποτέλεσμα $r = -2$, αλλά όπως είναι διατυπωμένο το "*Θεώρημα*" (αν και αληθές) δεν μας προσφέρει κάτι σημαντικό.

Όταν μελετάμε ένα Θεώρημα ένα *φυσιολογικό/αυθόρμητο* ερώτημα, το οποίο (πρέπει να) έρχεται στο μυαλό μας είναι: Ισχύει το αντίστροφο;

Δεν ξεχνάμε ότι ένα Θεώρημα είναι μια αληθής Πρόταση. Στο προηγούμενο κεφάλαιο (σελ. 52) είχαμε μιλήσει για τις αντίστροφες Προτάσεις και για (Λογικά) ισοδύναμες Προτάσεις.

Ας δούμε δύο παραδείγματα:

i. "Έστω n, m δύο φυσικοί αριθμοί, όπου τουλάχιστον ένας εξ αυτών είναι άρτιος, τότε το γινόμενο $n \cdot m$ είναι άρτιος αριθμός."

[8] Εκφράσεις του τύπου "τι θέλει να πει ο ποιητής" δεν έχουν θέση στην μελέτη των Μαθηματικών.

Η αντίστροφη αυτής της Πρότασης είναι η εξής:

"Έστω n, m δύο φυσικοί αριθμοί, αν το γινόμενο $n \cdot m$ είναι άρτιος αριθμός, τότε τουλάχιστον ένας εξ αυτών είναι άρτιος."

Οι δύο αυτές Προτάσεις είναι προφανώς (γιατί;) και οι δύο αληθείς. Επομένως, αποτελούν Θεωρήματα. Μάλιστα θα μπορούσαν να διατυπωθούν ενιαία ως εξής:

"Έστω n, m δύο φυσικοί αριθμοί, τότε το γινόμενο $n \cdot m$ είναι άρτιος αριθμός, αν και μόνο αν τουλάχιστον ένας εξ αυτών είναι άρτιος."

ii. "Έστω n, m δύο περιττοί φυσικοί αριθμοί, τότε το άθροισμα $n+m$ είναι άρτιος αριθμός."

Η πρόταση αυτή είναι αληθής, άρα αποτελεί Θεώρημα.

Η αντίστροφη αυτής της Πρότασης είναι η εξής:

"Έστω n, m δύο φυσικοί αριθμοί, αν το άθροισμα $n+m$ είναι άρτιος αριθμός, τότε οι n και m είναι περιττοί."

Προφανώς (γιατί;) η Πρόταση αυτή είναι ψευδής, άρα δεν αποτελεί Θεώρημα.

Ας τροποποιήσουμε το προηγούμενο παράδειγμα.

"Έστω n, m δύο φυσικοί αριθμοί, αν το άθροισμα $n+m$ είναι άρτιος αριθμός, τότε, είτε και οι δύο n, m είναι περιττοί ή και δύο n, m είναι άρτιοι."

Εύκολα βλέπουμε ότι η Πρόταση αυτή είναι αληθής. Μάλιστα δε και η αντίστροφή της

"Έστω n, m δύο φυσικοί αριθμοί, αν και οι δύο n, m είναι περιττοί ή και δύο n, m είναι άρτιοι, τότε το άθροισμα $n+m$ είναι άρτιος αριθμός." είναι αληθής.

Γενικά η διατύπωση του αντιστρόφου ενός Θεωρήματος δεν είναι πάντα εύκολη. Η προσπάθεια όμως για την διατύπωσή του μας βοηθά να κατανοήσουμε και να διακρίνουμε την διαφορά μεταξύ υπόθεσης και συμπεράσματος.

3.1.2 Η απόδειξη Θεωρημάτων

Το κύριο μέλημα στη σπουδή των Μαθηματικών είναι να μάθουμε να αποδεικνύουμε Θεωρήματα. Όπως είδαμε στην προηγουμένη παράγραφο, πριν προχωρήσουμε στην απόδειξη ενός Θεωρήματος, είναι αναγκαίο να κατανοήσουμε την σημασία του. Εδώ ελλοχεύει *ο κίνδυνος* να επαναπαυθούμε και να πούμε: Μας αρκεί αυτό, μπορούμε να προχωρήσουμε στην "χρήση" του Θεωρήματος.

Η αλήθεια ενός Θεωρήματος **δεν** επιβάλλεται από κάποια εξουσία: *Είναι αληθές διότι το λέω εγώ.*, **δεν** αποφασίζεται με...δημοκρατικές διαδικασίες: *Κατόπιν ψηφοφορίας αποδεχόμεθα την αλήθεια του Θεωρήματος.*, **ούτε** υποδεικνύεται μέσω οραμάτων και χρησμών. Η αλήθεια ενός Θεωρήματος καθορίζεται και τεκμηριώνεται μέσω Μαθηματικής απόδειξης.

Αυτό δεν είναι εύκολο και χρειάζεται προσπάθεια και εξάσκηση. Πολλοί φοιτητές προσπαθούν να αποφύγουν τον *περιττό κόπο* και προσπερνούν τις αποδείξεις[9]. Αυτό είναι μια κακιά συνήθεια, η οποία έχει δυσμενείς επιπτώσεις στην μελέτη των Μαθηματικών. Υπάρχουν πολλοί, οι οποίοι *γυρίζουν την πλάτη* σε αυτήν την ομορφιά των Μαθηματικών προβάλλοντας επιχειρήματα του τύπου:

[9] Δυστυχώς, πολλές φορές, παροτρυνόμενοι από "δασκάλους".

> "Γιατί να διαβάσω μια απόδειξη;", "Γιατί πρέπει να αποδείξω κάτι, αφού το έχουν αποδείξει άλλοι και τους πιστεύω;" ή ακόμη εντονότερα "Δεν χρειάζονται οι αποδείξεις, δεν τις καταλαβαίνω, τις μισώ...."

Η απάντηση θα μπορούσε να είναι ένα σλόγκαν:

> "Μην πιστεύετε αυτά που σας *σερβίρουν*."

Πέραν όμως αυτού, που αφορά όλη την κοινωνία, στα Μαθηματικά υπάρχουν πολλοί και ισχυροί λόγοι, οι οποίοι υπαγορεύουν να μελετάμε τις αποδείξεις και να μάθουμε να κάνουμε αποδείξεις. Ας αναφέρουμε μερικούς.

Μαθαίνουμε να επιχειρηματολογούμε. Η ικανότητα αυτή σε λίγο γίνεται εμφανής και εκτός "Μαθηματικού περιβάλοντος".

Εντοπίζουμε τις αδυναμίες μας και φροντίζουμε να τις "επουλώσουμε".

Ενδέχεται, όταν μελετάμε μια απόδειξη, εκείνη την στιγμή να μην συνειδητοποιούμε ορισμένα πράγματα. Αλλά σε ανύποπτο χρόνο διαπιστώνουμε πως η μελέτη αυτή μας ενδυνάμωσε στην ικανότητα να διατυπώνουμε σύνθετους συλλογισμούς. Αυτό μας επιβεβαιώνει και μας γεμίζει αυτοπεποίθηση.

Τέλος, η χαρά της ανακάλυψης και της δημιουργίας, για τον καθένα ξεχωριστά, κατά την γνώμη μας, δεν έχει αντάλλαγμα. Απλώς αποτελεί το αντάλλαγμα στην προσπάθειά μας για πορεία στους δύσβατους, αλλά τόσο όμορφους, δρόμους της Μαθηματικής Επιστήμης. Αλλά τι είναι (Μαθηματική) απόδειξη;

Η απόδειξη ενός Θεωρήματος είναι μια (συνήθως γραπτή) επαλήθευση ότι το Θεώρημα είναι οριστικά και κατηγορηματικά αληθές. Αυτό σημαίνει ότι, άπαξ και ένα Θεώρημα έχει αποδειχθεί, παραμένει αληθές για πάντα. Αλλά έως ότου αποδειχθεί παραμένει απλώς μια εικασία.

Η επαλήθευση αυτή επιτυγχάνεται με την παράθεση (βήμα–βήμα) μιας ακολουθίας λογικών επιχειρημάτων, εκ των οποίων καθένα συνεπάγεται το επόμενο. Ορισμοί, Θεωρήματα, τα οποία έχουν ήδη αποδειχθεί, όπως επίσης και αξιώματα, τα οποία, όπως έχουμε προείπει, αποτελούν τα σημεία εκκίνησης για την θεμελίωση των Μαθηματικών, επικαλούνται/επιστρατεύονται για να αποδειχθούν άλλα Θεωρήματα.

Μια απόδειξη πρέπει να είναι κατανοητή και πειστική[10] για έναν, ο οποίος κατέχει το απαιτούμενο υπόβαθρο και γνώση, συμπεριλαμβανομένων της κατανόησης της σημασίας κάθε λέξης και συμβόλου, που εμφανίζεται στην πορεία. Είναι κρίσιμο, αμφότεροι, ο "συγγραφέας" και ο "αναγνώστης" μιας απόδειξης να συμφωνούν επακριβώς στην σημασία κάθε λέξης και συμβόλου (δεν ξεχνάμε το προηγούμενο σχόλιο στην σελίδα 78). Διαφορετικά καταλήγουμε σε... Βαβέλ.

Τέλος, θα θέλαμε να επισημάνουμε ότι είναι διαφορετική η σημασία της Μαθηματικής απόδειξης από την σημασία της απόδειξης στην καθημερινότητα (ή στο δικαστήριο). Εκεί επιτρέπονται *αποδείξεις* (με ανοχές), οι οποίες αποδεικνύουν ότι κάτι είναι αληθές... με μεγάλη πιθανότητα. Στα Μαθηματικά δεν επιτρέπονται εκφράσεις του τύπου "*...είμαι σχεδόν σίγουρος*".

Μελετώντας και κατανοώντας αποδείξεις.

Όπως προείπαμε, αναπόσπαστο μέρος της μελέτης ενός Θεωρήματος αποτελεί η μελέτη και η κατανόηση της απόδειξής του. Αυτό αποτελεί και απαραίτητη προϋπόθεση να αποκτήσουμε την ικανότητα να καταστρώνουμε εμείς Μαθηματικές αποδείξεις.

[10]Το τι σημαίνει πειστικό επιχείρημα, έχει φιλοσοφικές προεκτάσεις. Εμείς παραμένουμε σ' αυτό, που...υπαγορεύει η κοινή Λογική.

Πρέπει να έχουμε συνειδητοποιήσει εξαρχής ότι η μελέτη μιας απόδειξης δεν είναι "εύκολη υπόθεση".

Απαραίτητη προϋπόθεση στην μελέτη μιας απόδειξης αποτελεί η ενεργή συμμετοχή μας. Ένας λόγος, που μια απόδειξη φαντάζει βαρετή και απωθητική, είναι διότι την διαβάζουμε σαν ένα κοινό ανάγνωσμα "βολεμένοι στον καναπέ". Επαναλαμβάνουμε ότι απαιτεί *μολύβι και χαρτί*. Πρέπει να αναπτυχθεί ένας διάλογος μεταξύ του μελετητή και του (απόντος) συγγραφέα. Αυτός ο διάλογος αναπτύσεται θέτοντας συνεχώς ερωτήματα και προσπαθώντας να έλθουμε στην θέση του συγγραφέα. Εδώ θα εντοπίσουμε κενά. Υπάρχουν πολλοί λόγοι για την ύπαρξη κενών σε μια απόδειξη, όπως: Σκοπιμότητα, από πλευράς συγγραφέα, για να είμαστε σε εγρήγορση. Ο συγγραφέας θεωρεί κάτι προφανές....Μέχρι ο συγγραφέας να σφάλλει. Ό,τι και να συμβαίνει, τα κενά αυτά πρέπει να πληρωθούν.

Δεν είναι κακό να ανατρέχουμε σε βοήθεια, όταν "κολλάμε" κάπου. Συνήθως, όταν φθάνουμε σε αδιέξοδο, τα εγκαταλείπουμε. Μέγα λάθος. Ενδείκνυται να προχωράμε πιο κάτω, χωρίς να ξεχνάμε τις εκκρεμότητες, και να επανερχόμαστε.

Χωρίζουμε την απόδειξη σε μέρη και εντοπίζουμε σε ποια σημεία χρησιμοποιούνται οι υποθέσεις. Σημειώνουμε πού χρησιμοποιούνται Ορισμοί και πού προηγούμενα Θεωρήματα. Προσπαθούμε να δούμε ομοιότητες με προηγούμενα αποτελέσματα, αλλά και να διακρίνουμε διαφορές. Αυτές οι διαφορές, πολλές φορές, είναι δυσδιάκριτες, αλλά πολύ σημαντικές. Ενδέχεται ένα προηγούμενο Θεώρημα να χρησιμοποιείται διαφορετικά, ανάλογα με το τι θέλουμε να αποδείξουμε, σε επόμενες αποδείξεις. Προσπαθούμε να βρούμε παραδείγματα, όπου εφαρμόζεται, όχι μόνο το συμπέρασμα του Θεωρήματος, αλλά και η απόδειξη αυτή καθ' εαυτή.

Προηγουμένως είπαμε ότι η "καχυποψία" μας για την αλήθεια ενός Θεωρήματος, ξεδιαλύνεται μέσω της απόδειξής του. Εδώ επισημαίνουμε ότι πρέπει να είμαστε καχύποπτοι και ως προς την ορθότητα της απόδειξης. Ενδέχεται ο ισχυρισμός ενός Θεωρήματος να είναι σωστός, αλλά η απόδειξη, που μας παρουσιάζουν, να εμπεριέχει λάθη[11]. Ένας από τους λόγους, που τα Μαθηματικά είναι όμορφα, είναι ότι δεν "κουκουλώνουν" και δεν αποσιωπούν λάθη.

Όταν τελειώσουμε με την απόδειξη ενός Θεωρήματος, πριν προχωρήσουμε, την μελετάμε ολοκληρωμένη από την αρχή και βεβαιωνόμαστε ότι "ρέει".

Τέλος, έρχεται το ερώτημα: Πώς "απομνημονεύουμε" μια απόδειξη; Η απάντηση, κατά την γνώμη μας, είναι:

Δεν απομνημονεύουμε αποδείξεις. Τις κατανοούμε.

Αν έχουμε κατανοήσει μια απόδειξη, τότε δεν χρειάζεται να την απομνημονεύσουμε, διότι έχουμε αποκτήσει κάτι σημαντικότερο, την ικανότητα να την ανακτούμε και να την επαναφέρουμε στο προσκήνιο, και το κυριότερο μαθαίνουμε σιγά–σιγά να κατασκευάζουμε λογικά επιχειρήματα και να γράφουμε αποδείξεις.

Θα κλείσουμε την παράγραφο μελετώντας ένα Θεώρημα και την απόδειξή του. Στο πρώτο Κεφάλαιο στην σελίδα 18 είχαμε δει το εξής Θεώρημα:

Θεώρημα 3.1.4. *(Ο νόμος του Morgan ως προς τα συμπληρώματα συνόλων).*
Έστω E ένα σύνολο και A, B δύο υποσύνολά του, τότε ισχύει ότι:

i $(A \cap B)^c = A^c \cup B^c$.

ii $(A \cup B)^c = A^c \cap B^c$.

[11] Ενδιαφέρον είναι να ανατρέξει κανείς, με την βοήθεια και του διαδικτύου, και να διαπιστώσει πόσες από τις "αποδείξεις" του Πυθαγορείου Θεωρήματος είναι πράγματι αποδείξεις.

(Εδώ χρησιμοποιούμε τον συμβολισμό, που είχαμε αναφέρει στο Σχόλιο στην σελίδα 18 στο πρώτο Κεφάλαιο).

Πριν μελετήσουμε την απόδειξη, ας δούμε την μορφή του Θεωρήματος. Το Θεώρημα είναι διατυπωμένο στην μορφή

"Αν P,....τότε Q".

Εδώ η Πρόταση P (η υπόθεση) είναι η

"Το E είναι ένα σύνολο και A, B δύο υποσύνολά του"

Η Πρόταση Q (το συμπέρασμα) είναι η

"*i.* $(A \cap B)^c = A^c \cup B^c$.

ii. $(A \cup B)^c = A^c \cap B^c$."

Ως προς την υπόθεση. Το μόνο, που χρειάζεται, είναι η έννοια του συνόλου και του υποσυνόλου.

Ως προς το συμπέρασμα. Εδώ εμφανίζονται διάφορα σύμβολα. Πριν προχωρήσουμε, πρέπει να ερμηνεύσουμε τα σύμβολα αυτά. Εμφανίζεται το σύμβολο του συμπληρώματος ενός υποσυνόλου ως προς ένα σύνολο. Πρέπει να πάμε στον αντίστοιχο Ορισμό 1.1.34 στο πρώτο Κεφάλαιο, καθώς και στο Σχόλιο στη σελίδα 18 του πρώτου Κεφαλαίου και να τον επαναφέρουμε στο προσκήνιο. Επίσης, πρέπει να έχουμε στο προσκήνιο τον ορισμό της τομής και της ένωσης συνόλων. Το συμπέρασμα έχει δύο *δυϊκά* σκέλη, όπου εναλλάσσονται η τομή με την ένωση.

Πριν προχωρήσουμε, στην απόδειξη εξετάζουμε "ακραίες περιπτώσεις", όπου ένα από τα υποσύνολα A και B είναι το κενό σύνολο ή όλο το σύνολο E. Βλέπουμε ότι στην περίπτωση αυτή το συμπέρασμα ισχύει κατά προφανή τρόπο (αρκεί ο ορισμός του συμπληρώματος).

Ας προχωρήσουμε στην απόδειξη του Θεωρήματος.

Απόδειξη. Θέλουμε να αποδείξουμε την ισότητα δύο συνόλων.

i. Έστω $x \in (A \cap B)^c$. Από τον ορισμό του συμπληρώματος, αυτό σημαίνει ότι $x \notin A \cap B$. Από την σχέση αυτή (και τον ορισμό της τομής συνόλων) έχουμε ότι $x \notin A$ ή $x \notin B$. Αν $x \notin A$, τότε από την Πρόταση 1.1.36 στο πρώτο Κεφάλαιο, έχουμε ότι $x \in A^c$. Αν $x \notin B$, τότε (πάλι από την ίδια πρόταση) έχουμε $x \in \mathrm{B}^c$. Άρα $x \in A^c$ ή $x \in \mathrm{B}^c$. Δηλαδή, από τον ορισμό της ένωσης συνόλων, έχουμε ότι $(A \cap B)^c \subseteq A^c \cup B^c$.

   Αντίστροφα, έστω $x \in A^c \cup B^c$, τότε (από τον ορισμό της ένωσης συνόλων) $x \notin A$ ή $x \notin B$. Αν $x \notin A$, τότε $x \in A^c \subseteq (A \cap B)^c$ (αφού ισχύει το *ii*) της Πρότασης 1.1.38 στο πρώτο Κεφάλαιο. Όμοια, αν $x \notin B$, έπεται ότι $x \in (A \cap B)^c$. Άρα $A^c \cup B^c \subseteq (A \cap B)^c$. Το αποτέλεσμα τώρα έπεται από το Θεώρημα 1.1.6 στο πρώτο Κεφάλαιο.

ii. Θέτουμε στην θέση του συνόλου A το σύνολο A^c και στην θέση του συνόλου B το σύνολο B^c, εφαρμόζουμε το *i*) λαμβάνοντας υπόψιν ότι ισχύει το *i*) της Πρότασης 1.1.38 στο πρώτο Κεφάλαιο. Οπότε, έπεται το ζητούμενο. (Να συμπληρωθούν οι τεχνικές λεπτομέρειες από τον αναγνώστη).

ό.έ.δ.

Όπως βλέπουμε, η παρούσα απόδειξη **δεν** διαφέρει ουσιαστικά με την απόδειξη, που είχαμε κάνει στο πρώτο κεφάλαιο, τα μόνα σημεία, που επισημάναμε είναι η επίκληση προτάσεων και ορισμών, τα οποία, σιωπηλά μεν συνειδητά δε, είχαμε και εκεί χρησιμοποιήσει.

3.2 Τεχνικές απόδειξης

Υπάρχουν διάφορες στρατηγικές για την απόδειξη ενός Θεωρήματος. Στα επόμενα θα αναπτύξουμε μερικές, χωρίς αυτό να σημαίνει ότι είναι οι μόνες. Το σημαντικό είναι ότι ένα Θεώρημα μπορεί να αποδειχθεί με διαφορετικούς τρόπους και εκτός της προσωπικής προτίμησης αυτού, που κάνει μια απόδειξη, ενδιαφέρον είναι να προσπαθούμε να προσεγγίσουμε την απόδειξη ενός Θεωρήματος με εναλλακτικούς τρόπους. Η προσπάθεια αυτή πολλές φορές αποκαλύπτει *μυστικά και αλήθειες* που ενδέχεται να κρύβει ένα Θεώρημα και τα οποία δεν είναι ορατά με την πρώτη ματιά.

Είχαμε επισημάνει ότι, όταν μελετούμε μια απόδειξη, πρέπει να προσπαθούμε να έλθουμε στη θέση του συγγραφέα. Όταν κάνουμε μια απόδειξη, εναλλάσσονται οι ρόλοι του συγγραφέα και του αναγνώστη και πρέπει να προσπαθούμε να έλθουμε στην θέση του αναγνώστη και να αναρωτηθούμε: Τι απαιτούμε να γνωρίζει ο αναγνώστης για να του είναι κατανοητή η απόδειξη; Τι ερωτήσεις και απορίες ενδέχεται να εγείρει μια απόδειξη; Τι προσδοκούμε να αποκομίσει ο αναγνώστης από μια απόδειξη;

Τέλος, το προφανές και πλέον σημαντικό. Δεν ξεκινάμε να αποδείξουμε ένα Θεώρημα, αν δεν έχουμε συνειδητοποιήσει τι έχουμε ως δεδομένα (υποθέσεις) και τι ως απαιτούμενα (συμπεράσματα).

Στα επόμενα γίνεται μια προσπάθεια (κυρίως για οργανωτικούς λόγους) κατάταξης των αποδείξεων, χωρίς, όπως προείπαμε, να είναι ανάγκη να ακολουθούμε αποκλειστικά έναν (αμιγή) τρόπο απόδειξης.

Κάθε είδος απόδειξης συνοδεύεται από παραδείγματα απόδειξης Θεωρημάτων[12], τα οποία λίγο–πολύ είναι γνωστά και στοιχειώδη. Εδώ μας ενδιαφέρει ο τρόπος απόδειξής τους.

3.2.1 Η ευθεία απόδειξη

Η μέθοδος αυτή αποτελεί την πλέον απλή προσέγγιση στην απόδειξη ενός Θεωρήματος.

Θέτουμε το προς απόδειξη Θεώρημα στην μορφή "A $\Longrightarrow$ B" (Η Πρόταση A είναι η υπόθεση και η Πρόταση B το συμπέρασμα). Σκοπός μας είναι να παραθέσουμε μεταξύ της Πρότασης A και της Πρότασης B μια σειρά συνεπαγωγών

$$\mathrm{A} \Longrightarrow \mathrm{A}_1 \Longrightarrow \cdots \Longrightarrow \mathrm{A}_k \Longrightarrow \mathrm{B},$$

οι οποίες, επικαλούμενοι Ορισμούς, Αξιώματα και Θεωρήματα που έχουν αποδειχθεί προηγουμένως, είναι προφανείς[13]. Εκφράσεις του τύπου "*εύκολα βλέπουμε*", "*είναι προφανές ότι ισχύει*" πρέπει να χρησιμοποιούνται με προσοχή και φειδώ και να

[12]Εδώ πάντα θα χρησιμοποιούμε τον όρο "Θεώρημα", αν και ορισμένες είναι προφανείς παρατηρήσεις, χωρίς να κάνουμε διαβάθμιση ως προς την σημασία ή την δυσκολία, ιδέ Σχόλια 3.1.3. Απλώς για να καταδεικνύεται ότι πρόκειται για έναν ισχυρισμό, σαφώς διατυπωμένο, με την απόδειξή του να έπεται.

[13]Εδώ είναι το κρίσιμο σημείο. Το προφανές **δεν** πρέπει να είναι προφανές (μόνο) στον συγγραφέα, αλλά στον αναγνώστη. Διαφορετικά, θα φθάναμε στην ακραία περίπτωση, για σχεδόν όλες τις συνεπαγωγές "A $\Longrightarrow$ B", να ισχυριζόμαστε ότι είναι προφανείς.

αποτελούν μια έμμεση παρότρυνση από τον συγγραφέα προς τον αναγνώστη να θέσει τα "*γιατί*", τα οποία πρέπει να απαντήσει μόνος του.

Ας δούμε μερικά Παραδείγματα.

Θεώρημα 3.2.1. *Υποθέτουμε ότι ο ακέραιος αριθμός n είναι περιττός. Τότε ο n^2 είναι περιττός.*

Απόδειξη. Υποθέτουμε ότι ο ακέραιος αριθμός n είναι περιττός. Από τον ορισμό των περιττών αριθμών έχουμε ότι υπάρχει ένας ακέραιος αριθμός k τέτοιος, ώστε $n = 2k + 1$. Έχοντας υπόψιν πού θέλουμε να καταλήξουμε, υψώνουμε και τα δύο μέλη της τελευταίας ισότητας στο τετράγωνο και έχουμε

$$n^2 = (2k+1)^2 = (2k+1)(2k+1) = 4k^2 + 2k + 2k + 1 = 2(2k^2 + 2k) + 1.$$

Ο αριθμός $m = 2k^2 + 2k$ είναι ακέραιος, συνεπώς (από τον ορισμό του περιττού αριθμού) ο ακέραιος αριθμός $n^2 = 2m + 1$ είναι περιττός.

Άρα φθάσαμε στο συμπέρασμα. ό.έ.δ.

Θεώρημα 3.2.2. *Έστω m και n πραγματικοί αριθμοί. Υποθέτουμε ότι $n > m > 0$, τότε ισχύει*

$$\frac{m+1}{n+1} > \frac{m}{n}.$$

Απόδειξη. Έχουμε ως υπόθεση ότι $n > m$. Προσθέτουμε και στα δύο μέλη της ανισότητας τον αριθμό mn και έχουμε $mn + n > mn + m$. Βγάζοντας κοινούς παράγοντες έχουμε $(m + 1)n > (n + 1)m$. Πολλαπλασιάζοντας και τα δύο μέλη της ανισότητας αυτής με τον θετικό αριθμό $\frac{1}{n}$ η στροφή της ανισότητας παραμένει και έχουμε

$$(m+1)n \cdot \frac{1}{n} > (n+1)m \cdot \frac{1}{n}.$$

Δηλαδή $m + 1 > (n + 1)m \cdot \frac{1}{n}$. Πολλαπλασιάζοντας και τα δύο μέλη της ανισότητας αυτής με τον θετικό αριθμό $\frac{1}{n+1}$ η στροφή της ανισότητας παραμένει και έχουμε

$$(m+1) \cdot \frac{1}{n+1} > (n+1)m \cdot \frac{1}{n} \cdot \frac{1}{n+1}.$$

Δηλαδή $\frac{m+1}{n+1} > \frac{m}{n}$, το ζητούμενο. ό.έ.δ.

Πριν προχωρήσουμε, ας δούμε μια εν δυνάμει απορία του αναγνώστη.

> Πώς σκέφθηκε ο συγγραφέας να ξεκινήσει την απόδειξη προσθέτοντας και στα δύο μέλη της ανισότητας τον αριθμό mn; Εγώ θα μπορούσα να το σκεφθώ;

Ας κάνουμε την εξής σκέψη. Αν (προσωρινά) υποθέσουμε ότι ισχύει το αποτέλεσμα $\frac{m+1}{n+1} > \frac{m}{n}$, τότε θα ισχύει και η ανισότητα $(m+1) \cdot n > m \cdot (n+1)$, διότι ο πολλαπλασιασμός των μελών μιας ανισότητας με θετικούς αριθμούς δεν αλλάζει την στροφή της ανισότητας.

Αυτό είναι που (πιθανόν) οδήγησε τον συγγραφέα να ξεκινήσει την απόδειξη με αυτόν τον τρόπο. Έκανε αυτό, το οποίο συνηθίζουμε να αποκαλούμε ***ανάλυση του προβλήματος***.

Θεώρημα 3.2.3. *Η ακολουθία* $a_n = \dfrac{n^3+3}{n^2+1}$ *τείνει στο άπειρο.*

Εδώ το Θεώρημα δεν είναι διατυπωμένο στην μορφή "A $\Longrightarrow$ B", αλλά είναι σαφές, όπως έχουμε ήδη σχολιάσει, ποια είναι η υπόθεση και ποίο το συμπέρασμα.

Πριν προχωρήσουμε, στην απόδειξη, πρέπει να ανακαλέσουμε στο προσκήνιο δύο Ορισμούς:[14]

1. Μια ακολουθία (πραγματικών αριθμών) είναι μια απεικόνιση από το σύνολο $\mathbb{N}$ των φυσικών αριθμών στο σύνολο $\mathbb{R}$ των πραγματικών αριθμών.
2. Μια ακολουθία $(a_n)_{n\in N}$ πραγματικών αριθμών τείνει στο άπειρο, αν, δοθέντος ενός πραγματικού αριθμού a, υπάρχει ένας $n_0 \in \mathbb{N}$ (εξαρτώμενος από τον a), έτσι ώστε $a_n > a$, για κάθε $n > n_0$.

Απόδειξη. Θα προσπαθήσουμε να "προσαρμοστούμε" και να φθάσουμε σε ένα σημείο, όπου ικανοποιείται ο ανωτέρω ορισμός.

Έστω ένας πραγματικός αριθμός a. Ξεκινάμε με τον όρο $a_n = \dfrac{n^3+3}{n^2+1}$, σκοπός μας είναι να βρούμε έναν φυσικό αριθμό n_0, ώστε $\dfrac{n^3+3}{n^2+1} > a$ για κάθε $n > n_0$.

Παρατηρούμε ότι $a_n = \dfrac{n^3+3}{n^2+1} > \dfrac{n^3}{n^2+1}$ (ένα κλάσμα μικραίνει αν ελαττώσουμε τον αριθμητή του).

Τώρα συνεχίζουμε και έχουμε $\dfrac{n^3}{n^2+1} \geq \dfrac{n^3}{n^2+n^2} = \dfrac{n}{2}$. (ένα κλάσμα μικραίνει αν αυξήσουμε τον παρονομαστή του και παραμένει το ίδιο αν από τους όρους του διαγράψουμε τον ίδιο παράγοντα).

Επιλέγουμε έναν $n_0 \in \mathbb{N}$ ώστε $n_0 > 2a$, τότε προφανώς $a_n > n/2 > a$ για κάθε $n > n_0$.

Επομένως, πληρούνται οι απαιτήσεις του ανωτέρω ορισμού. Συνεπώς, η δοθείσα ακολουθία τείνει στο άπειρο και η απόδειξη ολοκληρώθηκε;

Προσοχή!!!! Στο τελευταίο βήμα: Είναι προφανές ότι για κάθε πραγματικό αριθμό r υπάρχει φυσικός αριθμός m με $m > r$;

Αυτό διαισθητικά φαντάζει προφανές, αλλά δεν είναι και τόσο προφανές. Θα το δούμε αργότερα, όταν θα θεμελιώσουμε (αυστηρά) τους φυσικούς και πραγματικούς αριθμούς (ιδέ Θεώρημα 7.1.33). ό.έ.δ.

Ας δούμε τώρα μερικές "αποδείξεις".

i. Ελέγξτε τις ακόλουθες συνεπαγωγές και ανακαλύψτε ποια είναι ψευδής.

Έστω δύο ίσοι πραγματικοί αριθμοί.

$$\begin{aligned} a = b &\Longrightarrow a^2 = ab \\ &\Longrightarrow a^2 + a^2 = a^2 + ab \\ &\Longrightarrow 2a^2 - 2ab = a^2 + ab - 2ab \\ &\Longrightarrow 2(a^2 - ab) = a^2 - ab \\ &\Longrightarrow 2 = 1 \ [15]. \end{aligned}$$

[14] Εδώ μας είναι αρκετός ο ορισμός της ακολουθίας. Περισσότερα περί ακολουθιών θα δούμε στο Παράρτημα Α και συγκεκριμένα στην Παράγραφο A.1.0.2.

[15] Προφανώς η τελευταία συνεπαγωγή είναι λάθος (γιατί;).

ii. Ας δούμε τώρα μια άλλη "απόδειξη" γιατί $2=1$.

$$\begin{aligned} -2 = -2 &\Longrightarrow 4-6 = 1-3 \\ &\Longrightarrow 4-6+9/4 = 1-3+9/4 \\ &\Longrightarrow (2-3/2)^2 = (1-3/2)^2 \\ &\Longrightarrow 2-3/2 = 1-3/2 \\ &\Longrightarrow 2 = 1. \end{aligned}$$

Ποια συνεπαγωγή είναι λάθος και γιατί;

iii. Θέλουμε να αποδείξουμε ότι $\sqrt{2}+\sqrt{6}<\sqrt{15}$. Έχουμε

$$\begin{aligned} \sqrt{2}+\sqrt{6}<\sqrt{15} &\Longrightarrow (\sqrt{2}+\sqrt{6})^2<15 \\ &\Longrightarrow 2+2\sqrt{12}+6<15 \\ &\Longrightarrow 8+2\sqrt{12}<15 \Longrightarrow 2\sqrt{12}<7 \\ &\Longrightarrow (2\sqrt{12})^2<49 \\ &\Longrightarrow 48<49, \end{aligned}$$

η τελευταία ανισότητα προφανώς ισχύει, άρα πράγματι $\sqrt{2}+\sqrt{6}<\sqrt{15}$. Υπάρχει λάθος σε κάποια από τις συνεπαγωγές; Προφανώς όχι! Άρα όλα είναι σωστά; Όχι, το λάθος έγκειται στο ότι θεωρήσαμε το προς απόδειξη συμπέρασμα ως αληθές και προχωρήσαμε. Άρα δεν κάναμε τίποτε!

Δεν ξεχνάμε τον πίνακα αληθείας για την συνεπαγωγή $\mathrm{A}\Longrightarrow\mathrm{B}$. Ενδέχεται η Πρόταση Α να είναι ψευδής, αλλά η συνεπαγωγή να είναι αληθής (βλέπε το Παράδειγμα *ii*) στην σελίδα 76).

Στην συγκεκριμένη περίπτωση δεν γνωρίζουμε αν η Πρόταση "$\sqrt{2}+\sqrt{6}<\sqrt{15}$" είναι αληθής ή ψευδής, αυτό θέλουμε να εξετάσουμε. Αυτό είναι ένα σύνηθες λάθος, όπου μπερδεύουμε την υπόθεση με το συμπέρασμα[16].

Παρατήρηση 3.2.4. Στο τελευταίο παράδειγμα, αν προσπαθήσουμε να αντιστρέψουμε τις συνεπαγωγές, δηλαδή

$$48<49 \Longrightarrow (2\sqrt{12})^2<49 \Longrightarrow \cdots \Longrightarrow (\sqrt{2}+\sqrt{6})^2<15 \Longrightarrow \sqrt{2}+\sqrt{6}<\sqrt{15},$$

θα δούμε πράγματι ότι όλες είναι σωστές, άρα έχουμε μια σωστή απόδειξη του ισχυρισμού $\sqrt{2}+\sqrt{6}<\sqrt{15}$. Εδώ το πρόβλημα είναι: Πώς θα φανταστούμε να ξεκινήσουμε από την ανισότητα $48<49$ και να την "μεταμορφώσουμε" στην επιθυμητή ανισότητα $\sqrt{2}+\sqrt{6}<\sqrt{15}$;

Εδώ δεν μπορούμε να μιλήσουμε για *ανάλυση του προβλήματος* (βλέπε την παρατήρηση στο τέλος της απόδειξης του Θεωρήματος 3.2.2), δεδομένου ότι η επιλογή να ξεκινήσουμε από την ανισότητα $48<49$ φαντάζει (και είναι) αυθαίρετη.

[16]Εδώ, ίσως πρέπει να επικαλεσθούμε το εξής: "It isn't that they can't see the solution. It is that they can't see the problem. G.K. Chesterton, The Scandal of Father Brown – 'The Point of a Pin' ". Μια ρήση, που δεν διέπει μόνο τα Μαθηματικά....

3.2.2 Απόδειξη εξαντλώντας όλες τις περιπτώσεις

Ορισμένες φορές, για να αποδείξουμε ένα Θεώρημα, είναι προτιμότερο να το διαχωρίσουμε σε επιμέρους περιπτώσεις και να το αποδείξουμε στις μερικές αυτές περιπτώσεις. Έπειτα να διαπιστώσουμε ότι οι επιμέρους περιπτώσεις καλύπτουν όλες τις δυνατότητες και τέλος να αποφανθούμε για την αλήθεια του Θεωρήματος συνολικά.

Τυπικά, αν θέλουμε να αποδείξουμε την αλήθεια της συνεπαγωγής $P \implies Q$ και η Πρόταση P μπορεί να γραφεί ως $P = A \vee B$, τότε ως γνωστόν (γιατί;)[17] η συνεπαγωγή $(A \vee B) \implies Q$ είναι ισοδύναμη με την $(A \implies Q) \wedge (B \implies Q)$. Επομένως, είναι αρκετό να αποδείξουμε την αλήθεια της συνεπαγωγής $A \implies Q$ **και** $B \implies Q$

Για παράδειγμα: Αν θέλουμε να αποφανθούμε ότι κάτι ισχύει για όλους τους ακεραίους αριθμούς, ενδέχεται να είναι πιο εύκολο να αποδείξουμε ξεχωριστά ότι ο ισχυρισμός ισχύει για τους αρνητικούς ακεραίους, ξεχωριστά για τους θετικούς ακεραίους και ξεχωριστά για το μηδέν. Σε άλλη περίπτωση ίσως να είναι πιο εύκολο να αποδείξουμε ξεχωριστά για τους άρτιους ακεραίους και ξεχωριστά για τους περιττούς ακεραίους.

Στα επόμενα παραδείγματα θα δούμε πώς αντιμετωπίζουμε διάφορα προβλήματα εξαντλώντας (όλες τις) επιμέρους περιπτώσεις.

Θεώρημα 3.2.5. *Το τετράγωνο ενός ακεραίου αριθμού είναι της μορφής* $3k$ *ή* $3k+1$.

Απόδειξη. Ξεκινώντας με έναν τυχαίο ακέραιο αριθμό a και λαμβάνοντας το τετράγωνό του a^2 είναι δύσκολο με ευθεία απόδειξη να καταλήξουμε στο επιθυμητό συμπέρασμα.

Θεωρούμε γνωστό το εξής προφανές (;) αποτέλεσμα: Για κάθε ακέραιο αριθμό a υπάρχουν ακέραιοι αριθμοί m και r έτσι ώστε $a = 3m + r$ και $r \in \{0, 1, 2\}$.

Επομένως

$$a^2 = (3m + r)^2 = 9m^2 + 6mr + r^2 = 3(3m^2 + 2mr) + r^2.$$

Θέτοντας $k = 3m^2 + 2mr$ η προηγουμένη ισότητα γίνεται $a^2 = 3k + r^2$.

Διακρίνουμε τρεις περιπτώσεις:

i. $r = 0$, τότε $a^2 = 3k$.

ii. $r = 1$, τότε $a^2 = 3k + 1$.

iii. $r = 2$, τότε $a^2 = 3k + 2^2 = 3k + 4 = 3k + 3 + 1 = 3(k + 1) + 1$.

Όπως βλέπουμε, και στις τρεις περιπτώσεις ο ισχυρισμός του θεωρήματος είναι αληθής. ό.έ.δ.

Θεώρημα 3.2.6. *Για κάθε φυσικό αριθμό* n*, ο ακέραιος αριθμός* $1 + (-1)^n(2n - 1)$ *είναι πολλαπλάσιο του* 4.

Απόδειξη. Όπως παρατηρούμε, ανάλογα με το αν ο n είναι άρτιος ή περιττός, ο αριθμός $1 + (-1)^n(2n - 1)$ είναι είτε θετικός ή μηδέν ή αρνητικός.

Επομένως, διακρίνουμε περιπτώσεις.

i. Ο n είναι άρτιος. Τότε έχουμε ότι $(-1)^n = 1$. Οπότε, έχουμε

$$1 + (-1)^n(2n - 1) = 1 + (2n - 1) = 2n.$$

Αλλά ο n έχει υποτεθεί άρτιος ($n = 2k$). Συνεπώς, $2n = 4k$.

[17] Για το (γιατί;) μπορείτε να κατασκευάσετε τους αντίστοιχους πίνακες αληθείας.

ii. Ο n είναι περιττός. Τότε έχουμε ότι $(-1)^n = -1$. Οπότε, έχουμε

$$1 + (-1)^n(2n-1) = 1 - (2n-1) = -2n + 2.$$

Αλλά ο n έχει υποτεθεί περιττός ($n = 2k+1$). Οπότε, συνεχίζουμε και έχουμε

$$-2n + 2 = -2(2k+1) + 2 = -4k - 2 + 2 = 4(-k).$$

Όπως βλέπουμε και στις δύο περιπτώσεις, ο αριθμός $1 + (-1)^n(2n-1)$ είναι πάντα πολλαπλάσιο του 4. ό.έ.δ.

Παρατήρηση 3.2.7. Πρέπει να είμαστε προσεκτικοί, να εξαντλούμε όλες τις περιπτώσεις, διαφορετικά η απόδειξη δεν είναι πλήρης. Όπως είδαμε στα παραδείγματα, οι περιπτώσεις που είμαστε υποχρεωμένοι να εξετάσουμε, δεν είναι πολλές. Υπάρχουν όμως και περιπτώσεις, όπου χρειάζονται να διακρίνουμε πολύ περισσότερες περιπτώσεις.

Για την ιστορία αναφέρουμε ότι στην πρώτη απόδειξη του *προβλήματος των τεσσάρων χρωμάτων*[18] χρειάστηκε να διακρίνουν 1936 περιπτώσεις. Στην πορεία, οι απαιτούμενες περιπτώσεις για την επίλυση του προβλήματος περιορίστηκαν περίπου στις 600, οι οποίες παραμένουν πολλές.

3.2.3 Ασκήσεις

1. Αποδείξτε το εξής Θεώρημα:

   Έστω $n \in \mathbb{N}$ με $n > 1$, αν ο n δεν είναι πρώτος, τότε ο $2^n - 1$ δεν είναι πρώτος.

2. Σε συνέχεια της προηγουμένης άσκησης. Μπορούμε να αποδείξουμε το "Θεώρημα";

   Έστω n άρτιος, τότε ο $2^n - 1$ δεν είναι πρώτος.

3. Εξετάστε τι *δεν πάει καλά* στον συλλογισμό.

   "Από την ακολουθία συνεπαγωγών.

   $$2 = 4 \implies 2\pi = 4\pi \implies \sin 2\pi = \sin 4\pi \implies 0 = 0.$$

   Συμπεραίνουμε ότι $2 = 4$."

   Ποια συνεπαγωγή δεν αντιστρέφεται;

4. Έστω $x_1, x_2, \ldots, x_n$ μια αναδιάταξη/μετάθεση των φυσικών αριθμών $1, 2, \ldots, n$. Δείξτε ότι: Αν ο n είναι περιττός, τότε το γινόμενο $(x_1 - 1)(x_2 - 2) \cdots (x_n - n)$ είναι άρτιος αριθμός.

   Ισχύει ο ισχυρισμός: Αν ο n είναι άρτιος, τότε αυτό το γινόμενο είναι περιττός;

[18] Το περίφημο πρόβλημα των τεσσάρων χρωμάτων συνίσταται στο εξής: Δοθέντος ενός χάρτη (ένας κοινός γεωγραφικός χάρτης) αρκούν μόνο τέσσερα χρώματα να χρωματίσουμε τον χάρτη, έτσι ώστε όμορες χώρες να έχουν διαφορετικό χρώμα. Στην αρχή χρειάστηκε ηλεκτρονικός υπολογιστής ώστε να ελεγχθούν όλες οι δυνατές περιπτώσεις χαρτών που μπορούν να σχηματισθούν. Αξίζει να σημειωθεί ότι πολύ αργότερα το θεώρημα απεδείχθη και θεωρητικά με την χρήση αλγεβροτοπολογικών μεθόδων.

5. Να βρεθεί το λάθος στην "απόδειξη" ότι το άθροισμα δυο ρητών αριθμών είναι ρητός αριθμός.

   Έστω m, n δύο ρητοί αριθμοί. Γνωρίζουμε ότι κάθε ρητός αριθμός είναι ένα κλάσμα με όρους ακεραίους αριθμούς. Συνεπώς, $m = p/q$ και $n = r/s$, όπου p, q, r, s είναι ακέραιοι με q, s διάφοροι του μηδενός. Επομένως, $m + n = p/q + r/s$. Αλλά το άθροισμα κλασμάτων είναι κλάσμα, άρα το άθροισμα $m + n$ είναι κλάσμα, δηλαδή ρητός.

6. Να βρεθεί το λάθος στην "απόδειξη" του εξής Θεωρήματος:

   Για κάθε φυσικό αριθμό n, ο αριθμός $n^2 + 5n + 6$ δεν είναι πρώτος.

   Αν ο αριθμός $n^2 + 5n + 6$ δεν είναι πρώτος, υπάρχουν φυσικοί αριθμοί p, q με $p \geq 1$, $q \geq 1$ και $n^2 + 5n + 6 = pq$.

   Επειδή $p < n^2 + 5n + 6$ και $q < n^2 + 5n + 6$, έχουμε ότι ο αριθμός $n^2 + 5n + 6$ δεν είναι πρώτος.

   Μπορείτε να δώσετε μια σωστή απόδειξη του ανωτέρω ισχυρισμού;

7. Να βρεθεί το λάθος στην "απόδειξη" του εξής Θεωρήματος:

   Για όλους τους πραγματικούς αριθμούς x, y ισχύει ότι:

   $$\frac{1}{2}(x + y) \geq \sqrt{xy}.$$

   Υψώνουμε και τα δύο μέλη της ανισότητας στο τετράγωνο.

   Κατόπιν πολλαπλασιάζουμε και τα δύο μέλη της ανισότητας με το 4 και έχουμε

   $$x^2 + 2xy + y^2 \geq 4xy.$$

   Αφαιρούμε το $4xy$ και από τα δύο μέλη και έχουμε

   $$x^2 - 2xy + y^2 \geq 0.$$

   Δηλαδή $(x - y)^2 \geq 0$, κάτι που πάντα ισχύει. Επομένως, το θεώρημα έχει αποδειχθεί.

   Μπορείτε να δώσετε μια σωστή απόδειξη του ανωτέρω ισχυρισμού;

8. Δείξτε ότι για κάθε φυσικό αριθμό n ισχύει ότι

   $$1 + 2 + 3 + \cdots n = \frac{n(n+1)}{2}.$$

   Υπόδειξη. Μπορείτε να διακρίνετε περιπτώσεις, αν ο n είναι άρτιος ή περιττός.

9. Για κάθε πραγματικό αριθμό x με $0 < x < 4$ δείξτε ότι

   $$\frac{4}{x(4-x)} \geq 1.$$

10. Υποθέτουμε ότι για τους πραγματικούς αριθμούς x, y ισχύει ότι

    $$x^2 + 5y = y^2 + 5x.$$

    Δείξτε ότι $x = y$ ή $x + y = 5$.

11. Δείξτε ότι για κάθε φυσικό αριθμό $n \geq 2$ υπάρχουν n το πλήθος διαδοχικοί φυσικοί αριθμοί, οι οποίοι είναι όλοι σύνθετοι.

    Διαφορετικά, υπάρχουν οσοδήποτε μεγάλα "χάσματα" μεταξύ πρώτων αριθμών.

    Υπόδειξη. Θεωρήστε τους αριθμούς $n! + 2$, $n! + 3$, ...

12. Να αποδείξετε το αντίστροφο του Θεωρήματος 3.2.6. Δηλαδή για κάθε ακέραιο αριθμό a, ο οποίος είναι πολλαπλάσιο του 4, υπάρχει φυσικός αριθμός n ώστε

$$a = 1 + (-1)^n(2n - 1).$$

13. Να αποδείξετε, διακρίνοντας περιπτώσεις, την γνωστή (;) *τριγωνική ιδιότητα*:

    Για κάθε $x, y \in \mathbb{R}$ ισχύει ότι $| x + y | \leq | x | + | y |$.

14. Έστω ABC ένα τρίγωνο. Δείξτε ότι υπάρχει μοναδικός κύκλος, ο οποίος διέρχεται από τις τρεις κορυφές του τριγώνου (Κάθε τρίγωνο είναι εγγράψιμο σε κύκλο).

15. Έστω ABC ένα τρίγωνο. Δείξτε ότι υπάρχει μοναδικός κύκλος, ο οποίος εφάπτεται στις τρεις πλευρές του τριγώνου. (Κάθε τρίγωνο είναι περιγράψιμο σε κύκλο).

    Αν "επιτρέψουμε" ένας κύκλος να εφάπτεται στους φορείς των πλευρών ενός τριγώνου, πόσοι τέτοιοι κύκλοι υπάρχουν;

3.2.4 Η εις άτοπο απαγωγή

Στο προηγούμενο κεφάλαιο (Παρατήρηση 2.1.3) είχαμε αναφερθεί στον Νόμο του ενδιάμεσου αποκλεισμού. Δηλαδή μια Πρόταση είναι είτε αληθής ή ψευδής. Αυτό μας δίνει την δυνατότητα να αναπτύξουμε μια άλλη τεχνική απόδειξης.

Υποθέτουμε (προσωρινά) ότι το προς απόδειξη συμπέρασμα του Θεωρήματος δεν ισχύει (η Πρόταση είναι ψευδής) και με (Λογικές) συνεπαγωγές καταλήγουμε σε ένα συμπέρασμα, το οποίο είναι πασιφανώς ψευδές (άτοπο) (π.χ. $0 = 1$ ή...η θάλασσα είναι μελάνι), επομένως η (προσωρινή) υπόθεσή μας είναι λάθος. Άρα το αρχικό συμπέρασμα δεν μπορεί να είναι ψευδές. Δηλαδή...είναι αληθές.

Ενδέχεται κάποιος να έχει κάποια *καχυποψία* κατά πόσον αυτή η τεχνική απόδειξης μπορεί να θεωρηθεί αποδεκτή. Ας ανατρέξουμε στους πίνακες αληθείας. Στο προηγούμενο κεφάλαιο (Παρατήρηση $2.1.13_4$) είχαμε σχολιάσει την άρνηση της συνεπαγωγής $\mathrm{A} \Longrightarrow \mathrm{B}$. Συγκεκριμένα είχαμε τον εξής πίνακα αληθείας:

A	B	$\mathrm{A} \Longrightarrow \mathrm{B}$	$\neg\,(\mathrm{A} \Longrightarrow \mathrm{B})$	$\mathrm{A} \wedge (\neg\,\mathrm{B})$
A	A	A	Ψ	Ψ
A	Ψ	Ψ	A	A
Ψ	A	A	Ψ	Ψ
Ψ	Ψ	A	Ψ	Ψ

Παρατηρούμε ότι η άρνηση $\neg\,(\mathrm{A} \Longrightarrow \mathrm{B})$ είναι ισοδύναμη με την Πρόταση $\mathrm{A} \wedge (\neg\,\mathrm{B})$. Επομένως, για να χρησιμοποιήσουμε την τεχνική της εις άτοπον απαγωγής, πρέπει να αποδείξουμε ότι με την υπόθεση $\mathrm{A} \wedge (\neg\,\mathrm{B})$ οδηγούμαστε σε αντίφαση (άτοπο).

Ας δούμε μερικά παραδείγματα.

Θεώρημα 3.2.8. *Ο πραγματικός αριθμός $\sqrt{2}$ είναι άρρητος.*

Απόδειξη. Πριν ξεκινήσουμε, φέρνουμε στο *προσκήνιο* πότε ένας πραγματικός αριθμός ονομάζεται άρρητος.

Ένας πραγματικός αριθμός r ονομάζεται άρρητος αν δεν είναι ρητός, δηλαδή $r \neq m/n$ για κάθε $m, n \in \mathbb{Z}$, $n \neq 0$.

Επίσης υπενθυμίζουμε, σε ένα κλάσμα m/n μπορεί να υποτεθεί ότι οι όροι m, n δεν είναι και οι δύο άρτιοι (γιατί;).

Θέλουμε να αποδείξουμε ότι ο $\sqrt{2}$ είναι άρρητος. Δεν έχουμε ένα "ορατό" σημείο για να ξεκινήσουμε. Αν όμως υποθέσουμε ότι ισχύει η άρνηση της Πρότασης "Ο πραγματικός αριθμός $\sqrt{2}$ είναι άρρητος", δηλαδή ότι "Ο πραγματικός αριθμός $\sqrt{2}$ είναι ρητός", τότε έχουμε ένα σημείο *εκκίνησης*.

Έστω ότι $\sqrt{2} = m/n$ με m, n ακεραίους, τότε υψώνοντας και τα δύο μέλη στο τετράγωνο έχουμε ότι $2 = m^2/n^2$, δηλαδή $2n^2 = m^2$. Από την τελευταία σχέση έπεται ότι ο m^2 είναι άρτιος, δηλαδή ο m είναι άρτιος (γιατί;). Επομένως, από την προηγούμενη επισήμανση, αφού ο m είναι άρτιος, ο n μπορεί να θεωρηθεί περιττός. Αλλά τότε έχουμε ότι και ο n^2 είναι περιττός.

Συνεπώς, μέχρι τούδε έχουμε ότι ο m είναι άρτιος, δηλαδή της μορφής $m = 2k$, $k \in Z$ και ο n^2 είναι περιττός.

Οπότε, από την σχέση $2n^2 = m^2$, έχουμε $2n^2 = (2k)^2$, δηλαδή $n^2 = 2k^2$. Τούτο έρχεται σε αντίφαση με το ότι προηγουμένως είχαμε καταλήξει στο ότι ο n^2 είναι περιττός.

Γιατί καταλήξαμε στην ψευδή Πρόταση "Ο n^2 είναι περιττός **και** ο n^2 είναι άρτιος"; Διότι στην αρχή υποθέσαμε (ψευδώς) ότι "Ο πραγματικός αριθμός $\sqrt{2}$ είναι ρητός".

Άρα, με το άτοπο στο οποίο καταλήξαμε, έχουμε αποδείξει τον αρχικό ισχυρισμό του θεωρήματος. ό.έ.δ.

Θεώρημα 3.2.9. *Υπάρχουν άπειροι, το πλήθος, πρώτοι αριθμοί.*

Απόδειξη. Υποθέτουμε ότι ισχύει η άρνηση της Πρότασης, δηλαδή ότι: Υπάρχει πεπερασμένο το πλήθος πρώτοι αριθμοί.

Επομένως, μπορούμε να τους απαριθμήσουμε: $p_1, p_2, \ldots, p_k$. Λαμβάνουμε τον ακέραιο αριθμό $n = p_1\, p_2 \cdots p_k + 1$. Ο αριθμός αυτός είναι διαφορετικός από όλους τους πρώτους p_i, επομένως δεν είναι πρώτος. Επειδή είναι μεγαλύτερος από το 1, υπάρχει (τουλάχιστον) ένας πρώτος αριθμός που τον διαιρεί (γιατί;), έστω ο p_i, δηλαδή $n = p_i c$. Τότε, από την ισότητα $n = p_1\, p_2 \cdots p_k + 1$, έχουμε ότι

$$c = (p_1\, p_2 \cdots p_{i-1} p_{i+1} \cdots p_k) + 1/p_i.$$

Από την τελευταία σχέση έπεται ότι ο αριθμός $1/p_i$ είναι ακέραιος, αυτό όμως είναι άτοπο.

Πώς καταλήξαμε στην αντίφαση αυτή; Διότι υποθέσαμε (ψευδώς) ότι το πλήθος των πρώτων αριθμών είναι πεπερασμένο. ό.έ.δ.

Παρατηρήσεις 3.2.10.

1. Αυτό το Θεώρημα έχει αποδειχθεί πριν από περίπου 2300 χρόνια από τον αρχαίο Έλληνα Μαθηματικό Ευκλείδη και μάλιστα με την μέθοδο της εις άτοπον απαγωγής.

2. Το θεώρημα αυτό ίσως θεωρηθεί πρωθύστερο, δεδομένου ότι δεν έχουμε μελετήσει διεξοδικά τους πρώτους αριθμούς. Αυτό δεν σημαίνει ότι με τις λιγοστές γνώσεις που διαθέτουμε δεν μπορούμε να το αποδείξουμε, εδώ, άλλωστε, μας ενδιαφέρει η μέθοδος της απόδειξης.

3. Πίσω από το *γιατί;*, που εμφανίζεται στην απόδειξη, υπάρχει η εξής Πρόταση: "Για κάθε θετικό ακέραιο, μεγαλύτερο του 1, υπάρχει ένας πρώτος αριθμός, ο οποίος τον διαιρεί."

   Μπορείτε να την αποδείξετε; (ιδέ Πρόταση 6.1.34).

   (Η απόδειξη του αποτελέσματος αυτού δεν απαιτεί το αποτέλεσμα, που μόλις αποδείξαμε. Επομένως, δεν αποτελεί πρωθύστερο η επίκλησή του εδώ).

4. Η απόδειξη του προηγουμένου θεωρήματος προσφέρει κάτι περισσότερο απ' ό,τι αναφέρεται στην εκφώνηση.

   Μας δίνει μια μέθοδο "παραγωγής" πρώτων αριθμών.

   Ας ξεκινήσουμε από τον πρώτο αριθμό $p_1 = 2$, θέτουμε $p_2 = p_1 + 1 = 3$, $p_3 = p_1 \cdot p_2 + 1 = 7$, $p_4 = p_1 \cdot p_2 \cdot p_3 + 1 = 43, \ldots$, και ούτω καθ' εξής. Όλοι οι αριθμοί που προκύπτουν με αυτήν την διαδικασία είναι πρώτοι (γιατί;).

   Εδώ πρέπει να επισημάνουμε ότι: Η μέθοδος αυτή δεν μας δίνει έναν "τύπο" να υπολογίζουμε τον πρώτο p_n ως μια συνάρτηση του n, αλλά πρέπει, αναδρομικά, να υπολογίζουμε όλους τους προηγούμενους πρώτους για να μπορέσουμε να υπολογίσουμε τον p_n.

   Επίσης, πρέπει να επισημάνουμε ότι με την μέθοδο αυτή ΔΕΝ κατασκευάζουμε όλους τους πρώτους, παρ' όλα ταύτα, αποτελεί μια απλή και πολύ χρήσιμη μέθοδο παραγωγής πρώτων αριθμών, δεδομένου ότι δεν υπάρχει, μέχρι τώρα, ένας (απλός) τρόπος να υπολογίζουμε όλους τους πρώτους αριθμούς.

Ας δούμε ένα ακόμη παράδειγμα.

Θεώρημα 3.2.11. *Ισχύει ότι* $\sqrt{2} + \sqrt{6} < \sqrt{15}$.

Απόδειξη. Υποθέτουμε ότι ισχύει η άρνηση της Πρότασης, δηλαδή

$$\sqrt{2} + \sqrt{6} \geq \sqrt{15}.$$

Υψώνουμε και τα δύο μέλη αυτής της ανισότητας εις το τετράγωνο και η ανισότητα διατηρείται (γιατί;). Επομένως, έχουμε

$$(\sqrt{2} + \sqrt{6})^2 \geq (\sqrt{15})^2$$

και με διαδοχικές πράξεις έχουμε

$$2 + 2\sqrt{2} \cdot \sqrt{6} + 6 \geq 15 \implies 8 + 2\sqrt{12} \geq 15 \implies 2\sqrt{12} \geq 7.$$

Στην τελευταία ανισότητα υψώνουμε και τα δύο μέλη εις το τετράγωνο και έχουμε

$$48 \geq 49.$$

Η τελευταία ανισότητα προφανώς δεν ισχύει. Πώς φθάσαμε σε αυτήν την αντίφαση; Διότι υποθέσαμε (ψευδώς) ότι $\sqrt{2} + \sqrt{6} \geq \sqrt{15}$. Άρα πράγματι ισχύει ότι

$$\sqrt{2} + \sqrt{6} < \sqrt{15}.$$ ό.έ.δ.

Παρατήρηση 3.2.12. Την ανισότητα αυτή την είχαμε δει στα παραδείγματα με λάθος αποδείξεις (σελ. 86). Εκεί δεν είχαμε ένα σημείο *εκκίνησης* και πέσαμε στην παγίδα να θεωρήσουμε το συμπέρασμα ως υπόθεση. Κατόπιν, στην εκεί παρατήρηση, είδαμε ότι θα μπορούσαμε να ξεκινήσουμε από την ανισότητα $48 < 49$ και αντιστρέφοντας τις συνεπαγωγές να αποδείξουμε την ζητουμένη ανισότητα. Αλλά είχαμε προβληματιστεί. Πώς θα σκεφθούμε να ξεκινήσουμε από την ανισότητα $48 < 49$; Στην πραγματικότητα αυτό κάναμε στην προηγουμένη απόδειξη.

Θα κλείσουμε την παράγραφο με την εξής παρατήρηση: Όταν αποδεικνύουμε ένα θεώρημα με την μέθοδο της εις άτοπον απαγωγής, ενδέχεται κάπου να κάνουμε ένα λάθος και να φθάσουμε σε άτοπο. Η αντίφαση, που προκύπτει, δεν οφείλεται στην αρχική μας υπόθεση, αλλά στο ενδιάμεσο λάθος. Επομένως, πρέπει να είμαστε προσεκτικοί στο σημείο αυτό.

3.2.5 Η μέθοδος της αντιθετοαντιστροφής

Στο προηγούμενο κεφάλαιο (Ορισμός 2.1.14$_c$) είχαμε δει ότι, αν έχουμε την συνεπαγωγή "Αν Α, τότε Β", τότε ορίζεται η αντιθετοαντίστροφη συνεπαγωγή "Αν $\neg$ Β, τότε $\neg$ Α".

Μάλιστα δε ο πίνακας αληθείας για τις δύο αυτές Προτάσεις είναι ο

Α	Β	$\Α \Longrightarrow \Β$	$\neg\ \Β \Longrightarrow \neg\ \Α$
Α	Α	Α	Α
Α	Ψ	Ψ	Ψ
Ψ	Α	Α	Α
Ψ	Ψ	Α	Α

Από τον οποίο συνάγεται ότι:

> *Η αντιθετοαντιστροφή μιας συνεπαγωγής είναι ισοδύναμη (ως Πρόταση) με την (αρχική) συνεπαγωγή.*

Επομένως, ορισμένες φορές αντί να προσπαθήσουμε να αποδείξουμε την αλήθεια της συνεπαγωγής $\Α \Longrightarrow \Β$, είναι προτιμότερο να προσπαθήσουμε να αποδείξουμε την αλήθεια της συνεπαγωγής $\neg\ \Β \Longrightarrow \neg\ \Α$.

Πριν δούμε ορισμένα παραδείγματα ας κάνουμε κάποιες παρατηρήσεις.

Παρατηρήσεις 3.2.13.

1. Πολλές φορές γίνεται σύγχυση μεταξύ της αντιθετοαντίστροφης Πρότασης και της αντίστροφης Πρότασης. Η αντίστροφη Πρόταση της "Αν Α, τότε Β" είναι η "Αν Β, τότε Α", η οποία, όπως έχουμε επισημάνει, δεν είναι πάντα ισοδύναμη με την αρχική "Αν Α, τότε Β".

2. Δεν πρέπει να συγχέουμε την αντιθετοαντιστροφή με την εις άτοπον απαγωγή. Και οι δύο έχουν ως πρώτο μέρος της συνεπαγωγής την $\neg$Β, αλλά στην μεν αντιθετοαντιστροφή έχουμε ως σκοπό να καταλήξουμε στην $\neg$ Α, ενώ στην εις άτοπον απαγωγή ο σκοπός μας είναι να καταλήξουμε σε ένα συμπέρασμα, το οποίο είναι πασιφανώς ψευδές (άτοπο).

Ως πρώτο παράδειγμα θα αποδείξουμε το ίδιο Θεώρημα, τόσο με ευθεία απόδειξη, όσο και με την μέθοδο της αντιθετοαντιστροφής.

Θεώρημα 3.2.14. *Για $x \in \mathbb{Z}$, αν ο $7x + 5$ είναι άρτιος, τότε ο x είναι περιττός.*

Απόδειξη. Ευθεία απόδειξη.

Υποθέτουμε ότι ο $7x + 5$ είναι άρτιος. Τότε υπάρχει ακέραιος αριθμός a έτσι ώστε $7x + 5 = 2a$.

Από την τελευταία σχέση έχουμε ότι

$$x = 2a - 6x - 5 = 2a - 6x - 6 + 1 = 2(a - 3x - 3) + 1.$$

Άρα $x = 2k + 1$, όπου ο $k = a - 3x - 3$ είναι πάντα ακέραιος αριθμός (για οποιονδήποτε ακέραιο x). Συνεπώς, ο x είναι περιττός.

Αντιθετοαντιστροφή.

Υποθέτουμε ότι ο x δεν είναι περιττός, δηλαδή είναι άρτιος. Συνεπώς, $x = 2k$, τότε

$$7x + 5 = 7(2k) + 5 = 2(7k) + 4 + 1 = 2(7k + 2) + 1 = 2m + 1,$$

άρα ο $7x + 5$ είναι περιττός, δηλαδή όχι άρτιος. Άτοπο. ό.έ.δ.

Οπότε,...διαλέγουμε και παίρνουμε....

Αν όμως εντρυφήσουμε περισσότερο, θα δούμε ότι η μέθοδος της αντιθετοαντιστροφής "ρέει" ομαλότερα. Δεδομένου ότι στην ευθεία απόδειξη είχαμε πληροφορίες για τον αριθμό $7x + 5$ και έπρεπε να εξάγουμε πληροφορίες για τον αριθμό x, ενώ στην αντιθετοαντιστροφή είχαμε πληροφορίες για τον αριθμό x και θέλαμε να εξάγουμε πληροφορίες για τον αριθμό $7x + 5$.

Θεώρημα 3.2.15. *Έστω $x, y \in \mathbb{Z}$. Υποθέτουμε ότι το 5 δεν διαιρεί το γινόμενο xy. Τότε το 5 δεν διαιρεί τον x και το 5 δεν διαιρεί τον y.*

Απόδειξη. Για να εφαρμόσουμε αντιθετοαντιστροφή, πρέπει να υποθέσουμε ότι δεν είναι αληθής η Πρόταση

"Το 5 δεν διαιρεί τον x **και** το 5 δεν διαιρεί τον y".

Εδώ πρέπει να είμαστε προσεκτικοί. Ποια είναι η άρνησή της; Δεν είναι αληθές ότι το 5 δεν διαιρεί τον x ή δεν είναι αληθές ότι το 5 δεν διαιρεί τον y. Συνεπώς, η άρνηση είναι η εξής:

"Το 5 διαιρεί τον x **ή** το 5 διαιρεί τον y".

Υποθέτουμε ότι το 5 διαιρεί τον x. Τότε υπάρχει ακέραιος a, έτσι ώστε $x = 5a$, οπότε

$$xy = (5a)y = 5(ay).$$

Όμοια, αν υποθέσουμε ότι το 5 διαιρεί τον y. Τότε υπάρχει ακέραιος b, έτσι ώστε $y = 5b$, οπότε

$$xy = x(5b) = 5(xb).$$

Δηλαδή, πάντα το 5 διαιρεί το γινόμενο xy. Άρα η Πρόταση

"Το 5 δεν διαιρεί το γινόμενο xy".

δεν είναι αληθής. Οπότε, από την αρχή της αντιθετοαντιστροφής έπεται ότι ο αρχικός ισχυρισμός είναι αληθής και τέλος. ό.έ.δ.

Στην προηγουμένη απόδειξη θα μπορούσαμε, όταν φθάσαμε στη διαπίστωση ότι πάντα το 5 διαιρεί το γινόμενο xy, να πούμε ότι φθάσαμε σε αντίφαση με την αρχική υπόθεση ότι το 5 δεν διαιρεί το γινόμενο xy. Άτοπο.

Ας θυμηθούμε τον Ορισμό, πότε μια απεικόνιση ονομάζεται ένα προς ένα[19].

> Μια απεικόνιση $f : A \longrightarrow B$ ονομάζεται ένα προς ένα, αν για $x, y \in A$ με $x \neq y$ έχουμε ότι $f(x) \neq f(y)$.

Τις περισσότερες όμως φορές, για να δείξουμε ότι μια απεικόνιση είναι ένα προς ένα, μπορούμε να χρησιμοποιήσουμε την αντιθετοαντίστροφη και να έχουμε έναν ισοδύναμο ορισμό. Πράγματι έχουμε.

Θεώρημα 3.2.16. *Η απεικόνιση $f : A \longrightarrow B$ είναι ένα προς ένα αν για $x, y \in A$ με $f(x) = f(y)$ έχουμε ότι $x = y$.*

Απόδειξη. Έχουμε την Πρόταση

"Για $x, y \in A$ με $x \neq y \Longrightarrow f(x) \neq f(y)$".

Η αντιθετοαντίστροφη αυτής της συνεπαγωγής είναι η συνεπαγωγή

"Για $x, y \in A$ με $f(x) = f(y) \Longrightarrow x = y$".

Λόγω της ισοδυναμίας των δύο Προτάσεων έχουμε τον ισοδύναμο ορισμό του ένα προς ένα μιας απεικόνισης. ό.έ.δ.

3.2.6 Ασκήσεις

1. Έστω $a, b, c \in \mathbb{Z}$. Αν $a^2 + b^2 = c^2$, Δείξτε ότι ο a ή ο b είναι άρτιος.

2. Έστω $a, b \in \mathbb{Z}$. Αν το 4 διαιρεί το άθροισμα $a^2 + b^2$, δείξτε ότι οι a και b δεν είναι και οι δύο περιττοί.

3. Έστω $a, b \in \mathbb{Z}$. Υποθέτουμε ότι και οι δύο είναι άρτιοι ή και οι δύο περιττοί. Δείξτε ότι από τους αριθμούς $3a + 7$ και $7b - 4$ μόνο ο ένας είναι άρτιος.

4. Δείξτε ότι η εξίσωση $x^7 + 3x^3 + 5$ δεν έχει ρητές ρίζες.

5. Έστω $x \in R$ με $x^5 + 7x^3 + 5x \geq x^4 + x^2 + 8$. Δείξτε ότι $x > 0$.

6. Δείξτε, με την εις άτοπον απαγωγή, ότι υπάρχει άπειρο το πλήθος ρητών μεταξύ του 0 και του 1.

7. Έστω ένας ρητός αριθμός $a < \sqrt{2}$. Δείξτε ότι υπάρχει ρητός αριθμός b με $a < b < \sqrt{2}$.

   Δηλαδή δεν υπάρχει μέγιστος ρητός αριθμός μικρότερος του $\sqrt{2}$.

8. Ο αριθμός $\sqrt{2} + \sqrt{3}$ είναι ρητός ή άρρητος;

9. Ο αριθμός $\sqrt[3]{2}$ είναι ρητός ή άρρητος;

[19] Εδώ κάνουμε πρωθύστερο, καθότι οι απεικονίσεις μελετώνται στο επόμενο Κεφάλαιο. Αυτό δεν αποτελεί πρόβλημα, διότι εδώ μόνο θέλουμε να δείξουμε μια σημαντική εφαρμογή της μεθόδου της αντιθετοαντιστροφής.

10. Έστω $f : A \longrightarrow B$ και $g : B \longrightarrow C$ δύο απεικονίσεις. Υποθέτουμε ότι η σύνθεση $g \circ f$ είναι ένα προς ένα και επί. Δείξτε ότι η f είναι ένα προς ένα και η g επί[20].

11. Δείξτε ότι οι μόνοι διαδοχικοί, μη αρνητικοί, ακέραιοι a, b, c, έτσι ώστε

$$a^2 + b^2 = c^2$$

είναι οι $3, 4, 5$.

12. Έστω οι ακέραιοι αριθμοί a, b, c. Υποθέτουμε ότι υπάρχει ένας ακέραιος αριθμός d, ο οποίος διαιρεί τον a και τον b, αλλά δεν διαιρεί τον c. Δείξτε ότι δεν υπάρχουν ακέραιοι αριθμοί x, y, οι οποίοι να ικανοποιούν την ισότητα $ax + by = c$.

13. Δείξτε ότι για κάθε πραγματικό αριθμό $\vartheta \in [0, \pi/2]$ ισχύει ότι $\sin \vartheta + \cos \vartheta \geq 1$.

14. Δείξτε ότι δεν υπάρχουν ρητοί αριθμοί x, y, οι οποίοι να ικανοποιούν την εξίσωση $x^2 + y^2 - 3 = 0$.

15. Χρησιμοποιώντας την προηγούμενη άσκηση να δείξετε ότι ο αριθμός $\sqrt{3}$ είναι άρρητος.

    Μπορείτε να γενικεύσετε και να αποδείξετε ότι για κάθε θετικό περιττό ακέραιο k ο αριθμός $\sqrt{3^k}$ είναι άρρητος;

16. Δείξτε ότι ο $\log_2 3$ είναι άρρητος. (Εξ ορισμού, ο $\log_2 3$ είναι ένας πραγματικός αριθμός x, έτσι ώστε $2^x = 3$).

17. Δείξτε ότι οι διχοτόμοι των γωνιών ενός τριγώνου ABC διέρχονται από ένα σημείο.

18. Δείξτε ότι οι μεσοκάθετοι των πλευρών ενός τριγώνου ABC διέρχονται από ένα σημείο.

19. Δείξτε ότι τα ύψη ενός τριγώνου ABC διέρχονται από ένα σημείο.

20. Θα *δείξουμε* ότι το 1 είναι ο μεγαλύτερος ακέραιος αριθμός.

    Υποθέτουμε ότι το 1 δεν είναι ο μεγαλύτερος ακέραιος αριθμός. Έστω n ο μεγαλύτερος ακέραιος αριθμός. Τότε $n > 1$. Πολλαπλασιάζοντας και τα δύο μέλη της ανισότητας αυτής με τον θετικό αριθμό n έχουμε $n^2 > 1 \cdot n = n$. Ο n^2 είναι ακέραιος. Δηλαδή βρήκαμε έναν ακέραιο αριθμό, τον n^2, (γνήσια) μεγαλύτερο από τον μεγαλύτερο ακέραιο αριθμό n, άτοπο. Συνεπώς, η υπόθεσή μας ότι το 1 δεν είναι ο μεγαλύτερος ακέραιος αριθμός είναι ψευδής. Άρα, πράγματι το 1 είναι ο μεγαλύτερος ακέραιος αριθμός.

    Τι συμβαίνει; Πού υπάρχει λάθος;

[20] Εδώ, όπως προείπαμε κάνουμε πρωθύστερο, καθότι οι απεικονίσεις μελετώνται στο επόμενο κεφάλαιο. Αυτό δεν αποτελεί πρόβλημα. Μπορεί κάποιος, ο οποίος γνωρίζει τους σχετικούς ορισμούς, να επιχειρήσει να δώσει εδώ μια απόδειξη και μετά να ανατρέξει στο Θεώρημα 4.5.33 και να συγκρίνει την τεχνική απόδειξης, που εφάρμοσε εδώ, με την τεχνική της απόδειξης που εφαρμόζεται εκεί.

3.2.7 Διάψευση Προτάσεων (αντιπαραδείγματα)

Όταν μιλήσαμε, για πρώτη φορά, για θεωρήματα (ιδέ σελ. 73), είχαμε πει ότι ένα θεώρημα, έως ότου αποδειχθεί, αποτελεί εικασία. Επομένως, η *πρόκληση* είναι να αποδείξουμε ή να διαψεύσουμε την εικασία.

Στα προηγούμενα κεφάλαια αναπτύξαμε διάφορες τεχνικές απόδειξης θεωρημάτων. Ορισμένες φορές είναι ανάγκη να διαψεύσουμε μια εικασία. Εδώ πρέπει να διακρίνουμε δύο περιπτώσεις.

Πρώτον, μας είναι γνωστό ότι μια εικασία δεν είναι αληθής και εμείς καλούμαστε να το επιβεβαιώσουμε/αποδείξουμε.

Δεύτερον, δεν γνωρίζουμε αν η εικασία είναι ή δεν είναι αληθής και, στην προσπάθειά μας να την επιβεβαιώσουμε/αποδείξουμε, να διαπιστώσουμε ότι δεν είναι αληθής, οπότε η εικασία διαψεύδεται/καταρρίπτεται.

Η πρώτη περίπτωση είναι σχετικά εύκολα διαχειρίσιμη δεδομένου ότι, αν έχουμε να αποδείξουμε ότι η Πρόταση P δεν είναι αληθής, τότε στην πραγματικότητα καλούμαστε να αποδείξουμε ότι η Πρόταση $\neg$ P είναι αληθής. Οπότε, έχοντας τις τεχνικές απόδειξης που παρουσιάσαμε μπορούμε να προχωρήσουμε.

Η δεύτερη περίπτωση είναι πιο δύσκολα διαχειρίσιμη, δεδομένου ότι υπάρχει μια διάχυτη αβεβαιότητα, που περιβάλλει την εικασία.

Τα παραδείγματα, που ακολουθούν, δεν είναι δύσκολες εικασίες, που παραμένουν αναπάντητες και, όπως προείπαμε, τροφοδοτούν την Μαθηματική έρευνα. Είναι απλά παραδείγματα για να εξοικειωθούμε με την αντιμετώπιση τέτοιων περιπτώσεων. Πριν παραθέσουμε συγκεκριμένα παραδείγματα, ας δούμε μια γενικότερη αντιμετώπιση.

Είπαμε ότι για να διαψεύσουμε μια Πρόταση P, αρκεί να επαληθεύσουμε την άρνησή της $\neg$ P. Αυτό, εκτός από τις τεχνικές απόδειξης που έχουμε αναπτύξει, μπορεί να γίνει, ορισμένες φορές, με απλούστερο τρόπο.

Ας υποθέσουμε ότι έχουμε να αποδείξουμε ότι η Πρόταση

"Για κάθε $x \in S$ ισχύει η $\mathrm{p}(x)$"

δεν είναι αληθής, τότε πρέπει να δείξουμε ότι η άρνησή της

$\neg$(Για κάθε $x \in S$ ισχύει η $\mathrm{p}(x)$)

είναι αληθής. Στο προηγούμενο κεφάλαιο, στην παράγραφο "Ποσοδείκτες", είχαμε δει ότι η Πρόταση $\neg$(Για κάθε $x \in S$ ισχύει η $\mathrm{p}(x)$) είναι ισοδύναμη με την

"Υπάρχει $x \in S$, ώστε η $\mathrm{p}(x)$ να μην ισχύει".

Επομένως, αρκεί να βρούμε ένα $x \in S$, ώστε η $\mathrm{p}(x)$ να είναι ψευδής. Δηλαδή αρκεί ένα παράδειγμα για να καταρρίψουμε την εικασία

"Για κάθε $x \in S$ ισχύει η $\mathrm{p}(x)$".

Ένα τέτοιο παράδειγμα θα ονομάζεται **αντιπαράδειγμα**[21].

Όμοια, αν έχουμε να διαψεύσουμε την αλήθεια της συνεπαγωγής

$$\mathrm{p}(x) \Longrightarrow \mathrm{q}(x),\ x \in S,$$

αρκεί να βρούμε ένα αντιπαράδειγμα ενός $x \in S$, ώστε η $\mathrm{p}(x)$ να είναι αληθής, ενώ η $\mathrm{q}(x)$ να είναι ψευδής.

Δυϊκά, αν έχουμε να αποδείξουμε ότι η Πρόταση

[21] Δεν ξεχνάμε την εξής ρήση: *Some facts can be seen more clearly by example than by proof* Leonard Euler.

"Υπάρχει $x \in S$, ώστε να ισχύει η $\mathrm{p}(x)$"

δεν είναι αληθής, τότε πρέπει να δείξουμε ότι η άρνησή της

"¬(Υπάρχει $x \in S$, ώστε να ισχύει η $\mathrm{p}(x)$)"

είναι αληθής. Όμως η Πρόταση

"¬(Υπάρχει $x \in S$, ώστε να ισχύει η $\mathrm{p}(x)$)"

είναι ισοδύναμη με την Πρόταση

"Για κάθε $x \in S$ ισχύει η ¬$\mathrm{p}(x)$".

Εδώ δεν αρκεί να δώσουμε ένα παράδειγμα, πρέπει να εφαρμόσουμε μια από τις τεχνικές απόδειξης, που έχουμε παρουσιάσει, για να δώσουμε μια απόδειξη.

Παραδείγματα 3.2.17.

1. Δείξτε ότι η Πρόταση

   "Για κάθε ακέραιο αριθμό n, ο αριθμός $n^2 - n + 11$ είναι πρώτος."

   είναι ψευδής.

   Εδώ αρκεί να βρούμε έναν ακέραιο a, για τον οποίο ο αριθμός $a^2 - a + 11$ να είναι σύνθετος. Παρατηρούμε ότι για $a = 11$ έχουμε ότι $11^2 - 11 + 11 = 11^2$, άρα σύνθετος. Επομένως, αρκεί το αντιπαράδειγμα $a = 11$ για να αποδείξουμε ότι η δοθείσα Πρόταση είναι ψευδής.

2. Να αποδείξετε ή να καταρρίψετε την εικασία:

   "Υπάρχει πραγματικός αριθμός a με $a^4 < a < a^2$".

   Επειδή δεν γνωρίζουμε αν η Πρόταση είναι αληθής ή ψευδής, θα κάνουμε *διερεύνηση* του προβλήματος. Ο ζητούμενος πραγματικός αριθμός (αν υπάρχει) πρέπει να είναι θετικός (γιατί;).

   Αν υποθέσουμε ότι υπάρχει ένας τέτοιος πραγματικός αριθμός, τότε επειδή θα είναι θετικός και μη μηδενικός από την σχέση $a^4 < a < a^2$ έπεται ότι $a^3 < 1 < a$. Δηλαδή ο a πρέπει να είναι μεγαλύτερος του 1. Αλλά

   $$1 < a \implies a < a^2 \implies a^2 < a^3,$$

   δηλαδή τελικά $1 < a^3$. Άτοπο, αφού πρέπει $a^3 < 1 < a$.

   Επομένως, δεν υπάρχει πραγματικός αριθμός με την ιδιότητα $a^4 < a < a^2$.

   Η προηγούμενη αποδεικτική διαδικασία θα μπορούσε φορμαλιστικά να παρουσιαστεί ως εξής:

   Θεωρούμε την Πρόταση

   "Υπάρχει πραγματικός αριθμός a με $a^4 < a < a^2$".

   Η άρνησή της είναι η εξής:

   "Για κάθε πραγματικό αριθμό ¬$(a^4 < a < a^2)$".

   Αν αποδείξουμε ότι αυτή η Πρόταση είναι αληθής, τότε η αρχική Πρόταση είναι ψευδής.

   Εμείς προηγουμένως, με την μέθοδο της εις άτοπον απαγωγής, αποδείξαμε ότι αυτή η Πρόταση είναι αληθής.

3.2.8 Απόδειξη ισοδυναμιών

Έστω οι Προτάσεις P και Q. Στο προηγούμενο Κεφάλαιο και ειδικότερα στην Παράγραφο "Η (Λογική) ισοδυναμία Προτάσεων", είχαμε αναφερθεί στην ισοδυναμία

$$\mathrm{P} \Longleftrightarrow \mathrm{Q}.$$

Όταν θέλουμε να αποδείξουμε αυτήν την ισοδυναμία, στην πραγματικότητα πρέπει να αποδείξουμε την αλήθεια δύο (ανεξάρτητων) συνεπαγωγών

$$\text{της } \mathrm{P} \Longrightarrow \mathrm{Q} \text{ και της } \mathrm{P} \Longleftarrow \mathrm{Q}.$$

Η απόδειξη κάθε μιας από αυτές μπορεί να γίνει με κάποια από τις τεχνικές που έχουμε ήδη παρουσιάσει. Δεν είναι αναγκαίο να εφαρμόσουμε την ίδια τεχνική απόδειξης και για τις δύο κατευθύνσεις.

Εδώ θα πρέπει να επισημάνουμε το εξής: Υποθέτουμε ότι έχουμε να αποδείξουμε την ισοδυναμία των Προτάσεων.

$$\mathrm{P} \Longleftrightarrow \mathrm{Q}.$$

Αποδεικνύουμε, για παράδειγμα, πρώτα την συνεπαγωγή $\mathrm{P} \Longrightarrow \mathrm{Q}$. Για να αποδείξουμε την αντίστροφη συνεπαγωγή $\mathrm{Q} \Longrightarrow \mathrm{P}$, ενδέχεται να ενδείκνυται να την αποδείξουμε με την μέθοδο της αντιθετοαντιστροφής. Δηλαδή να αποδείξουμε την συνεπαγωγή $\neg\mathrm{P} \Longrightarrow \neg\mathrm{Q}$. Αυτό, ορισμένες φορές, ενδέχεται να μας παρασύρει και για την απόδειξη της συνεπαγωγής $\mathrm{Q} \Longrightarrow \mathrm{P}$ να αποδείξουμε την συνεπαγωγή $\neg\mathrm{Q} \Longrightarrow \neg\,\mathrm{P}$.

Στην πραγματικότητα έχουμε αποδείξει πάλι την συνεπαγωγή $\mathrm{P} \Longrightarrow \mathrm{Q}$!

Παραδείγματα 3.2.18.

1. Στα προηγούμενα έχουμε συναντήσει, πολλές φορές, τις εξής συνεπαγωγές:

   "Αν ο φυσικός αριθμός n είναι άρτιος, τότε ο n^2 είναι άρτιος"

   "Έστω ο φυσικός αριθμός n. Αν ο n^2 είναι άρτιος, τότε ο n είναι άρτιος"

   Εδώ απλώς επισημαίνουμε ότι πρόκειται για την ισοδυναμία

   Ο φυσικός αριθμός n είναι άρτιος $\Longleftrightarrow$ ο n^2 είναι άρτιος.

2. Ο ακέραιος αριθμός a διαιρείται με το 6, αν και μόνο αν διαιρείται με το 2 και με το 3.

   Υποθέτουμε ότι ο a διαιρείται με το 6. Επομένως, υπάρχει ακέραιος αριθμός b, ώστε $a = 6b = 2 \cdot 3 \cdot b$, δηλαδή ο a είναι πολλαπλάσιο του 2 **και** του 3. Άρα διαιρείται με το δύο και με το τρία.

   Αντίστροφα, υποθέτουμε ότι ο a διαιρείται με το 2 και με το 3. Επομένως, υπάρχει ακέραιος c, ώστε $a = 3 \cdot c$. Ισχυρισμός: Ο c είναι άρτιος. Αν ο c ήταν περιττός, τότε το γινόμενο $3 \cdot c$ θα ήταν περιττός αριθμός. Αυτό είναι άτοπο, διότι υποθέσαμε ότι ο $a = 3 \cdot c$ διαιρείται και με το 2, άρα είναι άρτιος. Άρα $c = 2 \cdot d$ και κατά συνέπεια $a = 3 \cdot 2 \cdot d = 6 \cdot d$.

3. Έστω a ακέραιος αριθμός. Ο αριθμός $a^2 + 4a + 5$ είναι άρτιος αν και μόνο αν ο a είναι περιττός.

   Υποθέτουμε ότι ο a^2+4a+5 είναι άρτιος, τότε ο αριθμός $a^2+4a = (a^2+4a+5)-5$ είναι περιττός (γιατί;). Αφού ο αριθμός $a^2 + 4a = a(a+4)$ είναι περιττός, τότε αναγκαστικά **και** οι δύο παράγοντες a και $a+4$ είναι περιττοί (γιατί;). Συνεπώς, ο αριθμός a είναι περιττός.

Αντίστροφα, υποθέτουμε ότι ο αριθμός a είναι περιττός, τότε ο αριθμός $a+4$ είναι περιττός, ως άθροισμα ενός περιττού και ενός αρτίου, άρα και το γινόμενο $a(a+4) = a^2+4a$ είναι περιττός αριθμός. Επομένως, ο αριθμός a^2+4a+5 είναι άρτιος, ως άθροισμα δύο περιττών, τέλος.

Πολλές φορές στα Μαθηματικά απαιτείται να αποδείξουμε την ισοδυναμία περισσοτέρων από δύο Προτάσεων. Στην περίπτωση αυτή, πρέπει να αποδείξουμε όλες τις απαιτούμενες ισοδυναμίες. Υπάρχει τρόπος να αποδείξουμε "οικονομικά" όλες τις ισοδυναμίες; Ας υποθέσουμε ότι θέλουμε να αποδείξουμε τις ισοδυναμίες

$$\mathrm{A} \iff \mathrm{B},\ \mathrm{B} \iff \mathrm{C},\ \mathrm{A} \iff \mathrm{C}.$$

Αυτό σημαίνει ότι, αν όλες οι ισοδυναμίες αποδειχθούν, τότε, είτε όλες οι Προτάσεις A, B, C είναι αληθείς είτε όλες είναι ψευδείς (γιατί;).

Ας υποθέσουμε ότι αποδεικνύουμε μόνο τις συνεπαγωγές

$$\mathrm{A} \implies \mathrm{B},\ \mathrm{B} \implies \mathrm{C},\ \mathrm{C} \implies \mathrm{A}.$$

Τότε πάλι, είτε όλες οι Προτάσεις A, B, C είναι αληθείς είτε όλες είναι ψευδείς.

Πράγματι υποθέτουμε ότι μια είναι αληθής και μια είναι ψευδής. Χωρίς βλάβη (γιατί χωρίς βλάβη;) μπορούμε να υποθέσουμε ότι η A είναι αληθής και η C είναι ψευδής. Από την αλήθεια της συνεπαγωγής $\mathrm{B} \implies \mathrm{C}$ έπεται ότι αναγκαστικά η B είναι ψευδής (γιατί;). Τώρα, από την αλήθεια της συνεπαγωγής $\mathrm{A} \implies \mathrm{B}$, έπεται ότι αναγκαστικά η A είναι ψευδής, άτοπο. Γιατί καταλήξαμε σε άτοπο; Διότι υποθέσαμε ότι υπάρχει μια αληθής και μια ψευδής Πρόταση.

Συνεπώς, έχουμε το εξής:

Συμπέρασμα. Για να αποδείξουμε την αλήθεια των ισοδυναμιών

$$\mathrm{A} \iff \mathrm{B},\ \mathrm{B} \iff \mathrm{C},\ \mathrm{A} \iff \mathrm{C}$$

πρέπει και αρκεί να αποδείξουμε την αλήθεια των συνεπαγωγών

$$\mathrm{A} \implies \mathrm{B},\ \mathrm{B} \implies \mathrm{C},\ \mathrm{C} \implies \mathrm{A}.$$

Θεώρημα 3.2.19. *Έστω $a, b \in \mathbb{Z}$. Δείξτε ότι ο a διαιρεί τον b, αν και μόνο ο a διαιρεί τον $a-b$, αν και μόνο αν ο a διαιρεί τον $ka+b$ για κάθε $k \in \mathbb{Z}$.*

Απόδειξη. Έστω οι Προτάσεις

A: "Ο a διαιρεί τον b."
B: "Ο a διαιρεί τον $a-b$."
C: "Ο a διαιρεί τον $ka+b$ για κάθε $k \in \mathbb{Z}$."

Υποθέτουμε ότι η Πρόταση A είναι αληθής. Άρα υπάρχει $r \in \mathbb{Z}$, ώστε $b = ra$, τότε $a-b = a-ra = (1-r)a$, δηλαδή ο a διαιρεί την διαφορά $a-b$. Συνεπώς, αποδείξαμε την συνεπαγωγή

$$\mathrm{A} \implies \mathrm{B}$$

Υποθέτουμε ότι ο a διαιρεί την διαφορά $a-b$, άρα $a-b = sa$ για κάποιο $s \in \mathbb{Z}$. Τότε, για κάθε $k \in \mathbb{Z}$, έχουμε ότι $ka+b = (k+1)a-(a-b) = (k+1)a-sa = (k+1-s)a$, δηλαδή ο a διαιρεί τον αριθμό $ka+b$. Συνεπώς, αποδείξαμε την συνεπαγωγή

$$\mathrm{B} \implies \mathrm{C}$$

Υποθέτουμε ότι ο a διαιρεί τον αριθμό $ka+b$ για κάθε $k \in \mathbb{Z}$, τότε για $k = 0$ έχουμε ότι ο a διαιρεί τον b. Συνεπώς, αποδείξαμε την συνεπαγωγή

$$\text{C} \implies \text{A}.$$

Άρα, βάσει των προηγουμένων έχουμε αποδείξει τις ισοδυναμίες

$$\begin{aligned}\text{“Ο } a \text{ διαιρεί τον } b\text{”} &\iff \text{“Ο } a \text{ διαιρεί τον } a-b\text{”} \\ &\iff \text{“Ο } a \text{ διαιρεί τον } ka+b \text{ για κάθε } k \in \mathbb{Z}.\text{”}\end{aligned}$$

ό.έ.δ.

3.2.9 Ασκήσεις

1. Αποφανθείτε ποιοι από τους ακόλουθους ισχυρισμούς είναι αληθείς και ποιοι ψευδείς. Δώστε μια απόδειξη στην περίπτωση, όπου ο ισχυρισμός είναι αληθής και ένα αντιπαράδειγμα στην περίπτωση, όπου ο ισχυρισμός είναι ψευδής. Συγκρίνατε με την “απόδειξη” που δίνεται στην άσκηση 3.2.3$_7$.

   (i) Για όλους τους πραγματικούς αριθμούς x και y ισχύει ότι

   $$\sqrt{xy} \leq \frac{x+y}{2}.$$

   (ii) Για όλους τους πραγματικούς αριθμούς x και y ισχύει ότι

   $$xy \leq \frac{x+y}{2}.$$

   (iii) Για όλους τους μη αρνητικούς πραγματικούς αριθμούς x και y ισχύει ότι

   $$\sqrt{xy} \leq \frac{x+y}{2}.$$

2. Αποφανθείτε ποιοι από τους ακόλουθους ισχυρισμούς είναι αληθείς και ποιοι ψευδείς. Δώστε μια απόδειξη στην περίπτωση, όπου ο ισχυρισμός είναι αληθής και ένα αντιπαράδειγμα στην περίπτωση, όπου ο ισχυρισμός είναι ψευδής.

   (i) Για τον ακέραιο αριθμό a υποθέτουμε ότι υπάρχει ένας ακέραιος αριθμός n, έτσι ώστε ο a να διαιρεί τον $8n+7$ και τον $4n+1$. Τότε ο a διαιρεί τον 5.

   (ii) Για τον ακέραιο αριθμό a υποθέτουμε ότι υπάρχει ένας ακέραιος αριθμός n, έτσι ώστε ο a να διαιρεί τον $9n+5$ και τον $6n+1$. Τότε ο a διαιρεί τον 7.

   (iii) Αν ο ακέραιος αριθμός n είναι περιττός, τότε το 8 διαιρεί τον αριθμό

   $$n^4 + 4n^2 + 11.$$

   (iv) Αν ο ακέραιος αριθμός n είναι περιττός, τότε το 8 διαιρεί τον αριθμό

   $$n^4 + n^2 + 2n.$$

3. Αποφανθείτε αν ο ακόλουθος ισχυρισμός είναι αληθής.

   Για κάθε θετικό ακέραιο αριθμό a υπάρχει θετικός ακέραιος b, έτσι ώστε

   $$\frac{1}{2b^2+b} < \frac{1}{ab^2}.$$

4. Δώστε ένα αντιπαράδειγμα για να δείξετε ότι ο ισχυρισμός

   "Για κάθε πραγματικό αριθμό x με $x(x-1) \neq 0$ ισχύει ότι $\frac{1}{x(1-x)} \geq 4$."

   είναι ψευδής.

   Να αποδείξετε τον ισχυρισμό

   "Για κάθε πραγματικό αριθμό x με $0 < x < 1$ ισχύει ότι $\frac{1}{x(1-x)} \geq 4$."

5. Έστω r ένας θετικός ακέραιος με δεκαδική παράσταση

   $$r = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10 + a_0,$$

   όπου $1 \leq a_k \leq 9,\ 0 \leq a_i \leq 9,\ i = 0, \ldots, k-1$. Δείξτε ότι ο r διαιρείται με το 9 αν και μόνο αν το άθροισμα $s = a_0 + a_1 + \cdots + a_k$ διαιρείται με το 9.

6. Έστω $x, y \in \mathbb{R}$. Δείξτε ότι $x^3 + x^2 y = y^2 + xy$, αν και μόνο αν $y = x^2$ ή $y = -x$.

7. Έστω $a, b \in \mathbb{Z}$. Δείξτε ότι ο $(a-3)b^2$ είναι περιττός, αν και μόνο αν ο a είναι άρτιος και ο b είναι περιττός.

8. Όλοι γνωρίζουμε το **Πυθαγόρειο Θεώρημα**:

   "Αν ABC είναι ένα ορθογώνιο τρίγωνο με μήκη πλευρών a, b, c, όπου c είναι η υποτείνουσα, τότε ισχύει ότι $c^2 = a^2 + b^2$".

   Μπορείτε να διατυπώσετε το αντίστροφό του και να αποδείξετε και τα δύο θεωρήματα;

9. Δείξτε ότι ένα παραλληλόγραμμο είναι ρόμβος,[22] αν και μόνο αν οι διαγώνιοί του είναι κάθετες μεταξύ τους.

10. Δείξτε ότι ένα τρίγωνο είναι ισοσκελές, αν και μόνο αν έχει δύο γωνίες ίσες μεταξύ τους, αν και μόνο αν έχει ένα ύψος το οποίο ισούται με την αντίστοιχη διάμεσο.

11. Δείξτε ότι ένα τρίγωνο είναι ισόπλευρο, αν και μόνο αν έχει και τις τρεις γωνίες του ίσες, αν και μόνο αν έχει και τα τρία ύψη του ίσα, αν και μόνο αν έχει και τις τρεις διχοτόμους του ίσες, αν και μόνο αν έχει και τις τρεις διαμέσους του ίσες, αν και μόνο αν τα ύψη του συμπίπτουν με τις διαμέσους του, αν και μονο αν τα ύψη του συμπίπτουν με τις διχοτόμους του, αν και μόνο αν....

[22] Ένα παραλληλόγραμμο ονομάζεται *ρόμβος*, αν όλες οι πλευρές του είναι ίσες μεταξύ τους,

Μπορείτε να συνεχίσετε διατυπώνοντας τουλάχιστον ακόμη μια ισοδύναμη Πρόταση; Κατόπιν αναδιατυπώσετε τον προηγούμενο ισχυρισμό με την μορφή Προτάσεων και συνεπαγωγών;

π.χ. A : "Το τρίγωνο ABC είναι ισόπλευρο."

B : "$\sphericalangle A = \sphericalangle B = \sphericalangle C$".

A $\Longrightarrow$ B

B $\Longrightarrow$ A

$\vdots$

3.2.10 Η Αρχή της Μαθηματικής Επαγωγής

Στην παράγραφο *"Απόδειξη εξαντλώντας όλες τις περιπτώσεις"* είχαμε δει ότι πολλές φορές για να αποδείξουμε έναν ισχυρισμό, μπορούμε να τον διαχωρίσουμε σε επιμέρους περιπτώσεις και να τον αποδείξουμε ξεχωριστά σε κάθε επιμέρους περίπτωση. Για να αποφανθούμε όμως για την αλήθεια του ισχυρισμού, **πρέπει** οι επιμέρους περιπτώσεις, συνολικά, να καλύπτουν όλες τις δυνατές περιπτώσεις.

Υπάρχουν όμως περιπτώσεις, όπου οι επιμέρους περιπτώσεις, που πρέπει να εξετασθούν, είναι άπειρες το πλήθος, οπότε είναι ανέφικτο να εξετασθεί κάθε μία ξεχωριστά.

Για παράδειγμα, στο Θεώρημα 3.2.6 αρκούσε να διαμερίσουμε το σύνολο των φυσικών αριθμών σε δύο κατηγορίες (άρτιους και περιττούς) και να αποδείξουμε το θεώρημα για κάθε κατηγορία ξεχωριστά.

Ας δούμε όμως τον εξής ισχυρισμό:

"Για κάθε φυσικό αριθμό n ο αριθμός $6^n - 1$ είναι πολλαπλάσιο του 5 (διαιρείται με το 5)."

Εδώ, αν προσπαθήσουμε να αποδείξουμε τον ισχυρισμό εξετάζοντας περιπτώσεις, π.χ. όταν ο n είναι άρτιος και όταν ο n είναι περιττός, θα δούμε ότι η προσπάθεια είναι ατελέσφορη (προσπαθήστε το!).

Αν προσπαθήσουμε να αποδείξουμε τον ισχυρισμό εξετάζοντας ξεχωριστά για κάθε n (κάθε φυσικός αριθμός n και ξεχωριστή περίπτωση), τότε θα δούμε ότι για $n = 1, 2, 3, \ldots$ πράγματι ο ισχυρισμός είναι αληθής. Αλλά για να αποφανθούμε ότι ο ισχυρισμός είναι αληθής, πρέπει να *δοκιμάσουμε* όλους τους φυσικούς αριθμούς, πράγμα αδύνατον. Επομένως, πρέπει να βρούμε έναν αποτελεσματικό τρόπο να *εξαντλούμε/δοκιμάζουμε* όλους τους φυσικούς αριθμούς.

Ας θέσουμε το πρόβλημα γενικότερα.

Έστω οι (ανοικτές) Προτάσεις $P(n)$, $n \in \mathbb{N}$. Θέλουμε να αποφανθούμε ότι για κάθε φυσικό αριθμό n η αντίστοιχη Πρόταση $P(n)$ είναι αληθής (στο προηγούμενο παράδειγμα $P(n)$: "Ο αριθμός $6^n - 1$ είναι πολλαπλάσιο του 5"). Δοκιμάζουμε τον αριθμό $n = 1$ και διαπιστώνουμε ότι η Πρόταση $P(1)$ είναι αληθής. Με το δεδομένο αυτό αποδεικνύουμε ότι η Πρόταση $P(2)$ είναι αληθής και συνεχίζουμε....

Γενικά κάνουμε την υπόθεση ότι για κάποιον φυσικό αριθμό k η Πρόταση $P(k)$ είναι αληθής, κατόπιν με κάποιον τρόπο (π.χ. ευθεία απόδειξη, απόδειξη με αντιθετοαντιστροφή κ.λ.π.) αποδεικνύουμε ότι η Πρόταση $P(k+1)$ είναι αληθής. Τότε αυτό σημαίνει (διαισθητικά) ότι η Πρόταση $P(n)$ είναι αληθής για κάθε φυσικό αριθμό $n \in \mathbb{N}$.

Τώρα είμαστε σε θέση να διατυπώσουμε το εξής:

Αρχή της Μαθηματικής Επαγωγής.

Θεώρημα 3.2.20. *Έστω οι Προτάσεις $P(n)$, $n \in \mathbb{N}$. Υποθέτουμε ότι:*

i. Η $P(1)$ είναι αληθής.

ii. Για κάθε $k \in \mathbb{N}$ αποδεικνύουμε την αλήθεια της συνεπαγωγής $P(k) \implies P(k+1)$ (δηλαδή, αν η Πρόταση $P(k)$ είναι αληθής, τότε και η Πρόταση $P(k+1)$ είναι αληθής).

Τότε η Πρόταση $P(n)$ είναι αληθής για όλα τα $n \in \mathbb{N}$.

Πριν δούμε μερικά παραδείγματα, ας κάνουμε ορισμένες παρατηρήσεις.

Παρατηρήσεις 3.2.21.

1. Μια επιπόλαιη ματιά στο προηγούμενο θεώρημα ίσως μας δώσει την εντύπωση ότι δεχόμαστε ως υπόθεση αυτό που θέλουμε να αποδείξουμε. Δεν ισχύει κάτι τέτοιο. Θέλουμε να αποδείξουμε ότι κάθε Πρόταση $P(n)$ είναι αληθής και αυτό επιτυγχάνεται με την απόδειξη ότι η Πρόταση $P(1)$ είναι αληθής και την απόδειξη της αλήθειας της συνεπαγωγής $P(k) \implies P(k+1)$ για κάθε $k \in \mathbb{N}$.

   Συγκεκριμένα, το δεύτερο σκέλος του θεωρήματος έχει την μορφή "Α $\implies$ Β". Για να αποδείξουμε την αλήθεια αυτής της συνεπαγωγής, δεν αποδεικνύουμε ότι η Πρόταση Α είναι αληθής, ούτε ότι η Πρόταση Β είναι αληθής, αλλά την αλήθεια της συνεπαγωγής "Α $\implies$ Β".

2. Ο έλεγχος ότι η Πρόταση $P(1)$ είναι αληθής αποτελεί το **πρώτο βήμα** της επαγωγής.

   Η υπόθεση ότι η Πρόταση $P(k)$ είναι αληθής αποτελεί την **επαγωγική υπόθεση**.

   Η απόδειξη της συνεπαγωγής "Αν η Πρόταση $P(k)$ είναι αληθής, τότε και η Πρόταση $P(k+1)$ είναι αληθής". Αποτελεί **το επαγωγικό βήμα**.

3. Όπως έχουμε προείπει, έως ότου αποδείξουμε ότι η Πρόταση $P(n)$ είναι αληθής για όλα τα $n \in \mathbb{N}$, ο ισχυρισμός αυτός αποτελεί μια εικασία. Ορισμένες φορές μπορεί να χρειαστεί να κάνουμε αρκετές δοκιμές και να διαπιστώσουμε ότι οι Προτάσεις $P(1)$, $P(2)$, ... είναι αληθείς, αυτό ενισχύει την εικασία, αλλά **δεν** την αποδεικνύει[23].

4. Στο προηγούμενο θεώρημα δεν δίνουμε απόδειξη. Στην πραγματικότητα αποτελεί αναδιατύπωση (μέρους) του Αξιώματος του Peano της θεμελίωσης των Φυσικών αριθμών (ιδέ Παράρτημα Α και συγκεκριμένα στην σελίδα 326).

5. Θα μπορούσε κάποιος να κάνει τον εξής παραλληλισμό: Θεωρούμε ένα ντόμινο όπου τα διαδοχικά πλακίδια είναι οι Προτάσεις

$$P(1),\ P(2),\ \ldots,\ P(k),\ P(k+1),\ \ldots.$$

   Η διαπίστωση ότι η Πρόταση $P(1)$ είναι αληθής σημαίνει ότι το πρώτο πλακίδιο ανατρέπεται, οπότε συμπαρασύρει και ανατρέπει το δεύτερο πλακίδιο (η Πρόταση $P(2)$ είναι αληθής), το δεύτερο πλακίδιο συμπαρασύρει και ανατρέπει το τρίτο πλακίδιο (η Πρόταση $P(3)$ είναι αληθής) και ούτω καθ' εξής.

[23] Εδώ αξίζει να αναφέρουμε την εξής "εικασία" του Euler. Η τιμή της συνάρτησης $f(n) = n^2+n+41$ είναι πρώτος αριθμός για κάθε $n \in \mathbb{N}$. Αν δοκιμάσουμε θα δούμε ότι για $n = 1, 2, 3, \ldots 39$ πάντα ο αντίστοιχος $f(n)$ είναι πρώτος αριθμός, άρα αφού έχουμε...κουραστεί... συμπεραίνουμε ότι πάντα ο $f(n)$ είναι πρώτος αριθμός! Αλλά $f(40) = 41^2$.

6. Δεν πρέπει να συγχέουμε το επαγωγικό βήμα (και γενικότερα την αρχή της Μαθηματικής Επαγωγής) με τον *Επαγωγικό συλλογισμό*, ο οποίος σημαίνει ότι μέσω μιας (νοητικής) διαδικασίας καταλήγουμε στο συμπέρασμα ότι κάτι (πιθανόν) είναι αληθές, βασιζόμενοι σε προηγούμενες παρατηρήσεις παρομοίων καταστάσεων. Μια μέθοδος εξαγωγής συμπερασμάτων σε πολλές Επιστήμες, αλλά **όχι** στα Μαθηματικά.

Θεώρημα 3.2.22. *Για κάθε $n \in \mathbb{N}$ ισχύει ότι $2^n \leq 2^{n+1} - 2^{n-1} - 1$.*

Απόδειξη. Για την απόδειξη θα χρησιμοποιήσουμε την Αρχή της Μαθηματικής Επαγωγής.

Έστω ότι $n = 1$, τότε η προς απόδειξη ανισότητα γίνεται

$$2^1 \leq 2^{1+1} - 2^{1-1} - 1$$

η οποία προφανώς ισχύει. (Το πρώτο βήμα της Επαγωγής).

Έστω $k \geq 1$. Υποθέτουμε ότι η ανισότητα

$$2^k \leq 2^{k+1} - 2^{k-1} - 1$$

είναι αληθής (Η Επαγωγική υπόθεση).

Θα δείξουμε ότι και η ανισότητα

$$2^{k+1} \leq 2^{(k+1)+1} - 2^{(k+1)-1} - 1$$

είναι αληθής (Το Επαγωγικό βήμα).

Ξεκινούμε με την υπόθεση $2^k \leq 2^{k+1} - 2^{k-1} - 1$. Πολλαπλασιάζουμε και τα δύο μέλη της με τον (θετικό) αριθμό 2 και έχουμε

$$2(2^k) \leq 2(2^{k+1} - 2^{k-1} - 1),$$

οπότε, κάνοντας πράξεις, έχουμε

$$2^{k+1} \leq 2^{(k+1)+1} - 2^{(k+1)-1} - 2.$$

Προσθέτοντας στο δεύτερο μέρος το 1 ενισχύουμε την ανισότητα και έχουμε

$$2^{k+1} \leq 2^{(k+1)+1} - 2^{(k+1)-1} - 1.$$

Άρα, από την Αρχή της Μαθηματικής Επαγωγής, συμπεραίνουμε:

Για κάθε $n \in \mathbb{N}$ ισχύει ότι $2^n \leq 2^{n+1} - 2^{n-1} - 1$. ό.έ.δ.

Θεώρημα 3.2.23. *Για κάθε $n \in \mathbb{N}$ ισχύει ότι ο αριθμός $8^n - 3^n$ είναι πολλαπλάσιο του 5.*

Απόδειξη. Έστω ότι $n = 1$, τότε έχουμε $8^1 - 3^1 = 5$, οποίο είναι πολλαπλάσιο του 5. (Το πρώτο βήμα της Επαγωγής).

Έστω $k \geq 1$. Υποθέτουμε ότι ο αριθμός $8^k - 3^k$ είναι πολλαπλάσιο του 5, δηλαδή $8^k - 3^k = 5m$, m ακέραιος (Η Επαγωγική υπόθεση).

Θα δείξουμε ότι και ο αριθμός $8^{k+1} - 3^{k+1}$ είναι πολλαπλάσιο του 5 (Το Επαγωγικό βήμα).

Έχουμε

$$\begin{aligned} 8^{k+1} - 3^{k+1} &= 8 \cdot 8^k - 3 \cdot 3^k \\ &= (5+3) \cdot 8^k - 3 \cdot 3^k \\ &= 5 \cdot 8^k + 3 \cdot 8^k - 3 \cdot 3^k \\ &= 5 \cdot 8^k + 3 \cdot (8^k - 3^k). \end{aligned}$$

Εδώ δεν ξεχνάμε την υπόθεση $8^k - 3^k = 5m$, οπότε η τελευταία ισότητα συνεχίζεται και έχουμε

$$\begin{aligned} 8^{k+1} - 3^{k+1} &= 8 \cdot 8^k - 3 \cdot 3^k \\ &= (5+3) \cdot 8^k - 3 \cdot 3^k \\ &= 5 \cdot 8^k + 3 \cdot 8^k - 3 \cdot 3^k \\ &= 5 \cdot 8^k + 3 \cdot (8^k - 3^k) \\ &= 5 \cdot 8^k + 3 \cdot (5m) \\ &= 5 \cdot (8^k + 3 \cdot m) \end{aligned}$$

με τον αριθμό $8^k + 3 \cdot m$ να είναι ακέραιος.

Άρα, από την Αρχή της Μαθηματικής Επαγωγής, συμπεραίνουμε:

Για κάθε $n \in \mathbb{N}$ ισχύει ότι ο αριθμός $8^n - 3^n$ είναι πολλαπλάσιο του 5. ό.έ.δ.

Στο προηγούμενο θεώρημα θα μπορούσε κάποιος να χρησιμοποιήσει την (γνωστή;) ταυτότητα: Για $a, b \in \mathbb{R}$ και $n \in \mathbb{N}$ ισχύει ότι

$$a^n - b^n = (a-b) \cdot (a^{n-1} + a^{n-2}b + \cdots ab^{n-2} + b^{n-1})$$

και να έχει μια ευθεία απόδειξη. Αλλά κατά πόσον είναι γνωστή αυτή η ταυτότητα και (το κυριότερο) κατά πόσο είμαστε σε θέση να την αποδείξουμε;

Θεώρημα 3.2.24. *Δίνεται η (αναδρομική) ακολουθία a_n) με $a_{n+1} = \frac{1}{5}(a_n^2 + 6)$ και $a_1 = \frac{5}{2}$. Η a_n είναι φθίνουσα, δηλαδή $a_{n+1} \leq a_n$ για κάθε $n \in \mathbb{N}$.*

Απόδειξη. Θεωρούμε την Πρόταση $P(n) : a_{n+1} \leq a_n$.

Παρατηρούμε ότι η Πρόταση $P(1)$ είναι αληθής.

Πράγματι

$$a_2 = \frac{1}{5}(a_1^2 + 6) = \frac{1}{5}((\frac{5}{2})^2 + 6) = \cdots = \frac{49}{20} < \frac{5}{2} = a_1.$$

(Το πρώτο βήμα της Επαγωγής).

Υποθέτουμε ότι $a_{k+1} \leq a_k$, για $k \geq 1$. (Η Επαγωγική υπόθεση).

Από την σχέση $a_{k+1} \leq a_k$ έπεται ότι $a_{k+1}^2 \leq a_k^2$ (γιατί;), οπότε συνεχίζουμε και έχουμε $a_{k+1}^2 + 6 \leq a_k^2 + 6$, δηλαδή

$$\frac{1}{5}(a_{k+1}^2 + 6) \leq \frac{1}{5}(a_k^2 + 6).$$

Άρα $a_{k+2} \leq a_{k+1}$ (Το Επαγωγικό βήμα).

Άρα, από την Αρχή της Μαθηματικής Επαγωγής, συμπεραίνουμε:

$$a_{n+1} \leq a_n \text{ για κάθε } n \in \mathbb{N}.$$ ό.έ.δ.

Στο πρώτο κεφάλαιο (σελ. 22) είχαμε αποδείξει την Πρόταση 1.1.44. Ας δούμε τώρα μια άλλη απόδειξη.

Θεώρημα 3.2.25. *Έστω X ένα σύνολο με n το πλήθος στοιχεία. Το πλήθος των υποσυνόλων του είναι ίσον με 2^n.*

Απόδειξη. Αν το σύνολο X είναι μονοσύνολο, δηλαδή $X = \{a\}$, τότε υπάρχουν δύο υποσύνολα, το κενό και όλο το σύνολο X. Άρα ο ισχυρισμός είναι αληθής για $n = 1$. (Το πρώτο βήμα της Επαγωγής).

Υποθέτουμε ότι ο ισχυρισμός είναι αληθής για όλα τα σύνολα με k το πλήθος στοιχεία. (Η επαγωγική υπόθεση).

Έστω $S = \{a_1, a_2, \dots, a_k, a_{k+1}\}$ ένα σύνολο με $k+1$ το πλήθος στοιχεία.

Το σύνολο $T = \{a_1, a_2, \dots, a_k\}$ έχει k το πλήθος στοιχεία, άρα από την Επαγωγική υπόθεση το πλήθος των υποσυνόλων του είναι ίσον με 2^k.

Προφανώς κάθε υποσύνολο του T είναι και υποσύνολο του S.

Για κάθε υποσύνολο A του συνόλου T το σύνολο $A \cup \{a_{k+1}\}$ αποτελεί ένα υποσύνολο του συνόλου S. Μάλιστα δε, για δύο διαφορετικά υποσύνολα A και B του T και τα σύνολα $A \cup \{a_{k+1}\}$ και $B \cup \{a_{k+1}\}$ είναι διαφορετικά υποσύνολα του συνόλου S. Επομένως, το σύνολο S έχει τουλάχιστον $2^k + 2^k = 2^{k+1}$ το πλήθος υποσύνολα.

Έστω A ένα υποσύνολο του συνόλου S. Τότε το στοιχείο a_{k+1}, είτε δεν ανήκει στο υποσύνολο A είτε ανήκει στο υποσύνολο A. Στην πρώτη περίπτωση έχουμε ότι το υποσύνολο A είναι υποσύνολο του συνόλου T. Στην δεύτερη περίπτωση έχουμε ότι το σύνολο $A \setminus \{a_{k+1}\}$ είναι υποσύνολο του συνόλου T. Άρα υπάρχουν ακριβώς $2^k + 2^k = 2^{k+1}$ το πλήθος υποσύνολα του συνόλου S. (Το επαγωγικό βήμα).

Η απόδειξη έχει ολοκληρωθεί. ό.έ.δ.

Παρατηρήσεις 3.2.26.

1. Ορισμένες φορές, όταν θέλουμε να αποδείξουμε την αλήθεια των Προτάσεων $P(n)$ για όλα τα $n \in \mathbb{N}$, μπορούμε να *κινηθούμε* ως εξής:

   (i) Ελέγχουμε ότι η Πρόταση $P(1)$ είναι αληθής.

   (ii) Για να χρησιμοποιήσουμε το επιχείρημα της εις άτοπον απαγωγής, υποθέτουμε ότι οι Προτάσεις $P(n)$ δεν είναι όλες αληθείς.

   (iii) Έστω $k > 1$ ο μικρότερος φυσικός αριθμός, ώστε η Πρόταση $P(k)$ να είναι ψευδής. Συνεπώς, η Πρόταση $P(k-1)$ είναι αληθής.

   (iv) Με την υπόθεση ότι η Πρόταση $P(k-1)$ είναι αληθής, αποδεικνύουμε την αλήθεια της συνεπαγωγής $P(k-1) \implies P(k)$. Άτοπο, πού έγκειται το άτοπο; Μα στο γεγονός ότι η μόνη περίπτωση, όπου η συνεπαγωγή $A \implies B$ είναι ψευδής, είναι όταν η Πρόταση Α είναι αληθής και η Πρόταση Β ψευδής.

   Δεν πρόκειται για κάποια νέα τεχνική απόδειξης, απλώς ο τρόπος παρουσίασης διαφέρει. Παρ' όλα ταύτα, ορισμένες φορές αναφέρεται ως η μέθοδος του *Ελαχίστου αντιπαραδείγματος*.

2. Η Αρχή της Μαθηματικής Επαγωγής χρησιμοποιείται (κατά κύριο λόγο) για να αποδείξουμε ότι οι Προτάσεις $P(n)$ είναι αληθείς για κάθε $n \geq 1$. Υπάρχουν όμως περιπτώσεις, όπως θα δούμε στην επομένη παράγραφο, όπου το πρώτο βήμα δεν ξεκινά από το 1, αλλά από κάποιον άλλο φυσικό αριθμό.

   Πολύ δε περισσότερο, ενδέχεται το πρώτο βήμα να ξεκινά από έναν τυχαίο ακέραιο αριθμό k. Στην περίπτωση αυτή αποδεικνύουμε ότι κάθε Πρόταση $P(n)$ είναι αληθής για $n \geq k$.

Εναλλακτικές μορφές της Αρχής της Μαθηματικής Επαγωγής.

Ορισμένες φορές, όταν θέλουμε να εφαρμόσουμε την Αρχή της Μαθηματικής Επαγωγής, ενδέχεται να έχουμε δυσκολία στην εφαρμογή του επαγωγικού βήματος, δηλαδή με την υπόθεση ότι η Πρόταση $P(k)$ είναι αληθής να αποδείξουμε ότι η Πρόταση $P(k+1)$ είναι αληθής. Στις περιπτώσεις αυτές, ίσως, να χρειάζεται να υποθέσουμε "κάτι" περισσότερο από την αλήθεια της Πρότασης $P(k)$ για να αποδείξουμε την αλήθεια της Πρότασης $P(k+1)$.

Για τις περιπτώσεις αυτές μπορούμε να χρησιμοποιήσουμε μια, ελαφρώς παραλλαγμένη Επαγωγή.

Η Αρχή της Ισχυρής Μαθηματικής Επαγωγής.[24]

Θεώρημα 3.2.27. *Έστω $r, k \in \mathbb{N}$ με $r \leq k$ και οι Προτάσεις $P(n)$ με $n \in \mathbb{N}$.*

Υποθέτουμε ότι η $P(r)$ είναι αληθής.

Υποθέτουμε ότι, αν οι Προτάσεις $P(j)$, για $r \leq j \leq k$ είναι αληθείς, τότε μπορούμε να αποδείξουμε ότι και η Πρόταση $P(k+1)$ είναι αληθής, δηλαδή η συνεπαγωγή

$$(P(r) \wedge P(r+1) \wedge \cdots \wedge P(k)) \Longrightarrow P(k+1)$$

είναι αληθής.

Τότε οι Προτάσεις $P(n)$ είναι αληθείς για κάθε $n \geq r$.

Πριν σχολιάσουμε το θεώρημα αυτό, ας δούμε ένα παράδειγμα.

Παράδειγμα 3.2.28. [25] Δείξτε ότι για κάθε $n \in \mathbb{N}$ ο αριθμός $n^4 - n^2$ είναι πολλαπλάσιο του 12.

Προφανώς για $n = 1$ έχουμε ότι πράγματι το $1^4 - 1^2 = 0$ είναι πολλαπλάσιο του 12 (το πρώτο βήμα).

Υποθέτουμε ότι για $k \in \mathbb{N}$ ο αριθμός $k^4 - k^2$ είναι πολλαπλάσιο του 12, δηλαδή $k^4 - k^2 = 12a$ (η επαγωγική υπόθεση).

Θα προσπαθήσουμε να αποδείξουμε ότι και ο αριθμός $(k+1)^4 - (k+1)^2$ είναι πολλαπλάσιο του 12 (το επαγωγικό βήμα). Έχουμε

$$\begin{aligned}
(k+1)^4 - (k+1)^2 &= (k+1)^2[(k+1)^2 - 1] \\
&= (k^2 + 2k + 1)(k^2 + 2k) \\
&= k^4 + 2k^3 + 2k^3 + 4k^2 + k^2 + 2k \\
&= k^4 + 4k^3 + 5k^2 + 2k \\
&= (k^4 - k^2) + 4k^3 + 6k^2 + 2k \\
&= 12a + (4k^3 + 6k^2 + 2k).
\end{aligned}$$

Για να προχωρήσουμε στην τελευταία ισότητα πρέπει να αποδείξουμε ότι η ποσότητα $4k^3 + 6k^2 + 2k$ είναι πολλαπλάσιο του 12, κάτι που δεν είναι και τόσο προφανές.

Στο παράδειγμα αυτό θα προσπαθήσουμε να εφαρμόσουμε το προηγούμενο θεώρημα. Θεωρούμε την Πρόταση

$P(n)$: "Ο αριθμός $n^4 - n^2$ είναι πολλαπλάσιο του 12".

[24] Ορισμένοι Μαθηματικοί την αναφέρουν ως *Πλήρη Μαθηματική Επαγωγή*. Προς διάκριση, στο εξής την Αρχή της Μαθηματικής Επαγωγής θα την αναφέρουμε απλώς ως Επαγωγή.

[25] Προφανώς το παράδειγμα αυτό μπορεί να αντιμετωπιστεί στοιχειωδώς (π.χ. διακρίνοντας περιπτώσεις αν ο n είναι άρτιος ή περιττός). Προσπαθήστε το! Εδώ όμως μας ενδιαφέρει η αντιμετώπισή του με Επαγωγή.

Είναι εύκολο να διαπιστώσουμε (κάντε το!) ότι η Πρόταση $P(j)$ είναι αληθής για κάθε $1 \leq j \leq 6$.

Έστω $k \geq 6$. Υποθέτουμε ότι η Πρόταση $P(j)$ είναι αληθής για όλα τα $1 \leq j \leq k$. Δηλαδή ο αριθμός $j^4 - j^2$ είναι πολλαπλάσιο του 12. Θα δείξουμε ότι η Πρόταση $P(k+1)$ είναι αληθής, δηλαδή ο αριθμός $(k+1)^4 - (k+1)^2$ είναι πολλαπλάσιο του 12.

Από την υπόθεσή μας έχουμε ότι η Πρόταση $P(k-5)$ είναι αληθής (εδώ $j = k-5$). Επομένως, ο αριθμός $(k-5)^4 - (k-5)^2$ είναι πολλαπλάσιο του 12, δηλαδή

$$(k-5)^4 - (k-5)^2 = 12a.$$

Θέτουμε $m = k-5$, οπότε έχουμε για τον αριθμό

$$\begin{aligned}
(k+1)^4 - (k+1)^2 &= (m+6)^4 - (m+6)^2 \\
&= (m+6)^2 \cdot [(m+6)^2 - 1] \\
&= (m^2 + 12m + 36) \cdot (m+7) \cdot (m+5) \\
&= (m^2 + 12m + 36) \cdot (m^2 + 12m + 35) \\
&= m^4 + 12m^3 + 35m^2 + (12m + 36) \cdot (m^2 + 12m + 35) \\
&= m^4 - m^2 + 12m^3 + 36m^2 + (12m + 36) \cdot (m^2 + 12m + 35)
\end{aligned}$$

(το $35m^2 = 36m^2 - m^2$)

$$= (m^4 - m^2) + 12m^3 + 36m^2 + (12m + 36) \cdot (m^2 + 12m + 35).$$

Στην τελευταία ισότητα όλοι οι όροι είναι πολλαπλάσια του 12 (δεν ξεχνάμε την (επαγωγική) υπόθεση ότι ο αριθμός $(k-5)^4 - (k-5)^2 = m^4 - m^2$ είναι πολλαπλάσιο του 12).

Συνεπώς, ο αριθμός $(k+1)^4 - (k+1)^2$ είναι πολλαπλάσιο του 12, άρα βάσει της Αρχής της Ισχυρής Μαθηματικής Επαγωγής έχουμε ότι η Πρόταση

$P(n)$: "Ο αριθμός $n^4 - n^2$ είναι πολλαπλάσιο του 12"

είναι αληθής για κάθε $n \in \mathbb{N}$.

Σχόλια 3.2.29.

1. Στο προηγούμενο θεώρημα δεν δίνουμε απόδειξη. Απαιτείται πρώτα να *κολυμπήσουμε στα βαθιά νερά* της αυστηρής θεμελίωσης των Φυσικών αριθμών. Θα δώσουμε μια απόδειξη στο Παράρτημα Α (ιδέ Πρόταση A.1.15 και την σχετική συζήτηση).

2. Όπως βλέπουμε, το πρώτο βήμα της επαγωγής δεν είναι αναγκαίο να ξεκινά από το 1, αλλά από κάποιον φυσικό αριθμό r.

3. Στην πράξη υπάρχουν παραλλαγές της Ισχυρής Μαθηματικής Επαγωγής. Μια σημαντική είναι η εξής: Αντί να υποθέσουμε ότι όλες οι Προτάσεις $P(j)$, για $r \leq j \leq k$ είναι αληθείς και να προσπαθήσουμε να αποδείξουμε ότι και η Πρόταση $P(k+1)$ είναι αληθής, αρκεί μόνο να υποθέσουμε ότι οι Προτάσεις $P(k-1)$ και $P(k)$ είναι αληθείς και να προσπαθήσουμε να αποδείξουμε ότι και η Πρόταση $P(k+1)$ είναι αληθής. Στην περίπτωση αυτή όμως πρέπει να ελέγξουμε ότι οι $P(1)$ **και** $P(2)$ είναι αληθείς (μπορείτε να δείτε το γιατί;).

4. Ο παραλληλισμός της Αρχής της Ισχυρής Μαθηματικής Επαγωγής με το ντόμινο είναι ο εξής: Αν κάθε φορά που η πτώση των k πρώτων πλακιδίων (οι Προτάσεις $P(1), P(2), \dots, P(k)$ είναι αληθείς) προκαλεί και την πτώση του $k+1$ πλακιδίου (και η Πρόταση $P(k+1)$ είναι αληθής), τότε όλα τα πλακίδια πρέπει να πέσουν (τότε όλες οι Προτάσεις είναι αληθείς).

Στην σελίδα 81 είχαμε σχολιάσει την απόδειξη του *νόμου του Morgan*. Συγκεκριμένα είχαμε αποδείξει:
Έστω E ένα σύνολο και A, B δύο υποσύνολά του, τότε ισχύει ότι:

i. $(A \cap B)^c = A^c \cup B^c$.

ii. $(A \cup B)^c = A^c \cap B^c$.

Θα γενικεύσουμε για περισσότερα των δύο υποσυνόλων.

Θεώρημα 3.2.30. *Έστω $A_1, A_2, \dots, A_n$ υποσύνολα ενός συνόλου E, $n \geq 2$. Τότε ισχύει ότι:*

i. $(A_1 \cap A_2 \cap \cdots \cap A_n)^c = A_1^c \cup A_2^c \cup \cdots \cup A_n^c$.

ii. $(A_1 \cup A_2 \cup \cdots \cup A_n)^c = A_1^c \cap A_2^c \cap \cdots \cap A_n^c$.

Απόδειξη. i) Αν έχουμε $n = 2$, τότε το αποτέλεσμα είναι η πρόταση που προαναφέραμε. Έστω $k \geq 2$. Υποθέτουμε ότι το αποτέλεσμα ισχύει αν έχουμε k ή λιγότερα το πλήθος υποσύνολα του συνόλου E. Έστω τώρα $A_1, A_2, \dots, A_{k-1}, A_k, A_{k+1}$ υποσύνολα του συνόλου E. Τότε έχουμε

$$\begin{aligned}(A_1 \cap A_2 \cap \cdots \cap A_{k-1} \cap A_k \cap A_{k+1})^c &= (A_1 \cap A_2 \cap \cdots \cap A_{k-1} \cap (A_k \cap A_{k+1}))^c \\ &= A_1^c \cup A_2^c \cup \cdots \cup A_{k-1}^c \cup (A_k \cap A_{k+1})^c \\ &= A_1^c \cup A_2^c \cup \cdots \cup A_{k-1}^c \cup A_k^c \cap A_{k+1}^c.\end{aligned}$$

Όπου, για να εφαρμόσουμε το επαγωγικό επιχείρημα, θεωρήσαμε, προς στιγμήν, το σύνολο $A_k \cap A_{k+1}$ ως ένα σύνολο. Άρα με ισχυρή επαγωγή έπεται το αποτέλεσμα για οσαδήποτε $n \geq 2$ το πλήθος υποσύνολα του E.
ii. Με το ίδιο επιχείρημα μπορείτε να αποδείξετε και αυτόν τον ισχυρισμό. ό.έ.δ.

Σημείωση. Το προηγούμενο θεώρημα είναι η Άσκηση $1.1.3_{18}$.

3.2.11 Ασκήσεις.

1. Δείξτε ότι οι κάτωθι ισότητες ισχύουν για όλους τους φυσικούς αριθμούς n.

   (α) $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$ [26].

   (β) $1 + 3 + 5 + \cdots + (2n-1) = n^2$.

   (γ) $1^2 + 2^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

[26] Την άσκηση αυτή την είχαμε συναντήσει νωρίτερα (ιδέ άσκηση $3.2.3_8$. Εκεί θέλαμε να την αποδείξουμε διακρίνοντας περιπτώσεις. Εδώ θέλουμε να την αποδείξουμε με Επαγωγή.

(δ) $1^3 + 2^3 + \cdots + n^3 = \dfrac{n^2(n+1)^2}{4}$.

(ε) $1^3 + 3^3 + 5^3 + \cdots + (2n-1)^3 = n^2(2n^2-1)$.

(στ) $1 \cdot 2 + 2 \cdot 3 + \cdots + n \cdot (n+1) = \dfrac{n(n+1)(n+2)}{3}$.

(ζ) $\dfrac{1}{1 \cdot 2} + \dfrac{1}{2 \cdot 3} + \cdots + \dfrac{1}{n \cdot (n+1)} = \dfrac{n}{n+1}$.

2. Δείξτε ότι, για κάθε μη αρνητικό ακέραιο, ο αριθμός $2^{3n+1}+5$ είναι πολλαπλάσιο του 7.

3. Δείξτε ότι, για κάθε $n \in \mathbb{N}$, ισχύει $2^{n-1} < n!$.

   Να βρεθούν όλα τα $n \in \mathbb{N}$ για τα οποία ισχύει $2^n < n!$.

4. Δείξτε ότι $\dfrac{1}{1} + \dfrac{1}{2} + \dfrac{1}{3} + \cdots + \dfrac{1}{2^n - 1} + \dfrac{1}{2^n} \geq 1 + \dfrac{n}{2}$, για κάθε $n \in \mathbb{N}$.

5. Δείξτε ότι $1 + 2n \leq 3^n$, για κάθε $n \in \mathbb{N}$.

6. Για ποιους φυσικούς αριθμούς n ισχύει η ανισότητα $n^2 - 9n + 19 > 0$;

7. Δείξτε ότι $(1 + \dfrac{1}{n})^n < n$ για όλα τα $n \in \mathbb{N}$ με $n \geq 3$.

8. Δείξτε ότι $7n < 2^n$ για όλα τα $n \in \mathbb{N}$ με $n \geq 6$.

9. Δείξτε ότι, αν $n \in \mathbb{N}$ και $n \geq 4$, τότε $3^n > n^3$.

10. Δείξτε ότι, αν $n \in \mathbb{N}$ και $n \geq 5$, τότε $4^n > n^4$.

    Συγκρίνοντας με την προηγούμενη άσκηση, μπορείτε να διατυπώσετε μια γενική *εικασία*;

11. Δείξτε ότι $\displaystyle\sum_{i=1}^{n} \frac{i}{2^i} = 2 - \frac{n+2}{2^n}$, για κάθε $n \in \mathbb{N}$.

12. Δείξτε ότι $\displaystyle\sum_{i=1}^{n} \frac{1}{\sqrt{i}} > \sqrt{n}$, για κάθε $n \in \mathbb{N}$ με $n \geq 2$.

13. Έστω $x_1 = 0$, $x_2 = 2$ και $x_n = \dfrac{1}{2}(x_{n-1} + x_{n-2})$. Δείξτε ότι $x_n = \dfrac{2^{n-1} + (-1)^n}{3 \cdot 2^{n-2}}$, για κάθε $n \geq 3$.

14. Έστω $f : \mathbb{N} \longrightarrow \mathbb{N} \cup \{0\}$ μια απεικόνιση. Υποθέτουμε ότι $f(1) = 0$ και, αν $n < m$, τότε $f(n) < f(m)$, για όλα τα $n, m \in \mathbb{N}$. Δείξτε ότι για κάθε $x \in \mathbb{N}$ υπάρχουν μοναδικοί $n, p \in \mathbb{N}$, έτσι ώστε $f(n) < x \leq f(n+1)$ και $x = f(n) + p$.

    Σημειώσεις: 1. Στην άσκηση αυτή, όπως και σε όλες τις ασκήσεις που έχουν σχέση με φυσικούς αριθμούς, μπορούμε να χρησιμοποιούμε τις γνωστές ιδιότητες των φυσικών αριθμών, που διαισθητικά ισχύουν. Όταν "έλθει η ώρα", όλες αυτές οι ιδιότητες θα αποδειχθούν αυστηρά.

    2. Έστω $b \in \mathbb{N}$, ορίζουμε την απεικόνιση $f : \mathbb{N} \longrightarrow \mathbb{N} \cup \{0\}$ με $f(n) = (n-1)b$, τότε μπορούμε να έχουμε μια εναλλακτική απόδειξη για τον *Ευκλείδειο Αλγόριθμο της Διαίρεσης* (ιδέ Θεώρημα 6.1.19).

15. Έστω $n \in \mathbb{N}$, με $n \geq 2$. δείξτε ότι, είτε ο n είναι πρώτος είτε υπάρχουν πεπερασμένο το πλήθος μοναδικοί πρώτοι $p_1, p_2, \ldots, p_k$, έτσι ώστε $n = p_1\, p_2 \cdots p_k$, όπου η σειρά των παραγόντων, στο ανωτέρω γινόμενο, δεν έχει σημασία.

    Παρατήρηση. Η άσκηση αυτή είναι το γνωστό *Θεμελιώδες Θεώρημα της Αριθμητικής* (ιδέ Θεώρημα 6.1.35). Αυτό δεν σημαίνει ότι δεν μπορούμε να δώσουμε μια απόδειξη από μόνοι μας. Επ' αυτού θα επανερχόμαστε συχνά–πυκνά.

16. Για κάθε $n \in \mathbb{N}$ και κάθε $x \in \mathbb{R}$ με $x > -1$, δείξτε ότι $(1+x)^n \geq 1 + nx$.

    (Η ανισότητα αυτή αναφέρεται ως **ανισότητα Bernoulli**).

17. Αν $n \in \mathbb{N}$ και $\vartheta \in \mathbb{R}$, Να δείξετε ότι $[\cos(\vartheta) + i\sin(\vartheta)]^n = \cos(n\vartheta) + i\sin(n\vartheta)$ (Το Θεώρημα του de Moivre).

    Υπόδειξη. Για να εφαρμόσετε το Επαγωγικό βήμα, πρέπει να γνωρίζετε τις τριγωνομετρικές ταυτότητες: $\cos(\varphi + \vartheta) = \cos(\varphi)\cos(\vartheta) - \sin(\varphi)\sin((\vartheta)$ και $\sin(\varphi + \vartheta) = \sin(\varphi)\cos(\vartheta) + \cos(\varphi)\sin((\vartheta)$.

    Μπορείτε να τις αποδείξετε;

18. Δείξτε το *Διωνυμικό Θεώρημα*: $(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^{n-r} y^r$, για όλα τα $n \in \mathbb{N}$ και όλους τους πραγματικούς αριθμούς x, y.

    Υπενθύμιση. $\binom{n}{r} = \dfrac{n!}{(n-r)!r!}$, για όλα τα $0 \leq r \leq n$.

19. Δείξτε ότι $\sum_{i=1}^{n} |\, x_i \,| \geq |\, \sum_{i=1}^{n} x_i \,|$, για $x_i \in \mathbb{R}$. (Η γενικευμένη τριγωνική ανισότητα).

    Υπόδειξη. Στην Άσκηση $3.2.3_{18}$ ζητείται να αποδειχθεί η ανισότητα για $n = 2$. Το βήμα αυτό είναι αναγκαίο για την γενική περίπτωση.

20. Υποθέτουμε ότι $x_1, x_2, \ldots x_n$ είναι μη αρνητικοί πραγματικοί αριθμοί. Δείξτε ότι

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 x_2 \cdots x_n}, \text{ για κάθε } n \geq 2.$$

    (Η γνωστή(;) ανισότητα: *Ο αριθμητικός μέσος είναι μεγαλύτερος ή ίσος του γεωμετρικού μέσου.*

21. Στο δεύτερο ερώτημα της πρώτης άσκησης ζητείται να αποδειχθεί η ισότητα

$$1 + 3 + 5 + \cdots + (2n-1) = n^2,$$

    για κάθε φυσικό αριθμό. Υπάρχει ο εξής ισχυρισμός:

$$1 + 3 + 5 + \cdots + (2n-1) = n^2 + 1.$$

    Μάλιστα δίνεται και η εξής "απόδειξη":

    Υποθέτουμε ότι η ισότητα ισχύει για τον φυσικό αριθμό n. Προσθέτουμε και στα δύο μέλη τον αριθμό $2n+1$ και έχουμε

$$1 + 3 + 5 + \cdots + (2n-1) + (2n+1) = n^2 + 1 + 2n + 1 = (n+1)^2 + 1.$$

Δηλαδή έχουμε το ίδιο αποτέλεσμα αν αντί του n έχουμε τον $n+1$, επομένως, με Επαγωγή, η ισότητα ισχύει για κάθε φυσικό αριθμό.

Τι συμβαίνει; Πού υπάρχει λάθος;

22. Αναφέρουμε ένα Επαγωγικό επιχείρημα ευρέως γνωστό(;).

"Όλα τα άλογα είναι ομοιόχρωμα".[27]

Θεωρούμε την Πρόταση $\mathrm{P}(n)$: Σε κάθε σύνολο, αποτελούμενο από n το πλήθος άλογα, όλα τα άλογα είναι ομοιόχρωμα. Θα δείξουμε ότι η Πρόταση είναι αληθής για όλα τα $n \in \mathbb{N}$.

Υποθέτουμε ότι $n = 1$. Τότε προφανώς σε κάθε σύνολο αποτελούμενο από ένα άλογο, όλα τα άλογα που ανήκουν στο σύνολο αυτό είναι ομοιόχρωμα. Συνεπώς, η $\mathrm{P}(1)$ είναι αληθής.

Υποθέτουμε τώρα ότι η Πρόταση είναι είναι αληθής για κάποιο n, δηλαδή σε κάθε σύνολο, αποτελούμενο από n το πλήθος άλογα, όλα τα άλογα είναι ομοιόχρωμα.

Θα δείξουμε ότι η συνεπαγωγή $\mathrm{P}(n) \Longrightarrow \mathrm{P}(n+1)$ είναι αληθής.

Λαμβάνουμε ένα σύνολο $\{h_1, h_2, \ldots, h_{n+1}\}$ αποτελούμενο από $n+1$ το πλήθος άλογα. Τα υποσύνολα $\{h_1, h_2, \ldots, h_n\}$ και $\{h_2, h_3, \ldots, h_{n+1}\}$ έχουν από n το πλήθος άλογα, επομένως, από την επαγωγική υπόθεση, σε κάθε ένα από αυτά όλα τα άλογα είναι ομοιόχρωμα. Δηλαδή τα άλογα h_n και h_{n+1} είναι ομοιόχρωμα. Άλλα όλα τα άλογα $h_1, h_2, \ldots, h_n$ είναι ομοιόχρωμα. Τελικά όλα τα $h_1, h_2, \ldots, h_n, h_{n+1}$ είναι ομοιόχρωμα. Άρα η Πρόταση $\mathrm{P}(n+1)$ είναι αληθής και απεδείχθη το Επαγωγικό βήμα. Επομένως, όλα τα άλογα είναι ομοιόχρωμα.

Τι συμβαίνει; Πού υπάρχει λάθος;

Εν κατακλείδι.

Από τα προηγηθέντα είναι σαφές ότι ένα από τα σημαντικότερα θέματα στην μελέτη των Μαθηματικών είναι η γραφή Μαθηματικών αποδείξεων.

Δεν ξεχνάμε ότι υπάρχει μεγάλη απόσταση μεταξύ του "Λύνω ένα πρόβλημα" και του "Παρουσιάζω την λύση ενός προβλήματος".

Χωρίς σχολαστικότητα και ακριβολογία τα Μαθηματικά...δεν είναι Μαθηματικά.

Η γραφή Μαθηματικών αποδείξεων είναι μια ικανότητα, την οποία αποκτούμε σιγά–σιγά κατόπιν μεγάλης προσπάθειας.

Στα επόμενα συνοψίζουμε ορισμένες "αρχές" που πρέπει να ακολουθούμε κατά την γραφή μιας απόδειξης.

- Γνωρίζουμε το "ακροατήριο", στο οποίο απευθύνεται η απόδειξη.

  Κάθε συγγραφέας πρέπει να λαμβάνει υπόψιν το αναγνωστικό κοινό, στο οποίο απευθύνεται. Στα Μαθηματικά αυτό είναι επιτακτικότερο. Διαφορετικά παρουσιάζεται μια απόδειξη ενός Θεωρήματος, η οποία απευθύνεται σε πρωτοετείς φοιτητές των Μαθηματικών και διαφορετικά παρουσιάζεται μια απόδειξη του ιδίου Θεωρήματος, η οποία απευθύνεται σε ένα Μαθηματικώς ώριμο κοινό.

  Σε μια απόδειξη εμφανίζονται εκφράσεις του τύπου "ως γνωστόν ισχύει...", "είναι προφανές ότι...", "εύκολα βλέπουμε ότι...". Αυτό ορισμένες φορές γίνεται

[27] Αν δεν θέλετε με άλογα,...επιχειρήστε με τον ισχυρισμό: "Όλοι οι άνθρωποι έχουν τον ίδιο αριθμό τριχών".

σκόπιμα[28] για να είναι ο αναγνώστης σε εγρήγορση. Εδώ πρέπει να είμαστε προσεκτικοί. Ο "αποδέκτης" είναι σε θέση να αντιληφθεί από μόνος του το προφανές;

- Συνήθως, όταν δίνεται ένα πρόβλημα προς λύση, η διατύπωσή του ξεκινά με μια φράση του τύπου "Δείξτε ότι....". Ενδείκνυται να αναδιατυπώνουμε το πρόβλημα σε μορφή Θεωρήματος, όπου να είναι σαφές ποια είναι η υπόθεση και ποιο το συμπέρασμα. Κατόπιν κάνουμε σαφές πού τελειώνει η "εκφώνηση" του προβλήματος και πού ξεκινά η απόδειξη.

- Οι προτάσεις πρέπει να ξεκινούν με λέξεις και όχι με σύμβολα και σχέσεις. Η τήρηση των γραμματικών και συντακτικών κανόνων, όχι απλώς ενδείκνυται, αλλά είναι απαραίτητη στην γραφή ενός Μαθηματικού κειμένου. Επίσης, είναι απαραίτητη η σωστή χρήση των σημείων στίξεως.

  Ενδείκνυται στην έκφραση να χρησιμοποιούμε το πρώτο πληθυντικό πρόσωπο και την ενεργητική φωνή (*...Θα εφαρμόσουμε το εξής επιχείρημα...*). Η δημιουργία ενός κλίματος, όπου ο συγγραφέας και ο αναγνώστης συμμετέχουν από κοινού στην Μαθηματική διαδικασία, μόνο θετικές επιπτώσεις θα έχει στην παρότρυνση του αναγνώστη να συνεχίσει να μελετά τα Μαθηματικά.

- Η παράθεση επεξηγηματικών λέξεων και φράσεων μεταξύ συμβόλων και σχέσεων είναι απαραίτητη. Πολλές φορές εντυπωσιαζόμαστε (ή το χειρότερο θέλουμε να εντυπωσιάσουμε) με την παράθεση συμβόλων και σχέσεων και την απουσία λέξεων και φράσεων. Αυτό προκαλεί σύγχυση και οδηγεί σε παρανοήσεις.

  Διαφορετικά γίνεται μια προφορική παρουσίαση μιας απόδειξης στον πίνακα, όπου ο "παρουσιαστής" συμπληρώνει τα γραφόμενα με επεξηγηματικές λέξεις και φράσεις και διαφορετικά η γραπτή παρουσίαση, όπου ο συγγραφέας "απουσιάζει", όταν διαβάζεται η απόδειξη από έναν τρίτο.

  Φανταστείτε έναν, ο οποίος εισέρχεται σε μια αίθουσα διδασκαλίας και αντικρίζει έναν πίνακα όπου παρουσιάζεται μια καλογραμμένη απόδειξη. Θα μπορέσει να εικάσει τις λέξεις και φράσεις που ειπώθηκαν και δεν είναι γραμμένες στον πίνακα;

- Η λελογισμένη χρήση συμβόλων είναι απαραίτητη. Μάλιστα δε, όπου είναι δυνατόν, ενδείκνυται αντί συμβόλων να χρησιμοποιούμε λέξεις και φράσεις. Όπως θα έχετε παρατηρήσει (το έχουμε άλλωστε επισημάνει), αποφεύγουμε την χρήση των συμβόλων $\forall$, $\exists$, $\Longrightarrow$ και αντ' αυτών χρησιμοποιούμε τις φράσεις "για όλα", "υπάρχει", "συνεπάγεται/έπεται".

  Για παράδειγμα: Τι σημαίνει η παράθεση $(\forall\, x \in \mathbb{R})\,(\exists\, y \in R)\,(x + y = 0)$;

  Δεν θα ήταν προτιμότερο να γράψουμε: Για κάθε πραγματικό αριθμό x υπάρχει πραγματικός αριθμός y, έτσι ώστε $x + y = 0$;

  Εδώ θα πρέπει να επισημάνουμε στην σωστή χρήση των ισοδυνάμων εκφράσεων της Πρότασης "Αν Α τότε Β" (ιδέ την αντίστοιχη παράγραφο στο προηγούμενο κεφάλαιο, σελ. 50).

[28] Δεν πρέπει να αποκλείουμε το ενδεχόμενο, πίσω από τέτοιες εκφράσεις, να "κρύπτεται" η ανικανότητα και άγνοια του συγγραφέα.

- Ορισμένες φορές ενδείκνυται να προειδοποιούμε τον αναγνώστη για την μέθοδο απόδειξης, που θα ακολουθήσουμε, π.χ. "Θα εφαρμόσουμε την εις άτοπον απαγωγή....". "Εδώ χρησιμοποιούμε την μέθοδο της αντιθετοαντιστροφής...", "Θα εφαρμόσουμε την Αρχή της Μαθηματικής Επαγωγής...", με αυτόν τον τρόπο διευκολύνουμε την παρακολούθηση της "ροής" της απόδειξης.

- Γράφουμε ένα σχεδιάγραμμα της απόδειξης και κατόπιν το διαβάζουμε και επ' αυτού επιχειρούμε να γράψουμε την απόδειξη στην τελική της μορφή. Στην προσπάθεια αυτή θα εντοπίσουμε λάθη και ασάφειες, πολλές φορές θα αναγκαστούμε να αναθεωρήσουμε την αρχική γραφή και να ξεκινήσουμε από την αρχή. Το "τελικό προϊόν" πρέπει να είναι σαφές, διαυγές και πλήρως τεκμηριωμένο.

  Δεν ξεχνάμε ότι πίσω από μια κομψή, *καλογυαλισμένη* και *καλοσερβιρισμένη* απόδειξη κρύβεται μεγάλος κόπος με σχεδιαγράμματα, αποτυχημένες προσπάθειες....και πολλά μουτζουρωμένα χαρτιά..

  Ένας αποτελεσματικός τρόπος για να εκτιμήσουμε την "απήχηση" που θα έχει μια απόδειξη, που γράψαμε, είναι να την αφήσουμε για ένα χρονικό διάστημα (μέρες, μήνες...) και να ασχοληθούμε πάλι ως αναγνώστες. Πολλές φορές θα εκπλαγούμε με το τι γράψαμε και με το τι θα έπρεπε να γράψουμε.

...και δύο *αποφθέγματα:*

> "*Learn as much by writing as by reading.*" Lord Acton, Lectures on Modern History, 1906

> "*The importance of proofs goes well beyond a university degree. It is eventually about using reason in everyday life. This could contribute to solving major and global problems.*"[29]

Βιβλιογραφία

[1] Thomas Bieske. *An Introduction to Writing Mathematical Proofs: Shifting Gears from Calculus to Upper-Level Mathematics Classe*. Independently published, 2020. ISBN: 979-85-6123-065-3.

[2] E.D. Bloch. *Proofs and Fundamentals: A first course in Abstract Mathematics*. Second Edition. Springer, 2011. ISBN: 978-14-4197-126-5.

[3] J. Cummings. *Proofs: A Long-Form Mathematics Textbook*. Independently published, 2021. ISBN: 979-85-9526-597-3.

[4] Joel David Hamkins. *Proof and the Art of Mathematics*. MIT Press, 2020. ISBN: 978-02-6253-979-1.

[5] K. Houston. *How to Think Like a Mathematician*. Cambridge University Press, 2009. ISBN: 978-05-1150-645-1.

[6] Steven G. Krantz. *The Elements of Advanced Mathematics*. Fourth Edition. Textbooks in mathematics. CRC Press Taylor and Francis Group, 2018. ISBN: 978-11-3850-631-2.

[7] M. Liebeck. *A Concise Introduction to Pure Mathematics*. Third Edition. Chapman Hall CRC Press, 2011. ISBN: 978-14-3983-598-2.

[29] *Proofs and Mathematical Reasoning* by Agata Stefanowicz, University of Birbingham 2014, σελ. 32

[8] Bernd S. W. Schröder. *Fundamentals of Mathematics: An Introduction to Proofs, Logic, Sets and Numbers*. First Edition Wiley, 2010. ISBN: 978-04-7055-138-7.

[9] C. Schumacher. *Chapter Zero: Fundamental Notions of Abstract Mathematics*. Second Edition. Addison-Wesley, 2001. ISBN: 02-0143-724-4.

[10] A. Stefanowitz. *Proofs and Mathematical Reasoning*. University of Birmingham, 2014.

[11] I. Stewart & D. Tall. *The Foundations of Mathematics*. Second Edition. Oxford University Press, 2015.

[12] T. Sundstrom. *Mathematical Reasoning, Writing and Proof*. Version 2.1, May 26, 2020.

ΚΕΦΑΛΑΙΟ 4

ΣΧΕΣΕΙΣ - ΑΠΕΙΚΟΝΙΣΕΙΣ

4.1 Σχέσεις μεταξύ συνόλων

4.1.1 Ορισμοί- Βασικές έννοιες

Ας ξεκινήσουμε με ένα παράδειγμα: Υποθέτουμε ότι έχουμε ένα σύνολο ανθρώπων, έστω

$$A = \{a_1, a_2, \ldots, a_n\}$$

και ένα σύνολο από χώρες, έστω

$$\mathrm{B} = \{b_1, b_2, \ldots, b_m\}$$

και θεωρούμε ότι ένας άνθρωπος (ένα στοιχείο του συνόλου A) *σχετίζεται* με μια χώρα (ένα στοιχείο του συνόλου B), αν κατάγεται από την χώρα αυτή. Δηλαδή θα μπορούσαμε να πούμε: *Ο* a_i *κατάγεται από την χώρα* b_j. Οπότε, θα μπορούσαμε να σχηματίσουμε το εξής σύνολο:

$$\mathrm{R} = \{(a_i, b_j) \in A \times B \mid \text{ο } a_i \text{ κατάγεται από την χώρα } b_j\}.$$

Το σύνολο R είναι ένα υποσύνολο του καρτεσιανού γινομένου $A \times B$ και περιλαμβάνει μόνο τα διατεταγμένα ζεύγη (a, b), των οποίων το πρώτο μέλος a (ο άνθρωπος) σχετίζεται με το δεύτερο μέλος b (την χώρα) ως προς την ιδιότητα:

"Ο a κατάγεται από την χώρα b".

Πριν προχωρήσουμε, ας δούμε ένα άλλο παράδειγμα: Υποθέτουμε ότι έχουμε το σύνολο των ακεραίων αριθμών $\mathbb{Z}$. Θεωρούμε ότι δύο φυσικοί αριθμοί $a, b \in \mathbb{Z}$ *σχετίζονται* μεταξύ τους αν ο a διαιρεί τον b. Οπότε, θα μπορούσαμε να σχηματίσουμε το εξής σύνολο:

$$\mathrm{F} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid \text{ ο } a \text{ διαιρεί τον } b\}.$$

Το σύνολο F είναι ένα υποσύνολο του καρτεσιανού γινομένου $\mathbb{Z}\times\mathbb{Z}$ και περιλαμβάνει μόνο τα διατεταγμένα ζεύγη (a, b), των οποίων το πρώτο μέλος a σχετίζεται με το δεύτερο μέλος b ως προς την ιδιότητα: "Ο a διαιρεί τον b" [1].

Γενικεύοντας θα μπορούσαμε να δώσουμε τον εξής ορισμό:

Ορισμός 4.1.1. Έστω δύο σύνολα A και B. Μια σχέση μεταξύ στοιχείων του σύνολου A και στοιχείων του σύνολου B είναι ένα υποσύνολο, έστω R, του καρτεσιανού γινομένου $A \times B$ [2].

Παρατηρήσεις 4.1.2.

1. Πολλές φορές αντί της έκφρασης "*μια σχέση μεταξύ στοιχείων του σύνολου A και στοιχείων του σύνολου B*", χρησιμοποιούμε την έκφραση "*μια σχέση από το σύνολο A στο σύνολο B*".

2. Τα σύνολα A και B δεν είναι κατ' ανάγκην διαφορετικά. Στην περίπτωση όπου έχουμε ένα σύνολο A και ένα υποσύνολο R του καρτεσιανού γινομένου $A \times \mathrm{A}$, τότε λέμε ότι έχουμε μια σχέση (εντός) του συνόλου A ή ότι το σύνολο A είναι εφοδιασμένο με την σχέση R και θα συμβολίζουμε (A, R)[3].

   Εκτός από τα κεφαλαία γράμματα του Λατινικού αλφαβήτου για τον συμβολισμό μιας σχέσης χρησιμοποιούμε και διάφορα άλλα σύμβολα, π.χ.

   $$\subseteq, \leq, \prec, \sim, \equiv, \ldots .$$

3. Προφανώς μπορούμε να ορίσουμε τόσες σχέσεις από ένα σύνολο A σε ένα σύνολο B, όσα είναι και τα δυνατά υποσύνολα του καρτεσιανού γινομένου $A \times B$.

   Ένα από τα υποσύνολα του $A \times B$ είναι και το κενό σύνολο. Στην περίπτωση αυτή θα ομιλούμε για την κενή σχέση.

   Στην περίπτωση, όπου ως υποσύνολο του $A \times B$ λάβουμε όλο το σύνολο $A \times B$, θα ομιλούμε για την καθολική σχέση.

   Προφανώς, αν (τουλάχιστον) ένα από τα σύνολα A και B είναι το κενό σύνολο, τότε έχουμε μόνο την κενή σχέση. Για τον λόγο αυτόν, σιωπηλά, θα θεωρούμε ότι τα σύνολα A και B είναι μη κενά.

4. Υποθέτουμε ότι τα στοιχεία $a \in A$ και $b \in B$ σχετίζονται μέσω της σχέσης $\mathrm{R} \subseteq A \times B$, δηλαδή $(a, b) \in \mathrm{R}$. Τότε έχει επικρατήσει να συμβολίζουμε $a\,\mathrm{R}\,b$ (αντί του $(a, b) \in \mathrm{R}$).

5. Έστω μια σχέση $\mathrm{R} \subseteq A \times B$ από το σύνολο A στο σύνολο B. Τότε μπορούμε να ορίσουμε την **αντίστροφη** σχέση $\mathrm{R}^{-1} \subseteq B \times A$ από το σύνολο B στο σύνολο A ως εξής: $b\,\mathrm{R}^{-1}\,a$ αν, $a\,\mathrm{R}\,b$.

   Για παράδειγμα: Είχαμε ορίσει την σχέση

   $$\mathrm{F} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid \text{ ο } a \text{ διαιρεί τον } b\}.$$

[1] Όταν λέμε ότι ο ακέραιος a διαιρεί τον ακέραιο b, εννοούμε ότι υπάρχει ένας ακέραιος c έτσι ώστε $b = a \cdot c$. Επίσης, έχει επικρατήσει ο συμβολισμός (και αυτόν θα χρησιμοποιούμε εφεξής) αντί του "Ο a διαιρεί τον b" να γράφουμε $a \mid b$.

[2] Πολλοί χρησιμοποιούν την έκφραση μια αντιστοίχιση μεταξύ στοιχείων του συνόλου A και στοιχείων του σύνολου B.

[3] Πολλές φορές, επειδή έχουμε δύο στοιχεία του συνόλου A να σχετίζονται μεταξύ τους, λέμε ότι έχουμε μια *διμελή* σχέση στο σύνολο A.

Η αντίστροφη σχέση είναι η

$$\mathrm{F}^{-1} = \{(b, a) \in \mathbb{Z} \times \mathbb{Z} \mid \text{ο } b \text{ διαιρείται από τον } a\}.$$

Προφανώς (γιατί;), η αντίστροφη σχέση R^{-1} μιας σχέσης R είναι μοναδική και η αντίστροφη σχέση της (αντίστροφης) σχέσης R^{-1} είναι η αρχική σχέση R

$$(R^{-1})^{-1} = R.$$

6. Έστω ότι έχουμε μια σχέση $\mathrm{R} \subseteq A \times B$ από το σύνολο A στο σύνολο B. Τότε μπορούμε να ορίσουμε την **συμπληρωματική** σχέση $\mathrm{R}^c \subseteq A \times B$ από το σύνολο A στο σύνολο B ως εξής:

$$(a, b) \in \mathrm{R}^c \text{ αν } (a, b) \notin \mathrm{R}.$$

Δηλαδή η συμπληρωματική σχέση R^c δεν είναι τίποτε άλλο από το συνολοθεωρητικό συμπλήρωμα του υποσυνόλου $\mathrm{R} \subseteq A \times B$.

Παράδειγμα 4.1.3. Έστω A ένα σύνολο. Μια προφανής και πολύ σημαντική σχέση, που μπορούμε να ορίσουμε, είναι η εξής:

$$\mathrm{R} = \{(a, a) \in A \times A \mid a \in A\}.$$

Η σχέση αυτή είναι η γνωστή σχέση **ισότητας**, την οποία ως γνωστόν την συμβολίζουμε $a = a$. Προφανώς η αντίστροφη σχέση $=^{-1}$ ταυτίζεται με την ίδια την σχέση της ισότητας και η συμπληρωματική σχέση είναι η σχέση ανισότητας $\neq$.

Έστω ότι έχουμε τρία σύνολα A, B, C και τις σχέσεις $\mathrm{R} \subseteq A \times B$ και $\mathrm{F} \subseteq B \times C$. Τότε μπορούμε να ορίσουμε μια νέα σχέση μεταξύ των συνόλων A και C ως εξής:

$$\mathrm{G} = \{(a, c), \text{ αν υπάρχει } b \in B, \text{ έτσι ώστε } (a, b) \in \mathrm{R} \text{ και } (b, c) \in \mathrm{F}\} \subseteq A \times C.$$

Η σχέση G θα ονομάζεται **σύνθεση** των σχέσεων R και F και θα συμβολίζεται $\mathrm{F} \circ \mathrm{R}$. Δηλαδή έχουμε ότι

$$a \,\mathrm{R}\, b \text{ και } b \,\mathrm{F}\, c \quad \Longrightarrow \quad a \,(\mathrm{F} \circ \mathrm{R})\, c.$$

Παραδείγματα 4.1.4.

1. Έστω A το σύνολο όλων των κατοίκων της Υφηλίου. Στο σύνολο A ορίζουμε μια σχέση $\mathrm{R} \subseteq A \times A$ ως εξής: $a \,\mathrm{R}\, b$, αν ο κάτοικος a έχει ανταλλάξει (τουλάχιστον μία φορά) χειραψία με τον κάτοικο b. Επίσης, στο σύνολο A ορίζουμε μια άλλη σχέση $\mathrm{F} \subseteq A \times A$ ως εξής: $b \,\mathrm{F}\, c$, αν ο κάτοικος b είναι γονέας του κατοίκου c. Τότε η σύνθεση $\mathrm{F} \circ \mathrm{R}$ αποτελείται από όλα τα ζεύγη (a, c) κατοίκων με την ιδιότητα: Ο κάτοικος a έχει ανταλλάξει χειραψία με τον γονέα, έστω b, του κατοίκου c.

2. Στο σύνολο $\mathbb{Z}$ των ακεραίων αριθμών ορίζουμε μια σχέση $\mathrm{R} \subseteq \mathbb{Z} \times \mathbb{Z}$ ως εξής: $a \,\mathrm{R}\, b$, αν ο ακέραιος b είναι το τετράγωνο του αριθμού a ($b = a^2$). Επίσης, στο σύνολο $\mathbb{Z}$ ορίζουμε μια άλλη σχέση $\mathrm{F} \subseteq \mathbb{Z} \times \mathbb{Z}$ ως εξής: $b \,\mathrm{F}\, c$, αν ο b είναι πρώτος αριθμός και ο c είναι ο επόμενος του b. Δηλαδή, b πρώτος και $c = b+1$. Τότε η σύνθεση $\mathrm{R} \circ \mathrm{F}$ αποτελείται από όλα τα ζεύγη (a, c) ακεραίων αριθμών με την ιδιότητα: Υπάρχει ακέραιος αριθμός b με $b = a^2$, ο b είναι πρώτος αριθμός και $c = b + 1$. Όπως παρατηρούμε, δεν υπάρχει ακέραιος αριθμός b με την παραπάνω ιδιότητα, δηλαδή να είναι ταυτόχρονα τετράγωνο ακεραίου και πρώτος. Δηλαδή, δεν υπάρχουν ακέραιοι αριθμοί, οι οποίοι να σχετίζονται μέσω της σχέσης $\mathrm{F} \circ \mathrm{R}$. Συνεπώς, η σχέση $\mathrm{F} \circ \mathrm{R}$ είναι η κενή σχέση.

3. Έστω (A, R) εφοδιασμένο με την σχέση R. Τότε ορίζεται η σύνθεση $\mathrm{R} \circ \mathrm{R}$ της R με τον εαυτό της, την οποία συμβολίζουμε $\mathrm{R}^2 = \mathrm{R} \circ \mathrm{R}$. Γενικά για κάθε φυσικό αριθμό n ορίζεται, αναδρομικά, $\mathrm{R}^n = \mathrm{R}^{n-1} \circ \mathrm{R}$.

   Στο πρώτο παράδειγμα, στο σύνολο A των κατοίκων της Υφηλίου είχαμε ορίσει την σχέση $b \,\mathrm{F}\, c$, αν ο κάτοικος b είναι γονέας του κατοίκου c. Οπότε, αν πάρουμε το τετράγωνο F^2, τότε $a \,\mathrm{F}^2\, c$ αν ο a είναι ο παππούς του c.

Έστω ότι έχουμε δύο σχέσεις R και F μεταξύ των συνόλων A και B. Τότε ορίζεται η **τομή** $\mathrm{R} \cap \mathrm{F}$ των δύο σχέσεων. Όμοια ορίζεται η **ένωση** $\mathrm{R} \cup \mathrm{F}$ των δύο σχέσεων, οι οποίες, προφανώς, είναι νέες σχέσεις μεταξύ των συνόλων A και B.

Παράδειγμα 4.1.5. Στο σύνολο των ακεραίων αριθμών ορίζουμε δύο σχέσεις:

$$\mathrm{R} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid \text{ο } a \text{ είναι άρτιος και ο } b \text{ είναι περιττός}\}$$

και

$$\mathrm{Q} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid \text{ο } a \text{ είναι περιττός και ο } b \text{ είναι άρτιος}\},$$

τότε προφανώς (;) $\mathrm{R} \cap \mathrm{Q} = \varnothing$ και

$$\mathrm{R} \cup \mathrm{Q} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid \text{οι } a, b \text{ δεν είναι αμφότεροι άρτιοι ή αμφότεροι περιττοί}\}.$$

Έστω R μια σχέση μεταξύ στοιχείων του σύνολου A και στοιχείων του σύνολου B και $A_1 \subseteq A$, $B_1 \subseteq B$, τότε η τομή

$$\mathrm{F} = \mathrm{R} \cap (A_1 \times B_1) \subseteq A_1 \times B_1$$

ορίζει μια σχέση μεταξύ στοιχείων του σύνολου A_1 και στοιχείων του σύνολου B_1. Η σχέση αυτή θα ονομάζεται ο **περιορισμός** της R στα (υπο)σύνολα A_1 και B_1 και συμβολίζεται

$$\mathrm{R}_{|(A_1 \times B_1)}.$$

Σχόλιο 4.1.6. Όπως αντιλαμβανόμεθα, ο περιορισμός μιας σχέσης δεν είναι τίποτε άλλο από την τομή δύο σχέσεων, μόνο που στην περίπτωση αυτή θέλουμε να δώσουμε περισσότερη "βαρύτητα" σε μια από αυτές.

Για παράδειγμα: Έστω η σχέση

$$\mathrm{R} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid \text{ο } a \text{ διαιρεί τον } b\}$$

και

$$A_1 \times B_1 = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid \text{ο } a \text{ είναι πρώτος και ο } b \text{ είναι τυχαίος ακέραιος}\}.$$

Τότε ο περιορισμός $\mathrm{R}_{|(A_1 \times B_1)}$ της R στο $A_1 \times B_1$ αποτελείται από όλα τα ζεύγη ακεραίων αριθμών (a, b), όπου ο a είναι πρώτος διαιρέτης του b.

Η πλέον συνήθης μορφή περιορισμού σχέσης είναι η εξής: Έστω (A, R) ένα σύνολο εφοδιασμένο με την σχέση R και B ένα υποσύνολό του. Τότε ο περιορισμός της σχέσης R επί του υποσυνόλου $B \times B$, δηλαδή η τομή $\mathrm{R} \cap B \times B$, αποτελείται από όλα τα ζεύγη στοιχείων του υποσυνόλου B, τα οποία σχετίζονται μέσω της σχέσης R. Στην περίπτωση αυτή, ο περιορισμός $\mathrm{R}_{|B \times B}$ συμβολίζεται $\mathrm{R}_{|B}$ και αποτελεί μια σχέση στο (υπο)-σύνολο B. Για τον λόγο αυτόν ονομάζεται η **επαγόμενη** σχέση από την (αρχική) σχέση R.

4.1.2 Ασκήσεις

1. Στο σύνολο των πραγματικών αριθμών ορίζουμε τις εξής σχέσεις:

$$\begin{aligned} \mathrm{P} &= \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \neq y\}, \\ \mathrm{Q} &= \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}, \\ \mathrm{R} &= \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 \leq y\}, \\ \mathrm{S} &= \{(1, y) \in \mathbb{R} \times \mathbb{R}\}, \\ \mathrm{T} &= \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 1\}. \end{aligned}$$

   Για κάθε μια από τις σχέσεις αυτές να ορίσετε την αντίστροφή της και την συμπληρωματική της.

   Για κάθε δύο από αυτές τις σχέσεις να ορίσετε την σύνθεσή τους (όλες τις περιπτώσεις).

   Για κάθε δύο από αυτές τις σχέσεις να ορίσετε την τομή τους και την ένωσή τους (όλες τις περιπτώσεις).

   Για κάθε μία από αυτές τις σχέσεις να βρείτε τον περιορισμό της στο σύνολο των ακεραίων $\mathbb{Z}$.

   Μπορείτε να παραστήσετε, γεωμετρικά, κάθε μια από αυτές σχέσεις στο επίπεδο με την βοήθεια ενός συστήματος ορθογωνίων αξόνων;

2. Δίνεται ένα πεπερασμένο σύνολο A με n το πλήθος στοιχεία. Να υπολογίσετε το πλήθος των σχέσεων, οι οποίες μπορούν να ορισθούν στο σύνολο A.

   Υπόδειξη. Ανατρέξτε στην Πρόταση 1.1.44 και στην Άσκηση $1.1.7_3$.

   Εφαρμογή. Να υπολογίσετε όλες τις σχέσεις, που μπορούν να ορισθούν στο σύνολο $A = \{a, b\}$.

   Σε κάθε μία από αυτές να υπολογίσετε την αντίστροφή της και την συμπληρωματική της.

3. Στην Παρατήρηση $4.1.2_5$ ισχυριζόμαστε ότι: Προφανώς (γιατί;), η αντίστροφη σχέση R^{-1} μιας σχέσης R είναι μοναδική και η αντίστροφη σχέση της (αντίστροφης) σχέσης R^{-1} είναι η αρχική σχέση R $((R^{-1})^{-1} = R)$.

   Να δικαιολογήσετε, με κάθε λεπτομέρεια, το (γιατί;).

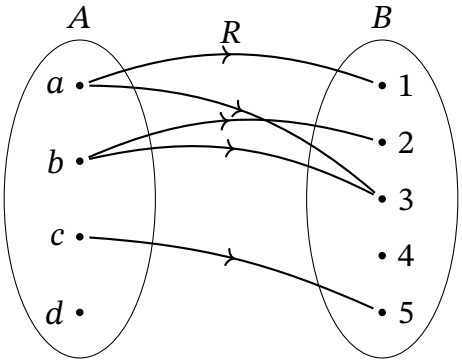
4.2 Παράσταση Σχέσεων

Έστω ότι έχουμε μια σχέση $\mathrm{R} \subset A \times B$ από το σύνολο A στο σύνολο B. Η σχέση R, ως σύνολο θα μπορούσε να ορισθεί ή με αναγραφή των στοιχείων ή με περιγραφή των στοιχείων της. Ορισμένες φορές, ειδικά όταν τα σύνολα A και B είναι πεπερασμένα, μπορούμε να παραστήσουμε την σχέση "εποπτικά" με διαφορετικούς τρόπους, οι οποίοι μας βοηθούν να κατανοήσουμε την σχέση R καλύτερα. Πριν προχωρήσουμε, ας δούμε ένα παράδειγμα:

Παράδειγμα 4.2.1. Έστω ότι έχουμε τα σύνολα $A = \{a, b, c, d\}, B = \{1, 2, 3, 4, 5\}$ και την σχέση

$$\mathrm{R} = \{(a, 1), (a, 3), (b, 2), (b, 3), (c, 5)\}.$$

Θα μπορούσαμε να "παραστήσουμε" τη σχέση αυτή "διαγραμματικά" όπως φαίνεται στο σχήμα 4.1.[4]



Σχήμα 4.1: *Διάγραμμα της σχέσης R.*

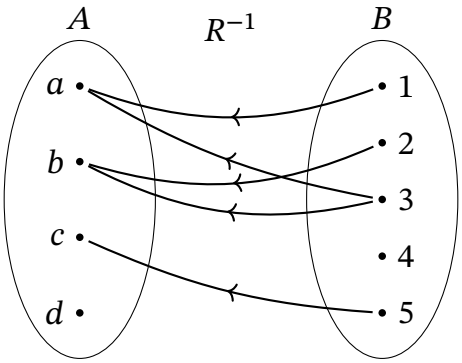
Επίσης, θα μπορούσαμε να παραστήσουμε την σχέση αυτή με έναν πίνακα "διπλής εισόδου" ως εξής:

	1	2	3	4	5
a	(a, 1)		(a, 3)		
b		(b, 2)	(b, 3)		
c					(c, 5)
d					

Η αντίστροφη σχέση του προηγουμένου παραδείγματος είναι η

$$\mathrm{R}^{-1} = \{(1, a), (3, a), (2, b), (3, b), (5, c)\}.$$

Διαγραμματικά η σχέση αυτή παρίσταται στο σχήμα 4.2.



Σχήμα 4.2: *Διάγραμμα της σχέσης* R^{-1}.

Όπως παρατηρούμε στο σχήμα αυτό, απλώς αντιστρέφεται η φορά των βελών στο προηγούμενο σχήμα.

Η παράσταση της αντίστροφης σχέσης R^{-1} με έναν πίνακα διπλής εισόδου είναι ο "ανάστροφος" του προηγουμένου πίνακα, δηλαδή ο πίνακας

[4]Τα διαγράμματα αυτά, όπου ένα στοιχείο $a \in A$ ενώνεται με ένα στοιχείο $b \in \mathrm{B}$ με ένα βέλος, αν $a\mathrm{R}b$, αναφέρονται από ορισμένους συγγραφείς ως "βελοειδή διαγράμματα".

	a	b	c	d
1	(1, a)			
2		(2, b)		
3	(3, a)	(3, b)		
4				
5			(5, c)	

Η παράσταση μιας σχέσης με έναν πίνακα μπορεί να γίνει και διαφορετικά έτσι ώστε να μπορούμε να μελετούμε πράξεις μεταξύ σχέσεων.

Έστω

$$A = \{a_1, a_2, \ldots, a_m\}, \quad B = \{b_1, b_2, \ldots, b_n\}$$

και $\mathrm{R} \subset A \times B$. Η διάταξη αναγραφής των στοιχείων των δύο συνόλων είναι αυθαίρετη, αλλά στο εξής θα διατηρείται. Στη σχέση R αντιστοιχούμε έναν πίνακα με m γραμμές και n στήλες ως εξής: Στη θέση $i\,j$ έχει 1 αν $(a_i, b_j) \in \mathrm{R}$ και έχει 0 αν $(a_i, b_j) \notin \mathrm{R}$. Προφανώς, αν αλλάξει η διάταξη των στοιχείων των δύο συνόλων, τότε αλλάζει και ο αντίστοιχος πίνακας.

Στο προηγούμενο παράδειγμα έχουμε τον εξής πίνακα:

$$\mathrm{M_R} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

(Να συγκρίνετε τον πίνακα αυτόν με τον πίνακα "διπλής εισόδου", που αντιστοιχεί στην ίδια σχέση).

Προφανώς, ισχύει και το αντίστροφο. Αν έχουμε δύο πεπερασμένα σύνολα A και B με m και n το πλήθος στοιχεία αντίστοιχα και προκαθορισμένη διάταξη των στοιχείων τους, τότε κάθε πίνακας με m γραμμές και n στήλες και στοιχεία 0 και 1 ορίζει μοναδικά μια σχέση από το σύνολο A στο σύνολο B.

Παράδειγμα 4.2.2. Έστω

$$A = \{a, b, c, d\}, \quad B = \{1, 2, 3, 4, 5\}$$

και ο πίνακας

$$\mathrm{K} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix},$$

τότε ο πίνακας αυτός ορίζει την εξής σχέση μεταξύ των A και B,

$$\mathrm{S} = \{(a, 1), (a, 3), (b, 1), (b, 3), (c, 2), (c, 5), (d, 2), (d, 4)\}.$$

Ο τρόπος αυτός παράστασης μιας σχέσης μας δίνει τη δυνατότητα να κάνουμε εύκολα πράξεις μεταξύ σχέσεων. Έστω δύο σχέσεις R και S μεταξύ των συνόλων A και B με αντίστοιχους πίνακες M_{R} και M_{S}.

Ο πίνακας $M_{\mathrm{R}\cap\mathrm{S}}$ που αντιστοιχεί στην τομή $\mathrm{R}\cap\mathrm{S}$ των δύο σχέσεων στη θέση $i\,j$ έχει 1, αν **και** οι δύο πίνακες M_{R} και M_{S} έχουν 1 στη θέση $i\,j$, διαφορετικά, αν τουλάχιστον σε έναν από τους δύο πίνακες στη θέση $i\,j$ υπάρχει μηδέν, τότε στον πίνακα της τομής $\mathrm{R}\cap\mathrm{S}$ στην αντίστοιχη θέση $i\,j$ έχουμε 0. Ο πίνακας $M_{\mathrm{R}\cup\mathrm{S}}$ που αντιστοιχεί στην ένωση $\mathrm{R}\cup\mathrm{S}$ των δύο σχέσεων στη θέση $i\,j$ έχει 0 αν **και** οι δύο πίνακες M_{R} και M_{S} έχουν 0 στη θέση $i\,j$, διαφορετικά, αν τουλάχιστον σε έναν από τους δύο πίνακες στη θέση $i\,j$ υπάρχει 1, τότε στον πίνακα της ένωσης $\mathrm{R}\cup\mathrm{S}$ στην αντίστοιχη θέση $i\,j$ έχουμε 1.

Παράδειγμα 4.2.3. Έστω

$$A = \{a, b, c, d\}, \quad B = \{1, 2, 3, 4, 5\}$$

και R, S δύο σχέσεις μεταξύ των συνόλων A και B με αντίστοιχους πίνακες

$$M_R = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ και } M_S = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix},$$

τότε έχουμε

$$M_{R\cap S} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ και } M_{R\cup S} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Έστω R μια σχέση μεταξύ των συνόλων A και B και T μια σχέση μεταξύ των συνόλων B και C. Τότε, ως γνωστόν, ορίζεται η σύνθεση $T \circ R$ των δύο σχέσεων ως μια σχέση μεταξύ των συνόλων A και C με $(a, c) \in T \circ R$, αν υπάρχει $b \in B$ έτσι ώστε $(a, b) \in R$ και $(b, c) \in T$.

Ας δούμε ένα παράδειγμα.

Παράδειγμα 4.2.4. Έστω $A = \{a, b, c, d\}$, $B = \{1, 2, 3, 4, 5\}$ και $C = \{x, y, z\}$. Έστω

$$R = \{(a, 1), (a, 3), (b, 1), (b, 3), (c, 2), (c, 5), (d, 2), (d, 4)\}$$

μια σχέση μεταξύ των A και B και

$$T = \{(1, x), (2, x), (2, z), (4, y), (4, z), (5, x)\}$$

μια σχέση μεταξύ των B και C. Τότε η σύνθεση των δύο σχέσεων είναι η

$$T \circ R = \{(a, x), (b, x), (c, x), (c, z), (d, x), (d, y), (d, z)\}.$$

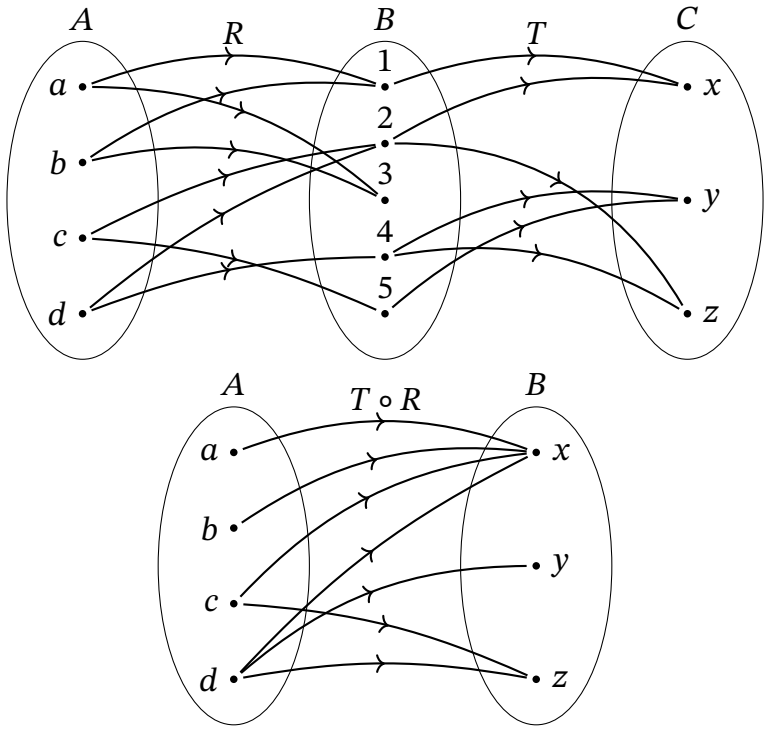
Θα μπορούσαμε να "παραστήσουμε" τη σχέση αυτή "διαγραμματικά" όπως φαίνεται στο σχήμα 4.3. Όπως βλέπουμε, υπάρχει βέλος που ενώνει ένα στοιχείο του συνόλου A με ένα στοιχείο του συνόλου C, μόνο στην περίπτωση όπου υπάρχει "αλληλουχία βελών", δια μέσου στοιχείων του συνόλου B.

Έστω τώρα R μια σχέση μεταξύ των συνόλων A και B και T μια σχέση μεταξύ των συνόλων B και C με αντίστοιχους πίνακες M_R και M_T. Γεννάται το ερώτημα:

> Μπορούμε να υπολογίσουμε τον αντίστοιχο πίνακα $M_{T\circ R}$ της σύνθεσης $T \circ R$ με την *βοήθεια* των πινάκων M_R και M_T;

Η απάντηση είναι καταφατική. Πριν δούμε πώς το επιτυγχάνουμε, θα υπενθυμίσουμε[5] τον "πολλαπλασιασμό" και την "πρόσθεση" κατά Boole.

[5]Για όσους δεν είναι εξοικειωμένοι με αυτές τις πράξεις, δεν πειράζει, θα μας δοθεί η ευκαιρία στα επόμενα να επανέλθουμε.



Σχήμα 4.3: *Διάγραμμα της σχέσης* $T \circ R$.

Ορίζουμε ως πρόσθεση και συμβολίζουμε με $\oplus$ ως εξής:

$$1 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1.$$

Ορίζουμε ως πολλαπλασιασμό και συμβολίζουμε με $\odot$ ως εξής:

$$1 \odot 1 = 1$$
$$1 \odot 0 = 0$$
$$0 \odot 0 = 0$$
$$0 \odot 1 = 0.$$

Έστω $M = (a_{ij})$ ένας πίνακας με m το πλήθος γραμμές και n το πλήθος στήλες και $N = (b_{ij})$ ένας πίνακας με n το πλήθος γραμμές και r το πλήθος στήλες και με στοιχεία μηδέν και ένα. Ορίζουμε, ως γινόμενο $M \otimes N$ των δύο πινάκων, έναν πίνακα K με m το πλήθος γραμμές και r το πλήθος στήλες, όπου στη θέση $i\,j$ έχει το στοιχείο

$$c_{ij} = (a_{i1} \odot b_{1j}) \oplus (a_{i2} \odot b_{2j}) \oplus \cdots \oplus (a_{in} \odot b_{nj}).$$

Επισημαίνουμε ότι, για να ορισθεί το γινόμενο πινάκων, αναγκαία προϋπόθεση είναι: Το πλήθος των στηλών του πρώτου πίνακα πρέπει να ισούται με το πλήθος των γραμμών του δευτέρου πίνακα.

Παράδειγμα 4.2.5. Έστω οι πίνακες

$$\mathrm{M} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ και } \mathrm{N} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix},$$

τότε έχουμε

$$M \otimes \mathrm{N} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

(Να ελέγξετε τις πράξεις).

Πρόταση 4.2.6. *Έστω* R *μια σχέση μεταξύ των (πεπερασμένων) συνόλων* A *και* B *και* T *μια σχέση μεταξύ των συνόλων* B *και* C *με αντίστοιχους πίνακες* M_{R} *και* M_{T}. *Ο Πίνακας* $M_{\mathrm{T}\circ\mathrm{R}}$ *της σύνθεσης* $\mathrm{T} \circ \mathrm{R}$ *ισούται με το γινόμενο* $M_{\mathrm{R}} \otimes M_{\mathrm{T}}$.

Απόδειξη. Η απόδειξη είναι άμεση εφαρμογή του ορισμού του γινομένου πινάκων, το οποίο ορίστηκε αμέσως προηγουμένως και του ορισμού της σύνθεσης σχέσεων. Όπου, αν $a \in A$ και $c \in C$, το ζεύγος $(a, c) \in \mathrm{T} \circ \mathrm{R}$, αν υπάρχει $b \in B$ έτσι ώστε $(a, b) \in \mathrm{R}$ και $(b, c) \in \mathrm{T}$. ό.έ.δ.

Παράδειγμα 4.2.7. Στο Παράδειγμα 4.2.4 είχαμε τα σύνολα

$$A = \{a, b, c, d\},\ B = \{1, 2, 3, 4, 5\} \text{ και } C = \{x, y, z\}$$

και τις σχέσεις

$$\mathrm{R} = \{(a, 1), (a, 3), (b, 1), (b, 3), (c, 2), (c, 5), (d, 2), (d, 4)\}$$

μεταξύ των A και B και

$$\mathrm{T} = \{(1, x), (2, x), (2, z), (4, y), (4, z), (5, x)\}$$

μεταξύ των B και C. Επομένως, η σύνθεση των δύο σχέσεων είναι η

$$\mathrm{T} \circ \mathrm{R} = \{(a, x), (b, x), (c, x), (c, z), (d, x), (d, y), (d, z)\}.$$

Εύκολα βλέπουμε ότι ο πίνακας της R είναι ο πίνακας

$$\mathrm{M}_{\mathrm{R}} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

και ο πίνακας της T ο πίνακας

$$M_{\mathrm{T}} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Ο πίνακας της σύνθεσης $\mathrm{T} \circ \mathrm{R}$ είναι ο πίνακας

$$M_{\mathrm{T}\circ\mathrm{R}} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Αν πολλαπλασιάσουμε τους πίνακες M_{R} και M_{T} έχουμε:

$$M_{\mathrm{R}} \otimes M_{\mathrm{T}} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Δηλαδή $M_{\mathrm{R}} \otimes M_{\mathrm{T}} = M_{\mathrm{T}\circ\mathrm{R}}$, όπως αναμενόταν.

4.2.1 Ασκήσεις

1. Στο σύνολο $A = \{2, 3, 5, 6, 9, 10, \}$ ορίζουμε μια σχέση $\mid$ ως εξής: $a \mid b$, αν ο a διαιρεί τον b. Να παραστήσετε την σχέση αυτή με έναν πίνακα.

   Ποια είναι η αντίστροφη σχέση της;

2. Έστω η σχέση R μεταξύ των συνόλων

   $$A = \{1, 2, 3, 4, 5\} \text{ και } B = \{4, 6, 10, 12, 14, 22\},$$

   η οποία ορίζεται ως εξής: $(a, b) \in \mathrm{R}$, αν ο b είναι πολλαπλάσιο του a.

   Να την παραστήσετε με ένα διάγραμμα και με πίνακες.

   Να υπολογίσετε την R^{-1}.

3. Έστω R μια σχέση μεταξύ των συνόλων A και B με αντίστοιχο πίνακα M_{R}. Να υπολογίσετε (συναρτήσει του πίνακα M_{R}) τον πίνακα $M_{\mathrm{R}-1}$, ο οποίος αντιστοιχεί στην αντίστροφη σχέση R^{-1} και τον πίνακα M_{R^c}, ο οποίος αντιστοιχεί στην συμπληρωματική σχέση.

4.3 Ιδιότητες σχέσεων

Από όλες τις σχέσεις, που μπορούν να ορισθούν μεταξύ στοιχείων του σύνολου A και στοιχείων του σύνολου B, υπάρχουν μερικές, οι οποίες έχουν κάποιες ιδιότητες και για τον λόγο αυτόν παρουσιάζουν ιδιαίτερο ενδιαφέρον[6]. Θα παρουσιάσουμε μερικές ιδιότητες σχέσεων.

1. Μια σχέση $\mathrm{R} \subseteq A \times B$ θα ονομάζεται **επί** του συνόλου B (ή απλώς επί), αν για κάθε $b \in B$ υπάρχει (τουλάχιστον) ένα $a \in A$ ούτως ώστε $a\,\mathrm{R}\,b$. Δηλαδή όλα τα στοιχεία του συνόλου B σχετίζονται με στοιχεία του συνόλου A.

   Για παράδειγμα η σχέση

   $$\mathrm{F} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid \text{ ο } a \text{ διαιρεί τον } b\}$$

   είναι επί (γιατί;).

2. Μια σχέση $\mathrm{R} \subseteq A \times B$ θα ονομάζεται **ένα προς ένα** (ή απλώς 1-1), αν για κάθε $b \in B$ υπάρχει το πολύ ένα $a \in A$ ούτως ώστε $a\,\mathrm{R}\,b$. Δηλαδή, θα μπορούσαμε να πούμε ότι η σχέση είναι 1-1, αν κάθε φορά που έχουμε $a_1\,\mathrm{R}\,b$ και $a_2\,\mathrm{R}\,c$ με $a_1 \neq a_2$, τότε $b \neq c$. Ισοδύναμα η σχέση είναι 1-1, αν κάθε φορά που έχουμε $a_1\,\mathrm{R}\,b$ και $a_2\,\mathrm{R}\,b$, τότε $a_1 = a_2$.

[6] Η έκφραση "ιδιαίτερο ενδιαφέρον" έχει και υποκειμενικό χαρακτήρα, εδώ την χρησιμοποιούμε με την έννοια ότι οι σχέσεις που εξετάζουμε είναι ενδιαφέρουσες από Μαθηματικής άποψης.

3. Μια σχέση $\mathrm{R} \subseteq A \times \mathrm{A}$ στο σύνολο A θα ονομάζεται **αυτοπαθής** (ή *ανακλαστική*), αν κάθε στοιχείο του συνόλου A σχετίζεται με τον εαυτό του. Δηλαδή για κάθε $a \in A$ ισχύει $a \,\mathrm{R}\, a$. Σχηματικά θα μπορούσαμε να πούμε ότι η σχέση είναι αυτοπαθής, αν περιέχει την "διαγώνιο"

$$D = \{(a, a) \mid a \in A\}.$$

(Σύμφωνα με την προηγουμένη παράγραφο, σε ένα πεπερασμένο σύνολο, μια σχέση είναι αυτοπαθής, αν και μόνο αν ο πίνακας, που την παριστά, στην κυρία διαγώνιο έχει μόνο 1).

4. Μια σχέση $\mathrm{R} \subseteq A \times \mathrm{A}$ στο σύνολο A θα ονομάζεται **συμμετρική**, αν

$$(a \,\mathrm{R}\, b) \Longrightarrow (b \,\mathrm{R}\, a),$$

Δηλαδή κάθε φορά, που το στοιχείο a σχετίζεται με το στοιχείο b, τότε και το στοιχείο b σχετίζεται με το στοιχείο a.

(Σύμφωνα με την προηγουμένη παράγραφο, σε ένα πεπερασμένο σύνολο, μια σχέση είναι συμμετρική, αν και μόνο αν ο πίνακας, που την παριστά, είναι συμμετρικός ως προς την κυρία διαγώνιο).

5. Μια σχέση $\mathrm{R} \subseteq A \times \mathrm{A}$ στο σύνολο A θα ονομάζεται **μεταβατική**, αν

$$(a \,\mathrm{R}\, b) \text{ και } (b \,\mathrm{R}\, c) \Longrightarrow (a \,\mathrm{R}\, c).$$

6. Μια σχέση $\mathrm{R} \subseteq A \times \mathrm{A}$ στο σύνολο A θα ονομάζεται **αντισυμμετρική**, αν

$$(a \,\mathrm{R}\, b) \text{ και } (b \,\mathrm{R}\, a) \Longrightarrow (a = b).$$

Παραδείγματα 4.3.1.

1. Η σχέση ισότητας $\mathrm{R} = \{(a, a) \in A \times A \mid a \in A\}$, που ορίζεται σε ένα σύνολο A, είναι προφανώς (;) αυτοπαθής, συμμετρική και μεταβατική. Επίσης, είναι επί και 1-1 (γιατί;).

2. Η σχέση ανισότητας $\neq$ σε ένα σύνολο δεν είναι αυτοπαθής, είναι συμμετρική, αλλά δεν είναι μεταβατική (γιατί;).

3. Στο αρχικό μας παράδειγμα, όπου έχουμε ορίσει την σχέση

$$\mathrm{F} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid \text{ο } a \mid b\},$$

είναι εύκολο να ελέγξουμε ότι η F είναι αυτοπαθής και μεταβατική, αλλά δεν είναι ούτε συμμετρική ούτε αντισυμμετρική (γιατί;).

Αν όμως πάρουμε την επαγόμενη σχέση στο σύνολο των φυσικών αριθμών $\mathbb{N}$, τότε η σχέση αυτή είναι και αντισυμμετρική (γιατί;).

4.3.1 Ασκήσεις

1. Στις παρακάτω περιπτώσεις να ελέγξετε αν οι οριζόμενες σχέσεις είναι αυτοπαθείς, συμμετρικές και μεταβατικές. Να τεκμηριώσετε τις απαντήσεις σας.

   i. Στο σύνολο των ακεραίων $\mathbb{Z}$ ορίζουμε την σχέση $a\,\mathrm{R}\,b$, αν $\mid a-b \mid < 1$.

   ii. Στο σύνολο των ακεραίων $\mathbb{Z}$ ορίζουμε την σχέση $a\,\mathrm{R}\,b$, αν $\mid a-b \mid \leq 1$.

   iii. Στο σύνολο των πραγματικών αριθμών $\mathbb{R}$ ορίζουμε την σχέση $a\,\mathrm{R}\,b$, αν $a-b \in \mathbb{Z}$.

   iv. Στο σύνολο των ακεραίων $\mathbb{Z}$ ορίζουμε την σχέση $a\,\mathrm{R}\,b$, αν η διαφορά a^2-b^2 είναι πολλαπλάσιο του 4.

2. Στην Άσκηση 4.1.2$_2$ είχαμε ορίσει όλες τις σχέσεις στο σύνολο $A = \{a, b\}$. Εδώ να ελέγξετε ποιες από αυτές είναι αυτοπαθείς, ποιες συμμετρικές, ποιες μεταβατικές, ποιες 1-1 και ποιες επί.

3. Έστω μια R σχέση σε ένα σύνολο A. Υποθέτουμε ότι είναι μεταβατική και συμμετρική. Ένας φοιτητής ισχυρίζεται ότι είναι και αυτοπαθής και επιχειρηματολογεί ως εξής:

   Έστω $a, b \in A$ με $a\,\mathrm{R}\,b$. Επειδή η σχέση έχει υποτεθεί συμμετρική, θα ισχύει ότι $b\mathrm{R}\,a$. Αλλά η σχέση έχει υποτεθεί και μεταβατική, επομένως από τα $a\,\mathrm{R}\,b$ και $b\mathrm{R}\,a$ έπεται ότι $a\mathrm{R}\,a$. Συνεπώς, η σχέση είναι αυτοπαθής.

   Είναι ο ισχυρισμός του φοιτητή σωστός;

4. Δείξτε τον ισοδύναμο ορισμό μιας 1-1 σχέσης: Η σχέση $\mathrm{R} \subseteq A \times B$ είναι 1-1, αν και μόνο αν, κάθε φορά, που έχουμε $a_1\,\mathrm{R}\,b_1$ και $a_2\,\mathrm{R}\,b_2$, με $b_1 \neq b_2$, τότε $a_1 \neq a_2$.

5. Έστω A ένα σύνολο εφοδιασμένο με μια σχέση R, η οποία είναι αυτοπαθής. Δείξτε ότι $\mathrm{R} \subset \mathrm{R} \circ \mathrm{R}$.

4.4 Είδη σχέσεων

Στην παράγραφο αυτή θα επικεντρωθούμε σε δύο είδη σχέσεων σε ένα σύνολο, οι οποίες είναι πολύ σημαντικές, λόγω των ιδιοτήτων που έχουν, στην σπουδή των Μαθηματικών.

4.4.1 Σχέσεις Ισοδυναμίας

Έστω $(A, \sim)$ ένα (μη κενό) σύνολο εφοδιασμένο με την σχέση $\sim$. Η σχέση $\sim$ θα ονομάζεται σχέση **ισοδυναμίας** (ή απλά ισοδυναμία), αν είναι αυτοπαθής, συμμετρική και μεταβατική.

Παραδείγματα 4.4.1.

1. Σε κάθε μη κενό σύνολο A ορίζεται μια σχέση ισοδυναμίας, η διαγώνιος

$$D = \{(a, a) \mid a \in A\}.$$

   Η σχέση αυτή δεν είναι τίποτε άλλο από την γνωστή σχέση της ισότητας μεταξύ των στοιχείων του συνόλου A.

2. Προφανώς η συμπληρωματική σχέση της ισότητας, η σχέση ανισότητας,
$$\{(a, b) \in A \times A \mid a \neq b\}$$
δεν είναι σχέση ισοδυναμίας.

3. Έστω A το σύνολο των μη μηδενικών διανυσμάτων με κοινή αρχή το σημείο $(0, 0, 0)$ στον τρισδιάστατο χώρο. Στο σύνολο A ορίζουμε μια σχέση ως εξής: $\vec{v} \sim \vec{u}$, αν $\vec{v}$ και $\vec{u}$ έχουν τον ίδιο φορέα. Προφανώς η σχέση αυτή είναι σχέση ισοδυναμίας.

4. Στο σύνολο των ακεραίων $\mathbb{Z}$ ορίζουμε μια σχέση $\equiv$ ως εξής: $a \equiv b$, αν το 2 διαιρεί την διαφορά $a-b$. Προφανώς (γιατί;) η σχέση $\equiv$ είναι σχέση ισοδυναμίας.

   Γενικά, για κάθε θετικό ακέραιο m, μπορούμε στο σύνολο των ακεραίων να ορίσουμε μια σχέση $\equiv_m$ ως εξής: $a \equiv_m b$, αν το m διαιρεί την διαφορά $a - b$. Προφανώς (γιατί;) η σχέση αυτή είναι σχέση ισοδυναμίας.

5. Στο σύνολο $\mathbb{R}$ των πραγματικών αριθμών ορίζουμε μια σχέση $a \sim b$, αν η διαφορά $a - b$ είναι ακέραιος αριθμός. Προφανώς (γιατί;) η σχέση αυτή είναι σχέση ισοδυναμίας.

6. Στο σύνολο $\mathbb{R}$ των πραγματικών αριθμών ορίζουμε μια σχέση $a \sim b$, αν η διαφορά $a-b$ είναι ρητός αριθμός. Προφανώς (γιατί;) η σχέση αυτή είναι σχέση ισοδυναμίας.

Έστω $A, \sim$ ένα σύνολο εφοδιασμένο με μια σχέση ισοδυναμίας. Για κάθε $a \in A$ ορίζουμε το σύνολο
$$C_a = \{b \in A \mid b \sim a\}.$$
Το σύνολο C_a θα ονομάζεται η **κλάση ισοδυναμίας** του στοιχείου a.

Πρόταση 4.4.2. *Έστω $(A, \sim)$ ένα σύνολο εφοδιασμένο με μια σχέση ισοδυναμίας.*

1. *Έστω $a, b \in A$. Τότε ισχύει ότι: $a \sim b$, αν και μόνο αν $C_a = C_b$.*
2. *Έστω $a, b \in A$. Τότε ισχύει ότι: $a \nsim b$, αν και μόνο αν $C_a \cap C_b = \emptyset$.*
3. *Η οικογένεια $(C_a)_{a \in A}$ αποτελεί μια διαμέριση του συνόλου A.*

Απόδειξη. Για τα (1) και (2) το αποτέλεσμα είναι άμεσο από τον ορισμό της σχέσεως ισοδυναμίας και τον ορισμό της κλάσεως ισοδυναμίας.

Για το (3) αρκεί (ιδέ τον Ορισμό 1.1.49) να αποδειχθεί ότι κάθε κλάση ισοδυναμίας είναι μη κενό σύνολο, ανά δύο οι κλάσεις ισοδυναμίας είτε ταυτίζονται είτε είναι ξένες μεταξύ τους και επιπλέον ότι η ένωσή τους ισούται με όλο το σύνολο A.
Όλα αυτά προφανώς ισχύουν (γιατί;). ό.έ.δ.

Έστω $(A, \sim)$ ένα σύνολο εφοδιασμένο με μια σχέση ισοδυναμίας. Έστω
$$A/\sim = \{C_a\}$$
το σύνολο των διακεκριμένων κλάσεων ισοδυναμίας. Το σύνολο αυτό καλείται σύνολο των **πηλίκων** ως προς την σχέση $\sim$.[7] Έστω
$$T = \{a \mid C_a \in A/\sim\}.$$

[7] Σε πολλά συγγράμματα αναφέρεται και ως σύνολο πηλίκο.

Δηλαδή από κάθε διακεκριμένη κλάση ισοδυναμίας επιλέγουμε ένα (οποιοδήποτε) στοιχείο. Το σύνολο T θα καλείται σύνολο **αντιπροσώπων**, ως προς την $\sim$.

Στο Παράδειγμα 4.4.1$_4$ ένα σύνολο αντιπροσώπων είναι το $T = \{0, 1, \dots, m-1\}$ (γιατί;)

Στην προηγουμένη πρόταση είδαμε ότι μια σχέση ισοδυναμίας, σε ένα σύνολο, ορίζει μια διαμέριση. Θα δούμε ότι ισχύει και το αντίστροφο.

Πρόταση 4.4.3. *Έστω A ένα μη κενό σύνολο και $\mathcal{D} = (A_i)_{i\in I}$ μια διαμέριση του A. Στο σύνολο A ορίζουμε μια σχέση $\sim$ ως εξής: $a \sim b$, αν υπάρχει $i \in I$ έτσι ώστε $a, b \in A_i$. Η σχέση $\sim$ είναι σχέση ισοδυναμίας. Μάλιστα δε, η διαμέριση που ορίζεται από την $\sim$, σύμφωνα με την προηγουμένη πρόταση, είναι η αρχική διαμέριση $\mathcal{D}$. Δηλαδή,*

$$\mathcal{D} = A/\sim .$$

Απόδειξη. Είναι εύκολο να επαληθεύσουμε (η επαλήθευση αφήνεται ως άσκηση) ότι η σχέση που ορίζεται με αυτόν τον τρόπο είναι πράγματι σχέση ισοδυναμίας.

Έστω τώρα C_a μια κλάση ισοδυναμίας, ως προς την $\sim$. Επειδή το σύνολο $\mathcal{D}$ αποτελεί, εξ υποθέσεως, διαμέριση του συνόλου A, υπάρχει (μοναδικό) $i \in I$ έτσι ώστε $a \in A_i$. Από τον τρόπο ορισμού της σχέσης $\sim$ έπεται ότι $C_a \subseteq A_i$.

Αντίστροφα, έστω $b \in A_i$, τότε υπάρχει το $a \in A_i$ με την ιδιότητα $b \sim a$, άρα $b \in C_a$. Συνεπώς, $C_a = A_i$.

Τέλος, επειδή τα $\mathcal{D}$ και $A/\sim$ αποτελούν διαμερίσεις του ιδίου συνόλου A, $\mathcal{D} = A/\sim$. ό.έ.δ.

Παραδείγματα 4.4.4.

1. Στο Παράδειγμα 4.4.1$_4$ οι κλάσεις ισοδυναμίας είναι οι

$$\begin{aligned} C_0 &= \{mk \mid k \in \mathbb{Z}\}, \\ C_1 &= \{mk+1 \mid k \in \mathbb{Z}\}, \\ C_2 &= \{mk+2 \mid k \in \mathbb{Z}\}, \\ &\vdots \\ C_{m-1} &= \{mk+(m-1) \mid k \in \mathbb{Z}\} \end{aligned}$$

   (γιατί;).

2. Στο Παράδειγμα 4.4.1$_5$, αν r είναι ένας πραγματικός αριθμός, η κλάση ισοδυναμίας στην οποία ανήκει ο r είναι η

$$C_r = \{r + k \mid k \in \mathbb{Z}\}.$$

   Μάλιστα δε, ένα σύνολο αντιπροσώπων είναι οι πραγματικοί αριθμοί s με την ιδιότητα $0 \le s < 1$.

   Πράγματι, για κάθε πραγματικό αριθμό r υπάρχει μοναδικός ακέραιος αριθμός m με την ιδιότητα $m \le r < m+1$ [8], οπότε $r = m + s$ με $0 \le s < 1$. Συνεπώς, από τον ορισμό της συγκεκριμένης σχέσης ισοδυναμίας, έχουμε ότι $r \sim s$ και κατά συνέπεια $C_r = C_s$.

[8] Όπως έχουμε επισημάνει και σε προηγούμενο σημείο, η ιδιότητα αυτή (αν και φαντάζει προφανής) δεν είναι προφανής και χρήζει αποδείξεως.

3. Στο σύνολο $A = \{a, b, c, d, e\}$ μια διαμέριση είναι το σύνολο

$$\mathcal{D} = \{\{a, b\}, \{c\}, \{d, e\}\}.$$

Επομένως, ορίζεται η σχέση ισοδυναμίας

$$\mathrm{R} = \{(a, a), (b, b), (a, b), (b, a), (c, c), (d, d), (e, e), (d, e), (e, d)\}.$$

4.4.2 Ασκήσεις

1. Να ολοκληρώσετε, με κάθε λεπτομέρεια, τις αποδείξεις των Προτάσεων 4.4.2 και 4.4.3.

2. Έστω (A, R) ένα σύνολο εφοδιασμένο με μια σχέση, η οποία είναι συμμετρική και μεταβατική. Υποθέτουμε επιπλέον ότι η R είναι επί. Δηλαδή για κάθε $b \in A$ υπάρχει $a \in A$ έτσι ώστε $a\,\mathrm{R}\,b$. Δείξτε ότι η R είναι σχέση ισοδυναμίας.

3. Στα δύο τελευταία παραδείγματα από τα 4.4.1 να κάνετε σύγκριση μεταξύ των αντιστοίχων κλάσεων ισοδυναμίας.

4. Στο σύνολο $A = \{a, b\}$ να βρεθούν όλες οι σχέσεις ισοδυναμίας.

   Όμοια στο σύνολο $B = \{a, b, c\}$ να βρεθούν όλες οι σχέσεις ισοδυναμίας.

   Να παραστήσετε τις σχέσεις αυτές με τρεις τρόπους: Με βελοειδή διαγράμματα, με πίνακες διπλής εισόδου και με πίνακες των οποίων τα στοιχεία είναι 0 ή 1 (ιδέ την Παράγραφο 4.2).

5. Στο σύνολο των ακεραίων αριθμών ορίζουμε μια σχέση

$$a \sim b, \text{ αν το 4 διαιρεί τον αριθμό } a + 3b.$$

   Δείξτε ότι είναι σχέση ισοδυναμίας και να περιγράψετε τις κλάσεις ισοδυναμίας.

6. Στο σύνολο $\mathbb{R}$ των πραγματικών αριθμών ορίζουμε μια σχέση ως εξής:

$$a \sim b, \text{ αν } \lfloor a \rfloor = \lfloor b \rfloor,$$

   όπου με $\lfloor x \rfloor$ συμβολίζουμε τον μεγαλύτερο ακέραιο, ο οποίος είναι μικρότερος ή ίσος του x. Δείξτε ότι η σχέση αυτή είναι σχέση ισοδυναμίας και περιγράψτε τις κλάσεις ισοδυναμίας.

7. Στο καρτεσιανό γινόμενο $\mathbb{R} \times \mathbb{R}$ ορίζουμε την σχέση:

$$(x_1, y_1) \approx (x_2, y_2), \text{ αν } 2x_1 + 3y_1 = 2x_2 + 3y_2.$$

   Δείξτε ότι η σχέση αυτή είναι σχέση ισοδυναμίας. Να περιγράψετε τις κλάσεις ισοδυναμίας.

8. Στο καρτεσιανό γινόμενο $\mathbb{Z} \times \mathbb{Z}$ ορίζουμε μια σχέση $\sim$ ως εξής:

$$(a_1, a_2) \sim (b_1, b_2), \text{ αν } a_1 + b_2 = a_2 + b_1.$$

   Δείξτε ότι είναι σχέση ισοδυναμίας και να περιγράψετε τις κλάσεις ισοδυναμίας.

9. Στο καρτεσιανό γινόμενο $\mathbb{Z} \times \mathbb{Z}^*$, όπου $\mathbb{Z}^*$ είναι το σύνολο των μη μηδενικών ακεραίων, ορίζουμε μια σχέση $\sim$ ως εξής:

$$(a_1, a_2) \sim (b_1, b_2), \text{ αν } a_1 \cdot b_2 = a_2 \cdot b_1.$$

Δείξτε ότι είναι σχέση ισοδυναμίας και να περιγράψετε τις κλάσεις ισοδυναμίας[9].

10. Στο σύνολο $\mathbb{R}^2$ ορίζουμε μια σχέση ως εξής:

$$(a, b) \sim (c, d), \text{ αν } a^2 + b^2 = c^2 + d^2.$$

Δείξτε ότι η σχέση αυτή είναι σχέση ισοδυναμίας. Να προσδιορίσετε τις κλάσεις ισοδυναμίας. Μπορείτε να τις περιγράψετε γεωμετρικά;

Δείξτε ότι ένα σύνολο αντιπροσώπων είναι το σύνολο

$$\{(x, 0) \mid x \geq 0\}.$$

Να βρεθούν τέσσερα στοιχεία, τα οποία να ανήκουν στην κλάση ισοδυναμίας $C_{(3,4)}$.

11. Έστω $M = \mathbb{R} \times \mathbb{R} \setminus (0, 0)$ το σύνολο τω σημείων του επιπέδου εκτός από το 0-σημείο. Στο σύνολο αυτό ορίζουμε μια σχέση ως εξής:

$$(a_1, a_2) \sim (b_1, b_2), \quad \begin{array}{l}\text{αν υπάρχει ευθεία του επιπέδου,}\\ \text{η οποία διέρχεται από το σημείο } (0, 0) \text{ και}\\ \text{η οποία περιέχει και τα δύο σημεία } (a_1, a_2) \text{ και } (b_1, b_2).\end{array}$$

Δείξτε ότι η σχέση αυτή είναι σχέση ισοδυναμίας.

Μπορείτε να περιγράψετε γεωμετρικά το σύνολο πηλίκων $M/\sim$ λαμβάνοντας από κάθε κλάση ισοδυναμίας έναν αντιπρόσωπο;

12. Έστω R_1 και R_2 δύο σχέσεις ισοδυναμίας επί του ιδίου συνόλου A. Εξετάστε αν οι σχέσεις $\mathrm{R}_1 \cap \mathrm{R}_2$ και $\mathrm{R}_1 \cup \mathrm{R}_2$ αποτελούν σχέσεις ισοδυναμίας.

13. Έστω R_1 και R_2 δύο σχέσεις ισοδυναμίας επί του ιδίου συνόλου A και D_1, D_2 οι αντίστοιχες διαμερίσεις του συνόλου A, που ορίζονται από τις σχέσεις αυτές. Δείξτε ότι $\mathrm{R}_1 \subset \mathrm{R}_2$, αν και μόνο αν η D_1 είναι επιλέπτυνση της D_2. Δηλαδή κάθε υποσύνολο του A, το οποίο ανήκει στην D_1, είναι υποσύνολο ενός υποσυνόλου, το οποίο ανήκει την D_2.

14. Μια σχέση R θα ονομάζεται *κυκλική* αν

$$(a \,\mathrm{R}\, b \text{ και } b \,\mathrm{R}\, c) \Longrightarrow c \,\mathrm{R}\, a.$$

Δείξτε ότι μια σχέση R σε ένα σύνολο A είναι σχέση ισοδυναμίας, αν και μόνο αν είναι αυτοπαθής και κυκλική.

---

[9] Αυτή η σχέση ισοδυναμίας είναι μια από τις πλέον σημαντικές σχέσεις ισοδυναμίας στα Μαθηματικά. Αποτελεί την κατασκευή των ρητών αριθμών $\mathbb{Q}$. Επ' αυτού θα επανέλθουμε αργότερα.

4.4.3 Σχέσεις Διάταξης

Έστω (A, R) ένα σύνολο εφοδιασμένο με την σχέση R. Ένα υποσύνολο $B \subseteq A$ θα ονομάζεται **αλυσίδα**, ως προς την σχέση R, αν όλα τα στοιχεία του B σχετίζονται μεταξύ τους, δηλαδή,

$$\text{για } a, b \in B \text{ θα ισχύει } a \,\mathrm{R}\, b \text{ ή } b \,\mathrm{R}\, a.$$

Ορισμός 4.4.5. Έστω (A, R) ένα σύνολο εφοδιασμένο με την σχέση R. Η σχέση R θα ονομάζεται **σχέση προδιάταξης** ή απλά προδιάταξη, αν είναι αυτοπαθής και μεταβατική. Δηλαδή

$$a \,\mathrm{R}\, a \text{ για κάθε } a \in A \text{ και, αν } (a \,\mathrm{R}\, b) \text{ και } (b \,\mathrm{R}\, c) \implies (a \,\mathrm{R}\, c).$$

Συνήθως μια σχέση προδιάταξης συμβολίζεται ως $\prec$ και το σύνολο $(A, \prec)$ ονομάζεται **προδιατεταγμένο** σύνολο. Επίσης, αν ισχύει $a \prec b$, τότε λέμε ότι το στοιχείο a *προηγείται* του στοιχείου b (ή δυϊκά ότι το b *έπεται* του a).

Προφανώς, αν B είναι ένα υποσύνολο του προδιατεταγμένου συνόλου $(A, \prec)$, τότε η επαγόμενη σχέση επί του B, από την προδιάταξη $\prec$, είναι και αυτή μια προδιάταξη στο σύνολο B.

Ορισμός 4.4.6. Έστω $(A, \prec)$ ένα προδιατεταγμένο σύνολο. Αν επιπλέον υποθέσουμε ότι η σχέση $\prec$ είναι αντισυμμετρική, δηλαδή ισχύει:

$$\big((a \prec b) \text{ και } (b \prec a)\big) \implies (a = b),$$

τότε η σχέση ονομάζεται **μερική διάταξη** και το σύνολο $(A, \prec)$ **μερικώς διατεταγμένο** σύνολο.

Παραδείγματα 4.4.7.

1. Το σύνολο των ακεραίων $\mathbb{Z}$ με την γνωστή διάταξη $\leq$ *...του μικρότερον ή ίσον...* είναι μερικώς διατεταγμένο σύνολο.

2. Στο σύνολο των ακεραίων $\mathbb{Z}$ ορίζουμε μια άλλη σχέση ως εξής:

   $$a \prec b, \text{ αν και μόνο αν } |\, a \,| \leq |\, b \,|\,.$$

   Προφανώς (γιατί;) η σχέση αυτή είναι σχέση προδιάταξης, αλλά δεν είναι μερική διάταξη.

3. Η σχέση της διαιρετότητας στους ακεραίους (ιδέ το Παράδειγμα 4.3.1) είναι σχέση προδιάταξης, αλλά δεν είναι μερική διάταξη.

4. Αν στο προηγούμενο παράδειγμα πάρουμε την επαγόμενη (περιορισμό) σχέση στο σύνολο $\mathbb{N}$ των φυσικών αριθμών, τότε αυτή είναι μερική διάταξη.

5. Έστω $\mathcal{P}(X)$ το δυναμοσύνολο ενός συνόλου X. Το $\mathcal{P}(X)$ εφοδιασμένο με την σχέση $\subseteq$ *του περιέχεσθαι* είναι ένα μερικώς διατεταγμένο σύνολο.

Ορισμός 4.4.8. Ένα μερικώς διατεταγμένο σύνολο $(A, \prec)$, το οποίο επιπλέον είναι αλυσίδα, δηλαδή

$$\text{για } a, b \in A \text{ ισχύει } a \prec b \text{ ή } b \prec a,$$

θα ονομάζεται **ολικώς διατεταγμένο** ή **γραμμικώς διατεταγμένο** σύνολο[10].

Στα προηγούμενα παραδείγματα. Στο μεν πρώτο Παράδειγμα το σύνολο $(\mathbb{Z}, \leq)$ είναι ολικώς διατεταγμένο, στο δε πέμπτο Παράδειγμα το σύνολο $(\mathcal{P}(X), \subseteq)$ δεν είναι ολικώς διατεταγμένο σύνολο.

Παρατήρηση 4.4.9. Σε ένα ολικώς διατεταγμένο σύνολο, ανά δύο τα στοιχεία του σχετίζονται. Υπάρχει και το άλλο "άκρο", όπου υπάρχει περίπτωση να έχουμε ένα μερικά διατεταγμένο σύνολο $(A, \leq)$, με την ιδιότητα: Για $a, b \in A$ ισχύει $a \leq b$, αν και μόνο αν $a = b$. Πράγματι, η σχέση αυτή είναι σχέση μερικής διάταξης (γιατί;), αλλά δύο διαφορετικά στοιχεία δεν σχετίζονται μεταξύ τους. Ένα τέτοιο σύνολο θα ονομάζεται **ολικώς μη διατεταγμένο** σύνολο[11].

Ορισμοί 4.4.10. Έστω $(A, \prec)$ ένα προδιατεταγμένο σύνολο.

1. Ένα στοιχείο $m \in A$ θα ονομάζεται **μεγαλύτερο** αν για ένα $a \in A$ με την ιδιότητα $m \prec a$ συνεπάγεται ότι $a \prec m$. Αυτό σημαίνει ότι, είτε κανένα στοιχείο $a \in A$ δεν έπεται του m είτε, αν κάποιο $a \in A$ έπεται του m, τότε αυτό προηγείται του m.

   Δυϊκά, ένα στοιχείο $e \in A$ θα ονομάζεται **μικρότερο** αν για ένα $a \in A$ με την ιδιότητα $a \prec e$ συνεπάγεται ότι $e \prec a$.

   Προφανώς, σε ένα μερικά διατεταγμένο σύνολο A, η έκφραση

   > "...το m είναι μεγαλύτερο στοιχείο..."

   είναι ισοδύναμη με την έκφραση

   > "...ένα στοιχείο του A είτε δεν σχετίζεται με το m είτε προηγείται του m...".

   Παρομοίως, σε ένα μερικά διατεταγμένο σύνολο A, η έκφραση

   > "...το e είναι μικρότερο στοιχείο..."

   είναι ισοδύναμη με την έκφραση

   > "...ένα στοιχείο του A είτε δεν σχετίζεται με το e είτε έπεται του e...".

2. Έστω $(A, \leq)$ ένα μερικά διατεταγμένο σύνολο. Ένα στοιχείο $m \in A$ θα ονομάζεται ***το*** *μέγιστο στοιχείο*, αν

   $$x \leq m, \text{ για κάθε } x \in A.$$

   Δυϊκά, ένα στοιχείο $e \in A$ θα ονομάζεται ***το*** *ελάχιστο στοιχείο*, αν

   $$e \leq x, \text{ για κάθε } x \in A.$$

[10]Τα επίθετα "μερική", αντίστοιχα "ολική" διάταξη δηλώνουν ακριβώς αυτό που ισχύει. Στην πρώτη περίπτωση ενδέχεται να υπάρχουν στοιχεία του συνόλου, τα οποία δεν είναι "συγκρίσιμα", ενώ στην δεύτερη περίπτωση, όλα τα στοιχεία είναι (ανά δύο) "συγκρίσιμα". Επίσης, θα χρησιμοποιούμε (μην τηρώντας την ενιαία γραφή), αδιακρίτως τα επιρρήματα *μερικά*, *μερικώς*, *ολικά*, *ολικώς* και *γραμμικά*, *γραμμικώς*.

[11]Εδώ έχουμε ένα γλωσσικό λογοπαίγνιο, όπου ομιλούμε για ένα μερικώς διατεταγμένο σύνολο, το οποίο είναι ολικώς....μη διατεταγμένο.

Το πρώτο, το οποίο πρέπει να επισημάνουμε, είναι ότι δεν πρέπει να συγχέουμε την έννοια **του** μέγιστου στοιχείου με την έννοια **ενός** μεγαλύτερου στοιχείου. Όμοια, την έννοια **του** ελαχίστου στοιχείου με την έννοια **ενός** μικροτέρου στοιχείου[12]. Το επόμενο παράδειγμα είναι διευκρινιστικό.

Παράδειγμα 4.4.11. Έστω Y το σύνολο όλων των μη κενών υποσυνόλων ενός συνόλου X με τουλάχιστον δύο στοιχεία ($Y = \mathcal{P}(X) \setminus \emptyset$). Το σύνολο $(Y, \subseteq)$ είναι μερικά διατεταγμένο σύνολο με πολλά μικρότερα στοιχεία, αλλά δεν έχει το ελάχιστο στοιχείο (γιατί;). Ποια είναι τα μικρότερα στοιχεία του;

Ένας πιθανός λόγος, όπου, στην αρχή, συγχέουμε τις δύο έννοιες, είναι ότι παρασυρόμαστε και θεωρούμε όλα τα μερικώς διατεταγμένα σύνολα ως ολικώς διατεταγμένα. Συγκεκριμένα ισχύει το εξής:

Θεώρημα 4.4.12. *Έστω $(A, \leq)$ ένα ολικά διατεταγμένο σύνολο. Ένα $x \in A$ είναι το ελάχιστο (αντίστοιχα το μέγιστο) στοιχείο αν και μόνο αν είναι το (μοναδικό) μικρότερο (αντίστοιχα το (μοναδικό) μεγαλύτερο) στοιχείο του A.*

Απόδειξη. Η απόδειξη είναι εύκολη. Αρκεί να εφαρμόσουμε τους αντίστοιχους ορισμούς 4.4.8 και 4.4.10 ό.έ.δ.

Στο προηγούμενο παράδειγμα είδαμε ότι σε ένα μερικά διατεταγμένο σύνολο ενδέχεται να έχουμε πολλά μικρότερα στοιχεία. Από την άλλη πλευρά, στον ορισμό του ελαχίστου και του μέγιστου στοιχείου ενός συνόλου χρησιμοποιήσαμε το οριστικό άρθρο **το** υποδηλώνοντας ότι πρόκειται για μοναδικό στοιχείο. Πράγματι, περί αυτού πρόκειται.

Θεώρημα 4.4.13. *Έστω $(A, \leq)$ ένα μερικώς διατεταγμένο σύνολο. Υποθέτουμε ότι έχει ένα μέγιστο στοιχείο. Τότε αυτό είναι μοναδικό. Όμοια, αν έχει ένα ελάχιστο στοιχείο, τότε αυτό είναι μοναδικό.*

Απόδειξη. Υποθέτουμε ότι υπάρχουν δύο μέγιστα στοιχεία, έστω m και μ. Τότε, σύμφωνα με τον Ορισμό 4.4.10 $_2$ του μέγιστου στοιχείου, έχουμε

$$m \leq \mu \text{ και } \mu \leq m,$$

αλλά έχουμε μερική διάταξη (ισχύει η αντισυμμετρική ιδιότητα), επομένως $m = \mu$. Όμοια για το ελάχιστο στοιχείο. ό.έ.δ.

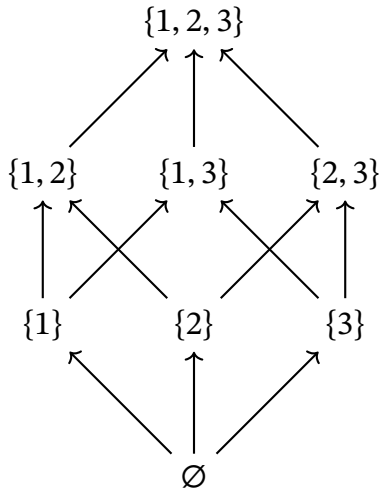
Όταν έχουμε ένα μερικώς διατεταγμένο σύνολο με μικρό αριθμό στοιχείων, τότε μπορούμε να χρησιμοποιήσουμε *διαγράμματα*[13] και να έχουμε μια διαισθητική εικόνα της διάταξης των στοιχείων του συνόλου.

Πριν προχωρήσουμε, ας δούμε ένα παράδειγμα.

Έστω το σύνολο $A = \{1, 2, 3\}$ και $(\mathcal{P}(A), \subseteq)$ το δυναμοσύνολο του A εφοδιασμένο με την μερική διάταξη $\subseteq$ του "περιέχεσθαι". Στο σχήμα 4.4 παρουσιάζεται η διάταξη των στοιχείων του συνόλου $(\mathcal{P}(A), \subseteq)$.

[12] Στην ξενόγλωσση βιβλιογραφία ένα μεγαλύτερο στοιχείο ονομάζεται maximal, ενώ το μέγιστο στοιχείο ονομάζεται the greatest ή the maximum. Όμοια, ένα μικρότερο στοιχείο ονομάζεται minimal, ενώ το ελάχιστο στοιχείο ονομάζεται the least ή the minimum. Στην Ελληνική βιβλιογραφία έχει γίνει προσπάθεια αποφυγής της σύγχυσης ονομάζοντας ένα μικρότερο στοιχείο ως *ελαχιστικό* και ένα μεγαλύτερο στοιχείο ως *μεγιστικό*. Οι λέξεις ελαχιστικό και μεγιστικό είναι "κατασκευασμένες", για τον λόγο αυτόν, στο παρόν βιβλίο, προτιμούμε τους όρους μικρότερο και μεγαλύτερο αντίστοιχα. Επίσης, στην Ελληνική βιβλιογραφία ένα μικρότερο στοιχείο αναφέρεται και ως *ελάσσον* και ένα μεγαλύτερο στοιχείο αναφέρεται ως *μείζον*.

[13] Εδώ χρησιμοποιούμε την έννοια του διαγράμματος εντελώς εμπειρικά, όπου έχουμε κορυφές και ακμές με άκρα κορυφές.



Σχήμα 4.4: *Διάταξη των στοιχείων του συνόλου* $(\mathcal{P}(A), \subseteq)$..

Χωρίς να προχωρήσουμε σε τεχνικές ("δύσκαμπτες") λεπτομέρειες, θα παρουσιάσουμε την φιλοσοφία κατασκευής του διαγράμματος αυτού. Κορυφές του διαγράμματος είναι τα στοιχεία του συνόλου. Ένα στοιχείο του συνόλου είναι μικρότερο (σχετίζεται) ενός άλλου, αν και μόνο αν υπάρχει ένα μονοπάτι (με κατεύθυνση προς τα "άνω"), το οποίο συνδέει τα δύο στοιχεία. [Το μονοπάτι αυτό ενδέχεται να διέρχεται και από άλλα στοιχεία (κορυφές).] Κάθε φορά που κινούμαστε στο διάγραμμα κατά μήκος ενός μονοπατιού από κάτω προς τα άνω, στοιχεία, τα οποία βρίσκονται στο "ίδιο επίπεδο" δεν σχετίζονται μεταξύ τους. Όπως επίσης, ένα στοιχείο, το οποίο βρίσκεται σε ένα επίπεδο δεν μπορεί να είναι μικρότερο ενός στοιχείου που βρίσκεται σε κατώτερο επίπεδο.

Όπως βλέπουμε, ο σχεδιασμός ενός διαγράμματος, που παριστά την διάταξη των στοιχείων ενός συνόλου, είναι ένα μάλλον (αλλά πολύ χρήσιμο) διαισθητικό επιχείρημα.

Παρατηρήσεις 4.4.14.

1. Όταν έχουμε παραστήσει ένα μερικά διατεταγμένο σύνολο υπό μορφήν διαγράμματος, τότε παρατηρούμε ότι ένα υποσύνολο, του οποίου τα στοιχεία βρίσκονται σε ένα μονοπάτι, αποτελεί αλυσίδα, σύμφωνα με τον ορισμό που δώσαμε στην αρχή της παραγράφου (σελ. 134). Εξ' ου και ο ορισμός αλυσίδα.

2. Όταν έχουμε να παραστήσουμε το διάγραμμα ενός ολικώς διατεταγμένου συνόλου, τότε όλα τα σημεία βρίσκονται σε μια κάθετη γραμμή και συνδέονται με ένα μονοπάτι. Σημειωτέον ότι σε κάθε επίπεδο βρίσκεται ακριβώς ένα στοιχείο (σε ένα ολικώς διατεταγμένο σύνολο δεν υπάρχουν στοιχεία που δεν σχετίζονται μεταξύ τους.

   Στο άλλο άκρο, όταν έχουμε να παραστήσουμε, σε διάγραμμα, τα στοιχεία ενός ολικώς μη διατεταγμένου συνόλου, τότε αυτά μπορούν να τοποθετηθούν σε μια οριζόντια γραμμή (ένα επίπεδο), αλλά χωρίς να συνδέονται μεταξύ τους με ένα μονοπάτι.

3. Θα πρέπει να παρατηρήσουμε ότι, όπως το παρουσιάσαμε, σε ένα διάγραμμα, το οποίο παριστά τα στοιχεία ενός μερικώς διατεταγμένου συνόλου δεν αναπαριστάται η αυτοπαθής ιδιότητα της μερικής διάταξης.

Ερώτηση Εάν θέλουμε να αναπαραστήσουμε την αυτοπαθή ιδιότητα, πώς θα "συμπληρώσουμε" το διάγραμμα;

Όπως αντιλαμβανόμαστε, εάν έχουμε ένα (μη κενό) σύνολο A, τότε το πλήθος των μερικών διατάξεων που μπορούν να ορισθούν στο σύνολο αυτό εξαρτάται από το πλήθος των στοιχείων και όχι από την φύση των στοιχείων του. Δεν ξεχνάμε ότι μια μερική διάταξη είναι ένα υποσύνολο του καρτεσιανού γινομένου $A \times A$. Με την βοήθεια των διαγραμμάτων μπορείτε να προσπαθήσετε να "ανακαλύψετε" όλες τις μερικές διατάξεις, οι οποίες μπορούν να ορισθούν σε ένα σύνολο με δύο, τρία ή τέσσερα στοιχεία. Όπως θα διαπιστώσετε, το πλήθος τους αυξάνει ραγδαία, σε σχέση με το πλήθος των στοιχείων του συνόλου. Εκεί θα διαπιστώσετε ότι κάποιες μερικές διατάξεις είναι *ίδιες* (ισόμορφες). Στο τέλος της παραγράφου θα επανέλθουμε.

Έστω $(A, \leq)$ ένα μερικώς διατεταγμένο σύνολο. Υποθέτουμε ότι έχουμε δύο διαφορετικά στοιχεία a και b, τα οποία σχετίζονται μεταξύ τους, δηλαδή ισχύει $a \leq b$ και $a \neq b$. Τότε έχει επικρατήσει να γράφουμε $a < b$.

Ένα μερικά διατεταγμένο σύνολο $(A, \leq)$, θα λέμε ότι, *υπακούει* στον νόμο της τριχοτομίας, αν για κάθε δύο στοιχεία $a, b \in A$ ισχύει ακριβώς μια από τις σχέσεις

$$a < b, a = b, b < a.$$

Ο νόμος της τριχοτομίας δεν είναι τίποτα άλλο από μια ισοδύναμη εκδοχή του ολικά διατεταγμένου συνόλου.

Πρόταση 4.4.15. *Ένα μερικά διατεταγμένο σύνολο $(A, \leq)$ υπακούει στον νόμο της τριχοτομίας, αν και μόνο αν είναι ολικά διατεταγμένο.*

Απόδειξη. Η απόδειξη είναι εύκολη και απλά στηρίζεται στη σύγκριση των δύο ορισμών. ό.έ.δ.

Έστω $(A, \leq)$ ένα μερικώς διατεταγμένο σύνολο και B ένα υποσύνολό του A. Τότε, ως γνωστόν, η μερική διάταξη $\leq$ επάγει, δια του περιορισμού της, μια μερική διάταξη $\leq_B$ επί του B (την οποία, όταν δεν υπάρχει το ενδεχόμενο σύγχυσης, θα συμβολίζουμε πάλι $\leq$). Η μελέτη του μερικά διατεταγμένου συνόλου $(B, \leq)$ αφορά την "συμπεριφορά" της μερικής διάταξης "τοπικά".

Ορισμός 4.4.16. Έστω $(A, \leq)$ ένα μερικώς διατεταγμένο σύνολο και $b \in A$. Ένα $a \in A$ θα ονομάζεται ο **αμέσως επόμενος** του b, αν

$$b \leq a \text{ και δεν υπάρχει } x \in A \text{ με } b < x < a.$$

Δυϊκά ορίζεται ο **αμέσως προηγούμενος** ενός $b \in A$.

Ενδέχεται ένα στοιχείο $b \in A$ να έχει πολλούς αμέσως επόμενους/προηγούμενους ή και να μην υπάρχουν αμέσως επόμενοι/προηγούμενοι. Προφανώς, σε ένα ολικά διατεταγμένο σύνολο ένας αμέσως επόμενος/προηγούμενος ενός στοιχείου, αν υπάρχει, είναι μοναδικός (γιατί;).

Ορισμοί 4.4.17. Έστω B ένα υποσύνολο του μερικώς διατεταγμένου συνόλου $(A, \leq)$.

1. Ένα $a \in A$ ονομάζεται **άνω φράγμα** του B, αν

$$\text{για κάθε } b \in B \text{ ισχύει } b \leq a.$$

Δυϊκά ορίζεται το **κάτω φράγμα** ενός υποσυνόλου.

Αν υπάρχει άνω (αντιστ. κάτω) φράγμα για ένα υποσύνολο B, τότε το B θα ονομάζεται άνω (αντιστ. κάτω) φραγμένο.

2. Ένα $a \in A$ ονομάζεται το **ελάχιστο άνω φράγμα** του B, αν είναι άνω φράγμα του B και για κάθε άλλο άνω φράγμα c του B ισχύει $a \leq c$.

   Δυϊκά ορίζεται το **μέγιστο κάτω φράγμα** ενός υποσυνόλου.

3. Στην περίπτωση όπου το ελάχιστο άνω (αντίστοιχ. μέγιστο κάτω) φράγμα του B, έστω a, είναι στοιχείο του υποσυνόλου B ($a \in B$), τότε το a θα ονομάζεται το **μέγιστο** (αντίστοιχα το **ελάχιστο**) στοιχείο του υποσυνόλου B.[14]

Πρέπει να επισημανθεί ότι, όταν ομιλούμε για άνω (αντίστ. κάτω) φράγμα ενός υποσυνόλου ενός μερικώς διατεταγμένου συνόλου, το φράγμα αυτό, αφ' ενός μεν δεν είναι, κατ' ανάγκην, μοναδικό, αφ' ετέρου δεν ανήκει, κατ' ανάγκην, στο υποσύνολο.

Τουναντίον, όταν ομιλούμε για το ελάχιστο άνω (αντίστ. μέγιστο κάτω) φράγμα ενός υποσυνόλου ενός μερικώς διατεταγμένου συνόλου, το φράγμα αυτό είναι μοναδικό (γιατί;).[15]

Για παράδειγμα, στο ανοικτό διάστημα $(0, 1)$ των πραγματικών όλοι οι αρνητικοί αριθμοί αποτελούν κάτω φράγματα, δεν υπάρχει ελάχιστο στοιχείο (δηλαδή δεν υπάρχει $a \in (0, 1)$ με την ιδιότητα: $a \leq x$ για κάθε $x \in (0, 1)$), ούτε μέγιστο στοιχείο. Ενώ υπάρχει μοναδικό μέγιστο κάτω φράγμα, το 0 ($\inf(0, 1) = 0$) και μοναδικό ελάχιστο άνω φράγμα, το 1 ($\sup(0, 1) = 1$).

Ορισμός 4.4.18. Ένα μερικώς διατεταγμένο σύνολο $(A, \leq)$ θα ονομάζεται **καλώς διατεταγμένο** αν κάθε μη κενό υποσύνολό του B έχει ελάχιστο στοιχείο. Δηλαδή,

$$\text{υπάρχει } b_0 \in B \text{ έτσι ώστε } b_0 \leq b, \text{ για κάθε } b \in B.$$

Ένα καλώς διατεταγμένο σύνολο είναι ολικώς διατεταγμένο. Πράγματι, αν το σύνολο είναι μονοσύνολο, τότε προφανώς ο ισχυρισμός ισχύει. Αν το σύνολο έχει τουλάχιστον δύο στοιχεία, τότε κάθε υποσύνολό του, με δύο στοιχεία, έχει ελάχιστο στοιχείο. Δηλαδή ανά δύο τα στοιχεία του συνόλου σχετίζονται.

Το αντίστροφο δεν ισχύει. Πράγματι, το σύνολο $(\mathbb{Z}, \leq)$ των ακεραίων, με την συνήθη διάταξη, είναι ολικώς διατεταγμένο, αλλά δεν είναι καλώς διατεταγμένο, διότι το υποσύνολο των αρνητικών ακεραίων δεν έχει αρχικό στοιχείο. Τουναντίον, το σύνολο $(\mathbb{N}, \leq)$ είναι καλώς διατεταγμένο. [16]

Προηγουμένως (ιδέ σελίδα 138) είχαμε αναφερθεί στις ισόμορφες διατάξεις. Για να εντυφήσουμε περισσότερο είμαστε αναγκασμένοι να κάνουμε ένα πρωθύστερο και να επικαλεσθούμε την έννοια της απεικόνισης. Ένας, ο οποίος είναι εξοικειωμένος με τις απεικονίσεις, μπορεί άνετα να συνεχίσει. Για έναν, ο οποίος δεν είναι εξοικειωμένος, συνιστούμε, όταν μελετήσει την έννοια της απεικόνισης (Παράγραφο 4.5.2), να επανέλθει.

Ορισμός 4.4.19.

i. Έστω $(A, \leq_A)$, $(B, \leq_B)$ δύο μερικώς διατεταγμένα σύνολα και $f : A \longrightarrow B$ μια απεικόνιση. Η f διατηρεί τις διατάξεις, αν,

$$\text{για όλα τα } x, y \in A, \text{ η σχέση } x \leq_A y \text{ συνεπάγεται την } f(x) \leq_B f(y).$$

[14] Το μέγιστο και το ελάχιστο στοιχείο ενός υποσυνόλου (αν υπάρχουν), ορισμένες φορές, ονομάζονται το τελικό και το αρχικό στοιχείο του υποσυνόλου αντίστοιχα.

[15] Το μοναδικό ελάχιστο άνω (αντίστοιχ. μέγιστο κάτω) φράγμα είθισται να ονομάζεται supremum του B (αντίστ. infimum του B) και συμβολίζονται $\sup B$ και $\inf B$ αντίστοιχα.

[16] Το ότι το σύνολο των φυσικών αριθμών είναι καλώς διατεταγμένο, είναι ισοδύναμο με το αξίωμα της Μαθηματικής Επαγωγής. Όταν, αργότερα, θα ορίσουμε αυστηρά το σύνολο των φυσικών αριθμών, τότε θα επανέλθουμε επ' αυτού, ιδέ το Θεώρημα A.1.10 και το Θεώρημα A.1.12.

ii. Έστω $(A, \leq_A)$, $(B, \leq_B)$ δύο μερικώς διατεταγμένα σύνολα και $f : A \longrightarrow B$ μια απεικόνιση. Η f ονομάζεται **ισομορφισμός διατάξεων**, αν είναι 1-1 και επί και αν, τόσον η f, όσον και η f^{-1} διατηρούν τις διατάξεις.

Θα αναφέρουμε μόνο μια πρόταση και δεν θα επεκταθούμε περισσότερο αφήνοντας μερικά "προφανή" μεν, σημαντικά δε αποτελέσματα, ως ασκήσεις.

Πρόταση 4.4.20. *Έστω $(A, \leq_A)$ ένα ολικώς διατεταγμένο σύνολο και $(B, \leq_B)$ ένα μερικώς διατεταγμένο σύνολο και $f : A \longrightarrow B$ μια απεικόνιση, η οποία είναι επί και διατηρεί τις διατάξεις. Το σύνολο $(B, \leq_B)$ είναι ολικώς διατεταγμένο.*

Απόδειξη. Έστω $r, s \in B$. Πρέπει να δείξουμε ότι αυτά σχετίζονται μέσω της $\leq_B$.

Επειδή η f είναι επί, υπάρχουν $x, y \in A$ με $f(x) = r$ και $f(y) = s$. Το σύνολο A έχει υποτεθεί ολικώς διατεταγμένο, άρα ισχύει

$$x \leq_A y, \text{ ή } y \leq_A x.$$

Η f διατηρεί τις διατάξεις, επομένως

$$f(x) \leq_B f(y), \text{ ή } f(y) \leq_B f(x).$$

Συνεπώς,

$$r \leq_B s, \text{ ή } s \leq_b r.$$

Τα $r, s \in B$ είναι τυχαία. Δηλαδή η $\leq_B$ είναι ολική διάταξη (Ορισμός 4.4.8). ό.έ.δ.

Επεκτάσεις μερικών διατάξεων.

Έστω $(A, \leq)$ ένα ολικά διατεταγμένο σύνολο. Δεν ξεχνάμε ότι η σχέση ολικής διάταξης $\leq$ είναι ένα υποσύνολο του καρτεσιανού γινομένου $A \times A$, όπου για κάθε δύο στοιχεία $a, b \in A$, ισχύει

$$(a, b) \in \leq \text{ ή } (b, a) \in \leq \quad (a \leq b, \text{ ή } b \leq a).$$

Αν από την σχέση αυτή διαγράψουμε ορισμένα ζεύγη, τότε ενδέχεται να προκύπτει μια "άλλη" σχέση, η οποία να είναι σχέση μερικής διάταξης στο σύνολο A.

Παράδειγμα 4.4.21. Έστω $(\mathbb{Z}, \leq)$ το ολικά διατεταγμένο σύνολο των ακεραίων. Από την σχέση

$$\leq = \{\ldots, (-1, -1), (-1, 0), \ldots, (1, 2), (1, 3), \ldots\}$$

"εξαιρούμε" το ζεύγος $(1, 2)$, δηλαδή θεωρούμε ότι οι αριθμοί 1 και 2 δεν σχετίζονται μεταξύ τους, τότε η εναπομείνασα σχέση

$$\leq = \leq \setminus (1, 2),$$

προφανώς, είναι σχέση μερικής διάταξης στο σύνολο των ακεραίων.

Το ερώτημα, που προκύπτει, είναι, αν ισχύει το αντίστροφο. Δηλαδή, αν έχουμε ένα μερικώς διατεταγμένο σύνολο $(A, \leq)$, μπορούμε να "επεκτείνουμε" την υπάρχουσα σχέση μερικής διάταξης σε μια σχέση ολικής διάταξης επισυνάπτοντας ορισμένα διατεταγμένα ζεύγη στην ήδη υπάρχουσα σχέση; Συγκεκριμένα αναζητούμε μια σχέση ολικής διάταξης, έστω $\preceq$, η οποία να έχει την ιδιότητα:

$$\text{Αν } a \leq b \text{ τότε } a \preceq b.$$

Θα απαντήσουμε στο ερώτημα αυτό στην περίπτωση όπου έχουμε ένα πεπερασμένο μερικώς διατεταγμένο σύνολο.

Λήμμα 4.4.22. *Έστω $(A, \leq)$ ένα πεπερασμένο μερικώς διατεταγμένο σύνολο. Τότε το σύνολο έχει μικρότερο στοιχείο.*

Απόδειξη. Επιλέγουμε ένα $a_1 \in A$ (όπως πάντα, θεωρούμε το A μη κενό). Αν αυτό είναι μικρότερο στοιχείο, έχει καλώς. Υποθέτουμε ότι δεν είναι μικρότερο. Τότε, σύμφωνα με τον ορισμό μικροτέρου στοιχείου (Ορισμός 4.4.10) υπάρχει $a_2 \in A$ έτσι ώστε $a_2 \leq a_1$. Αν το a_2 είναι μικρότερο στοιχείο, έχει καλώς. Διαφορετικά συνεχίζουμε. Επειδή το σύνολο A είναι πεπερασμένο, τελικά καταλήγουμε[17] ότι υπάρχει (τουλάχιστον) ένα μικρότερο στοιχείο στο σύνολο A. ό.έ.δ.

Θεώρημα 4.4.23. *Έστω $(A, \leq)$ ένα πεπερασμένο μερικώς διατεταγμένο σύνολο. Τότε, στο σύνολο A, μπορούμε να ορίσουμε μια σχέση ολικής διάταξης, έστω $\preceq$, η οποία επεκτείνει την υπάρχουσα μερική διάταξη $\leq$.*

Απόδειξη. Σύμφωνα με το προηγούμενο λήμμα, το σύνολο A έχει μικρότερο στοιχείο έστω a_0. Λαμβάνουμε το σύνολο

$$A_1 = A \setminus \{a_0\}.$$

Αν το σύνολο αυτό είναι το κενό σύνολο, τότε το αρχικό σύνολο είναι μονοσύνολο και έχουμε τελειώσει. Υποθέτουμε ότι το σύνολο αυτό δεν είναι το κενό σύνολο. Τότε, από το προηγούμενο λήμμα, το σύνολο αυτό έχει (τουλάχιστον) ένα μικρότερο στοιχείο. Έστω a_1 ένα από αυτά τα μικρότερα στοιχεία. Ξεκινάμε και ορίζουμε την νέα διάταξη ως εξής: Ορίζουμε $a_0 \preceq a_1$. Έστω τώρα το σύνολο

$$A_2 = A_1 \setminus \{a_1\}.$$

Αν το σύνολο αυτό είναι το κενό, τότε έχουμε τελειώσει. Υποθέτουμε ότι δεν είναι το κενό. Τότε, πάλι από το προηγούμενο λήμμα, το σύνολο αυτό έχει (τουλάχιστον) ένα μικρότερο στοιχείο. Έστω a_2 ένα από αυτά τα μικρότερα στοιχεία. Συνεχίζουμε τον ορισμό της νέας διάταξης ορίζοντας $a_1 \preceq a_2$. Η διαδικασία αυτή συνεχίζεται μέχρι εξαντλήσεως όλων των στοιχείων του αρχικού συνόλου A, το οποίο έχει υποτεθεί πεπερασμένο.

Προφανώς η νέα σχέση διάταξης $\preceq$ είναι ολική διάταξη (γιατί;). Επίσης, αποτελεί επέκταση της αρχικής μερικής διάταξης $\leq$, καθότι, από τον τρόπο ορισμού της, αν $a \leq b$ τότε $a \preceq b$. ό.έ.δ.

Παρατήρηση 4.4.24. Όπως παρατηρούμε, από τον τρόπο "κατασκευής" της ολικής διάταξης, η διάταξη αυτή δεν είναι μοναδική. Πράγματι, σε κάθε στάδιο, όταν υπάρχουν περισσότερα του ενός μικρότερα στοιχεία, έχουμε την ευχέρεια να επιλέξουμε ένα (τυχαίο) από αυτά και να συνεχίσουμε.

Παράδειγμα 4.4.25. Έστω το σύνολο

$$A = \{2, 3, 4, 6, 9, 10, 12\}$$

εφοδιασμένο με την επαγόμενη σχέση $|$ διαιρετότητας, η οποία είναι μερική διάταξη. Θέλουμε να ορίσουμε μια ολική διάταξη, έστω $\preccurlyeq$, η οποία να επεκτείνει την διάταξη $|$. Παρατηρούμε ότι το σύνολο A έχει δύο μικρότερα στοιχεία, το 2 και το 3. Επιλέγουμε (τυχαία/αυθαίρετα) ένα από αυτά, έστω το 3, τότε το σύνολο

$$A_1 = A \setminus \{3\}$$

[17] Εδώ δεν κάνουμε χρήση του ορισμού ενός πεπερασμένου συνόλου,...αρκούμαστε στην διαίσθησή μας.

έχει δύο μικρότερα στοιχεία, το 2 και το 9 (γιατί αυτά είναι τα μικρότερα στοιχεία του A_1;). Επιλέγουμε ένα από αυτά, έστω το 9, και ορίζουμε $3 \preccurlyeq 9$. Το σύνολο

$$A_2 = A_1 \setminus \{9\}$$

έχει μόνο ένα μικρότερο στοιχείο, το 2 (γιατί;), οπότε (αναγκαστικά) επιλέγουμε αυτό και ορίζουμε $9 \preccurlyeq 2$. Οπότε, προς το παρόν, έχουμε $3 \preccurlyeq 9 \preccurlyeq 2$. Συνεχίζουμε με το σύνολο

$$A_3 = A_2 \setminus \{2\} = \{4, 6, 10, 12\}.$$

Το σύνολο αυτό έχει τρία μικρότερα στοιχεία, τα 4, 6 και 10 (γιατί;). Επιλέγουμε ένα από αυτά έστω το 10 και ορίζουμε $2 \preccurlyeq 10$. Συνεχίζοντας ορίζουμε διαδοχικά

$$10 \preccurlyeq 6 \preccurlyeq 4 \preccurlyeq 12.$$

Οπότε, τελικά έχουμε ορίσει στο σύνολο A την εξής ολική διάταξη

$$3 \preccurlyeq 9 \preccurlyeq 2 \preccurlyeq 10 \preccurlyeq 6 \preccurlyeq 4 \preccurlyeq 12.$$

Η διάταξη αυτή είναι ολική και αποτελεί επέκταση της αρχικής διάταξης $|$. Για παράδειγμα έχουμε ότι

$$6 \mid 12 \implies 6 \preccurlyeq 12.$$

Όπως βλέπουμε, μπορούμε (προσπαθήστε το!) να ορίσουμε πολλές ολικές διατάξεις, οι οποίες επεκτείνουν την αρχική μερική διάταξη $|$.

Παρατήρηση 4.4.26. Όπως είδαμε, κάθε μερική διάταξη σε ένα πεπερασμένο σύνολο μπορεί να επεκταθεί σε μία ολική διάταξη. Επομένως, γεννάται το ερώτημα: Μπορούμε να ισχυρισθούμε ότι κάτι ανάλογο συμβαίνει και σε σύνολα με άπειρο το πλήθος στοιχεία;

Εδώ ισχύει ένα διαφορετικής υφής αποτέλεσμα. "Σε κάθε (μη κενό) σύνολο μπορούμε να ορίσουμε μια καλή διάταξη". Ο ισχυρισμός αυτός είναι ισοδύναμος με το "Αξίωμα της επιλογής". Επ' αυτού δεν θα επεκταθούμε περισσότερο, αλλά στην περίπτωση των αριθμησίμων συνόλων θα δώσουμε μια απόδειξη (ιδέ Θεώρημα B.2.15).

Η λεξικογραφική διάταξη.

Για να είναι εύχρηστο ένα λεξικό, οι λέξεις πρέπει να είναι γραμμένες σε (αυστηρή) αλφαβητική σειρά. Το πώς επιτυγχάνεται αυτό, θα το δούμε στην συνέχεια.

Έστω $(A_1, \preceq_1)$ και $(A_2, \preceq_2)$ δύο μερικώς διατεταγμένα σύνολα. Στο καρτεσιανό γινόμενο $A_1 \times A_2$ θα ορίσουμε μια μερική διάταξη, έστω $\preceq$, επαγομένη από τις μερικές διατάξεις $\preceq_1$ και $\preceq_2$. Έστω $(a_1, a_2), (b_1, b_2) \in A_1 \times A_2$, ορίζουμε

$$(a_1, a_2), \preceq (b_1, b_2) \text{ αν, } \begin{array}{l} \text{είτε } a_1 \preceq_1 b_1, \\ \text{είτε } a_1 = b_1 \text{ και } a_2 \preceq_2 b_2. \end{array}$$

Είναι εύκολο (προσπαθήστε το!) να αποδείξουμε ότι το σύνολο $(A_1 \times A_2, \preceq)$ είναι μερικώς διατεταγμένο σύνολο.

Ορισμός 4.4.27. Η μερική διάταξη $\preceq$, η οποία ορίστηκε προηγουμένως ονομάζεται *λεξικογραφική* διάταξη επαγομένη από τις μερικές διατάξεις $\preceq_1$ και $\preceq_2$.

Παρατήρηση 4.4.28. Αν τα σύνολα $(A_1, \preceq_1)$ και $(A_2, \preceq_2)$ είναι ολικώς διατεταγμένα, τότε έπεται ότι και το σύνολο $(A_1 \times A_2, \preceq)$ είναι ολικώς διατεταγμένο. Επιπλέον, αν τα σύνολα $(A_1, \preceq_1)$ και $(A_2, \preceq_2)$ είναι καλώς διατεταγμένα, τότε έπεται ότι και το σύνολο $(A_1 \times A_2, \preceq)$ είναι καλώς διατεταγμένο.

Μπορούμε να γενικεύσουμε την ανωτέρω "κατασκευή" και να ορίσουμε λεξικογραφική διάταξη επί ενός καρτεσιανού γινομένου μερικώς διατεταγμένων συνόλων.

Έστω ότι τα σύνολα

$$(A_1, \preceq_1), (A_2, \preceq_2), \ldots, (A_n, \preceq_n)$$

είναι μερικώς διατεταγμένα σύνολα. Στο καρτεσιανό γινόμενο $A_1 \times A_2 \times \cdots A_n$ ορίζουμε μια μερική διάταξη, έστω $\preceq$, ως εξής:

$$\begin{aligned}(a_1, a_2, \ldots, a_n) \preceq (b_1, b_2, \ldots, b_n)\ \alpha\nu, \quad & \text{είτε} \quad a_1 \preceq_1 b_1, \\ & \text{είτε} \quad \text{υπάρχει } i > 0 \text{ με} \\ & \qquad a_1 = b_1, \ldots, a_i = b_i \text{ και} \\ & \qquad a_{i+1} \preceq_{i+1} b_{i+1}.\end{aligned}$$

Πράγματι, η διάταξη $\preceq$ είναι μια μερική διάταξη επί του καρτεσιανού γινομένου $A_1 \times A_2 \times \cdots A_n$.

Θα μπορούσαμε να περιγράψουμε την ανωτέρω μερική διάταξη ως εξής: Μια πλειάδα n στοιχείων είναι μικρότερη μιας άλλης πλειάδας n στοιχείων, αν στην πρώτη θέση (ξεκινώντας από αριστερά προς τα δεξιά), όπου οι δύο πλειάδες διαφέρουν, η εγγραφή της πρώτης πλειάδας είναι μικρότερη από την αντίστοιχη εγγραφή της δεύτερης πλειάδας.

Όμως, όπως όλοι γνωρίζουμε, όταν έχουμε να καταγράψουμε τις λέξεις μιας γλώσσας σε ένα λεξικό, υπάρχουν λέξεις με διαφορετικό αριθμό γραμμάτων. Οπότε, η ανωτέρω διαδικασία δεν μπορεί να εφαρμοστεί "κατά γράμμα".

Έστω $(A, \preceq)$ ένα μερικώς διατεταγμένο σύνολο. Θα ορίσουμε μια λεξικογραφική διάταξη $\ll$ επί του συνόλου S όλων των *λέξεων*/ συμβολοσειρών της μορφής

$$a_1, a_2, \ldots, a_n$$

με στοιχεία/χαρακτήρες από το σύνολο A, όπου το μήκος n δεν είναι σταθερό.

Θεωρούμε, κατ' εκδοχή, έναν επιπλέον χαρακτήρα, τον κενό χαρακτήρα ∂, με την παραδοχή $\partial \preceq a$ για κάθε $a \in A$.

Έστω δύο λέξεις $a_1\, a_2 \ldots a_n$ και $b_1\, b_2 \ldots b_m$ με χαρακτήρες από το σύνολο $(A, \preceq)$, όπου τα μήκη n και m δεν είναι κατ' ανάγκη ίσα και έστω $t = \max(n, m)$. Στο τέλος της λέξης με το μικρότερο μήκος επισυνάπτουμε τον κενό χαρακτήρα τόσες φορές, ώστε οι δύο λέξεις να έχουν το ίδιο πλήθος χαρακτήρων. Τώρα συγκρίνουμε τις (ιδίου μήκους) λέξεις, όπως έχουμε δει προηγουμένως, θεωρώντας ότι ανήκουν στο καρτεσιανό γινόμενο

$$\underbrace{A \times A \times \cdots \times A}_{t}.$$

Στο τέλος αγνοούμε τους κενούς χαρακτήρες που επισυνάψαμε.

Εύκολα επαληθεύουμε ότι η διάταξη αυτή είναι μια μερική διάταξη επί του συνόλου S όλων των λέξεων με χαρακτήρες από το σύνολο A. Μάλιστα δε, αν το σύνολο $(A, \preceq)$ είναι ολικώς διατεταγμένο, τότε και το σύνολο $(S, \ll)$ είναι ολικώς διατεταγμένο.

Πρέπει να επισημάνουμε ότι, κάθε φορά που "συγκρίνουμε" δύο λέξεις στο καρτεσιανό γινόμενο

$$\underbrace{A \times A \times \cdots \times A}_{t},$$

το t είναι διαφορετικό και εξαρτάται από τα μήκη των δύο "συγκρινομένων" λέξεων.

Παράδειγμα 4.4.29. Έστω ότι θέλουμε να διατάξουμε λεξικογραφικά τις λέξεις *αλήθεια*, *αληθής*, *αληθείς*, *αληθινός*, όπου στο ελληνικό αλφάβητο έχουμε την γνωστή διάταξη α, β, γ,....

Η λέξη *αληθείς*, αν και με περισσότερους χαρακτήρες, προηγείται της λέξης *αληθής*, ενώ η λέξη *αλήθεια* προηγείται της λέξης *αληθείς*. Οπότε, συνεχίζοντας, τελικά, επιτυγχάνουμε, την ήδη γνωστή, διάταξη *αλήθεια*, *αληθείς*, *αληθής*, *αληθινός*.

Σχόλιο 4.4.30. Θα μπορούσαμε, αντί να επισυνάπτουμε εικονικά τον κενό χαρακτήρα, να ορίσουμε την λεξικογραφική διάταξη $\ll$ επί του συνόλου S διαφορετικά. Έστω δύο λέξεις

$$a_1\, a_2\, \ldots\, a_n \text{ και } b_1\, b_2\, \ldots\, b_m$$

χαρακτήρες από το σύνολο $(A, \preceq)$, όπου τα μήκη n και m δεν είναι κατ' ανάγκη ίσα και έστω $r = \min(n, m)$. Συγκρίνουμε τις λέξεις

$$a_1\, a_2\, \ldots\, a_r \text{ και } b_1\, b_2\, \ldots\, b_r.$$

Αν $a_1\, a_2\, \ldots\, a_r \prec b_1\, b_2\, \ldots\, b_r$ στο καρτεσιανό γινόμενο $\underbrace{A \times A \times \cdots \times A}_{r}$, τότε θέτουμε

$$a_1\, a_2\, \ldots\, a_n \ll b_1\, b_2\, \ldots\, b_m.$$

Αν $a_1\, a_2\, \ldots\, a_r = b_1\, b_2\, \ldots\, b_r$ και $n < m$, τότε θέτουμε

$$a_1\, a_2\, \ldots\, a_n \ll b_1\, b_2\, \ldots\, b_m.$$

Μπορούμε εύκολα (;) να διαπιστώσουμε ότι, με όποιον τρόπο και να ορίσουμε την λεξικογραφική διάταξη $\ll$, στην πραγματικότητα πρόκειται για την ίδια διάταξη.

4.4.4 Ασκήσεις

1. Έστω $(A, \prec)$ ένα προδιατεταγμένο σύνολο. Στο A ορίζουμε μια άλλη σχέση $\sim$ ως εξής:

   $$\text{Για δύο } a, b \in A \text{ ορίζουμε } a \sim b, \text{ αν } a \prec b \text{ και } b \prec a.$$

   Δείξτε ότι η σχέση $\sim$ είναι σχέση ισοδυναμίας. Στο σύνολο πηλίκων $A/\sim$ ορίζουμε μια σχέση $\ll$ ως εξής:

   $$C_a \ll C_b, \text{ αν } a \prec b.$$

   Δείξτε ότι το σύνολο $(A/\sim, \ll)$ είναι μερικά διατεταγμένο.

2. Έστω $(A, \preceq)$ ένα μερικά διατεταγμένο σύνολο. Τότε, ως γνωστόν, ορίζεται η αντίστροφη σχέση $\preceq^{-1}$, όπου, (εξ ορισμού) για $a, b \in A$,

   $$a \preceq^{-1} b \text{ αν και μόνο αν } b \preceq a.$$

   Δείξτε ότι το σύνολο $(A, \preceq^{-1})$ είναι μερικά διατεταγμένο σύνολο και ότι οι έννοιες μεγαλύτερο/μικρότερο, μέγιστο/ελάχιστο στο σύνολο $(A, \preceq)$ *αντιστρέφονται* και γίνονται μικρότερο/μεγαλύτερο, ελάχιστο/μέγιστο στο σύνολο $(A, \preceq)$.

   Σημείωση: Όπως θα έχετε καταλάβει, η αντίστροφη σχέση $\preceq^{-1}$ δεν είναι τίποτε άλλο από τη σχέση $\succeq$ του "μεγαλύτερον ή ίσον".

3. Έστω ένα πεπερασμένο μερικώς διατεταγμένο σύνολο. Δείξτε ότι, στην παράσταση της μερικής διάταξης με έναν πίνακα, αν ένα στοιχείο εκτός της κυρίας διαγωνίου ισούται με 1, τότε το συμμετρικό του ισούται με 0.

4. Έστω το σύνολο $A = \{1, 2, 3, 4, 5, 6\}$. Στο A ορίζουμε μια σχέση $|$ ως εξής:

$$a \mid b \text{ αν ο } \alpha \text{ διαιρεί τον } b.$$

Προφανώς η σχέση αυτή είναι μερική διάταξη. Να βρεθεί ο πίνακας, έστω $M_{|}$, ως προς τη διάταξη αυτή.

5. Να δώσετε ένα παράδειγμα ενός μερικώς διατεταγμένου συνόλου $(A, \leq)$ και ενός $b \in A$, το οποίο να έχει πολλούς αμέσως επόμενους. Όπως και ένα παράδειγμα ενός μερικώς διατεταγμένου συνόλου $(A, \leq)$ και ενός $b \in A$, το οποίο να μην έχει αμέσως επόμενο.

6. Δείξτε ότι το κλειστό διάστημα $[0, 1]$ των πραγματικών αριθμών αν και είναι ολικώς διατεταγμένο σύνολο, δεν είναι καλώς διατεταγμένο.

7. Δείξτε ότι στην περίπτωση ενός πεπερασμένου συνόλου ισχύει και το αντίστροφο. Δηλαδή κάθε μερικώς διατεταγμένο σύνολο είναι καλώς διατεταγμένο.

8. Έστω $(A \leq)$ ένα μερικώς διατεταγμένο σύνολο. Το σύνολο αυτό λέγεται ότι πληροί την ιδιότητα *του ελαχίστου άνω φράγματος*, αν κάθε μη κενό άνω φραγμένο υποσύνολό του έχει ελάχιστο άνω φράγμα. (Δυϊκά ορίζεται η ιδιότητα του μεγίστου κάτω φράγματος).

   i. Έστω $(A \leq)$ ένα μερικώς διατεταγμένο σύνολο και $K \subset A$. Ορίζουμε

   $$L_K = \{x \in A \mid x \text{ είναι ένα κάτω φράγμα του K}\}.$$

   Υποθέτουμε ότι το L_K έχει ελάχιστο άνω φράγμα. Δείξτε ότι αυτό είναι το μέγιστο κάτω φράγμα του K ($supL_K = infK$).

   ii. Έστω $(A \leq)$ ένα μερικώς διατεταγμένο σύνολο, το οποίο πληροί την ιδιότητα του ελαχίστου άνω φράγματος. Δείξτε ότι το σύνολο αυτό πληροί και την ιδιότητα του μεγίστου κάτω φράγματος.

   iii. Δείξε ότι, για κάθε μη κενό σύνολο X, το σύνολο $(\mathcal{P}(X), \subset)$ πληροί την ιδιότητα του ελαχίστου άνω φράγματος.

Το πλέον ενδιαφέρον παράδειγμα συνόλου με την ιδιότητα του ελαχίστου άνω φράγματος είναι το σύνολο των πραγματικών αριθμών $(\mathbb{R}, \leq)$ με την συνήθη διάταξη. Αυτό αναφέρεται ως η αρχή της "**πληρότητας**" για τους πραγματικούς αριθμούς και, ανάλογα με τον τρόπο ορισμού των πραγματικών αριθμών είτε αποδεικνύεται ή τείθεται ως αξίωμα. Επ' αυτού θα επανέλθουμε αργότερα (ιδέ Πρόταση 7.1.11).

9. Έστω $(A \leq)$ ένα μερικώς διατεταγμένο σύνολο και $X \subseteq Y \subseteq A$.

Υποθέτουμε ότι όλα τα ελάχιστα άνω (supremum) και όλα τα μέγιστα κάτω (infimum) φράγματα υπάρχουν. Δείξτε ότι:

$$inf(Y) \leq inf(X) \leq sup(X) \leq sup(Y).$$

Να βρεθούν δύο υποσύνολα X και Y του $(\mathbb{R}, \leq)$ με το X να είναι γνήσιο υποσύνολο του Y, αλλά να ισχύει

$$inf(Y) = inf(X) \text{ και } sup(X) = sup(Y).$$

10. Έστω το σύνολο $A = \{0, 1\}$ εφοδιασμένο με τη διάταξη $0 \leq 1$. Να διατάξετε λεξικογραφικά τις συμβολοσειρές

$$1,\ 0,\ 1\,0,\ 1\,1\,0,\ 1\,0\,0\,1,\ 1\,1\,1\,1,\ 1\,0\,1\,1$$

Τι παρατηρείτε;

11. Έστω το σύνολο $S = \{2, 3, 4, 5\}$ εφοδιασμένο με την γνωστή διάταξη του μικρότερον ή ίσον. Στο σύνολο $S \times S$, εφοδιασμένο με την λεξικογραφική διάταξη, να βρείτε όλα τα ζεύγη (a, b) με

$$(3, 4) \leq (a, b) \leq (5, 3).$$

12. Να αποδείξετε τον ισχυρισμό που αναφέρεται στην Παρατήρηση 4.4.28.

13. Έστω $(A, \leq_A)$, $(B, \leq_B)$ δύο μερικώς διατεταγμένα σύνολα και $f : A \longrightarrow B$ μια απεικόνιση, η οποία είναι 1-1. Τα ακόλουθα είναι ισοδύναμα.

    i. Η f είναι ισομορφισμός διατάξεων.

    ii. Για όλα τα $x, y \in A$, ισχύει ότι $x \leq_A y$, αν και μόνο αν $f(x) \leq_B f(y)$.

4.5 Απεικονίσεις/Συναρτήσεις

Είδαμε ότι η έννοια του συνόλου είναι θεμελιώδης στα Μαθηματικά, αλλά χωρίς την έννοια της συνάρτησης μεταξύ δύο συνόλων τα σύνολα παραμένουν απλώς "συλλογές αντικειμένων". Όλοι έχουμε μια προπαιδεία, κυρίως από τον Λογισμό επί του συνόλου των πραγματικών αριθμών, για την έννοια της συνάρτησης και την "χρήση" αυτής της έννοιας. Αλλά η σημασία της έννοιας αυτής είναι πέραν της συνήθους χρήσης της στον Λογισμό των πραγματικών αριθμών. Αλλά τι είναι μια συνάρτηση;

Για παράδειγμα, βλέπουμε την συνάρτηση $f(x) = x^2$ και, περισσότερο διαισθητικά, παρά αυστηρά Μαθηματικά, εννοούμε ότι στον (κάθε) αριθμό x "αντιστοιχούμε" το (μοναδικό) τετράγωνό του x^2.

Παρ' όλα ταύτα, μια συνάρτηση δεν είναι μόνο ένας "τύπος", που σχετίζει δύο αριθμούς (στο προηγούμενο παράδειγμα τον αριθμό x με το τετράγωνό του x^2). Για παράδειγμα, θα μπορούσαμε να ορίσουμε μια συνάρτηση μεταξύ του συνόλου όλων των κατοίκων της γης και του συνόλου των ημερών ενός έτους (θεωρώντας ότι ο Φεβρουάριος έχει 29 ημέρες), όπου σε κάθε άτομο αντιστοιχούμε την μοναδική ημερομηνία των γενεθλίων του.

Ας "αναπαράγουμε" έναν, διαισθητικό, ορισμό της συνάρτησης.

Ορισμός 4.5.1. Μια συνάρτηση μεταξύ του συνόλου A και του συνόλου B είναι ένας "κανόνας/διαδικασία", που "σχετίζει/συνδέει" κάθε στοιχείο του συνόλου A με ένα μόνο στοιχείο του συνόλου B.

Στον ορισμό αυτό δεν υπάρχει κάτι το εμφανώς μη σωστό, αλλά δεν μας λέει και κάτι συγκεκριμένο. Καθότι δεν είναι πλήρως και διαυγώς καθορισμένο τι σημαίνει "κανόνας/διαδικασία" και τι σημαίνει "σχετίζει/συνδέει". Μια έκφραση του τύπου "συναρτά" κάθε στοιχείο του συνόλου A με ένα μόνο στοιχείο του συνόλου B αποτελεί αυτοεπίκληση. Παρ' όλα ταύτα, για έναν ο οποίος βρίσκεται στην αρχή της σπουδής των Μαθηματικών, είναι ένας "επαρκής" ορισμός.

Στο παράδειγμα, όπου αντιστοιχούμε σε κάθε αριθμό το τετράγωνό του, ο κανόνας είναι ο εξής:

> "Πολλαπλασιάζουμε κάθε αριθμό με τον εαυτό του και σχετίζουμε τον αριθμό αυτόν με το τετράγωνό του" ($f(x) = x^2$).

Στο παράδειγμα, όπου σχετίζουμε κάθε άνθρωπο με την ημερομηνία των γενεθλίων του, δεν έχουμε κάποιον "τύπο" που να περιγράφει την διαδικασία αυτή. Παρ' όλα ταύτα, μπορούμε να σχηματίσουμε όλα τα ζεύγη, π.χ. της μορφής

(Δημήτριος Βάρσος, 30 Νοεμβρίου), (Κωστής Παλαμάς, 13 Ιανουαρίου),....

Αλλά και στο πρώτο παράδειγμα μπορούμε να σχηματίσουμε όλα τα ζεύγη, π.χ. της μορφής

$$(0, 0), (-2, 4), (2, 4), ...$$

Σε μια άλλη περίπτωση, ο κανόνας/διαδικασία εισόδου–εξόδου, θα μπορούσε να είναι ένα πρόγραμμα σε υπολογιστή[18], ένας πίνακας, μια προφορική (ή γραπτή) περιγραφή κ.λ.π. Επομένως, οδηγούμαστε στον εξής Ορισμό, ο οποίος αίρει κάθε αμφιβολία και δυσπιστία.

Ορισμός 4.5.2. Έστω A και B δύο σύνολα. Μια **συνάρτηση** ή **απεικόνιση** από το σύνολο A στο σύνολο B είναι μια σχέση, δηλαδή ένα υποσύνολο $\mathrm{F} \subset A \times B$ με την ιδιότητα:

> Για **κάθε** $a \in A$ υπάρχει **μοναδικό** $b \in B$ με $(a, b) \in \mathrm{F}$.

Το σύνολο A θα ονομάζεται **πεδίο ορισμού** και το σύνολο B θα ονομάζεται **πεδίο τιμών** της F.

Παρατηρήσεις 4.5.3.

1. Οι λέξεις συνάρτηση και απεικόνιση (εξ ορισμού) εκφράζουν την ίδια Μαθηματική έννοια και επομένως μπορούν να χρησιμοποιούνται αδιακρίτως. Εδώ θα χρησιμοποιούμε τον όρο απεικόνιση και μόνο, όταν αναφερόμαστε σε *επώνυμες* συναρτήσεις, π.χ., συνάρτηση του Euler, θα χρησιμοποιούμε τον όρο συνάρτηση.

2. Δεδομένου ότι μια απεικόνιση είναι μια σχέση μεταξύ δύο συνόλων, μπορούμε να μιλάμε για απεικονίσεις 1-1, για απεικονίσεις επί, για σύνθεση απεικονίσεων κ.λ.π. Στα επόμενα θα μελετήσουμε διεξοδικά αυτές τις ιδιότητες των απεικονίσεων.

3. Μια απεικόνιση, όπως όλες οι σχέσεις, θα μπορούσε να παρασταθεί με πολλούς τρόπους, όπως με βελοειδή διαγράμματα, πίνακες κ.λ.π. Στην περίπτωση, όπου το πεδίο ορισμού και το πεδίο τιμών είναι το σύνολο των πραγματικών αριθμών ή υποσύνολά του, τότε μπορεί να παρασταθεί με ένα γράφημα (ιδέ τα παραδείγματα που ακολουθούν).

[18] Φανταστείτε την "αόρατη" διαδικασία στο εσωτερικό ενός υπολογιστή, όπου μέσω αυτής σε κάθε τετραγωνικό πίνακα επιτυγχάνεται η αντιστοίχιση με την μοναδική ορίζουσά του.

4. Όπως σε όλες τις σχέσεις μεταξύ δύο συνόλων, θα μπορούσαμε να χρησιμοποιήσουμε τον γενικό συμβολισμό μιας απεικόνισης F ως εξής:

$$\mathrm{F} \subset A \times B \text{ ή } (a, b) \in \mathrm{F} \text{ ή } a\,\mathrm{F}\,b.$$

Αντ' αυτού του συμβολισμού έχει καθιερωθεί ο (γνωστός) συμβολισμός

$$F : A \longrightarrow B$$

όπου για κάθε $x \in A$ με $F(x)$ θα παριστούμε το μοναδικό στοιχείο του B για το οποίο ισχύει ότι $(x, F(x)) \in \mathrm{F}$. Το $F(x)$ θα ονομάζεται *εικόνα* του (προτύπου) x μέσω της F.

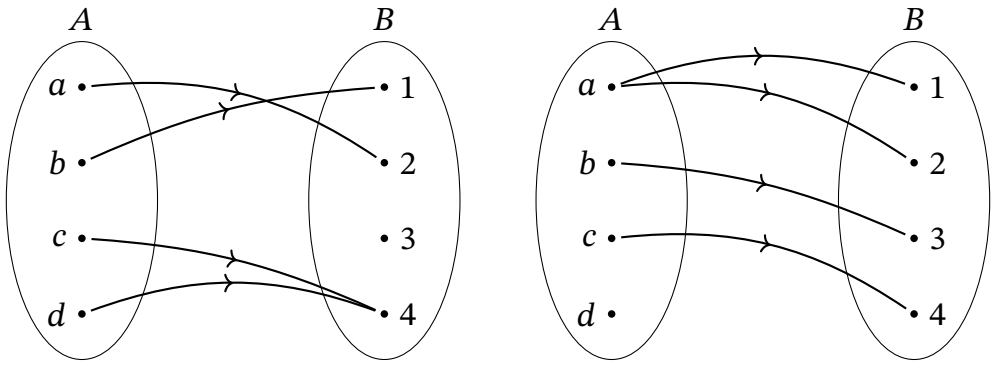
Εδώ πρέπει να επισημάνουμε ότι, λανθασμένα χρησιμοποιούμε την έκφραση "η απεικόνιση $F(x)$", αντί του ορθού "η απεικόνιση F". Όλα αυτά βέβαια υπό την προϋπόθεση ότι έχει διευκρινιστεί ποιο είναι το πεδίο ορισμού και ποιο το πεδίο τιμών.

5. Όταν μας δίνεται μια απεικόνιση $f : A \longrightarrow B$, συνήθως κάθε στοιχείο x του πεδίου ορισμού ονομάζεται ανεξάρτητη μεταβλητή, ενώ η εικόνα του $y = f(x)$ ονομάζεται εξαρτημένη μεταβλητή.

6. Προφανώς, όταν ένα από τα δύο σύνολα (πεδίο ορισμού, πεδίο τιμών) είναι το κενό σύνολο, τότε η μόνη σχέση που ορίζεται μεταξύ των δύο αυτών συνόλων είναι η κενή σχέση και δεν έχουμε κάτι να πούμε επ' αυτής. Επομένως, όταν αναφερόμαστε σε απεικονίσεις, θα εννοούμε (χωρίς ιδιαίτερη μνεία) ότι τόσο το πεδίο ορισμού, όσο και το πεδίο τιμών είναι μη κενά σύνολα.

Ας δούμε μερικά παραδείγματα.

Παράδειγμα 4.5.4. Έστω τα σύνολα $A = \{a, b, c, d\}$ και $B = \{1, 2, 3, 4\}$. Στα βελοειδή διαγράμματα στο σχήμα 4.5 παριστάνονται δύο σχέσεις από το σύνολο A στο



Σχήμα 4.5: *Σχέσεις από το σύνολο A στο σύνολο B.*

σύνολο B. Όπως εύκολα παρατηρούμε, στο πρώτο (από αριστερά) διάγραμμα παριστάνεται μια απεικόνιση, έστω f, ενώ στο δεύτερο η σχέση, έστω g, που παριστάνεται, δεν είναι απεικόνιση (γιατί;). Μα για δύο λόγους. Πρώτον, για το στοιχείο $d \in A$ δεν υπάρχει $r \in B$, ώστε το ζεύγος $(d, r) \in g$. Δεύτερον, τα ζεύγη $(a, 1), (a, 2) \in g$, κάτι που αντίκειται στην απαίτηση του ορισμού

"...για κάθε $x \in A$ υπάρχει μοναδικό $y \in B$ ώστε $(x, y) \in g$".

Με αφορμή το προηγούμενο παράδειγμα. Όταν μας δίνεται μια σχέση μεταξύ δύο συνόλων, για να ελέγξουμε ότι είναι απεικόνιση πρέπει πρώτα να εξασφαλίσουμε ότι τα δοθέντα σύνολα αποτελούν πράγματι το πεδίο ορισμού και το πεδίο τιμών της δοθείσης σχέσεως. Δεύτερον ότι πληρούνται **και** τα δύο σκέλη του Ορισμού 4.5.2. Η διαπίστωση, ότι όντως πρόκειται για απεικόνιση, συνήθως εκφράζεται ως εξής: *Η δοθείσα σχέση πράγματι αποτελεί απεικόνιση ή η απεικόνιση είναι "καλά (καλώς) ορισμένη".*

Παράδειγμα 4.5.5. Δίνεται η απεικόνιση

$$f(x) = \frac{x(x-3)}{2}.$$

Ποιο είναι το πεδίο ορισμού της και ποιο το πεδίο τιμών της;

Η ερώτηση όπως είναι διατυπωμένη είναι ασαφής. Διαισθητικά παραπέμπει ότι το πεδίο ορισμού και το πεδίο τιμών είναι το σύνολο των πραγματικών αριθμών.

Ας δούμε όμως και το εξής παράδειγμα. Έστω ένα (κυρτό) πολύγωνο με n το πλήθος κορυφές. Ας συμβολίσουμε με $r(n)$ το πλήθος των διαγωνίων του. Αναρωτιόμαστε κατά πόσο μπορούμε να υπολογίσουμε αυτό το πλήθος $r(n)$. Άρα, θα έλεγε κάποιος, έχουμε μια απεικόνιση, η οποία στο πλήθος των κορυφών ενός πολυγώνου αντιστοιχίζει το πλήθος των διαγωνίων του.

Ένα n-γωνο για να έχει διαγωνίους πρέπει να έχει τουλάχιστον τέσσερις κορυφές (γιατί;), επειδή για κάθε φυσικό αριθμό $n \geq 4$ υπάρχουν πολύγωνα με n το πλήθος κορυφές και επειδή το πλήθος των διαγωνίων ενός (κυρτού) πολυγώνου δεν εξαρτάται από το σχήμα του, αλλά μόνο από το πλήθος των κορυφών του (γιατί;), η απεικόνιση r έχει ως πεδίο ορισμού το σύνολο $\mathbb{N} \setminus \{1, 2, 3\}$ και ως πεδίο τιμών το σύνολο των φυσικών αριθμών. Δηλαδή

$$r : \mathbb{N} \setminus \{1, 2, 3\} \longrightarrow \mathbb{N}.$$

Τώρα ως γνωστόν[19] το πλήθος των διαγωνίων ενός n-γώνου ισούται με

$$r(n) = \frac{n(n-3)}{2}.$$

Όπως βλέπουμε, οι δύο απεικονίσεις f και r έχουν τον "ίδιο τύπο". Πρόκειται για την ίδια απεικόνιση; Προφανώς όχι!

Από το προηγούμενο παράδειγμα φαίνεται ότι είναι αναγκαίο να ορίσουμε πότε δύο απεικονίσεις είναι ίσες.

Έστω

$$f : A \longrightarrow B \text{ και } g : C \longrightarrow D$$

δύο απεικονίσεις. Οι απεικονίσεις είναι σχέσεις, δηλαδή υποσύνολα καρτεσιανών γινομένων, στην συγκεκριμένη περίπτωση

$$f \subseteq A \times B \text{ και } g \subseteq C \times D.$$

Επομένως, θα μπορούσαμε να πούμε ότι για να θεωρηθούν οι απεικονίσεις ίσες θα πρέπει $f = g$ ως σύνολα. Για να δούμε όμως τι απορρέει από την απαίτηση αυτή.

[19] Είναι μια ωραία άσκηση, την οποία καλείσθε να αποδείξετε.

Επειδή πρόκειται για απεικονίσεις, κάθε στοιχείο του πεδίου ορισμού τους αποτελεί την πρώτη συντεταγμένη στα ζεύγη που ανήκουν στα υποσύνολα f και g. Συνεπώς, τα υποσύνολα αυτά θα είναι της μορφής:

$$f = A \times B_1 \text{ και } g = C \times D_1,$$

όπου $B_1 \subseteq B$ και $D_1 \subseteq D$. Επομένως, η απαίτηση $f = g$ μας οδηγεί στην απαίτηση

$$A = C.$$

Άρα για να είναι οι δύο απεικονίσεις ίσες πρέπει να έχουν το ίδιο πεδίο ορισμού και $f = g$. Είναι όμως αυτό αρκετό;

Ας δούμε ένα παράδειγμα:

Παράδειγμα 4.5.6. Θεωρούμε τις απεικονίσεις $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ και $g : \mathbb{Z} \longrightarrow \mathbb{N}$ με

$$f(x) = \mid x \mid +1 \text{ και } g(x) = \mid x \mid +1.$$

Σύμφωνα με τα προηγούμενα, οι δύο απεικονίσεις θα μπορούσαν να θεωρηθούν ίσες, δεδομένου ότι έχουν το ίδιο πεδίο ορισμού και $f = g$ ως σύνολα ($f(x) = g(x)$ για κάθε $x \in \mathbb{Z}$). Αλλά ας θέσουμε το εξής ερώτημα: Επιλέγουμε ένα τυχαίο στοιχείο στο πεδίο τιμών της f, έστω $r \in \mathbb{Z}$. Αναζητούμε αν υπάρχει $x \in \mathbb{Z}$, ώστε $f(x) = r$. Παρατηρούμε ότι, αν το r είναι αρνητικός αριθμός, τότε δεν υπάρχει $x \in \mathbb{Z}$ με $f(x) = r$. Τουναντίον για κάθε $r \in \mathbb{N}$, το πεδίο τιμών της g, παρατηρούμε ότι υπάρχει (τουλάχιστον) ένα $x \in \mathbb{Z}$ (π.χ. $x = r - 1$) με $g(x) = r$.

Δηλαδή οι δύο απεικονίσεις **δεν** έχουν τις ίδιες ιδιότητες.

Μετά την επισήμανση αυτή μπορούμε να δώσουμε τον εξής ορισμό:

Ορισμός 4.5.7. Δύο απεικονίσεις f και g θα ονομάζονται **ίσες**, αν έχουν το ίδιο πεδίο ορισμού, το ίδιο πεδίο τιμών και για κάθε x στοιχείο του (κοινού) πεδίου ορισμού τους ισχύει ότι $f(x) = g(x)$.

Πριν προχωρήσουμε, θα ορίσουμε μερικές απεικονίσεις, τις οποίες θα επικαλούμαστε στα επόμενα.

Ορισμός 4.5.8. Έστω A, B δύο σύνολα και $S \subseteq A$.

- **Σταθερή** απεικόνιση είναι κάθε απεικόνιση $f : A \longrightarrow B$ με την ιδιότητα

  $$f(x) = b, \text{ για όλα τα } x \in A,$$

  όπου b είναι ένα σταθερό στοιχείο του πεδίου τιμών B.

- Η **ταυτοτική** απεικόνιση στο σύνολο A είναι η απεικόνιση

  $$1_A : A \longrightarrow A \text{ με } 1_A(x) = x \text{ για κάθε } x \in A.$$

- Η απεικόνιση **εγκλεισμού** από το υποσύνολο S στο σύνολο A είναι η απεικόνιση

  $$i : S \longrightarrow A \text{ με } i(x) = x \text{ για όλα τα } x \in S.$$

- Ο **περιορισμός** μιας απεικόνισης $f : A \longrightarrow B$ επί του υποσυνόλου S είναι η απεικόνιση

  $$f_{|S} : S \longrightarrow B \text{ με } f_{|S}(x) = f(x) \text{ για κάθε } x \in S.$$

- Έστω $g : S \longrightarrow B$ μια απεικόνιση. Μια **επέκταση** της g στο A είναι κάθε απεικόνιση $G : A \longrightarrow B$ με την ιδιότητα $G_{|S} = g$.

  Προσοχή! Υπάρχει μόνο ένας περιορισμός μιας απεικόνισης σε ένα υποσύνολο του πεδίου ορισμού. Αλλά, πάντα υπάρχουν πολλές επεκτάσεις μιας απεικόνισης σε ένα (γνήσιο) υπερσύνολο του πεδίου ορισμού της (ιδέ τις Ασκήσεις 4.5.1$_{9,10}$).

- Οι **προβολές** από το καρτεσιανό γινόμενο $A \times B$ είναι οι απεικονίσεις

$$\begin{array}{lll} \pi_1 : A \times B \longrightarrow A & \text{και} & \pi_2 : A \times B \longrightarrow B \text{ με} \\ \pi_1((a, b)) = a & \text{και} & \pi_2((a, b)) = b, \end{array}$$

  για κάθε $(a, b) \in A \times B$.

4.5.1 Ασκήσεις

1. Έστω $A = \{0, 1, 2, 3, 4\}$ και $B = \{2, 3, 4, 5\}$.

   Εξετάστε αν η σχέση $f = \{(0, 3), (1, 3), (2, 4), (3, 2), (4, 2)\}$ αποτελεί απεικόνιση από το σύνολο A στο σύνολο B.

   Να παραστήσετε την απεικόνιση f με βελοειδές διάγραμμα.

   Να βρεθούν όλα τα στοιχεία $x \in A$ με την ιδιότητα $f(x) = 2$.

   Να βρεθούν όλα τα στοιχεία $x \in A$ με την ιδιότητα $f(x) = 5$.

2. Υπάρχουν οκτώ απεικονίσεις με πεδίο ορισμού το σύνολο $A = \{a, b, c\}$ και πεδίο τιμών το σύνολο $B = \{0, 1\}$.

   Μπορείτε να τις προσδιορίσετε;

3. Θεωρούμε τα σύνολα

$$f = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 3x + y = 6\} \text{ και } g = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x + 3y = 6\}.$$

   Ορίζουν αυτά τα σύνολα απεικονίσεις με πεδίο ορισμού το $\mathbb{Z}$;

4. Θεωρούμε τα σύνολα

$$f = \{(x^2, x) \mid x \in \mathbb{R}\} \text{ και } g = \{(x^3, x) \mid x \in \mathbb{R}\}.$$

   Ορίζουν αυτά τα σύνολα απεικονίσεις με πεδίο ορισμού το $\mathbb{R}$;

5. Θα μπορούσε το σύνολο

$$F = \{((x, y), (y, 2x, x + y)) \mid x, y \in \mathbb{R}\}$$

   να είναι μια απεικόνιση μεταξύ δύο συνόλων; Αν ναι, ποιο είναι το πεδίο ορισμού και ποιο το πεδίο τιμών της;

6. Για κάθε φυσικό αριθμό n ορίζουμε ως $d(n)$ το πλήθος των θετικών διαιρετών του (συμπεριλαμβανομένων των 1 και n) και ως $\sigma(n)$ το άθροισμα των θετικών διαιρετών του. Για παράδειγμα:

$$d(10) = 4 \text{ και } \sigma(10) = 1 + 2 + 5 + 10 = 18.$$

Δείξτε ότι οι $d : \mathbb{N} \longrightarrow \mathbb{N}$ και $\sigma : \mathbb{N} \longrightarrow \mathbb{N}$ είναι απεικονίσεις.

Να βρεθούν όλα τα $n \in \mathbb{N}$ με την ιδιότητα

$$d(n) = 2 \text{ και όλα τα } m \in \mathbb{N} \text{ με } d(m) = 3.$$

Να βρεθούν δύο $n \in \mathbb{N}$ με την ιδιότητα $\sigma(n) = 2n$.

7. Έστω $A = \{a, b, c, d\}$ και

$$f = \{(X, |X|) \mid X \subseteq A\},$$

όπου με $|X|$ παριστάνουμε το πλήθος των στοιχείων ενός συνόλου X.

Θα μπορούσε η f να είναι μια απεικόνιση; Αν ναι, ποιο είναι το πεδίο ορισμού της; Ποιο το πεδίο τιμών της;

Να βρεθούν όλα τα υποσύνολα C του A με την ιδιότητα: $f(C) = 3$.

8. Δίνονται οι απεικονίσεις

$$f : \mathbb{R} \longrightarrow \mathbb{R} \text{ με } f(x) = x^2 - 5x \text{ και } g : \mathbb{Z} \longrightarrow \mathbb{Z} \text{ με } g(m) = m^2 - 5m.$$

Να βρεθούν όλα τα $x \in \mathbb{R}$ με $f(x) = 6$.

Να βρεθούν όλα τα $x \in \mathbb{R}$ με $f(x) = 2$.

Να βρεθούν όλα τα $m \in \mathbb{Z}$ με $g(m) = 6$.

Να βρεθούν όλα τα $m \in \mathbb{Z}$ με $g(m) = 2$.

9. Έστω η απεικόνιση

$$f : \mathbb{N} \longrightarrow \mathbb{Z} \text{ με } f(x) = x + 1.$$

Δείξτε ότι οι απεικονίσεις

$$F : \mathbb{Z} \longrightarrow \mathbb{Z} \text{ με } F(x) = x + 1 \text{ και } G : \mathbb{Z} \longrightarrow \mathbb{Z} \text{ με } G(x) = |x| + 1$$

αποτελούν δύο (διαφορετικές) επεκτάσεις της (ίδιας) απεικόνισης f.

Μπορείτε να ορίσετε μια άλλη απεικόνιση $H : \mathbb{Z} \longrightarrow \mathbb{Z}$, η οποία να είναι και αυτή επέκταση της f;

10. Έστω A, B δύο σύνολα και $f : A \longrightarrow B$ μια απεικόνιση. Αν $S \subseteq A$ και $f_{|S}$ είναι ο περιορισμός της f επί το υποσυνόλου S, θεωρούμε μια επέκταση $g : A \longrightarrow B$ της $f_{|S}$.

Είναι κατ' ανάγκη $f = g$; Μπορείτε να δώσετε ένα παράδειγμα, όπου $f \neq g$;

11. Να βρεθούν τα μεγαλύτερα (ως προς την σχέση του περιέχεσθαι) υποσύνολα A και B του $\mathbb{R}$, ώστε να ορίζονται απεικονίσεις $f : A \longrightarrow \mathbb{R}$ και $g : B \longrightarrow \mathbb{R}$ με

$$f(x) = \frac{1}{x^4 - 3}, \text{ για κάθε } x \in A \text{ και } g(x) = \sqrt{1 - x^2}, \text{ για κάθε } x \in B.$$

4.5.2 Απεικονίσεις ένα προς ένα, απεικονίσεις επί

Έστω μια απεικόνιση $f : A \longrightarrow B$. Στον ορισμό της **δεν** απαιτείται δύο διαφορετικά πρότυπα $x_1, x_2 \in A$ να έχουν διαφορετικές εικόνες $f(x_1), f(x_2)$. Δηλαδή ενδέχεται να έχουμε $x_1 \neq x_2$, αλλά $f(x_1) = f(x_2)$. Επίσης, στον ορισμό της **δεν** απαιτείται κάθε στοιχείο του πεδίου τιμών να έχει πρότυπο. Δηλαδή ενδέχεται να υπάρχει $b \in B$ για το οποίο δεν υπάρχει $a \in A$, έτσι ώστε $f(a) = b$.

Στην παράγραφο, όπου αναφερόμασταν στις ιδιότητες σχέσεων (σελ. 127), είχαμε δει πότε μια σχέση ονομάζεται ένα προς ένα και πότε επί. Οι ιδιότητες αυτές είναι πολύ σημαντικές, ειδικά όταν μελετάμε απεικονίσεις. Θα επαναλάβουμε τους σχετικούς ορισμούς.

Ορισμός 4.5.9. Έστω $f : A \longrightarrow B$ μια απεικόνιση.

- Η f θα ονομάζεται **ένα προς ένα** (εν συντομία 1-1), αν για κάθε $x_1, x_2 \in A$ με $x_1 \neq x_2$ έπεται ότι $f(x_1) \neq f(x_2)$[20].
- Η f θα ονομάζεται **επί** (του B), αν για κάθε $y \in B$ υπάρχει (τουλάχιστον) ένα $x \in A$, έτσι ώστε $f(x) = y$.

Σχόλια 4.5.10. Χρησιμοποιώντας την έννοια της αντιθετοαντιστροφής, θα μπορούσαμε να πούμε ότι η απεικόνιση είναι ένα προς ένα, αν

$$\text{για όλα τα } x_1, x_2 \in A \text{ με } f(x_1) = f(x_2) \text{ έπεται ότι } x_1 = x_2 \text{ (ιδέ Θεώρημα 3.2.16).}$$

Επίσης, το ότι η απεικόνιση f δεν είναι ένα προς ένα, σημαίνει ότι

$$\text{υπάρχουν } x_1, x_2 \in A \text{ με } x_1 \neq x_2 \text{ και } f(x_1) = f(x_2).$$

Επομένως, το να δείξουμε ότι μια απεικόνιση δεν είναι ένα προς ένα αρκεί να βρούμε δύο (διαφορετικά) στοιχεία στο πεδίο ορισμού, των οποίων οι εικόνες είναι ίσες.

Το ότι η απεικόνιση δεν είναι επί, σημαίνει ότι

$$\text{υπάρχει } y \in B, \text{ έτσι ώστε για όλα τα } x \in A \text{ να ισχύει } f(x) \neq y.$$

Επομένως, το να δείξουμε ότι μια απεικόνιση δεν είναι επί, πρέπει να αποδείξουμε ότι υπάρχει ένα στοιχείο του πεδίου τιμών, για το οποίο δεν υπάρχει πρότυπο.

Εδώ πρέπει να επισημάνουμε την ουσιώδη διαφορά που υπάρχει, μεταξύ του ορισμού μιας απεικόνισης και του "ένα προς ένα" μιας απεικόνισης. Στον ορισμό της απεικόνισης απαιτούμε,

$$\text{για όλα τα } x_1, x_2 \in A \text{ με } f(x_1) \neq f(x_2), \text{ έπεται ότι } x_1 \neq x_2,$$

σε αντιδιαστολή με τον ορισμό του "ένα προς ένα", όπου

$$\text{από το } x_1 \neq x_2 \text{ έπεται ότι } f(x_1) \neq f(x_2).$$

Επίσης, στον ορισμό της απεικόνισης απαιτούμε, για κάθε στοιχείο του πεδίου ορισμού να υπάρχει (μοναδική) εικόνα, σε αντιδιαστολή με τον ορισμού του "επί",

[20] Θα θέλαμε να επισημάνουμε την (σωστή κατ' εμάς) προτροπή από ορισμένους Μαθηματικούς, ότι μια απεικόνιση ένα προς ένα θα ήταν προτιμότερο να ονομάζεται "δύο προς δύο", δεδομένου ότι η ιδέα είναι: Δύο διαφορετικά στοιχεία του πεδίου ορισμού απεικονίζονται σε δύο διαφορετικά στοιχεία του πεδίου τιμών.

όπου απαιτούμε για κάθε στοιχείο του πεδίου τιμών να υπάρχει (τουλάχιστον) ένα πρότυπο.

Επομένως, πρέπει να είμαστε προσεκτικοί στην κατανόηση και διατύπωση των ανωτέρω ορισμών. Μια απλή ανάγνωση (με πρόθεση αποστήθισης) θα μας δημιουργεί προβλήματα.

Παραδείγματα 4.5.11.

1. Προφανώς (;) η ταυτοτική απεικόνιση σε ένα σύνολο A με $1_A : A \longrightarrow A$ με $1_A(x) = x$ για κάθε $x \in A$ είναι 1-1 και επί.

2. Προφανώς (;) η απεικόνιση εγκλεισμού $i : S \longrightarrow A$ από ένα υποσύνολο S ενός συνόλου A στο σύνολο A με $i(x) = x$ για όλα τα $x \in S$.είναι 1-1.

3. Οι προβολές

$$\begin{array}{lll} \pi_1 : A \times B \longrightarrow A & \text{και} & \pi_2 : A \times B \longrightarrow B \text{ με} \\ \pi_1((a,b)) = a & \text{και} & \pi_2((a,b)) = b, \end{array}$$

για κάθε $(a,b) \in A \times B$ είναι προφανώς(;) απεικονίσεις επί, αλλά δεν είναι 1-1 [21].

4. Η απεικόνιση $f : \mathbb{R} \setminus \{0\} \longrightarrow \mathbb{R}$ με $f(x) = \dfrac{1}{x} + 1$ είναι 1-1.

   Έστω $a, b \in \mathbb{R} \setminus \{0\}$ με $f(a) = f(b)$, δηλαδή

$$\frac{1}{a} + 1 = \frac{1}{b} + 1.$$

   Από την τελευταία ισότητα έπεται εύκολα ότι $a = b$. Άρα η f είναι πράγματι 1-1. Η f όμως δεν είναι επί. Πράγματι για τον πραγματικό αριθμό 1 ισχύει ότι

$$\frac{1}{x} + 1 \neq 1$$

   για κάθε $x \in \mathbb{R} \setminus \{0\}$.

5. Δίνεται η απεικόνιση $\vartheta : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ με $\vartheta(x,y) = 6x - 9y$ [22].

   Παρατηρούμε ότι η ϑ δεν είναι ούτε 1-1, ούτε επί. Πράγματι, έστω

$$(x_1, y_1), (x_2, y_2) \in \mathbb{Z} \times \mathbb{Z} \text{ με } \vartheta(x_1, y_1) = \vartheta(x_2, y_2),$$

   δηλαδή

$$6x_1 - 9y_1 = 6x_2 - 9y_2.$$

   Από την τελευταία ισότητα βλέπουμε ότι για όλα τα ζεύγη της μορφής

$$(x - 3k, y - 2k), k \in \mathbb{Z}$$

   έχουμε ότι

$$\vartheta(x,y) = \vartheta(x - 3k, y - 2k).$$

[21] Υπάρχει περίπτωση μια προβολή να είναι 1-1; Ελέγξτε το!!

[22] Επισημαίνουμε ότι θα έπρεπε να γράψουμε $\vartheta((x,y)) = 6x - 9y$, καθ' ότι το πεδίο ορισμού είναι ένα καρτεσιανό γινόμενο και τα στοιχεία του είναι ζεύγη, αλλά για λόγους ευκολίας (χωρίς αυτό να προκαλεί σύγχυση), αντί του $\vartheta((x,y))$, γράφουμε $\vartheta(x,y)$.

Δηλαδή η απεικόνιση ϑ δεν είναι 1-1.

Επίσης, παρατηρούμε ότι για οποιοδήποτε ζεύγος ακεραίων αριθμών (x, y) η εικόνα του $\vartheta(x, y) = 6x - 9y$ είναι πολλαπλάσιο του 3. Συνεπώς, αν έχουμε έναν ακέραιο αριθμό r, οποίος δεν είναι πολλαπλάσιο του τρία, τότε δεν υπάρχει ζεύγος $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ με $\vartheta(a, b) = r$. Δηλαδή η απεικόνιση ϑ δεν είναι επί.

Μάλιστα δε, μπορούμε να παρατηρήσουμε ότι, αν έχουμε έναν ακέραιο αριθμό s, οποίος είναι πολλαπλάσιο του τρία, δηλαδή $s = 3k$, τότε

$$\vartheta(-k, -k) = 6(-k) - 9(-k) = 3k = s.$$

Άρα για όλα τα πολλαπλάσια του τρία υπάρχει πρότυπο, ενώ για όλα τα μη πολλαπλάσια του τρία δεν υπάρχει πρότυπο.

6. Ας δούμε την απεικόνιση $f(x) = x^2$. Είναι η f 1-1, είναι επί;

   Το ερώτημα, όπως τίθεται είναι ασαφές, καθότι, όπως έχουμε επισημάνει, στον ορισμό μιας απεικόνισης **δεν** αρκεί ο "τύπος της". Πρέπει να έχει προσδιοριστεί το πεδίο ορισμού της και το πεδίο τιμών της.

   Ας δούμε πώς το πεδίο ορισμού και το πεδίο τιμών καθορίζουν πότε η απεικόνιση f είναι 1-1 και πότε επί.

   Έστω το διάστημα $[0, \infty)$, δηλαδή

   $$[0, \infty) = \{x \in \mathbb{R} \mid x \geq 0\}.$$

   Ορίζουμε τις απεικονίσεις

   $$\begin{aligned} f_1 &: [0, \infty) \longrightarrow [0, \infty) \text{ με} & f_1(x) &= x^2, \\ f_2 &: [0, \infty) \longrightarrow \mathbb{R} \text{ με} & f_2(x) &= x^2, \\ f_3 &: \mathbb{R} \longrightarrow [0, \infty) \text{ με} & f_3(x) &= x^2 \text{ και} \\ f_4 &: \mathbb{R} \longrightarrow \mathbb{R} \text{ με} & f_4(x) &= x^2. \end{aligned}$$

   Παρατηρούμε (να κάνετε τον έλεγχο!) ότι η f_1 είναι 1-1 και επί, η f_2 είναι 1-1, αλλά όχι επί, η f_3 δεν είναι 1-1, αλλά είναι επί και η f_4 δεν είναι ούτε 1-1 ούτε επί.

7. **Η φυσική απεικόνιση**

   Έστω $(A, \sim)$ ένα (μη κενό) σύνολο εφοδιασμένο με την σχέση $\sim$, η οποία είναι ισοδυναμία και έστω $A/\sim$ το σύνολο πηλίκων της, δηλαδή το σύνολο όλων των κλάσεων ισοδυναμίας. (Για να προχωρήσουμε, πρέπει να ανατρέξουμε στην Παράγραφο 4.4.1, όπου αναφέρονται οι σχετικές έννοιες).

   Ορίζουμε μια απεικόνιση

   $$\varphi : A \longrightarrow A/\sim$$

   ως εξής:

   $$\varphi(a) = C_a,$$

   δηλαδή κάθε στοιχείο του συνόλου A απεικονίζεται στην κλάση ισοδυναμίας του

   $$C_a = \{b \in A \mid b \sim a\}.$$

Πρώτα θα δούμε ότι φ είναι πράγματι απεικόνιση. Για κάθε $a \in A$ ορίζεται μοναδικά η κλάση ισοδυναμίας του (ιδέ Πρόταση 4.4.2). Άρα πράγματι η φ είναι απεικόνιση.

Η απεικόνιση φ είναι προφανώς επί, δεδομένου ότι, για κάθε $C_a \in A/\sim$, υπάρχει το $a \in A$ με $\varphi(a) = C_a$.

Ας εξετάσουμε αν η απεικόνιση $\varphi(a)$ είναι 1-1. Έστω δύο $a, b \in A$ με $a \neq b$. Είναι οι εικόνες C_a και C_b διαφορετικές; Όχι κατ' ανάγκη δεδομένου ότι ενδέχεται τα a και b να είναι ισοδύναμα, οπότε $C_a = C_b$ (Πρόταση 4.4.2). Άρα η απεικόνιση φ, εν γένει, δεν είναι 1-1.

Στην ακραία όμως περίπτωση όπου **κάθε** κλάση ισοδυναμίας είναι μονοσύνολο (δηλαδή πρόκειται για την σχέση ισότητας), τότε η απεικόνιση φ είναι 1-1.

Έστω τώρα $C_a \in A/\sim$ ένα στοιχείο του πεδίου τιμών της φ. Ας αναζητήσουμε ποια στοιχεία $b \in A$ έχουν ως εικόνα το C_a μέσω της φ. Από τον ορισμό της φ έχουμε ότι $\varphi(b) = C_b$. Αν απαιτήσουμε όμως $\varphi(b) = C_a$, τότε πρέπει $C_a = C_b$. Αυτό όμως σημαίνει ότι $b \sim a$.

Αντίστροφα αν $b \sim a$, τότε $C_a = C_b$ (Πρόταση 4.4.2) και συνεπώς $\varphi(b) = C_a$.

Άρα, ένα $b \in A$ έχει ως εικόνα το C_a, αν και μόνο αν $b \sim a$, αν και μόνο αν $b \in C_a$.

Από τα προηγούμενα έπεται ότι, όταν έχουμε μια απεικόνιση $f : A \longrightarrow B$ μεταξύ των συνόλων A και B, ορισμένες φορές, είναι αναγκαίο να αναζητήσουμε μέσα στο πεδίο τιμών της, το σύνολο B, μόνο τις εικόνες των στοιχείων του πεδίου ορισμού της.

Ορισμός 4.5.12. Έστω $f : A \longrightarrow B$ μια απεικόνιση μεταξύ των συνόλων A και B. Ορίζουμε

$$f(A) = \{ f(a) \mid a \in A \}.$$

Δηλαδή το σύνολο $f(A)$ είναι το υποσύνολο του πεδίου τιμών της f, το οποίο αποτελείται μόνο από τις εικόνες των στοιχείων του πεδίου ορισμού της f.

Το σύνολο $f(A)$ θα ονομάζεται η **εικόνα** της f ή το **σύνολο τιμών** της f.

Μια άμεση συνέπεια του προηγουμένου ορισμού είναι η πρόταση:

Πρόταση 4.5.13. [23] *Έστω A και B δύο σύνολα και $f : A \longrightarrow B$ μια απεικόνιση. Η f είναι επί, αν και μόνο αν το σύνολο τιμών της, δηλαδή το $f(A) = \{ f(x) \mid x \in A \}$, ισούται με το πεδίο τιμών της B.*

Απόδειξη. Η απόδειξη είναι άμεση, από τους Ορισμούς 4.5.9 και 4.5.12. Απλώς να την επαναλάβετε. ό.έ.δ.

Η αντίστροφη απεικόνιση.

Υπενθυμίζουμε ότι, αν έχουμε μια σχέση $\mathrm{R} \subseteq A \times B$ από ένα σύνολο A σε ένα σύνολο B, τότε μπορούμε να ορίσουμε την αντίστροφη σχέση $\mathrm{R}^{-1} \subseteq B \times A$ από το σύνολο B στο σύνολο A ως εξής:

$$b \,\mathrm{R}^{-1}\, a, \text{ αν } a \,\mathrm{R}\, b.$$

[23] Το σύνηθες λάθος εδώ είναι η *ταυτοποίηση* των εννοιών "πεδίο τιμών" και "σύνολο τιμών". Κάτι που οδηγεί στο *συμπέρασμα:* Όλες οι απεικονίσεις είναι επί!

Μια απεικόνιση $f : A \longrightarrow B$ από ένα σύνολο A σε ένα σύνολο B είναι μια σχέση μεταξύ των συνόλων A και B. Συγκεκριμένα

$$f = \{(a, f(a)) \mid a \in A\} \subseteq A \times B.$$

Οπότε, ορίζεται η αντίστροφη σχέση

$$f^{-1} = \{(f(a), a) \mid a \in A\} \subseteq B \times A.$$

Το ερώτημα που προκύπτει είναι το εξής: Είναι η αντίστροφη σχέση f^{-1} απεικόνιση; Πριν προχωρήσουμε, ας δούμε ένα παράδειγμα.

Έστω τα σύνολα $A = \{a, b, c, d\}$ και $B = \{1, 2, 3, 4\}$ και οι απεικονίσεις

$$f : A \longrightarrow B \text{ με } \quad f(a) = 1, f(b) = 2, f(c) = 3, f(d) = 4$$

και

$$g : A \longrightarrow B \text{ με } \quad g(a) = 1, g(b) = 1, g(c) = 3, f(d) = 4.$$

Παρατηρούμε ότι οι αντίστροφες σχέσεις είναι οι εξής:

$$f^{-1} = \{(1, a), (2, b), (3, c), (4, d)\} \text{ και } g^{-1} = \{(1, a), (1, b), (3, c), (4, d)\}.$$

Η σχέση f^{-1} είναι απεικόνιση με πεδίο ορισμού το σύνολο B και πεδίο τιμών το σύνολο A (γιατί;). Μα, προφανώς διότι πληρούνται οι προϋποθέσεις του Ορισμού της απεικόνισης (Ορισμός 4.5.2).

Η σχέση g^{-1} όμως δεν είναι απεικόνιση (γιατί;). Μα, αφού δεν πληροίται καμία από τις προϋποθέσεις του Ορισμού 4.5.2, αφού για μεν το στοιχείο $2 \in B$ δεν υπάρχει $x \in A$, ώστε $(2, x) \in g^{-1}$ και για το στοιχείο $1 \in B$ υπάρχουν δύο στοιχεία $a, b \in A$ με $(1, a), (1, b) \in g^{-1}$.

Γενικά, από το προηγούμενο παράδειγμα, παρατηρούμε ότι, αν μια απεικόνιση $h : K \longrightarrow L$ δεν είναι επί, τότε η αντίστροφή της σχέση h^{-1} δεν είναι απεικόνιση. Άρα αναγκαία συνθήκη, για να είναι η αντίστροφη σχέση h^{-1} απεικόνιση, είναι η απεικόνιση h να είναι επί.

Επίσης, από το προηγούμενο παράδειγμα, βλέπουμε ότι η σχέση g^{-1} δεν είναι απεικόνιση και για έναν άλλο λόγο. Η απεικόνιση g δεν είναι 1-1, επομένως η σχέση g^{-1} δεν είναι απεικόνιση, δεδομένου ότι για το στοιχείο $1 \in B$ υπάρχουν δύο στοιχεία $a, b \in A$ με $(1, a), (1, b) \in g^{-1}$.

Επομένως, γενικά, αν μια απεικόνιση $h : K \longrightarrow L$ δεν είναι 1-1, τότε η αντίστροφή της σχέση h^{-1} δεν είναι απεικόνιση. Άρα αναγκαία συνθήκη, για να είναι η αντίστροφη σχέση h^{-1} απεικόνιση, είναι η απεικόνιση h να είναι 1-1.

Από τα προηγούμενα έπεται ότι αναγκαίες συνθήκες, για να είναι η αντίστροφη σχέση μιας απεικόνισης και αυτή απεικόνιση, είναι η απεικόνιση να 1-1 και επί.

Είναι αυτές οι συνθήκες ικανές; Προφανώς ναι. Πράγματι, αν έχουμε μια απεικόνιση $h : K \longrightarrow L$, η οποία είναι 1-1 και επί, τότε για κάθε στοιχείο $y \in L$, αφού η g είναι επί, υπάρχει πρότυπο $x \in K$ με $h(x) = y$. Το στοιχείο $x \in K$ είναι το μοναδικό με την ιδιότητα $h(x) = y$, διότι αν υπήρχε και ένα άλλο $x_1 \in K$ με

$$x_1 \neq x \text{ και } h(x_1) = h(x) = y,$$

τότε η απεικόνιση h δεν θα ήταν 1-1, άτοπο.

Θεώρημα 4.5.14. *Έστω A, B δύο μη κενά σύνολα και $f : A \longrightarrow B$ μια απεικόνιση. Η αντίστροφη σχέση f^{-1} είναι απεικόνιση αν και μόνο αν η απεικόνιση f είναι 1-1 και επί.*

Απόδειξη. Η απόδειξη στην πραγματικότητα έχει προηγηθεί.
Να την επαναλάβετε εδώ με κάθε λεπτομέρεια. ό.έ.δ.

Δεδομένου ότι η αντίστροφη μιας σχέσης R είναι μοναδική (ιδέ Παρατήρηση 4.1.2$_5$), μπορούμε να δώσουμε τον ακόλουθο ορισμό.

Ορισμός 4.5.15. Έστω μια απεικόνιση $f : A \longrightarrow B$, η οποία είναι 1-1 και επί. Η (μοναδική) αντίστροφη σχέση f^{-1}, η οποία είναι απεικόνιση, θα ονομάζεται η **αντίστροφη απεικόνιση** της f και η f θα ονομάζεται **αντιστρέψιμη απεικόνιση**.

Πρόταση 4.5.16. *Έστω μια απεικόνιση $f : A \longrightarrow B$, η οποία είναι 1-1 και επί. Η αντίστροφή της απεικόνιση f^{-1} είναι και αυτή 1-1 και επί.*

Απόδειξη. Αρκεί να παρατηρήσουμε ότι $(f^{-1})^{-1} = f$ (ιδέ Παρατήρηση 4.1.2). ό.έ.δ.

Παρατήρηση 4.5.17. Έστω $f : A \longrightarrow B$ μια 1-1 και επί απεικόνιση (δηλαδή αντιστρέψιμη απεικόνιση). Αν δούμε την f και την αντίστροφή της f^{-1} ως σχέσεις, τότε έχουμε

$$f = \{(x, f(x)) \mid x \in A\} \text{ και } f^{-1} = \{(f(x), x) \mid x \in A\}.$$

Τι σημαίνει όμως $(f(x), x) \in f^{-1}$ και $(x, f(x)) \in f$; Προφανώς, (μόνο) από τον ορισμό της σχέσης, ότι

$$f^{-1}(f(x)) = x,$$

για κάθε $x \in A$. Επίσης, για κάθε $y \in B$, υπάρχει μοναδικό $x \in A$ με $f^{-1}(y) = x$ (ισοδύναμα $f(x) = y$), συνεπώς

$$f(f^{-1}(y)) = f(x) = y.$$

Επ' αυτού θα επανέλθουμε όταν μιλήσουμε για την σύνθεση απεικονίσεων.

Παραδείγματα 4.5.18.

1. Η απεικόνιση $h : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ με

$$h(x, y) = (x + y, x + 2y)$$

είναι 1-1 και επί.

Πρώτα[24] ελέγχουμε ότι η h είναι πράγματι απεικόνιση. Πράγματι, για κάθε ζεύγος ακεραίων αριθμών (m, n) το ζεύγος

$$(m + n, m + 2n) = h(m, n)$$

είναι ένα ζεύγος ακεραίων αριθμών. Μάλιστα δε, αν $(m_1, n_1) = (m_2, n_2)$, τότε εύκολα έπεται ότι

$$(m_1 + n_1, m_1 + 2n_1) = (m_2 + n_2, m_2 + 2n_2),$$

[24] Γενικά, όταν δίνεται μια απεικόνιση, θεωρούμε δεδομένο ότι είναι πράγματι απεικόνιση (καλά ορισμένη). Πολλές φορές αυτό δεν είναι προφανές και χρειάζεται αιτιολόγηση. Εδώ το κάνουμε για την εξοικείωση.

δηλαδή

$$h(m_1, n_1) = h(m_2, n_2).$$

Άρα πράγματι η h είναι καλά ορισμένη.

Για να αποδείξουμε ότι η h είναι 1-1 (ιδέ σχόλια 4.5.10), υποθέτουμε ότι έχουμε

$$h(m_1, n_1) = h(m_2, n_2),$$

δηλαδή

$$(m_1 + n_1, m_1 + 2n_1) = (m_2 + n_2, m_2 + 2n_2).$$

Από την σχέση αυτή, εύκολα(;) έπεται ότι

$$(m_1, n_1) = (m_2, n_2),$$

άρα η απεικόνιση h είναι 1-1.

Θα αποδείξουμε ότι η h είναι επί. Έστω (a, b) ένα τυχαίο στοιχείο του πεδίου τιμών $\mathbb{Z} \times \mathbb{Z}$. Αναζητούμε (αν υπάρχει) $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, έτσι ώστε

$$h(x, y) = (a, b).$$

Αυτό σημαίνει ότι αναζητούμε ένα ζεύγος ακεραίων αριθμών (x, y), ώστε

$$(x + y, x + 2y) = (a, b).$$

Από την τελευταία (απαιτητή) ισότητα έπεται εύκολα(;) ότι, για $x = 2a - b$ και $y = b - a$, πράγματι ισχύει ότι

$$(x + y, x + 2y) = (a, b).$$

Δηλαδή

$$h(2a - b, b - a) = (a, b)$$

συνεπώς η απεικόνιση h είναι επί.

Εφόσον αποδείξαμε ότι η απεικόνιση h είναι 1-1 και επί, η h είναι αντιστρέψιμη. Ποια είναι η αντίστροφή της h^{-1};

Παρατηρούμε ότι, αν ορίσουμε την $h^{-1} : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ ως

$$h^{-1}(a, b) = (2a - b, b - a)$$

τότε πράγματι

$$h(h^{-1}(a, b)) = h(2a - b, b - a) = (a, b)$$

και

$$h^{-1}(h(a, b)) = h^{-1}(a+b, a+2b) = (2(a+b)-(a+2b), (a+2b)-(a+b)) = (a, b).$$

Άρα σωστά ορίσαμε την h^{-1}.

Ένα εύλογο ερώτημα είναι το εξής: Πώς σκεφθήκαμε να ορίσουμε έτσι την h^{-1}; Οδηγηθήκαμε σε αυτήν την σκέψη από αυτά που προηγήθηκαν για να αποδείξουμε ότι η απεικόνιση είναι επί.

2. Θα εξετάσουμε αν η απεικόνιση $f : \mathbb{R} \setminus \{2\} \longrightarrow \mathbb{R} \setminus \{5\}$ με

$$f(x) = \frac{5x+1}{x-2}$$

είναι 1-1 και επί.

Εδώ θεωρούμε δεδομένο ότι η f είναι πράγματι απεικόνιση.

Θα εξετάσουμε, αν η f είναι 1-1. Έστω $x_1, x_2 \in \mathbb{R} \setminus \{2\}$ με $x_1 \neq x_2$, τότε $f(x_1) \neq f(x_2)$. Πράγματι, αν υποθέσουμε ότι

$$f(x_1) = f(x_2),$$

τότε θα έχουμε ότι

$$\frac{5x_1+1}{x_1-2} = \frac{5x_2+1}{x_2-2}.$$

Από την τελευταία σχέση με στοιχειώδεις πράξεις καταλήγουμε ότι

$$x_1 = x_2,$$

άτοπο. Πώς καταλήξαμε σε άτοπο; Υποθέτοντας ότι $f(x_1) = f(x_2)$. Άρα

$$f(x_1) \neq f(x_2),$$

συνεπώς η απεικόνιση f είναι 1-1.

Θα εξετάσουμε αν η απεικόνιση f είναι επί. Έστω y ένα τυχαίο στοιχείο του πεδίου τιμών $\mathbb{R} \setminus \{5\}$. Θα προσπαθήσουμε να δούμε, αν υπάρχει στοιχείο x του πεδίου ορισμού $\mathbb{R} \setminus \{2\}$ ώστε

$$f(x) = y.$$

Δηλαδή αναζητούμε ένα $x \in \mathbb{R} \setminus \{2\}$ ώστε

$$\frac{5x+1}{x-2} = y.$$

Από την τελευταία (απαιτητή) ισότητα έχουμε ότι

$$5x+1 = y(x-2),$$

δηλαδή πρέπει

$$5x - yx = -2y - 1.$$

Άρα πρέπει

$$x(5-y) = -2y - 1,$$

συνεπώς αναγκαστικά πρέπει

$$x = \frac{2y+1}{y-5}.$$

Υπάρχει τέτοιο x; φυσικά, διότι το $y \in \mathbb{R} \setminus \{5\}$. Άρα η απεικόνιση f είναι επί.

(Η διαδικασία που ακολουθήσαμε εδώ, συνήθως αναφέρεται ως "*επίλυση ως προς x*").

Εφόσον αποδείξαμε ότι η απεικόνιση f είναι 1-1 και επί, η f είναι αντιστρέψιμη. Ποια είναι η αντίστροφή της;

Όπως στο προηγούμενο παράδειγμα, θα "εκμεταλλευτούμε" ότι για το τυχαίο $y \in \mathbb{R} \setminus \{5\}$ βρήκαμε το (μοναδικό)

$$x = \frac{2y+1}{y-5} \in \mathbb{R} \setminus \{2\}$$

με $f(x) = y$. Συνεπώς, η αντίστροφη απεικόνιση $f^{-1} : \mathbb{R} \setminus \{5\} \longrightarrow \mathbb{R} \setminus \{2\}$ είναι η

$$f^{-1}(y) = \frac{2y+1}{y-5}.$$

Για επαλήθευση, εύκολα μπορούμε να ελέγξουμε ότι

$$f(f^{-1}(y)) = y,$$

για κάθε $y \in \mathbb{R} \setminus \{5\}$ και

$$f^{-1}(f(x)) = x,$$

για κάθε $x \in \mathbb{R} \setminus \{2\}$, (ιδέ Παρατήρηση 4.5.17).

Παρατήρηση 4.5.19. Όπως βλέπουμε και από τα προηγούμενα παραδείγματα, η εύρεση της αντίστροφης απεικόνισης μιας αντιστρέψιμης απεικόνισης, δεν είναι πάντα εύκολη διαδικασία. Μάλιστα δε ορισμένες φορές είναι αδύνατη. Τις περισσότερες φορές είναι αρκετό να εξασφαλίσουμε (με κάποιο τρόπο) ότι μια απεικόνιση είναι αντιστρέψιμη και δεν είναι αναγκαίο να βρούμε ποια είναι η αντίστροφή της.

4.5.3 Ασκήσεις

1. Έστω $A = \{1, 2, 3\}$ και $B = \{a, b, c\}$.

   Να βρεθούν όλες οι απεικονίσεις $f : A \longrightarrow B$, οι οποίες είναι 1-1.

   Να βρεθούν όλες οι απεικονίσεις $g : A \longrightarrow B$, οι οποίες είναι επί.

2. Έστω η απεικόνιση $f : \mathbb{R} \longrightarrow R$ με

   $$f(x) = ax^2 + bx + c, \ a, b, c \in R, a \neq 0.$$

   Δείξτε ότι η f δεν είναι 1-1 για όλα τα $a, b, c \in R$, $a \neq 0$. Είναι η f επί;

3. Έστω $f : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ η απεικόνιση με

   $$f(x, y) = -x^2y + 3y.$$

   Εξετάστε αν η f είναι 1-1.

   Εξετάστε αν η f είναι επί.

   Δικαιολογήστε την απάντησή σας.

4. Για τις ακόλουθες απεικονίσεις εξετάστε αν είναι 1-1 και επί.

   Στην περίπτωση, όπου είναι 1-1 και επί να βρεθεί η αντίστροφή τους.

   (α) $f : \mathbb{R} \longrightarrow \mathbb{R}$ με $f(x) = 5x + 3$.

(β) $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$ με $\varphi(x) = 5x + 3$.

(γ) $g : (\mathbb{R} \setminus \{4\}) \longrightarrow \mathbb{R}$ με $g(x) = \dfrac{3x}{x-4}$.

(δ) $\vartheta : (\mathbb{R} \setminus \{4\}) \longrightarrow (\mathbb{R} \setminus \{3\})$ με $\vartheta(x) = \dfrac{3x}{x-4}$.

5. Να εξετάσετε αν η απεικόνιση $f : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R} \times \mathbb{R}$ με

$$f(x, y) = (2x + y, x - y)$$

είναι 1-1 και επί.

6. Δείξτε ότι η απεικόνιση $f : \mathbb{N} \longrightarrow \mathbb{Z}$ με

$$f(n) = \frac{(-1)^n(2n-1)+1}{4}$$

είναι 1-1 και επί.

7. Δίνεται η απεικόνιση $f : \mathbb{R} \longrightarrow (-1, 1)$ με

$$f(x) = \begin{cases} \dfrac{x^2}{x^2+1} & \text{αν } x \geq 0 \\ \dfrac{-x^2}{x^2+1} & \text{αν } x < 0 \end{cases}$$

Χωρίς να "καταφύγετε" σε επιχειρήματα Απειροστικού Λογισμού, να αποδείξετε ότι η f είναι 1-1 και επί.

8. Έστω $\vartheta : \mathcal{P}(\Omega) \longrightarrow \mathcal{P}(\Omega)$ με

$$\vartheta(X) = X^c,$$

για κάθε $X \subseteq \Omega$. Δείξτε ότι η ϑ είναι 1-1 και επί.

9. Έστω $B = \{2^n \mid n \in \mathbb{Z}\} = \{\ldots, 1/4, 1/2, 1, 2, 4, \ldots\}$ και $f : \mathbb{Z} \longrightarrow B$ με

$$f(n) = 2^n.$$

Δείξτε ότι η f είναι 1-1 και επί. Να βρεθεί η f^{-1}.

10. Έστω A, B, C τρία σύνολα. Δείξτε ότι η απεικόνιση

$$f : (A \times B) \times C \longrightarrow A \times (B \times C)$$

με

$$((a, b), c) \xrightarrow{f} (a, (b, c)),$$

για $a \in A$, $b \in B$, $c \in C$ είναι 1-1 και επί. (Ανατρέξτε στην Παρατήρηση 1.1.54).

11. Έστω η απεικόνιση $f : A \longrightarrow B$ και $a \in A$, $b \in B$. Υποθέτουμε ότι η f είναι 1-1 και επί. Δείξτε ότι υπάρχει μια 1-1 και επί απεικόνιση $g : A \longrightarrow B$ με

$$g(a) = b.$$

4.5.4 Η εικόνα απεικόνισης και η αντίστροφη εικόνα απεικόνισης

Έστω η απεικόνιση $f : A \longrightarrow B$. Όπως προείπαμε, ορισμένες φορές αναζητούμε (αν υπάρχουν) πρότυπα στοιχείων του πεδίου τιμών της (για παράδειγμα ιδέ Άσκηση 4.5.1$_8$ και το Παράδειγμα 4.5.11). Στην προηγουμένη παράγραφο είχαμε ορίσει (Ορισμός 4.5.12) το σύνολο τιμών της απεικόνισης ως

$$f(A) = \{ f(a) \mid a \in A \}$$

Γενικά, όταν έχουμε ένα M υποσύνολο του πεδίου ορισμού A και N ένα υποσύνολο του πεδίου τιμών B της f, τότε μπορούμε να ορίσουμε τα εξής σύνολα:

Ορισμός 4.5.20. Έστω η απεικόνιση $f : A \longrightarrow B$, $M \subseteq A$ και $N \subseteq B$.

Ως **εικόνα**, μέσω της απεικόνισης f, του υποσυνόλου M ορίζουμε το σύνολο

$$f(M) = \{ f(x) \mid x \in M \} = \{ b \in B \mid b = f(x) \text{ για κάποιο } x \in M \}.$$

Ως **(πλήρη) αντίστροφη εικόνα** του υποσυνόλου N ορίζουμε το σύνολο

$$f^{-1}(N) = \{ a \in A \mid f(a) \in N \} \subseteq A.$$

Προφανώς, για κάθε απεικόνιση $f : A \longrightarrow B$, ισχύει

$$f(\varnothing) = \varnothing$$

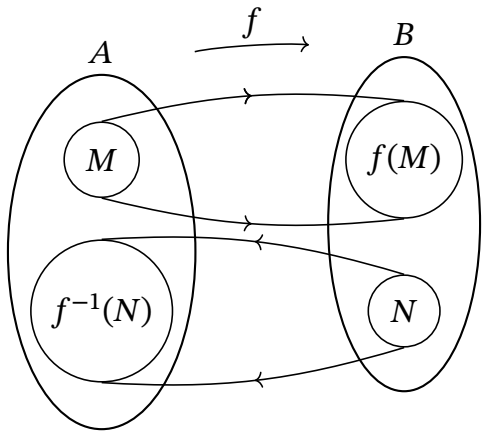
και αν $\varnothing \neq M \subseteq A$, τότε

$$f(M) \neq \varnothing.$$

Επίσης, ισχύει ότι

$$f^{-1}(B) = A \text{ (γιατί;)}.$$

Στο σχήμα 4.6 φαίνονται διαγραμματικά τα σύνολα $f(M)$ και $f^{-1}(N)$.



Σχήμα 4.6: *Διαγραμματικά τα σύνολα $f(M)$ και $f^{-1}(N)$.*.

Πριν προχωρήσουμε, ας δούμε ένα παράδειγμα.

Παράδειγμα 4.5.21. Έστω $A = \{a, b, c, d, e\}$ και $B = \{1, 2, 3, 4, 5, 6\}$. Δίνεται η απεικόνιση $f : A \longrightarrow B$, η οποία ορίζεται ως εξής:

$$f = \{(a, 2), (b, 4), (c, 2), (d, 5), (e, 6),\}.$$

Η απεικόνιση f προφανώς δεν είναι ούτε 1-1 ούτε επί. Μπορούμε να ελέγξουμε ότι:

$$f(\{a, c\}) = \{2\}, \qquad f(\{a, d\}) = \{2, 5\}, \qquad f(\{b, c, e\}) = \{4, 2, 6\},$$
$$f^{-1}(\{2\}) = \{a, c\}, \qquad f^{-1}(\{3\}) = \varnothing, \qquad f^{-1}(\{1, 5\}) = \{d\}.$$

Μια πρώτη επισήμανση, από το προηγούμενο παράδειγμα, είναι η εξής:

$$f^{-1}(\{2\}) = \{a, c\},$$

ενώ η γραφή $f^{-1}(2)$ **δεν** έχει νόημα. Επίσης, υπάρχει μια διακριτή διαφορά μεταξύ του $f(a) = 2$ και του $f(\{a\}) = \{2\}$.

Μετά τις πρώτες επισημάνσεις, δεδομένου ότι, στο εξής, θα γίνεται ευρεία χρήση των συμβολισμών $f(M)$ και $f^{-1}(N)$, για να μην γίνονται παρανοήσεις και λάθη, ας κάνουμε κάποια σχόλια.

Σχόλια 4.5.22. Μέχρι τώρα με $f(a)$ συμβολίζαμε την εικόνα του στοιχείου a μέσω της απεικόνισης f. Τώρα το ίδιο σύμβολο f χρησιμοποείται στο $f(M)$, όπου το M είναι υποσύνολο του πεδίου ορισμού A και όχι στοιχείο του. Επίσης, το σύμβολο f^{-1} συμβολίζει την αντίστροφη απεικόνιση της f, αν υπάρχει η αντίστροφη απεικόνιση. Εδώ χρησιμοποιείται (ακόμη και όταν η αντίστροφη απεικόνιση της f δεν υπάρχει) για να δηλώσουμε την πλήρη αντίστροφη εικόνα ενός υποσυνόλου (όχι στοιχείου!) του πεδίου τιμών της f. Η χρήση του ιδίου συμβόλου για δύο διαφορετικές έννοιες είναι η "πηγή του προβλήματος". Παρ' όλα ταύτα, η προσεκτική (και κυρίως συνειδητή) χρήση των συμβόλων f και f^{-1}, όχι μόνο δεν δημιουργεί προβλήματα, αλλά μας "απαλλάσσει" από το βάρος της αναζήτησης και χρήσης διαφορετικών συμβολισμών. Στο τέλος της παραγράφου θα επανέλθουμε επ' αυτού.

Ας δούμε ένα παράδειγμα ακόμη.

Παράδειγμα 4.5.23. Έστω η απεικόνιση $f : \mathbb{R} \longrightarrow \mathbb{R}$ με

$$f(x) = x^2.$$

Παρατηρούμε ότι

$$f(\{0, 1, 2\}) = \{0, 1, 4\} \qquad f^{-1}(\{0, 1, 4\}) = \{-2, -1, 0, 1, 2\}.$$

Επίσης

$$f^{-1}([-4, 4]) = [0, 2] \qquad f([0, 2]) = [0, 4].$$

Το παράδειγμα αυτό είναι αρκετό να συμπεράνουμε ότι: Αν $f : A \longrightarrow B$ είναι μια απεικόνιση και $X \subseteq A,\ Y \subseteq B$, τότε εν γένει

$$f(f^{-1}(Y)) \neq Y \text{ και } f^{-1}(f(X)) \neq X.$$

Θεώρημα 4.5.24. *Έστω $f : A \longrightarrow B$ μια απεικόνιση, $C, D \subseteq A$ και $R, S \subseteq B$, Τότε ισχύουν τα εξής:*

1. $f(C \cap D) \subseteq f(C) \cap f(D)$.
2. $f(C \cup D) = f(C) \cup f(D)$.
3. $f^{-1}(R \cap S) = f^{-1}(R) \cap f^{-1}(S)$.
4. $f^{-1}(R \cup S) = f^{-1}(R) \cup f^{-1}(S)$.
5. $C \subseteq f^{-1}(f(C))$.
6. $f(f^{-1}(R)) \subseteq R$.

Απόδειξη. Η απόδειξη των ανωτέρω ισχυρισμών είναι εύκολη.

Εδώ, ενδεικτικά, θα αποδείξουμε το (2) και το (6), αφήνοντας τα υπόλοιπα ως άσκηση.

(2). Έστω $y \in f(C \cup D)$. Από τον Ορισμό 4.5.20, έπεται ότι υπάρχει $x \in C \cup D$ έτσι ώστε $y = f(x)$. Επειδή $x \in C \cup D$, έπεται ότι το

$$x \in C \text{ ή } x \in D.$$

Αν $x \in C$, τότε, πάλι από τον ίδιο ορισμό, έχουμε ότι

$$y = f(x) \in f(C).$$

Όμοια, αν $x \in D$, τότε $y = f(x) \in f(D)$. Σε κάθε περίπτωση έχουμε ότι

$$y = f(x) \in f(C) \cup f(D).$$

Δηλαδή αποδείξαμε ότι

$$f(C \cup D) \subseteq f(C) \cup f(D).$$

Αντίστροφα, Έστω $y \in f(C) \cup f(D)$, τότε $y \in f(C)$ ή $y \in f(D)$. Αν $y \in f(C)$, τότε υπάρχει $x \in C$, ώστε $y = f(x)$. Αν $y \in f(D)$, τότε υπάρχει $x \in D$, ώστε $y = f(x)$. Άρα πάντα υπάρχει ένα $x \in C \cup D$ με $y = f(x) \in f(C \cup D)$. Συνεπώς

$$f(C) \cup f(D) \subseteq f(C \cup D).$$

Από τις δύο σχέσεις εγκλεισμού

$$f(C \cup D) \subseteq f(C) \cup f(D) \text{ και } f(C) \cup f(D) \subseteq f(C \cup D)$$

έπεται το ζητούμενο.

(6). Έστω $y \in f(f^{-1}(R))$. Από τον Ορισμό 4.5.20, έπεται ότι υπάρχει $x \in f^{-1}(R)$ με $y = f(x)$. Τι σημαίνει $x \in f^{-1}(R)$; Πάλι από τον ίδιο ορισμό έχουμε ότι $y = f(x) \in R$. Άρα πράγματι ισχύει ότι

$$f(f^{-1}(R)) \subseteq R. \qquad \text{ό.έ.δ.}$$

Παρατηρήσεις 4.5.25.

1. Στο προηγούμενο θεώρημα παρατηρούμε ότι, ενώ στις περιπτώσεις 2, 3, 4 έχουμε ισότητες συνόλων, στην περίπτωση 1 έχουμε εγκλεισμό υποσυνόλων. Στο προηγούμενο παράδειγμα, όπου είχαμε την απεικόνιση $f : \mathbb{R} \longrightarrow \mathbb{R}$ με $f(x) = x^2$, θέτουμε

   $$C = \{-2\} \text{ και } D = \{2\}.$$

   Οπότε, $C \cap D = \emptyset$, άρα $f(C \cap D) = \emptyset$, ενώ $f(C) \cap f(D) = \{4\}$. Δηλαδή έχουμε

   $$f(C \cap D) \subsetneq f(C) \cap f(D).$$

   Πού οφείλεται αυτή η *παραφωνία;*

   Έστω $y \in f(C) \cap f(D)$, τότε υπάρχουν $c \in C$ και $d \in D$ με

   $$y = f(c) = f(d).$$

   Προσοχή! Δεν σημαίνει ότι $c = d$. Αν όμως η f ήταν 1-1, τότε $c = d \in C \cap D$ και συνεπώς

   $$y = f(c) = f(d) \in f(C \cap D).$$

   Άρα ικανή συνθήκη για να έχουμε $f(C \cap D) = f(C) \cap f(D)$ είναι η απεικόνιση f να είναι 1-1.

   Ισχύει και το αντίστροφο, ιδέ Άσκηση $4.5.5_2$.

2. Στο Παράδειγμα 4.5.23 είχαμε ήδη παρατηρήσει ότι εν γένει

$$C \neq f^{-1}(f(C)) \text{ και } f(f^{-1}(R)) \neq R.$$

Στο προηγούμενο θεώρημα είδαμε ότι ισχύει

$$C \subseteq f^{-1}(f(C)) \text{ και } f(f^{-1}(R)) \subseteq R.$$

Το ερώτημα που προκύπτει είναι το εξής: Υπό ποιες συνθήκες οι ανωτέρω εγκλεισμοί είναι ισότητες συνόλων;

Ας κάνουμε την ανάλυση του προβλήματος για την πρώτη περίπτωση. Αναρωτιόμαστε αν υπάρχει περίπτωση ώστε $f^{-1}(f(C)) \subseteq C$. Έστω $x \in f^{-1}(f(C))$, αυτό σημαίνει ότι $f(x) \in f(C)$. Από τον Ορισμό του συνόλου εικόνα έπεται ότι υπάρχει κάποιο $c \in C$, έτσι ώστε $f(x) = f(c)$ (Προσοχή! δεν σημαίνει ότι $x = c$). Αν όμως η απεικόνιση f ήταν 1-1, τότε από την σχέση $f(x) = f(c)$ αναγκαστικά θα είχαμε $x = c$, δηλαδή

$$f^{-1}(f(C)) \subseteq C.$$

Άρα ικανή συνθήκη για να έχουμε $f^{-1}(f(C)) = C$ είναι η απεικόνιση f να είναι 1-1.

Ας κάνουμε την ανάλυση του προβλήματος, για την δεύτερη περίπτωση. Αναρωτιόμαστε αν υπάρχει περίπτωση ώστε $R \subseteq f(f^{-1}(R))$. Έστω $y \in R$, αυτό δεν σημαίνει ότι υπάρχει $x \in A$, έτσι ώστε $f(x) = y$, διότι η f δεν είναι, κατ' ανάγκη, επί. Αν όμως η απεικόνιση f ήταν επί, τότε θα υπήρχε (τουλάχιστον) ένα $x \in A$ με $f(x) = y$. Τι σημαίνει αυτό; Από τον Ορισμό 4.5.20 έπεται ότι $x \in f^{-1}(R)$, δηλαδή $y = f(x) \in f(f^{-1}(R))$. Συνεπώς,

$$R \subseteq f(f^{-1}(R)).$$

Άρα ικανή συνθήκη για να έχουμε $R = f(f^{-1}(R))$ είναι η απεικόνιση f να είναι επί.

Για τις ανωτέρω περιπτώσεις ισχύει και το αντίστροφο, ιδέ Άσκηση $4.5.5_2$.

3. Θα μπορούσαμε να γενικεύσουμε το προηγούμενο θεώρημα. Αντί να πάρουμε την τομή και την ένωση δύο συνόλων, να πάρουμε την τομή και την ένωση οικογένειας συνόλων. Συγκεκριμένα, ισχύει η ακόλουθη Πρόταση:

Πρόταση 4.5.26. *Έστω $f : A \longrightarrow B$ μια απεικόνιση, $(A_i)_{i\in I}$ μια οικογένεια υποσυνόλων του πεδίου ορισμού A και $(B_j)_{j\in J}$ μια οικογένεια υποσυνόλων του πεδίου τιμών B. Τότε ισχύουν τα εξής:*

1. $f\left(\cap_{i\in I}A_i\right) \subseteq \cap_{i\in I}f\left(A_i\right)$.
2. $f\left(\cup_{i\in I}A_i\right) = \cup_{i\in I}f\left(A_i\right)$.
3. $f^{-1}\left(\cap_{j\in J}B_j\right) = \cap_{j\in J}f^{-1}\left(B_j\right)$.
4. $f^{-1}\left(\cup_{j\in J}B_j\right) = \cup_{j\in J}f^{-1}\left(B_j\right)$.

Απόδειξη. Η απόδειξη είναι ακριβώς η ίδια με την απόδειξη του προηγουμένου θεωρήματος. Απλώς να την επαναλάβετε. ό.έ.δ.

Παράδειγμα 4.5.27. Προηγουμένως, στο Παράδειγμα 4.5.11$_7$, είχαμε ορίσει την φυσική απεικόνιση. Συγκεκριμένα, αν έχουμε ένα σύνολο $(A, \sim)$ εφοδιασμένο με μια σχέση ισοδυναμίας και $A/\sim$ είναι το σύνολο πηλίκων της, τότε ορίζεται η (φυσική) απεικόνιση

$$\varphi : A \longrightarrow A/\sim \text{ με } \varphi(a) = C_a.$$

Τα στοιχεία του πεδίου τιμών είναι οι κλάσεις ισοδυναμίας C_a, δηλαδή είναι σύνολα.

Έστω το μονοσύνολο $\{C_a\}$ (υποσύνολο του πεδίου τιμών $A/\sim$), τότε η (πλήρης) αντίστροφη εικόνα του ορίζεται και είναι η

$$\varphi^{-1}(\{C_a\}) = C_a \text{ (γιατί;)}.$$

Εδώ θέλουμε να επισημάνουμε ότι είναι λάθος (δεν έχει νόημα) να γράφουμε $\varphi^{-1}(C_a)$, δεδομένου ότι η απεικόνιση φ δεν αντιστρέφεται και άρα δεν ορίζονται εικόνες (μέσω αυτής) στοιχείων του πεδίου τιμών $A/\sim$. Προσοχή! Μια κλάση ισοδυναμίας C_a είναι στοιχείο του πεδίου τιμών $A/\sim$, ενώ είναι υποσύνολο του πεδίου ορισμού A. Επομένως, η εικόνα $\varphi(C_a) = \{C_a\}$, αλλά είναι λάθος (δεν έχει νόημα) να γράφουμε $\varphi(C_a) = C_a$.

Όταν μελετούσαμε τις σχέσεις ισοδυναμίας, είχαμε δει ότι μια σχέση ισοδυναμίας σε ένα σύνολο ορίζει μια (μοναδική) διαμέριση στο σύνολο και αντίστροφα μια διαμέριση ενός συνόλου ορίζει (μοναδική) σχέση ισοδυναμίας στο σύνολο αυτό. Δηλαδή οι δύο έννοιες σχέση ισοδυναμίας και διαμέριση αποτελούν τις "δύο όψεις του ιδίου νομίσματος". Στο Παράδειγμα 4.5.11$_7$ είχαμε ορίσει την φυσική απεικόνιση. Θα δούμε ότι υπάρχει και μια "τρίτη όψη του ιδίου νομίσματος".

Πρόταση 4.5.28. *Έστω A ένα μη κενό σύνολο. Οι ακόλουθες Προτάσεις είναι ισοδύναμες.*

i. Στο σύνολο ορίζεται μια σχέση $\sim$, η οποία είναι σχέση ισοδυναμίας.

ii. Στο σύνολο A ορίζεται μια διαμέριση.

iii. Υπάρχει ένα σύνολο B και μια απεικόνιση $h : A \longrightarrow B$, η οποία είναι επί.

Απόδειξη. Οι Προτάσεις *i)* και *ii)* είναι ισοδύναμες (Προτάσεις 4.4.2 και 4.4.3).

Η *i)* συνεπάγεται την *iii)*. Είναι το Παράδειγμα 4.5.11$_7$.

Υποθέτουμε ότι ισχύει η *iii)*. Για κάθε $b \in B$ λαμβάνουμε το σύνολο

$$C_b = h^{-1}(\{b\}) \subseteq A.$$

Το σύνολο

$$\mathcal{D} = \{C_b \mid b \in B\}$$

αποτελεί μια διαμέριση του συνόλου A (γιατί;). Επομένως, από την *iii)* έπεται η *ii)*.

Εναλλακτικά, στο σύνολο A ορίζουμε μια σχέση ως εξής:

$$a_1 \sim a_2, \text{ αν } h(a_1) = h(a_2).$$

Η σχέση αυτή είναι σχέση ισοδυναμίας (γιατί;).

Σε κάθε περίπτωση, έχουμε αποδείξει την ισοδυναμία των τριών Προτάσεων. ό.έ.δ.

Έστω $f : A \longrightarrow B$ μια απεικόνιση και $M \subseteq A$, $N \subseteq B$. Στην αρχή της παραγράφου είχαμε δώσει τον ορισμό της εικόνας $f(M)$ του υποσυνόλου M και τον ορισμό της (πλήρους) αντίστροφης εικόνας του υποσυνόλου N (Ορισμός 4.5.20). Μετά είχαμε σχολιάσει (Σχόλια 4.5.22) την χρήση των συμβόλων f και f^{-1} (ακόμη και αν η απεικόνιση f δεν αντιστρέφεται). Εδώ θα τα εξετάσουμε υπό (ελαφρώς) διαφορετική γωνία.

Έστω $f : A \longrightarrow B$ μια απεικόνιση μεταξύ των συνόλων A και B. Ορίζουμε τις εξής απεικονίσεις:

$$f_* : \mathcal{P}(A) \longrightarrow \mathcal{P}(B) \quad \text{και} \quad f^* : \mathcal{P}(B) \longrightarrow \mathcal{P}(A) \text{ με}$$
$$f_*(X) = f(X), \text{ για κάθε } X \in \mathcal{P}(A) \quad \text{και} \quad f^*(Y) = f^{-1}(Y), \text{ για κάθε } Y \in \mathcal{P}(\mathrm{B}).$$

Είναι εύκολο να δούμε ότι οι δύο απεικονίσεις f_* και f^* είναι πράγματι απεικονίσεις. Οι f_* και f^* θα ονομάζονται οι **επαγόμενες απεικονίσεις** από την απεικόνιση f.

Όπως βλέπουμε, το σύνολο εικόνα $f(X)$ (βάσει του Ορισμού 4.5.20) είναι η εικόνα του στοιχείου $X \in \mathcal{P}(A)$ μέσω της απεικόνισης f_* και η (πλήρης) αντίστροφη εικόνα $f^{-1}(Y)$ (βάσει του Ορισμού 4.5.20) είναι η εικόνα του στοιχείου $Y \in \mathcal{P}(\mathrm{B})$ μέσω της απεικόνισης f^*. Η θεώρηση αυτή είναι πιο κομψή και τεχνικά ορθή. Παρ' όλα ταύτα, αν κάνουμε σωστή και συνειδητή χρήση των συμβόλων f και f^{-1} (ιδέ Σχόλια 4.5.22) δεν υπάρχει ανάγκη να "καταφεύγουμε" στις απεικονίσεις f_* και f^*.

Εδώ απλώς επισημαίνουμε ότι δεν ισχύει το αντίστροφο. Υπάρχουν απεικονίσεις

$$F : \mathcal{P}(A) \longrightarrow \mathcal{P}(B),$$

οι οποίες δεν επάγονται από κάποια απεικόνιση $f : A \longrightarrow B$ (ιδέ Άσκηση 4.5.5$_9$).

4.5.5 Ασκήσεις

1. Να αποδείξετε, με κάθε λεπτομέρεια, το Θεώρημα 4.5.24.

2. Έστω $f : A \longrightarrow B$ μια απεικόνιση.

   Δείξτε ότι η f είναι 1-1, αν και μόνο αν

   $$f(C \cap D) = f(C) \cap f(D), \text{ για κάθε } C, D \subseteq A.$$

   Δείξτε ότι η f είναι 1-1, αν και μόνο αν

   $$f^{-1}(f(C)) = C, \text{ για κάθε } C \subseteq A.$$

   Δείξτε ότι η απεικόνιση είναι επί, αν και μόνο αν

   $$f(f^{-1}(R)) = R, \text{ για κάθε } R \subseteq B.$$

3. Έστω $f : A \longrightarrow B$ μια απεικόνιση.

   Δείξτε ότι για κάθε $X \subseteq A$ και $Y \subseteq B$ ισχύει ότι:

   $$f(f^{-1}(f(X))) = f(X)$$
   $$f^{-1}(f(f^{-1}(Y))) = f^{-1}(Y).$$

4. Έστω $f : A \longrightarrow B$ μια απεικόνιση.

   Δείξτε ότι:

   Η f είναι 1-1, αν και μόνο αν για κάθε $b \in B$ το σύνολο $f^{-1}(\{b\})$ είναι το πολύ μονοσύνολο.

   Η f είναι επί, αν και μόνο αν, για κάθε $b \in B$ το σύνολο $f^{-1}(\{b\})$, είναι μη κενό.

   Η f είναι 1-1 και επί, αν και μόνο αν, για κάθε $b \in B$ το σύνολο $f^{-1}(\{b\})$, είναι μονοσύνολο.

5. Έστω η απεικόνιση $g : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ με

$$g(m, n) = 2^m 3^n.$$

   Αν $A = \{1, 2, 3\}$ και $B = \{1, 4, 6, 8, 9, 12\}$, να υπολογίσετε τα εξής σύνολα:

$$g(A \times A), \qquad g^{-1}(g(A \times A)), \qquad g^{-1}(B), \qquad g(g^{-1}(B)).$$

6. Έστω A, B δύο σύνολα και $X \subseteq A$, $Y \subseteq B$. Αν π_1 και π_2 είναι οι προβολές

$$\pi_1 : A \times B \longrightarrow A \quad \pi_2 : A \times B \longrightarrow B \text{ (ιδέ τον Ορισμό 4.5.8)},$$

   να υπολογίσετε τα σύνολα

$$\pi_1^{-1}(X),\ \pi_2^{-1}(Y) \text{ και } \pi_1^{-1}(X) \cap \pi_2^{-1}(Y).$$

   Έστω $P \subseteq A \times B$. Εξετάστε αν ισχύει

$$\pi_1(P) \times \pi_2(P) = P.$$

7. Έστω η απεικόνιση $f : A \longrightarrow B$, $K, L \subseteq A$ και $R, S \subseteq B$. Δείξτε ότι:

   i. $f(K) \setminus f(L) \subseteq f(K \setminus L)$.
      Ισχύει η αντίστροφη σχέση $f(K \setminus L) \subseteq f(K) \setminus f(L)$;
   ii. $f^{-1}(R) \setminus f^{-1}(S) = f^{-1}(R \setminus S)$.

8. Έστω η απεικόνιση $f : A \longrightarrow B$ και

$$f_* : \mathcal{P}(A) \longrightarrow \mathcal{P}(B) \text{ και } f^* : \mathcal{P}(B) \longrightarrow \mathcal{P}(A)$$

   οι επαγόμενες απεικονίσεις (ιδέ σελίδα 168). Δείξτε ότι:

   Η f_* είναι 1-1, αν και μόνο αν η f είναι 1-1.

   Η f_* είναι επί, αν και μόνο αν η f είναι επί.

   Η f^* είναι 1-1, αν και μόνο αν η f είναι επί.

   Η f^* είναι επί, αν και μόνο αν η f είναι 1-1.

   Η f^* είναι 1-1 και επί αν και μόνο αν η f_* είναι 1-1 και επί, αν και μόνο αν η f είναι 1-1 και επί.

   Υποθέτουμε ότι η f είναι 1-1 και επί. Τότε $f_*^{-1} = f^*$.

9. Δίνεται το σύνολο $A = \{1, 2, 3\}$ και η απεικόνιση $F : \mathcal{P}(A) \longrightarrow \mathcal{P}(A)$ με

$$F(\varnothing) = \{2\}, \quad F(\{1\}) = \varnothing, \quad F(\{2\}) = \{1\}, \quad F(\{1, 2\}) = \{1\}.$$

   Δείξτε ότι

$$F(\varnothing \cap \{2\}) \not\subseteq F(\varnothing) \cap F(\{2\}).$$

   Αυτό έρχεται σε *αντίφαση* με το Θεώρημα $4.5.24_1$; Αν ναι, τι πταίει;

   Να βρεθεί, αν υπάρχει, απεικόνιση $f : A \longrightarrow A$, έτσι ώστε $f_* = F$.

4.5.6 Η σύνθεση απεικονίσεων

Στην αρχή του κεφαλαίου (σελ. 119) είχαμε ορίσει την σύνθεση δύο σχέσεων. Συγκεκριμένα, αν έχουμε τρία σύνολα A, B, C και τις σχέσεις $\mathrm{R} \subseteq A \times B$ και $\mathrm{F} \subseteq B \times C$, τότε ορίζεται σύνθεση $\mathrm{F} \circ \mathrm{R}$ των δύο σχέσεων ως μια σχέση μεταξύ των συνόλων A και C ως εξής:

$$\mathrm{F} \circ \mathrm{R} = \{(a, c), \text{ αν υπάρχει } b \in B \text{ έτσι ώστε } (a, b) \in \mathrm{R} \text{ και } (b, c) \in \mathrm{F}\} \subseteq A \times C.$$

Δηλαδή έχουμε ότι $a\,\mathrm{R}\,b$ και $b\,\mathrm{F}\,c \implies a\,(\mathrm{F} \circ \mathrm{R})\,c$.

Όπως γνωρίζουμε, οι απεικονίσεις είναι ειδικού τύπου σχέσεις μεταξύ συνόλων. Επομένως, αν $f : A \longrightarrow B$ και $g : B \longrightarrow C$ είναι δύο απεικονίσεις, τότε ορίζεται η σύνθεσή τους $g \circ f$ ως μια σχέση μεταξύ των συνόλων A και C. Το ερώτημα, που προκύπτει, είναι το εξής:

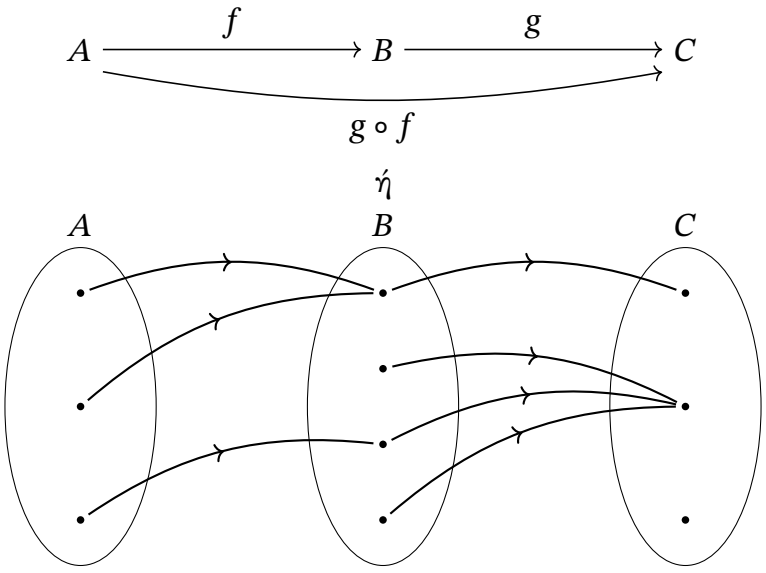
> Είναι η σύνθεση $g \circ f$ των δύο απεικονίσεων απεικόνιση;

Η απάντηση είναι καταφατική. Πράγματι, αν ανατρέξουμε στον ορισμό της σύνθεσης σχέσεων, θα παρατηρήσουμε ότι ένα στοιχείο $a \in A$ σχετίζεται με ένα στοιχείο $c \in C$, μέσω της σύνθεσης, αν υπάρχει $b \in B$ με την ιδιότητα $f(a) = b$ και $g(b) = c$. Αλλά για κάθε $a \in A$ υπάρχει μοναδικό $b \in B$ με $f(a) = b$ (γιατί;). Μα αφού η f είναι απεικόνιση. Επίσης, για το $f(a) = b \in B$ υπάρχει μοναδικό $c \in C$ με $g(b) = g(f(a)) \in C$. Συνεπώς, για κάθε $a \in A$ υπάρχει το μοναδικό $c = g(f(a)) \in C$, ώστε $(a, c) \in g \circ f$. Δηλαδή η σύνθεση $g \circ f$ είναι απεικόνιση, μάλιστα δε ισχύει

$$(g \circ f)(a) = g(f(a)), \text{ για κάθε } a \in A.$$

Άρα συμπερασματικά, αν έχουμε δύο απεικονίσεις f και g, όπου το πεδίο τιμών της f ισούται με το πεδίο ορισμού της g, τότε η σύνθεση $g \circ f$ των δύο απεικονίσεων είναι απεικόνιση.

Διαγραμματικά η σύνθεση δύο απεικονίσεων θα μπορούσε να παρασταθεί όπως φαίνεται στο σχήμα 4.7.



Σχήμα 4.7: *Σύνθεση απεικονίσεων.*

Σχόλια 4.5.29.

1. Αν και η απεικόνιση f "εφαρμόζεται" πρώτα και μετά "ακολουθεί" η απεικόνιση g, έχει επικρατήσει ο συμβολισμός $g \circ f$, όπου πρώτα γράφουμε την g και μετά την f. Αυτό ενδέχεται στην αρχή να μας δημιουργεί προβλήματα, δεδομένου ότι στην ελληνική γλώσσα γράφουμε από τα αριστερά προς τα δεξιά. Αλλά η προσεκτική και συνειδητή χρήση αυτού του συμβολισμού, με την *τριβή* δεν θα μας δημιουργεί προβλήματα[25].

2. Το σύμβολο $g \circ f$ είναι το όνομα μιας νέας απεικόνισης και ο συμβολισμός $(g \circ f)(x)$ αναφέρεται στην εικόνα του προτύπου x. Επομένως, είναι λάθος να λέμε και να γράφουμε η απεικόνιση $(g \circ f)(x)$. Επίσης, η γραφή $g \circ f(x)$ είναι παντελώς λάθος, καθ' ότι το σύμβολο $\circ$ συνθέτει δύο απεικονίσεις και όχι μια απεικόνιση, την g, και ένα στοιχείο, το $f(x)$.

3. Έστω $f : A \longrightarrow A$ μια απεικόνιση. Για κάθε $n \in \mathbb{N}$ μπορούμε αναδρομικά να ορίσουμε τις απεικονίσεις $f^n : A \longrightarrow A$, όπου

$$f^1 = f,\ f^2 = f \circ f,\ \ldots,\ f^{n+1} = f^n \circ f.$$

4. Προηγουμένως, είδαμε ότι, για να είναι η σύνθεση $g \circ f$ δύο απεικονίσεων απεικόνιση, αρκεί το πεδίο τιμών της f να ισούται με το πεδίο ορισμού της g. Είναι η συνθήκη αυτή αναγκαία;

   Αν παρατηρήσουμε πιο προσεκτικά θα δούμε ότι, αν το σύνολο τιμών της απεικόνισης f είναι υποσύνολο του πεδίου ορισμού, της απεικόνισης g, τότε η σύνθεση $g \circ f$ είναι απεικόνιση. Μάλιστα δε η συνθήκη αυτή είναι αναγκαία (γιατί;). Ιδέ άσκηση 4.5.7$_2$ και Παράδειγμα 4.5.30$_3$.

Παραδείγματα 4.5.30.

1. Έστω P το σύνολο όλων των κατοίκων της γης και $h : P \longrightarrow P$ η απεικόνιση, η οποία απεικονίζει κάθε άνθρωπο στην μητέρα του. Τότε ορίζεται η σύνθεση $h \circ h$ και είναι μια απεικόνιση, η οποία απεικονίζει κάθε άνθρωπο στην γιαγιά του (από την πλευρά της μητέρας του).

2. Έστω $A = \{a, b, c, d\}$, $B = \{1, 3, 5, 7\}$, $C = \{2, 4, 6, 8\}$.

   Ορίζουμε τις εξής απεικονίσεις:

$$\begin{array}{lll} f : A \longrightarrow B & \text{και} & g : B \longrightarrow C \quad \text{με} \\ f = \{(a, 1), (b, 3), (c, 1), (d, 7)\} & \text{και} & g = \{(1, 2), (3, 4)(5, 6), (7, 8)\}. \end{array}$$

   Η σύνθεση $g \circ f : A \longrightarrow C$ είναι η απεικόνιση

$$g \circ f = \{(a, 2), (b, 4), (c, 2), (d, 8)\}.$$

[25] Φανταστείτε πόσο πιο αποτελεσματικό θα ήταν σε μια απεικόνιση f για την εικόνα ενός στοιχείου x του πεδίου ορισμού της, αντί του $f(x)$, να γράφαμε $(x)f$ (πρώτα γράφουμε το πρότυπο επί του οποίου "δρα" η f). Οπότε, για την σύνθεση θα είχαμε $((x)f)g$ (γράφουμε από τα αριστερά προς τα δεξιά). Αλλά η μακρόχρονη χρήση του συμβολισμού $g(f(x))$ *...έχει δημιουργήσει δίκαιο.*

3. Δίνονται οι απεικονίσεις $f : \mathbb{R} \longrightarrow \mathbb{R}$ και $g : \mathbb{R} \setminus \{-1\}$ με

$$f(x) = x^2 + 1 \text{ και } g(x) = \frac{1}{x+1}.$$

Παρατηρούμε ότι το σύνολο τιμών της f είναι το

$$f(\mathbb{R}) = \{r \in \mathbb{R} \mid r \geq 1\},$$

το οποίο είναι υποσύνολο του πεδίου ορισμού της g, το $\mathbb{R} \setminus \{-1\}$. Επομένως, για κάθε $x \in \mathbb{R}$ έχουμε ότι η εικόνα του μέσω της f, η

$$f(x) = x^2 + 1 \in \mathbb{R} \setminus \{-1\},$$

συνεπώς ορίζεται η εικόνα

$$g(f(x)) = \frac{1}{f(x)+1} = \frac{1}{x^2+2}.$$

Άρα πράγματι η σύνθεση $g \circ f$ είναι απεικόνιση.

4. Έστω οι απεικονίσεις $\vartheta : \mathbb{R} \longrightarrow \mathbb{R}$ και $\varphi : \mathbb{R} \longrightarrow \mathbb{R}$ με

$$\vartheta(x) : x^2 + x - 1 \text{ και } \varphi(x) = x^2 + 1.$$

Για την σύνθεση $\vartheta \circ \varphi$ έχουμε

$$\begin{aligned}(\vartheta \circ \varphi)(x) &= \vartheta(\varphi(x)) \\ &= \vartheta(x^2+1) \\ &= (x^2+1)^2 + (x^2+1) - 1 \\ &= x^4 + 3x^2 + 1.\end{aligned}$$

Για την σύνθεση $\varphi \circ \vartheta$ έχουμε

$$\begin{aligned}(\varphi \circ \vartheta)(x) &= \varphi(\vartheta(x)) \\ &= \varphi(x^2 + x - 1) \\ &= (x^2 + x - 1)^2 + 1 \\ &= x^4 + x^2 + 1 + 2x^3 - 2x^2 - 2x + 1 \\ &= x^4 + 2x^3 - x^2 - 2x + 2.\end{aligned}$$

Όπως βλέπουμε, από το τελευταίο παράδειγμα, γενικά οι δύο απεικονίσεις $\vartheta \circ \varphi$ και $\varphi \circ \vartheta$ δεν είναι ίσες. Δηλαδή,

"Η σύνθεση απεικονίσεων δεν είναι μεταθετική" ($\vartheta \circ \varphi \neq \varphi \circ \vartheta$).

Πρόταση 4.5.31. *Έστω $f : A \longrightarrow B$, $g : B \longrightarrow C$, $h : C \longrightarrow D$ τρεις απεικονίσεις. Τότε ισχύει ότι*

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Δηλαδή ισχύει *"Ο νόμος της προσεταιριστικότητας στην σύνθεση απεικονίσεων"*. Επομένως, θα μπορούμε να γράφουμε (χωρίς παρενθέσεις) $h \circ g \circ f$.

Απόδειξη. Έστω $x \in A$, τότε

$$\begin{aligned}(h \circ (g \circ f))(x) &= h((g \circ f)(x)) \\ &= h(g(f(x))) \\ &= (h \circ g)(f(x)) \\ &= ((h \circ g) \circ f)(x).\end{aligned}$$

Όλες οι ισότητες είναι προφανείς από τον ορισμό της σύνθεσης απεικονίσεων. Επομένως, οι απεικονίσεις είναι ίσες, δεδομένου ότι έχουν το ίδιο πεδίο ορισμού, το σύνολο A και το ίδιο πεδίο τιμών, το D. ό.έ.δ.

Έστω $f : A \longrightarrow B$ μια αντιστρέψιμη απεικόνιση. Στην Παρατήρηση 4.5.17 είχαμε παρατηρήσει ότι για κάθε $x \in A$ ισχύει ότι

$$f^{-1}(f(x)) = x = 1_A(x)$$

και για κάθε $y \in B$ ισχύει ότι

$$f(f^{-1}(y)) = y = 1_B(y),$$

όπου 1_A και 1_B είναι οι ταυτοτικές απεικονίσεις στα σύνολα A και B αντίστοιχα. Από τον ορισμό της σύνθεσης απεικονίσεων έχουμε ότι

$$f^{-1}(f(x)) = (f^{-1} \circ f)(x).$$

Όμοια

$$f(f^{-1}(y)) = (f \circ f^{-1})(y).$$

Συνεπώς, ισχύει ότι

$$f^{-1} \circ f = 1_A \text{ και } f \circ f^{-1} = 1_B$$[26]

Έστω $f : A \longrightarrow B$ και $g : B \longrightarrow C$ δύο απεικονίσεις και $g \circ f$ η σύνθεσή τους. Ένα ερώτημα που προκύπτει είναι κατά πόσον από ιδιότητες των απεικονίσεων f και g μπορούμε να εξάγουμε συμπεράσματα για ιδιότητες της σύνθεσης $g \circ f$ και αντίστροφα, από ιδιότητες της σύνθεσης $g \circ f$ να εξάγουμε συμπεράσματα για τις απεικονίσεις f και g. Ας γίνουμε πιο συγκεκριμένοι.

Θεώρημα 4.5.32. *Έστω A, B, C τρία μη κενά σύνολα και $f : A \longrightarrow B$, $g : B \longrightarrow C$ δύο απεικονίσεις.*

i. Υποθέτουμε ότι οι f και g είναι 1-1, τότε και η σύνθεση $g \circ f$ είναι 1-1.

ii. Υποθέτουμε ότι οι f και g είναι επί, τότε και η σύνθεση $g \circ f$ είναι επί.

iii. Υποθέτουμε ότι οι f και g είναι 1-1 και επί, τότε και η σύνθεση $g \circ f$ είναι 1-1 και επί.

Μάλιστα δε ισχύει ότι $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Απόδειξη.

[26] Πολλοί συγγραφείς δίνουν τον εξής ορισμό της αντιστρέψιμης απεικόνισης. "Έστω $f : A \longrightarrow B$ μια απεικόνιση. Η f ονομάζεται αντιστρέψιμη αν υπάρχει μια $f^{-1} : B \longrightarrow A$ απεικόνιση, ώστε $f^{-1} \circ f = 1_A$ και $f \circ f^{-1} = 1_B$."

i. Θέλουμε να δείξουμε ότι η σύνθεση $g \circ f$ είναι 1-1. Έστω $x_1, x_2 \in A$, το πεδίο ορισμού της $g \circ f$. Υποθέτουμε ότι

$$x_1 \neq x_2.$$

Επειδή η f έχει υποτεθεί 1-1, έπεται ότι

$$f(x_1) \neq f(x_2).$$

Οι εικόνες $f(x_1)$ και $f(x_2)$ ανήκουν στο B, το οποίο είναι το πεδίου ορισμού της g, η οποία έχει υποτεθεί 1-1, συνεπώς

$$g(f(x_1)) \neq g(f(x_2)).$$

Δηλαδή

$$(g \circ f)(x_1) \neq (g \circ f)(x_2).$$

Άρα αποδείξαμε ότι η απεικόνιση $g \circ f$ είναι 1-1.

ii. Θέλουμε να δείξουμε ότι η σύνθεση $g \circ f$ είναι επί. Έστω

$$c \in C,$$

το πεδίο τιμών της σύνθεσης $g \circ f$, το οποίο είναι και πεδίο τιμών της απεικόνισης g. Η απεικόνιση g έχει υποτεθεί επί, επομένως υπάρχει $b \in B$, το οποίο είναι το πεδίο ορισμού της, έτσι ώστε

$$g(b) = c.$$

Αλλά το σύνολο B είναι και πεδίο τιμών της απεικόνισης f, η οποία έχει υποτεθεί επί. Συνεπώς, υπάρχει $a \in A$, έτσι ώστε

$$f(a) = b.$$

Οπότε, αντικαθιστώντας στην σχέση $g(b) = c$, έχουμε $g(f(a)) = c$. Δηλαδή

$$(g \circ f)(a) = c.$$

Άρα για το (τυχαίο) $c \in C$, του πεδίου τιμών της σύνθεσης $g \circ f$, υπάρχει $a \in A$, στο πεδίο ορισμού της σύνθεσης $g \circ f$, έτσι ώστε

$$(g \circ f)(a) = c,$$

συνεπώς η σύνθεση $g \circ f$ είναι επί.

iii. Το ότι η η σύνθεση $g \circ f$ είναι 1-1 και επί είναι προφανές από τα προηγούμενα.

Αφού οι f και g είναι αντιστρέψιμες, ορίζονται οι απεικονίσεις

$$f^{-1} : B \longrightarrow A, g^{-1} : C \longrightarrow B$$

καθώς και η σύνθεση

$$f^{-1} \circ g^{-1} : C \longrightarrow A.$$

Έστω $z \in C$. Επειδή η g είναι 1-1 και επί, υπάρχει μοναδικό $y \in B$, έτσι ώστε $g(y) = z$. Αυτό σημαίνει

$$g^{-1}(z) = y.$$

Επειδή η f είναι 1-1 και επί, υπάρχει μοναδικό $x \in A$ με $f(x) = y$. Αυτό σημαίνει

$$f^{-1}(y) = x.$$

Από τις σχέσεις $g(y) = z$ και $f(x) = y$ έπεται ότι για το (τυχαίο) $z \in C$ υπάρχει το $x \in A$ με $(g \circ f)(x) = z$. Αυτό σημαίνει ότι

$$(g \circ f)^{-1}(z) = x.$$

Επίσης, από τις σχέσεις $g^{-1}(z) = y$ και $f^{-1}(y) = x$ έπεται ότι για το (τυχαίο) $z \in C$ υπάρχει το $x \in A$, έτσι ώστε

$$(f^{-1} \circ g^{-1})(z) = x.$$

Δηλαδή αποδείξαμε ότι για κάθε $z \in C$ ισχύει ότι

$$(g \circ f)^{-1}(z) = (f^{-1} \circ g^{-1})(z).$$

Άρα $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ (Ο ορισμός της ισότητας απεικονίσεων). ό.έ.δ.

Θεώρημα 4.5.33. [27] *Έστω A, B, C τρία μη κενά σύνολα και $f : A \longrightarrow B$, $g : B \longrightarrow C$ δύο απεικονίσεις.*

i. Υποθέτουμε ότι σύνθεση $g \circ f$ είναι 1-1, τότε η f είναι 1-1.

ii. Υποθέτουμε ότι σύνθεση $g \circ f$ είναι επί, τότε η g είναι επί.

Απόδειξη.

i. Για να δείξουμε ότι η απεικόνιση f είναι 1-1, πρέπει και αρκεί να αποδείξουμε ότι για $x_1, x_2 \in A$ με $x_1 \neq x_2$, έπεται ότι $f(x_1) \neq f(x_2)$.

Έστω $x_1, x_2 \in A$ με

$$x_1 \neq x_2.$$

Υποθέτουμε ότι $f(x_1) = f(x_2)$. Επομένως, επειδή η g είναι απεικόνιση, θα έχουμε $g(f(x_1)) = g(f(x_2))$. Δηλαδή

$$(g \circ f)(x_1) = (g \circ f)(x_2).$$

Αυτό όμως είναι άτοπο, διότι έχει υποτεθεί ότι η σύνθεση $g \circ f$ είναι 1-1, της οποίας το πεδίο ορισμού είναι το σύνολο A. Άρα,

$$f(x_1) \neq f(x_2),$$

δηλαδή η f είναι 1-1.

ii. Για να δείξουμε ότι η απεικόνιση g είναι επί, πρέπει και αρκεί να αποδείξουμε ότι για κάθε $c \in C$ υπάρχει $b \in B$ με $g(b) = c$. Έστω $c \in C$, η σύνθεση $g \circ f$ έχει υποτεθεί ότι είναι επί. Συνεπώς, για το $c \in C$ υπάρχει $a \in A$, έτσι ώστε $(g \circ f)(a) = c$, δηλαδή $g(f(a)) = c$. Επομένως, το $b = f(a) \in B$ έχει την ιδιότητα $g(b) = c$. Άρα η g είναι επί. ό.έ.δ.

[27] Το Θεώρημα αυτό είχε τεθεί "προκλητικά" ως άσκηση στο προηγούμενο κεφάλαιο (Άσκηση $3.2.6_{10}$).

Παρατήρηση 4.5.34. Στο Θεώρημα 4.5.32 βλέπουμε ότι μια ικανή συνθήκη, για να είναι η σύνθεση $g \circ f$ δύο απεικονίσεων 1-1 (ή επί), είναι και οι δύο απεικονίσεις να είναι 1-1 (ή επί). Απεναντίας, στο Θεώρημα 4.5.33 βλέπουμε ότι μια αναγκαία συνθήκη για να είναι η σύνθεση $g \circ f$ δύο απεικονίσεων 1-1, είναι μόνο η απεικόνιση f να είναι 1-1. Επίσης, μια αναγκαία συνθήκη για να είναι η σύνθεση $g \circ f$ δύο απεικονίσεων επί, είναι μόνο η απεικόνιση g να είναι επί. Δηλαδή, ενδέχεται η σύνθεση $g \circ f$ να είναι 1-1, χωρίς να είναι αναγκαστικά η g 1-1. Επίσης, ενδέχεται η σύνθεση $g \circ f$ να είναι επί, χωρίς να είναι αναγκαστικά η f επί. Στην Άσκηση $4.5.7_1$ καλείστε να διερευνήσετε περιπτώσεις που δεν "καλύπτονται" από τα δύο ανωτέρω θεωρήματα.

Γενίκευση της αντιστρέψιμης απεικόνισης. Αντιστρέψιμες από τα δεξιά και αντιστρέψιμες από τα αριστερά απεικονίσεις.

Έστω A, B, C τρία μη κενά σύνολα και $f : A \longrightarrow B$, $g : B \longrightarrow C$ δύο απεικονίσεις. Από την προηγουμένη παρατήρηση βλέπουμε ότι είναι αναγκαίο η απεικόνιση f να είναι 1-1 (αλλά δεν είναι ικανό από μόνο του), για να είναι η σύνθεση $g \circ f$ 1-1. Όπως επίσης, είναι αναγκαίο η απεικόνιση g να είναι επί (αλλά δεν είναι ικανό από μόνο του) για να είναι η σύνθεση $g \circ f$ επί. Επίσης, στα Σχόλια $4.5.29_3$ είχαμε δει ότι, αν το σύνολο τιμών $f(A)$ της f είναι υποσύνολο του πεδίου τιμών B της g, τότε πάντα ορίζεται η σύνθεση $g \circ f$. Όλα αυτά μας οδηγούν στα εξής ερωτήματα:

> "Έστω μία απεικόνιση $f : A \longrightarrow B$, η οποία είναι 1-1. Υπάρχει απεικόνιση $h : B \longrightarrow A$, ώστε η σύνθεση $h \circ f$ να είναι αντιστρέψιμη απεικόνιση;"
>
> "Έστω μία απεικόνιση $f : A \longrightarrow B$, η οποία είναι επί. Υπάρχει απεικόνιση $g : B \longrightarrow A$, ώστε η σύνθεση $f \circ g$ να είναι αντιστρέψιμη απεικόνιση;".

Η απάντηση και στα δύο αυτά ερωτήματα είναι καταφατική. Μάλιστα δε οι απεικονίσεις, που μπορούμε να κατασκευάσουμε, είναι *πολύ καλές*.

Ας απαντήσουμε στο πρώτο ερώτημα. Έχουμε ως υπόθεση ότι η απεικόνιση f είναι 1-1. Θεωρούμε το σύνολο τιμών της $f(A)$. Ορίζουμε την απεικόνιση $\varphi : f(A) \longrightarrow A$ ως εξής:

$$\varphi(f(a)) = a, \text{ για κάθε } f(a) \in f(A).$$

Η φ είναι πράγματι απεικόνιση, διότι κάθε στοιχείο του συνόλου $f(A)$ είναι της μορφής $f(a)$ με $a \in A$ και η απεικόνιση f έχει υποτεθεί ότι είναι 1-1. Προσοχή! Η απεικόνιση φ **δεν** είναι (κατ' ανάγκη) αντίστροφη της f (γιατί;).

Έστω $h : B \longrightarrow A$ μια επέκταση της φ, δηλαδή

$$h_{|f(A)} = \varphi.$$

Πάντα ορίζεται (τουλάχιστον) μια τέτοια επέκταση (γιατί; Ανατρέξτε στον Ορισμό 4.5.8). Αν λάβουμε την σύνθεση

$$A \xrightarrow{f} B \xrightarrow{h} A,$$

παρατηρούμε ότι, για κάθε $a \in A$, έχουμε

$$(h \circ f)(a) = h(f(a)) = \varphi(f(a)) = a.$$

Άρα

$$h \circ f = 1_A.$$

Μια απεικόνιση $h : B \longrightarrow A$, με την ιδιότητα

$$h \circ f = 1_A,$$

Θα ονομάζεται **αριστερή αντίστροφη** της f.

Ας απαντήσουμε στο δεύτερο ερώτημα. Έχουμε ως υπόθεση ότι η απεικόνιση f είναι επί. Αυτό σημαίνει ότι για κάθε $b \in B$ υπάρχει (τουλάχιστον) ένα $a \in A$, έτσι ώστε $f(a) = b$, δηλαδή το σύνολο $f^{-1}(\{b\})$ δεν είναι το κενό σύνολο (ιδέ και Άσκηση $4.5.5_4$).

Ορίζουμε την απεικόνιση $g : B \longrightarrow A$ ως εξής: Για κάθε $b \in B$ επιλέγουμε (και σταθεροποιούμε) ένα $a \in f^{-1}(\{b\})$ και ορίζουμε $g(b) = a$. Η g είναι πράγματι απεικόνιση, διότι για κάθε $b \in B$ υπάρχει το μοναδικό $a \in A$, το οποίο επιλέξαμε και σταθεροποιήσαμε, έτσι ώστε $g(b) = a$. Αν λάβουμε την σύνθεση

$$B \xrightarrow{g} A \xrightarrow{f} B,$$

παρατηρούμε ότι, για κάθε $b \in B$, έχουμε

$$(f \circ g)(b) = f(g(b)) = f(a) = b,$$

δεδομένου ότι $a \in f^{-1}(\{b\})$. Άρα

$$f \circ g = 1_B.$$

Μια απεικόνιση $g : B \longrightarrow A$, με την ιδιότητα

$$f \circ g = 1_B,$$

Θα ονομάζεται **δεξιά αντίστροφη** της f.

Όλα τα ανωτέρω συνοψίζονται στο εξής Θεώρημα:

Θεώρημα 4.5.35. *Έστω $f : A \longrightarrow B$.*

i. *Υπάρχει μια αριστερή αντίστροφη απεικόνιση $h : B \longrightarrow A$ της f, αν και μόνο αν η f είναι 1-1.*

ii. *Υπάρχει μια δεξιά αντίστροφη απεικόνιση $g : B \longrightarrow A$ της f, αν και μόνο αν η f είναι επί.*

iii. *Η απεικόνιση f έχει αριστερή και δεξιά αντίστροφη, αν και μόνο αν είναι αντιστρέψιμη.*

   Στην περίπτωση αυτή υπάρχει μόνο μια αριστερή και μόνο μια δεξιά αντίστροφη και είναι ίσες με την (μοναδική) αντίστροφη απεικόνιση της f.

Απόδειξη. Η απόδειξη, στην πραγματικότητα έχει προηγηθεί, δεδομένου ότι ισχύει και το Θεώρημα 4.5.33.

Εδώ να την επαναλάβετε με κάθε λεπτομέρεια. ό.έ.δ.

4.5.7 Ασκήσεις

1. Στις ακόλουθες περιπτώσεις να δώσετε ένα παράδειγμα ή να εξηγήσετε γιατί δεν υπάρχει τέτοιο παράδειγμα απεικονίσεων $f : A \longrightarrow B$ και $g : B \longrightarrow C$, οι οποίες να ικανοποιούν τους ακόλουθους ισχυρισμούς:

   (α) Η απεικόνιση f είναι επί, αλλά η σύνθεση $g \circ f$ δεν είναι επί.

   (β) Η απεικόνιση f είναι 1-1, αλλά η σύνθεση $g \circ f$ δεν είναι 1-1.

   (γ) Η απεικόνιση g είναι επί, αλλά η σύνθεση $g \circ f$ δεν είναι επί.

   (δ) Η απεικόνιση g είναι 1-1, αλλά η σύνθεση $g \circ f$ δεν είναι 1-1.

   (ε) Η απεικόνιση f δεν είναι επί, αλλά η σύνθεση $g \circ f$ είναι επί.

   (στ) Η απεικόνιση f δεν είναι 1-1, αλλά η σύνθεση $g \circ f$ είναι 1-1.

   (ζ) Η απεικόνιση g δεν είναι επί, αλλά η σύνθεση $g \circ f$ είναι επί.

   (η) Η απεικόνιση g δεν είναι 1-1, αλλά η σύνθεση $g \circ f$ είναι 1-1.

2. Έστω οι απεικονίσεις $f : A \longrightarrow B$ και $g : C \longrightarrow D$. Δείξτε ότι η σύνθεση $g \circ f$ είναι απεικόνιση αν και μόνο το σύνολο τιμών της f είναι υποσύνολο του πεδίου ορισμού της g. Δηλαδή $f(A) \subseteq C$.

3. Να βρεθούν δύο απεικονίσεις $f,\ g : \mathbb{R} \longrightarrow \mathbb{R}$, οι οποίες να μην είναι σταθερές, αλλά η σύνθεση $g \circ f$ να είναι σταθερή απεικόνιση.

4. Έστω $A = \{1, 2, 3\}$ και οι απεικονίσεις $f, g : A \longrightarrow A$ με

$$f = \{(1, 2), (2, 1), (3, 2)\} \text{ και } g = \{(1, 2), (2, 3), (3, 3)\}.$$

   Να υπολογίσετε τις συνθέσεις

$$f \circ g \text{ και } g \circ f.$$

5. Έστω οι απεικονίσεις $f, g : \mathbb{R} \longrightarrow \mathbb{R}$ με

$$f(x) = \frac{1}{x^2 + 1} \text{ και } g(x) = 2x - 1.$$

   Για κάθε $x \in \mathbb{R}$ να υπολογίσετε τις εικόνες $(g \circ f)(x)$ και $(f \circ g)(x)$.

6. Έστω οι απεικονίσεις $f, g : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ με

$$f(m, n) = (mn, m^2) \text{ και } g(m, n) = (m + 1, m - n).$$

   i. Για κάθε $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ να υπολογίσετε τις εικόνες

$$f^2(m, n),\ g^2(m, n), (g \circ f)(m, n) \text{ και } (f \circ g)(m, n).$$

   ii. Να δείξετε ότι η απεικόνιση g είναι αντιστρέψιμη και να υπολογίσετε την εικόνα

$$(g^{-1} \circ f \circ g)(m, n),$$

   για κάθε $(m, n) \in \mathbb{Z} \times \mathbb{Z}$.

7. Έστω $a, b \in R$ και $f : \mathbb{R} \longrightarrow \mathbb{R}$ με $f(x) = ax + b$.

   Για κάθε $n \in \mathbb{N}$ να υπολογίσετε την εικόνα $f^n(x)$, για κάθε $x \in \mathbb{R}$.

   Υποθέτουμε ότι $a \neq 0$. Να υπολογίσετε την $(f^3)^{-1}$.

   Επιλέγουμε και σταθεροποιούμε ένα $r \in \mathbb{R}$ και ορίζουμε την απεικόνιση

   $$\varphi : \mathbb{N} \longrightarrow \mathbb{R} \text{ με } \varphi(n) = f^n(r).$$

   Να δώσετε μια ικανή και αναγκαία συνθήκη, ώστε η φ να είναι 1-1.

8. Έστω οι απεικονίσεις

   $$f : [0, \infty) \longrightarrow \mathbb{R} \text{ με } f(x) = x^3 + 4 \text{ και}$$
   $$g : \mathbb{R} \longrightarrow [0, \infty) \text{ με } g(x) = | x |.$$

   Να βρεθούν δύο αριστερά αντίστροφες απεικονίσεις για την απεικόνιση f και δύο δεξιά αντίστροφες απεικονίσεις για την απεικόνιση g.

9. Έστω $f : A \longrightarrow B$ μια απεικόνιση. Δείξτε ότι, αν η f έχει δύο διαφορετικές δεξιά αντίστροφες απεικονίσεις, τότε δεν έχει αριστερά αντίστροφη απεικόνιση.

   Δυϊκά, αν η f έχει δύο διαφορετικές αριστερά αντίστροφες απεικονίσεις, τότε δεν έχει δεξιά αντίστροφη απεικόνιση.

Βιβλιογραφία

[1] E.D. Bloch. *Proofs and Fundamentals: A first course in Abstract Mathematics*. Second Edition. Springer, 2011. ISBN: 978-14-4197-126-5.

[2] Richard Hammack. *Book of Proof*. Edition 2.2. Virginia Commonwealth University Richard Hammack (publisher). Department of Mathematics and Applied Mathematics, 2013.

[3] K. Houston. *How to Think Like a Mathematician*. Cambridge University Press, 2009. ISBN: 978-05-2189-546-0.

[4] M. Liebeck. *A Concise Introduction to Pure Mathematics*. Third Edition. Chapman Hall CRC Press, 2011. ISBN: 978-14-3983-598-2.

[5] T. Sundstrom. *Mathematical Reasoning, Writing and Proof*. Version 2.1 May 26. 2020.

[6] C. Schumacher. *Chapter Zero: Fundamental Notions of Abstract Mathematics*. Second Edition. Addison-Wesley, 2021. ISBN: 02-0143-724-4.

[7] I. Stewart & D. Tall. *The Foundations of Mathematics*. Second Edition. Oxford University Press, 2015.

ΚΕΦΑΛΑΙΟ 5

ΠΡΑΞΕΙΣ ΣΕ ΣΥΝΟΛΑ - ΑΛΓΕΒΡΙΚΕΣ ΔΟΜΕΣ

5.1 Πράξεις σε σύνολα

Στο προηγούμενο κεφάλαιο, όπου μελετήσαμε τις απεικονίσεις μεταξύ συνόλων, είχαμε δει παραδείγματα (και ασκήσεις) απεικονίσεων με πεδίο ορισμού το καρτεσιανό γινόμενο ενός συνόλου με τον εαυτό του και πεδίο τιμών το σύνολο αυτό. Για παράδειγμα, αναφέρουμε το Παράδειγμα 4.5.11$_5$ και την Άσκηση 4.5.3$_3$. Οι απεικονίσεις αυτές είναι πολύ σημαντικές, καθ' ότι, μέσω αυτού του είδους τις απεικονίσεις, μπορούμε να ορίσουμε "Αλγεβρική δομή" σε ένα σύνολο.

Ας γίνουμε πιο συγκεκριμένοι.

Ορισμός 5.1.1. Έστω A ένα (μη κενό) σύνολο. Μια απεικόνιση $\varphi : A \times A \longrightarrow A$ θα ονομάζεται (διμελής εσωτερική)[1] **πράξη** στο σύνολο A.

Μια πράξη $\varphi : A \times A \longrightarrow A$ σε ένα σύνολο, ως απεικόνιση είναι μια σχέση από το σύνολο $A \times A$ στο σύνολο A, επομένως είναι ένα υποσύνολο του συνόλου $(A \times A) \times A$ ($\varphi \subseteq (A \times A) \times A$). Μάλιστα, όπως είχαμε δει, αν η εικόνα ενός ζεύγους $(x, y) \in A \times A$ μέσω της φ είναι η z, τότε αντί του $\varphi(x, y) = z$, θα μπορούσαμε να γράψουμε $(x, y)\,\varphi\, z$.

Αντί όλων αυτών των συμβολισμών, για την πράξη $\varphi : A \times A \longrightarrow A$, έχει επικρατήσει ο εξής συμβολισμός: $x \varphi y = z$. Το στοιχείο z θα ονομάζεται το **αποτέλεσμα** της πράξης φ μεταξύ των στοιχείων x και y.

[1] Η απεικόνιση αυτή ονομάζεται διμελής, διότι "σχετίζει" δύο στοιχεία του συνόλου (τα μέλη ενός διατεταγμένου ζεύγους) με ένα τρίτο στοιχείο του ιδίου συνόλου. Με το ίδιο σκεπτικό, θα μπορούσαμε να ορίσουμε μια n-μελή πράξη ως μια απεικόνιση $\vartheta : \underbrace{A \times A \times \cdots \times A}_{n} \longrightarrow A$. Εμείς εδώ θα ασχοληθούμε με διμελείς πράξεις, τις οποίες θα αναφέρουμε απλώς ως πράξεις.

Επίσης, αντί των γραμμάτων $f, g, h, \varphi, \vartheta, \ldots$, τα οποία χρησιμοποιούμε συνήθως για τον συμβολισμό μιας απεικόνισης, για τον συμβολισμό μιας πράξης συνήθως χρησιμοποιούμε τα σύμβολα

$$+, \cdot, \circ, *, \odot, \ldots .$$

Όταν έχουμε μια πράξη $* : A \times A \longrightarrow A$ στο σύνολο A, τότε συνήθως συμβολίζουμε $(A, *)$ και λέμε ότι το σύνολο A είναι εφοδιασμένο με την πράξη $*$[2]. Όταν έχουμε ένα πεπερασμένο σύνολο, έστω $A = \{a_1, a_2, a_3, \ldots, a_n\}$, εφοδιασμένο με μια πράξη $*$, ορισμένες φορές, μας διευκολύνει να παραστήσουμε την πράξη με έναν πίνακα ως εξής:

$*$	a_1	a_2	$\cdot$	$\cdot$	$\cdot$	a_j	$\cdot$	$\cdot$	$\cdot$	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	$\cdot$	$\cdot$	$\cdot$	$a_1 * a_j$	$\cdot$	$\cdot$	$\cdot$	$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	$\cdot$	$\cdot$	$\cdot$	$a_2 * a_j$	$\cdot$	$\cdot$	$\cdot$	$a_2 * a_n$
$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
a_i	$a_i * a_1$	$a_i * a_2$	$\cdot$	$\cdot$	$\cdot$	$a_i * a_j$	$\cdot$	$\cdot$	$\cdot$	$a_i * a_n$
$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
a_n	$a_n * a_1$	$a_n * a_2$	$\cdot$	$\cdot$	$\cdot$	$a_n * a_j$	$\cdot$	$\cdot$	$\cdot$	$a_n * a_n$

Όπως παρατηρούμε, στην πρώτη θέση της πρώτης γραμμής του πίνακα εμφανίζεται το σύμβολο της πράξης και στις υπόλοιπες θέσεις εμφανίζονται τα στοιχεία του συνόλου A. Στην πρώτη θέση της πρώτης στήλης του πίνακα εμφανίζεται το σύμβολο της πράξης και στις υπόλοιπες θέσεις εμφανίζονται τα στοιχεία του συνόλου A (κατά προτίμηση με την ίδια διάταξη όπως στην πρώτη γραμμή). Σε κάθε άλλη θέση (i, j) εμφανίζεται το αποτέλεσμα της πράξης $a_i * a_j$. Ο πίνακας αυτός συνήθως ονομάζεται, **ο πίνακας** της πράξης $*$[3].

Από όλες τις πράξεις, οι οποίες είναι δυνατόν να οριστούν σε ένα σύνολο, ενδιαφέρον παρουσιάζουν αυτές, οι οποίες πληρούν κάποιες ιδιότητες.

Ορισμός 5.1.2. Έστω $(A, *)$ ένα σύνολο εφοδιασμένο με μια πράξη.

1. Η πράξη $*$ θα ονομάζεται **προσεταιριστική**, αν για $a, b, c \in A$ ισχύει ότι

$$a * (b * c) = (a * b) * c.$$

2. Η πράξη $*$ θα ονομάζεται **μεταθετική**, αν

$$a * b = b * a$$

για όλα τα $a, b \in A$.

3. Ένα στοιχείο $e \in A$ θα ονομάζεται **ουδέτερο** ή ταυτοτικό, αν

$$a * e = e * a = a,$$

για όλα τα $a \in A$.

Πριν προχωρήσουμε, μια απλή, αλλά σημαντική πρόταση.

[2] Ένα σύνολο εφοδιασμένο με μία πράξη ορισμένες φορές ονομάζεται **ομαδοειδές**, το δε σύνολο, επί του οποίου είναι ορισμένη η πράξη ονομάζεται υποκείμενο ή φέρον σύνολο.

[3] Η "όψη" του πίνακα εξαρτάται από την σειρά που αναγράφονται τα στοιχεία του συνόλου στην πρώτη γραμμή και πρώτη στήλη του πίνακα, αλλά στην πραγματικότητα πρόκειται για τον (ίδιο) πίνακα, ο οποίος παριστά την δομή του συνόλου ως προς την πράξη αυτή.

Πρόταση 5.1.3. *Έστω $(A, *)$ ένα σύνολο εφοδιασμένο με μια πράξη. Υποθέτουμε ότι υπάρχει ουδέτερο στοιχείο ως προς την πράξη $*$, τότε αυτό είναι μοναδικό.*

Απόδειξη. Υποθέτουμε ότι υπάρχουν δύο ουδέτερα στοιχεία, τα e και ϵ, τότε έχουμε

$$e * \epsilon = e \qquad \text{(το στοιχείο } \epsilon \text{ έχει υποτεθεί ουδέτερο)}$$

Επίσης

$$e * \epsilon = \epsilon \qquad \text{(το στοιχείο } e \text{ έχει υποτεθεί ουδέτερο)}$$

Επομένως

$$e = \epsilon.$$

ό.έ.δ.

Όταν η πράξη σε ένα σύνολο είναι προσεταιριστική, από την σχέση

$$a * (b * c) = (a * b) * c,$$

συμπεραίνουμε ότι δεν έχει σημασία η σειρά με την οποία "εκτελούμε" την πράξη, αρκεί να μην αλλάζουμε την σειρά των στοιχείων a, b, c. Επομένως, θα μπορούσαμε, παραλείποντας τις παρενθέσεις, να γράψουμε

$$a * (b * c) = (a * b) * c = a * b * c.$$

Όταν έχουμε τα στοιχεία $a_1, a_2, \ldots, a_n \in A$, τότε, διατηρώντας την σειρά των στοιχείων, μπορούμε, με την βοήθεια της πράξης, να υπολογίσουμε νέα στοιχεία. Για παράδειγμα:

$$(a_1 * a_2) * (a_3 * a_4) * a_5 * \cdots a_n \text{ ή } (a_1 * a_2 * \cdots * a_{n-1}) * a_n$$

κ.λ.π. Δυνητικά μπορούμε να υπολογίσουμε τόσα στοιχεία, όσοι είναι οι τρόποι παρεμβολής παρενθέσεων μεταξύ των στοιχείων $a_1, a_2, \ldots, a_n$, δεδομένου ότι η πράξη είναι διμελής και κάθε φορά μπορούμε να υπολογίσουμε το αποτέλεσμα της πράξης μεταξύ δύο στοιχείων. Η πράξη όμως έχει υποτεθεί ότι είναι προσεταιριστική και επομένως στην πραγματικότητα όλοι οι δυνατοί τρόποι, με τους οποίους μπορούμε να εκτελέσουμε τις πράξεις, δίνουν το ίδιο αποτέλεσμα. Συγκεκριμένα έχουμε:

Πρόταση 5.1.4. *Έστω $(A, *)$ ένα σύνολο εφοδιασμένο με μια προσεταιριστική πράξη. Τότε, με οποιονδήποτε τρόπο εκτελέσουμε τις πράξεις μεταξύ των στοιχείων $a_1, a_2, \ldots, a_n$ (διατηρώντας την σειρά), επιτυγχάνουμε το ίδιο αποτέλεσμα.*

Απόδειξη. Θα εφαρμόσουμε επαγωγή επί του n. Προφανώς, για $n = 2$ ή $n = 3$ ο ισχυρισμός ισχύει. Υποθέτουμε ότι για κάθε $3 \leq k < n$ ο ισχυρισμός ισχύει. Δηλαδή, για τα στοιχεία $a_1, a_2, \ldots, a_k$ με $k < n$ όλοι οι τρόποι εκτέλεσης των πράξεων δίνουν το ίδιο αποτέλεσμα

$$(\cdots((a_1 * a_2) * a_3) * \cdots * a_k) = a_1 * a_2 * \cdots * a_k.$$

Στο τελευταίο στάδιο του υπολογισμού του αποτελέσματος των πράξεων μεταξύ n στοιχείων, έχουμε να υπολογίσουμε το αποτέλεσμα μεταξύ δύο στοιχείων, καθένα

από τα οποία έχει προέλθει ως αποτέλεσμα πράξεων μεταξύ μικροτέρου το πλήθος στοιχείων. Δηλαδή έχουμε να υπολογίσουμε το αποτέλεσμα

$$(a_1 * a_2 * \cdots * a_k) * (a_{k+1} * a_{k+2} * \cdots * a_n).$$

Αν $k = n-1$, τότε έχουμε

$$(a_1 * a_2 * \cdots * a_k) * (a_{k+1} * a_{k+2} * \cdots * a_n) = (a_1 * a_2 * \cdots * a_{n-1}) * a_n = a_1 * a_2 \cdots * a_n$$

και τέλος.

Αν $k < n-1$, για τον υπολογισμό του αποτελέσματος

$$(a_1 * a_2 * \cdots * a_k) * (a_{k+1} * a_{k+2} * \cdots * a_n),$$

έχουμε

$$\begin{aligned}(a_1 * a_2 * \cdots * a_k) * (a_{k+1} * a_{k+2} * \cdots * a_n) &= \\ &= (a_1 * a_2 * \cdots * a_k) * ((a_{k+1} * a_{k+2} * \cdots * a_{n-1}) * a_n) \\ &\qquad \text{(επειδή η πράξη έχει υποτεθεί προσεταιριστική)} \\ &= ((a_1 * a_2 * \cdots * a_k) * (a_{k+1} * a_{k+2} * \cdots * a_{n-1})) * a_n \\ &\qquad \text{(από την υπόθεση της επαγωγής)} \\ &= (a_1 * a_2 * \cdots * a_k * a_{k+1} * \cdots * a_{n-1}) * a_n \\ &= a_1 * a_2 * \cdots * a_k * a_{k+1} * \cdots * a_{n-1} * a_n.\end{aligned}$$

Άρα, με οποιονδήποτε τρόπο και να εκτελέσουμε τις πράξεις, τελικά έχουμε το ίδιο αποτέλεσμα

$$a_1 * a_2 * \cdots * a_k * a_{k+1} * \cdots * a_{n-1} * a_n$$

και η απόδειξη έχει ολοκληρωθεί. ό.έ.δ.

Έστω $(A, *)$ ένα σύνολο εφοδιασμένο με μια προσεταιριστική πράξη $*$ και ένα στοιχείο $a \in A$. Τότε, κατ' αναλογία με τις δυνάμεις πραγματικών αριθμών, χρησιμοποιούμε *εκθέτες* και συνήθως συμβολίζουμε με $a^2 = a * a$ και γενικά

$$a^n = (a^{n-1}) * a = \underbrace{a * a \cdots * a}_{n}.$$

Οπότε, για δύο φυσικούς αριθμούς m, n και $a \in A$, ισχύει ότι

$$a^m * a^n = a^{m+n} \text{ και } (a^m)^n = a^{mn} \text{ (γιατί;)}.$$

Προσοχή! Δεν πρέπει να παρασυρθούμε, όταν έχουμε δύο διαφορετικά στοιχεία $a, b \in A$ και έναν φυσικό αριθμό n, γενικά **δεν** ισχύει ότι $a^n * b^n = (a * b)^n$.

Ορισμός 5.1.5. Έστω $(A, *)$ ένα σύνολο εφοδιασμένο με μια πράξη. Υποθέτουμε ότι υπάρχει ουδέτερο στοιχείο e ως προς την πράξη $*$. Ένα στοιχείο $a \in A$ θα ονομάζεται **αντιστρέψιμο**, αν υπάρχει $\bar{a} \in A$ με την ιδιότητα:

$$a * \bar{a} = \bar{a} * a = e.$$

Το στοιχείο $\bar{a}$, θα ονομάζεται **αντίστροφο** του στοιχείου a.

Σχόλια 5.1.6. Για να αναζητήσουμε την ύπαρξη αντιστρόφου ενός στοιχείου, πρέπει να έχουμε εξασφαλίσει την ύπαρξη ουδετέρου ως προς την πράξη.

Ορισμένες πράξεις έχει καθιερωθεί να έχουν ονόματα και ειδικό συμβολισμό.

Για παράδειγμα, μια πράξη ενδέχεται να ονομάζεται *πρόσθεση*. Στην περίπτωση αυτή συνήθως την συμβολίζουμε με $+$ και το ουδέτερο στοιχείο, αν υπάρχει, θα ονομάζεται *μηδέν* και θα συμβολίζεται ως 0. Το αντίστροφο ενός στοιχείου a, αν υπάρχει, θα ονομάζεται *αντίθετο* και θα συμβολίζεται ως $-a$.

Μια πράξη ενδέχεται να ονομάζεται *πολλαπλασιασμός*. Στην περίπτωση αυτή συνήθως συμβολίζεται με $\cdot$ ή $*$[4] και το ουδέτερο στοιχείο, αν υπάρχει, θα ονομάζεται *μοναδιαίο* (ή μονάδα) και θα συμβολίζεται ως 1. Το αντίστροφο ενός στοιχείου a, αν υπάρχει, θα συμβολίζεται ως a^{-1}.

Από την σχέση $a * \bar{a} = \bar{a} * a = e$ έπεται άμεσα ότι και το στοιχείο $\bar{a}$ είναι αντιστρέψιμο. Μάλιστα δε, το αντίστροφό του είναι το στοιχείο a. Δηλαδή $\bar{\bar{a}} = a$.

Εδώ πρέπει να επισημάνουμε ότι, όταν έχουμε ένα σύνολο $(A, +)$ εφοδιασμένο με μια πρόσθεση, η οποία είναι προσεταιριστική και ένα στοιχείο $a \in A$, τότε χρησιμοποιούμε *συντελεστές* και συμβολίζουμε $2a = a + a$ και γενικά

$$na = (n-1)a + a = \underbrace{a + a \cdots + a}_{n}.$$

Οπότε, για δύο φυσικούς αριθμούς m, n και $a \in A$, ισχύει ότι

$$ma + na = (m+n)a \text{ και } n(ma) = (nm)a \text{ (γιατί;)}.$$

Προσοχή! Το σύμβολο $+$ μεταξύ των φυσικών αριθμών m και n παριστά την πρόσθεση στους φυσικούς αριθμούς, ενώ το ίδιο σύμβολο $+$ μεταξύ των στοιχείων ma και na του συνόλου A παριστά την πράξη της πρόσθεσης στο σύνολο A, κάτι που δεν (πρέπει να) δημιουργεί σύγχυση.

Πρόταση 5.1.7. *Έστω $(A, *)$ ένα σύνολο εφοδιασμένο με μια πράξη. Υποθέτουμε ότι η πράξη είναι προσεταιριστική και ότι υπάρχει ουδέτερο στοιχείο e ως προς την πράξη $*$.*

i. Αν το στοιχείο $a \in A$ είναι αντιστρέψιμο, τότε υπάρχει μοναδικό αντίστροφο του a.

ii. Έστω $a, b \in A$ δύο αντιστρέψιμα στοιχεία. Τότε το γινόμενο $a * b$ είναι αντιστρέψιμο στοιχείο, μάλιστα δε $(a * b)^{-1} = b^{-1} * a^{-1}$[5].

Απόδειξη.

i. Υποθέτουμε ότι για το στοιχείο a υπάρχουν δύο αντίστροφα στοιχεία, το a^{-1} και το $\bar{a}$. Τότε έχουμε:

$$a^{-1} = a^{-1} * e = a^{-1} * (a * \bar{a}) = (a^{-1} * a) * \bar{a} = e * \bar{a} = \bar{a}.$$

[4] Ορισμένες φορές, όταν δεν υπάρχει ο κίνδυνος της σύγχυσης, το σύμβολο του πολλαπλασιασμού παραλείπεται και απλώς παραθέτουμε τα δύο στοιχεία, τα οποία πολλαπλασιάζονται, δηλαδή αντί του $a \cdot b$ γράφουμε ab.

[5] Στην Μαθηματική αργκό υπάρχει ο εξής άκομψος παραλληλισμός "*Πρώτα βάζουμε τις κάλτσες και μετά τα παπούτσια, ενώ πρώτα βγάζουμε τα παπούτσια και μετά τις κάλτσες*".

ii. Έστω $a, b \in A$ δύο αντιστρέψιμα στοιχεία. Τότε προφανώς,

$$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1} * e * b = b^{-1} * b = e.$$

Ομοίως $(a * b) * (b^{-1} * a^{-1}) = e.$ ό.έ.δ.

Προφανώς μπορούμε να γενικεύσουμε και να αποδείξουμε ότι για τα αντιστρέψιμα στοιχεία $a_1, a_2, \ldots, a_n \in A$, ισχύει

$$(a_1 * a_2 * \cdots * a_n)^{-1} = a_n^{-1} * a_{n-1}^{-1} * \cdots * a_1^{-1}.$$

Στην περίπτωση, όπου έχουμε ένα αντιστρέψιμο στοιχείο $a \in A$, τότε προφανώς ισχύει

$$(a^n)^{-1} = (a^{-1})^n,$$

για κάθε φυσικό αριθμό n. Μάλιστα δε, έχει επικρατήσει να γράφουμε

$$(a^n)^{-1} = (a^{-1})^n = a^{-n}.$$

Επισημαίνουμε, όταν χρησιμοποιούμε προσθετικό συμβολισμό, τότε αντί του $a * b^{-1}$ γράφουμε $a + (-b) = a - b$, οπότε έχουμε ότι $n(-a) = (-n)a$.

Παραδείγματα 5.1.8. Πριν ξεκινήσουμε τα παραδείγματα, επισημαίνουμε, όπως το έχουμε ήδη τονίσει και προηγουμένως, ότι θεωρούμε γνωστές τις πράξεις (και τις ιδιότητές τους) πρόσθεση και πολλαπλασιασμό στα σύνολα των φυσικών, των ακεραίων, των ρητών και των πραγματικών αριθμών.

Τα σύνολα αυτά και οι πράξεις, πρόσθεση και πολλαπλασιασμός, θα ορισθούν αργότερα, όπου εκεί θα αποδειχθούν και οι ιδιότητες αυτών των πράξεων.

1. Στο σύνολο $\mathbb{N}$ των φυσικών αριθμών η πράξη της πρόσθεσης είναι προσεταιριστική και μεταθετική, αλλά δεν υπάρχει ουδέτερο. Οπότε, δεν αναζητούμε αν ένας φυσικός αριθμός έχει αντίθετο ως προς την πρόσθεση.

2. Στο (ίδιο) σύνολο $\mathbb{N}$ των φυσικών αριθμών η πράξη του πολλαπλασιασμού είναι προσεταιριστική και μεταθετική. Για την πράξη του πολλαπλασιασμού υπάρχει ουδέτερο στοιχείο, το 1, και είναι το μόνο αντιστρέψιμο στοιχείο.

3. Στο σύνολο $\mathbb{Z}$ των ακεραίων αριθμών η πράξη της πρόσθεσης είναι προσεταιριστική, μεταθετική και έχει ουδέτερο, το μηδέν. Μάλιστα δε, κάθε ακέραιος αριθμός a έχει αντίθετο ως προς την πρόσθεση, τον $-a$.

   Στο σύνολο των ακεραίων η πράξη του πολλαπλασιασμού είναι προσεταιριστική, μεταθετική και έχει ουδέτερο, το 1. Αλλά τα μόνα αντιστρέψιμα στοιχεία είναι μόνο το 1 και το -1.

4. Στο σύνολο $\mathbb{Q}$ των ρητών αριθμών η πράξη της πρόσθεσης είναι προσεταιριστική, μεταθετική και έχει ουδέτερο, το μηδέν. Μάλιστα δε, κάθε ρητός αριθμός $\frac{\kappa}{\lambda}$ έχει αντίθετο, ως προς την πρόσθεση, τον

   $$-\frac{\kappa}{\lambda} = \frac{-\kappa}{\lambda}.$$

   Στο σύνολο των ρητών η πράξη του πολλαπλασιασμού είναι προσεταιριστική, μεταθετική και έχει ουδέτερο, το 1. Μάλιστα δε, κάθε μη μηδενικός ρητός αριθμός $\frac{\kappa}{\lambda}$ έχει αντίστροφο, τον

   $$(\frac{\kappa}{\lambda})^{-1} = \frac{\lambda}{\kappa}.$$

5. Στο σύνολο $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}$ των μη μηδενικών ρητών αριθμών ορίζουμε μια πράξη (την διαίρεση) ως εξής:

$$a/b \diamond c/d = a/b \cdot d/c.$$

Είναι εύκολο(;) να δούμε ότι η πράξη αυτή δεν έχει ουδέτερο, δεν είναι μεταθετική, δεν είναι προσεταιριστική (γιατί;).

6. Σε ένα σύνολο $A = \{a, b\}$ με δύο στοιχεία μπορούμε να ορίσουμε πολλές πράξεις. Για παράδειγμα, οι πράξεις με πίνακες

$*$	a	b
a	a	a
b	a	b

και

$\cdot$	a	b
a	a	b
b	b	b

Γενικά σε ένα σύνολο με δύο στοιχεία μπορούν να ορισθούν συνολικά 16 (διαφορετικές) πράξεις. Μπορείτε να εξηγήσετε το γιατί; Επίσης, μπορείτε να εξηγήσετε γιατί ο αριθμός των πράξεων, οι οποίες μπορούν να ορισθούν εξαρτάται μόνο από τον αριθμό των στοιχείων του συνόλου και όχι από το είδος των στοιχείων;

7. Στο σύνολο των ακεραίων $\mathbb{Z}$ επιλέγουμε και σταθεροποιούμε έναν ακέραιο αριθμό t. Ορίζουμε μια πράξη $* : \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}$ ως εξής:

$$a * b = a + t + b,$$

όπου $+$ παριστά στην συνήθη πράξη της πρόσθεσης στους ακεραίους.

Η πράξη αυτή είναι προσεταιριστική. Πράγματι, για $a, b, c \in \mathbb{Z}$ έχουμε

$$\begin{aligned}(a * b) * c &= (a + t + b) * c \\ &= (a + t + b) + t + c \\ &= a + t + (b + t + c) \\ &\text{(η πρόσθεση } + \text{ είναι προσεταιριστική στους ακεραίους)} \\ &= a + t + (b * c) \\ &= a * (b * c).\end{aligned}$$

Ως προς την πράξη $*$ υπάρχει ουδέτερο. Ας το ανακαλύψουμε. Αναζητούμε (αν υπάρχει) έναν ακέραιο αριθμό e με την ιδιότητα

$$e * a = a * e = a$$

για όλα τα $a \in \mathbb{Z}$. Δηλαδή πρέπει και αρκεί

$$e + t + a = a + t + e = a$$

για όλα τα $a \in Z$. Οπότε, προφανώς, για $e = -t$, τα ανωτέρω ισχύουν (το $-t$ είναι το αντίθετο του t ως προς την πρόσθεση $+$). Συνεπώς, το ουδέτερο ως προς την πράξη $*$ είναι το $-t$.

Ας αναζητήσουμε αν ένα στοιχείο $a \in \mathbb{Z}$ έχει αντίστροφο ως προς την πράξη $*$. Αναζητούμε (αν υπάρχει) ένα $\bar{a}$ με την ιδιότητα

$$a * \bar{a} = \bar{a} * a = -t.$$

Δηλαδή αναζητούμε ένα $\bar{a}$ έτσι ώστε

$$a + t + \bar{a} = \bar{a} + t + a = -t,$$

Οπότε, εύκολα βλέπουμε ότι, $\bar{a} = -t - t - a$.

8. Μεταξύ δύο ακεραίων a και b ορίζουμε

$$a \oplus b = (a + b)/2.$$

Εδώ δεν πρόκειται για πράξη στο $\mathbb{Z}$, καθότι δεν ορίζεται απεικόνιση

$$\oplus : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \text{ με } \oplus(a, b) = (a + b)/2 \in \mathbb{Z}.$$

9. Στο σύνολο των ακεραίων $\mathbb{Z}$ η πράξη $*$ με

$$a * b = ab + 1$$

δεν είναι προσεταιριστική καθ' ότι

$$(a * b) * c = (ab + 1) * c = (ab + 1)c + 1,$$

ενώ

$$a * (b * c) = a * (bc + 1) = a(bc + 1) + 1.$$

Δηλαδή

$$(a * b) * c \neq a * (b * c).$$

10. Έστω A ένα (μη κενό) σύνολο και $c \in A$. Στο σύνολο A ορίζουμε την πράξη

$$a \diamond b = c,$$

για όλα τα $a, b \in A$. Η πράξη αυτή προφανώς (;) είναι προσεταιριστική, αλλά δεν έχει ουδέτερο στοιχείο (εκτός εάν το σύνολο A είναι μονοσύνολο).

Η πράξη αυτή θα ονομάζεται **σταθερή** πράξη.

Παρατήρηση 5.1.9. Όπως παρατηρούμε και από τα προηγηθέντα (διαφορετικά μεταξύ τους) παραδείγματα, γενικά, ο στόχος είναι να *ανακαλύπτουμε αλήθειες*, οι οποίες διέπουν τις Αλγεβρικές δομές (σύνολα εφοδιασμένα με μία ή περισσότερες πράξεις ή ακόμα γενικότερα εφοδιασμένα με σχέσεις) και είναι ανεξάρτητες από την φύση των στοιχείων των συνόλων. Το μόνο που χρειαζόμαστε είναι να γνωρίζουμε τι ιδιότητες έχουν οι πράξεις και να προσπαθούμε να ανακαλύψουμε συνέπειες αυτών των ιδιοτήτων. Αυτός είναι και ο λόγος, όπου αυτός ο κλάδος των Μαθηματικών ονομάζεται ***Αφηρημένη Άλγεβρα***.

Ορισμός 5.1.10. Ένα σύνολο $(A, *)$ εφοδιασμένο με μια πράξη θα ονομάζεται **ημιομάδα**, αν η πράξη $*$ είναι προσεταιριστική. Μια ημιομάδα $(A, *)$ θα ονομάζεται **μονοειδές**, αν έχει ουδέτερο ως προς την πράξη $*$.

Για παράδειγμα, το σύνολο $(\mathbb{N}, +)$ των φυσικών αριθμών είναι ημιομάδα ως προς την πρόθεση, αλλά δεν είναι μονοειδές. Τουναντίον το σύνολο $(\mathbb{N}, \cdot)$ των φυσικών αριθμών είναι μονοειδές.

Έστω A ένα (μη κενό) σύνολο και $P(A)$ το σύνολο όλων των απεικονίσεων με πεδίο ορισμού και πεδίο τιμών το σύνολο A. Δηλαδή

$$P(A) = \{ f : A \longrightarrow A \}.$$

Το σύνολο $P(A)$ εφοδιάζεται με μια πράξη $\circ$, την σύνθεση απεικονίσεων. Προφανώς, (ιδέ την Παράγραφο 4.5.6 στο Κεφάλαιο 4) το σύνολο $(P(A), \circ)$ είναι ένα μονοειδές, καθότι η σύνθεση απεικονίσεων είναι προσεταιριστική και υπάρχει ουδέτερο ως προς την σύνθεση απεικονίσεων, η ταυτοτική απεικόνιση 1_A.

Γενίκευση της έννοιας του ουδετέρου στοιχείου και της έννοιας του αντιστρόφου στοιχείου

Ορισμός 5.1.11. Έστω $(A, *)$ ένα σύνολο εφοδιασμένο με την πράξη $*$. Ένα στοιχείο $e \in A$, θα ονομάζεται **αριστερό** ουδέτερο (ή ουδέτερο από τα αριστερά), αν

$$e * a = a,$$

για όλα τα $a \in A$. Όμοια, ένα στοιχείο $\epsilon \in A$, θα ονομάζεται **δεξιό** ουδέτερο (ή ουδέτερο από τα δεξιά), αν

$$a * \epsilon = a,$$

για όλα τα $a \in A$.

Ένα σύνολο ενδέχεται να έχει αριστερά (αντίστοιχα δεξιά) ουδέτερα, αλλά να μην έχει δεξιά (αντίστοιχα αριστερά) ουδέτερα. Για παράδειγμα, η προβολή $\pi_1 : A \times A \longrightarrow A$ με $\pi_1(a, b) = a$ είναι μια πράξη, η οποία έχει πολλά δεξιά ουδέτερα (όλα τα στοιχεία του συνόλου A), ενώ δεν έχει κανένα αριστερό ουδέτερο.

Προφανώς (γιατί;), αν σε ένα σύνολο $(A, *)$ υπάρχουν αριστερά και δεξιά ουδέτερα ως προς την πράξη $*$, τότε υπάρχει ένα (και μοναδικό) ουδέτερο στοιχείο ως προς την πράξη $*$.

Ορισμός 5.1.12. Έστω $(A, *)$ ένα σύνολο εφοδιασμένο με την πράξη $*$. Υποθέτουμε ότι υπάρχει ουδέτερο στοιχείο, έστω e. Ένα στοιχείο $a \in A$ έχει **αριστερό αντίστροφο**, αν υπάρχει ένα $\bar{a} \in A$ με την ιδιότητα

$$\bar{a} * a = e.$$

Όμοια, Ένα στοιχείο $a \in A$ έχει **δεξιό αντίστροφο**, αν υπάρχει ένα $\underline{a} \in A$ με την ιδιότητα

$$a * \underline{a} = e.$$

Προφανώς αν ένα στοιχείο είναι αντιστρέψιμο, τότε το αντίστροφό του είναι ταυτόχρονα αριστερό και δεξιό αντίστροφο. Επίσης, από την σχέση $\bar{a} * a = e$ έπεται ότι "συνυπάρχουν" αριστερά και δεξιά αντίστροφα (το $\bar{a}$ είναι αριστερό αντίστροφο του a και το a είναι δεξιό αντίστροφο του $\bar{a}$.

Παραδείγματα 5.1.13.

1. Στην παράγραφο 4.5.6.1 και ειδικότερα στο Θεώρημα 4.5.35 του Κεφαλαίου 4 είχαμε δει ότι για μια απεικόνιση υπάρχουν (υπό προϋποθέσεις) αριστερές αντίστροφες ή δεξιές αντίστροφες απεικονίσεις.

   Συγκεκριμένα, αν στο σύνολο $(P(A), \circ)$ των απεικονίσεων με πεδίο ορισμού και πεδίο τιμών το σύνολο A έχουμε ένα στοιχείο $f : A \longrightarrow A$, η οποία είναι 1-1, τότε πάντα υπάρχει μια απεικόνιση $h : A \longrightarrow A$, η οποία είναι επί, με

   $$h \circ f = 1_A.$$

   Επομένως, η h είναι αριστερή αντίστροφη της f και η f είναι δεξιά αντίστροφη της h.

2. Βάσει του προηγουμένου γενικού παραδείγματος, θα δούμε ένα συγκεκριμένο παράδειγμα: Έστω η απεικόνιση $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ με

$$\varphi(x) = 2x.$$

Η φ είναι 1-1, άρα υπάρχει μια αριστερή αντίστροφη $\vartheta : \mathbb{N} \longrightarrow \mathbb{N}$. Για παράδειγμα, η $\vartheta : \mathbb{N} \longrightarrow \mathbb{N}$ με

$$\vartheta(2x) = x \text{ και } \vartheta(2x-1) = x.$$

Τότε πράγματι έχουμε ότι

$$(\vartheta \circ \varphi)(x) = x,$$

για όλα τα $x \in \mathbb{N}$, άρα

$$\vartheta \circ \varphi = 1_{\mathbb{N}}.$$

Συνεπώς, η απεικόνιση ϑ είναι ένα αριστερό αντίστροφο του στοιχείου

$$\varphi \in (P(A), \circ).$$

3. Στο παράδειγμα $5.1.8_5$ είχαμε ορίσει την πράξη της διαίρεσης μεταξύ μη μηδενικών ρητών αριθμών ως εξής:

$$a/b \diamond c/d = a/b \cdot d/c.$$

Προφανώς το στοιχείο $1 \in (\mathbb{Q}^*, \diamond)$ είναι δεξιό ουδέτερο, αλλά δεν είναι αριστερό ουδέτερο. Επίσης, κάθε $a/b \in (\mathbb{Q}^*, \diamond)$ έχει δεξιό αντίστροφο (ως προς το δεξιό ουδέτερο 1), το b/a [6].

Σχόλιο 5.1.14. Στο Παράδειγμα 2 η απεικόνιση ϑ δεν είναι η μοναδική αριστερή αντίστροφη της απεικόνισης φ. Μπορείτε να υπολογίσετε μια άλλη αριστερή αντίστροφη απεικόνιση της φ; Επίσης, η απεικόνιση φ δεν έχει δεξιά αντίστροφη απεικόνιση (γιατί;) (Ιδέ και τις Ασκήσεις $4.5.7_{8,9}$).

Συμπερασματικά, σε ένα σύνολο $(A, *)$, όπου για την πράξη $*$ υπάρχει ουδέτερο στοιχείο, ενδέχεται ένα στοιχείο $a \in A$ να έχει πολλά αριστερά αντίστροφα και κανένα δεξιό αντίστροφο. Όπως επίσης ένα στοιχείο $b \in A$ ενδέχεται να έχει πολλά δεξιά αντίστροφα και κανένα αριστερό αντίστροφο.

Το ερώτημα που προκύπτει είναι το εξής: Υπάρχει περίπτωση ένα στοιχείο να έχει αριστερό αντίστροφο και δεξιό αντίστροφο, τα οποία να είναι διαφορετικά μεταξύ τους; Συγκεκριμένα ισχύει η εξής Πρόταση:

Πρόταση 5.1.15. *Έστω $(A, *)$ ένα σύνολο εφοδιασμένο με μια προσεταιριστική πράξη, ως προς την οποία υπάρχει ουδέτερο στοιχείο, έστω e. Αν για ένα στοιχείο $a \in A$ υπάρχουν αριστερά και δεξιά αντίστροφα, τότε υπάρχει μόνο ένα, το οποίο είναι αντίστροφο στοιχείο.*

Απόδειξη. Υποθέτουμε ότι για το στοιχείο $a \in A$ το στοιχείο $\bar{a}$ είναι αριστερό αντίστροφο και το στοιχείο $\underline{a}$ δεξιό αντίστροφο. Τότε έχουμε:

$$\bar{a} = \bar{a} * e = \bar{a} * (a * \underline{a}) = (\bar{a} * a) * \underline{a} = e * \underline{a} = \underline{a}. \qquad \text{ό.έ.δ.}$$

[6] Εδώ βλέπουμε τις διαφορετικές ιδιότητες που αποκτά το ίδιο στοιχείο 1 στο σύνολο των μη μηδενικών ρητών, ανάλογα με την αλγεβρική δομή, με την οποία θεωρούμε ότι είναι εφοδιασμένο το σύνολο $\mathbb{Q}^*$.

5.1.1 Ασκήσεις

1. Ποιες από τις ακόλουθες σχέσεις είναι πράξεις στα αντίστοιχα σύνολα;

   (α) Η αφαίρεση $a - b$ στο σύνολο $\mathbb{Z}$ των ακεραίων αριθμών.

   (β) Η αφαίρεση στο σύνολο $\{ x \in \mathbb{Z} \mid x > 0 \}$ των θετικών ακεραίων αριθμών.

   (γ) $a * b = a^b$, όπου $a, b \in \{ x \in \mathbb{Z} \mid x > 0 \}$.

   (δ) $a * b$ να είναι ρίζα της εξίσωσης $x^2 - a^2 b^2 = 0$ με $a, b \in \mathbb{R}$.

   (ε) Στο σύνολο των σημείων ενός επιπέδου (E) το $A * B$ είναι το μέσον του ευθυγράμμου τμήματος AB (Στην περίπτωση, όπου $A = B$, τότε $A * A = A$).

   (στ) Έστω A ένα μη κενό σύνολο. $a * b = a$, για $a, b \in A$ (η προβολή ως προς την πρώτη συντεταγμένη).

2. Για τις ακόλουθες πράξεις να ελέγξετε, αν είναι προσεταιριστικές, μεταθετικές, έχουν ουδέτερο, αν ένα στοιχείο έχει αντίστροφο.

   (α) $(\mathbb{Z}, *)$ με $a * b = a + b + 2y + 4$.

   (β) $(\mathbb{R}, *)$ με $a * b = \mid a - b \mid$.

   (γ) $(\mathbb{R}, *)$ με $a * b = \mid a + b \mid$.

   (δ) $(\mathbb{R}, *)$ με $a * b = \max(a, b)$.

   (ε) $(\mathbb{R}^+, *)$ με $a * b = \max(a, b)$, όπου $\mathbb{R}^+ = \{ x \in \mathbb{R} \mid x \geq 0 \}$.

   (στ) Έστω A ένα (μη κενό) σύνολο. Στο δυναμοσύνολο $\mathcal{P}(A)$ ορίζονται οι πράξεις της τομής $\cap$, της ένωσης $\cup$ και της συμμετρικής διαφοράς $\oplus$. Να ελέγξετε τις πράξεις αυτές ως προς τα ανωτέρω ερωτήματα.

   (ζ) Έστω $A = \{ a, b \}$ ένα σύνολο με δύο στοιχεία. Στο Παράδειγμα 5.1.8$_5$ είδαμε ότι ορίζονται 16 το πλήθος πράξεις στο σύνολο A.

   Να τις καταγράψετε όλες και σε κάθε μια από αυτές να απαντήσετε στα ανωτέρω ερωτήματα.

3. Έστω $B = \{ a, b, c \}$ ένα σύνολο με τρία στοιχεία. Πόσες πράξεις μπορούν να οριστούν στο σύνολο B;

   Από τις πράξεις αυτές να βρεθεί μια (μη σταθερή), η οποία να είναι προσεταιριστική και να έχει ουδέτερο.

4. Έστω $(A, *)$ ένα σύνολο εφοδιασμένο με μια πράξη. Υποθέτουμε ότι η πράξη έχει ουδέτερο και ότι $a * (b * c) = (a * c) * b$, για όλα τα $a, b, c \in A$. Δείξτε ότι η πράξη $*$ είναι μεταθετική και προσεταιριστική.

5. Έστω $(A, *)$ ένα σύνολο εφοδιασμένο με μια πράξη. Στο σύνολο

$$\mathcal{R} = \mathcal{P}(A) \setminus \{\varnothing\}$$

   όλων των μη κενών υποσυνόλων του A ορίζουμε μια πράξη $*$ (με το ίδιο σύμβολο), ως εξής: Για $S, T \subseteq A$ ορίζουμε

$$S * T = \{ s * t \mid s \in S, t \in T \}.$$

   Δείξτε ότι η νέα πράξη είναι προσεταιριστική αν και μόνο αν η αρχική πράξη είναι προσεταιριστική.

   Εξετάστε αν η νέα πράξη έχει ουδέτερο.

5.1.2 Ομάδες

Οι ομάδες είναι, ίσως, η πλέον σημαντική Αλγεβρική δομή, δεδομένου ότι επ' αυτής βασίζονται άλλες Αλγεβρικές δομές, όπως οι Δακτύλιοι και οι Διανυσματικοί χώροι. Επίσης, μέσω των ομάδων μελετώνται ιδιότητες, οι οποίες χαρακτηρίζουν "Γεωμετρικά αντικείμενα". Η επίδραση όμως της έννοιας της ομάδας δεν αφορά μόνο τα Μαθηματικά αυτά καθ' εαυτά[7].

Διαδοχικά είδαμε ότι, ένα σύνολο εφοδιασμένο με μια πράξη αποτελεί ένα ομαδοειδές. Ένα ομαδοειδές, όπου η πράξη είναι προσεταιριστική, αποτελεί μια ημιομάδα. Μια ημιομάδα, όπου ως προς την πράξη υπάρχει ουδέτερο, αποτελεί ένα μονοειδές. Τώρα ένα μονοειδές, όπου ως προς την πράξη κάθε στοιχείο έχει αντίστροφο, θα ονομάζεται ομάδα. Δηλαδή, έχουμε τον εξής ορισμό:

Ορισμός 5.1.16. Έστω $(G, \circ)$ ένα σύνολο εφοδιασμένο με μια πράξη. Το $(G, \circ)$ θα ονομάζεται **ομάδα**, αν ισχύουν οι εξής ιδιότητες:

i. Η πράξη $\circ$ είναι προσεταιριστική. Δηλαδή, για $a, b, c \in G$ ισχύει ότι

$$a \circ (b \circ c) = (a \circ b) \circ c.$$

ii. Υπάρχει ουδέτερο e. Δηλαδή,

$$a \circ e = e \circ a = a,$$

για όλα τα $a \in G$.

iii. Κάθε στοιχείο έχει αντίστροφο. Δηλαδή, για κάθε $a \in G$ υπάρχει $a^{-1} \in G$ με την ιδιότητα:

$$a \circ a^{-1} = a^{-1} \circ a = e.$$

Αν επιπλέον η πράξη $\circ$ είναι μεταθετική, δηλαδή

$$a \circ b = b \circ a$$

για όλα τα $a, b \in G$, τότε η ομάδα $(G, \circ)$, θα ονομάζεται μεταθετική ή **αβελιανή** ομάδα.

Προφανώς σε μια ομάδα το ουδέτερο στοιχείο είναι μοναδικό. Επίσης, κάθε στοιχείο μιας ομάδας έχει μοναδικό αντίστροφο (ιδέ Πρόταση 5.1.7).

Το πλήθος των στοιχείων μιας ομάδας G [8] θα ονομάζεται **τάξη** της ομάδας και θα συμβολίζεται με $| G |$, μια ομάδα με πεπερασμένο το πλήθος στοιχεία θα ονομάζεται πεπερασμένη, διαφορετικά θα ονομάζεται άπειρη.

Παραδείγματα 5.1.17. Στα επόμενα παραδείγματα, όπως πάντα, πρέπει να συμπληρώνονται όλα τα κενά, τα οποία ηθελημένα ή μη, υπάρχουν στους προβαλλόμενους ισχυρισμούς.

---

[7] The notion of a "group," viewed only 30 years ago as the epitome of sophistication, is today one of the mathematical concepts most widely used in physics, chemistry, biochemistry, and mathematics itself. *Alexey Sosinsky, 1991.*

[8] Όταν αναφερόμαστε γενικά σε μια ομάδα ή όταν δεν υπάρχει σύγχυση για την πράξη της ομάδας, συνήθως παραλείπουμε το σύμβολο της πράξης και αντί του $(G, *)$ απλώς γράφουμε G.

1. Τα σύνολα $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ των ακεραίων, των ρητών και των πραγματικών αριθμών εφοδιασμένα με την (γνωστή;) πράξη της πρόσθεσης αποτελούν ομάδες. Μάλιστα δε, είναι αβελιανές ομάδες. Οι ομάδες αυτές ονομάζονται οι *προσθετικές ομάδες των ακεραίων, των ρητών και των πραγματικών αριθμών* αντίστοιχα.

2. Έστω $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ και $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. Τα σύνολα $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ εφοδιασμένα με την (γνωστή;) πράξη του πολλαπλασιασμού αποτελούν ομάδες. Μάλιστα δε, είναι αβελιανές ομάδες. Οι ομάδες αυτές ονομάζονται οι *πολλαπλασιαστικές ομάδες των ρητών και των πραγματικών αριθμών* αντίστοιχα.

3. Στο σύνολο των ακεραίων Z επιλέγουμε και σταθεροποιούμε έναν ακέραιο αριθμό t. Ορίζουμε την εξής πράξη $* : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ ως εξής:

$$a * b = a + t + b,$$

όπου $+$ παριστά την συνήθη πράξη της πρόσθεσης στους ακεραίους. Στο Παράδειγμα 5.1.8$_7$ είχαμε αποδείξει ότι το σύνολο $(\mathbb{Z}, *)$ είναι ομάδα. Δηλαδή, σε ένα σύνολο μπορεί να οριστούν περισσότερες της μίας αλγεβρικές δομές ομάδας.

4. Έστω A ένα μη κενό σύνολο. Στην σελίδα 188 είχαμε ορίσει το σύνολο

$$P(A) = \{ f : A \longrightarrow A \}$$

όλων των απεικονίσεων με πεδίο ορισμού και πεδίο τιμών το σύνολο A και είχαμε δει ότι το σύνολο $(P(A), \circ)$, εφοδιασμένο με την πράξη $\circ$ της σύνθεσης απεικονίσεων, αποτελεί ημιομάδα με μονάδα. Εδώ θεωρούμε το (υπο)σύνολο

$$S_A = \{ f : A \longrightarrow A \mid \text{η } \varphi \text{ είναι 1-1 και επί } \}.$$

Ως γνωστόν(;) η σύνθεση δύο 1-1 και επί απεικονίσεων είναι και αυτή 1-1 και επί. Επίσης, μια απεικόνιση 1-1 και επί έχει αντίστροφη, η οποία είναι και αυτή 1-1 και επί.

Συνεπώς, το σύνολο $(S_A, \circ)$ αποτελεί ομάδα, η οποία ονομάζεται η **συμμετρική** ομάδα του συνόλου A. Κάθε απεικόνιση $f : A \longrightarrow A$, η οποία είναι 1-1 και επί "μεταθέτει" τα στοιχεία του συνόλου A, για τον λόγο αυτόν ονομάζεται **μετάθεση** των στοιχείων του συνόλου A και η ομάδα $(S_A, \circ)$ αναφέρεται και ως η ομάδα μεταθέσεων του συνόλου A.

5. Εξειδικεύουμε το προηγούμενο παράδειγμα. Έστω $A = \{1, 2, 3\}$, τότε έχουμε τις εξής μεταθέσεις του συνόλου A: Την ταυτοτική:

$$1_A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad \rho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$
$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \phi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Όπου, στην παρουσίαση αυτή των μεταθέσεων, υπό μορφή πίνακα, στην πρώτη γραμμή εμφανίζονται τα στοιχεία του πεδίου ορισμού και ακριβώς από κάτω, στην δεύτερη γραμμή, εμφανίζονται οι εικόνες τους μέσω της αντίστοιχης μετάθεσης.

Γιατί οι μόνες μεταθέσεις είναι αυτές που αναγράφονται; Παρατηρούμε ότι

$$\pi^{-1} = \pi,\ \rho^{-1} = \rho, \sigma^{-1} = \sigma,\ \tau^{-1} = \phi.$$

Επίσης, $\pi \circ \rho = \tau$, ενώ $\rho \circ \pi = \phi$, άρα

$$\pi \circ \rho \neq \rho \circ \pi.$$

Δηλαδή η ομάδα $(S_A, \circ)$ δεν είναι αβελιανή.

Στα επόμενα θα επανέλθουμε στις ομάδες μεταθέσεων.

6. Θεωρούμε μια "σκακιέρα" με τέσσερα μόνο τετραγωνίδια, όπως φαίνεται στο σχήμα

1	2
3	4

Σε ένα από τα τέσσερα τετραγωνίδια υπάρχει ένα πιόνι. Το πιόνι αυτό μπορεί να μετακινηθεί ως εξής: Παραμένει ακίνητο (η παραμονή στην ίδια θέση θεωρείται ως τετριμμένη μετακίνηση), Οριζοντίως, Καθέτως, Διαγωνίως.

Το πιόνι, όταν μετακινηθεί από μια θέση σε μια άλλη, μπορεί να μετακινηθεί, πάλι με τον ίδιο τρόπο, σε μία άλλη θέση. Επομένως, μπορούμε να θεωρήσουμε ότι η συνολική διαδρομή του πιονιού στα τετραγωνίδια αποτελεί έναν συνδυασμό διαδοχικών μετακινήσεων, όπως αυτές περιγράφονται ανωτέρω.

Ας δούμε πώς αυτές οι κινήσεις μπορούν να περιγραφούν από απεικονίσεις 1-1 και επί από το σύνολο $\{1, 2, 3, 4\}$ στον εαυτό του, δηλαδή από μεταθέσεις.

Η παραμονή στην ίδια θέση παριστάνεται από την ταυτοτική μετάθεση

$$I = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix},$$

η οριζόντια μετακίνηση παριστάνεται από την μετάθεση

$$H = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

η κάθετη μετακίνηση παριστάνεται από την μετάθεση

$$V = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

και η διαγώνια μετακίνηση παριστάνεται από την μετάθεση

$$D = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Όπου η πρώτη γραμμή παριστά την αρχική θέση του πιονιού και η δεύτερη την θέση στην οποία μετακινείται.

Προφανώς (;) η συνολική διαδρομή του πιονιού μπορεί να περιγραφεί από την σύνθεση των ανωτέρω μεταθέσεων. Ας δούμε, ως παράδειγμα, πώς μπορούμε να δούμε την τελική θέση του πιονιού μετά τον συνδυασμό των κινήσεων $H \circ V \circ D \circ H$.

$$\begin{aligned}
1 &\xrightarrow{H} 2 \xrightarrow{D} 3 \xrightarrow{V} 1 \xrightarrow{H} 2,\\
2 &\xrightarrow{H} 1 \xrightarrow{D} 4 \xrightarrow{V} 2 \xrightarrow{H} 1,\\
3 &\xrightarrow{H} 4 \xrightarrow{D} 1 \xrightarrow{V} 3 \xrightarrow{H} 4,\\
4 &\xrightarrow{H} 3 \xrightarrow{D} 2 \xrightarrow{V} 4 \xrightarrow{H} 3.
\end{aligned}$$

Δηλαδή, αν το πιόνι ξεκινούσε από την θέση 1, θα κατέληγε στην θέση 2 και ούτω καθ' εξής. Μα αυτό θα μπορούσε να πραγματοποιηθεί μετακινούμενο μόνο μια φορά οριζόντια. Άρα ισχύει

$$H \circ V \circ D \circ H = H.$$

Μπορούμε να δούμε (ιδέ Άσκηση 5.1.3$_9$) ότι το σύνολο $(G, \circ)$ όλων των δυνατών κινήσεων του πιονιού, εφοδιασμένο με την πράξη της σύνθεσης απεικονίσεων, αποτελεί ομάδα.

7. Στην σελίδα 182 είχαμε δει ότι, αν έχουμε ένα πεπερασμένο σύνολο εφοδιασμένο με μια πράξη, τότε μπορούμε να παραστήσουμε την πράξη αυτή με τον πολλαπλασιαστικό της πίνακα. Επομένως, αν έχουμε μια ομάδα με πεπερασμένο το πλήθος στοιχεία, μπορούμε να την παραστήσουμε με τον πολλαπλασιαστικό της πίνακα. Μάλιστα δε, επειδή εδώ έχουμε ομάδα, η οποία περιέχει ουδέτερο στοιχείο και κάθε στοιχείο της έχει αντίστροφο, ο πολλαπλασιαστικός της πίνακας μπορεί να κατασκευαστεί σχετικά εύκολα.

   Για παράδειγμα, παραθέτουμε τον πολλαπλασιαστικό πίνακα της ομάδας μεταθέσεων του συνόλου $A = \{1, 2, 3\}$ (ιδέ το προπροηγούμενο παράδειγμα).

$\circ$	1_A	π	ρ	σ	τ	ϕ
1_A	1_A	π	ρ	σ	τ	ϕ
π	π	$\pi \circ \pi = 1_A$	$\pi \circ \rho = \tau$	$\pi \circ \sigma = \phi$	$\pi \circ \tau = \rho$	$\pi \circ \phi = \sigma$
ρ	ρ	$\rho \circ \pi = \phi$	$\rho \circ \rho = 1_A$	$\rho \circ \sigma = \tau$	$\rho \circ \tau = \sigma$	$\rho \circ \phi = \pi$
σ	σ	$\sigma \circ \pi = \tau$	$\sigma \circ \rho = \phi$	$\sigma \circ \sigma = 1_A$	$\sigma \circ \tau = \pi$	$\sigma \circ \phi = \rho$
τ	τ	$\tau \circ \pi = \sigma$	$\tau \circ \rho = \pi$	$\tau \circ \sigma = \rho$	$\tau \circ \tau = \phi$	$\tau \circ \phi = 1_A$
ϕ	ϕ	$\phi \circ \pi = \rho$	$\phi \circ \rho = \sigma$	$\phi \circ \sigma = \pi$	$\phi \circ \tau = 1_A$	$\phi \circ \phi = \tau$

8. **Ομάδες συμμετριών**

   Η ανάγκη της μελέτης των συμμετριών ενός Γεωμετρικού Σχήματος οδήγησε στην διαμόρφωση της έννοιας της ομάδας.

   Έκτοτε "...Κύλισε πολύ νερό στο αυλάκι" της Μαθηματικής διανόησης για να καταλήξουμε στην σημερινή μορφή της Θεωρίας Ομάδων. Παρ' όλη την εξέλιξη της Θεωρίας, η μελέτη των συμμετριών αποτελεί, ακόμη και σήμερα, έναν ενεργό κλάδο της Θεωρίας Ομάδων. Εδώ εμείς θα προσπαθήσουμε να δώσουμε μια μόνο γεύση περιοριζόμενοι μόνο σε παραδείγματα.

   Χάριν οργανώσεως, στο Παράρτημα, όπου γίνεται μια εκ νέου "επίσκεψη" στις ομάδες, παραθέτουμε μια σχετική παράγραφο (ιδέ Παράγραφο Γ.1.2).

9. Για κάθε $(a, b) \in \mathbb{R}^2$ ορίζουμε την απεικόνιση $T_{(a,b)} : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ με

$$T_{(a,b)}(x, y) = (x + a, y + b).$$

Το σύνολο

$$Tr = \{ T_{(a,b)} \mid (a, b) \in \mathbb{R}^2 \}$$

με πράξη την σύνθεση απεικονίσεων αποτελεί ομάδα. Εδώ πρώτα πρέπει να ελέγξουμε, αν η σύνθεση δύο στοιχείων του συνόλου G μας δίνει απεικόνιση, η οποία ανήκει στο σύνολο G. Πράγματι, είναι εύκολο(;) να διαπιστώσουμε ότι

$$T_{(a,b)} \circ T_{(c,d)} = T_{(a+c,b+d)}.$$

Οπότε, μπορούμε να διαπιστώσουμε ότι πράγματι το σύνολο $(G, \circ)$ είναι ομάδα και μάλιστα αβελιανή.

Η ομάδα αυτή ονομάζεται η ομάδα **μεταφορών** στο επίπεδο.

10. Έστω A ένα μη κενό σύνολο και B, C δύο υποσύνολά του, τότε ως γνωστόν ορίζεται η συμμετρική διαφορά

$$B \oplus C = (B \cup C) \setminus (B \cap C),$$

(Για τον ορισμό και ιδιότητες της συμμετρικής διαφοράς συνόλων ιδέ τον Ορισμό 1.1.35 και τις Ασκήσεις $1.1.3_{5,6,7}$). Το δυναμοσύνολο $\mathcal{P}(A)$ εφοδιασμένο με την πράξη $\oplus$ αποτελεί ομάδα και μάλιστα αβελιανή (γιατί; ποιο είναι το ουδέτερο στοιχείο, ποιο το αντίστροφο ενός $B \in \mathcal{P}(A)$;)

11. Έστω $\mathcal{F}(\mathbb{R})$ το σύνολο όλων των απεικονίσεων με πεδίο ορισμού και πεδίο τιμών το σύνολο των πραγματικών αριθμών. Ως γνωστόν(;), στο σύνολο $\mathcal{F}(\mathbb{R})$ ορίζεται η πρόσθεση απεικονίσεων ως εξής: Για $f, g \in \mathcal{F}(\mathbb{R})$ ορίζουμε

$$f + g : \mathbb{R} \longrightarrow R \text{ με } (f + g)(x) = f(x) + g(x),$$

για όλα τα $x \in \mathbb{R}$. Είναι εύκολο (ιδέ Άσκηση $5.1.3_2$) να δούμε ότι το σύνολο $(\mathcal{F}(\mathbb{R}), +)$ αποτελεί ομάδα. Με ουδέτερο στοιχείο την μηδενική απεικόνιση

$$0 : \mathbb{R} \longrightarrow R \text{ με } 0(x) = 0,$$

για όλα τα $x \in \mathbb{R}$.

Όπως έχουμε επισημάνει, ήδη από τον ορισμό της απεικόνισης (Κεφάλαιο 4), το πλήθος και οι ιδιότητες των απεικονίσεων, μεταξύ δύο συνόλων, δεν εξαρτώνται από την φύση των στοιχείων των συνόλων. Στα Παραδείγματα 4 και 5 ανωτέρω είχαμε δει την ομάδα μεταθέσεων $(S_A, \circ)$ ενός συνόλου A. Επομένως, το πλήθος των μεταθέσεων ενός συνόλου δεν εξαρτάται από την φύση των στοιχείων του συνόλου, αλλά από το πλήθος των στοιχείων του. Συγκεκριμένα ισχύει η πρόταση:

Πρόταση 5.1.18. *Έστω A ένα πεπερασμένο σύνολο με n το πλήθος στοιχεία. Το πλήθος των στοιχείων της ομάδας μεταθέσεων του συνόλου A ισούται με $n! = 1 \cdot 2 \cdot \cdots \cdot (n-1) \cdot n$, δηλαδή*

$$| S_A | = n!.$$

Απόδειξη. Έστω $A = \{a_1, a_2, \dots, a_n\}$. Για να κατασκευάσουμε μια μετάθεση

$$\pi : A \longrightarrow A,$$

αν λάβουμε το στοιχείο $a_1 \in A$, έχουμε n το πλήθος επιλογές για την εικόνα του $\pi(a_1)$. Εφόσον έχουμε επιλέξει την εικόνα $\pi(a_1)$, για την εικόνα του a_2 έχουμε $n-1$ το πλήθος επιλογές (γιατί; Δεν ξεχνάμε ότι η απεικόνιση π είναι 1-1). Εφόσον έχουμε επιλέξει την εικόνα $\pi(a_2)$, για την εικόνα του a_3 έχουμε $n-2$ το πλήθος επιλογές. Οπότε συνεχίζοντας, εφόσον έχουμε επιλέξει και την εικόνα $\pi(a_{n-1})$, για την εικόνα του a_n έχουμε μόνο μια επιλογή. Άρα βλέπουμε ότι το πλήθος των στοιχείων της ομάδας είναι ίσον με $n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1$. ό.έ.δ.

Μετά την πρόταση αυτήν, αντί του συμβόλου S_A μπορούμε να χρησιμοποιούμε το σύμβολο $S_{|A|}$ ή γενικότερα S_n, στην περίπτωση όπου $|A| = n$ και να λέμε η ομάδα μεταθέσεων n το πλήθος συμβόλων.

Ιδιότητες των Ομάδων.

Η (αλγεβρική) δομή μιας ομάδας είναι πλούσια. Θα αναφέρουμε μερικές χαρακτηριστικές ιδιότητες των ομάδων, όπου πέραν των ιδιοτήτων αυτών καθ' εαυτών, γίνεται αντιληπτό ότι οι ιδιότητες των ομάδων δεν εξαρτώνται από την φύση των στοιχείων του (υποκειμένου) συνόλου, αλλά από την πράξη, η οποία ικανοποιεί τις απαιτήσεις του Ορισμού 5.1.16 (ιδέ και την Παρατήρηση 5.1.9).

Στον ορισμό της ομάδος δεν είναι αναγκαίο να απαιτούμε την ύπαρξη ουδετέρου και την ύπαρξη αντιστρόφου στοιχείου για κάθε στοιχείο της ομάδας. Είναι αρκετό να εξασφαλίσουμε την ύπαρξη δεξιού ουδετέρου και την ύπαρξη δεξιού αντιστρόφου. Συγκεκριμένα έχουμε:

Πρόταση 5.1.19. *Ένα σύνολο $(G, \circ)$ εφοδιασμένο με μια προσεταιριστική πράξη είναι ομάδα αν και μόνο αν*

α. Υπάρχει δεξιό ουδέτερο e. Δηλαδή, $a \circ e = a$, για όλα τα $a \in G$.

β. Κάθε στοιχείο έχει δεξιό αντίστροφο. Δηλαδή, για κάθε $a \in G$ υπάρχει $a^{-1} \in G$ με την ιδιότητα: $a \circ a^{-1} = e$.

Απόδειξη. Αν το σύνολο $(G, \circ)$ είναι ομάδα, τότε προφανώς ισχύουν τα α) και β).

Αντίστροφα, υποθέτουμε ότι ισχύουν τα α) και β). Θα δείξουμε ότι το a^{-1} είναι και αριστερό αντίστροφο του στοιχείου a. Όπως επίσης ότι το e είναι και αριστερό ουδέτερο.

Έχουμε,

$$a^{-1} \circ a = (a^{-1} \circ a) \circ e = (a^{-1} \circ a) \circ (a^{-1} \circ (a^{-1})^{-1})$$

(γιατί;) Μα το στοιχείο a^{-1}, εξ υποθέσεως, έχει δεξιό αντίστροφο, το $(a^{-1})^{-1}$. Επομένως, συνεχίζουμε την προηγουμένη ισότητα και έχουμε

$$\begin{aligned} a^{-1} \circ a &= (a^{-1} \circ a) \circ e \\ &= (a^{-1} \circ a) \circ (a^{-1} \circ (a^{-1})^{-1}) \\ &= (a^{-1} \circ (a \circ a^{-1}) \circ (a^{-1})^{-1} \\ &= a^{-1} \circ e \circ (a^{-1})^{-1} \\ &= a^{-1} \circ (a^{-1})^{-1} = e. \end{aligned}$$

Δηλαδή το a^{-1} είναι και αριστερό αντίστροφο του a.

Τώρα,

$$e \circ a = (a \circ a^{-1}) \circ a = a \circ (a^{-1} \circ a) = a \circ e = a.$$

Δηλαδή το e είναι και αριστερό ουδέτερο. ό.έ.δ.

Προφανώς η ανωτέρω πρόταση ισχύει, αν αντί για την ύπαρξη δεξιού ουδετέρου και δεξιού αντιστρόφου, υποθέσουμε την ύπαρξη αριστερού ουδετέρου και αριστερού αντιστρόφου.

Εδώ πρέπει να επισημάνουμε ότι δεν ισχύει το αποτέλεσμα, αν υποθέσουμε την ύπαρξη δεξιού (αντίστοιχα αριστερού) ουδετέρου και την ύπαρξη αριστερού (αντίστοιχα δεξιού) αντιστρόφου για κάθε στοιχείο του συνόλου $(A, \circ)$. (γιατί;)

Πρόταση 5.1.20. *Μια ημιομάδα $(G, \circ)$ είναι ομάδα αν και μόνο οι εξισώσεις*

$$a \circ x = b \text{ και } y \circ a = b$$

έχουν λύση στην G, για όλα τα $a, b \in G$.

Απόδειξη. Προφανώς, αν η ημιομάδα $(G, \circ)$ είναι ομάδα, κάθε στοιχείο έχει αντίστροφο. Επομένως, υπάρχει το στοιχείο $x = a^{-1} \circ b \in G$ με την ιδιότητα

$$a \circ (a^{-1} \circ b) = b.$$

Όμοια για το στοιχείο $y = b \circ a^{-1}$ έχουμε ότι

$$(b \circ a^{-1}) \circ a = b.$$

Αντίστροφα, υποθέτουμε ότι οι ανωτέρω εξισώσεις έχουν λύση για όλα τα $a, b \in G$. Επομένως, για δοθέν $a \in G$, υπάρχει $e \in G$ που ικανοποιεί την εξίσωση

$$a \circ x = a \text{ (δηλαδή } a \circ e = a).$$

Θα δείξουμε ότι το e είναι δεξιό ουδέτερο, δηλαδή

$$b \circ e = b,$$

για όλα τα $b \in G$. Πράγματι, έχουμε υποθέσει ότι η εξίσωση $y \circ a = b$ έχει λύση στην G, για όλα τα $a, b \in G$. Έστω $r \in G$ μια λύση. Τότε έχουμε

$$b \circ e = (r \circ a) \circ e = r \circ (a \circ e) = r \circ a = b.$$

Επίσης, έχει υποτεθεί ότι η εξίσωση $a \circ x = e$ έχει λύση, αυτό σημαίνει ότι το $a \in G$ έχει δεξιό αντίστροφο.

Άρα τελικά έχουμε αποδείξει ότι για την ημιομάδα $(G, \circ)$ υπάρχει δεξιό ουδέτερο και κάθε στοιχείο έχει δεξιό αντίστροφο. Οπότε, το αποτέλεσμα έπεται από την προηγουμένη πρόταση. ό.έ.δ.

Παρατήρηση 5.1.21. Επισημαίνουμε ότι οι δύο προηγούμενες προτάσεις αποτελούν χαρακτηρισμούς, δηλαδή ισοδύναμους ορισμούς της ομάδας.

Υποομάδες ομάδων.

Έστω $(A, *)$ ένα σύνολο εφοδιασμένο με μία πράξη και B ένα υποσύνολο του συνόλου A. Τότε μπορούμε να πάρουμε τον περιορισμό της πράξης $*$ στο σύνολο $B \times B$. Δηλαδή την απεικόνιση

$$*_{|B} \ : \ B \times B \longrightarrow A,$$

η οποία είναι ο περιορισμός[9] της απεικόνισης $* \ : \ A \times A \longrightarrow A$. Το υποσύνολο $B \subseteq A$ θα ονομάζεται **κλειστό**, ως προς την πράξη $*$, αν

$$*(B \times B) \subseteq B,$$

Δηλαδή, $b_1 * b_2 \in B$, για όλα τα $b_1, b_2 \in B$.

Για παράδειγμα: Αν πάρουμε το σύνολο $(\mathbb{Q}, +)$ των ρητών αριθμών εφοδιασμένο με την πράξη της πρόσθεσης, τότε το (υπο)σύνολο $\mathbb{Z} \subseteq \mathbb{Q}$ των ακεραίων αριθμών είναι κλειστό ως προς την πρόσθεση ρητών αριθμών, διότι $a + b \in Z$, για όλα τα $a, b \in \mathbb{Z}$.

Αν πάρουμε το σύνολο $\mathbb{Q}^*$ των μη μηδενικών ρητών αριθμών, εφοδιασμένο με την πράξη της διαίρεσης (ιδέ το Παράδειγμα 5.1.8$_5$), τότε το υποσύνολο των $\mathbb{Z}^*$ των μη μηδενικών ακεραίων δεν είναι κλειστό ως προς την διαίρεση, δεδομένου ότι για δύο τυχαίους ακεραίους αριθμούς r, s έχουμε ότι

$$r/1 \diamond s/1 \ = \ r/1 \cdot 1/s \ = \ r/s \ \notin \mathbb{Z}^*.$$

Ορισμός 5.1.22. Έστω $(G, \circ)$ μια ομάδα. Ένα μη κενό υποσύνολο $S \subseteq G$ θα ονομάζεται **υποομάδα** της ομάδας $(G, \circ)$, αν το σύνολο $(S, \circ_{|S})$ αποτελεί ομάδα. Στην περίπτωση αυτή θα συμβολίζουμε $S \leq G$.

Σχόλια 5.1.23. Από τον ορισμό έπεται ότι για να ελέγξουμε αν ένα μη κενό υποσύνολο S μιας ομάδας είναι υποομάδα, είναι αναγκαίο να εξασφαλίσουμε ότι το υποσύνολο S είναι κλειστό ως προς την πράξη της ομάδας και φυσικά να ελέγξουμε ότι πληρούνται οι απαιτήσεις του ορισμού της ομάδας (Ορισμός 5.1.16).

Όταν εξασφαλίσουμε ότι το σύνολο S είναι κλειστό ως προς την πράξη, τότε για $a, b, c \in S$, δεδομένου ότι τα στοιχεία αυτά είναι και στοιχεία της ομάδας G και η πράξη $\circ$ είναι προσεταιριστική στην G, έπεται ότι

$$(a \circ b) \circ c \ = \ a \circ (b \circ c) \in S.$$

Επομένως, δεν είναι αναγκαίο να αποδείξουμε (πάλι) ότι ο περιορισμός της πράξης στο σύνολο S ικανοποιεί την προσεταιριστική ιδιότητα. Άρα απομένει να αποδείξουμε ότι για κάθε $a \in S$, το αντίστροφο $a^{-1} \in S$ και ότι το ουδέτερο στοιχείο $e \in S$. Αλλά, αν για κάθε στοιχείο $a \in S$ εξασφαλίσουμε ότι το αντίστροφο $a^{-1} \in S$, τότε δεδομένου ότι έχουμε εξασφαλίσει ότι το σύνολο S είναι κλειστό, ως προς την πράξη $\circ$ έχουμε ότι

$$a \circ a^{-1} \ = \ a^{-1} \circ a \ = \ e \in S.$$

Συνεπώς, για να ελέγξουμε ότι ένα υποσύνολο μιας ομάδας είναι υποομάδα, πρέπει και αρκεί να εξασφαλίσουμε την κλειστότητα ως προς την πράξη της ομάδας και την *κλειστότητα* ως προς το αντίστροφο ($a \in S \implies a^{-1} \in S$).

Μάλιστα δε αυτός ο έλεγχος μπορεί να γίνει ταυτόχρονα.

[9] Για υπενθύμιση του ορισμού του περιορισμού απεικόνισης ανατρέξτε στον Ορισμό 4.5.8.

Πρόταση 5.1.24. *Έστω* $(G, \circ)$ *μια ομάδα. Ένα μη κενό υποσύνολο* $S \subseteq G$ *είναι υποομάδα της* G *αν και μόνο αν*

$$a \circ b^{-1} \in S, \text{ για όλα τα } a, b \in S.$$

Απόδειξη. Η απόδειξη στην πραγματικότητα έχει προηγηθεί. Την παραθέτουμε για λόγους πληρότητας.

Προφανώς, αν το υποσύνολο S αποτελεί υποομάδα της G, τότε

$$a \circ b^{-1} \in S, \text{ για όλα τα } a, b \in S.$$

Αντίστροφα, υποθέτουμε ότι

$$a \circ b^{-1} \in S, \text{ για όλα τα } a, b \in S.$$

Τότε για κάθε $a \in S$ έχουμε ότι

$$a \circ a^{-1} = e \in S.$$

Επομένως, για κάθε $a \in S$ έχουμε ότι

$$e \circ a^{-1} = a^{-1} \in S.$$

Τώρα, για $a, b \in S$ έχουμε ότι

$$a \circ b = a \circ (b^{-1})^{-1} \in S \text{ (γιατί;)}.$$

Άρα, πράγματι το υποσύνολο S είναι υποομάδα της ομάδας G. ό.έ.δ.

Παρατήρηση 5.1.25. Στον ορισμό της υποομάδας (Ορισμός 5.1.22) απαιτούμε ένα υποσύνολο μιας ομάδας να είναι ομάδα ως προς τον περιορισμό της πράξης. Αλλά δεν αναφέρεται ότι το ουδέτερο της υποομάδας συμπίπτει με το ουδέτερο της ομάδας. Όπως επίσης, δεν αναφέρεται ότι το αντίστροφο ενός στοιχείου της υποομάδας συμπίπτει με το αντίστροφο του στοιχείου αυτού, ως στοιχείου της ομάδας.

Στα προηγηθέντα σχόλια αυτό δεν αναφέρεται, μάλιστα θεωρείται δεδομένο. Είναι πράγματι έτσι;

Στην περίπτωση, όπου έχουμε ένα πεπερασμένο υποσύνολο μιας ομάδας, τότε είναι αρκετό να είναι κλειστό ως προς την πράξη της ομάδας, για να είναι υποομάδα. Συγκεκριμένα έχουμε:

Πρόταση 5.1.26. *Έστω* $(G, \circ)$ *μια ομάδα και* S *ένα μη κενό πεπερασμένο υποσύνολό της. Το* S *είναι υποομάδα, αν και μόνο αν*

$$a \circ b \in S, \text{ για όλα τα } a, b \in S.$$

Απόδειξη. Υποθέτουμε ότι

$$a \circ b \in S, \text{ για όλα τα } a, b \in S.$$

Τότε για ένα $a \in S$ έχουμε ότι όλες οι δυνάμεις $a, a^2 = a \circ a, a^3, \ldots$ είναι στοιχεία του συνόλου S. Το S έχει υποτεθεί πεπερασμένο, επομένως δεν είναι δυνατόν οι δυνάμεις αυτές να είναι διάφορες μεταξύ τους. Άρα υπάρχουν θετικοί ακέραιοι $m < n$ με $a^m = a^n$. Από την σχέση αυτή έπεται ότι

$$a^r = e \in S,$$

όπου $r = n - m$ και e το ουδέτερο της ομάδας. Από την σχέση $a^r = e$ έπεται ότι

$$a^{-1} = a^{r-1} \in S$$

και επομένως το S είναι υποομάδα της G.

Η αντίστροφη κατεύθυνση είναι προφανής. ό.έ.δ.

Παραδείγματα 5.1.27. Στα επόμενα παραδείγματα, όπως πάντα, πρέπει να συμπληρώνονται όλα τα κενά, τα οποία ηθελημένα ή μη, υπάρχουν στους προβαλλόμενους ισχυρισμούς.

1. Για κάθε ομάδα $(G, \circ)$ το σύνολο $\{e\}$, όπου e είναι το ουδέτερο της ομάδας, προφανώς(;) αποτελεί υποομάδα της G και θα ονομάζεται η **τετριμμένη** (υπο)ομάδα. Επίσης, η ίδια η ομάδα G είναι υποομάδα του εαυτού της.

   Μια $S \leq G$, η οποία δεν ισούται ούτε με την τετριμμένη, ούτε με την G, θα ονομάζεται **γνήσια** (μη τετριμμένη) υποομάδα.

2. Η ομάδα $(\mathbb{Z}, +)$ των ακεραίων με πράξη την πρόσθεση ακεραίων αριθμών, προφανώς είναι υποομάδα της ομάδας $(\mathbb{Q}, +)$ των ρητών αριθμών με πράξη την πρόσθεση ρητών αριθμών. Η οποία (με τη σειρά της) είναι υποομάδα της ομάδας $(\mathbb{R}, +)$ των πραγματικών αριθμών με πράξη την πρόσθεση πραγματικών αριθμών.

3. Το σύνολο

   $$2\mathbb{Z} = \{2r \mid r \in \mathbb{Z}\}$$

   των αρτίων ακεραίων αριθμών είναι υποομάδα της ομάδας $(\mathbb{Z}, +)$.

   Γενικότερα, αν $m \in \mathbb{Z}$, το σύνολο

   $$m\mathbb{Z} = \{mr \mid r \in \mathbb{Z}\}$$

   όλων των πολλαπλασίων του m είναι υποομάδα της ομάδας $(\mathbb{Z}, +)$.

   Το σύνολο όμως

   $$\{2r + 1 \mid r \in \mathbb{Z}\}$$

   των περιττών ακεραίων αριθμών δεν αποτελεί υποομάδα της ομάδας $(\mathbb{Z}, +)$ (γιατί;)

4. Το σύνολο $\mathbb{N}$ των φυσικών αριθμών, αν και είναι κλειστό ως προς την πρόσθεση φυσικών αριθμών, δεν είναι υποομάδα της ομάδας $(\mathbb{Z}, +)$ (γιατί δεν ισχύει η Πρόταση 5.1.26;).

5. Η πολλαπλασιαστική $(\mathbb{Q}^*, \cdot)$ ομάδα των ρητών αριθμών είναι υποομάδα της πολλαπλασιαστικής ομάδας $(\mathbb{R}^*, \cdot)$ των πραγματικών αριθμών. Αλλά, αν και $\mathbb{Q}^* \subseteq \mathbb{R}$, δεν έχει νόημα να πούμε ότι η ομάδα $(\mathbb{Q}^*, \cdot)$ είναι υποομάδα της προσθετικής $(\mathbb{R}, +)$ ομάδας των πραγματικών αριθμών (γιατί;).

6. Έστω G μια ομάδα και $a \in G$. Το σύνολο

   $$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$$

   είναι προφανώς υποομάδα της G.

   Η υποομάδα αυτή ονομάζεται η **κυκλική** υποομάδα η παραγόμενη από το στοιχείο a. Στο Τρίτο Παράρτημα και συγκεκριμένα στην Παράγραφο Γ.1.1 θα επανέλθουμε διεξοδικότερα στις κυκλικές ομάδες.

7. Στο Παράδειγμα 5.1.17$_{11}$ είχαμε δει ότι το σύνολο $(\mathcal{F}(\mathbb{R}), +)$ των απεικονίσεων με πεδίο ορισμού και πεδίο τιμών το σύνολο των πραγματικών αριθμών είναι ομάδα με πράξη την πρόσθεση απεικονίσεων. Έστω $\mathcal{C}(\mathbb{R})$ το σύνολο των συνεχών απεικονίσεων με πεδίο ορισμού και πεδίο τιμών το σύνολο των πραγματικών αριθμών. Είναι εύκολο να δούμε (ιδέ Άσκηση 5.1.3$_2$) ότι

$$(\mathcal{C}(\mathbb{R}), +) \leq (\mathcal{F}(\mathbb{R}), +).$$

Πρόταση 5.1.28. *Έστω $(G, \cdot)$ μια ομάδα και $A, B \leq G$. Τότε η τομή*

$$A \cap B$$

είναι υποομάδα της G. Γενικά, αν $(A_i)_{i\in I}$ είναι μια οικογένεια υποομάδων της G, τότε η τομή

$$\bigcap_{i\in I} A_i$$

είναι υποομάδα της G.

Απόδειξη. Έστω $a, b \in A \cap B$, τότε $a, b \in A$ και $a, b \in B$. Επειδή οι A και B είναι υποομάδες, έχουμε ότι

$$ab^{-1} \in A \text{ και } ab^{-1} \in \text{B (γιατί;)}.$$

Μα ισχύει η Πρόταση 5.1.24. Συνεπώς

$$ab^{-1} \in A \cap B.$$

Άρα η τομή $A \cap B$ είναι υποομάδα της G[10](γιατί;).

Όμοια αποδεικνύεται ότι και η τομή $\bigcap_{i\in I} A_i$ είναι υποομάδα της G. ό.έ.δ.

Δεν ισχύει μια αντίστοιχη πρόταση για την ένωση υποομάδων. Πιο συγκεκριμένα, έχουμε:

Πρόταση 5.1.29. *Έστω $(G, \cdot)$ μια ομάδα και $A, B \leq G$. Τότε η ένωση $A \cup B$ είναι υποομάδα της G, αν και μόνο αν $A \subseteq B$ ή $B \subseteq A$.*

Απόδειξη. Προφανώς, αν $A \subseteq B$ ή $B \subseteq A$, τότε η ένωση $A \cup B$ είναι υποομάδα της G.

Αντίστροφα, έστω ότι η ένωση $A \cup B$ είναι υποομάδα της G. Υποθέτουμε ότι ο ισχυρισμός $A \subseteq B$ ή $B \subseteq A$ είναι ψευδής. Δηλαδή,

$$A \nsubseteq B, \text{ και } B \nsubseteq A.$$

Επομένως, υπάρχει $a \in A$ με $a \notin B$ και $b \in B$ με $b \notin A$. Το στοιχείο $ab \in A \cup B$ (γιατί;). Μα αφού η ένωση έχει υποτεθεί υποομάδα της G. Επομένως,

$$ab \in A \text{ ή } ab \in B.$$

- Αν $ab \in A$, τότε $a^{-1}(ab) = b \in A$, άτοπο.
- Αν $ab \in B$, τότε $(ab)b^{-1} = a \in B$, πάλι άτοπο.

Άρα δεν είναι δυνατόν $A \nsubseteq B$, και $B \nsubseteq A$ και η απόδειξη ολοκληρώθηκε. ό.έ.δ.

[10]Όπως έχουμε προείπει, όταν δεν υπάρχει σύγχυση, αντί του $a\cdot b^{-1}$, γράφουμε ab^{-1} παραλείποντας το σύμβολο της πράξης.

Σύμπλοκα υποομάδων.

Στο τέταρτο Κεφάλαιο είχαμε μελετήσει τις σχέσεις ισοδυναμίας σε σύνολα καθώς και τις διαμερίσεις συνόλων. Εδώ θα δούμε μια πολύ σημαντική εφαρμογή.

Έστω $(G, \cdot)$ μια ομάδα και H μια υποομάδα της. Στο σύνολο G ορίζουμε μια σχέση ως εξής:

$$a \sim b, \text{ αν } a^{-1} \cdot b \in H.$$

Θα δείξουμε ότι η σχέση αυτή είναι σχέση ισοδυναμίας.

Για κάθε $a \in G$ έχουμε ότι $a \sim a$, δεδομένου ότι

$$a^{-1} \cdot a = 1 \in H.$$

Άρα η σχέση είναι αυτοπαθής.

Υποθέτουμε ότι $a \sim b$, δηλαδή $a^{-1} \cdot b \in H$. Η H είναι υποομάδα, συνεπώς

$$(a^{-1} \cdot b)^{-1} \in H,$$

αλλά $(a^{-1} \cdot b)^{-1} = b^{-1} \cdot a$ (γιατί;), συνεπώς

$$b^{-1} \cdot a \in H,$$

δηλαδή $b \sim a$, επομένως η σχέση είναι συμμετρική.

Υποθέτουμε ότι $a \sim b$ και $b \sim c$, τότε

$$a^{-1} \cdot b \in H \text{ και } b^{-1} \cdot c \in H.$$

Η H έχει υποτεθεί υποομάδα της G, συνεπώς

$$(a^{-1} \cdot b) \cdot (b^{-1} \cdot c) = a^{-1}(\cdot b \cdot b^{-1}) \cdot c = a^{-1} \cdot c \in H.$$

Δηλαδή $a \sim c$, επομένως η σχέση είναι μεταβατική.

Άρα πράγματι η σχέση αυτή είναι σχέση ισοδυναμίας.

Ας υπολογίσουμε τις κλάσεις ισοδυναμίας. Έστω $a \in G$. Εξ ορισμού, η κλάση ισοδυναμίας του είναι η

$$C_a = \{r \in G \mid a \sim r\} = \{r \in G \mid a^{-1} \cdot r \in H\} = \{r \in G \mid r = a \cdot h \mid h \in H\},$$

άρα

$$C_a \subseteq \{a \cdot h \mid h \in H\}.$$

Προφανώς (γιατί;) ισχύει και η αντίστροφη σχέση εγκλεισμού

$$\{a \cdot h \mid h \in H\} \subseteq C_a.$$

Άρα

$$C_a = \{a \cdot h \mid h \in H\}.$$

Η κλάση ισοδυναμίας C_a ονομάζεται **(αριστερό) σύμπλοκο** της υποομάδας H στην ομάδα G και θα συμβολίζεται στο εξής με aH.

Όπως γνωρίζουμε, σε μια σχέση ισοδυναμίας, οι κλάσεις ισοδυναμίας αποτελούν μια διαμέριση του συνόλου (ιδέ Πρόταση 4.4.2), επομένως ισχύει μια αντίστοιχη πρόταση.

Πρόταση 5.1.30. *Έστω G μια ομάδα και H μια υποομάδα της. Για $a, b \in G$, οι ακόλουθες προτάσεις είναι ισοδύναμες:*

1. $a^{-1}b \in H$.
2. $aH = bH$.
3. $a \in bH$, $b \in aH$.

Απόδειξη. Η απόδειξη είναι προφανής, απόρροια του ορισμού της σχέσης ισοδυναμίας. Παρ' όλα ταύτα, να την επαναλάβετε. ό.έ.δ.

Πόρισμα 5.1.31. *Έστω G μια ομάδα, H μια υποομάδα της και $a, b \in G$, τότε ισχύει ότι,*

$$\text{είτε } aH = bH \text{ ή } aH \cap bH = \emptyset.$$

Απόδειξη. Δεν ξεχνάμε ότι οι κλάσεις ισοδυναμίας, σε ένα σύνολο, αποτελούν διαμέριση του συνόλου (ιδέ Πρόταση 4.4.2). ό.έ.δ.

Έστω G μια ομάδα και H μια υποομάδα της, τότε, ως γνωστόν (ιδέ σελ. 130), ορίζεται το σύνολο πηλίκων

$$G/\sim = \{\, aH \mid a \in G \,\}.$$

Αν T είναι ένα σύνολο αντιπροσώπων, τότε ο πληθικός αριθμός

$$|\, T \,| = |\, G/\sim |$$

ονομάζεται **δείκτης** της υποομάδας H στην ομάδα G και θα συμβολίζεται ως

$$[G \,:\, H].$$

Επομένως, επειδή το σύνολο των (διακεκριμένων) συμπλόκων αποτελεί διαμέριση του συνόλου G, κατά φυσιολογικό τρόπο, έχει αποδειχθεί ένα από τα σημαντικότερα θεωρήματα, το οποίο διέπει όλα τα Μαθηματικά και όχι μόνο τον κλάδο της "*Θεωρίας Ομάδων*".

Θεώρημα 5.1.32. *(Θεώρημα του Lagrange) Έστω G μια ομάδα, H μια υποομάδα της και T ένα σύνολο αντιπροσώπων της H στην G. Τότε ισχύει η σχέση:*

$$G = \bigcup_{a \in T} aH.$$

Πρόταση 5.1.33. *Έστω G μια ομάδα, H μια υποομάδα της και $a \in H$. Το σύμπλοκο aH είναι ισοπληθικό*[11] *με το σύνολο H.*

Απόδειξη. Έστω η απεικόνιση $f : H \longrightarrow aH$ με

$$f(h) = ah \in aH.$$

Είναι προφανές (γιατί;) ότι η απεικόνιση f είναι πράγματι απεικόνιση (είναι καλά ορισμένη).

[11] Για όσους δεν είναι εξοικειωμένοι με την έννοια των ισοπληθικών συνόλων παραπέμπουμε στο Δεύτερο Παράρτημα Ορισμός B.0.5.

Έστω $h, r \in H$ με $h \neq r$ τότε

$$f(h) = ah \neq ar = f(r) \text{ (γιατί;)}.$$

Άρα η f είναι 1-1.

Έστω $s \in aH$ τότε υπάρχει (μοναδικό) $h \in H$, ώστε $s = ah$. Το στοιχείο

$$a^{-1}s = h \in H$$

και έχει την ιδιότητα

$$f(h) = ah = a(a^{-1}s) = s.$$

Άρα η απεικόνιση f είναι επί. Επομένως, απεδείχθη ότι τα δύο σύνολα H και aH είναι ισοπληθικά για όλα τα $a \in G$. ό.έ.δ.

Θεώρημα 5.1.34. *(Το Θεώρημα του Lagrange για πεπερασμένες ομάδες)*
Έστω G μια πεπερασμένη ομάδα και H μια υποομάδα της. Τότε ισχύει ότι:

$$|\, G \,| = [G : H] \cdot |\, H \,|.$$

Απόδειξη. Έστω $\mathrm{T} = \{a_1, a_2, \ldots, a_k\}$ ένα σύστημα αντιπροσώπων της H στην G. Από το Θεώρημα 5.1.32 έχουμε ότι

$$G = \bigcup_{a \in T} aH.$$

Η ένωση είναι διακεκριμένη, επομένως

$$|\, G \,| = |\, a_1H \,| + |\, a_2H \,| + \cdots + |\, a_kH \,|.$$

Από την προηγουμένη πρόταση έχουμε ότι $|\, a_iH \,| = |\, H \,|$, για όλα τα a_i. Άρα

$$|\, G \,| = [G : H] \cdot |\, H \,|,$$

δεδομένου ότι, εξ ορισμού, ο δείκτης $[G : H] = |\, T \,|$. ό.έ.δ.

Παραδείγματα 5.1.35.

1. Έστω $(\mathbb{Z}, +)$ η προσθετική ομάδα των ακεραίων αριθμών και m ένας θετικός ακέραιος, τότε τα σύμπλοκα της υποομάδας $m\mathbb{Z} = \{mr \mid r \in \mathbb{Z}\}$, ως προς την ομάδα $(\mathbb{Z}, +)$, είναι τα

   $$0 + m\mathbb{Z},\ 1 + m\mathbb{Z},\ \ldots,\ (m-1) + m\mathbb{Z}$$ [12]

   (γιατί; Παραβάλλετε με το Παράδειγμα $4.4.4_1$).

2. Στο Παράδειγμα $5.1.17_5$ είχαμε δει την ομάδα μεταθέσεων S_3 σε 3 σύμβολα. Έστω $H = \{1, \pi\}$, όπου

   $$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

   Προφανώς (γιατί;) η H είναι υποομάδα της S_3, ας υπολογίσουμε τα αριστερά σύμπλοκα της H στην S_3. Σύμφωνα με τα προηγούμενα, θα έχουμε (φαινομενικά) τα εξής σύμπλοκα:

   $$1H,\ \pi H, \rho H,\ \sigma H,\ \phi H,\ \tau H.$$

[12] Προσοχή στον συμβολισμό, εδώ έχουμε προσθετικό συμβολισμό.

Αλλά, συμβουλευόμενοι και τον πολλαπλασιαστικό πίνακα της S_3 (ιδέ το Παράδειγμα 5.1.17 $_7$, έχουμε ότι

$$1H = \pi H, \rho H = \phi H, \sigma H = \tau H.$$

Δηλαδή υπάρχουν 3 το πλήθος (διαφορετικά) σύμπλοκα. Αναμενόμενο, διότι ο δείκτης της H στην S_3 είναι ίσος με 3 (ιδέ το Θεώρημα 5.1.34).

Σχόλιο 5.1.36. Έστω G μια ομάδα και A, B δύο υποομάδες της. Τότε, ως γνωστόν (ιδέ Άσκηση 5.1.1$_5$), ορίζεται το γινόμενο

$$AB = \{ab \mid a \in A, b \in B\},$$

το οποίο όμως δεν είναι, εν γένει, υποομάδα της G.

5.1.3 Ασκήσεις

1. Έστω $(M, *)$ μια ημιομάδα με την ιδιότητα:

   Για κάθε $a \in M$ υπάρχει μοναδικό $\bar{a} \in M$, έτσι ώστε $a * \bar{a} * a = a$.

   Δείξτε ότι το $(M, *)$ είναι ομάδα.

2. Αποδείξτε, με κάθε λεπτομέρεια, ότι το σύνολο $\mathcal{F}(\mathbb{R})$ όλων των απεικονίσεων με πεδίο ορισμού και πεδίο τιμών το σύνολο των πραγματικών αριθμών είναι ομάδα με πράξη την πρόσθεση απεικονίσεων (ιδέ Παράδειγμα 5.1.17$_{11}$).

   Επίσης, δείξτε ότι το σύνολο των $(\mathcal{C}(\mathbb{R}), +)$ των συνεχών απεικονίσεων με πεδίο ορισμού και πεδίο τιμών το σύνολο των πραγματικών αριθμών είναι υποομάδα της $(\mathcal{F}(\mathbb{R}), +)$ [13].

3. *Ο Νόμος της διαγραφής στις Ομάδες.* Έστω $(G, \circ)$ μια ομάδα και $a, b, c \in G$.

   Δείξτε ότι,

   $$\text{αν } a \circ b = a \circ c, \text{ τότε ισχύει ότι } b = c.$$

   Όπως επίσης,

   $$\text{αν } b \circ a = c \circ a, \text{ τότε ισχύει ότι } b = c.$$

   Μπορούμε από την σχέση $a \circ b = c \circ a$ να συμπεράνουμε ότι $b = c$;

   Δείξτε ότι, αν από την σχέση $a \circ b = c \circ a$ έπεται ότι $b = c$, για όλα τα $a, b, c \in A$, τότε η ομάδα A είναι αβελιανή.

   Μπορείτε να δώσετε ένα παράδειγμα ενός συνόλου $(A, *)$, το οποίο δεν είναι ομάδα, αλλά ισχύει ο Νόμος της διαγραφής;

4. Δείξτε ότι μια ομάδα G είναι αβελιανή, αν και μόνο αν

   $$(ab)^{-1} = a^{-1}b^{-1}, \text{ για όλα τα } a, b \in G.$$

5. Δείξτε ότι στον πολλαπλασιαστικό πίνακα μιας ομάδας κάθε στοιχείο της ομάδας, σε κάθε γραμμή και κάθε στήλη, εμφανίζεται ακριβώς μια φορά.

[13] Θα χρειασθεί η "στοιχειώδης; γνώση" το τι σημαίνει συνεχής απεικόνιση και ότι το άθροισμα συνεχών απεικονίσεων είναι συνεχής απεικόνιση.

6. Έστω μια ομάδα με ημιτελή τον πολλαπλασιαστικό της πίνακα

$*$	e	a	b	c	d
e	e				
a		b			e
b		c	d	e	
c		d		a	b
d					

Μπορείτε να τον συμπληρώσετε;

Δείξτε ότι η ομάδα G, η οποία έχει αυτόν τον πολλαπλασιαστικό πίνακα, είναι αβελιανή.

Να δείξετε ότι, για κάθε $e \neq r \in G$, υπάρχουν k_1, k_2, k_3, k_4 θετικοί ακέραιοι (εξαρτώμενοι από το r), ώστε

$$a = r^{k_1},\ b = r^{k_2},\ c = r^{k_3},\ d = r^{k_4}.$$

Είναι οι ακέραιοι αυτοί μοναδικοί;

7. Έστω ένα σύνολο με τρία το πλήθος στοιχεία. Στο σύνολο αυτό μπορούν να ορισθούν πολλές πράξεις (ιδέ Άσκηση 5.1.1$_3$). Δείξτε ότι μόνο μια από αυτές ορίζει ομάδα.

Να κατασκευάσετε τον πολλαπλασιαστικό της πίνακα.

8. Στο Παράδειγμα 5.1.17$_7$ είχαμε δει τον πολλαπλασιαστικό πίνακα της ομάδας μεταθέσεων επί ενός συνόλου με τρία στοιχεία. Να κάνετε (ενδελεχή) έλεγχο για την ορθότητά του.

9. Στο Παράδειγμα 5.1.17$_6$ είχαμε περιγράψει τις κινήσεις ενός πιονιού σε μια 2×2 σκακιέρα. Δείξτε, με κάθε λεπτομέρεια, ότι το σύνολο αυτό, με πράξη την σύνθεση απεικονίσεων, αποτελεί ομάδα.

Να κατασκευάσετε τον πολλαπλασιαστικό της πίνακα. Δείξετε ότι για κάθε στοιχείο R αυτής της ομάδας ισχύει ότι

$$R^2 = I.$$

Δείξτε ότι η ομάδα αυτή είναι υποομάδα της ομάδας μεταθέσεων του συνόλου

$$X = \{1, 2, 3, 4\}$$

10. Δείξτε ότι, αν για δύο στοιχεία a, b μιας ομάδας ισχύει $(ab)^2 = a^2b^2$, τότε

$$ab = ba.$$

11. Δείξτε ότι το σύνολο

$$\{3^m 6^n \mid m, n \in \mathbb{Z}\}$$

αποτελεί υποομάδα της πολλαπλασιαστικής ομάδας των ρητών αριθμών.

12. Έστω G μια πεπερασμένη ομάδα. Δείξτε ότι το πλήθος των στοιχείων της G με την ιδιότητα $r^3 = 1_G$ είναι περιττό, ενώ το πλήθος των στοιχείων της G με την ιδιότητα $s^2 \neq 1_G$ είναι άρτιο.

13. Στο Παράδειγμα 5.1.17$_{10}$ είχαμε δει ότι το δυναμοσύνολο $\mathcal{P}(A)$ ενός συνόλου A με πράξη την συμμετρική διαφορά συνόλων αποτελεί ομάδα. Έστω

$$A = \{a, b, c\}$$

ένα σύνολο με τρία το πλήθος στοιχεία, να κατασκευάσετε τον πολλαπλασιαστικό πίνακα της ομάδας

$$(\mathcal{P}(A), \oplus).$$

14. Έστω $(G, \cdot)$ μια ομάδα και $a, b, c \in G$. Να βρεθεί ένα στοιχείο $x \in G$, ώστε να αληθεύουν ταυτόχρονα οι ισότητες:

$$x^2a = bxc^{-1} \text{ και } acx = xac.$$

Όπως επίσης οι ισότητες:

$$(xax)^3 = bx \text{ και } x^2a = (xa)^{-1}.$$

15. Έστω G μια ομάδα και $a, b, c \in G$. Εξετάστε αν οι ακόλουθες συνεπαγωγές είναι αληθείς:

i. $a^2 = b^2 \Longrightarrow a = b.$

ii. $abc = 1_G \Longrightarrow bca = 1_G \Longrightarrow cab = 1_G.$

iii. $(ab)^2 = a^2b^2 \Longrightarrow ab = ba.$

iv. $a^2b^2 = b^2a^2 \Longrightarrow ab = ba.$

16. Έστω G μια πεπερασμένη ομάδα και

$$S = \{g \in G \mid g \neq g^{-1}\}.$$

Δείξτε ότι το σύνολο S έχει άρτιο το πλήθος στοιχεία.

17. Έστω G μια πεπερασμένη ομάδα με άρτιο το πλήθος στοιχεία. Δείξτε ότι υπάρχει τουλάχιστον ένα $r \in G$ με

$$r \neq 1 \text{ και } r = r^{-1}.$$

18. Έστω $G = \{a_1, a_2, \ldots, a_n\}$ μια πεπερασμένη αβελιανή ομάδα. Δείξτε ότι:

i. $(a_1 \cdot a_2 \cdot \cdots \cdot a_n)^2 = 1.$

ii. Αν δεν υπάρχει $x \in G$ με $x \neq 1$ και $x = x^{-1}$, τότε

$$a_1 \cdot a_2 \cdot \cdots \cdot a_n = 1.$$

iii. Αν υπάρχει ακριβώς ένα $x \in G$ με $x \neq 1$ και $x = x^{-1}$, τότε

$$a_1 \cdot a_2 \cdot \cdots \cdot a_n = x.$$

19. (*Το καρτεσιανό γινόμενο ομάδων*).

Έστω $(A, \circ)$, $(B, *)$ δύο ομάδες. Στο καρτεσιανό γινόμενο $A \times B$ ορίζουμε μια πράξη (κατά συντεταγμένες) ως εξής:

$$(a_1, b_1) \diamond (a_2, b_2) = (a_1 \circ a_2, b_1 * b_2),$$

για όλα τα $a_1, a_2 \in A$ και $b_1, b_2 \in B$. Δείξτε, με κάθε λεπτομέρεια, ότι το σύνολο $(A \times B, \diamond)$ είναι ομάδα.

20. Δείξτε ότι κάθε υποομάδα της προσθετικής ομάδας των ακεραίων αριθμών είναι της μορφής

$$m\mathbb{Z} = \{ mr \mid r \in \mathbb{Z} \},$$

για κάποιο $m \in \mathbb{Z}$ (παράβαλλε με το Παράδειγμα 5.1.27$_3$).

21. i. Έστω H μία γνήσια υποομάδα της προσθετικής ομάδας των ακεραίων αριθμών, η οποία περιέχει, ως στοιχεία, τους ακεραίους 18, 30 και 40. Να προσδιορίσετε όλα τα στοιχεία της H.

ii. Να προσδιορίσετε όλες τις γνήσιες υποομάδες της προσθετικής ομάδας των ακεραίων αριθμών, οι οποίες περιέχουν, ως στοιχεία τους αριθμούς 12, 30 και 54.

22. Έστω G μια ομάδα και $a, b \in G$. Δείξτε ότι υπάρχει $x \in G$, ούτως ώστε

$$xax = b, \text{ αν και μόνο αν } ab = c^2,$$

για κάποιο $c \in G$.

23. Έστω G ομάδα. Δείξτε ότι:

Αν $a \in G$ με $a^2 = 1$, τότε υπάρχει $z \in G$ με $z^3 = a$.

Αν $b \in G$ με $b^3 = 1$, τότε υπάρχει $w \in G$ με $w^2 = b$.

24. Έστω G μια ομάδα, H μια υποομάδα της και $a \in G$. Δείξτε ότι ισχύει η ισότητα

$$aH = H, \text{ αν και μόνο αν } a \in H,$$
$$\text{αν και μόνο αν το } aH \text{ είναι υποομάδα της } G.$$

25. Έστω $G = \mathbb{R} \times \mathbb{R}$ η ομάδα των σημείων του επιπέδου με πράξη την (κατά συντεταγμένες) πρόσθεση. Έστω

$$H = \{ (a, a) \mid a \in \mathbb{R} \}.$$

Δείξτε ότι η H είναι υποομάδα της G. Να περιγράψετε γεωμετρικά τα σύμπλοκα της H στην G.

26. Έστω G μια ομάδα και A, B δύο υποομάδες της. Τότε, ως γνωστόν (ιδέ Άσκηση 5.1.1$_5$), ορίζεται το γινόμενο

$$AB = \{ ab \mid a \in A, b \in B \},$$

το οποίο όμως δεν είναι, εν γένει, υποομάδα της G (ιδέ Σχόλιο 5.1.36). Δείξτε ότι το γινόμενο AB είναι υποομάδα της G, αν και μόνο αν $AB = BA$,

5.1.4 Δακτύλιοι - Σώματα

Όπως έχουμε δει, σε ένα σύνολο ενδέχεται να έχουν ορισθεί περισσότερες της μίας πράξεις. Σε τέτοιες περιπτώσεις, ενδιαφέρον έχει να δούμε πώς οι δύο πράξεις *συνδέονται* μεταξύ τους. Για παράδειγμα, το σύνολο των ακεραίων $\mathbb{Z}$ είναι εφοδιασμένο με δύο πράξεις, την πρόσθεση και τον πολλαπλασιασμό. Οι δύο αυτές πράξεις συνδέονται μεταξύ τους με τον εξής *τρόπο*:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \text{ και } (b + c) \cdot a = (b \cdot a) + (c \cdot a),$$

για όλα τα $a, b, c \in \mathbb{Z}$.

Η συνύπαρξη αυτών των δύο πράξεων προσδίδει στους ακεραίους τις γνωστές ιδιότητες, οι οποίες δεν απορρέουν, αν θεωρήσουμε μεμονωμένα την πράξη της πρόσθεσης και μεμονωμένα την πράξη του πολλαπλασιασμού.

Το ίδιο συμβαίνει και με το σύνολο των ρητών αριθμών, όπου και αυτό είναι εφοδιασμένο με τις πράξεις της πρόσθεσης και του πολλαπλασιασμού, οι οποίες πάλι συνδέονται με τον ίδιο τρόπο

$$r \cdot (s + t) = (r \cdot s) + (r \cdot t) \text{ και } (s + t) \cdot r = (s \cdot r) + (t \cdot r),$$

για όλα τα $r, s, t \in \mathbb{Q}$.

Η πλέον σημαντική Αλγεβρική δομή εφοδιασμένη με δύο πράξεις, οι οποίες συνδέονται μεταξύ τους, είναι ο δακτύλιος.

Ορισμός 5.1.37. Ένας **δακτύλιος** είναι ένα σύνολο $(R, +, \cdot)$ εφοδιασμένο με δύο πράξεις, μια *πρόσθεση* και έναν *πολλαπλασιασμό*, ως προς τις οποίες ισχύουν τα εξής:

i. Ως προς την πρόσθεση το σύνολο $(R, +)$ είναι μια αβελιανή ομάδα.

ii. Ως προς τον πολλαπλασιασμό το σύνολο $(R, \cdot)$ είναι μια ημιομάδα (δηλαδή η πράξη του πολλαπλασιασμού είναι προσεταιριστική).

iii. Ο πολλαπλασιασμός είναι επιμεριστικός ως προς την πρόσθεση, δηλαδή ισχύει

$$r \cdot (s + t) = (r \cdot s) + (r \cdot t) \text{ και } (s + t) \cdot r = (s \cdot r) + (t \cdot r),$$

για όλα τα $r, s, t \in R$.

Πριν προχωρήσουμε, πρέπει να επισημάνουμε τα εξής:

Σε έναν δακτύλιο έχει σημασία ποια πράξη χαρακτηρίζουμε ως *πρόσθεση* και ποια ως *πολλαπλασιασμό*, δεδομένου ότι απαιτούμε η πράξη του πολλαπλασιασμού να είναι επιμεριστική ως προς την πράξη της πρόσθεσης και όχι το αντίστροφο.

Δεν απαιτούμε, η πράξη του πολλαπλασιασμού να είναι μεταθετική. Στην περίπτωση, όπου ο πολλαπλασιασμός είναι μεταθετικός, ο δακτύλιος θα ονομάζεται **μεταθετικός** (επισημαίνουμε ότι η πράξη της πρόσθεσης, εξ ορισμού, είναι πάντα μεταθετική).

Δεν απαιτούμε ως προς την πράξη του πολλαπλασιασμού, να υπάρχει ουδέτερο. Στην περίπτωση, όπου ο πολλαπλασιασμός έχει ουδέτερο, ο δακτύλιος ονομάζεται **δακτύλιος με μονάδα**.

Το ουδέτερο ενός δακτυλίου R ως προς τον πολλαπλασιασμό, αν υπάρχει, θα συμβολίζεται με 1_R και το ουδέτερο ως προς την πρόσθεση, το οποίο πάντα υπάρχει, θα συμβολίζεται με 0_R. Μάλιστα δε, όταν δεν υπάρχει κίνδυνος σύγχυσης, απλώς θα μιλάμε για το ένα 1 και το μηδέν 0 αντίστοιχα.

Επίσης, όταν δεν υπάρχει κίνδυνος σύγχυσης, αντί του συμβολισμού $(R, +, \cdot)$, θα γράφουμε απλώς ο δακτύλιος R.

Σε έναν δακτύλιο με μονάδα δεν απαιτούμε όλα τα στοιχεία του να έχουν αντίστροφο ως προς τον πολλαπλασιασμό, ενώ ως προς την πρόσθεση, εξ ορισμού, όλα τα στοιχεία έχουν αντίθετο.

Πρόταση 5.1.38. *Έστω $(R, +, \cdot)$ ένας δακτύλιος με μονάδα. Το σύνολο $U(R)$ των αντιστρεψίμων, ως προς τον πολλαπλασιασμό, στοιχείων του R αποτελεί ομάδα, η οποία θα ονομάζεται η* ***πολλαπλασιαστική*** *ομάδα του δακτυλίου.*

Απόδειξη. Το σύνολο $U(R)$ είναι μη κενό (γιατί;). Έστω $r, s \in U(R)$, τότε $r \cdot s \in U(R)$ (γιατί;). Μα αφού ισχύει η Πρόταση 5.1.7. Οπότε, πράγματι το $U(R)$ αποτελεί ομάδα ως προς τον πολλαπλασιασμό. ό.έ.δ.

Προφανώς (γιατί;) το σύνολο $(\mathbb{Z}+, \cdot)$ των ακεραίων αριθμών εφοδιασμένο με τις γνωστές πράξεις της πρόσθεσης και του πολλαπλασιασμού είναι ένας μεταθετικός δακτύλιος με μονάδα, του οποίου η πολλαπλασιαστική ομάδα είναι η

$$U(\mathbb{Z}) = \{1, -1\}.$$

Επίσης, τα σύνολα των ρητών και των πραγματικών αριθμών εφοδιασμένα με τις γνωστές πράξεις της πρόσθεσης και του πολλαπλασιασμού είναι μεταθετικοί δακτύλιοι με μονάδα και οι πολλαπλασιαστικές ομάδες τους, και στις δύο περιπτώσεις, αποτελούνται από όλα τα μη μηδενικά στοιχεία. Δηλαδή

$$U(\mathbb{Q}) = \mathbb{Q}^* \text{ και } U(\mathbb{R}) = \mathbb{R}^*.$$

Πριν δούμε άλλα παραδείγματα δακτυλίων, ας δούμε ορισμένες ιδιότητες δακτυλίων, οι οποίες απορρέουν από την επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση.

Πρόταση 5.1.39. [14] *Έστω a, b στοιχεία ενός δακτυλίου R. Τότε ισχύουν τα εξής:*

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$.
3. $(-a) \cdot (-b) = a \cdot b$.

Απόδειξη.

1. Έχουμε ότι
$$a \cdot 0 + 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$
Από τον πρώτο όρο και τον τελευταίο όρο των ανωτέρω διαδοχικών ισοτήτων έπεται (λόγω του Νόμου της διαγραφής στις ομάδες) ότι πράγματι
$$a \cdot 0 = 0.$$

[14] Οι ιδιότητες αυτές είναι οι γνωστές ιδιότητες που ισχύουν στον δακτύλιο των ακεραίων και πολλές φορές μερικοί τις θεωρούν...Αξιώματα. Εδώ παραπέμπουμε στην Παρατήρηση 6.1.13.

2. Έχουμε ότι
$$a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0.$$
Επομένως, το στοιχείο $a \cdot (-b)$ είναι το αντίθετο του $a \cdot b$, άρα
$$a \cdot (-b) = -(a \cdot b).$$
Όμοια
$$(-a) \cdot b = -(a \cdot b).$$

3. Το αποτέλεσμα είναι άμεσο από τα προηγούμενα. ό.έ.δ.

Σχόλια 5.1.40.

1. Υπενθυμίζουμε ότι, αν n είναι ένας θετικός ακέραιος και R ένας δακτύλιος, τότε για $r \in R$ ορίζουμε
$$r^n = \underbrace{r \cdot r \cdot \cdots \cdot r}_{n} \text{ και } n \cdot r = \underbrace{r + r + \cdots + r}_{n}.$$
Οπότε, μπορούμε να αποδείξουμε "ανάλογα" αποτελέσματα με την προηγουμένη πρόταση. Ιδέ Άσκηση 5.1.5$_4$.

2. Ένας δακτύλιος με ένα μόνο στοιχείο, το μηδέν, θα ονομάζεται ο **τετριμμένος** δακτύλιος ή ο **μηδενικός** δακτύλιος.

   Σε έναν μη τετριμμένο δακτύλιο με μονάδα, το μηδέν, το ουδέτερο ως προς την πρόσθεση, και το ένα, το ουδέτερο ως προς τον πολλαπλασιασμό, είναι διαφορετικά στοιχεία.

   Πράγματι, υποθέτουμε ότι $0 = 1$, τότε για ένα στοιχείο r του δακτυλίου θα έχουμε
   $$r = r \cdot 1 = r \cdot 0 = 0,$$
   δηλαδή όλα τα στοιχεία του δακτυλίου συμπίπτουν με το μηδενικό στοιχείο, άτοπο.

Μια σημαντική κατηγορία δακτυλίων, η οποία παρουσιάζει μεγάλο ενδιαφέρον είναι τα σώματα.

Ορισμός 5.1.41. Ένας μεταθετικός δακτύλιος με μονάδα, όπου όλα τα μη μηδενικά στοιχεία του έχουν αντίστροφο, ονομάζεται **σώμα**.

Προφανώς, ο δακτύλιος
$$(\mathbb{Q}, +, \cdot)$$
των ρητών αριθμών είναι σώμα, όπως και ο δακτύλιος
$$(\mathbb{R}, +, \cdot)$$
των πραγματικών αριθμών είναι σώμα. Ενώ ο δακτύλιος
$$(\mathbb{Z}, +, \cdot)$$
των ακεραίων δεν είναι σώμα.

Στην πορεία θα συναντήσουμε και άλλα σώματα.

Παραδείγματα 5.1.42.

1. Στο Παράδειγμα 5.1.17$_{10}$ είχαμε δει ότι το δυναμοσύνολο $\mathcal{P}(A)$ ενός συνόλου A αποκτά την δομή ομάδας με πράξη την συμμετρική διαφορά συνόλων. Στο σύνολο αυτό ορίζουμε ως πράξη του "πολλαπλασιασμού" την τομή συνόλων.

   Όπως γνωρίζουμε, η τομή συνόλων είναι επιμεριστική ως προς την συμμετρική διαφορά συνόλων. Γιατί ισχύει αυτό; Αρκεί να ανατρέξουμε στο πρώτο Κεφάλαιο στην Άσκηση 1.1.3$_9$. Επομένως, δεδομένου ότι για την τομή συνόλων ισχύει η προσεταιριστική ιδιότητα (ιδέ Θεώρημα 1.1.25), έχουμε ότι (με τις λεπτομέρειες να αφήνονται ως άσκηση) το σύνολο

   $$(\mathcal{P}(A), \oplus, \cap)$$

   είναι μεταθετικός δακτύλιος με μονάδα.

2. (Το καρτεσιανό γινόμενο δακτυλίων).

   Έστω $(R_1, +, \cdot)$, $(R_2, +\cdot)$ δύο δακτύλιοι. Στο καρτεσιανό γινόμενο $R_1 \times R_2$ ορίζουμε δύο πράξεις κατά συντεταγμένες ως εξής: Την πρόσθεση

   $$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$

   και τον πολλαπλασιασμό

   $$(a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot b_1, a_2 \cdot b_2),$$

   για όλα τα $a_1, b_1 \in R_1$ και $a_2, b_2 \in R_2$. Είναι εύκολο να δούμε ότι το σύνολο

   $$(R_1 \times R_2, +, \cdot)$$

   είναι δακτύλιος. (Παράβαλλε με την Άσκηση 5.1.3$_{19}$).

   Σημείωση. Στο παράδειγμα αυτό (σκοπίμως) χρησιμοποιούμε το ίδιο σύμβολο $+$ της πρόσθεσης για τρεις διαφορετικές προσθέσεις, την πρόσθεση στον δακτύλιο R_1, την πρόσθεση στον δακτύλιο R_2 και την πρόσθεση στο καρτεσιανό γινόμενο $R_1 \times R_2$. Όμοια για το σύμβολο $\cdot$ του πολλαπλασιασμού. Αυτό για να εξοικειωνόμαστε με την χρήση των συμβόλων χωρίς να προκαλείται σύγχυση.

3. Στον δακτύλιο $(\mathbb{Z}, +, \cdot)$ των ακεραίων ορίζουμε δύο νέες πράξεις ως εξής: Μια πρόσθεση

   $$a \oplus b = a + b - 1$$

   και έναν πολλαπλασιασμό

   $$a \odot b = a + b - a \cdot b.$$

   Το σύνολο

   $$(\mathbb{Z}, \oplus, \odot)$$

   ως προς τις πράξεις αυτές αποκτά μια άλλη δομή δακτυλίου. Μάλιστα δε, ο νέος δακτύλιος είναι και αυτός μεταθετικός με μονάδα, αλλά το ουδέτερο $0_\oplus$ ως προς την πρόσθεση ισούται με το 1 και το μοναδιαίο $1_\odot$ ως προς τον πολλαπλασιασμό ισούται με το μηδέν.

   Το παράδειγμα αυτό αποτελεί άλλο ένα χαρακτηριστικό παράδειγμα, όπου η αλγεβρική δομή ενός συνόλου αλλάζει άρδην, αν αλλάξουμε τις πράξεις επί των οποίων ορίζεται η εκάστοτε αλγεβρική δομή.

4. (Ο δακτύλιος Boole)

   Στο δεύτερο Κεφάλαιο (σελ. 42) είχαμε δει τους πίνακες αληθείας για την σύζευξη και αποκλειστική διάζευξη προτάσεων. Συγκεκριμένα:

   Ο πίνακας αληθείας για την σύζευξη Προτάσεων είναι ο εξής:

P	Q	P ∧ Q
Α	Α	Α
Α	Ψ	Ψ
Ψ	Α	Ψ
Ψ	Ψ	Ψ

   Ο πίνακας αληθείας για την αποκλειστική διάζευξη είναι ο εξής:

P	Q	P $\underline{\vee}$ Q
Α	Α	Ψ
Α	Ψ	Α
Ψ	Α	Α
Ψ	Ψ	Ψ

   Στο σύνολο $B = \{\Α, \Psi\}$, η αποκλειστική διάζευξη και η σύζευξη αποτελούν πράξεις. Το σύνολο $(B, \underline{\vee}, \wedge)$ είναι ένας μεταθετικός δακτύλιος με μονάδα, όπου πρόσθεση είναι η αποκλειστική διάζευξη και πολλαπλασιασμός η σύζευξη.

   Να κάνετε τον έλεγχο.

   Συγκρίνατε με το πρώτο Παράδειγμα.

Υποδακτύλιοι.

Ορισμός 5.1.43. Έστω $(R, +, \cdot)$ ένας δακτύλιος. Ένα S, μη κενό, υποσύνολο του R θα ονομάζεται υποδακτύλιος του R και θα συμβολίζεται $S \leq R$, αν είναι δακτύλιος ως προς τον περιορισμό επί του S της πρόσθεσης και του πολλαπλασιασμού.

Για τον έλεγχο, κατά πόσο ένα υποσύνολο ενός δακτυλίου, αποτελεί υποδακτύλιο δεν χρειάζεται να ελέγξουμε (από την αρχή), αν ισχύουν όλες οι ιδιότητες του ορισμού του δακτυλίου. Ισχύει ένα ανάλογο κριτήριο με την Πρόταση 5.1.24 για τις ομάδες.

Πρόταση 5.1.44. *Ένα μη κενό υποσύνολο S ενός δακτυλίου $(R, +, \cdot)$ είναι υποδακτύλιος αν και μόνο αν ισχύει*

$$a - b,\ a \cdot b \in S,$$

για όλα τα $a, b \in S$. Δηλαδή το σύνολο S είναι κλειστό ως προς την αφαίρεση και τον πολλαπλασιασμό.

Απόδειξη. Η απόδειξη είναι παρόμοια με την απόδειξη της Πρότασης 5.1.24, μόνο που εδώ (για την ομάδα) έχουμε τον προσθετικό συμβολισμό. ό.έ.δ.

Πρόταση 5.1.45. *Έστω R ένας δακτύλιος και $(S_i)_{i\in I}$ μια οικογένεια υποδακτυλίων του R, τότε η τομή*

$$\bigcap_{i\in I} S_i$$

είναι υποδακτύλιος του R.

Απόδειξη. Η απόδειξη είναι παρόμοια με την απόδειξη της Πρότασης 5.1.28, απλώς εδώ να την επαναλάβετε με κάθε λεπτομέρεια. ό.έ.δ.

Παραδείγματα 5.1.46.

1. Προφανώς, σε κάθε δακτύλιο R ο τετριμμένος δακτύλιος και όλος ο δακτύλιος R είναι υποδακτύλιοι του R.

2. Ο δακτύλιος των ακεραίων είναι υποδακτύλιος του δακτυλίου των ρητών, όπως επίσης ο δακτύλιος των ρητών είναι υποδακτύλιος του δακτυλίου των πραγματικών αριθμών.

3. Όπως έχουμε δει, για κάθε θετικό ακέραιο αριθμό m ορίζεται η υποομάδα

$$m\mathbb{Z} = \{mr \mid r \in \mathbb{Z}\}$$

της προσθετικής ομάδας των ακεραίων αριθμών. Είναι εύκολο να δούμε ότι το σύνολο αυτό είναι κλειστό ως προς τον πολλαπλασιασμό ακεραίων αριθμών, συνεπώς είναι υποδακτύλιος του δακτυλίου $\mathbb{Z}$. Μάλιστα δε, οι μόνοι υποδακτύλιοι του δακτυλίου των ακεραίων αριθμών είναι αυτής της μορφής (γιατί; Παράβαλλε με την Άσκηση $5.1.3_{20}$).

Παρατήρηση 5.1.47. Όπως βλέπουμε, σε έναν υποδακτύλιο δεν κληρονομούνται όλες οι ιδιότητες του αρχικού δακτυλίου.

Στο δεύτερο παράδειγμα, ο δακτύλιος των ακεραίων, παρ' ότι είναι υποδακτύλιος του σώματος των ρητών, δεν είναι σώμα.

Επίσης, στο τρίτο παράδειγμα, ο δακτύλιος $m\mathbb{Z}$, για $m > 1$, δεν έχει ουδέτερο ως προς τον πολλαπλασιασμό, παρ' ότι είναι υποδακτύλιος των ακεραίων, όπου εκεί έχουμε ουδέτερο ως προς τον πολλαπλασιασμό.

Θα επανέλθουμε στους δακτυλίους αναφέροντας μερικές ιδιότητες επιπλέον των δακτυλίων, καθώς και κάποιες αξιοσημείωτες κατηγορίες δακτυλίων (ιδέ το τρίτο Παράρτημα).

5.1.5 Ασκήσεις

1. Στα τρία Παραδείγματα 5.1.42 να συμπληρώσετε, με κάθε λεπτομέρεια, όλα τα κενά που υπάρχουν στην επιχειρηματολογία.

2. Έστω R ένας δακτύλιος. Δείξτε ότι

$$a^2 - b^2 = (a + b) \cdot (a - b),$$

για όλα τα $a, b \in R$, αν και μόνο αν ο δακτύλιος είναι μεταθετικός.

3. Δείξτε ότι σε έναν δακτύλιο R, αν ισχύει $a \cdot b = -(b \cdot a)$, τότε

$$(a + b)^2 = (a - b)^2 = a^2 + b^2.$$

4. Έστω R ένας δακτύλιος, $a, b \in R$ και m, n ακέραιοι αριθμοί. Δείξτε ότι:

   i. $(m + n) \cdot a = m \cdot a + n \cdot a.$

   ii. $m \cdot (ab) = (m \cdot a)b = a(m \cdot b).$

iii. $(m \cdot a)(n \cdot b) = (mn) \cdot (ab)$.

iv. $n \cdot (-a) = (-n) \cdot a = -(n \cdot a)$.

5. Στο Παράδειγμα 5.1.46$_3$ είχαμε περιγράψει όλους τους υποδακτυλίους του δακτυλίου των ακεραίων αριθμών. Να προσδιορίσετε την τομή

$$2\mathbb{Z} \cap 3\mathbb{Z}.$$

Μπορείτε, γενικά, να προσδιορίσετε την τομή

$$m\mathbb{Z} \cap n\mathbb{Z},$$

όπου m, n είναι τυχαίοι θετικοί ακέραιοι αριθμοί;

6. Έστω ένα σύνολο $(R, +, \cdot)$ εφοδιασμένο με δύο πράξεις, το οποίο ικανοποιεί όλες τις ιδιότητες ενός δακτυλίου εκτός, ίσως, της μεταθετικότητας της πρόσθεσης, δηλαδή ενδέχεται να υπάρχουν $a, b \in R$ με

$$a + b \neq b + a.$$

Δείξτε ότι αυτό δεν μπορεί να συμβαίνει, δηλαδή η ιδιότητα

$$a + b = b + a,$$

για όλα τα $a, b \in R$, είναι απόρροια των υπολοίπων ιδιοτήτων και επομένως το σύνολο είναι όντως δακτύλιος.

7. Δείξτε ότι το σύνολο

$$R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

είναι υποδακτύλιος, με μονάδα, του σώματος $(\mathbb{R}, +, \cdot)$ των πραγματικών αριθμών. Μπορείτε να υπολογίσετε την πολλαπλασιαστική του ομάδα $U(R)$;

8. Στο σύνολο $\mathbb{Q}$ των ρητών αριθμών ορίζουμε μια πρόσθεση και έναν πολλαπλασιασμό ως εξής:

$$r \oplus s = r + s + 1 \text{ και } r \odot s = r \cdot s + r + s,$$

για όλα τα $r, s \in \mathbb{Q}$, όπου $+$, $\cdot$ είναι οι γνωστές πράξεις της πρόσθεσης και του πολλαπλασιασμού στους ρητούς αριθμούς.

Δείξτε ότι το σύνολο $(\mathbb{Q}, \oplus, \odot)$ είναι σώμα.

9. Στο Παράδειγμα 5.1.17$_{11}$ είχαμε δει ότι το σύνολο $\mathcal{F}(\mathbb{R})$ όλων των απεικονίσεων με πεδίο ορισμού και πεδίο τιμών το σύνολο των πραγματικών αριθμών είναι ομάδα με πράξη την πρόσθεση απεικονίσεων. Στο σύνολο αυτό ορίζουμε και έναν πολλαπλασιασμό ως εξής:

$$(f \cdot g)(x) = f(x) \cdot g(x),$$

για όλους τους πραγματικούς αριθμούς.

Δείξτε ότι το σύνολο $\mathcal{F}(\mathbb{R})$ εφοδιασμένο με τις πράξεις αυτές είναι ένας μεταθετικός δακτύλιος με μονάδα.

Μπορείτε να περιγράψετε τα αντιστρέψιμα στοιχεία αυτού του δακτυλίου;

Να βρεθούν δύο μη μηδενικά στοιχεία του δακτυλίου $\mathcal{F}(\mathbb{R})$, ώστε το γινόμενό τους να είναι ίσο με το μηδέν.

10. Στο Παράδειγμα 5.1.42$_2$ είχαμε ορίσει το καρτεσιανό γινόμενο δύο δακτυλίων R_1 και R_2.

    Δείξτε ότι ο δακτύλιος $R_1 \times R_2$ είναι μεταθετικός, αν και μόνο αν οι δακτύλιοι είναι μεταθετικοί.

    Δείξτε ότι τα σύνολα

    $$\bar{R}_1 = \{(r, 0) \mid r \in R_1\} \text{ και } \bar{R}_2 = \{(0, s) \mid s \in R_2\}$$

    είναι υποδακτύλιοι του $R_1 \times R_2$.

    Να βρεθούν δύο μη μηδενικά στοιχεία του δακτυλίου $R_1 \times R_2$, ώστε το γινόμενό τους να ισούται με το μηδέν (Υποτίθεται ότι οι δακτύλιοι είναι μη μηδενικοί).

    Υποτίθεται ότι οι δύο δακτύλιοι έχουν ουδέτερο ως προς τον πολλαπλασιασμό. Δείξτε ότι και ο δακτύλιος $R_1 \times R_2$ έχει ουδέτερο ως προς τον πολλαπλασιασμό. Μπορείτε να περιγράψετε τα αντιστρέψιμα στοιχεία του $R_1 \times R_2$;

11. Δίνεται ένας δακτύλιος R με την ιδιότητα $a^2 = a$, για όλα τα $a \in R$. Δείξτε ότι ο δακτύλιος είναι μεταθετικός (Ο δακτύλιος δεν υποτίθεται ότι έχει μοναδιαίο στοιχείο).

    Μπορείτε να απαντήσετε στο ίδιο ερώτημα, αν αντί του $a^2 = a$, για όλα τα $a \in R$, υποθέσουμε ότι $a^3 = a$, για όλα τα $a \in R$;

12. Έστω R ένας μεταθετικός δακτύλιος με μονάδα. Έστω $a, b \in R$, υποθέτουμε ότι το a είναι αντιστρέψιμο και ότι $b^2 = 0$. Δείξτε ότι το στοιχείο $a + b$ είναι αντιστρέψιμο.

    (Η απάντηση είναι $(a+b)^{-1} = a^{-1} - a^{-2}b$. Μπορείτε να εικάσετε πώς φθάσαμε σε αυτήν την απάντηση;)

13. Στην Άσκηση 3.2.11$_{18}$ είχαμε δει το διωνυμικό Θεώρημα για πραγματικούς αριθμούς. Αν παρατηρήσουμε την απόδειξη, πουθενά δεν αναφερόμαστε στην φύση των πραγματικών αριθμών. Επομένως μπορούμε να αποδείξουμε ότι το ίδιο αποτέλεσμα ισχύει σε κάθε μεταθετικό δακτύλιο. Δηλαδή σε έναν μεταθετικό δακτύλιο R ισχύει:

    $$(x + y)^n = \sum_{r=0}^{n} \binom{n}{r} x^{n-r} y^r,$$

    για όλα τα $n \in \mathbb{N}$ και όλα τα $x, y \in R$.

    Να επαναλάβετε την απόδειξη.

14. Ένα στοιχείο a ενός δακτυλίου R ονομάζεται **μηδενοδύναμο** αν $a^n = 0$, για κάποιον θετικό ακέραιο n.

    Έστω R ένας δακτύλιος με μονάδα. Αν το στοιχείο $a \in R$ είναι μηδενοδύναμο, δείξτε ότι τα στοιχεία $1 - a$ και $1 + a$ είναι αντιστρέψιμα.

    Αντίστροφα, αν το στοιχείο $1 - a$ είναι μηδενοδύναμο, τότε το στοιχείο a είναι αντιστρέψιμο.

    Υποθέτουμε ότι τα στοιχεία $1-a$, $1-b$ είναι μηδενοδύναμα και ότι $a \cdot b = b \cdot a$. Δείξτε ότι το στοιχείο $1 - ab$ είναι μηδενοδύναμο.

    Σε έναν μεταθετικό δακτύλιο δείξτε ότι το άθροισμα δύο μηδενοδυνάμων στοιχείων είναι μηδενοδύναμο στοιχείο.

15. Έστω ένας δακτύλιος R με την ιδιότητα:

$$\text{Υπάρχει } n > 1, \text{ ώστε } r^n = r, \text{ για όλα τα } r \in R.$$

Αν για το στοιχείο $a \in R$ ισχύει $a^m = 0$, για κάποιον θετικό ακέραιο, δείξτε ότι $a = 0$.

Επίσης, δείξτε ότι αν $a \cdot b = 0$, τότε και $b \cdot a = 0$.

Βιβλιογραφία

[1] E.D. Bloch. *Proofs and Fundamentals: A first course in Abstract Mathematics*. Second Edition. Springer, 2011. ISBN: 978-14-4197-126-5.

[2] Joseph A. Gallian. *Contemporary Abstract Algebra*. Seventh Edition. Brooks/Cole, 2009. ISBN: 978-05-4716-509-7.

[3] Charles C. Pinter. *A Book of Abstract Algebra*. Second Edition. Dover Dover Publications, Inc., Mineola, New York Originally published: 2nd ed. New York: McGraw-Hill, 1990. ISBN: 978-04-8647-417-5.

[4] Στυλιανός Ανδρεαδάκης. *Εισαγωγή στην Άλγεβρα*. Εκδόσεις Συμμετρία, 1993.

ΚΕΦΑΛΑΙΟ 6

Ο ΔΑΚΤΥΛΙΟΣ ΤΩΝ ΑΚΕΡΑΙΩΝ ΚΑΙ ΤΟ ΣΩΜΑ ΤΩΝ ΡΗΤΩΝ ΑΡΙΘΜΩΝ

Το σύνολο των ακεραίων αριθμών, με τις ιδιότητες που το διέπουν, το έχουμε συναντήσει (και *χρησιμοποιήσει*) από τα πρώτα βήματα στην ζωή μας (όχι, κατ' ανάγκη, της Μαθηματικής μας ζωής). Η προσέγγιση ήταν διαισθητική, αλλά αυτό δεν μας εμπόδιζε στην χρήση τους. Μάλιστα, πολλές φορές, τις ιδιότητες των ακεραίων αριθμών τις θεωρούσαμε ως κάτι το "*αυταπόδεικτο*" και *φυσιολογικό*.

Στα προηγούμενα κεφάλαια κάναμε χρήση, κατά κόρον, των ακεραίων αριθμών, βασιζόμενοι στην "εμπειρία μας" και την διαίσθησή μας, χωρίς ιδιαίτερα προβλήματα. Αυτό δεν σημαίνει ότι δεν είναι αναγκαίο να προσπαθήσουμε να ορίσουμε τους ακεραίους αριθμούς αυστηρώς Μαθηματικά.

Υπάρχουν πολλοί τρόποι για μια αξιωματική θεμελίωση των ακεραίων αριθμών.

Ένας τρόπος είναι να τους ορίσουμε αξιωματικά θέτοντας νέα αξιώματα.

Ένας άλλος τρόπος είναι να ορίσουμε αξιωματικά τους πραγματικούς αριθμούς και κατόπιν να θεωρήσουμε τους ακεραίους αριθμούς ως ένα "ειδικό" υποσύνολό τους.

Ένας τρίτος τρόπος είναι να χρησιμοποιήσουμε τους φυσικούς αριθμούς, τους οποίους μπορούμε να ορίσουμε ανεξάρτητα και αξιωματικά (Αξιώματα του Peano), και να τους "επεκτείνουμε" ορίζοντας τους ακεραίους αριθμούς.

Στο κεφάλαιο αυτό θα ακολουθήσουμε τον τρίτο τρόπο.

Στο Παράρτημα Α μελετώνται οι φυσικοί αριθμοί. Επομένως εδώ, θεωρώντας γνωστούς τους φυσικούς αριθμούς και με τις αναγκαίες αναφορές στο Παράρτημα Α, θα προσπαθήσουμε να κάνουμε μία πρώτη προσέγγιση των ακεραίων αριθμών.

6.1 Ο δακτύλιος των ακεραίων αριθμών

Το σύνολο των φυσικών αριθμών, εφοδιασμένο με τις πράξεις της πρόσθεσης και του πολλαπλασιασμού, καθώς και με την σχέση της διάταξης έχει πολλές καλές ιδιότητες. Παρ' όλα ταύτα, έχουμε παρατηρήσει ότι για την πρόσθεση φυσικών αριθμών δεν υπάρχει ουδέτερο.

Πράγματι, από την Πρόταση A.1.6 έπεται ότι για κάθε $a \in \mathbb{N}$ δεν υπάρχει $b \in \mathbb{N}$ με

$$a + b = b + a = a.$$

Επίσης, αφού δεν υπάρχει ουδέτερο ως προς την πρόσθεση, δεν μπορούμε να μιλάμε για την ύπαρξη αντιθέτου στοιχείου ως προς την πρόσθεση. Μάλιστα δε είχαμε δει (συνέπεια του Ορισμού A.1.7) ότι η διαφορά μεταξύ δύο φυσικών αριθμών δεν ορίζεται πάντοτε.

Ακόμη, ο πολλαπλασιασμός στους φυσικούς αριθμούς έχει ουδέτερο στοιχείο, το 1, αλλά κανένας φυσικός αριθμός, εκτός του 1, δεν έχει αντίστροφο στοιχείο.

Θέλουμε να κατασκευάσουμε ένα σύνολο, το οποίο να "περιέχει" το σύνολο των φυσικών αριθμών και να είναι εφοδιασμένο με μια πρόσθεση και έναν πολλαπλασιασμό. Ταυτόχρονα αυτές οι πράξεις να αποτελούν "επεκτάσεις" των αντιστοίχων πράξεων στους φυσικούς αριθμούς και να ικανοποιούν ιδιότητες, τις οποίες δεν ικανοποιούν οι αντίστοιχες πράξεις στους φυσικούς αριθμούς.

Επίσης, το σύνολο αυτό να είναι εφοδιασμένο με μια διάταξη, η οποία να επεκτείνει την διάταξη στους φυσικούς αριθμούς.

Η "κατασκευή" αυτή εδώ θα γίνει, όπως προείπαμε, βασιζόμενοι στους φυσικούς αριθμούς, οπότε θα έχουμε μια φυσιολογική επέκταση των φυσικών αριθμών και των ιδιοτήτων τους.

Διαισθητικά η κατασκευή στηρίζεται στην εξής παρατήρηση:

Επιλέγουμε και σταθεροποιούμε έναν φυσικό αριθμό k. Για κάθε φυσικό αριθμό a θέτουμε ως $a_k = a + k$. Παρατηρούμε ότι όλες οι διαφορές $a_k - a$ είναι ίσες για όλα τα $a \in \mathbb{N}$. Αυτό μας οδηγεί στον εξής ορισμό:

Ορισμός 6.1.1. Στο σύνολο $\mathbb{N} \times \mathbb{N}$ ορίζουμε μια σχέση $\sim$ ως εξής:

$$(a, b) \sim (c, d), \text{ αν } a + d = b + c.$$

Πρόταση 6.1.2. *Η σχέση $\sim$, στον προηγούμενο ορισμό, είναι μια σχέση ισοδυναμίας στο σύνολο $\mathbb{N} \times \mathbb{N}$.*

Απόδειξη. Η απόδειξη αποτελεί μια εύκολη άσκηση ελέγχου του ορισμού της σχέσης ισοδυναμίας. ό.έ.δ.

Για μια υπενθύμιση των σχετικών ορισμών της σχέσης ισοδυναμίας και των κλάσεων ισοδυναμίας, παραπέμπουμε στην Παράγραφο 4.4.1. Στα επόμενα θα αναφερόμαστε σε αποτελέσματα αυτής της παραγράφου χωρίς ιδιαίτερη μνεία.

Έστω $(a, b) \in \mathbb{N} \times \mathbb{N}$. Προς το παρόν, η κλάση ισοδυναμίας, στην οποία ανήκει το ζεύγος (a, b), θα συμβολίζεται με $[(a, b)]$, δηλαδή

$$[(a, b)] = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid a + y = b + x\}.$$

Ορισμός 6.1.3. Το σύνολο πηλίκων $\mathbb{N}\times\mathbb{N}/\sim$ των κλάσεων ισοδυναμίας θα ονομάζεται το σύνολο των **ακεραίων** αριθμών και θα συμβολίζεται με $\mathbb{Z}$.

Πριν προχωρήσουμε, στον ορισμό της πρόσθεσης, του πολλαπλασιασμού και της διάταξης στους ακεραίους αριθμούς θα κάνουμε την εξής παρατήρηση:

Παρατήρηση 6.1.4. Ως γνωστόν, για $a, b \in \mathbb{N}$, ισχύει ότι:

$$\text{είτε } a < b \text{ ή } a = b, \text{ ή } a > b$$

(Ο "νόμος της τριχοτομίας στους φυσικούς αριθμούς" Πρόταση A.1.8$_6$).

Επομένως, αν $a < b$, υπάρχει μοναδικό $k \in \mathbb{N}$, ώστε $b = a + k$. Όμοια, αν $a > b$, υπάρχει μοναδικό $k \in \mathbb{N}$, ώστε $a = b + k$.

Συνεπώς, άμεση απόρροια του ορισμού (γιατί;) είναι τα εξής:

- Όλα τα ζεύγη (a, a), για όλα τα $a \in \mathbb{N}$, είναι ισοδύναμα μεταξύ τους. Δηλαδή

$$[(a, a)] = \{(x, x) \in \mathbb{N} \times \mathbb{N}\}.$$

  Στην περίπτωση αυτή, η κλάση $[(a, a)]$ θα συμβολίζεται ως

$$0 = [(a, a)].$$

- Αν $a < b$ και $b = a + k$, τότε

$$[(a, b)] = \{(x, x + k) \in \mathbb{N} \times \mathbb{N} \mid x \in \mathbb{N}\}.$$

  Στην περίπτωση αυτή, η κλάση $[(a, b)] = [(x, x + k)]$ θα συμβολίζεται ως

$$-k = [(x, x + k)].$$

- Αν $a > b$ και $a = b + k$, τότε

$$[(a, b)] = \{(x + k, x) \in \mathbb{N} \times \mathbb{N} \mid x \in \mathbb{N}\}.$$

  Στην περίπτωση αυτή, η κλάση $[(a, b)] = [(x + k, x)]$ θα συμβολίζεται ως

$$+k = [(x + k, x)].$$

Στην ειδική περίπτωση, όπου $[(a, b)] = [(x + 1, x)]$, έχουμε

$$+1 = [(x + 1, x)].$$

Επίσης, αν $[(a, b)] \in \mathbb{Z}$, τότε ορίζουμε τον **αντίθετο**

$$-[(a, b)] = [(b, a)].$$

Στο σύνολο $\mathbb{Z}$ των ακεραίων αριθμών ορίζουμε δύο πράξεις.

Μια πρόσθεση $+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ ως εξής:

$$[(a, b)] + [(c, d)] = [(a + c, b + d)],$$

για όλα τα $[(a, b)], [(c, d)] \in \mathbb{Z}$.

Έναν πολλαπλασιασμό $\cdot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ ως εξής:

$$[(a, b)] \cdot [(c, d)] = [(ac + bd, ad + bc)],$$

για όλα τα $[(a, b)], [(c, d)] \in \mathbb{Z}$.

Στο σύνολο $\mathbb{Z}$ των ακεραίων αριθμών ορίζουμε μια σχέση $<$ ως εξής:

$$[(a, b)] < [(c, d)], \text{ αν } a + d < b + c,$$

για όλα τα $[(a, b)], [(c, d)] \in \mathbb{Z}$.

Οπότε, μπορούμε να ορίσουμε και μια άλλη σχέση $\leq$ ως εξής:

$$[(a, b)] \leq [(c, d)], \text{ αν } [(a, b)] < [(c, d)] \text{ ή } [(a, b)] = [(c, d)]$$

για όλα τα $[(a, b)], [(c, d)] \in \mathbb{Z}$.

Πριν προχωρήσουμε, πρέπει να παρατηρήσουμε ότι:

Οι πράξεις και οι σχέσεις, που ορίσαμε στο σύνολο των ακεραίων, ορίστηκαν με την βοήθεια των ήδη ορισμένων πράξεων και σχέσεων στους φυσικούς αριθμούς.

Επίσης, χρησιμοποιούμε τον ίδιο συμβολισμό. Αυτό δεν (πρέπει να) προκαλεί σύγχυση.

Επισημαίνουμε ότι (προς το παρόν) δεν έχει νόημα, για παράδειγμα, να προσθέσουμε έναν ακέραιο $[(a, b)]$ με έναν φυσικό αριθμό n, καθ' ότι πρόκειται για δύο διαφορετικά σύνολα. Το πρόβλημα αυτό αίρεται, όταν δούμε υπό ποίον τρόπο το σύνολο των φυσικών αριθμών "περιέχεται" στο σύνολο των ακεραίων αριθμών.

Επειδή το σύνολο των ακεραίων αποτελείται από κλάσεις ισοδυναμίας, οι πράξεις και οι σχέσεις, τις οποίες ορίσαμε, πρέπει να ελεγχθούν ότι είναι "καλώς ορισμένες", δηλαδή δεν εξαρτώνται από την επιλογή των αντιπροσώπων, αλλά από τις κλάσεις αυτές καθ' εαυτές.

Πρόταση 6.1.5. *Οι πράξεις της πρόσθεσης και του πολλαπλασιασμού, καθώς και η σχέση $<$ στο σύνολο των ακεραίων αριθμών είναι καλώς ορισμένες.*

Απόδειξη. Θα αποδείξουμε ότι η πράξη του πολλαπλασιασμού είναι καλώς ορισμένη, αφήνοντας τα υπόλοιπα ως άσκηση.

Έστω $(a, b), (c, d), (x, y), (z, w) \in \mathbb{N} \times \mathbb{N}$. Υποθέτουμε ότι

$$[(a, b)] = [(x, y)] \text{ και } [(c, d)] = [(z, w)].$$

Θα δείξουμε ότι

$$[(a, b)] \cdot [(c, d)] = [(x, y)] \cdot [(z, w)].$$

Από τον ορισμό του πολλαπλασιασμού και τον ορισμό των κλάσεων ισοδυναμίας η προς απόδειξη ισότητα γίνεται:

$$ac + bd + xw + yz = ad + bc + xz + yw.$$

Η ισότητα αυτή (η οποία πρέπει να επαληθευθεί) είναι μια ισότητα μεταξύ φυσικών αριθμών.

Η υπόθεση $[(a, b)] = [(x, y)]$ και $[(c, d)] = [(z, w)]$, σημαίνει ότι

$$a + y = b + x \tag{1}$$

και

$$c + w = d + z \tag{2}$$

Πολλαπλασιάζοντας και τα δύο μέλη της (1) με το c έχουμε

$$ac + yc = bc + xc \tag{i}$$

Πολλαπλασιάζοντας και τα δύο μέλη της (1) με το d (και αναστρέφοντας την σειρά των δύο όρων) έχουμε

$$bd + xd = ad + yd \tag{ii}$$

Πολλαπλασιάζοντας και τα δύο μέλη της (2) με το x έχουμε

$$cx + wx = dx + zx \tag{iii}$$

Πολλαπλασιάζοντας και τα δύο μέλη της (2) με το y (και αναστρέφοντας την σειρά των δύο όρων) έχουμε

$$dy + zy = cy + wy \tag{iv}$$

Προσθέτοντας τις (i), (ii), (iii), (iv) κατά μέλη και κάνοντας τις διαγραφές ομοίων όρων καταλήγουμε στην προς απόδειξη ισότητα

$$ac + bd + xw + yz = ad + bc + xz + yw.$$

Επισημαίνουμε ότι τα επιχειρήματα που επικαλεσθήκαμε ισχύουν, δεδομένου ότι ισχύει η Πρόταση A.1.6. ό.έ.δ.

Στο επόμενο Θεώρημα περιλαμβάνονται οι κυριότερες ιδιότητες των ακεραίων αριθμών.

Θεώρημα 6.1.6. *Έστω $x, y, z \in \mathbb{Z}$, τότε ισχύουν τα ακόλουθα:*

1. $(x + y) + z = x + (y + z)$ *(Η προσεταιριστική ιδιότητα της πρόσθεσης στους ακεραίους).*
2. $x + y = y + x$ *(Η πρόσθεση των ακεραίων είναι μεταθετική).*
3. $x + 0 = x$ *(Η πρόσθεση έχει ουδέτερο).*
4. $x + (-x) = 0$ *(Κάθε ακέραιος αριθμός έχει αντίθετο ως προς την πρόσθεση).*
5. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ *(Η προσεταιριστική ιδιότητα του πολλαπλασιασμού στους ακεραίους).*
6. $x \cdot y = y \cdot x$ *(Ο πολλαπλασιασμός των ακεραίων είναι μεταθετικός).*
7. $x \cdot (+1) = x$ *(Ο πολλαπλασιασμός έχει ουδέτερο).*
8. $x \cdot (y + z) = x \cdot y + x \cdot z$ *(Η επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση στους ακεραίους).*
9. *Αν $xy = 0$, τότε $x = 0$ ή $y = 0$ (Στους ακεραίους αριθμούς δεν υπάρχουν μηδενοδιαιρέτες)* [1].
10. *Ισχύει ακριβώς μια από τις σχέσεις $x < y, x = y, x > y$ (Ο νόμος της τριχοτομίας στους ακεραίους).*
11. *Αν $x < y$ και $y < z$, τότε $x < z$ (Η μεταβατική ιδιότητα της διάταξης στους ακεραίους).*

[1] Για τον ορισμό του μηδενοδιαιρέτη και παραδείγματα δακτυλίων με μηδενοδιαιρέτες παραπέμπουμε στο Παράρτημα Γ (Παρατήρηση Γ.2.6)

12. *Αν* $x \leq y$ *και* $y \leq x$, *τότε* $x = y$

13. *Αν* $x < y$, *τότε* $x + z < y + z$.

14. *Αν* $x < y$ *και* $z > 0$, *τότε* $xz < yz$.

15. $0 \neq +1$ *(Το σύνολο των ακεραίων έχει τουλάχιστον δύο στοιχεία).*

Απόδειξη. Η απόδειξη όλων των ανωτέρω στηρίζεται στον ορισμό των ακεραίων μέσω των φυσικών αριθμών. Οπότε, όπως στην προηγουμένη πρόταση, "μεταβαίνουμε" στους φυσικούς αριθμούς και επικαλούμαστε τις Προτάσεις A.1.6 και A.1.8.

Εδώ θα αποδείξουμε μόνο τις (3), (8), (9) και (11) αφήνοντας τις υπόλοιπες ως άσκηση.

Υποθέτουμε ότι $x = [(a, b)]$, $y = [(c, d)]$ και $z = [(e, f)]$ με $a, b, c, d, e, f \in \mathbb{N}$.

(3). Από τον ορισμό του 0 (ιδέ Παρατήρηση 6.1.4) έχουμε $0 = [(r, r)]$, για (οποιοδήποτε) $r \in \mathbb{N}$. Επομένως,

$$x + 0 = [(a, b)] + [(r, r)] = [(a + r, b + r)],$$

από τον ορισμό της πρόσθεσης. Αλλά, από τον ορισμό της σχέσης ισοδυναμίας, έχουμε ότι

$$[(a + r, b + r)] = [(a, b)] \text{ (γιατί;)}.$$

Συνεπώς,

$$x + 0 = [(a, b)] + [(r, r)] = [(a + r, b + r)] = [(a, b)] = x.$$

(8). Έχουμε

$$\begin{aligned} x(y + z) &= [(a, b)] \cdot ([(c, d)] + [(e, f)]) \\ &= [(a, b)] \cdot [(c + e, d + f)] \\ &= [(a(c + e) + b(d + f), a(d + f) + b(c + e))] \qquad (*) \end{aligned}$$

Επίσης

$$\begin{aligned} xy + xz &= [(a, b)] \cdot [(c, d)] + [(a, b)] \cdot [(e, f)] \\ &= [(ac + bd, ad + bc)] + [(ae + bf, af + be)] \\ &= [(ac + ae + bd + bf, ad + af + bc + be)] \\ &= [(a(c + e) + b(d + f), a(d + f) + b(c + e))] \qquad (**) \end{aligned}$$

Από τις $(*)$ και $(**)$ έπεται ότι $x(y + z) = xy + xz$.

(9). Υποθέτουμε ότι $xy = 0$ και ότι $x \neq 0$. Από την ισότητα $xy = 0$ έχουμε

$$[(a, b)] \cdot [(c, d)] = [(ac + bd, ad + bc)] = 0,$$

δηλαδή

$$ac + bd = ad + bc.$$

Από την σχέση $x \neq 0$ έχουμε ότι $a \neq b$. Οπότε, $a < b$ ή $a > b$ (γιατί; δεν ξεχνάμε τον νόμο της τριχοτομίας στους φυσικούς αριθμούς). Υποθέτουμε ότι $a < b$ (όμοια ενεργούμε, αν $a > b$), άρα $b = a + k$ με $k \in \mathbb{N}$.

Επομένως, από την σχέση $ac + bd = ad + bc$ έχουμε

$$ac + (a + k)d = ad + (a + k)c,$$

δηλαδή

$$ac + ad + kd = ad + ac + kc,$$

οπότε έχουμε ότι $d = c$. Άρα

$$y = [(c, d)] = 0.$$

(11). Υποθέτουμε $x < y$ και $y < z$. Δηλαδή

$$[(a, b)] < [(c, d)] \text{ και } [(c, d)] < [(e, f)].$$

Αυτό σημαίνει

$$a + d < b + c \text{ και } c + f < d + e.$$

Οι ανισώσεις αυτές είναι μεταξύ φυσικών αριθμών. Οπότε, από την Πρόταση A.1.8 εύκολα έπεται ότι $a + f < b + e$, δηλαδή

$$x = [(a, b)] < [(e, f)] = z.$$

ό.έ.δ.

Παρατηρήσεις 6.1.7.

1. Από τον νόμο της τριχοτομίας των ακεραίων αριθμών έχουμε τρεις κατηγορίες ακεραίων αριθμών. Αυτούς που είναι μικρότεροι από το μηδέν, αυτούς που είναι μεγαλύτεροι από το μηδέν και το μηδέν.

   Έστω ο ακέραιος $x = [(a, b)]$ με $a < b$, τότε, από το προηγούμενο Θεώρημα, έπεται ότι $x < 0$. Προφανώς ισχύει και το αντίστροφο. Αν $x = [(a, b)] < 0$, τότε $a < b$. Όμοια έπεται ότι $x = [(a, b)] > 0$, αν και μόνο αν με $a > b$.

   Έστω $x = [(a, b)] < 0$ με $b = a + k$. Στην Παρατήρηση 6.1.4 είχαμε συμβολίσει αυτόν τον ακέραιο με $-k$. Όμοια, αν $x = [(a, b)] > 0$ με $a = b + k$, τον είχαμε συμβολίσει με $+k$.

   Επομένως, έχουμε την γνωστή παράσταση των ακεραίων αριθμών

   $$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, +1, +2, +3, \ldots\}.$$

   Τους ακεραίους τους μικρότερους του μηδενός τους ονομάζουμε *αρνητικούς* (με αρνητικό πρόσημο) και τους ακεραίους τους μεγαλύτερους του μηδενός τους ονομάζουμε *θετικούς* (με θετικό πρόσημο). Στο μηδέν δεν προσάπτουμε πρόσημο.

2. Από τα προηγούμενα έπεται ότι η σχέση $\leq$ στους ακεραίους αριθμούς είναι σχέση ολικής διάταξης.

3. Στο Πέμπτο κεφάλαιο (σελ. 211) είχαμε αναφέρει, ως παράδειγμα, ότι το σύνολο των ακεραίων $(\mathbb{Z}, +, \cdot)$, εφοδιασμένο με τις πράξεις της πρόσθεσης και του πολλαπλασιασμού, είναι ένας μεταθετικός δακτύλιος με μονάδα. Εδώ αποδείξαμε ότι πράγματι αυτό ισχύει.

4. Η ιδιότητα (15) στο προηγούμενο θεώρημα, εκτός από προφανής, φαντάζει περιττή,...έχει όμως την σημασία της (ιδέ Σχόλια 5.1.40).

Στην επομένη πρόταση αποδεικνύεται πώς το σύνολο των φυσικών αριθμών εμφυτεύεται στο σύνολο των ακεραίων αριθμών, το οποίο "*συμφωνεί*" με την διαίσθησή μας.

Πρόταση 6.1.8. *Ορίζουμε την απεικόνιση* $i : \mathbb{N} \longrightarrow \mathbb{Z}$ *με*

$$i(n) = [(n+1, 1)],$$

για όλα τα $n \in \mathbb{N}$.

1. *Η* i *είναι 1-1.*
2. $i(\mathbb{N}) = \{x \in \mathbb{Z} \mid x > 0\}$.
3. $i(1) = +1$.
4. *(α)* $i(n+m) = i(n) + i(m)$, *για όλα τα* $n, m \in \mathbb{N}$.
   (β) $i(n \cdot m) = i(n) \cdot i(m)$, *για όλα τα* $n, m \in \mathbb{N}$.
   (γ) $n < m$, *αν και μόνο αν* $i(n) < i(m)$.

Απόδειξη. Η απόδειξη είναι εύκολη και στηρίζεται στον ορισμό των ακεραίων αριθμών και των πράξεων της πρόσθεσης και του πολλαπλασιασμού.

Θα αποδείξουμε την (2) και τις (4_α) και (4_γ) αφήνοντας τις υπόλοιπες ως άσκηση.

(2) Από τον τρόπο ορισμού της απεικόνισης i έπεται ότι

$$i(\mathbb{N}) \subseteq \{x \in \mathbb{Z} \mid x > 0\} \text{ (γιατί;)}.$$

Έστω $x \in \mathbb{Z}$ με $x > 0$, τότε $x = [(a, b)]$ με $a > b$, δηλαδή υπάρχει $k \in \mathbb{N}$ με $a = b+k$.

Προφανώς

$$x = [(a, b)] = [(b+k, b)] = [(k+1, 1)]$$

(γιατί ισχύει η τελευταία ισότητα;). Επομένως, $x = i(k)$ και κατά συνέπεια

$$\{x \in \mathbb{Z} \mid x > 0\} \subseteq i(\mathbb{N}).$$

(4_α) Έστω $n, m \in \mathbb{N}$. Τότε έχουμε

$$\begin{aligned} i(n) + i(m) &= [(n+1, 1)] + [(m+1, 1)] \\ &= [((n+1) + (m+1), 1+1)] \\ &= [(((n+m)+1)+1)), 1+1)] \\ &= [((n+m)+1, 1)] \\ &= i(n+m). \end{aligned}$$

(4_γ) Έστω $n, m \in \mathbb{N}$ με $n < m$, τότε υπάρχει $k \in \mathbb{N}$ με $n + k = m$. Επομένως,

$$i(n) = [(n+1, 1)] < [(n+k+1, 1)] = [(m+1, 1)] = i(m).$$

Αντίστροφα, υποθέτουμε ότι $i(n) < i(m)$. Δηλαδή

$$[(n+1, 1)] < [(m+1, 1)],$$

άρα

$$(n+1) + 1 < (m+1) + 1.$$

Από την τελευταία ανισότητα έπεται ότι $n < m$. ό.έ.δ.

Σύμφωνα με τον συμβολισμό της προηγουμένης παρατήρησης, μπορούμε να γράψουμε

$$i(n) = +n.$$

Η ταυτοποίηση των φυσικών αριθμών με τους θετικούς ακεραίους, μέσω της απεικόνισης i μας επιτρέπει να θεωρούμε το σύνολο των φυσικών αριθμών ως υποσύνολο των ακεραίων. Μάλιστα δε, τις περισσότερες φορές, μέσω της ταυτοποίησης αυτής, γράφουμε $k \equiv +k$ (παραλείπουμε το πρόσημο +).

Μερικές ακόμη, αξιοσημείωτες ιδιότητες, των ακεραίων αριθμών περιλαμβάνονται στην επομένη πρόταση.

Πρόταση 6.1.9. *Έστω $x, y, z \in \mathbb{Z}$, τότε ισχύουν τα ακόλουθα:*

1. *Αν $x + z = y + z$, τότε $x = y$ (ο νόμος της διαγραφής στην πρόσθεση).*
2. $-(-x) = x$.
3. $-(x + y) = (-x) + (-y)$.
4. $(-x)y = -(xy) = x(-y)$.
5. $x \cdot 0 = 0$.
6. *Αν $z \neq 0$ και $xz = yz$, τότε $x = y$ (ο νόμος διαγραφής στον πολλαπλασιασμό).*
7. $xy = 1$, *αν και μόνο αν* $x = y = 1$ *ή* $x = y = -1$.
8. $x > 0$, *αν και μόνο αν* $-x < 0$ *και* $x < 0$, *αν και μόνο αν* $-x > 0$.
9. $0 < 1$.
10. *Αν, $x > 0$ και $y > 0$, τότε $xy > 0$. Αν, $x > 0$ και $y < 0$, τότε $xy < 0$. Αν, $x < 0$ και $y < 0$, τότε $xy > 0$ (ο κανόνας των προσήμων).*

Απόδειξη. Η απόδειξη των ανωτέρω είναι εύκολη. Πολλές από τις ιδιότητες αυτές απορρέουν από τις ιδιότητες που έχουν αποδειχθεί στο Θεώρημα 6.1.6.

Επισημαίνουμε όμως ότι πολλές από τις ανωτέρω ιδιότητες, για παράδειγμα οι (1), (2), (3), (4) και (5), απορρέουν από τις γενικές ιδιότητες των δακτυλίων (ιδέ Πρόταση 5.1.39).

Εδώ θα αποδείξουμε μόνο την (6) αφήνοντας τις υπόλοιπες ως άσκηση.

Υποθέτουμε ότι

$$z \neq 0 \text{ και } xz = yz.$$

Από την σχέση αυτή έχουμε

$$xz - yz = yz - yz = 0.$$

Από την επιμεριστική ιδιότητα έπεται ότι

$$(x - y)z = 0.$$

Το z έχει υποτεθεί διάφορο του μηδενός και στους ακεραίους δεν υπάρχουν μηδενοδιαιρέτες, συνεπώς $x - y = 0$, δηλαδή $x = y$. ό.έ.δ.

Είχαμε αποδείξει ότι οι φυσικοί αριθμοί είναι διακριτοί, δηλαδή, για κάθε $a \in \mathbb{N}$ δεν υπάρχει $b \in \mathbb{N}$ με $a < b < a + 1$ (ιδέ Πρόταση A.1.8$_9$). Παρόμοιο αποτέλεσμα ισχύει και για τους ακεραίους αριθμούς.

Πρόταση 6.1.10. *Έστω $x \in \mathbb{Z}$. Δεν υπάρχει $y \in \mathbb{Z}$ με*

$$x < y < x + 1.$$

Απόδειξη. Έστω $x = [(a, b)]$ με $a, b \in \mathbb{N}$, τότε

$$x + 1 = [(a + 1, b)] \text{ (γιατί;)}.$$

Υποθέτουμε ότι υπάρχει $y = [(c, d)] \in \mathbb{Z}$ με $x < y < x + 1$. Τότε έχουμε, αφ' ενός μεν

$$[(a, b)] < [(c, d)],$$

αφ' ετέρου δε

$$[(c, d)] < [(a + 1, b)].$$

Από τον ορισμό της ανισότητας στους ακεραίους, θα πρέπει να έχουμε ταυτοχρόνως

$$a + d < b + c \text{ και } c + b < (a + 1) + d.$$

Δηλαδή,

$$a + d < b + c < (a + 1) + d,$$

άτοπο. Διότι οι αριθμοί $n = a + d$ και $m = b + c$ είναι φυσικοί αριθμοί, για τους οποίους δεν μπορεί να ισχύει $n < m < n+1$ (Πρόταση A.1.8$_9$). Συνεπώς, δεν υπάρχουν $x, y \in \mathbb{Z}$ με $x < y < x + 1$. ό.έ.δ.

Παρατήρηση 6.1.11. Η ιδιότητα των ακεραίων, που αποδείξαμε στην προηγουμένη πρόταση, δεν απορρέει από ιδιότητες των ακεραίων, οι οποίες έχουν αποδειχθεί προηγουμένως (π.χ. το Θεώρημα 6.1.6 και η Πρόταση 6.1.9). Όπως θα δούμε, όλες οι ιδιότητες που αναφέρονται στο Θεώρημα 6.1.6 και την Πρόταση 6.1.9 (εκτός από την (7) στην Πρόταση 6.1.9), ισχύουν και για τους ρητούς αριθμούς, παρ' όλα ταύτα, οι ρητοί αριθμοί δεν είναι διακριτοί.

Είχαμε δει (Θεώρημα A.1.10) ότι το σύνολο των φυσικών αριθμών είναι ένα καλώς διατεταγμένο σύνολο. Κάτι ανάλογο δεν ισχύει για το σύνολο των ακεραίων αριθμών.

Για παράδειγμα, το υποσύνολο των αρνητικών αριθμών δεν έχει ελάχιστο στοιχείο (γιατί;).

Παρ' όλα ταύτα, ισχύει ένα ανάλογο αποτέλεσμα με το Θεώρημα A.1.10.

Πρόταση 6.1.12. *Έστω S ένα μη κενό υποσύνολο των ακεραίων αριθμών. Υποθέτουμε ότι υπάρχει $r \in \mathbb{Z}$ με $r \leq s$, για όλα τα $s \in S$, τότε υπάρχει $m \in S$ με $m \leq s$, για όλα τα $s \in S$.*

Δηλαδή, κάθε κάτω φραγμένο υποσύνολο των ακεραίων αριθμών έχει ελάχιστο στοιχείο.

Απόδειξη. Η απόδειξη αυτή αποτελεί "προσαρμογή" της απόδειξης του Θεωρήματος A.1.10. Αρκεί να επικαλεσθούμε την Άσκηση A.1.1$_9$, και αφήνεται ως άσκηση. ό.έ.δ.

Παρατήρηση 6.1.13. Όπως αναφέραμε και στην αρχή του κεφαλαίου, οι ακέραιοι αριθμοί θα μπορούσαν να ορισθούν αξιωματικά. Οπότε, αποδεικνύεται ότι οι φυσικοί αριθμοί, ως ένα ειδικό υποσύνολο των ακεραίων, ικανοποιούν τα αξιώματα Peano.

Για μια τέτοια προσέγγιση παραπέμπουμε στο [1] (Section 1.4).

6.1.1 Ασκήσεις

1. Να αποδείξετε, με κάθε λεπτομέρεια, την Πρόταση 6.1.2.
2. Να ολοκληρώσετε την απόδειξη της Πρότασης 6.1.5.
3. Να ολοκληρώσετε την απόδειξη του Θεωρήματος 6.1.6.
4. Να ολοκληρώσετε την απόδειξη της Πρότασης 6.1.8.
5. Να ολοκληρώσετε την απόδειξη της Πρότασης 6.1.9.
6. Να ολοκληρώσετε την απόδειξη της Πρότασης 6.1.12.
7. Αποδείξτε την δυϊκή Πρόταση της Πρότασης 6.1.12.
   "Κάθε άνω φραγμένο υποσύνολο των ακεραίων αριθμών έχει μέγιστο στοιχείο."
8. Ορίζουμε την εξής απεικόνιση $j : \mathbb{N} \longrightarrow \mathbb{Z}$ με $j(n) = -n$, για όλα τα $n \in \mathbb{N}$.
   Προφανώς (;) η j είναι 1-1.
   Γιατί, για την απεικόνιση j, δεν ισχύουν ιδιότητες ανάλογες με τις ιδιότητες, που ισχύουν για την απεικόνιση i της Πρότασης 6.1.8;
9. Έστω $r, s, b \in \mathbb{Z}$ με $0 \leq r < b$ και $0 \leq s < b$. Δείξτε ότι $r - s < b$.

6.1.2 Η διαιρετότητα στους ακεραίους

Στο Θεώρημα 6.1.6 είδαμε τις κυριότερες ιδιότητες των ακεραίων αριθμών, οι οποίες σχετίζονται με τις πράξεις της πρόσθεσης και του πολλαπλασιασμού και με την σχέση της διάταξης. Στην παράγραφο αυτή θα δούμε πώς η πρόσθεση, ο πολλαπλασιασμός και η διάταξη "*συνδέονται*" μεταξύ τους.

Ας ξεκινήσουμε με έναν ορισμό.

Ορισμός 6.1.14. Έστω a, b δύο ακέραιοι αριθμοί. Ο ακέραιος αριθμός b **διαιρεί** τον ακέραιο αριθμό a, αν υπάρχει ακέραιος αριθμός k, ώστε $a = kb$. Στην περίπτωση αυτή θα συμβολίζουμε με $b \mid a$.

Ισοδύναμες εκφράσεις, που χρησιμοποιούμε είναι: Ο a **διαιρείται** από τον b ή ο a είναι **πολλαπλάσιο** του b.

Προφανώς, αν $b \neq 0$, ο ακέραιος k στην ισότητα $a = kb$ είναι μοναδικός (γιατί;) και θα συμβολίζεται ως a/b.

Πριν προχωρήσουμε, ας ορίσουμε την **απόλυτη** τιμή ενός ακεραίου αριθμού.

Έστω $a \in \mathbb{Z}$, τότε ορίζουμε

$$| a | = \begin{cases} a & \text{αν } a > 0 \\ -a & \text{αν } a < 0 \\ 0 & \text{αν } a = 0 \end{cases}$$ [2]

Ακολουθούν ορισμένες προφανείς παρατηρήσεις, τις οποίες οφείλουμε να επιβεβαιώσουμε ότι πράγματι ισχύουν (επικαλούμενοι το Θεώρημα 6.1.6 και την Πρόταση 6.1.9).

[2] Ισχύουν ορισμένες (προφανείς) ιδιότητες της απόλυτης τιμής, ιδέ την Πρόταση 7.1.31, όπου αναφερόμαστε στην απόλυτη τιμή ενός πραγματικού αριθμού, φυσικά στην περίπτωση των ακεραίων αριθμών οι ιδιότητες αυτές αποδεικνύονται ευκολότερα.

Παρατηρήσεις 6.1.15.

1. Αν ο ακέραιος αριθμός b διαιρεί τον ακέραιο αριθμό a, τότε ισχύει ότι ο b διαιρεί τον $-a$ και ο $-b$ διαιρεί τους a και $-a$.

2. Το 1 και το -1 διαιρεί κάθε ακέραιο αριθμό a.

3. Το 0 διαιρείται από κάθε ακέραιο αριθμό a.

4. Το 0 διαιρεί μόνο το 0.

5. Έστω a, b, c ακέραιοι αριθμοί. Αν ο a διαιρεί τους b και c, τότε ο a, για όλα τα $m, n \in \mathbb{Z}$, διαιρεί τον αριθμό $mb + nc$.

6. Αν ο ακέραιος a διαιρεί τον ακέραιο b και ο b διαιρεί τον ακέραιο c, τότε ο a διαιρεί τον c.

7. Αν ο ακέραιος a διαιρεί τον ακέραιο b και ο ακέραιος b διαιρεί τον ακέραιο a, τότε $a = b$ ή $a = -b$.

8. Αν ο ακέραιος a διαιρεί τον μη μηδενικό ακέραιο b, τότε $\mid a \mid \leq \mid b \mid$.

Στα επόμενα θα χρησιμοποιούμε τις παρατηρήσεις αυτές, χωρίς να αναφερόμαστε ρητά σε αυτές.

Ο μέγιστος κοινός διαιρέτης ακεραίων αριθμών.

Έστω $a_1, a_2, \ldots, a_n$ ακέραιοι αριθμοί, οι οποίοι δεν είναι όλοι μηδέν. Ένας ακέραιος αριθμός δ, ο οποίος διαιρεί κάθε έναν από τους a_i, $i = 1, 2, \ldots, n$, θα ονομάζεται **κοινός διαιρέτης** των a_i, $i = 1, 2, \ldots, n$.

Προφανώς υπάρχουν θετικοί κοινοί διαιρέτες των a_i, $i = 1, 2, \ldots, n$. Για παράδειγμα, το 1 είναι ένας θετικός κοινός διαιρέτης.

Επίσης, αν δ είναι ένας θετικός κοινός διαιρέτης των a_i, τότε ισχύει

$$\delta \leq \mid a_i \mid$$

για τουλάχιστον ένα από τα $i = 1, 2, \ldots, n$ (στην πραγματικότητα για όλα τα $a_i \neq 0$ γιατί;). [3]

Επομένως, αν S είναι το σύνολο όλων των θετικών κοινών διαιρετών των a_i, $i = 1, 2, \ldots, n$, αυτό είναι αφ' ενός μη κενό, αφ' ετέρου είναι άνω φραγμένο. Συνεπώς, έχει μέγιστο στοιχείο (γιατί;) (Δεν ξεχνάμε την Πρόταση 6.1.12 και την Άσκηση $6.1.1_7$), το οποίο είναι μοναδικό.

Ορισμός 6.1.16. $a_1, a_2, \ldots, a_n$ ακέραιοι αριθμοί, οι οποίοι δεν είναι όλοι μηδέν. Υπάρχει ο **μέγιστος κοινός διαιρέτης** των a_i, $i = 1, 2, \ldots, n$ και θα συμβολίζεται

$$\mu.κ.δ(a_1, a_2, \ldots, a_n) \text{ ή απλά } (a_1, a_2, \ldots, a_n).$$

Στην περίπτωση, όπου

$$\mu.κ.δ(a_1, a_2, \ldots, a_n) = 1,$$

οι αριθμοί a_i, $i = 1, 2, \ldots, n$ θα ονομάζονται σχετικά πρώτοι ή πρώτοι μεταξύ τους.

[3] Αυτό το γιατί απαντά, στην πιθανή απορία μας, γιατί εξ' ορισμού υποθέτουμε ότι οι ακέραιοι a_i δεν είναι όλοι ίσοι με το μηδέν.

Παράδειγμα 6.1.17. Προφανώς μ.κ.δ$(12, -18) = 6$ και μ.κ.δ$(8, 15) = 1$.

Θα παραθέσουμε μερικές ιδιότητες του μέγιστου κοινού διαιρέτη ακεραίων αριθμών.

Πρόταση 6.1.18. *Έστω a, b ακέραιοι αριθμοί, οι οποίοι δεν είναι και οι δύο ίσοι με το μηδέν. Τότε ισχύουν τα εξής:*

1. *Αν ο $a \mid b$, τότε μ.κ.δ$(a, b) = \mid a \mid$.*
2. *μ.κ.δ(a, b)=μ.κ.δ$(\mid a \mid, \mid b \mid)$.*
3. *Έστω $d =$μ.κ.δ(a, b), τότε ισχύει ότι*

$$\mu.\kappa.\delta(a/d, b/d) = 1.$$

4. *μ.κ.δ$(a, b) =$μ.κ.δ$(a + kb, b)$, για όλους τους ακεραίους αριθμούς k.*

Απόδειξη. Οι (1) (2) είναι προφανείς και αφήνονται ως άσκηση.

Θα θέλαμε όμως να επισημάνουμε ότι, βάσει αυτών των ιδιοτήτων, μπορούμε να υποθέτουμε, χωρίς βλάβη της γενικότητας, ότι οι ακέραιοι αριθμοί, για τον μ.κ.δ των οποίων ενδιαφερόμαστε, είναι όλοι μη μηδενικοί και θετικοί (δεν ξεχνάμε ότι το μηδέν διαιρείται από όλους τους ακεραίους αριθμούς).

(3) Θέτουμε

$$\delta = \mu.\kappa.\delta(a/d, b/d).$$

Έστω $a = rd$ και $b = sd$, με $r, s \in \mathbb{Z}$. Τότε

$$\delta = \mu.\kappa.\delta(a/d, b/d) = \mu.\kappa.\delta(r, s).$$

Συνεπώς, $r = t\delta$ και $s = u\delta$ με $t, u \in \mathbb{Z}$. τότε όμως θα ισχύει ότι

$$a = rd = t\delta d \text{ και } b = sd = u\delta d.$$

Αν υποθέσουμε ότι ο $\delta = \mu.\kappa.\delta(a/d, b/d)$ είναι διάφορος του 1, τότε ο ακέραιος αριθμός δd αφ' ενός είναι γνήσια μεγαλύτερος του d, αφ' ετέρου είναι ένας κοινός διαιρέτης των a και b, άτοπο. Επομένως, αναγκαστικά

$$\delta = \mu.\kappa.\delta(a/d, b/d) = 1.$$

(4) Θέτουμε

$$d = \mu.\kappa.\delta(a, b) \text{ και } \delta = \mu.\kappa.\delta(a + kb, b),\ k \in \mathbb{Z}.$$

Παρατηρούμε ότι ο d είναι ένας κοινός διαιρέτης των $a + kb$ και b (ιδέ Παρατήρηση $6.1.15_5$). Επομένως

$$d \leq \delta.$$

Επίσης, ο δ ως κοινός διαιρέτης των $a + kb$ και b, είναι κοινός διαιρέτης και του $(a + kb) - kb = a$ (πάλι από την Παρατήρηση $6.1.15_5$). Επομένως

$$\delta \leq d.$$

Άρα $\delta = d$ ό.έ.δ.

Πριν προχωρήσουμε, θα θέλαμε να επισημάνουμε ότι: Τόσο από τον ορισμό του μέγιστου κοινού διαιρέτη ακεραίων αριθμών, όσο και από τις ιδιότητες, που αναφέραμε στην προηγουμένη πρόταση, δεν απορρέει ένας τρόπος (ένας αλγόριθμος) με τον οποίο να υπολογίζουμε τον μέγιστο κοινό διαιρέτη δύο ή περισσοτέρων ακεραίων αριθμών.

Στα επόμενα θα παρουσιάσουμε και άλλες ιδιότητες του μ.κ.δ., καθώς και έναν αλγόριθμο υπολογισμού του. Επίσης, θα δώσουμε έναν άλλο ισοδύναμο ορισμό του μέγιστου κοινού διαιρέτη ακεραίων αριθμών.

Έστω a, b δύο ακέραιοι αριθμοί. Αν ο ένας είναι πολλαπλάσιο του άλλου (ισοδύναμα, ο ένας διαιρεί τον άλλο), τότε μπορούμε να εφαρμόσουμε όλα όσα είδαμε ανωτέρω. Τι γίνεται όμως αν κανένας δεν είναι πολλαπλάσιο του άλλου;

Θα διατυπώσουμε και θα αποδείξουμε το γνωστό (*από το Δημοτικό*) Θεώρημα.

Θεώρημα 6.1.19. *Έστω a, b ακέραιοι αριθμοί με τον $b > 0$. Υπάρχουν μοναδικοί ακέραιοι αριθμοί π, υ, ούτως ώστε*

$$a = \pi b + \upsilon \text{ και } 0 \leq \upsilon < b.$$

Ως γνωστόν, στην ανωτέρω σχέση $a = \pi b + \upsilon$ ο ακέραιος αριθμός a ονομάζεται **διαιρετέος**, ο ακέραιος αριθμός b ονομάζεται **διαιρέτης**, ο ακέραιος αριθμός π ονομάζεται **πηλίκον** και ο ακέραιος αριθμός υ ονομάζεται **υπόλοιπον**.

Απόδειξη. Θεωρούμε το σύνολο

$$S = \{ a - sb \mid s \in \mathbb{Z} \text{ και } a - sb \geq 0 \}.$$

Το σύνολο S είναι μη κενό. Πράγματι, αν $a \geq 0$, τότε το στοιχείο

$$a = a - 0b \in S.$$

Αν $a < 0$, τότε το στοιχείο $a(1 - b) = a - ab \geq 0$ (γιατί;), δηλαδή

$$a - ab \in S.$$

Εφόσον το S είναι μη κενό και κάτω φραγμένο υπάρχει (μοναδικό) $\upsilon \in S$, το οποίο είναι ελάχιστο στοιχείο του S.

Έστω $\pi \in \mathbb{Z}$, ώστε $a - \pi b = \upsilon$. Τότε $a = \pi b + \upsilon$. Θα δείξουμε ότι

$$0 \leq \upsilon < b.$$

Η πρώτη ανισότητα προφανώς ισχύει. Υποθέτουμε ότι

$$b \leq \upsilon = a - \pi b.$$

Τότε θα έχουμε αφ' ενός

$$0 \leq (a - \pi b) - b = a - (1 + \pi)b = \upsilon - b \in S,$$

αφ' ετέρου

$$\upsilon - b < \upsilon.$$

Αυτό είναι άτοπο, διότι το υ έχει υποτεθεί το ελάχιστο στοιχείο του S. Συνεπώς, πράγματι $0 \leq \upsilon < b$.

Τα π και υ είναι μοναδικά με τις ανωτέρω ιδιότητες. Πράγματι, υποθέτουμε ότι υπάρχουν $p, \pi, u, \upsilon \in \mathbb{Z}$ με

$$a = pb + u,\ 0 \leq u < b \text{ και } a = \pi b + \upsilon,\ 0 \leq \upsilon < b.$$

Αν $p = \pi$, τότε προφανώς(;) $u = \upsilon$.

Υποθέτουμε ότι $p \neq \pi$ και άνευ βλάβης ότι $p > \pi$, τότε θα έχουμε

$$(p - \pi)b = \upsilon - u > 0.$$

Αυτό είναι άτοπο, διότι έχουμε υποθέσει ότι

$$0 \leq \upsilon < b \text{ και } 0 \leq u < b.$$

Οπότε, η διαφορά $\upsilon - u$ είναι πάντα μικρότερη του b (γιατί; ιδέ Άσκηση 6.1.1$_9$). ό.έ.δ.

Σχόλια 6.1.20.

1. Όπως βλέπουμε, τόσο η ανωτέρω απόδειξη, όσο και ο ορισμός του μ.κ.δ. ακεραίων αριθμών στηρίζονται στην σημαντική ιδιότητα των ακεραίων αριθμών: "Κάθε άνω/κάτω φραγμένο μη κενό υποσύνολο των ακεραίων αριθμών, έχει μέγιστο/ελάχιστο στοιχείο", η οποία, με την σειρά της, στηρίζεται στην "Αρχή του ελαχίστου" στους φυσικούς αριθμούς (ιδέ Θεώρημα A.1.10), η οποία είναι ισοδύναμη με την Αρχή της Μαθηματικής Επαγωγής. Συγκρίνατε με την Άσκηση 3.2.11$_{14}$.

2. Αν παρατηρήσουμε προσεκτικά την ανωτέρω απόδειξη, θα δούμε ότι, στην πραγματικότητα πρόκειται για την γνωστή μέθοδο της διαίρεσης δύο ακεραίων αριθμών, όπου από τον διαιρετέο αφαιρούμε (ή προσθέτουμε δεν έχει σημασία) πολλαπλάσια του διαιρέτη για να καταλήξουμε στο υπόλοιπο, το οποίο πάντα θα είναι μεγαλύτερο ή ίσον του μηδενός και γνήσια μικρότερο του (θετικού) διαιρέτη.

3. Η υπόθεση ότι ο διαιρέτης είναι μη μηδενικός, είναι καίρια, διαφορετικά η απόδειξη δεν "προχωρά". Μπορείτε να εντοπίσετε σε πόσα σημεία της απόδειξης χρησιμοποιούμε ότι ο διαιρέτης είναι μη μηδενικός;

4. Η υπόθεση ότι ο διαιρέτης είναι θετικός δεν είναι σημαντική. Θα μπορούσαμε να επαναλάβουμε την απόδειξη χωρίς την υπόθεση ο διαιρέτης να είναι θετικός (αρκεί να είναι μη μηδενικός). Μόνη διαφορά είναι ότι στην περίπτωση του αρνητικού διαιρέτη το υπόλοιπο θα είναι μεγαλύτερο ή ίσο του μηδενός και γνήσια μικρότερο της απόλυτης τιμής του διαιρέτη (Ιδέ Άσκηση 6.1.3$_4$).

Πρόταση 6.1.21. *Έστω $a_1, a_2, \ldots, a_n$ ακέραιοι αριθμοί, οι οποίοι δεν είναι όλοι μηδέν. Υπάρχουν ακέραιοι αριθμοί $\lambda_1, \lambda_2, \ldots, \lambda_n$, ώστε*

$$\mu.\kappa.\delta.(a_1, a_2, \ldots, a_n) = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n.$$

Απόδειξη. Θεωρούμε το σύνολο

$$S = \{x_1 a_1 + x_2 a_2 + \cdots + x_n a_n > 0 \mid x_i \in \mathbb{Z},\ i = 1, \ldots, n\}.$$

Το σύνολο S είναι μη κενό. Πράγματι, από την υπόθεση υπάρχει τουλάχιστον ένα $a_i \neq 0$, επομένως ο ακέραιος αριθμός $\mid a_i \mid \in S$. Συγκεκριμένα στο σύνολο S ανήκουν όλα τα $\mid a_i \mid$ με $a_i \neq 0$.

Έστω δ το ελάχιστο στοιχείο του S, το οποίο θα είναι της μορφής

$$\delta = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n$$

με $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{Z}$. Αν

$$d = \mu.\kappa.\delta(a_1, a_2, \ldots, a_n),$$

τότε προφανώς ο d διαιρεί τον δ.

Ισχυρισμός: ο δ διαιρεί κάθε άλλο στοιχείο του S. Πράγματι, έστω

$$s = \mu_1 a_1 + \mu_2 a_2 + \cdots + \mu_n a_n \in S.$$

Από το προηγούμενο θεώρημα έχουμε ότι υπάρχουν π, υ ακέραιοι αριθμοί ώστε

$$s = \pi\delta + \upsilon,$$

δηλαδή

$$\upsilon = s - \pi\delta = (\mu_1 - \pi\lambda_1)a_1 + (\mu_2 - \pi\lambda_2)a_2 + \cdots + (\mu_n - \pi\lambda_n)a_n.$$

Αλλά $0 \leq \upsilon < \delta$. Αν $\upsilon \neq 0$, τότε από την προηγουμένη σχέση έχουμε ότι $\upsilon \in S$, αυτό είναι άτοπο, διότι το δ είναι το ελάχιστο στοιχείο του S. Άρα πράγματι το δ διαιρεί όλα τα στοιχεία του S.

Κατά συνέπεια, ο δ διαιρεί όλα τα a_i, $i = 1, \ldots, n$ (γιατί;), επομένως είναι ένας κοινός διαιρέτης των a_i, άρα, εξ ορισμού, $\delta \leq d$. Οπότε, επειδή έχουμε ήδη αποδείξει ότι ο d διαιρεί τον δ, έχουμε ότι

$$d = \delta = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n. \qquad \text{ό.έ.δ.}$$

Παρατηρήσεις 6.1.22.

1. Από την προηγουμένη πρόταση έπεται ότι κάθε κοινός διαιρέτης, έστω δ, των ακεραίων αριθμών $a_1, a_2, \ldots, a_n$ διαιρεί τον $\mu.\kappa.\delta(a_1, a_2, \ldots, a_n)$.

2. Στην προηγουμένη πρόταση αποδείξαμε ότι υπάρχουν ακέραιοι αριθμοί $\lambda_1, \lambda_2, \ldots, \lambda_n$, ώστε

   $$\mu.\kappa.\delta(a_1, a_2, \ldots, a_n) = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n,$$

   αλλά δεν είδαμε έναν τρόπο υπολογισμού των, ούτε γνωρίζουμε αν αυτά τα $\lambda_1, \lambda_2, \ldots, \lambda_n$ είναι μοναδικά.

   Στα επόμενα θα δούμε έναν τρόπο υπολογισμού των, όπως επίσης, θα δούμε ότι δεν είναι μοναδικά.

Θα δώσουμε έναν άλλο ισοδύναμο ορισμό του μέγιστου κοινού διαιρέτη ακεραίων αριθμών.

Ορισμός 6.1.23. Έστω $a_1, a_2, \ldots, a_n$ ακέραιοι αριθμοί, οι οποίοι δεν είναι όλοι μηδέν. Ένας μέγιστος κοινός διαιρέτης των a_i είναι ένας θετικός ακέραιος αριθμός d με τις ιδιότητες

i. $d \mid a_i$ για όλα τα $i = 1, \ldots, n$.

ii. Αν $\delta \in \mathbb{Z}$ με $\delta \mid a_i$ για όλα τα $i = 1, \ldots, n$, τότε $\delta \mid d$.

Από τον προηγούμενο ορισμό δεν έπεται ότι ο μέγιστος κοινός διαιρέτης των ακεραίων αριθμών a_i υπάρχει, ούτε ότι είναι μοναδικός.

Πράγματι, οι δύο ορισμοί είναι ισοδύναμοι.

Ας υποθέσουμε ότι έχουμε τον Ορισμό 6.1.16, τότε ισχύει η Πρόταση 6.1.21 και επομένως, για τον μέγιστο κοινό διαιρέτη των a_i πληρούνται οι απαιτήσεις του Ορισμού 6.1.23.

Αντίστροφα, το ελάχιστο στοιχείο δ του συνόλου

$$S = \{x_1a_1 + x_2a_2 + \cdots + x_na_n > 0 \mid x_i \in \mathbb{Z},\ i = 1, \ldots, n\}$$

πληροί τις ιδιότητες του Ορισμού 6.1.23, επομένως ο ορισμός αυτός είναι *"καλός"* και επιπλέον το ελάχιστο στοιχείο του συνόλου S είναι ο μεγαλύτερος από όλους τους κοινούς διαιρέτες των a_i [4].

Παράδειγμα 6.1.24. Για τους αριθμούς 8 και 12 έχουμε ότι μ.κ.δ.$(8, 12) = 4$. Επίσης, βλέπουμε ότι για $\lambda = -4$ και $\mu = 3$ ισχύει ότι

$$(-4) \cdot 8 + 3 \cdot 12 = 4,$$

αλλά και για $\lambda = 8$ και $\mu = -5$ πάλι έχουμε

$$8 \cdot 8 + (-5) \cdot 12 = 4.$$

Στο προηγούμενο παράδειγμα, όπως είχαμε επισημάνει, δεν εφαρμόσαμε έναν *"κανόνα"* για την γραφή του μ.κ.δ.$(8, 12)$ ως

$$\text{μ.κ.δ.}(8, 12) = (-4) \cdot 8 + 3 \cdot 12 = 8 \cdot 8 + (-5) \cdot 12 = 4.$$

Απλώς αρκεστήκαμε σε ένα *παρατηρούμε*.

Ο Ευκλείδιος Αλγόριθμος

Πρόταση 6.1.25. *Έστω $a, b \in \mathbb{Z}$ με $b \neq 0$. Αν $\pi, \upsilon \in \mathbb{Z}$ με*

$$a = \pi b + \upsilon \text{ και } 0 \leq \upsilon < |\, b \,|,$$

τότε

$$\text{μ.κ.δ.}(a, b) = \text{μ.κ.δ.}(\upsilon, b).$$

Απόδειξη. Η απόδειξη έχει προηγηθεί. Είναι η Πρόταση $6.1.18_4$. ό.έ.δ.

Η προηγουμένη πρόταση είναι σημαντική, διότι στην πραγματικότητα μας δίνει έναν αλγόριθμο υπολογισμού του μ.κ.δ. δύο ακεραίων αριθμών.

Η ιδέα είναι απλή και στηρίζεται σε δύο παρατηρήσεις:

1. Το μηδέν διαιρείται από όλους τους ακεραίους, οπότε

$$\text{μ.κ.δ.}(0, a) = |\, a \,|,$$

για κάθε μη μηδενικό ακέραιο a (ιδέ Πρόταση $6.1.18_1$).

[4] Εδώ πρέπει να παρατηρήσουμε ότι στους θετικούς ακεραίους αριθμούς έχουμε μια σχέση διάταξης, η οποία ορίζεται από την διαιρετότητα των ακεραίων αριθμών. Δηλαδή ορίζουμε $b \leq a$, αν $b \mid a$. Προφανώς ισχύει ότι, αν $b \leq a$, τότε $b \leq a$. (Ιδέ τα Παραδείγματα 4.4.7).

Επισημαίνουμε ότι, υπ' αυτήν την έννοια, ο δεύτερος ορισμός του μ.κ.δ. είναι γενικότερος και καλύπτει και άλλες περιοχές των Μαθηματικών, αλλά αυτά δεν είναι επί του παρόντος.

2. Το υπόλοιπο της διαίρεσης δύο ακεραίων αριθμών είναι γνήσια μικρότερο από την απόλυτη τιμή του διαιρέτη.

Επομένως, εφαρμόζοντας την προηγουμένη πρόταση, σε πεπερασμένα βήματα θα καταλήξουμε στον μέγιστο κοινό διαιρέτη των δύο δοθέντων ακεραίων αριθμών. Συγκεκριμένα, ο μ.κ.δ. αυτών των αριθμών είναι το τελευταίο μη μηδενικό υπόλοιπο στις διαδοχικές διαιρέσεις που θα πραγματοποιήσουμε.

Ας περιγράψουμε την διαδικασία.

Έστω $a, b \in \mathbb{Z}$ με (χωρίς βλάβη της γενικότητας) $b > 0$.

Εκτελούμε την διαίρεση του a με τον b.

$$a = \pi_1 b + \upsilon_1,$$

με $0 \leq \upsilon_1 < b$. Από την προηγουμένη πρόταση έχουμε ότι

$$\text{μ.κ.δ.}(a, b) = \text{μ.κ.δ.}(\upsilon_1, b).$$

Αν $\upsilon_1 = 0$, τότε

$$\text{μ.κ.δ.}(a, b) = b.$$

Αν $\upsilon_1 \neq 0$, εκτελούμε την διαίρεση του b με το υ_1.

$$b = \pi_2 \upsilon_1 + \upsilon_2,$$

με $0 \leq \upsilon_2 < \upsilon_1 < b$. Από την προηγουμένη πρόταση έχουμε ότι

$$\text{μ.κ.δ.}(a, b) = \text{μ.κ.δ.}(\upsilon_1, b) = \text{μ.κ.δ.}(\upsilon_1, \upsilon_2).$$

Αν $\upsilon_2 = 0$, τότε

$$\text{μ.κ.δ.}(a, b) = \upsilon_1.$$

Αν $\upsilon_2 \neq 0$, εκτελούμε την διαίρεση του υ_1 με το υ_2...και συνεχίζουμε. Οπότε, θα δημιουργηθεί μια "ακολουθία υπολοίπων"

$$0 = \upsilon_k < \upsilon_{k-1} < \cdots < \upsilon_1 < b.$$

Οπότε,

$$\text{μ.κ.δ.}(a, b) = \upsilon_{k-1}.$$

Γιατί σε πεπερασμένα βήματα θα έχουμε $0 = \upsilon_k$; Δεν ξεχνάμε την Πρόταση 6.1.10, οπότε προφανώς, $k \leq b$.

Ας δούμε και ένα παράδειγμα.

Παράδειγμα 6.1.26. Να υπολογιστεί ο μ.κ.δ. των αριθμών -243 και 117.

Εκτελούμε την διαίρεση του -243 με το 117 και έχουμε,

$$-243 = (-3)117 + 108,$$

οπότε

$$\text{μ.κ.δ.}(-243, 117) = \text{μ.κ.δ}(108, 117).$$

Εκτελούμε την διαίρεση του 117 με το 108 και έχουμε,

$$117 = 1 \cdot 108 + 9.$$

Οπότε,

$$\text{μ.κ.δ.}(-243, 117) = \text{μ.κ.δ}(108, 117) = \text{μ.κ.δ.}(9, 108).$$

Αλλά το 9 διαιρεί το 108, οπότε,

$$\text{μ.κ.δ.}(-243, 117) = \text{μ.κ.δ}(108, 117) = \text{μ.κ.δ.}(9, 108) = 9.$$

Από την Πρόταση 6.1.21 έπεται ότι υπάρχουν $x, y \in \mathbb{Z}$, έτσι ώστε

$$\text{μ.κ.δ}\,(-243, 117) = (-243) \cdot x + 117 \cdot y = 9.$$

Θα προσπαθήσουμε, λεπτολογώντας περισσότερο στην προηγουμένη διαδικασία, να υπολογίσουμε (τουλάχιστον) ένα ζεύγος τέτοιων ακεραίων αριθμών.

Στην ισότητα

$$(-243) \cdot x + 117 \cdot y = 9$$

αντικαθιστούμε το -243 με το ίσον του $(-3)117 + 108$ και έχουμε

$$((-3)117 + 108) \cdot x + 117 \cdot y = 9.$$

Από την τελευταία ισότητα, εκτελώντας τις πράξεις, έχουμε

$$117 \cdot (-3x + y) + 108 \cdot x = 9.$$

Στην ισότητα που προέκυψε αντικαθιστούμε το 117 με το ίσον του $108+9$ και κάνουμε τις πράξεις, οπότε καταλήγουμε στην ισότητα

$$9 \cdot (-3x + y) + 108 \cdot (-2x + y) = 9.$$

Από την τελευταία ισότητα παρατηρούμε ότι ένα ζεύγος (από τους ακεραίους αριθμούς που αναζητούμε) θα ικανοποιεί τις ισότητες

$$-3x + y = 1 \text{ και } -2x + y = 0.$$

Οπότε, η αρχική μας αναζήτηση ανάγεται στην επίλυση του (γραμμικού) συστήματος

$$\begin{cases} -3x + y = 1 \\ -2x + y = 0 \end{cases}$$

Από το οποίο εύκολα βλέπουμε ότι $x = -1$ και $y = -2$.

Επανερχόμενοι στην αρχική μας ισότητα, βλέπουμε ότι πράγματι

$$(-243) \cdot (-1) + 117 \cdot (-2) = 9.$$

Παρατήρηση 6.1.27. Από το προηγούμενο παράδειγμα, αν και αριθμητικό, βλέπουμε πώς μπορούμε γενικά, εφαρμόζοντας τον Ευκλείδιο αλγόριθμο, να υπολογίσουμε τους ακεραίους x, y στην έκφραση του μέγιστου κοινού διαιρέτη δύο ακεραίων a, b, ως

$$\text{μ.κ.δ.}\,(a, b) = ax + by.$$

Αλλά, δεν αποφαινόμαστε αν υπάρχουν μοναδικά x, y, ώστε να ικανοποιούν την ισότητα

$$\text{μ.κ.δ.}\,(a, b) = ax + by.$$

Η επομένη πρόταση δίνει την απάντηση.

Πρόταση 6.1.28. *Έστω* $a, b, c \in \mathbb{Z}$.

i. Υπάρχουν ακέραιοι αριθμοί x, y, *οι οποίοι ικανοποιούν την εξίσωση*

$$ax + by = c \qquad (*)$$

αν και μόνο αν ο μ.κ.δ.$(a, b) = d$ *διαιρεί τον* c.

ii. Αν ένα ζεύγος (x_0, y_0) *ακεραίων αριθμών ικανοποιεί την εξίσωση*

$$ax + by = c,$$

τότε για κάθε $t \in \mathbb{Z}$ *το ζεύγος*

$$(r = x_0 - \frac{b}{d}t, s = y_0 + \frac{a}{d}t)$$

ικανοποιεί την $(*)$.

Μόνο αυτά τα ζεύγη ικανοποιούν την $(*)$.

Απόδειξη.

i. Υποθέτουμε ότι υπάρχουν ακέραιοι αριθμοί x, y, οι οποίοι ικανοποιούν την εξίσωση $ax + by = c$. Προφανώς ο μ.κ.δ.$(a, b) = d$ διαιρεί τον c.

Αντίστροφα, υποθέτουμε ότι ο μ.κ.δ.$(a, b) = d$ διαιρεί τον c. Δηλαδή, $c = d \cdot k$. Από την Πρόταση 6.1.21 έπεται ότι υπάρχουν $\lambda, \mu \in \mathbb{Z}$, ώστε

$$\text{μ.κ.δ.}(a, b) = d = \lambda a + \mu b.$$

Συνεπώς,

$$c = d \cdot k = (\lambda a + \mu b) \cdot k.$$

Άρα οι ακέραιοι αριθμοί $\lambda \cdot k$ και $\mu \cdot k$ ικανοποιούν την $(*)$.

ii. Προφανώς, αν το ζεύγος (x_0, y_0) ακεραίων αριθμών ικανοποιεί την εξίσωση

$$ax + by = c,$$

τότε για κάθε $t \in \mathbb{Z}$ το ζεύγος

$$(r = x_0 - \frac{b}{d}t, s = y_0 + \frac{a}{d}t)$$

ικανοποιεί την $(*)$ (απλή αντικατάσταση και επαλήθευση).

Υποθέτουμε ότι, εκτός του ζεύγους (x_0, y_0), υπάρχει και το ζεύγος (r, s) ακεραίων αριθμών, το οποίο ικανοποιεί την $(*)$.

Τότε έχουμε ότι

$$ax_0 + by_0 = c \text{ και } ar + bs = c.$$

Αφαιρώντας κατά μέλη έχουμε ότι

$$a(x_0 - r) + b(y_0 - s) = 0,$$

απ' όπου έπεται ότι

$$a(x_0 - r) = b(s - y_0).$$

Διαιρούμε και τα δύο μέλη της ισότητας αυτής με τον $d = $μ.κ.δ. (a, b) και έχουμε

$$\frac{a}{d}(x_0 - r) = \frac{b}{d}(s - y_0).$$

Επειδή μ.κ.δ.$\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ (ιδέ Πρόταση 6.1.18$_3$), από την τελευταία ισότητα έπεται ότι ο ακέραιος αριθμός $\frac{a}{d}$ διαιρεί τον ακέραιο αριθμό $s - y_0$ και ο ακέραιος $\frac{b}{d}$ διαιρεί τον ακέραιο αριθμό $x_0 - r$ (γιατί; Ιδέ Άσκηση 6.1.3$_8$). Επομένως, υπάρχουν $t_1, t_2 \in \mathbb{Z}$, ώστε η ισότητα

$$\frac{a}{d}(x_0 - r) = \frac{b}{d}(s - y_0)$$

να λαμβάνει την μορφή

$$\frac{a}{d} \cdot \frac{b}{d} \cdot t_1 = \frac{b}{d} \cdot \frac{a}{d} \cdot t_2.$$

Από την ισότητα αυτή έπεται ότι $t_1 = t_2 = t$ και προφανώς

$$r = x_0 - \frac{b}{d}t,\ s = y_0 + \frac{a}{d}t.$$ ό.έ.δ.

Παρατήρηση 6.1.29. Οι εξισώσεις της μορφής $ax + by = c$, όπου οι a, b, c είναι ακέραιοι αριθμοί ονομάζονται **Διοφαντικές Εξισώσεις** με δύο μεταβλητές. Η προηγουμένη πρόταση ανάγει το πρόβλημα της αναζήτησης ακεραίων λύσεων μιας εξίσωσης της μορφής $ax + by = c$ στο πρόβλημα της γραφής του μέγιστου κοινού διαιρέτη δύο ακεραίων αριθμών ως γραμμικό συνδυασμό αυτών των αριθμών. Όμως το πρόβλημα αυτό έχει απαντηθεί (ιδέ Πρόταση 6.1.25 και το Παράδειγμα 6.1.26).

Δεν θα επεκταθούμε περισσότερο στην μελέτη των Διοφαντικών Εξισώσεων.

Ο Ευκλείδιος Αλγόριθμος αποτελεί μια μέθοδο υπολογισμού του μέγιστου κοινού διαιρέτη δύο ακεραίων αριθμών. Τι γίνεται όμως όταν πρέπει να υπολογίσουμε τον μέγιστο κοινό διαιρέτη τριών ή περισσοτέρων ακεραίων αριθμών;

Πρόταση 6.1.30. *Έστω $a, b, c \in \mathbb{Z}$, όχι όλοι μηδέν. Τότε ισχύει*

$$(a, b, c) = ((a, b), c).$$

Απόδειξη. Έστω $d = (a, b, c)$, $\mu = (a, b)$ και $\delta = ((a, b), c)$.

Προφανώς ο d διαιρεί τον μ (γιατί;) και τον c. Συνεπώς, ο d διαιρεί τον δ (ιδέ Παρατήρηση 6.1.22$_1$).

Αντίστροφα, ο δ διαιρεί τον μ και τον c, άρα διαιρεί τους a, b και c. Συνεπώς, διαιρεί και τον d.

Επομένως, οι d, δ *αλληλοδιαιρούνται* και είναι θετικοί, άρα $d = \delta$. ό.έ.δ.

Η προηγουμένη πρόταση ανάγει το πρόβλημα του υπολογισμού του μέγιστου κοινού διαιρέτη οσωνδήποτε το πλήθος ακεραίων αριθμών στον υπολογισμό του μέγιστου κοινού διαιρέτη δύο ακεραίων αριθμών.

Το ελάχιστο κοινό πολλαπλάσιο ακεραίων αριθμών

Η δυϊκή έννοια του μ.κ.δ. ακεραίων αριθμών είναι η έννοια του ελαχίστου κοινού πολλαπλασίου ακεραίων αριθμών.

Έστω $a_1, a_2, \dots, a_n$ μη μηδενικοί ακέραιοι αριθμοί, τότε υπάρχει (τουλάχιστον) ένας θετικός ακέραιος αριθμός, ο οποίος διαιρείται από κάθε a_i, δηλαδή είναι κοινό πολλαπλάσιο των a_i. Για παράδειγμα, ο θετικός ακέραιος $|\, a_1 \cdot a_2 \cdot \cdots \cdot a_n \,|$. Επομένως, το σύνολο των θετικών κοινών πολλαπλασίων των a_i είναι μη κενό και συνεπώς έχει ελάχιστο στοιχείο (Πρόταση 6.1.12).

Ορισμός 6.1.31. Έστω $a_1, a_2, \dots, a_n$ μη μηδενικοί ακέραιοι αριθμοί. Το **ελάχιστο κοινό πολλαπλάσιο** των a_i υπάρχει και θα συμβολίζεται

$$\text{ε.κ.π.}\ (a_1, a_2, \dots, a_n) \text{ ή ως } [a_1, a_2, \dots, a_n].$$

Για το ελάχιστο κοινό πολλαπλάσιο ακεραίων αριθμών δεν ισχύει μια ανάλογη πρόταση της Πρότασης 6.1.21, η οποία ισχύει για τον μέγιστο κοινό διαιρέτη ακεραίων αριθμών. Αλλά ισχύει το δυϊκό της Παρατήρησης 6.1.22[1].

Πρόταση 6.1.32. *Έστω $a_1, a_2, \dots, a_n$ μη μηδενικοί ακέραιοι αριθμοί. Ο ακέραιος αριθμός k είναι κοινό πολλαπλάσιο των a_i, αν και μόνο αν το*

$$m = \text{ε.κ.π.}\ (a_1, a_2, \dots, a_n)$$

διαιρεί τον k.

Απόδειξη. Υποθέτουμε ότι ο k είναι κοινό πολλαπλάσιο των a_i. Από την διαίρεση του k με τον m έχουμε $k = \pi m + \upsilon$ με $0 \leq \upsilon < m$. Αλλά τότε το $\upsilon = k - \pi m$ είναι ένα κοινό πολλαπλάσιο των a_i (γιατί;). Αν $\upsilon \neq 0$, τότε έχουμε άτοπο, διότι αντιβαίνουμε στον ορισμό του ελαχίστου κοινού πολλαπλασίου. Συνεπώς, $\upsilon = 0$.

Η αντίστροφη κατεύθυνση είναι προφανής. ό.έ.δ.

Ιδιότητες του ελαχίστου κοινού πολλαπλασίου δίνονται ως ασκήσεις.

Πρώτοι αριθμοί

Έστω a ένας ακέραιος αριθμός. Οι *προφανείς* διαιρέτες του είναι οι ± 1 και $\pm a$. Το ερώτημα που γεννάται είναι: Υπάρχουν και άλλοι διαιρέτες του ακεραίου a;

Ορισμός 6.1.33. Ένας θετικός ακέραιος p με $p > 1$ και μόνους θετικούς διαιρέτες το 1 και τον p θα ονομάζεται **πρώτος** αριθμός. [5]

Κάθε θετικός ακέραιος μεγαλύτερος του 1, ο οποίος δεν είναι πρώτος, θα ονομάζεται **σύνθετος** αριθμός.

Οι πρώτοι αριθμοί, όπως θα δούμε, είναι οι "δομικοί λίθοι" των ακεραίων αριθμών. Αν και η μελέτη τους έχει προχωρήσει σημαντικά, παραμένουν αναπάντητα πολλά και ενδιαφέροντα ερωτήματα.

Εμείς εδώ απλώς θα περιορισθούμε σε μερικές μόνο βασικές ιδιότητες των πρώτων αριθμών.

---

[5] 1. Όπως βλέπουμε, εξ ορισμού, το 1 **δεν** είναι πρώτος αριθμός. Αυτό έχει την σημασία του, αλλά δεν είναι επί του παρόντος.

2. Δεν πρέπει να γίνεται σύγχυση με τον όρο σχετικά πρώτοι αριθμοί (ιδέ Ορισμός 6.1.16), εκεί αναφερόμαστε/*συγκρίνουμε* σε τουλάχιστον δύο ακεραίους αριθμούς.

Πρόταση 6.1.34. *Κάθε ακέραιος αριθμός $n > 1$ έχει έναν πρώτο διαιρέτη.*

Απόδειξη. Ο ακέραιος n έχει θετικούς ακεραίους μεγαλύτερους του 1 (για παράδειγμα τον ίδιο τον n). Μεταξύ των θετικών διαιρετών του n των διαφορετικών του 1 επιλέγουμε τον ελάχιστο, έστω d. Ο d είναι πρώτος. Υποθέτουμε ότι δεν είναι πρώτος, τότε υπάρχουν ακέραιοι a, b με $d = a \cdot b$ και $1 < a, b < d$. Τότε όμως θα έχουμε ότι: Ο a διαιρεί τον d και κατά συνέπεια τον n. Δηλαδή ο d δεν είναι ο ελάχιστος θετικός διαιρέτης του n με $d > 1$, άτοπο. ό.έ.δ.

Το Θεμελιώδες Θεώρημα της αριθμητικής

Θεώρημα 6.1.35. *Κάθε ακέραιος αριθμός $n > 1$, είτε είναι πρώτος είτε υπάρχουν πεπερασμένο το πλήθος μοναδικοί πρώτοι $p_1, p_2, \dots, p_k$, έτσι ώστε*

$$n = p_1\, p_2 \cdots p_k,$$

όπου η σειρά των παραγόντων, στο ανωτέρω γινόμενο, δεν έχει σημασία.

Απόδειξη. Ο αριθμός $n = 2$ είναι πρώτος. Επομένως, ο ισχυρισμός ισχύει. Υποθέτουμε ότι ο ισχυρισμός ισχύει για όλους του ακεραίους m με $2 \leq m \leq n-1$. Εάν ο n είναι πρώτος, έχει καλώς. Διαφορετικά, από την προηγουμένη πρόταση, υπάρχει ένας πρώτος αριθμός, έστω p, ώστε

$$n = p \cdot m$$

με $1 < m \leq n-1$. Από την υπόθεσή μας, είτε ο m είναι πρώτος ή υπάρχουν (μοναδικοί) πρώτοι αριθμοί $p_1, p_2, \dots, p_r$, ώστε

$$m = p_1\, p_2 \cdots p_r.$$

Οπότε

$$n = p \cdot m = p \cdot p_1\, p_2 \cdots p_r.$$

Επομένως, πράγματι ο n μπορεί να γραφεί ως γινόμενο πρώτων αριθμών [6].

Υποθέτουμε ότι υπάρχουν θετικοί ακέραιοι μεγαλύτεροι του 1, ο οποίοι έχουν περισσότερες της μιας διαφορετικές αναλύσεις σε γινόμενο πρώτων αριθμών. Από την αρχή του ελαχίστου υπάρχει ένας ελάχιστος ακέραιος n με δύο διαφορετικές αναλύσεις σε γινόμενο πρώτων αριθμών, δηλαδή

$$n = p_1\, p_2 \cdots p_k = q_1\, q_2 \cdots q_s,$$

όπου οι $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_s$ είναι πρώτοι. Μάλιστα δε, μπορούμε να υποθέσουμε ότι

$$p_1 \leq p_2 \leq \cdots \leq p_k \text{ και } q_1 \leq q_2 \leq \cdots \leq q_s.$$

Από την σχέση αυτή έπεται ότι

$$p_1 = q_i \text{ και } q_1 = p_j$$

για κάποιο i και j (γιατί; ιδέ Άσκηση 6.1.3$_{12}$. Επομένως, θα έχουμε

$$p_1 = q_i \geq q_1 = p_j \geq p_1,$$

[6] Θα μπορούσαμε (αβασάνιστα) να ισχυριστούμε, ότι αφού για τον m υπάρχουν (μοναδικοί) πρώτοι αριθμοί $p_1, p_2, \dots, p_r$, ώστε $m = p_1\, p_2 \cdots p_r$ και για τον $n = p \cdot m$ έχουμε μοναδική γραφή ως γινόμενο πρώτων αριθμών;

δηλαδή

$$p_1 = q_1.$$

Συνεπώς,

$$n/p_1 = p_2 \cdots p_k = q_2 \cdots q_s < n.$$

Επειδή ο n έχει υποτεθεί ως ο μικρότερος θετικός ακέραιος με την ανωτέρω ιδιότητα, για τον ακέραιο n/p_1 αναγκαστικά θα ισχύει

$$k = s \text{ και } p_i = q_i,$$

για όλα τα $2 \leq i \leq k$.

Τελικά, $n = p_1\, p_2 \cdots p_k$ με τα p_i μοναδικά. ό.έ.δ.

Σχόλια 6.1.36.

1. Στην προηγουμένη απόδειξη βλέπουμε (έναν από τους λόγους) γιατί ο 1 δεν συμπεριλαμβάνεται μεταξύ των πρώτων αριθμών.

2. Προφανώς κάθε ακέραιος αριθμός n, διάφορος του μηδενός και του ± 1, μπορεί να παρασταθεί κατά μοναδικό τρόπο ως

$$n = \epsilon p_1^{\lambda_1}\, p_2^{\lambda_2} \cdots p_k^{\lambda_k},$$

όπου $\epsilon = \pm 1,\ p_1 < p_2 < \cdots < p_k$ και $\lambda \in \mathbb{N}$.

3. Το προηγούμενο θεώρημα δεν μας δίνει έναν τρόπο ανάλυσης ενός ακεραίου αριθμού σε γινόμενο πρώτων αριθμών, παρ' όλα ταύτα, είναι ένα από τα σημαντικότερα θεωρήματα στα Μαθηματικά.

Παράδειγμα 6.1.37. Προφανώς

$$120 = 2^3 \cdot 3 \cdot 5.$$

Επομένως, κάθε διαιρέτης του 120 θα είναι της μορφής

$$2^\lambda \cdot 3^\mu \cdot 5^\nu$$

με $0 \leq \lambda \leq 3,\ 0 \leq \mu \leq 1$ και $0 \leq \nu \leq 1$.

Ένα από τα μεγαλύτερα προβλήματα στα Μαθηματικά είναι να βρεθεί ένα κριτήριο, το οποίο να αποφαίνεται πότε ένας ακέραιος αριθμός είναι πρώτος.

Βέβαια θα μπορούσε να ισχυριστεί κάποιος ότι μπορούμε να αποφανθούμε, αν ένας ακέραιος $n > 1$ είναι (ή δεν είναι) πρώτος, εκτελώντας όλες τις διαιρέσεις του n με διαιρέτες b, όπου $1 < b \leq n$ [7]. Αλλά, προφανώς, μια τέτοια (*εξαντλητική*) προσπάθεια είναι ατελέσφορη και δεν αποτελεί κριτήριο για να αποφανθούμε αν ένας ακέραιος αριθμός είναι πρώτος.

Στα επόμενα θα αναφερθούμε απλώς σε μερικά αποτελέσματα, τα οποία αφορούν τους πρώτους αριθμούς.

Πρόταση 6.1.38. *Υπάρχουν άπειροι το πλήθος πρώτοι αριθμοί.*

[7] Μάλιστα αρκεί να δοκιμάσουμε τους διαιρέτες b, όπου $1 < b \leq \sqrt{n}$ (γιατί;)

Απόδειξη. Την απόδειξη αυτή την έχουμε ήδη δει, όταν παρουσιάζαμε παραδείγματα αποδείξεων με την μέθοδο της εις άτοπον απαγωγής. Είναι το Θεώρημα 3.2.9.

Εδώ θα δώσουμε μια, φαινομενικά, διαφορετική απόδειξη.

Για κάθε ακέραιο $n \geq 1$ θεωρούμε τον ακέραιο

$$k_n = n! + 1.$$

Από την πρόταση 6.1.34 υπάρχει ένας πρώτος p_n, ο οποίος διαιρεί τον ακέραιο k_n. Ο p_n είναι γνήσια μεγαλύτερος του n. Πράγματι, αν $p_n \leq n$, τότε ο p_n θα διαιρεί τον $n!$ (γιατί;). Αυτό όμως είναι άτοπο, διότι, θα είχαμε

$$p_n \mid (k_n - n!) = 1.$$

Συνεπώς, αποδείξαμε ότι για κάθε $n \geq 1$ υπάρχει ένας πρώτος $p_n > n$. ό.έ.δ.

Συγκρίνατε με την Παρατήρηση $3.2.10_3$.

Έστω x ένας θετικός πραγματικός αριθμός. Το ερώτημα που εγείρεται είναι κατά πόσον μπορούμε να υπολογίσουμε το πλήθος των πρώτων, οι οποίοι είναι μικρότεροι του δοθέντος x.

Το ερώτημα έχει απαντηθεί το 1896, ανεξάρτητα, από τους J. Hadamard και C.J. de la Vallée Poussin και αποτελεί ένα από τα σπουδαιότερα θεωρήματα των Μαθηματικών.

Εδώ απλώς το παραθέτουμε, δεδομένου ότι όλες οι δοθείσες αποδείξεις εκφεύγουν του σκοπού του παρόντος συγγράμματος.

Το Θεώρημα πρώτων αριθμών

Θεώρημα 6.1.39. *Έστω x ένας θετικός πραγματικός αριθμός. Αν $\pi(x)$ παριστά το πλήθος των πρώτων αριθμών των μικροτέρων από το x, τότε*

$$\lim_{x \longrightarrow \infty} (\pi(x) \frac{ln_e x}{x}) = 1.$$

Ένα άλλο ερώτημα που εγείρεται είναι κατά πόσον υπάρχει μια *κανονικότητα* στην κατανομή των πρώτων ανάμεσα στους θετικούς ακεραίους αριθμούς.

Πρόταση 6.1.40. *Για κάθε θετικό ακέραιο αριθμό n υπάρχουν τουλάχιστον n το πλήθος διαδοχικοί ακέραιοι, οι οποίοι είναι σύνθετοι.*

Απόδειξη. Οι διαδοχικοί ακέραιοι αριθμοί

$$(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + (n+1)$$

είναι όλοι σύνθετοι (γιατί;). ό.έ.δ.

Παρ' όλο που η προηγουμένη πρόταση μας εξασφαλίζει αυθαίρετα μεγάλα διαστήματα θετικών ακεραίων αριθμών, όπου απουσιάζουν οι πρώτοι αριθμοί, υπάρχουν (σχεδόν διαδοχικοί) [8] πρώτοι αριθμοί, για παράδειγμα οι 11, 13, οι 17, 19.

Δύο πρώτοι αριθμοί p, q, οι οποίοι διαφέρουν κατά 2, θα ονομάζονται **δίδυμοι**.

Υπάρχει η περίφημη εικασία:

Υπάρχουν άπειρα το πλήθος ζεύγη διδύμων πρώτων αριθμών.

[8] Οι μόνοι διαδοχικοί πρώτοι αριθμοί είναι οι 2 και 3.

Η εικασία αυτή παραμένει ανοικτή. Η τελευταία μεγάλη ώθηση, ως προς την επίλυσή της, εδόθη το 2013 από τον Y. Zhang και αμέσως μετά, το 2014, εδόθη μεγαλύτερη ώθηση από τους J. Maynard και T. Tao.

Δεδομένου ότι, όπως προαναφέραμε, δεν υπάρχει αλγόριθμος, ο οποίος να "κατασκευάζει/ανακαλύπτει" όλους τους πρώτους, έχουν γίνει πολλές προσπάθειες να κατασκευάζουμε πρώτους αριθμούς. Για παράδειγμα, ιδέ την Παρατήρηση 3.2.10$_3$. Προς την κατεύθυνση αυτή υπάρχει ένα θεώρημα (Dirichlet 1837), το οποίο απλώς παραθέτουμε.

Θεώρημα 6.1.41. *Έστω a, b σχετικά πρώτοι αριθμοί. Τότε στην αριθμητική πρόοδο*

$$an + b,\ n = 1, 2, \ldots$$

Υπάρχουν άπειροι το πλήθος όροι, οι οποίοι είναι πρώτοι αριθμοί.

Δεν θα επεκταθούμε περισσότερο. Θα κλείσουμε την παράγραφο παραθέτοντας την περίφημη εικασία του Goldbach:

> ***Κάθε άρτιος θετικός ακέραιος μεγαλύτερος του 2 μπορεί να γραφεί ως άθροισμα δύο πρώτων.***

Η συνάρτηση του Euler

Έστω n ένας θετικός ακέραιος. Ένα πρόβλημα που προκύπτει, είναι να προσδιορίσουμε όλους τους ακεραίους k, οι οποίοι είναι σχετικά πρώτοι προς τον n, δηλαδή

$$\text{μ.κ.δ.}(k, n) = 1.$$

Από την Πρόταση 6.1.25 έπεται ότι αρκεί να αναζητήσουμε μόνο τους ακεραίους

$$1 \leq k \leq n, \text{ ώστε μ.κ.δ.}(k, n) = 1.$$

Το πλήθος των ακεραίων με την ιδιότητα αυτή θα συμβολίζεται ως $\varphi(n)$, δηλαδή

$$\varphi(n) = |\{k \in \mathbb{Z} \mid 1 \leq k \leq n \text{ και μ.κ.δ.}(k, n) = 1\}|.$$

Δεδομένου ότι έχουμε ταυτίσει τους φυσικούς αριθμούς με τους θετικούς ακεραίους, πρόκειται για μια συνάρτηση/απεικόνιση

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}.$$

Η συνάρτηση αυτή ονομάζεται **συνάρτηση του Euler**.
Προφανώς

$$\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \ldots.$$

Το ερώτημα, το οποίο προκύπτει, είναι να μπορέσουμε να προσδιορίσουμε την τιμή $\varphi(n)$ για κάθε $n \in \mathbb{N}$.

Λήμμα 6.1.42.

i. Έστω p πρώτος αριθμός και k θετικός ακέραιος, τότε

$$\varphi(p^k) = p^k - p^{k-1}.$$

ii. Έστω p, q διαφορετικοί πρώτοι αριθμοί, τότε

$$\varphi(p \cdot q) = (p-1)(q-1).$$

Απόδειξη. Η απόδειξη είναι απλή και αφήνεται ως άσκηση (Άσκηση $6.1.3_{16}$). ό.έ.δ.

Λήμμα 6.1.43. *Έστω n, m θετικοί ακέραιοι με μ.κ.δ.$(n, m) = 1$. Εάν ο d_1 διατρέχει τους θετικούς διαιρέτες του n και ο d_2 διατρέχει τους θετικούς διαιρέτες του m, τότε ο $d_1 \cdot d_2$ διατρέχει (χωρίς επανάληψη) όλους τους διαιρέτες του $n \cdot m$.*

Απόδειξη. Προφανώς, αν $d_1 \mid n$ και $d_2 \mid m$, τότε

$$d_1 \cdot d_2 \mid n \cdot m \text{ και μ.κ.δ.}(d_1, d_2) = 1.$$

Αντίστροφα, έστω $d \mid n \cdot m$, τότε

$$d = (d, n \cdot m) = (d, n) \cdot (d, m) \text{ (γιατί; ιδέ Άσκηση } 6.1.3_9). \qquad \text{ό.έ.δ.}$$

Θεώρημα 6.1.44. *Έστω $n, m \in N$ σχετικά πρώτοι (μ.κ.δ.$(n, m) = 1$). Τότε ισχύει*

$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)\ ^{9}.$$

Απόδειξη. Υπάρχουν πολλές αποδείξεις αυτού του σημαντικού αποτελέσματος.

Θα σκιαγραφήσουμε μια αφήνοντας τις λεπτομέρειες να συμπληρωθούν από τον αναγνώστη.

Θα κινηθούμε δυϊκά. Από τον ορισμό της συνάρτησης του Euler έχουμε ότι το πλήθος των ακεραίων $1 \leq i \leq n \cdot m$ των μη πρώτων προς τον $n \cdot m$ ισούται με

$$n \cdot m - \varphi(n \cdot m).$$

Όμοια το πλήθος των ακεραίων $1 \leq j \leq n$ των μη πρώτων προς τον n ισούται με

$$n - \varphi(n)$$

και το πλήθος των ακεραίων $1 \leq k \leq m$ των μη πρώτων προς τον m ισούται με

$$m - \varphi(m).$$

Έχουμε τα εξής "είδη" ακεραίων $1 \leq i \leq n \cdot m$ των μη πρώτων προς τον $n \cdot m$.

i. $j \cdot k$, όπου $1 \leq j \leq n$ μη πρώτος προς τον n και $1 \leq k \leq m$ μη πρώτος προς τον m. Προφανώς υπάρχουν

$$(n - \varphi(n)) \cdot (m - \varphi(m))$$

το πλήθος ακεραίων αυτού του είδους.

ii. $j \cdot r$, όπου $1 \leq j \leq n$ μη πρώτος προς τον n και $1 \leq r \leq m$ πρώτος προς τον m. Προφανώς υπάρχουν

$$(n - \varphi(n)) \cdot \varphi(m)$$

το πλήθος ακεραίων αυτού του είδους.

---

[9] Γενικά μια συνάρτηση $f : \mathbb{N} \longrightarrow \mathbb{N}$ με την ιδιότητα $f(n \cdot m) = f(n) \cdot f(m)$ για όλα τα $n, m \in \mathbb{N}$ με $(n, m) = 1$, θα ονομάζεται **πολλαπλασιαστική**.

iii. $s \cdot k$, όπου $1 \leq s \leq n$ πρώτος προς τον n και $1 \leq k \leq m$ μη πρώτος προς τον m. Προφανώς υπάρχουν

$$\varphi(n) \cdot (m - \varphi(m))$$

το πλήθος ακεραίων αυτού του είδους.

Προφανώς τα τρία είδη είναι διαφορετικά μεταξύ τους (δεν υπάρχει ακέραιος $1 \leq i \leq n \cdot m$, ο οποίος να ανήκει σε ταυτοχρόνως σε δύο από τα ανωτέρω είδη).

Ένας ακέραιος $1 \leq i \leq n \cdot m$, μη πρώτος προς τον $n \cdot m$, ανήκει αναγκαστικά σε ένα από τα ανωτέρω είδη (γιατί;) Αυτό μας το εξασφαλίζει το Λήμμα 6.1.43.

Επομένως, δεν έχουμε παρά να συγκρίνουμε πληθικούς αριθμούς πεπερασμένων συνόλων.

$$[(n - \varphi(n)) \cdot (m - \varphi(m))] + [(n - \varphi(n)) \cdot \varphi(m)] + [\varphi(n) \cdot (m - \varphi(m))] = n \cdot m - \varphi(n \cdot m).$$

Εκτελώντας τις πράξεις στο πρώτο μέλος της ισότητας αυτής καταλήγουμε στο

$$n \cdot m - \varphi(n) \cdot \varphi(m) = n \cdot m - \varphi(n \cdot m).$$

Εξ'ου το αποτέλεσμα του ισχυρισμού. ό.έ.δ.

Πόρισμα 6.1.45. *Έστω $n = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k} > 1$ η ανάλυση του n σε γινόμενο πρώτων παραγόντων. Τότε ισχύει ότι:*

$$\begin{aligned} \varphi(n) &= (p_1^{\lambda_1} - p_1^{\lambda_1 - 1})(p_2^{\lambda_2} - p_2^{\lambda_2 - 1}) \cdots (p_k^{\lambda_k} - p_k^{\lambda_k - 1}) \\ &= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}). \end{aligned}$$

Απόδειξη. Δεν έχουμε παρά να εφαρμόσουμε διαδοχικά το προηγούμενο θεώρημα σε συνδυασμό με το Λήμμα 6.1.42. ό.έ.δ.

6.1.3 Ασκήσεις

1. Να αποδείξετε (με κάθε λεπτομέρεια) τους ισχυρισμούς, οι οποίοι αναφέρονται στις Παρατηρήσεις 6.1.15

2. Έστω $a, b, c, d \in \mathbb{Z}$. Υποθέτουμε ότι $a \mid b$ και $c \mid d$, δείξτε ότι $ac \mid bd$.

3. Έστω $a, b, c \in \mathbb{Z}$. Υποθέτουμε ότι $a \mid b$ και $c \mid b$. Είναι αληθές ότι $ac \mid b$;

4. Να αποδείξετε την εξής γενίκευση του Θεωρήματος 6.1.19:

   Έστω a, b ακέραιοι αριθμοί με τον $b \neq 0$. Υπάρχουν μοναδικοί ακέραιοι αριθμοί π, υ, ούτως ώστε $a = \pi b + \upsilon$ και $0 \leq \upsilon < |b|$.

5. Να αποδείξετε την αντίστροφη κατεύθυνση στο (3) της Πρότασης 6.1.18.

   Δηλαδή, για τον κοινό διαιρέτη d των a, b ισχύει ότι

$$d = \text{μ.κ.δ}(a, b), \text{ αν και μόνο αν } \text{μ.κ.δ}\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

6. Να βρεθούν δύο ζεύγη $(\lambda_1, \lambda_2), (\mu_1, \mu_2)$ ακεραίων αριθμών, ώστε

$$\text{μ.κ.δ } (5, 7) = 5\lambda_1 + 7\lambda_2 = 5\mu_1 + 7\mu_2.$$

7. Έστω $a, b \in \mathbb{Z}$ με μ.κ.δ $(a, b) = \lambda a + \mu b$, $\lambda, \mu \in \mathbb{Z}$. Δείξτε ότι μ.κ.δ. $(\lambda, \mu) = 1$.

8. Έστω $a, b, m \in \mathbb{Z}$ με μ.κ.δ. $(a, b) = 1$. Υποθέτουμε ότι ο αριθμός a διαιρεί το γινόμενο $b \cdot m$. Δείξτε ότι ο a διαιρεί τον m.

9. Έστω n, m, d μη μηδενικοί ακέραιοι με μ.κ.δ.$(n, m) = 1$. Δείξτε ότι

$$\text{μ.κ.δ.}(d, n \cdot m) = \text{μ.κ.δ.}(d, n) \cdot \text{μ.κ.δ.}\ (d, m).$$

10. Έστω $a_1, a_2, \ldots, a_n$ θετικοί ακέραιοι αριθμοί. Δείξτε ότι

$$[\, a_1, a_2, \ldots, a_n \,] = [\, [\, a_1, a_2, \ldots, a_{n-1} \,], a_n \,].$$

11. Έστω a, b, c μη μηδενικοί ακέραιοι αριθμοί. Δείξτε ότι

    i. $[a, b] = | a | \cdot | b |$, αν και μόνο αν $(a, b) = 1$.
    ii. $(a, b) \cdot [a, b] = | a | \cdot | b |$.
    iii. $(a, [b, c]) = [(a, b), (a, c)]$ και $[a, (b, c)] = ([a, b], [a, c])$.

12. i. Έστω $p, m, n \in \mathbb{Z}$. Αν ο p είναι πρώτος και $p \mid m \cdot n$, δείξτε ότι

$$p \mid m \text{ ή } p \mid n.$$

    ii. Έστω $p, p_1, p_2, \ldots, p_n$ πρώτοι αριθμοί. Υποθέτουμε ότι

$$p \mid p_1\, p_2 \cdots p_n,$$

    δείξτε ότι $p = p_i$ για κάποιο $1 \leq i \leq n$.

13. Έστω a, b θετικοί ακέραιοι. Υποθέτουμε ότι $a^3 \mid b^2$. Δείξτε ότι $a \mid b$.

14. Χωρίς την χρήση του Θεωρήματος 6.1.41 να αποδείξετε ότι υπάρχουν άπειροι το πλήθος πρώτοι της μορφής $4k + 3$.

15. Έστω p_n ο n-οστός όρος της ακολουθίας των πρώτων αριθμών. Δείξτε ότι

$$p_n < 2^{2^n},$$

    για όλα τα $n \in \mathbb{N}$.

    Υπόδειξη:. Δείξτε πρώτα ότι $p_{n+1} \leq p_1 p_2 \cdots p_n + 1$.

16. Να αποδείξετε, με κάθε λεπτομέρεια, το Λήμμα 6.1.42.

17. Να βρεθούν όλοι οι θετικοί ακέραιοι, για τους οποίους ισχύει:

    i. $\varphi(n) = \frac{1}{2} n$.
    ii. $\varphi(n) = \varphi(2n)$.
    iii. $\varphi(n) = 12$.
    iv. $\varphi(3n) = \varphi(4n) = \varphi(6n)$.

18. Δείξτε ότι για κάθε $n > 1$ το άθροισμα όλων των θετικών ακεραίων των μικρότερων του n και πρώτων προς τον n ισούται με $\frac{1}{2} n\varphi(n)$.

    Υπόδειξη: Θυμηθείτε ότι, αν $(n, m) = 1$, τότε $(m - n, m) = 1$.

6.2 Το σώμα των ρητών αριθμών

Αν και με την κατασκευή του δακτυλίου των ακεραίων αριθμών αντιμετωπίσαμε *αδυναμίες* του συνόλου των φυσικών αριθμών, ο δακτύλιος των ακεραίων εξακολουθεί να *πάσχει* ως προς τις (αλγεβρικές) ιδιότητες που έχουν. Για παράδειγμα οι μόνοι ακέραιοι, οι οποίοι έχουν αντίστροφο ως προς τον πολλαπλασιασμό είναι το +1 και το -1. Για να αρθεί η αδυναμία αυτή και κάθε (μη μηδενικός) ακέραιος να αποκτήσει αντίστροφο, θα κατασκευάσουμε τους ρητούς αριθμούς *επεκτείνοντας* κατάλληλα το σύνολο των ακεραίων αριθμών. Διαισθητικά αυτό το είχαμε κάνει με την κατασκευή των κλασμάτων. Εδώ θα ορίσουμε αυστηρά τους ρητούς αριθμούς.

Διαδικαστικά, θα μιμηθούμε την κατασκευή των ακεραίων αριθμών από τους φυσικούς αριθμούς μέσω μιας σχέσης ισοδυναμίας. Υπάρχει μια λεπτή, αλλά ουσιώδης διαφορά.

Έστω $\mathbb{Z}^* = \mathbb{Z}\backslash\{0\}$ το σύνολο των μη μηδενικών ακεραίων. Στο καρτεσιανό γινόμενο $\mathbb{Z}\times\mathbb{Z}^*$ ορίζουμε μια σχέση $\sim$ ως εξής:

$$(a, b) \sim (c, d), \text{ αν } a\cdot d = b\cdot c \ [10].$$

Πρόταση 6.2.1. *Η ανωτέρω σχέση $\sim$ είναι σχέση ισοδυναμίας.*

Απόδειξη. Η απόδειξη είναι εύκολη και αφήνεται ως άσκηση. ό.έ.δ.

Πρέπει να παρατηρήσουμε ότι στα ζεύγη (a, b) ακεραίων αριθμών η δεύτερη συντεταγμένη δεν είναι μηδενική. Γιατί αυτή η υπόθεση είναι αναγκαία για να αποδείξουμε ότι η σχέση $\sim$ είναι σχέση ισοδυναμίας;

Θα συμβολίζουμε με

$$[(a, b)] = \{(x, y) \in \mathbb{Z}\times\mathbb{Z}^* \mid (x, y) \sim (a, b)\}$$

την κλάση ισοδυναμίας του ζεύγους (a, b).

Παρατηρούμε ότι

$$[(0, 1)] = [(0, x)],$$

για όλα τα $x \in \mathbb{Z}^*$. Επίσης

$$[(1, 1)] = [(x, x)],$$

για όλα τα $x \in \mathbb{Z}^*$.

Θα συμβολίζουμε με $\hat{0} = [(0, 1)]$ και με $\hat{1} = [(1, 1)]$.

Ορισμός 6.2.2. Το σύνολο πηλίκων $\mathbb{Z}\times\mathbb{Z}^*/\sim$ των κλάσεων ισοδυναμίας θα ονομάζεται το σύνολο των **ρητών** αριθμών και θα συμβολίζεται με $\mathbb{Q}$.

Στο σύνολο $\mathbb{Q}$ των ρητών αριθμών ορίζουμε δύο πράξεις:

Μια πρόσθεση $+ : \mathbb{Q}\times\mathbb{Q} \longrightarrow \mathbb{Q}$ ως εξής:

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)], \text{ για όλα τα } [(a, b)], [(c, d)] \in \mathbb{Q}.$$

Έναν πολλαπλασιασμό $\cdot : \mathbb{Q}\times\mathbb{Q} \longrightarrow \mathbb{Q}$ ως εξής:

$$[(a, b)]\cdot[(c, d)] = [(ac, bd)], \text{ για όλα τα } [(a, b)], [(c, d)] \in \mathbb{Q}.$$

[10] Στην Άσκηση 4.4.2$_9$ είχαμε δει την σχέση αυτή ως ένα παράδειγμα σχέσεως ισοδυναμίας, θεωρώντας γνωστές τις ιδιότητες των ακεραίων αριθμών. Εδώ θα μελετήσουμε την σχέση αυτή.

Στο σύνολο $\mathbb{Q}$ των ρητών αριθμών ορίζουμε μια σχέση $<$ ως εξής:

$$[(a, b)] < [(c, d)], \text{ αν } ad < bc \text{ και } bd > 0 \text{ ή αν } ad > bc \text{ και } bd < 0$$

για όλα τα $[(a, b)], [(c, d)] \in \mathbb{Q}$.

Οπότε, μπορούμε να ορίσουμε και μια άλλη σχέση $\leq$ ως εξής:

$$[(a, b)] \leq [(c, d)], \text{ αν } [(a, b)] < [(c, d)] \text{ ή } [(a, b)] = [(c, d)]$$

για όλα τα $[(a, b)], [(c, d)] \in \mathbb{Q}$.

Πριν προχωρήσουμε, πρέπει να παρατηρήσουμε ότι:

Οι πράξεις και οι σχέσεις, που ορίσαμε στο σύνολο των ρητών, ορίστηκαν με την βοήθεια των ήδη ορισμένων πράξεων και σχέσεων στους ακεραίους αριθμούς.

Επίσης, χρησιμοποιούμε τον ίδιο συμβολισμό. Αυτό δεν (πρέπει να) προκαλεί σύγχυση.

Επισημαίνουμε ότι (προς το παρόν) δεν έχει νόημα, για παράδειγμα, να προσθέσουμε έναν ρητό $[(a, b)]$ με έναν ακέραιο αριθμό c, καθ' ότι πρόκειται για δύο διαφορετικά σύνολα. Το πρόβλημα αυτό αίρεται, όταν δούμε υπό ποιον τρόπο το σύνολο των ακεραίων αριθμών "περιέχεται" στο σύνολο των ρητών αριθμών.

Επειδή το σύνολο των ρητών αποτελείται από κλάσεις ισοδυναμίας, οι πράξεις και οι σχέσεις, τις οποίες ορίσαμε, πρέπει να ελεγχθούν ότι είναι "καλώς ορισμένες", δηλαδή δεν εξαρτώνται από την επιλογή των αντιπροσώπων, αλλά από τις κλάσεις αυτές καθ' εαυτές.

Πρόταση 6.2.3. *Οι πράξεις της πρόσθεσης και του πολλαπλασιασμού, καθώς και η σχέση $<$ στο σύνολο των ρητών αριθμών είναι καλώς ορισμένες.*

Απόδειξη. Θα αποδείξουμε ότι η σχέση $<$ είναι καλώς ορισμένη, αφήνοντας τα υπόλοιπα ως άσκηση.

Έστω $(a, b), (c, d), (x, y), (z, w) \in \mathbb{Z} \times \mathbb{Z}$. Υποθέτουμε ότι

$$[(a, b)] = [(x, y)] \text{ και } [(c, d)] = [(z, w)].$$

Από τις ισότητες

$$[(a, b)] = [(x, y)] \text{ και } [(c, d)] = [(z, w)]$$

έχουμε ότι

$$ay = bx \text{ και } cw = zd \qquad (*)$$

Θα δείξουμε ότι, αν $[(a, b)] < [(c, d)]$ τότε

$$[(x, y)] < [(z, w)].$$

Από τον ορισμό της σχέσης $<$ έχουμε ότι

$$ad < bc \text{ και } bd > 0 \text{ ή } ad > bc \text{ και } bd < 0.$$

1. Υποθέτουμε ότι $ad < bc$ και $bd > 0$. Διακρίνουμε δύο (υπο)περιπτώσεις:

   i_1. $yw > 0$ και

   i_2. $yw < 0$.

2. Υποθέτουμε ότι $ad > bc$ και $bd < 0$. Διακρίνουμε δύο (υπο)περιπτώσεις:

   ii$_1$. $yw > 0$ και

   ii$_2$. $yw < 0$.

Θα ασχοληθούμε με την i$_1$.. Δηλαδή έχουμε ως υπόθεση

$$ad < bc,\ bd > 0 \text{ και } yw > 0.$$

Από την σχέση $ad < bc$, πολλαπλασιάζοντας και τα δύο μέλη με τον θετικό ακέραιο $yw > 0$, έχουμε ότι

$$adyw < bcwy$$

(και αναδιατάσσοντας τους παράγοντες)

$$(ay)(dw) < (cw)(by).$$

Οπότε, από την $(*)$ έχουμε

$$(bx)(dw) < (zd)(by),$$

οπότε (αναδιατάσσοντας τους παράγοντες) έχουμε

$$(bd)(xw) < (bd)(yz),$$

αλλά $bd > 0$. Επομένως

$$xw < yz,$$

δηλαδή (δεδομένου ότι $yw > 0$)

$$[(x, y)] < [(z, w)].$$

Παρομοίως αντιμετωπίζονται και οι υπόλοιπες περιπτώσεις. ό.έ.δ.

Έστω $[(a, b)] \in \mathbb{Q}$, τότε θα συμβολίζουμε

$$-[(a, b)] = [(-a, b)].$$

Επίσης, αν $\hat{0} \neq [(a, b)] \in \mathbb{Q}$, τότε θα συμβολίζουμε

$$([(a, b)])^{-1} = [(b, a)].$$

Εδώ πρέπει να παρατηρήσουμε ότι, επειδή $\hat{0} \neq [(a, b)] \in \mathbb{Q}$, έχουμε ότι ο

$$([(a, b)])^{-1} = [(b, a)]$$

ορίζεται καλώς (ιδέ τον Ορισμό των ρητών αριθμών).

Στο επόμενο Θεώρημα περιλαμβάνονται οι κυριότερες ιδιότητες των ρητών αριθμών.

Θεώρημα 6.2.4. *Έστω $r, s, t \in \mathbb{Q}$, τότε ισχύουν τα ακόλουθα.*

1. $(r + s) + t = r + (s + t)$ *(Η προσεταιριστική ιδιότητα της πρόσθεσης στους ρητούς).*
2. $r + s = s + r$ *(Η πρόσθεση των ρητών είναι μεταθετική).*

3. $r + \hat{0} = r$ *(Η πρόσθεση έχει ουδέτερο).*
4. $r + (-r) = \hat{0}$ *(Κάθε ρητός αριθμός έχει αντίθετο ως προς την πρόσθεση).*
5. $(r \cdot s) \cdot t = r \cdot (s \cdot t)$ *(Η προσεταιριστική ιδιότητα του πολλαπλασιασμού στους ακεραίους).*
6. $r \cdot s = s \cdot t$ *(Ο πολλαπλασιασμός των ρητών είναι μεταθετικός).*
7. $r \cdot \hat{1} = r$ *(Ο πολλαπλασιασμός έχει ουδέτερο).*
8. *Αν* $r \neq \hat{0}$, *τότε* $r \cdot r^{-1} = \hat{1}$ *(Κάθε ρητός αριθμός, διάφορος του μηδενός, έχει αντίστροφο).*
9. $r \cdot (s + t) = r \cdot s + r \cdot t$ *(Η επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση στους ρητούς).*
10. $r \cdot \hat{0} = \hat{0}$.
11. *Ισχύει ακριβώς μια από τις σχέσεις* $r < s$, $r = s$, $r > s$ *(Ο νόμος της τριχοτομίας στους ρητούς).*
12. *Αν* $r < s$ *και* $s < t$, *τότε* $r < t$ *(Η μεταβατική ιδιότητα της διάταξης στους ρητούς).*
13. *Αν* $r \leq s$ *και* $s \leq r$, *τότε* $r = s$
14. *Αν* $r < s$, *τότε* $r + t < s + t$.
15. *Αν* $r < s$ *και* $t > 0$, *τότε* $rt < st$.
16. $\hat{0} \neq \hat{1}$ *(Το σύνολο των ρητών έχει τουλάχιστον δύο στοιχεία).*

Απόδειξη. Η απόδειξη όλων των ανωτέρω στηρίζεται στον ορισμό των ρητών μέσω των ακεραίων αριθμών. Οπότε, "μεταβαίνουμε" στους ακεραίους αριθμούς και επικαλούμαστε το Θεώρημα 6.1.6.

Εδώ θα αποδείξουμε μόνο την (8), αφήνοντας τις υπόλοιπες ως άσκηση.

Έστω $r = [(a, b)] \in \mathbb{Q}$ με $r \neq \hat{0}$, τότε $a \neq 0$. Επομένως, για τον ρητό αριθμό

$$r^{-1} = [(b, a)] \in \mathbb{Q}$$

έχουμε ότι

$$r \cdot r^{-1} = [(a, b)] \cdot [(b, a)] = [(ab, ba)] = \hat{1}. \qquad \text{ό.έ.δ.}$$

Παρατηρήσεις 6.2.5.

1. Από τα προηγούμενα έπεται ότι η σχέση $\leq$ στους ρητούς αριθμούς είναι σχέση ολικής διάταξης.
2. Στο Πέμπτο κεφάλαιο (σελ. 212) είχαμε αναφέρει, ως παράδειγμα, ότι το σύνολο των ρητών $(\mathbb{Q}, +, \cdot)$, εφοδιασμένο με τις πράξεις της πρόσθεσης και του πολλαπλασιασμού, είναι σώμα. Εδώ αποδείξαμε ότι πράγματι αυτό ισχύει. Μάλιστα δε αποδείξαμε κάτι περισσότερο. Η σχέση της διάταξης στους ρητούς αριθμούς είναι "συμβιβαστή" με τις πράξεις της πρόσθεσης και του πολλαπλασιασμού (συμβιβαστή υπό την έννοια των ιδιοτήτων (14) και (15) του προηγουμένου θεωρήματος). Δηλαδή πρόκειται για ένα **διατεταγμένο σώμα**.

3. Αν και το Θεώρημα 6.1.6, το οποίο αναφέρεται σε ιδιότητες των ακεραίων, με το Θεώρημα 6.2.4, το οποίο αναφέρεται σε ιδιότητες των ρητών, παρουσιάζουν πολλές *ομοιότητες*, τα δύο σύνολα των ακεραίων και των ρητών παρουσιάζουν ουσιώδεις διαφορές.

   Για παράδειγμα, τα μόνα αντιστρέψιμα (ως προς τον πολλαπλασιασμό) στοιχεία στον δακτύλιο των ακεραίων είναι το 1 και το -1, ενώ κάθε μη μηδενικός ρητός αριθμός έχει αντίστροφο.

4. Στην Πρόταση 6.1.10 είχαμε αποδείξει ότι το σύνολο των ακεραίων αριθμών είναι διακριτό. Επίσης, είχαμε αποδείξει ότι κάθε κάτω φραγμένο υποσύνολο των ακεραίων αριθμών έχει ελάχιστο στοιχείο (ιδέ την Πρόταση 6.1.12).

   Οι δύο αυτές ιδιότητες δεν ισχύουν στους ρητούς αριθμούς.

Πριν εντρυφήσουμε περισσότερο στην τελευταία παρατήρηση, θα δούμε πώς σε κάθε ακέραιο μπορούμε να αντιστοιχίσουμε έναν μοναδικό ρητό αριθμό και με αυτόν τον τρόπο να θεωρούμε τους ακεραίους αριθμούς ως υποσύνολο των ρητών.

Επίσης, θα δούμε πώς τα κλάσματα, με τα οποία είχαμε ασχοληθεί, περισσότερο διαισθητικά, κατά τα σχολικά μας χρόνια, τώρα μπορούν να ορισθούν αυστηρά και με αυτά πλέον να παριστάνουμε τους ρητούς αριθμούς.

Πρόταση 6.2.6. *Έστω η απεικόνιση* $i : \mathbb{Z} \longrightarrow \mathbb{Q}$ *με*

$$i(x) = [(x, 1)],$$

για όλα τα $x \in \mathbb{Z}$.

1. *Η* i *είναι 1-1.*
2. $i(0) = \hat{0}$ *και* $i(1) = \hat{1}$.
3. *Έστω* $x, y \in \mathbb{Z}$. *Ισχύουν τα ακόλουθα:*
   (α) $i(x + y) = i(x) + i(y)$.
   (β) $i(-x) = -i(y)$.
   (γ) $i(x \cdot y) = i(x) \cdot i(y)$.
   $x < y$, *αν και μόνο αν* $i(x) < i(y)$.
4. *Για κάθε* $r \in \mathbb{Q}$ *υπάρχουν* $x, y \in \mathbb{Z}$ *με* $y \neq 0$, *ώστε*

$$r = i(x) \cdot (i(y))^{-1}.$$

Απόδειξη. Θα αποδείξουμε μόνο το (4), αφήνοντας τα υπόλοιπα ως άσκηση.

Από τον ορισμό των ρητών αριθμών, υπάρχουν $x, y \in \mathbb{Z}$ με $y \neq 0$, ώστε

$$r = [(x, y)].$$

Από τον ορισμό της απεικόνισης i έχουμε ότι

$$i(x) = [(x, 1)] \text{ και } i(y) = [(y, 1)].$$

Από τον ορισμό του πολλαπλασιασμού στους ρητούς και του αντιστρόφου ενός ρητού έχουμε:

$$i(x) \cdot (i(y))^{-1} = [(x, 1)] \cdot [(1, y)] = [(x \cdot 1, 1 \cdot y)] = [(x, y)] = r \text{ [11]}. \qquad \text{ό.έ.δ.}$$

[11] Ερώτηση: Τα $x, y \in \mathbb{Z}$, που ικανοποιούν τις απαιτήσεις του ισχυρισμού είναι μοναδικά; Δοθέντος ενός ρητού r, μπορούμε να υπολογίσουμε όλα τα $x, y \in \mathbb{Z}$ με $y \neq 0$, ώστε $r = i(x) \cdot (i(y))^{-1}$;

Κάθε ρητός αριθμός (Ορισμός 6.2.2) είναι μια κλάση ισοδυναμίας

$$[(a, b)], \text{ με } a, b \in \mathbb{Z} \text{ και } b \neq 0.$$

Θα συμβολίζουμε τον ρητό αριθμό ως

$$a/b =: [(a, b)]$$

και θα τον ονομάζουμε το **κλάσμα** με αριθμητή τον a και παρονομαστή τον b.

Έστω δύο ίσοι ρητοί αριθμοί $[(a, b)] = [(c, d)]$. Αυτό σημαίνει ότι τα ζεύγη των ακεραίων (a, b) και (c, d) είναι ισοδύναμα, ενώ τα κλάσματα a/b και c/d είναι *ίσα* [12].

Αντίστροφα, έστω (a, b) ένα ζεύγος ακεραίων αριθμών με τον $b \neq 0$, τότε ορίζεται ο μοναδικός ρητός αριθμός a/b.

Δηλαδή η απεικόνιση $\varphi : \mathbb{Z} \times \mathbb{Z}^* \longrightarrow \mathbb{Q}$ με

$$(a, b) \xrightarrow{\varphi} a/b$$

δεν είναι τίποτε άλλο από την φυσική απεικόνιση (ιδέ Παράδειγμα 4.5.11).

Αυτά συνάδουν με το (4) της προηγουμένης πρότασης.

Εδώ πρέπει να επισημάνουμε ότι, αν έχουμε έναν ρητό αριθμό $[(a, b)]$, τότε υπάρχει μοναδικό ζεύγος (c, d) ακεραίων αριθμών με την ιδιότητα

$$\text{μ.κ.δ. } (c, d) = 1 \text{ και } [(a, b)] = [(c, d)] \text{ (γιατί;)}.$$

Στην περίπτωση αυτή το κλάσμα c/d θα ονομάζεται **ανάγωγο**.

Επίσης, αν έχουμε τους ρητούς αριθμούς r, s με $r \neq 0$, τότε, πολλές φορές, το γινόμενο $r^{-1} \cdot s$ θα το συμβολίζουμε και ως

$$\frac{s}{r}$$

δηλαδή έχουμε ένα *σύνθετο κλάσμα*.

Έχοντας τον συμβολισμό των ρητών αριθμών ως κλάσματα μπορούμε να αναδιατυπώσουμε τους γνωστούς ορισμούς και ιδιότητες των ρητών υπό μορφήν πρότασης.

Πρόταση 6.2.7. *Έστω $a, c \in Z$ και $b, d \in \mathbb{Z}^*$.*

1. $\frac{a}{b} = \frac{c}{d}$, *αν και μόνο αν* $ad = bc$.
2. $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$.
3. $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.
4. *Αν* $a \neq 0$, *τότε* $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.
5. *Αν* $bd > 0$, *τότε* $\frac{a}{b} < \frac{c}{d}$, *αν και μόνο αν* $ad < bc$.
   Αν $bd < 0$, *τότε* $\frac{a}{b} < \frac{c}{d}$, *αν και μόνο αν* $ad > bc$.

[12] Καταχρηστικώς έχει επικρατήσει να μιλάμε για ισοδύναμα κλάσματα.
Εδώ βλέπουμε ότι: *Ποτέ ο παρανομαστής ενός κλάσματος δεν είναι ίσος με το μηδέν.*

6. *Αν* $k \in \mathbb{Z}$, *τότε μέσω της απεικόνισης* i (*ιδέ Πρόταση* 6.2.1) *ο* k *ταυτοποιείται με το κλάσμα* $k/1$.

7. *Αν* $a \neq 0$, *τότε* $\dfrac{c/d}{a/b} = \dfrac{cb}{da}$.

Οπότε, εις το εξής θα χρησιμοποιούμε τους ρητούς (τα κλάσματα) όπως έχουμε μάθει *από το Δημοτικό*.

Επανερχόμαστε στην Παρατήρηση $6.2.5_4$.

Πρόταση 6.2.8. [13] *Έστω* $r, s \in Q$ *με* $r < s$. *Υπάρχει* $x \in \mathbb{Q}$, *ώστε*

$$r < x < s.$$

Απόδειξη. Υπάρχουν πολλοί τρόποι για να αποδείξουμε τον ισχυρισμό.

Θα παρουσιάσουμε αυτόν που υπαγορεύει η διαίσθησή μας.

Θα δείξουμε ότι "ανάμεσα" στους r και s βρίσκεται ο ρητός αριθμός

$$x = \frac{(r+s)}{2}.$$

Πράγματι, από την υπόθεση $r < s$ έπεται ότι

$$r + r < r + s,$$

δηλαδή

$$2r < r + s,$$

οπότε

$$r < 2^{-1}(r+s) = \frac{(r+s)}{2}.$$

Όμοια αποδεικνύεται ότι

$$x = \frac{(r+s)}{2} < s.$$ ό.έ.δ.

6.2.1 Ασκήσεις

1. Να αποδείξετε την Πρόταση 6.2.1.
2. Να ολοκληρώσετε την απόδειξη της Πρότασης 6.2.3.
3. Να ολοκληρώσετε την απόδειξη του Θεωρήματος 6.2.4.
4. Να ολοκληρώσετε την απόδειξη της Πρότασης 6.2.6.
5. Έστω $s \in \mathbb{Q}$ και $A = \{x \in \mathbb{Q} \mid s < x\}$. Δείξτε ότι δεν υπάρχει $m \in A$, ούτως ώστε $m \leq x$, για όλα τα $x \in A$. Δηλαδή, αν και το σύνολο A είναι κάτω φραγμένο δεν έχει ελάχιστο στοιχείο.
6. i. Έστω $r, s \in \mathbb{Q}$ με $s > 0$. Δείξτε ότι υπάρχει φυσικός αριθμός n, ούτως ώστε

$$r < n \cdot s$$ [14].

[13] Η ιδιότητα αυτή των ρητών αναφέρεται ως: *Το σύνολο των ρητών αριθμών είναι πυκνό (ως προς τον εαυτό του).*

[14] Η ιδιότητα αυτή είναι γνωστή ως η "Αρχιμήδεια ιδιότητα" του σώματος των ρητών αριθμών.

Στην ειδική περίπτωση όπου $s = 1$, έχουμε $r < n$. Η ιδιότητα αυτή αναφέρεται ως: *Το σύνολο των φυσικών αριθμών (ως υποσύνολο των ρητών) είναι ομοτελικό με το (υπερ)σύνολο των ρητών αριθμών.*

ii. Έστω $r \in \mathbb{Q}$ με $r > 0$. Δείξτε ότι υπάρχει θετικός ακέραιος αριθμός n, ούτως ώστε

$$1/n < r.$$

7. Έστω $r, s, t \in \mathbb{Q}$. Υποθέτουμε ότι $r < s \cdot t$, δείξτε ότι υπάρχουν $r_1, r_2 \in \mathbb{Q}$ με

$$r_1 < s,\ r_2 < t \text{ και } r = r_1 \cdot r_2.$$

8. i. Έστω $r, s \in \mathbb{Q}$ με $r > 0$ και $s > 0$. Υποθέτουμε ότι $r^2 < s$. Δείξτε ότι υπάρχει θετικός ακέραιος k, ούτως ώστε

$$\left(r + \frac{1}{k}\right)^2 < s.$$

ii. Έστω $t, u \in \mathbb{Q}$ με $t > 0$ και $u > 0$. Υποθέτουμε ότι $t^2 > u$. Δείξτε ότι υπάρχει θετικός ακέραιος m, ούτως ώστε

$$t - \frac{1}{m} > 0 \text{ και } \left(t - \frac{1}{m}\right)^2 > u.$$

9. Πόσοι ρητοί αριθμοί $\frac{r}{s}$ υπάρχουν, οι οποίοι πληρούν τις συνθήκες

$$\text{μ.κ.δ. } (r, s) = 1 \text{ και } 0 \leq r < s \leq n,$$

για δοθέντα θετικό ακέραιο n;

Βιβλιογραφία

[1] E.D. Bloch. *The Real Numbers and Real Analysis*. Springer, 2011. ISBN: 978-03-8772-176-7.

[2] Joseph A. Gallian. *Contemporary Abstract Algebra*. Seventh Edition. Brooks/Cole, 2009. ISBN: 978-05-4716-509-7.

[3] Thomas W. Judson. *Abstract Algebra Theory and Applications*. Version 1.2, November. Copyright 2000,2001,2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA, 2002.

[4] I. Niven, H. Zuckerman και H. Montgomery. *An Inroduction to the theory of Numbers*. John Wiley και Sons, Inc., 1991.

[5] Στυλιανός Ανδρεαδάκης. *Εισαγωγή στην Άλγεβρα*. Εκδόσεις Συμμετρία, 1993.

ΚΕΦΑΛΑΙΟ 7

ΤΟ ΣΩΜΑ ΤΩΝ ΠΡΑΓΜΑΤΙΚΩΝ ΚΑΙ ΤΟ ΣΩΜΑ ΤΩΝ ΜΙΓΑΔΙΚΩΝ ΑΡΙΘΜΩΝ

7.1 Το σώμα των πραγματικών αριθμών

Στα προηγούμενα κεφάλαια κάναμε χρήση, κατά κόρον, των πραγματικών αριθμών, βασιζόμενοι στην "εμπειρία μας" και την διαίσθησή μας, χωρίς ιδιαίτερα προβλήματα. Η προσέγγιση ήταν διαισθητική, αλλά αυτό δεν μας εμπόδιζε στην χρήση τους.

Αυτό δεν σημαίνει ότι δεν είναι αναγκαίο να προσπαθήσουμε να ορίσουμε τους πραγματικούς αριθμούς αυστηρώς Μαθηματικά.

Υπάρχουν πολλοί τρόποι για μια αξιωματική θεμελίωση των πραγματικών αριθμών.

Ένας τρόπος είναι να τους ορίσουμε αξιωματικά θέτοντας νέα αξιώματα. Οπότε, να πάρουμε, κατά φυσιολογικό τρόπο (υπό μιαν έννοια), ως υποσύνολα το σύνολο των ρητών αριθμών, το σύνολο των ακεραίων αριθμών και το σύνολο των φυσικών αριθμών με όλες τις γνωστές ιδιότητες.

Στο προηγούμενο κεφάλαιο ορίσαμε τους ακεραίους αριθμούς, *επεκτείνοντας* το σύνολο των φυσικών αριθμών. Μάλιστα δε είχαμε επισημάνει ότι οι ακέραιοι αριθμοί θα μπορούσαν να ορισθούν αξιωματικά *παρακάμπτοντας* τους φυσικούς αριθμούς (ιδέ Παρατήρηση 6.1.13). Κατόπιν ορίσαμε τους ρητούς αριθμούς *επεκτείνοντας* το σύνολο των ακεραίων αριθμών.

Έχοντας ορίσει τους ρητούς αριθμούς, ένας άλλος τρόπος για να ορίσουμε τους πραγματικούς αριθμούς, είναι να *επεκτείνουμε* τους ρητούς αριθμούς με έναν "κατάλληλο" τρόπο[1].

Ο πρώτος τρόπος είναι άμεσος, αλλά, κατά την γνώμη μας, σε ένα εισαγωγικό μάθημα στερεί από τον αναγνώστη αυτό που διαισθητικά έχει συνηθίσει (οι φυσικοί

[1] Δεν είναι ο μόνος τρόπος για να ορισθούν οι πραγματικοί αριθμοί μέσω των ρητών αριθμών. Για παράδειγμα, θα μπορούσαν να ορισθούν μέσω των ακολουθιών Cauchy. Αλλά, ο σκοπός μας δεν είναι αυτός.

αριθμοί, οι ακέραιοι αριθμοί, οι ρητοί αριθμοί,...οι πραγματικοί αριθμοί).

Ο δεύτερος τρόπος "ρέει φυσιολογικότερα", κατά την γνώμη μας, και αυτόν θα ακολουθήσουμε εδώ.

Πάντως, όποιον τρόπο και να ακολουθήσει κάποιος,...καταλήγει στο "κατώφλι" του σημαντικού κλάδου των Μαθηματικών, την Πραγματική Ανάλυση.

Πριν προχωρήσουμε, στην κατασκευή των πραγματικών αριθμών από τους ρητούς αριθμούς, θα αναφέρουμε κάποιους λόγους, για τους οποίους οι ρητοί αριθμοί δεν μας *επαρκούν*.

Ένας λόγος, για να επεκτείνουμε το σύνολο των ακεραίων αριθμών στο σύνολο των ρητών αριθμών, ήταν ότι ένας μη μηδενικός ακέραιος (εκτός του 1 και -1) δεν είχε αντίστροφο ως προς τον πολλαπλασιασμό.

Ένας λόγος (θα έλεγε κάποιος) για να επεκτείνουμε το σύνολο των ρητών στο σύνολο των πραγματικών αριθμών είναι ότι πολυώνυμα με ρητούς συντελεστές δεν έχουν ρητές ρίζες, αλλά έχουν πραγματικές ρίζες. Για παράδειγμα, το πολυώνυμο $x^2 - 2$ δεν έχει ρητές ρίζες, αλλά έχει πραγματικές ρίζες. Αλλά δεν λύνεται πλήρως αυτό το πρόβλημα, δεδομένου ότι το πολυώνυμο $x^2 + 2$ δεν έχει πραγματικές ρίζες.

Πέραν αυτού του λόγου υπάρχουν σημαντικότεροι λόγοι, τους οποίους θα δούμε σε λίγο. Εδώ θα αναφέρουμε αυτό που διαισθητικά, ίσως, αντιλαμβανόμαστε. Στο σύνολο των ρητών υπάρχουν "χάσματα" μεταξύ των στοιχείων του, τα οποία έρχονται να "πληρώσουν" οι πραγματικοί αριθμοί.

Αυτό θα γίνει σαφές με την κατασκευή των πραγματικών αριθμών, χρησιμοποιώντας την έννοια των *τομών Dedekind*, οι οποίες, παρ' ότι την ονομασία τους, είναι υποσύνολα των ρητών αριθμών (και όχι τομές συνόλων).

Οι τομές Dedekind.

Πριν ορίσουμε αυστηρά τις τομές Dedekind, ας κάνουμε μια διαισθητική προσέγγιση.

Όταν κατασκευάσαμε τους ακεραίους αριθμούς από τους φυσικούς αριθμούς, ήταν αρκετό να πάρουμε ζεύγη των φυσικών αριθμών και μεταξύ τους να ορίσουμε μια σχέση ισοδυναμίας. Όμοια, όταν κατασκευάσαμε τους ρητούς αριθμούς από τους ακεραίους, ήταν αρκετό να πάρουμε ζεύγη ακεραίων αριθμών και μεταξύ τους να ορίσουμε μια σχέση ισοδυναμίας. Στην κατασκευή των πραγματικών αριθμών από τους ρητούς αριθμούς δεν "επαρκούν" (όπως θα δούμε) τα ζεύγη των ρητών αριθμών. Αντί ζευγών, θα πάρουμε *κατάλληλα* υποσύνολα των ρητών αριθμών.

Η ιδέα είναι απλή. Σε κάθε πραγματικό αριθμό θα αντιστοιχίσουμε ένα υποσύνολο των ρητών αριθμών. Για παράδειγμα, στον (πραγματικό) αριθμό 1 αντιστοιχούμε το υποσύνολο

$$S_1 = \{ x \in \mathbb{Q} \mid x < 1 \}$$

και στον πραγματικό αριθμό $\sqrt{2}$ αντιστοιχούμε το σύνολο

$$S_{\sqrt{2}} = \{ x \in \mathbb{Q} \mid x < \sqrt{2} \}.$$

Οπότε, θα έλεγε κάποιος, γενικά σε κάθε πραγματικό αριθμό r αντιστοιχούμε το σύνολο

$$S_r = \{ x \in \mathbb{Q} \mid x < r \}$$

και θα μπορούσαμε να γράψουμε για το σύνολο $\mathbb{R}$ των πραγματικών αριθμών την εξής "ταυτοποίηση"

$$\mathbb{R} = \{ S_r \mid r \in \mathbb{R} \}.$$

Στην πραγματικότητα **δεν** κάναμε τίποτε, διότι δεν έχουμε ορίσει ακόμη τους πραγματικούς αριθμούς και δεν πρέπει να τους επικαλούμαστε για να τους ορίσουμε. Παρ' όλα ταύτα, το πρωθύστερο, που παρουσιάσαμε, μας "οδηγεί" στο πώς θα ορίσουμε τους πραγματικούς αριθμούς.

Ορισμός 7.1.1. Έστω A ένα υποσύνολο των ρητών αριθμών. Το A θα ονομάζεται **τομή Dedekind**, αν ισχύει ότι:

i. Το A είναι μη κενό και γνήσιο υποσύνολο των ρητών ($\varnothing \neq A \neq \mathbb{Q}$).

ii. Το A είναι "καθοδικά κλειστό". Δηλαδή, αν $x \in A$ και $y \in \mathbb{Q}$ με $y \leq x$, τότε $y \in A$.

iii. Το A δεν έχει μέγιστο στοιχείο. Δηλαδή, δεν υπάρχει $y \in A$ με $y \geq x$, για όλα τα $x \in A$ (ισοδύναμα, για κάθε $x \in A$ υπάρχει $y \in A$ με $x < y$)[2].

Έτσι που τίθεται ο προηγούμενος ορισμός, δεν είναι προφανές ότι υπάρχουν τομές Dedekind.

Παράδειγμα 7.1.2. Έστω $r \in \mathbb{Q}$. Το σύνολο

$$D_r = \{ x \in \mathbb{Q} \mid x < r \}$$

είναι τομή Dedekind.

1. Είναι μη κενό και γνήσιο υποσύνολο του $\mathbb{Q}$ (γιατί;).

2. Έστω $x \in D_r$, τότε $x < r$. Έστω ότι $y \in \mathbb{Q}$ με $y < x$, τότε $y < x < r$. Συνεπώς, $y < r$ και επομένως $y \in D_r$.

3. Έστω $x \in D_r$ τότε $x < \dfrac{x+r}{2} < r$ (γιατί;), συνεπώς $y = \dfrac{x+r}{2} \in D_r$.

Το προηγούμενο παράδειγμα μας δείχνει ότι ο προηγούμενος ορισμός δεν είναι κενός περιεχομένου, αλλά παραμένει το ερώτημα, αν οι μόνες τομές Dedekind είναι της ανωτέρω μορφής.

Αν οι μόνες τομές Dedekind ήταν αυτές, που περιγράφονται στο προηγούμενο παράδειγμα, δεν θα χρειαζόταν ο (φαινομενικά) τεχνητός Ορισμός 7.1.1.

Παράδειγμα 7.1.3. Έστω

$$S = \{ x \in \mathbb{Q},\, x < 0 \mid x^2 > 2 \}.$$

Το σύνολο S είναι τομή Dedekind.

Είναι εύκολο να δούμε ότι πληρούνται οι δύο πρώτες προϋποθέσεις του Ορισμού 7.1.1.

Εδώ θα ελέγξουμε, αν ισχύει η τρίτη προϋπόθεση. Έστω $x \in S$, τότε

$$x < 0 \text{ και } x^2 > 2.$$

[2] Στην συνέχεια θα χρησιμοποιούμε, κατά κόρον, τις έννοιες μέγιστο/ελάχιστο στοιχείο, φραγμένο/μη φραγμένο σύνολο κ.λ.π.. Για την σχετική ορολογία και ιδιότητες παραπέμπουμε στην Παράγραφο 4.4.3.

Θέτουμε $t = -x > 0$, τότε $t^2 > 2$ (γιατί;). Παρατηρούμε ότι μπορούμε να επικαλεσθούμε την Άσκηση 6.2.1$_{7ii}$. Οπότε υπάρχει m θετικός ακέραιος, ώστε

$$t - \frac{1}{m} > 0 \text{ και } \left(t - \frac{1}{m}\right)^2 > 2.$$

Αλλά $t = -x$, οπότε για

$$y = x + \frac{1}{m} = -\left(t - \frac{1}{m}\right) < 0$$

έχουμε ότι $y > x$ και

$$y^2 = \left(x + \frac{1}{m}\right)^2 = \left(-\left(t - \frac{1}{m}\right)\right)^2 = \left(t - \frac{1}{m}\right)^2 > 2.$$

Επομένως, $y \in S$, δηλαδή το S δεν έχει μέγιστο στοιχείο και συνεπώς το S είναι τομή Dedekind.

Επίσης, δεν υπάρχει $r \in \mathbb{Q}$ με

$$S = \{x \in \mathbb{Q}, x < 0 \mid x^2 > 2\} = D_r = \{x \in \mathbb{Q} \mid x < r\} \text{ (γιατί;)}.$$

Ως απάντηση του προηγουμένου (γιατί;). Αν υπήρχε ένας ρητός $r \in \mathbb{Q}$, ώστε

$$S = \{x \in \mathbb{Q}, x < 0 \mid x^2 > 2\} = D_r = \{x \in \mathbb{Q} \mid x < r\},$$

τότε είναι εύκολο να δούμε ότι ο r θα έπρεπε να πληροί την σχέση $r^2 = 2$. Αλλά έχουμε δει (Θεώρημα 3.2.8) ότι δεν υπάρχει ρητός, ώστε $r^2 = 2$ [3].

Επομένως, υπάρχουν τομές Dedekind, οι οποίες δεν είναι της μορφής του πρώτου παραδείγματος. Συγκεκριμένα, θα μπορούσαμε να διακρίνουμε δύο είδη: Τις ρητές, της μορφής

$$D_r = \{x \in \mathbb{Q} \mid x < r\},$$

για $r \in \mathbb{Q}$ και όλες τις υπόλοιπες (άρρητες) τομές.

Οπότε, διαισθητικά, οι ρητές τομές αντιστοιχούν στους ρητούς αριθμούς (όταν θεωρηθούν ως υποσύνολο των πραγματικών) και οι άρρητες στους υπολοίπους πραγματικούς αριθμούς, οι οποίοι έρχονται να "πληρώσουν" τα "χάσματα", που αφήνουν οι ρητοί αριθμοί. Για παράδειγμα, η τομή Dedekind στο Παράδειγμα 7.1.3 διαισθανόμαστε ότι αντιστοιχεί στον πραγματικό αριθμό $-\sqrt{2}$.

Πρόταση 7.1.4. *Έστω $A \subseteq \mathbb{Q}$ μια τομή Dedekind. Για το (συνολοθεωρητικό) συμπλήρωμα*

$$\mathbb{Q} \setminus A = \{x \in \mathbb{Q} \mid x \notin A\}$$

ισχύουν:

i. $\mathbb{Q} \setminus A = \{x \in \mathbb{Q} \mid x > a \text{ για όλα τα } a \in A\}$.

ii. Έστω $x \in \mathbb{Q} \setminus A$ και $y \in \mathbb{Q}$ με $y \geq x$, τότε $y \in \mathbb{Q} \setminus A$.

Απόδειξη.

[3] Εδώ, προς αποφυγή σύγχυσης, πρέπει να επισημάνουμε ότι στο Θεώρημα 3.2.8 είχαμε δεχθεί την ύπαρξη του πραγματικού αριθμού $\sqrt{2}$, αλλά εκεί ο σκοπός μας ήταν η παρουσίαση της αποδεικτικής διαδικασίας, δια της εις άτοπον απαγωγή.

i. Έστω $x \in \mathbb{Q} \setminus A$ και $a \in A$. Γνωρίζουμε ότι για τους ρητούς αριθμούς x και a, από τις σχέσεις $a = x$ ή $x < a$ ή $x > a$, μόνο μια ισχύει (ο νόμος της τριχοτομίας στους ρητούς αριθμούς). Οι δύο πρώτες περιπτώσεις δεν είναι δυνατόν να ισχύουν (γιατί; από τον ορισμό του συμπληρώματος και το ii. του Ορισμού 7.1.1). Συνεπώς

$$\mathbb{Q} \setminus A \subseteq \{ x \in \mathbb{Q} \mid x > a \text{ για όλα τα } a \in A \}.$$

Προφανώς ισχύει και η αντίστροφη κατεύθυνση

$$\mathbb{Q} \setminus A \supseteq \{ x \in \mathbb{Q} \mid x > a \text{ για όλα τα } a \in A \}$$

(γιατί; μα δεν είναι δυνατόν για έναν ρητό αριθμό y να ισχύει $y < y$).

ii. Είναι άμεση συνέπεια του i. και αφήνεται ως άσκηση (Άσκηση $7.1.1_1$). ό.έ.δ.

Όπως βλέπουμε, το συμπλήρωμα μιας τομής Dedekind δεν είναι τομή Dedekind.

Πρόταση 7.1.5. ***(Ο νόμος της τριχοτομίας)*** *Έστω $A, B \subseteq \mathbb{Q}$ τομές Dedekind. Τότε ακριβώς μια από τις περιπτώσεις $A \subset B$, $A = B$, $B \subset A$ ισχύει.*

Απόδειξη. Προφανώς το πολύ μια από τις παραπάνω περιπτώσεις μπορεί να ισχύει. Πρέπει να δείξουμε ότι ισχύει τουλάχιστον μια.

Υποθέτουμε ότι οι δύο πρώτες δεν ισχύουν. Δηλαδή $A \not\subseteq B$. Αυτό σημαίνει ότι υπάρχει $a \in A$ με $a \notin B$, δηλαδή $a \in \mathbb{Q} \setminus B$. Από την προηγουμένη πρόταση έχουμε ότι $a > b$, για όλα τα $b \in B$. Το σύνολο A έχει υποτεθεί ότι είναι τομή Dedekind, συνεπώς, εξ' ορισμού, είναι καθοδικά κλειστό, δηλαδή από την σχέση $a > b$, για όλα τα $b \in B$, έχουμε ότι $b \in A$. Άρα $B \subseteq A$ και, επειδή $A \neq B$, έχουμε $B \subset A$.

Όμοια, αν δεν ισχύουν οι δύο τελευταίες περιπτώσεις, δηλαδή ισχύει $B \not\subseteq A$.

Η περίπτωση, όπου $A \not\subseteq B$ και $B \not\subseteq A$ (με τα ίδια επιχειρήματα) δεν μπορεί να ισχύει. Άρα αναγκαστικά $A = B$. ό.έ.δ.

Πρόταση 7.1.6. *Έστω $\mathcal{S} \subseteq \mathcal{P}(\mathbb{Q})$ ένα (μη κενό) υποσύνολο υποσυνόλων του $\mathbb{Q}$. Υποθέτουμε ότι όλα τα στοιχεία του $\mathcal{S}$ είναι τομές Dedekind, αν η ένωση*

$$B = \bigcup_{A \in \mathcal{S}} A \neq \mathbb{Q},$$

τότε είναι τομή Dedekind.

Απόδειξη. Προφανώς $B \neq \emptyset$ (γιατί;)

Έστω $b \in B$ και $x \in \mathbb{Q}$ με $x \leq b$. Επίσης, υπάρχει ένα $A \in \mathcal{S}$, με $b \in A$, το A έχει υποτεθεί ότι είναι τομή Dedekind, επομένως $x \in A \subseteq B$. Επομένως, για το σύνολο B ικανοποιείται το ii. του Ορισμού 7.1.1.

Έστω $b \in B$, όπως προηγουμένως, υπάρχει ένα $A \in \mathcal{S}$, με $b \in A$, το A έχει υποτεθεί ότι είναι τομή Dedekind, επομένως δεν έχει μέγιστο στοιχείο, δηλαδή υπάρχει $x \in \mathbb{Q}$ με

$$b < x \text{ και } x \in A \subseteq B.$$

Συνεπώς, το σύνολο B δεν έχει μέγιστο στοιχείο και ικανοποιείται το iii. του Ορισμού 7.1.1. ό.έ.δ.

Το σώμα των πραγματικών αριθμών.

Ορισμός 7.1.7. Το υποσύνολο

$$\mathbb{R} = \{A \subseteq \mathbb{Q} \mid \text{όπου } A \text{ είναι τομή Dedekind } \} \subseteq \mathcal{P}(\mathbb{Q})$$

θα ονομάζεται το σύνολο των **πραγματικών αριθμών**.

Όπως έχουμε ήδη επισημάνει, σε αντίθεση με την κατασκευή των ακεραίων από τους φυσικούς αριθμούς και των ρητών από τους ακεραίους αριθμούς, όπου τα στοιχεία τους είναι κλάσεις ισοδυναμίας, στην κατασκευή των πραγματικών αριθμών δεν έχουμε κλάσεις ισοδυναμίας, αλλά απλώς (κατάλληλα) υποσύνολα των ρητών αριθμών.

Ορισμός 7.1.8. Στο σύνολο $\mathbb{R}$ των πραγματικών αριθμών ορίζουμε μια σχέση $\leq$ ως εξής: Έστω $A, B \in \mathbb{R}$, ορίζουμε

$$A \leq B \text{ αν } A \subseteq B$$

και

$$A < B \text{ αν } A \subseteq B \text{ και } A \neq B \text{ [4]}.$$

Πόρισμα 7.1.9. *Το σύνολο* $(\mathbb{R}, \leq)$ *των πραγματικών αριθμών εφοδιασμένο με την σχέση* $\leq$ *είναι ένα ολικά (γραμμικά) διατεταγμένο σύνολο.*

Απόδειξη. Η απόδειξη έχει προηγηθεί, είναι η Πρόταση 7.1.5, με τις λεπτομέρειες να αφήνονται ως άσκηση. ό.έ.δ.

Τώρα θα μπορούσαμε να έχουμε μια πρώτη, διαισθητική, παράσταση των πραγματικών αριθμών ως σημείων μιας ευθείας, όπου σε κάθε σημείο a της ευθείας αντιστοιχούμε το σύνολο όλων των ρητών αριθμών, οι οποίοι βρίσκονται στον αριστερό ανοικτό ημιάξονα $(-\infty, a)$, το οποίο, με την σειρά του, δεν είναι τίποτε άλλο από μια τομή Dedekind A, η οποία, με τη σειρά της αντιστοιχεί στο σημείο a (στον πραγματικό αριθμό a). Οπότε, το συμπλήρωμα $\mathbb{Q} \setminus A$ αντιστοιχεί σε όλους τους ρητούς αριθμούς, οι οποίοι βρίσκονται στον δεξιό ημιανοικτό ημιάξονα $[a, +\infty)$.

Εδώ βλέπουμε ότι, αν το σημείο a αντιστοιχεί σε ρητό αριθμό, τότε η αντίστοιχη τομή Dedekind είναι η ρητή τομή Dedekind

$$D_a = \{x \in \mathbb{Q} \mid x < a\},$$

ενώ αν το a δεν αντιστοιχεί σε ρητό αριθμό, τότε το "χάσμα" αυτό καλύπτεται από την αντίστοιχη (μη ρητή) τομή Dedekind.

Ορισμός 7.1.10. Έστω $\mathcal{B}$ ένα (μη κενό) υποσύνολο των πραγματικών αριθμών.

1. Ένα $A \in \mathbb{R}$ ονομάζεται *άνω φράγμα* του $\mathcal{B}$, αν για κάθε $X \in \mathcal{B}$ ισχύει $X \leq A$.
2. Ένα $B \in \mathbb{R}$ ονομάζεται *κάτω φράγμα* του $\mathcal{B}$, αν για κάθε $B \in \mathcal{B}$ ισχύει $B \leq Y$.

   Αν υπάρχει άνω (αντιστ. κάτω) φράγμα για ένα υποσύνολο $\mathcal{B} \subseteq \mathbb{R}$, τότε το $\mathcal{B}$ θα ονομάζεται *άνω φραγμένο* (αντιστ. *κάτω φραγμένο*).

[4] Απλώς αλλάξαμε τον συμβολισμό στην σχέση του περιέχεσθαι $\subseteq$ μεταξύ συνόλων, δεδομένου ότι αργότερα θα χρησιμοποιούμε τους πραγματικούς αριθμούς, όπως μέχρι τώρα τους *καταλαβαίνουμε* διαισθητικά.

3. Ένα $A \in \mathbb{R}$ ονομάζεται το *ελάχιστο άνω φράγμα* (καλούμενο και **supremum**) του $\mathcal{B}$, αν είναι άνω φράγμα του $\mathcal{B}$ και για κάθε άλλο άνω φράγμα C του $\mathcal{B}$ ισχύει $A \leq C$.

4. Ένα $B \in \mathbb{R}$ ονομάζεται το *μέγιστο κάτω φράγμα* (καλούμενο και **infimum**) του $\mathcal{B}$, αν είναι κάτω φράγμα του $\mathcal{B}$ και για κάθε άλλο κάτω φράγμα D του $\mathcal{B}$ ισχύει $D \leq B$.

5. Στην περίπτωση, όπου το ελάχιστο άνω (αντίστοιχ. μέγιστο κάτω) φράγμα του $\mathcal{B}$ είναι στοιχείο του υποσυνόλου $\mathcal{B}$, τότε το στοιχείο αυτό θα ονομάζεται το μέγιστο (αντίστοιχ. το ελάχιστο) στοιχείο του υποσυνόλου $\mathcal{B}$.

Επισημαίνουμε ότι, ο ανωτέρω ορισμός είναι ο Ορισμός 4.4.17 (προσαρμοσμένος στην περίπτωση των πραγματικών αριθμών).

Πρόταση 7.1.11. *Κάθε μη κενό άνω φραγμένο υποσύνολο $\mathcal{B}$ των πραγματικών αριθμών έχει ελάχιστο άνω φράγμα.*

Απόδειξη. Θεωρούμε το σύνολο

$$\mathcal{A} = \bigcup_{X \in \mathcal{B}} X$$

(προσοχή! τα $X \in \mathbb{R}$, συνεπώς είναι σύνολα). Για κάθε $X \in \mathcal{B}$ έχουμε ότι $X \leq \mathcal{A}$ (γιατί;). Συνεπώς το σύνολο $\mathcal{A} \subseteq \mathbb{Q}$ είναι ένα άνω φράγμα του συνόλου $\mathcal{B}$ (ως προς την σχέση του $\subseteq$ στο $\mathcal{P}(\mathbb{Q})$) και από το Θεώρημα 1.1.18($_4$) έπεται ότι $\mathcal{A} \subseteq Z$ για κάθε $Z \subseteq \mathbb{Q}$ με $X \subseteq Z$. Επομένως, τελειώσαμε(!;!)

Όχι, διότι δεν γνωρίζουμε ότι το $\mathcal{A} \in \mathbb{R}$. Προφανώς το $\mathcal{A}$ είναι μη κενό και επειδή $\mathcal{A} \subseteq Z$ για κάθε $Z \in \mathbb{R}$ με $X \subseteq Z$, έχουμε ότι $\mathcal{A} \neq \mathbb{Q}$ (δεν ξεχνάμε ότι κάθε $Z \in \mathbb{R}$ είναι τομή Dedekind, άρα γνήσιο υποσύνολο του $\mathbb{Q}$). Επομένως, από την Πρόταση 7.1.6 έπεται ότι το σύνολο $\mathcal{A}$ είναι τομή Dedekind, άρα $\mathcal{A} \in \mathbb{R}$. ό.έ.δ.

Ισχύει και η δυϊκή της ανωτέρω πρότασης.

Πρόταση 7.1.12. *Κάθε μη κενό κάτω φραγμένο υποσύνολο $\mathcal{B}$ των πραγματικών αριθμών έχει μέγιστο κάτω φράγμα.*

Απόδειξη. Θεωρούμε το σύνολο

$$U = \{X \in \mathbb{R} \mid X \leq B \text{ για όλα τα } B \in \mathcal{B}\}$$

όλων των κάτω φραγμάτων του συνόλου $\mathcal{B}$. Επομένως, (όλα) τα στοιχεία του συνόλου $\mathcal{B}$ αποτελούν άνω φράγματα για το σύνολο U. Συνεπώς, από την προηγουμένη πρόταση, το σύνολο U έχει ελάχιστο άνω φράγμα έστω C. Άρα $C \leq Y$, για όλα τα $Y \in \mathcal{B}$. Δηλαδή το C είναι ένα κάτω φράγμα του συνόλου $\mathcal{B}$ και ταυτόχρονα ένα ελάχιστο άνω φράγμα του συνόλου U, επομένως ισχύει η σχέση

$$X \leq C \leq Y,$$

για όλα τα $X \in U$ και όλα τα $Y \in \mathcal{B}$. Άρα το C είναι ένα μέγιστο κάτω φράγμα του συνόλου $\mathcal{B}$. ό.έ.δ.

Προφανώς ένα ελάχιστο άνω φράγμα και ένα μέγιστο κάτω φράγμα ενός υποσυνόλου των πραγματικών αριθμών, όταν υπάρχουν, είναι μοναδικά (γιατί;).

Οι δύο προηγούμενες προτάσεις είναι αυτές που καθορίζουν μια θεμελιώδη διαφορά μεταξύ του συνόλου των ρητών αριθμών και του συνόλου των πραγματικών αριθμών και αποτελούν την ***"Αρχή της πληρότητας"*** για τους πραγματικούς αριθμούς.

Για παράδειγμα, το σύνολο

$$S = \{ x \in \mathbb{Q}, \mid x^2 < 2 \} \subseteq \mathbb{Q},$$

είναι άνω και κάτω φραγμένο, ενώ δεν έχει ούτε ελάχιστο άνω φράγμα, ούτε μέγιστο κάτω φράγμα στο $\mathbb{Q}$ (γιατί; ανατρέξτε στην Άσκηση 6.2.1$_8$). Παράβαλλε με την Άσκηση 6.2.1$_5$.

Μια πρώτη αναφορά για ελάχιστο άνω φράγμα (αντίστοιχα μέγιστο κάτω φράγμα) ενός συνόλου έχει γίνει στην Άσκηση 4.4.4$_8$. Αν δεν έχετε ήδη απαντήσει, εφαρμόστε τα επιχειρήματα των δύο προηγουμένων προτάσεων.

Αλγεβρικές ιδιότητες των πραγματικών αριθμών.

Όπως θα δούμε, στο σύνολο των πραγματικών αριθμών μπορούμε να ορίσουμε δύο πράξεις, ως προς τις οποίες αποκτά την δομή ενός σώματος.

Ορισμός 7.1.13. Στο σύνολο των πραγματικών αριθμών $\mathbb{R}$ ορίζουμε μια πρόσθεση ως εξής: Για $A, B \in \mathbb{R}$ ορίζουμε

$$A \oplus B = \{ x + y \mid x \in A, \, y \in B \}.$$

Λήμμα 7.1.14. *Η πράξη της πρόσθεσης είναι καλώς ορισμένη.*

Απόδειξη. Αρκεί να δείξουμε ότι το άθροισμα $A \oplus B$ είναι πραγματικός αριθμός, δηλαδή είναι τομή Dedekind.

1. Το σύνολο $A \oplus B$ είναι γνήσιο υποσύνολο του $\mathbb{Q}$. Πράγματι, επειδή τα A, B είναι τομές Dedekind, Υπάρχουν $r, s \in \mathbb{Q}$ με $r > x$, για όλα τα $x \in A$ και $s > y$, για όλα τα $y \in B$ (ιδέ Πρόταση 7.1.4), επομένως
$$r + s > x + y,$$
για όλα τα $x \in A$, $y \in B$. Επίσης, προφανώς, το σύνολο $A \oplus B$ είναι μη κενό.

2. Έστω $r = x + y \in A \oplus B$ και $p \in \mathbb{Q}$ με $p < r$. Τότε
$$p - x < y \in B$$
και, επειδή το B είναι τομή Dedekind, έχουμε ότι $p - x \in B$. Συνεπώς
$$p = x + (p - x) \in A \oplus B,$$
Δηλαδή, το σύνολο $A \oplus B$ είναι καθοδικά κλειστό.

3. Το σύνολο $A \oplus B$ δεν έχει μέγιστο στοιχείο. Πράγματι, έστω $r = x + y \in A \oplus B$. Τότε, επειδή τα A, B δεν έχουν μέγιστο στοιχείο, υπάρχουν $\bar{x} \in A$ με $x < \bar{x}$ και $\bar{y} \in B$ με $y < \bar{y}$. Επομένως, έχουμε ότι
$$r = x + y < \bar{x} + \bar{y}$$
με $\bar{x} + \bar{y} \in A \oplus B$.

Άρα πράγματι το σύνολο $A \oplus B$ είναι πραγματικός αριθμός. ό.έ.δ.

Από τον τρόπο ορισμού της, η πρόσθεση πραγματικών αριθμών είναι μεταθετική.

Δηλαδή,

$$A \oplus B = B \oplus A,$$

για όλα τα $A, B \in \mathbb{R}$ (γιατί;).

Λήμμα 7.1.15. *Η Πράξη της πρόσθεσης $\oplus$ στους πραγματικούς αριθμούς είναι προσεταιριστική. Δηλαδή, για $A, B, C \in \mathbb{R}$ ισχύει ότι*

$$(A \oplus B) \oplus C = A \oplus (B \oplus C).$$

Απόδειξη. Η απόδειξη είναι προφανής και απορρέει από τον ορισμό της πρόσθεσης στους πραγματικούς αριθμούς (Ορισμός 7.1.13) και το ότι η πράξη της πρόσθεσης στους ρητούς αριθμούς είναι προσεταιριστική. Με τις λεπτομέρειες να αφήνονται ως άσκηση (Άσκηση $7.1.1_2$). ό.έ.δ.

Λήμμα 7.1.16. *Το σύνολο*

$$D_0 = \{ x \in \mathbb{Q} \mid x < 0 \}$$

είναι τομή Dedekind (ιδέ Παράδειγμα 7.1.2) και έχει την ιδιότητα

$$A \oplus D_0 = D_0 \oplus A,$$

για όλα τα $A \in \mathbb{R}$.

Απόδειξη. Έστω $A \in \mathbb{R}$, τότε

$$A \oplus D_0 = \{ x + y \mid x \in A,\ y \in D_0 \},$$

Προφανώς για κάθε $x \in A$ έχουμε ότι $x + y < x$ για όλα τα $y \in D_0$ και επειδή το σύνολο A είναι τομή Dedekind, έχουμε ότι

$$A \oplus D_0 \subseteq A.$$

Έστω $x \in A$, το A δεν έχει μέγιστο στοιχείο, συνεπώς υπάρχει $r \in A$ με $x < r$. Τότε έχουμε $x - r < 0$ και

$$x = r + (x - r) \in A \oplus D_0,$$

δηλαδή

$$A \subseteq A \oplus D_0.$$

Τελικά,

$$A \oplus D_0 = A = D_0 \oplus A.$$ ό.έ.δ.

Δηλαδή το στοιχείο D_0 είναι το (μοναδικό) ουδέτερο της πρόσθεσης στους πραγματικούς αριθμούς (γιατί το ουδέτερο της πρόσθεσης είναι μοναδικό; Ιδέ Πρόταση 5.1.3).

Εφόσον έχουμε εξασφαλίσει την ύπαρξη ουδετέρου, ως προς την πρόσθεση στους πραγματικούς αριθμούς, αναζητούμε, αν για έναν πραγματικό αριθμό A υπάρχει αντίθετος. Δηλαδή, αν υπάρχει $-A \in \mathbb{R}$ με την ιδιότητα:

$$A \oplus (-A) = D_0 = (-A) \oplus A.$$

Προφανώς, αν υπάρχει ένας τέτοιος πραγματικός αριθμός θα είναι μια τομή Dedekind, έστω N, με την ιδιότητα:

$$A \oplus N = \{ x + y \mid x \in A,\ y \in N \} = D_0.$$

Αυτό σημαίνει ότι, αφ' ενός μεν

$$x + y < 0,$$

για όλα τα $x \in A$ και $y \in N$, αφ' ετέρου δε, για κάθε ρητό αριθμό $r < 0$, υπάρχουν $x \in A$ και $y \in N$ με

$$r = x + y.$$

Από την προηγουμένη παρατήρηση έπεται ότι μπορούμε να "εικάσουμε" ποιος θα είναι, αν υπάρχει, ο αντίθετος ενός πραγματικού αριθμού.

Λήμμα 7.1.17. *Έστω $A \in \mathbb{R}$, το σύνολο*

$$-A = \{r \in \mathbb{Q}, \text{ για τα οποία υπάρχει } s \notin A \text{ με } -r > s\}$$

έχει τις εξής ιδιότητες:

i. Είναι τομή Dedekind (άρα πραγματικός αριθμός).

ii. Είναι το αντίθετο του στοιχείου $A \in \mathbb{R}$.

Απόδειξη.

i. Το σύνολο A, ως τομή Dedekind, είναι μη κενό και γνήσιο υποσύνολο του $\mathbb{Q}$, συνεπώς υπάρχει $s \notin A$. Θέτουμε $r = -s-1$, τότε $r < -s$ και επομένως $-r > s$, άρα

$$r \in -A.$$

Συνεπώς, το $-A$ είναι μη κενό.

Έστω $t \in A$ και s ένας ρητός με $-s > -t$, τότε $t > s$. Υποθέτουμε ότι $-t \in -A$, αυτό σημαίνει ότι υπάρχει $s \notin A$ με $-(-t) > s$, δηλαδή $t > s$, αλλά το A είναι τομή Dedekind, το οποίο σημαίνει ότι $s \in A$, άτοπο. Άρα

$$-t \notin -A.$$

Το οποίο αποδεικνύει ότι το $-A$ είναι γνήσιο υποσύνολο του $\mathbb{Q}$.

Έστω $r \in -A$ και $t < r$. Από τον ορισμό του $-A$ υπάρχει ρητός $s \notin A$ με $-r > s$, τότε $t < r < -s$, δηλαδή $-t > s$. Αυτό, πάλι από τον ορισμό του $-A$, σημαίνει ότι

$$t \in -A.$$

Άρα το $-A$ είναι καθοδικά κλειστό.

Έστω $r \in -A$. Από τον ορισμό του $-A$ έχουμε ότι υπάρχει ρητός $s \notin A$ με $-r > s$, τότε έχουμε

$$-r > \frac{-r+s}{2} > s.$$

Αν θέσουμε $-y = \dfrac{-r+s}{2}$, τότε $y > r$ και $-y > s$ με $s \notin A$. Αυτό σημαίνει ότι $y \in -A$. Δηλαδή το $-A$ δεν έχει μέγιστο στοιχείο.

Από όλα τα προηγούμενα έπεται ότι το $-A$ είναι τομή Dedekind.

ii. Θα δείξουμε ότι

$$A \oplus (-A) = D_0.$$

Έστω

$$t = x + y \in A \oplus (-A)$$

με $x \in A$ και $y \in -A$. Τότε, υπάρχει $s \notin A$ με $-y > s$, δηλαδή $y < -s$. Επίσης, ισχύει $x < s$ (γιατί; μα ισχύει η Πρόταση 7.1.4). Επομένως

$$t = x + y < s + (-s) = 0,$$

δηλαδή $t \in D_0$ και συνεπώς $A \oplus (-A) \subseteq D_0$.

Έστω $r \in D_0$, τότε ο $\dfrac{-r}{2}$ είναι θετικός ρητός. Τότε υπάρχει $t \in A$ με

$$\frac{-r}{2} + t \notin A \qquad (*)$$

Θεωρούμε τον ρητό αριθμό $s = \dfrac{-r}{2} + t$ και έχουμε $\dfrac{-r}{2} + s > s$, δηλαδή $-r + t > s$. Αυτό σημαίνει ότι $-(-r + t) \in -\mathrm{A}$, δηλαδή $r - t \in -\mathrm{A}$. Επομένως

$$r = t + (r - t) \in A \oplus (-A).$$

Δηλαδή, $D_0 \subseteq \mathrm{A} \oplus (-\mathrm{A})$. Άρα το ζητούμενο $\mathrm{A} \oplus (-\mathrm{A}) = D_0$;.

Δεν τελειώσαμε, ισχυριστήκαμε ότι ισχύει η σχέση $(*)$. Αυτό χρήζει αποδείξεως, ιδέ Άσκηση $7.1.1_3$. ό.έ.δ.

Προηγουμένως εικάσαμε ποιος είναι ο αντίθετος ενός πραγματικού αριθμού και αποδείξαμε ότι πράγματι έτσι είναι. Αυτό δεν αποκλείει, για έναν πραγματικό αριθμό, να υπάρχουν περισσότεροι του ενός αντίθετοι. Επομένως, πρέπει να αποδείξουμε ότι υπάρχει μοναδικός αντίθετος.

Αυτό όμως έχει ήδη αποδειχθεί, στην γενικότητά του, στην Πρόταση 5.1.7.

Ανακεφαλαιώνοντας, έχουμε το εξής θεώρημα.

Θεώρημα 7.1.18. *Το σύνολο* $(\mathbb{R}, \oplus)$, *εφοδιασμένο με την πράξη της πρόσθεσης, αποτελεί αβελιανή ομάδα.*

Απόδειξη. Η απόδειξη έχει προηγηθεί. ό.έ.δ.

Πόρισμα 7.1.19. *Έστω* A, B, C *πραγματικοί αριθμοί.*

i. $A = B$, *αν και μόνο αν* $A \oplus C = B \oplus C$.

ii. $A \leq B$, *αν και μόνο αν* $A \oplus C \leq b \oplus C$.

iii. $-D_0 = D_0$.

iv. Αν $A < D_0$, *τότε* $D_0 < -A$.

Απόδειξη.

i. Είναι ιδιότητα, η οποία ισχύει για κάθε ομάδα.

ii. Υποθέτουμε ότι $A \leq B$. Αυτό σημαίνει ότι $A \subseteq B$, ως υποσύνολα των ρητών αριθμών. Επίσης, από τον ορισμό της πρόσθεσης έχουμε ότι

$$A \oplus C = \{ x + z \mid x \in A,\ z \in C \} \text{ και } B \oplus C = \{ y + z \mid y \in B,\ z \in C \}.$$

Οπότε, κατά προφανή τρόπο, ισχύει

$$A \oplus C \subseteq B \oplus C.$$

Δηλαδή

$$A \oplus C \leq B \oplus C.$$

Αντίστροφα, υποθέτουμε ότι

$$A \oplus C \leq B \oplus C.$$

Από τον νόμο της τριχοτομίας (Πρόταση 7.1.5) έχουμε ότι

$$A \leq B \text{ ή } B \leq A.$$

Η δεύτερη περίπτωση δεν ισχύει, διότι, τότε από το πρώτο μέρος της απόδειξης θα είχαμε $B \oplus C \leq A \oplus C$. Συνεπώς

$$A \leq B.$$

Εδώ πρέπει να παρατηρήσουμε ότι από τα ανωτέρω έπεται ότι ισχύει η ισοδυναμία με αυστηρή ανισότητα ($A < B$, αν και μόνο αν $A \oplus C < B \oplus C$).

Τα iii. και iv. είναι πλέον προφανή. ό.έ.δ.

Το ουδέτερο D_0 της πρόσθεσης στους πραγματικούς αριθμούς, στο εξής, θα το συμβολίζουμε ως $\hat{0} = D_0$, εκτός από ορισμένα αποδεικτικά επιχειρήματα, όπου κρίνεται αναγκαίος ο συμβολισμός D_0, θεωρώντας ότι πρόκειται για σύνολο.

Ο νόμος της τριχοτομίας μας επιτρέπει να διακρίνουμε τους πραγματικούς αριθμούς σε τρεις κατηγορίες: Τους αρνητικούς ($A \in \mathbb{R}$ με $A < \hat{0}$), το μηδέν (το ουδέτερο της πρόσθεσης $\hat{0}$) και τους θετικούς ($B \in \mathbb{R}$ με $B > \hat{0}$).

Επίσης, μπορούμε να ορίσουμε την **απόλυτη τιμή** ενός πραγματικού αριθμού. Έστω $A \in \mathbb{R}$, ορίζουμε ως απόλυτη τιμή του A τον πραγματικό αριθμό

$$| A | = A \cup (-A).$$

Πρόταση 7.1.20. *Έστω $A \in \mathbb{R}$, τότε ισχύει:*

$$| A | = \begin{cases} A & \alpha\nu\ A > \hat{0} \\ -A & \alpha\nu\ A < \hat{0} \\ \hat{0} & \alpha\nu\ A = \hat{0} \end{cases}$$

Απόδειξη. Η απόδειξη αφήνεται ως άσκηση (Άσκηση $7.1.1_4$). ό.έ.δ.

Σχόλιο 7.1.21. Εδώ πρέπει να παρατηρήσουμε ότι συνηθίζεται η προηγουμένη πρόταση να δίνεται ως ορισμός της απόλυτης τιμής ενός πραγματικού αριθμού. Εδώ δίνουμε έναν άλλο ορισμό, από τον οποίο έπονται ιδιότητες της απόλυτης τιμής.

Ορισμός 7.1.22. Στο σύνολο των πραγματικών αριθμών ορίζουμε έναν πολλαπλασιασμό ως εξής: Έστω $A, B \in \mathbb{R}$.

α. Αν $A \geq \hat{0}$ και $B \geq \hat{0}$, ορίζουμε

$$A \odot B = D_0 \cup \{ xy \mid x \in A \text{ με } x \geq 0 \text{ και } y \in B \text{ με } y \geq 0 \}.$$

β. Αν $A \leq \hat{0}$ και $B \leq \hat{0}$, ορίζουμε

$$A \odot B = \mid A \mid \odot \mid B \mid .$$

γ. Αν $A \leq \hat{0}$ και $B \geq \hat{0}$ ή $A \geq \hat{0}$ και $B \leq \hat{0}$, ορίζουμε

$$A \odot B = -(\mid A \mid \odot \mid B \mid).$$

Λήμμα 7.1.23. *Η πράξη του πολλαπλασιασμού είναι καλώς ορισμένη.*

Απόδειξη. Αρκεί να αποδείξουμε ότι το γινόμενο είναι πραγματικός αριθμός, δηλαδή είναι τομή Dedekind.

Προφανώς (;) αρκεί να το δείξουμε για την πρώτη περίπτωση.

Έστω $A \geq \hat{0}$ και $B \geq \hat{0}$, τότε το σύνολο

$$A \odot B = D_0 \cup \{ xy \mid x \in A \text{ με } x \geq 0, \text{ και } y \in B \text{ με } y \geq 0 \}$$

προφανώς είναι μη κενό.

Επίσης, επειδή τα A, B είναι τομές Dedekind, υπάρχει $r \in \mathbb{Q} \setminus A$ και $s \in \mathbb{Q} \setminus A$ με $r > x$, για όλα τα $x \in A$ και $s > y$, για όλα τα $y \in B$ (ιδέ Πρόταση 7.1.4), επομένως

$$rs \notin A \odot B$$

και κατά συνέπεια το $A \odot B$ είναι γνήσιο υποσύνολο του $\mathbb{Q}$.

Έστω $t \in A \odot B$ και $r \in \mathbb{Q}$ με $r < t$. Αν $t \in D_0$ τότε

$$r \in D_0 \subseteq A \odot B.$$

Αν $t = 0$, τότε

$$r < 0 \text{ και } r \in D_0 \subseteq A \odot B.$$

Αν $t > 0$, τότε $t = xy$ με $x \in$ A, $y \in$ B και

$$r = \frac{1}{xy} \cdot r \cdot xy,$$

αλλά

$$s = \frac{1}{xy} \cdot r = \frac{r}{t} < 1,$$

συνεπώς

$$r = \left(\frac{1}{xy} \cdot r \cdot x \right) \cdot y = (s \cdot x) \cdot y$$

με το $s \cdot x < x$. Αλλά το A είναι τομή Dedekind, συνεπώς $s \cdot x \in A$ και επομένως

$$r \in A \odot B.$$

Δηλαδή το σύνολο $A \odot B$ είναι καθοδικά κλειστό.

Έστω $c \in A \odot B$. Αν $c \in D_0$, τότε υπάρχει

$$s \in D_0 \subseteq A \odot B$$

με $c < s$. Αν $c \notin D_0$, τότε

$$c = xy$$

με $x \in A$ και $y \in B$ και τα x, y μη αρνητικούς ρητούς αριθμούς. Τα A, B είναι τομές Dedekind, επομένως υπάρχουν $x_1 \in A$ με $x < x_1$ και $y_1 \in B$ με $y < y_1$. Τότε όμως θα έχουμε

$$c = xy < x_1 y_1$$

με το $x_1 y_1 \in A \odot B$. Συνεπώς, το σύνολο $A \odot B$ δεν έχει μέγιστο στοιχείο.

Δηλαδή αποδείξαμε ότι το σύνολο $A \odot B$ είναι τομή Dedekind. ό.έ.δ.

Ένα στοιχείο των πραγματικών αριθμών, το οποίο έχει σημαντικό ρόλο στην περαιτέρω μελέτη των πραγματικών αριθμών είναι το στοιχείο

$$D_1 = \{ x \in \mathbb{Q} \mid x < 1 \}.$$

Προφανώς ισχύει $D_0 < D_1$.

Έχοντας ορίσει τον πολλαπλασιασμό στους πραγματικούς αριθμούς μπορούμε να δούμε ορισμένες ιδιότητες.

Λήμμα 7.1.24. *Έστω A, B πραγματικοί αριθμοί.*

i. $A \odot B = B \odot A$. *(Η πράξη του πολλαπλασιασμού είναι μεταθετική).*

ii. $\hat{0} \odot A = A \odot \hat{0} = \hat{0}$.

iii. $D_1 \odot A = A \odot D_1 = A$.

Απόδειξη.

i. Είναι προφανές, εκ του ορισμού του πολλαπλασιασμού, δεδομένου ότι ο πολλαπλασιασμός στους ρητούς αριθμούς είναι μεταθετικός και ισχύουν το Πόρισμα 7.1.19 και η Πρόταση 7.1.20. Με τις λεπτομέρειες να αφήνονται ως άσκηση.

ii. Βάσει του Ορισμού 7.1.22 αρκεί να αποδείξουμε την ζητουμένη σχέση στην περίπτωση, όπου ο πραγματικός αριθμός A είναι μη αρνητικός (το $\hat{0} = D_0$ είναι μη αρνητικός). Οπότε, έχουμε

$$\hat{0} \odot A = \hat{0} \cup \{ xy \mid x \in \hat{0} \text{ και } x \geq 0,\ y \in A \text{ και } y \geq 0 \}.$$

Αλλά δεν υπάρχει $x \in D_0$ με $x \geq 0$, οπότε στην ανωτέρω ένωση συνόλων έχουμε ότι το σύνολο

$$\{ xy \mid x \in D_0 \text{ και } x \geq 0,\ y \in A \text{ και } y \geq 0 \}$$

είναι το κενό σύνολο. Άρα $D_0 \odot A = D_0$.

iii. Πάλι βάσει του Ορισμού 7.1.22 αρκεί να αποδείξουμε την ζητουμένη σχέση στην περίπτωση, όπου ο πραγματικός αριθμός A είναι μη αρνητικός (ο D_1 είναι μη αρνητικός). Οπότε, έχουμε

$$D_1 \odot A = D_0 \cup \{ xy \mid x \in D_0 \text{ με } 0 \leq x < 1, \text{ και } y \in A \text{ με } y \geq 0 \}.$$

Παρατηρούμε ότι

$$D_1 \odot A \subseteq A.$$

Πράγματι, $D_0 \subseteq A$ (γιατί; μα αφού ο A έχει υποτεθεί μη αρνητικός). Επίσης, για $0 \leq x < 1,\ y \in A$ και $y \geq 0$ έχουμε ότι

$$xy < y$$

και επειδή το A είναι καθοδικά κλειστό, έχουμε ότι

$$xy \in A.$$

Άρα $D_1 \odot A \subseteq A$.

Αντίστροφα, έστω $0 \geq r \in A$ τότε, επειδή το A δεν έχει μέγιστο στοιχείο, υπάρχει $s \in A$ με $s > r$. Οπότε, $\frac{r}{s} < 1$ και επομένως

$$\frac{r}{s} \in D_1.$$

Συνεπώς

$$r = \frac{r}{s} \cdot s \in D_1 \odot A.$$

Άρα $A \subseteq D_1 \odot A$.

Οπότε, πράγματι $D_1 \odot A = A \odot D_1 = A$. ό.έ.δ.

Από το iii. του προηγουμένου Λήμματος, βλέπουμε ότι η πράξη του πολλαπλασιασμού στους πραγματικούς αριθμούς έχει ουδέτερο.

Όπως το $\hat{0} = D_0$ είναι το μοναδικό ουδέτερο, στην περίπτωση της πρόσθεσης, έτσι και το D_1 είναι το μοναδικό ουδέτερο ως προς τον πολλαπλασιασμό, το οποίο θα συμβολίζουμε $\hat{1} = D_1$, εκτός από ορισμένα αποδεικτικά επιχειρήματα, όπου κρίνεται αναγκαίος ο συμβολισμός D_1, θεωρώντας ότι πρόκειται για σύνολο.

Εφόσον έχουμε εξασφαλίσει την ύπαρξη ουδετέρου, ως προς τον πολλαπλασιασμό στους πραγματικούς αριθμούς, αναζητούμε, αν για έναν πραγματικό αριθμό A υπάρχει αντίστροφος. Δηλαδή, αν υπάρχει $A^{-1} \in \mathbb{R}$ με την ιδιότητα:

$$A \odot A^{-1} = \hat{1} = A^{-1} \odot A.$$

Προφανώς, αν υπάρχει ένας τέτοιος πραγματικός αριθμός θα είναι μια τομή Dedekind, έστω N, με την ιδιότητα:

$$A \odot N = \hat{1}.$$

Επίσης, από το ii. του προηγουμένου Λήμματος, βλέπουμε ότι το $\hat{0}$ (το ουδέτερο της πρόσθεσης) δεν έχει αντίστροφο. Επομένως αναζητούμε, αν πραγματικοί αριθμοί, διάφοροι του $\hat{0}$, έχουν αντίστροφο.

Υποθέτουμε ότι έχουμε έναν πραγματικό αριθμό $A > \hat{0}$. Αναζητούμε έναν πραγματικό αριθμό N με την ιδιότητα

$$A \odot N = \hat{1}.$$

Από τον ορισμό του πολλαπλασιασμού έχουμε ότι ο N δεν μπορεί να είναι αρνητικός (γιατί;). Συνεπώς, θα πρέπει να έχουμε

$$xy < 1 \quad \left(x < \frac{1}{y}\right),$$

για όλα τα θετικά στοιχεία $x \in A$ και όλα τα θετικά στοιχεία $y \in N$.

Από την προηγουμένη ανάλυση έπεται ότι μπορούμε να "εικάσουμε" ποιος θα είναι ο αντίστροφος, αν υπάρχει, ενός μη μηδενικού πραγματικού αριθμού.

Λήμμα 7.1.25. *Έστω A ένας μη μηδενικός πραγματικός αριθμός. Υποθέτουμε ότι $A > \hat{0}$.*

i. Το σύνολο

$$A^{-1} = D_0 \cup \left\{ r \in Q \mid r \geq 0 \text{ και για τα } r > 0 \text{ να υπάρχει } \right.$$
$$\left. \text{ρητός αριθμός } c \notin A \text{ με } \frac{1}{r} > c \right\}$$

είναι τομή Dedekind. Μάλιστα δε, $A^{-1} > \hat{0}$.

ii. $A \odot A^{-1} = \hat{1}$.

Υποθέτουμε ότι $A < \hat{0}$.

i. Το σύνολο $A^{-1} = -(-A)^{-1}$ είναι τομή Dedekind.

ii. $A \odot A^{-1} = \hat{1}$.

Απόδειξη. Υποθέτουμε ότι $A > \hat{0}$.

i. Προφανώς το σύνολο

$$A^{-1} = D_0 \cup \left\{ r \in Q \mid r \geq 0 \text{ και για τα } r > 0 \text{ να υπάρχει } \right.$$
$$\left. \text{ρητός αριθμός } c \notin A \text{ με } \frac{1}{r} > c \right\}$$

είναι μη κενό.

Επίσης, το σύνολο A^{-1} είναι γνήσιο υποσύνολο του $\mathbb{Q}$.

Πράγματι, αν $\frac{k}{m} \in A$, με $\frac{k}{m} > 0$, τότε ο ρητός αριθμός

$$r = \frac{m}{k}$$

δεν ανήκει στο σύνολο A^{-1}, διότι

$$r \cdot \frac{k}{m} = 1,$$

ενώ θα έπρεπε, εκ του ορισμού του A^{-1}, να ίσχυε

$$r \cdot x < 1,$$

για όλα τα $x \in A$.

Έστω $r \in A^{-1}$. Αν $r \in D_0 \cup \{0\}$, τότε για κάθε $s < r$ έχουμε ότι

$$s \in D_0 \subseteq A^{-1}.$$

Αν $r > 0$, τότε για κάθε $s < r$ έχουμε

$$\frac{1}{s} > \frac{1}{r} > x,$$

για όλα τα $x \in A$. Αυτό σημαίνει ότι

$$s \in A^{-1}.$$

Δηλαδή το A^{-1} είναι καθοδικά κλειστό.

Επίσης, αν $r \in A^{-1}$, για τον οποίο υπάρχει ρητός αριθμός $c \notin A$ με $\frac{1}{r} > c$, τότε υπάρχει ρητός αριθμός s με

$$\frac{1}{r} > s > c,$$

αλλά τότε

$$t = \frac{1}{s} > r \text{ και } \frac{1}{t} = s > c$$

αυτό σημαίνει ότι

$$t \in A^{-1}.$$

Δηλαδή το σύνολο A^{-1} δεν έχει μέγιστο στοιχείο.

Επομένως, το σύνολο A^{-1} είναι τομή Dedekind.

Το ότι ισχύει $A^{-1} > \hat{0}$ είναι προφανές από τον ορισμό του A^{-1} και την υπόθεση ότι $A > \hat{0}$.

ii. Από τον ορισμό του πολλαπλασιασμού έχουμε ότι

$$\begin{aligned} A \odot A^{-1} &= D_0 \cup \{ xy \mid x \in A \text{ με } 0 \leq x \text{ και } y \in A^{-1} \text{ με } 0 \leq y \} \\ &= D_0 \cup \{ xy < 1 \mid 0 \leq x, 0 \leq y \} \\ &= D_1 = \hat{1}. \end{aligned}$$

Το δεύτερο μέρος του ισχυρισμού του Λήμματος έπεται παρομοίως και αφήνεται ως άσκηση (Άσκηση 7.1.1$_7$). ό.έ.δ.

Θα παραθέσουμε μια πρόταση, όπου εφαρμόζονται οι προηγούμενες ιδιότητες της πρόσθεσης και του πολλαπλασιασμού στις ρητές τομές Dedekind. Δηλαδή στις

$$D_r = \{ x \in \mathbb{Q} \mid x < r \}.$$

Πρόταση 7.1.26. *Έστω $r, s \in \mathbb{Q}$. Τότε ισχύει:*

1. $D_{-r} = -D_r$.
2. *Αν* $r \neq 0$, *τότε* $D_{r^{-1}} = (D_r)^{-1}$.
3. $D_{r+s} = D_r \oplus D_s$.
4. $D_{r \cdot s} = D_r \odot D_s$.
5. $r < s$, *αν και μόνο αν* $D_r < D_s$.

Απόδειξη. Θα αποδείξουμε τις (1) και (4) με τις υπόλοιπες να αφήνονται ως άσκηση (Άσκηση 7.1.1$_8$).

1. Από τον ορισμό της πρόσθεσης πραγματικών αριθμών έχουμε ότι

$$\begin{aligned} D_r \oplus D_{-r} &= \{ x+y \mid x, y \in \mathbb{Q} \text{ με } x \in D_r \text{ και } y \in D_{-r} \} \\ &= \{ x+y \mid x, y \in \mathbb{Q} \text{ με } x < r, y < -r \} \\ &= \{ x+y \mid x, y \in \mathbb{Q} \text{ και } x+y < r+(-r) = 0 \} \\ &= D_0. \end{aligned}$$

   Δηλαδή το D_{-r} ισούται με το μοναδικό αντίθετο του D_r. Άρα πράγματι

$$D_{-r} = -D_r.$$

4. Υποθέτουμε ότι $r > 0$, $s > 0$.

   Από τον ορισμό του πολλαπλασιασμού πραγματικών αριθμών έχουμε ότι

$$\begin{aligned} D_r \odot D_s &= D_0 \cup \{ xy \mid x, y \in \mathbb{Q} \text{ και } x \in D_r \text{ με } yx \geq 0 \text{ και } y \in D_s \text{ με } y \geq 0 \} \\ &= D_0 \cup \{ xy \mid x, y \in \mathbb{Q} \text{ με } 0 \leq x < r \text{ και } 0 \leq y < s \} \\ &= D_0 \cup \{ z \in \mathbb{Q} \mid 0 \leq z < r \cdot s \} \subseteq D_{r \cdot s}. \end{aligned}$$

   Αντίστροφα, έστω $x \in D_{r \cdot s}$, τότε

$$x < r \cdot y.$$

   Από την Άσκηση 6.2.1$_7$ έπεται ότι υπάρχουν ρητοί αριθμοί x_1, x_2 με

$$r = x_1 \cdot x_2 \text{ και } x_1 < r, x_2 < s.$$

   Επομένως

$$r \in D_r \odot D_s.$$

   Άρα πράγματι

$$D_{r \cdot s} = D_r \odot D_s.$$

Όμοια αντιμετωπίζονται και οι υπόλοιπες περιπτώσεις. ό.έ.δ.

Αν και το σώμα των ρητών αριθμών έχει, "εκ φύσεως", διαφορετικά στοιχεία από το σώμα των πραγματικών αριθμών, μπορεί να θεωρηθεί κατάλληλα ως υποσύνολο των πραγματικών αριθμών. Κάτι ανάλογο είχαμε δει στο πώς οι φυσικοί αριθμοί εμφυτεύονται στον δακτύλιο των ακεραίων αριθμών και ο δακτύλιος των ακεραίων αριθμών εμφυτεύεται στο σώμα των ρητών αριθμών (Πρόταση 6.2.6).

Πόρισμα 7.1.27. *Η απεικόνιση* $i : \mathbb{Q} \longrightarrow R$ *με*

$$i(r) = D_r$$

είναι ένας μονομορφισμός δακτυλίων. Μάλιστα δε ισχύει:

$$r < s, \text{ αν και μόνο αν } i(r) < i(s).$$

Απόδειξη. Η απόδειξη στην πραγματικότητα έχει προηγηθεί (είναι η Πρόταση 7.1.26) με τις λεπτομέρειες να αφήνονται ως άσκηση (Άσκηση 7.1.1$_9$). ό.έ.δ.

Στην σελίδα 260 είχαμε αναφερθεί σε μια διαισθητική αντιστοιχία μεταξύ των ρητών αριθμών και των ρητών τομών Dedekind, στο προηγούμενο πόρισμα αυτό επιτυγχάνεται *Μαθηματικώ τω τρόπω*.

Για τον ορισμό των πραγματικών αριθμών προτιμήσαμε την προσέγγιση μέσω των τομών Dedekind, οι οποίες είναι υποσύνολα των ρητών αριθμών.

Στο εξής, όταν αναφερόμαστε στους πραγματικούς αριθμούς, σπάνια θα αναφερόμαστε στις τομές Dedekind, παρά μόνο όταν χρειάζεται να τις επικαλεστούμε σε αποδεικτικά επιχειρήματα.

Επίσης, είχαμε αναφερθεί σε μια διαισθητική αντιστοιχία μεταξύ των πραγματικών αριθμών και των σημείων μιας ευθείας (σελ. 262). Με όσα έχουν προηγηθεί, η διαίσθηση αυτή γίνεται πιο *συνειδητή*.

Τώρα είμαστε σε θέση να ενοποιήσουμε τα προηγούμενα, επιμέρους, αποτελέσματα, αλλάζοντας και τους συμβολισμούς.

Στο εξής δεν θα χρησιμοποιούμε κεφαλαία γράμματα για να συμβολίσουμε τους πραγματικούς αριθμούς, δεδομένου ότι, όπως προείπαμε, δεν θα χρησιμοποιούμε την φύση των στοιχείων του συνόλου των πραγματικών αριθμών. Επίσης, λόγω της ταυτοποίησης των ρητών αριθμών με πραγματικούς αριθμούς (μέσω της απεικόνισης i του προηγουμένου πορίσματος), θα χρησιμοποιούμε, ανεξαρτήτως, το σύμβολο $+$ (αντί του $\oplus$) της πρόσθεσης και το σύμβολο $\cdot$ (αντί του $\odot$) του πολλαπλασιασμού μεταξύ πραγματικών αριθμών. Όπως και το 0 (αντί του $\hat{0}$) για το ουδέτερο ως προς την πρόσθεση και το 1 (αντί του $\hat{1}$) για το ουδέτερο ως προς τον πολλαπλασιασμό.

Θεώρημα 7.1.28. [5] *Έστω $r, s, t \in \mathbb{R}$, τότε ισχύουν τα ακόλουθα:*

1. $(r + s) + t = r + (s + t)$ *(Η προσεταιριστική ιδιότητα της πρόσθεσης στους πραγματικούς).*
2. $r + s = s + r$ *(Η πρόσθεση των πραγματικών είναι μεταθετική).*
3. $r + 0 = r$ *(Η πρόσθεση έχει ουδέτερο).*
4. $r + (-r) = 0$ *(Κάθε πραγματικός αριθμός έχει αντίθετο ως προς την πρόσθεση).*
5. $(r \cdot s) \cdot t = r \cdot (s \cdot t)$ *(Η προσεταιριστική ιδιότητα του πολλαπλασιασμού στους πραγματικούς).*
6. $r \cdot s = s \cdot t$ *(Ο πολλαπλασιασμός των πραγματικών είναι μεταθετικός).*
7. $r \cdot 1 = r$ *(Ο πολλαπλασιασμός έχει ουδέτερο).*
8. *Αν* $r \neq 0$, *τότε* $r \cdot r^{-1} = 1$ *(Κάθε πραγματικός αριθμός, διάφορος του μηδενός, έχει αντίστροφο).*
9. $r \cdot (s + t) = r \cdot s + r \cdot t$ *(Η επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση στους πραγματικούς).*
10. $r \cdot 0 = 0$.

[5] "...The construction of the real numbers proves that there exists a set with the properties that we would expect of the real numbers, but ultimately, it is the properties of the real numbers, not how they are constructed, that matter...". Εμείς δεν συμφωνούμε με την ανωτέρω γνώμη, η οποία διατυπώνεται σε πολλά ξενόγλωσσα συγγράμματα. Μάλλον θα έπρεπε να απευθύνεται σε μη Μαθηματικούς.

11. *Ισχύει ακριβώς μια από τις σχέσεις* $r < s$, $r = s$, $r > s$ *(Ο νόμος της τριχοτομίας στους πραγματικούς).*

12. *Αν* $r < s$ *και* $s < t$, *τότε* $r < t$ *(Η μεταβατική ιδιότητα της διάταξης στους πραγματικούς).*

13. *Αν* $r \leq s$ *και* $s \leq r$, *τότε* $r = s$

14. *Αν* $r < s$, *τότε* $r + t < s + t$.

15. *Αν* $r < s$ *και* $t > 0$, *τότε* $rt < st$.

16. $0 \neq 1$ *(Το σύνολο των πραγματικών έχει τουλάχιστον δύο στοιχεία).*

Απόδειξη. Η απόδειξη των ιδιοτήτων των πραγματικών αριθμών, που αναφέρονται στο ανωτέρω θεώρημα έχει προηγηθεί, εκτός των (5), (9), (15). Ανατρέξτε (κατά σειρά) στα 7.1.18, 7.1.19, 7.1.24, 7.1.25.

Η απόδειξη των ιδιοτήτων (5), (9), (15) αφήνεται ως άσκηση (Άσκηση $7.1.1_{12}$).[6] ό.έ.δ.

Παρατήρηση 7.1.29. Αν "συγκρίνουμε" τα Θεωρήματα 7.1.28 και 6.2.4, θα διαπιστώσουμε ότι το σώμα των ρητών αριθμών και το σώμα των πραγματικών αριθμών, ως Αλγεβρικές δομές, είναι *πανομοιότυπες* (πρόκειται για δύο διατεταγμένα σώματα). Το διαφοροποιόν στοιχείο είναι ότι στο μεν σώμα των πραγματικών αριθμών ισχύει η "Αρχή της πληρότητας", στο δε σώμα των ρητών αριθμών δεν ισχύει κάτι ανάλογο (ιδέ το σχόλιο μετά την απόδειξη της Πρότασης 7.1.12).

Επομένως, γεννάται το ερώτημα: Υπάρχουν και άλλα διατεταγμένα σώματα, τα οποία να ικανοποιούν την "Αρχή της πληρότητας", πέραν του σώματος των πραγματικών αριθμών;

Η απάντηση είναι όχι.

Συγκεκριμένα ισχύει:

Θεώρημα 7.1.30. *Έστω* $(R_1, +, \cdot, <)$, $(R_2, \oplus, \odot, \prec)$ *δύο διατεταγμένα σώματα, τα οποία ικανοποιούν την "Αρχή της πληρότητας". Τότε τα δύο σώματα είναι ισόμορφα. Δηλαδή υπάρχει μια απεικόνιση* $f : R_1 \longrightarrow R_2$, *η οποία είναι 1-1 και επί.*

Για $x, y \in R_1$ *ισχύουν:*

i. $f(x + y) = f(x) \oplus f(y)$.

ii. $f(x \cdot y) = f(x) \odot f(y)$.

iii. Αν $x < y$), *τότε* $f(x) \prec f(y)$.

Η απόδειξη του θεωρήματος αυτού είναι πολύ πέραν των σκοπών του παρόντος.

[6] Εδώ θέλουμε να επισημάνουμε ότι η ιδέα της απόδειξης είναι πολύ απλή (έλεγχος ισοτήτων), αλλά λόγω της φύσεως των πραγματικών αριθμών (είναι τομές Dedekind), χρειάζεται μια "ακροβατική/χειρουργική" αντιμετώπιση, όπως, ίσως, έχετε διαπιστώσει και σε προηγούμενες αποδείξεις.

Ορισμένες επιπλέον ιδιότητες των πραγματικών αριθμών.

Στην παράγραφο αυτή θα αναφέρουμε ορισμένες χαρακτηριστικές ιδιότητες των πραγματικών αριθμών, χωρίς να επεκταθούμε περισσότερο, δεδομένου ότι από το σημείο αυτό ξεκινά ένα πρώτο μάθημα "Απειροστικού Λογισμού".

Οι ιδιότητες αυτές θα παρατεθούν με κάποιες αποδείξεις και...περισσότερες υποδείξεις.

Πρόταση 7.1.31. *Έστω* $a, b \in \mathbb{R}$, *τότε ισχύουν:*

1. $|a| \geq 0$ *και* $|a| = 0$, *αν και μόνο αν* $a = 0$.
2. $-|a| \leq a \leq |a|$.
3. $|a| = |b|$, *αν και μόνο αν* $a = b$, *ή* $a = -b$.
4. $|a| < b$, *αν και μόνο αν* $-b < a < b$.
5. $|a \cdot b| = |a| \cdot |b|$.
6. $|a + b| \leq |a| + |b|$ *(Η τριγωνική ιδιότητα).*
7. $|a| - |b| \leq |a + b|$ *και* $|a| - |b| \leq |a - b|$.

Απόδειξη. Η απόδειξη στηρίζεται στον (ισοδύναμο) ορισμό της απόλυτης τιμής (ιδέ Πρόταση 7.1.20).

Εδώ θα αποδείξουμε μόνο τα (6) και (7), αφήνοντας τα υπόλοιπα ως άσκηση (Άσκηση $7.1.1_{10}$).

6. Θεωρούμε ότι ισχύει το (2) (το οποίο αποδεικνύεται χωρίς την χρήση της προς απόδειξη σχέσης).

   Επομένως, έχουμε ότι

   $$-|a| \leq a \leq |a|, \ -|b| \leq b \leq |b|.$$

   Οπότε, προσθέτοντας κατά μέλη τις ανωτέρω ισότητες έχουμε ότι

   $$-(|a| + |b|) \leq a + b \leq |a| + |b|.$$

   Οπότε, από το (4) έχουμε το ζητούμενο

   $$|a + b| \leq |a| + |b|.$$

7. Έχουμε ότι $a = (a - b) + b$, επομένως

   $$|a| = |(a - b) + b| \leq |a - b| + |b|.$$

   Οπότε, έπεται το ζητούμενο

   $$|a| - |b| \leq |a - b|.$$

   Θέτοντας $-b$, αντί b στην προηγουμένη σχέση έπεται ότι

   $$|a| - |b| \leq |a + b|.$$

ό.έ.δ.

Πρόταση 7.1.32. *Έστω A, B μη κενά υποσύνολα των πραγματικών αριθμών. Υποθέτουμε ότι $a \leq b$ για όλα τα $a \in A$ και $b \in B$. Τότε ισχύουν:*

i. Το σύνολο A έχει ελάχιστο άνω φράγμα, έστω m και το σύνολο B έχει μέγιστο κάτω φράγμα, έστω μ. Μάλιστα δε ισχύει $m \leq \mu$.

ii. $m = \mu$, αν και μόνο αν για κάθε $\epsilon > 0$, υπάρχουν $a \in A$ και $b \in B$ με $b - a < \epsilon$.

Απόδειξη.

i. Το σύνολο A είναι άνω φραγμένο από κάθε στοιχείο του συνόλου B, επομένως έχει ελάχιστο άνω φράγμα, έστω m. Όμοια το σύνολο B είναι κάτω φραγμένο από κάθε στοιχείο του συνόλου A, επομένως έχει μέγιστο κάτω φράγμα, έστω μ.

Υποθέτουμε ότι $m > \mu$. Θέτουμε

$$k = \frac{m - \mu}{2} > 0.$$

Προφανώς έχουμε ότι $\mu < k < m$.

Ισχυρισμός: Υπάρχει $a \in A$ με $m - k < a \leq m$ και $b \in B$ με $\mu \leq b < \mu + k$.

Επομένως, θα έχουμε

$$b < \mu + k = \mu + \frac{m - \mu}{2} = \frac{m + \mu}{2} = m - \frac{m + \mu}{2} < a.$$

Αυτό είναι άτοπο. Επομένως, η αποδεικτέα σχέση $m \leq \mu$.

Δεν τελειώσαμε, απομένει η απόδειξη του ισχυρισμού.

Επειδή $m - k < m$, το $m - k$ δεν μπορεί να είναι ένα άνω φράγμα του A, αφού το m είναι το ελάχιστο άνω φράγμα. Συνεπώς, υπάρχει $a \in A$ με $m - k < a$, αλλά $a \leq m$, δεδομένου ότι το m είναι άνω φράγμα του A. Άρα πράγματι

$$m - k < a \leq m.$$

Όμοια αποδεικνύεται ότι $b \in B$ με $\mu \leq b < \mu + k$.

Σημειωτέον ότι στην απόδειξη του ανωτέρω ισχυρισμού δεν χρησιμοποιήσαμε ότι $k = \frac{m - \mu}{2}$, παρά μόνο ότι $k > 0$. Συνεπώς, στη θέση του k, θα μπορούσε να είναι οποιοσδήποτε πραγματικός αριθμός $\epsilon > 0$.

ii. Υποθέτουμε ότι $m = \mu$. Έστω $\epsilon > 0$. Από τον ανωτέρω ισχυρισμό έπεται ότι υπάρχει $a \in A$ και $b \in B$ με $m - \frac{\epsilon}{2} < a \leq m$ και $\mu \leq b < \mu + \frac{\epsilon}{2}$. Συνδυάζοντας τις ανωτέρω ανισότητες έχουμε ότι

$$m - \frac{\epsilon}{2} < a \leq m = \mu \leq b < m + \frac{\epsilon}{2}.$$

Δηλαδή,

$$m - \frac{\epsilon}{2} < a \leq b < m + \frac{\epsilon}{2}.$$

Εξού $b - a < \epsilon$.

Αντίστροφα. Από το πρώτο ερώτημα γνωρίζουμε ότι $m \leq \mu$. Υποθέτουμε ότι $m < \mu$, ενώ για κάθε $\epsilon > 0$ υπάρχουν $a \in A$ και $b \in B$ με $b - a < \epsilon$.

Θέτουμε $\eta = \mu - m > 0$. Τότε, για οποιοδήποτε $x \in A$ και $y \in B$, έχουμε $m \leq x$ και $y \leq \mu$. Δηλαδή, για οποιαδήποτε $x \in A$ και $y \in B$, έχουμε $y - x \geq \eta$. Αυτό σημαίνει ότι για οποιαδήποτε $x \in A$ και $y \in B$, έχουμε $y - x \geq \eta > \eta/2$, άτοπο.

Άρα πράγματι $m = \mu$. ό.έ.δ.

Θεώρημα 7.1.33. *Έστω $a, b \in \mathbb{R}$ με $a > 0$. Υπάρχει φυσικός αριθμός n με $b < n \cdot a$.*

Απόδειξη. Προφανώς, αν $b \leq 0$, ισχύει ότι $b \leq 0 < 1 \cdot a$.

Έστω $b > 0$. Υποθέτουμε ότι δεν ισχύει το συμπέρασμα. Άρα $n \cdot a \leq b$, για όλα τα $n \in \mathbb{N}$.

Έστω $A = \{ n \cdot a \mid n \in \mathbb{N} \}$. Το σύνολο είναι μη κενό και άνω φραγμένο από το b, επομένως έχει ελάχιστο άνω φράγμα, έστω m.

Ισχυρισμός: Για κάθε $n \in \mathbb{N}$ ισχύει

$$na \leq m - a.$$

Πράγματι, αν υπήρχε $r \in \mathbb{N}$ με $ra > m - a$, τότε $(r+1)a > a$, με το $r + 1 \in \mathbb{N}$. Αυτό αντίκειται στον αρχικό μας ισχυρισμό $n \cdot a \leq b$, για όλα τα $n \in \mathbb{N}$. Επομένως, πράγματι $na \leq m - a < m$, για κάθε $n \in \mathbb{N}$. Αυτό έρχεται σε αντίφαση με το ότι το m είναι το ελάχιστο άνω φράγμα του συνόλου A. Επομένως έχουμε αντίφαση με την αρχική μας υπόθεση ότι $n \cdot a \leq b$, για όλα τα $n \in \mathbb{N}$. Συνεπώς, υπάρχει φυσικός αριθμός n με $b < n \cdot a$. ό.έ.δ.

Ο ισχυρισμός του προηγουμένου θεωρήματος, αν και φαίνεται προφανής, η απόδειξή του, όπως είδαμε, δεν είναι καθόλου προφανής.

Το προηγούμενο θεώρημα είναι πολύ σημαντικό, διότι "διευκρινίζει" πώς οι φυσικοί αριθμοί "τοποθετούνται" εντός του συνόλου των πραγματικών αριθμών.

Η ιδιότητα αυτή είναι γνωστή ως **Η Αρχιμήδεια ιδιότητα** των πραγματικών αριθμών.

Προφανώς, το σώμα των ρητών αριθμών, ως υπόσωμα των πραγματικών αριθμών, πληροί την Αρχιμήδεια ιδιότητα. Αυτό είχε επισημανθεί ήδη (Άσκηση $6.2.1_6$), εκεί η απόδειξη ήταν προφανής.

Στην ειδική περίπτωση, όπου $a = 1$, προκύπτει ότι για κάθε πραγματικό αριθμό x υπάρχει φυσικός αριθμός n με $x < n$. Δηλαδή το (υπο)σύνολο των φυσικών αριθμών είναι *ομοτελικό* με το (υπερ)σύνολο των πραγματικών αριθμών.

Ενδιαφέρον είναι ότι υπάρχουν διατεταγμένα σώματα, τα οποία δεν πληρούν την Αρχιμήδεια ιδιότητα. Αυτό είναι πολύ πέραν των σκοπών του παρόντος.

Πόρισμα 7.1.34. *Έστω $x \in \mathbb{R}$.*

i. Υπάρχει μοναδικός ακέραιος αριθμός n με $n - 1 \leq x < n$.

ii. Αν $x > 0$, υπάρχει φυσικός αριθμός m με $\dfrac{1}{m} < x$.

Απόδειξη.

i. Πρώτα θα δείξουμε την μοναδικότητα. Υποθέτουμε ότι υπάρχουν δύο διαφορετικοί ακέραιοι m, n, ώστε

$$m - 1 \leq x < m \text{ και } n - 1 \leq x < n.$$

Χωρίς βλάβη έστω $m < n$, τότε $m + 1 \leq n$, δηλαδή

$$m \leq n - 1,$$

οπότε από την σχέση $m - 1 \leq x < m$ έπεται ότι

$$x < m \leq n - 1,$$

άτοπο, δεδομένου ότι $n - 1 \leq x < n$.

Αν $x = 0$, τότε προφανώς $1 - 1 \leq x < 1$.

Υποθέτουμε ότι $x > 0$. Από το προηγούμενο θεώρημα έπεται ότι υπάρχει n φυσικός αριθμός με $x < n$.

Έστω m ο μικρότερος φυσικός αριθμός, ώστε $x < m$ (δεν ξεχνάμε την αρχή του ελαχίστου).

Προφανώς $m - 1 \leq x$ (γιατί; δεν ξεχνάμε τον νόμο της τριχοτομίας στους πραγματικούς αριθμούς).

Συνεπώς, $m - 1 \leq x < m$.

Η περίπτωση $x < 0$ αντιμετωπίζεται αναλόγως δεδομένου ότι $0 < -x$ με τις λεπτομέρειες να αφήνονται ως άσκηση (Άσκηση $7.1.1_{13}$).

ii. Η απόδειξη είναι προφανής. ό.έ.δ.

Πριν προχωρήσουμε, ας ανακεφαλαιώσουμε τι γνωρίζουμε, μέχρι τώρα, για τον πραγματικό αριθμό $\sqrt{2}$.

Πρώτον, με την προϋπόθεση ότι υπάρχει r πραγματικός αριθμός, ώστε $r^2 = 2$, είχαμε δει ότι ο r δεν μπορεί να είναι ρητός (Θεώρημα 3.2.8).

Δεύτερον, είχαμε σχολιάσει ότι ένας υποψήφιος πραγματικός αριθμός (μια τομή Dedekind) r, ώστε $r^2 = 2$ είναι ο

$$r = \{ x \in \mathbb{Q}, x < 0 \mid x^2 > 2 \}$$

(ιδέ το Παράδειγμα 7.1.3 και τα σχόλια, που ακολουθούν).

Θέτουμε

$$A = \{ x \in \mathbb{Q}, x < 0 \mid x^2 > 2 \}.$$

Τότε $A < D_0$ και επομένως $B = -A > D_0$.

Παρατηρούμε ότι, από τον ορισμό του B (ιδέ Λήμμα 7.1.17), έχουμε ότι

$$B = D_0 \cup \{ y \in \mathbb{Q} \mid y^2 < 2 \} \text{ (γιατί;)}.$$

Από τον ορισμό του πολλαπλασιασμού (Ορισμός 7.1.22) έχουμε ότι

$$\begin{aligned} B \odot B &= D_0 \cup \{ xy \mid x, y \in B \text{ με } x \geq 0 \text{ και } y \geq 0 \} \\ &= D_0 \cup \{ xy \mid x \geq 0, y \geq 0 \text{ και } xy < 2 \} \leq D_2. \end{aligned}$$

Αν αποδείξουμε την αντίστροφη ανισότητα $D_2 \leq B \odot B$, θα έχουμε αποδείξει ότι πράγματι ο πραγματικός αριθμός B είναι μια τετραγωνική ρίζα του πραγματικού αριθμού $D_2 \equiv 2$.

Αυτό δεν είναι εύκολο, διότι "λείπει" κάτι. Μια τομή Dedekind, ως υποσύνολο των ρητών αριθμών, ενώ είναι άνω φραγμένο σύνολο, δεν έχει ελάχιστο άνω φράγμα. Τί γίνεται όμως αν θεωρηθεί ως υποσύνολο των πραγματικών; Δεν ξεχνάμε ότι οι ρητοί μπορεί να θεωρηθούν υποσύνολο των πραγματικών αριθμών.

Πρόταση 7.1.35. *Έστω $r \in \mathbb{R}$ με $1 < r$. Υπάρχει μοναδικός θετικός πραγματικός αριθμός m με $m^2 = r$.*

Απόδειξη. Θεωρούμε το σύνολο $S = \{x \in \mathbb{R} \mid x^2 < r\}$. Το σύνολο αυτό είναι μη κενό (γιατί;) και άνω φραγμένο. Πράγματι, για κάθε $x \in S$ έχουμε ότι $x < r$ (γιατί;). Επομένως, το S έχει ένα ελάχιστο άνω φράγμα, έστω m με $m > 0$ (γιατί;). Θα δείξουμε ότι $m^2 = r$.

Θέτουμε

$$t = \frac{r(m+1)}{r+m}.$$

Παρατηρούμε ότι $t > 0$ (γιατί;)

Υποθέτουμε ότι $m^2 < r$. Τότε όμως θα έχουμε ότι $t > m$ (απλή επαλήθευση) και $t^2 < r$ (πάλι απλή επαλήθευση). Οι δύο τελευταίες δεν μπορεί να συναληθεύουν, διότι από την δεύτερη έχουμε ότι $t \in S$ και από την πρώτη ότι το t υπερβαίνει το ελάχιστο άνω φράγμα του S.

Υποθέτουμε ότι $m^2 > r$. Τότε $t < m$ (απλή επαλήθευση) και $t^2 > r$ (πάλι απλή επαλήθευση). Τότε όμως για κάθε $x \in S$ έχουμε ότι

$$x^2 < r < t^2,$$

επειδή $t > 0$, έπεται ότι $x < t$. Αυτό σημαίνει ότι το t είναι άνω φράγμα του S, άτοπο από την υπόθεση.

Επομένως, δεν μπορεί να ισχύει ούτε $m^2 < r$, ούτε $m^2 > r$. Άρα

$$m^2 = r.$$

Η απόδειξη ότι ο m είναι ο μοναδικός πραγματικός αριθμός, ώστε $m^2 = r$ είναι προφανής. ό.έ.δ.

Προφανώς, αν έχουμε έναν πραγματικό αριθμό r με $0 < r < 1$, τότε $\frac{1}{r} > 1$ και επομένως, σύμφωνα με την προηγουμένη πρόταση, υπάρχει $m \in \mathbb{R}$ με

$$0 < m^2 = \frac{1}{r},$$

οπότε

$$\left(\frac{1}{m}\right)^2 = r.$$

Πόρισμα 7.1.36. *Για κάθε μη αρνητικό πραγματικό αριθμό r υπάρχουν δύο πραγματικοί αριθμοί $m, -m$ με την ιδιότητα*

$$m^2 = (-m)^2 = r.$$

Από τους δύο αριθμούς m και $-m$, με την ανωτέρω ιδιότητα, ο θετικός θα ονομάζεται η (θετική) τετραγωνική ρίζα του r και θα συμβολίζεται $\sqrt{r}$.

Παρατήρηση 7.1.37. Όπως ορίσαμε την τετραγωνική ρίζα ενός θετικού πραγματικού αριθμού, έτσι μπορούμε να ορίσουμε, για κάθε $n \in \mathbb{N}$, την n-οστή ρίζα ενός θετικού πραγματικού αριθμού r, ως έναν θετικό πραγματικό αριθμό m με $m^n = r$.

Αποδεικνύεται ότι υπάρχει πάντα η θετική n-οστή ρίζα ενός πραγματικού αριθμού, αλλά η απόδειξη είναι πέραν του σκοπού μας. Γενικότερα, για κάθε $k \in \mathbb{R}$ και κάθε $0 < x$ πραγματικό αριθμό, ορίζεται ο πραγματικός αριθμός x^k. Αυτό όμως είναι πολύ πέραν του σκοπού μας. Απλώς επισημαίνουμε ότι παντού... *από πίσω* υπάρχει η αρχή του ελαχίστου άνω φράγματος.

Πρόταση 7.1.38. *Έστω r ένας φυσικός αριθμός. Υποθέτουμε ότι ο r δεν έχει ακεραία τετραγωνική ρίζα, δηλαδή δεν υπάρχει $u \in \mathbb{Z}$ με $u^2 = r$. Τότε δεν υπάρχει ρητή τετραγωνική ρίζα του r, δηλαδή δεν υπάρχει $s \in \mathbb{Q}$ με $s^2 = r$.*

Απόδειξη. Από την προηγουμένη πρόταση υπάρχει η τετραγωνική ρίζα του $\sqrt{r} \in \mathbb{R}$.

Από το Πόρισμα 7.1.34 υπάρχει μοναδικός ακέραιος n με

$$n \leq \sqrt{r} < n + 1.$$

Μάλιστα δε, από την υπόθεση, έχουμε ότι

$$n < \sqrt{r} < n + 1$$

και επειδή $r \geq 1$ ισχύει ότι $n \geq 1$.

Υποθέτουμε ότι υπάρχει (θετικός) ρητός s με $s^2 = r$, θα καταλήξουμε σε άτοπο.

Ο ρητός s μπορεί να γραφεί υπό μορφήν κλάσματος $s = \frac{\kappa}{\lambda}$ υπό πολλές μορφές, με $\kappa, \lambda \in \mathbb{N}$. Επιλέγουμε μια μορφή $s = \frac{\mu}{\nu}$ με τον ν τον μικρότερο δυνατόν. (Γιατί μπορούμε να το κάνουμε αυτό; μα ισχύει η αρχή του ελαχίστου). Από τα προηγούμενα έχουμε ότι

$$n < \frac{\mu}{\nu} < n + 1,$$

απ' όπου έπεται ότι $0 < \mu - n\nu < \nu$. Παρατηρούμε ότι

$$s = \frac{\mu}{\nu} = \frac{r\nu - n\mu}{\mu - n\nu}.$$

Να κάνετε τον έλεγχο ότι ισχύει η τελευταία ισότητα[7]. Αλλά αυτό έρχεται σε αντίφαση με την επιλογή του ν ως ελαχίστου (θετικού) παρονομαστή στην γραφή $s = \frac{\mu}{\nu}$. Συνεπώς, δεν υπάρχει ρητός s με $s^2 = r$. ό.έ.δ.

Θεώρημα 7.1.39. *Έστω $a, b \in \mathbb{R}$ με $a < b$.*

i. Υπάρχει ρητός αριθμός q με $a < q < b$.

ii. Υπάρχει άρρητος $r \in \mathbb{R} \setminus \mathbb{Q}$ με $a < r < b$.

Απόδειξη.

i. Από το Πόρισμα 7.1.34 υπάρχει $n \in \mathbb{N}$ με

$$\frac{1}{n} < b - a,$$

εκ του οποίου έπεται ότι $1 + na < nb$. Επίσης, πάλι από το ίδιο πόρισμα, υπάρχει ακέραιος αριθμός m, ώστε

$$m - 1 \leq na < m.$$

Συνδυάζοντας τις ανωτέρω ανισότητες έχουμε ότι $na < m < nb$. Οπότε, έπεται το ζητούμενο

$$a < \frac{m}{n} < b.$$

[7] Μπορείτε να εξηγήσετε πώς εικάσαμε ότι ισχύει η τελευταία ισότητα;

ii. Η τετραγωνική ρίζα $\sqrt{2}$ είναι θετική και άρρητος αριθμός. Επομένως, από την υπόθεση έχουμε ότι

$$\frac{a}{\sqrt{2}} < \frac{b}{\sqrt{2}}.$$

Από το πρώτο σκέλος του θεωρήματος, υπάρχει ρητός q με

$$\frac{a}{\sqrt{2}} < q < \frac{b}{\sqrt{2}}.$$

Ο q μπορεί να υποτεθεί μη μηδενικός (γιατί;). Συνεπώς

$$a < \sqrt{2}q < b.$$

Ο $\sqrt{2}q$ όμως είναι άρρητος (γιατί;). Οπότε, ολοκληρώθηκε η απόδειξη. ό.έ.δ.

Το τελευταίο θεώρημα είναι πολύ σημαντικό, διότι αποδεικνύει τον τρόπο, με τον οποίο *εμπλέκονται*, ως προς την διάταξη οι ρητοί και οι πραγματικοί αριθμοί.

Θα κλείσουμε την σύντομη εισαγωγή μας στους πραγματικούς αριθμούς επισημαίνοντας το εξής:

Όπως είδαμε, η ειδοποιός διαφορά μεταξύ του σώματος των πραγματικών αριθμών και του σώματος των ρητών αριθμών είναι ότι στο πρώτο ισχύει η αρχή της πληρότητας, ενώ στο δεύτερο δεν ισχύει.

Ένα φυσιολογικό ερώτημα είναι κατά πόσον η αρχή της πληρότητας μπορεί να αντικατασταθεί με ένα άλλο ισοδύναμο αξίωμα, με το οποίο να κατασκευάζουμε τους πραγματικούς αριθμούς.

Εδώ δεν θα επεκταθούμε περισσότερο, αλλά για τον ενδιαφερόμενο αναγνώστη παραπέμπουμε σε ένα οποιοδήποτε αξιοπρεπές σύγγραμμα Απειροστικού Λογισμού. Ενδεικτικά αναφέρουμε τα Theorem 3.5.4 και Theorem 8.3.17 στο [1].

7.1.1 Ασκήσεις

1. Δείξτε το ii, της Πρότασης 7.1.4.
2. Να αποδείξετε, με κάθε λεπτομέρεια, το Λήμμα 7.1.15.
3. Έστω r ένας θετικός ρητός αριθμός. Δείξτε ότι για κάθε πραγματικό αριθμό a υπάρχει $t \in a$ με $r + t \notin a$ (Δεν ξεχνάμε ότι οι πραγματικοί αριθμοί είναι τομές Dedekind, δηλαδή υποσύνολα των ρητών αριθμών).
4. Να αποδείξετε, με κάθε λεπτομέρεια, την Πρόταση 7.1.20.
5. Έστω A μη κενό υποσύνολο των πραγματικών αριθμών. Δείξτε ότι το A είναι φραγμένο, αν και μόνο αν υπάρχει $m \in \mathbb{R}$, ώστε $| x | \leq m$, για όλα τα $x \in A$.
6. Να συμπληρώσετε τα *κενά* στην απόδειξη του Λήμματος 7.1.24.
7. Να συμπληρώσετε την απόδειξη του Λήμματος 7.1.25.
8. Να συμπληρώσετε την απόδειξη της Πρότασης 7.1.26.
9. Να συμπληρώσετε την απόδειξη του Πορίσματος 7.1.27.

10. Να συμπληρώσετε την απόδειξη της Πρότασης 7.1.31.

11. Έστω $a, b \in \mathbb{R}$. Δείξτε ότι:

$$|\,a\,|-|\,b\,|\leq|\,(|\,a\,|-|\,b\,|)\,|\leq|\,a\pm b\,|\leq|\,a\,|+|\,b\,|\,.$$

Εξετάστε, πότε στις ανωτέρω ανισότητες ισχύει το ίσον.

12. Να συμπληρώσετε την απόδειξη του Θεωρήματος 7.1.28.

13. Να συμπληρώσετε τα κενά στην απόδειξη του Πορίσματος 7.1.34.

14. Έστω $a, r \in \mathbb{R}$ με $r > 0$.

i. Αν $x \in \mathbb{R}$, αποδείξτε ότι υπάρχει μοναδικός ακέραιος αριθμός n, ώστε

$$a+(n-1)r \leq x < a+nr.$$

ii. Έστω $x, y \in \mathbb{R}$. Υποθέτουμε ότι δεν υπάρχει $n \in \mathbb{Z}$, ώστε ο $a+nr$ να βρίσκεται αυστηρά μεταξύ των x και y. Δείξτε ότι

$$|\,x-y\,|\leq r.$$

7.2 Το σώμα των μιγαδικών αριθμών

7.2.1 Εισαγωγή - Η έννοια της φανταστικής μονάδας

Ας ξεκινήσουμε με ένα παράδειγμα:

Να βρεθούν δύο πραγματικοί αριθμοί x και y ώστε το γινόμενό τους να είναι ίσον με 6 και το άθροισμά τους ίσον με 5. Δηλαδή ζητούνται δύο πραγματικοί αριθμοί x και y ώστε να ικανοποιούν τις σχέσεις

$$x \cdot y = 6 \text{ και } x+y = 5.$$

Προφανώς η απάντηση είναι άμεση και έχουμε

$$x = 2 \text{ και } y = 3$$

(ή $x = 3$ και $y = 2$).

Αν τώρα έχουμε το ίδιο πρόβλημα, αλλά οι ζητούμενοι αριθμοί να ικανοποιούν τις σχέσεις

$$x \cdot y = 1 \text{ και } x+y = 4.$$

Τότε (λιγότερο άμεσα) μπορούμε να δούμε ότι πράγματι υπάρχουν πραγματικοί αριθμοί, οι οποίοι να ικανοποιούν αυτές τις σχέσεις, οι

$$x = 2-\sqrt{3} \text{ και } y = 2+\sqrt{3}$$

(και συμμετρικά $x = 2+\sqrt{3}$ και $y = 2-\sqrt{3}$).

Αν τώρα αναζητήσουμε πραγματικούς αριθμούς, οι οποίοι να ικανοποιούν τις σχέσεις

$$x \cdot y = 7 \text{ και } x+y = 4.$$

Τότε παρατηρούμε ότι **δεν** υπάρχουν πραγματικοί αριθμοί, οι οποίοι να ικανοποιούν τις σχέσεις αυτές. Πράγματι, από την δεύτερη σχέση έχουμε $y = 4 - x$, οπότε αντικαθιστώντας στην πρώτη έχουμε

$$x(4 - x) = 7,$$

δηλαδή

$$x^2 - 4x + 7 = 0,$$

απ' όπου έχουμε

$$(x - 2)^2 = -3.$$

Αυτό όμως είναι αδύνατον, διότι το τετράγωνο κάθε μη αρνητικού πραγματικού αριθμού δεν είναι αρνητικός αριθμός. Αν *αυθαιρετήσουμε* και από τα δύο μέλη της τελευταίας *ισότητας* λάβουμε τις τετραγωνικές ρίζες, οπότε έχουμε

$$x - 2 = \sqrt{-3},$$

δηλαδή

$$x = 2 + \sqrt{-3},$$

οπότε επανερχόμενοι στις αρχικές σχέσεις, έχουμε ότι

$$y = 2 - \sqrt{-3}$$

(συμμετρικά $x = 2 - \sqrt{-3}$ και $y = 2 + \sqrt{-3}$). Όπως βλέπουμε, αν θεωρήσουμε την *οντότητα* $\sqrt{-3}$ ως έναν "κατά φαντασίαν" αριθμό, μπορούμε με αλγεβρικούς "χειρισμούς" να απαντήσουμε στο αρχικό μας ερώτημα. Μάλιστα δε, θεωρώντας την σχέση

$$\sqrt{-3} = \sqrt{(-1)3} = \sqrt{-1} \cdot \sqrt{3},$$

το πρόβλημα εντοπίζεται στην *οντότητα* $\sqrt{-1}$. Για την υπερσκέλιση αυτού του προβλήματος τον 18^o αιώνα ο Euler επινόησε το σύμβολο i για την *οντότητα* $\sqrt{-1}$. Αμέσως απαντήθηκαν πολλά προβλήματα, τα οποία για πολλά χρόνια παρέμεναν αναπάντητα.

Για παράδειγμα, **κάθε** τετραγωνική εξίσωση

$$ax^2 + bx + c = 0,$$

με πραγματικούς συντελεστές a, b, c, έχει λύσεις, τις

$$\zeta_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

ανεξάρτητα αν η **διακρίνουσα** $\Delta = b^2 - 4ac$ είναι θετική, μηδέν ή αρνητική.

Στην πορεία το σύμβολο i έλαβε το όνομα **φανταστική μονάδα** και το σύνολο όλων των "εκφράσεων" της μορφής $a + ib$, όπου $a, b \in \mathbb{R}$ ονομάστηκε το σύνολο των **Μιγαδικών Αριθμών** και στο εξής θα συμβολίζεται με $\mathbb{C}$. Δηλαδή

$$\mathbb{C} = \{\, a + ib \mid a, b \in \mathbb{R} \,\}.$$

Χωρίς να ξεχνάμε ότι έχουμε *αυθαιρετήσει*,[8] θεωρώντας την φανταστική μονάδα

$$i = \sqrt{-1},$$

μπορούμε να *εφαρμόσουμε* τις γνωστές ιδιότητες των πράξεων στους πραγματικούς αριθμούς και να έχουμε

$$i^2 = (\sqrt{-1})^2 = -1,$$

οπότε μπορούμε να υπολογίσουμε όλες τις δυνάμεις i^n για κάθε φυσικό αριθμό n. Συγκεκριμένα ισχύει (γιατί;)

$$i^{4k+\upsilon} = i^{\upsilon} \text{ για } \upsilon = 0, 1, 2, 3.$$

Οπότε, μπορούμε να "επεκτείνουμε" την πρόσθεση και τον πολλαπλασιασμό, που ισχύουν στους πραγματικούς αριθμούς και να ορίσουμε πρόσθεση και πολλαπλασιασμό στους μιγαδικούς αριθμούς ως εξής:

$$(a + ib) \oplus (c + id) = (a + c) + i(b + d)$$

και

$$(a + ib) \odot (c + id) = (ac - bd) + i(ad + bc).$$

Παρατηρήσεις.

1. Στον ορισμό της πρόσθεσης και του πολλαπλασιασμού στους μιγαδικούς αριθμούς χρησιμοποιήσαμε, προσωρινά, τα σύμβολα $\oplus$ και $\odot$ αντίστοιχα για να δηλώσουμε ότι πρόκειται για "νέες" πράξεις στο "νέο" σύνολο $\mathbb{C}$.

2. Για τον ορισμό των πράξεων αυτών δεχθήκαμε η φανταστική μονάδα να "συμπεριφέρεται" όπως οι πραγματικοί αριθμοί (με μόνη επισήμανση ότι $i^2 = -1$) και εφαρμόσαμε τις γνωστές ιδιότητες της προσεταιριστικότητας και επιμερισμού του πολλαπλασιασμού ως προς την πρόσθεση.

3. Η έκφραση $a + ib$ ενός μιγαδικού αριθμού αποκτά τώρα έννοια και, όπως διαισθανόμαστε, ορίζουμε οι μιγαδικοί αριθμοί $a + ib$ και $c + id$ να είναι ίσοι, αν

   $$a = c \text{ και } b = d.$$

   Μάλιστα έχει επικρατήσει το μεν τμήμα a να ονομάζεται το *πραγματικό μέρος*, το δε τμήμα ib να ονομάζεται το *φανταστικό μέρος* του μιγαδικού αριθμού $a + ib$. (Πολλές φορές συνηθίζεται, χωρίς αυτό να δημιουργεί σύγχυση, ως φανταστικό μέρος να αναφέρεται το b).

Πριν προχωρήσουμε, στις ιδιότητες που αποκτά το σύνολο $(\mathbb{C}, \oplus, \odot)$ εφοδιασμένο με τις πράξεις που ορίσαμε, ας δούμε, πώς μπορούμε να "κατασκευάσουμε" τους μιγαδικούς αριθμούς με έναν πιο *αυστηρό* τρόπο, ο οποίος αφ' ενός αίρει τις προηγούμενες "αυθαιρεσίες", αφ' ετέρου ερμηνεύει την "συμπεριφορά" της φανταστικής μονάδας στον ορισμό της πρόσθεσης και πολλαπλασιασμού.

[8] Στην πραγματικότητα δεν πρόκειται για αυθαιρεσία. Είναι η δύναμη του ανθρωπίνου πνεύματος να επινοεί τρόπους, ώστε να υπερσκελίζει δυσκολίες και να λύνει προβλήματα....

7.3 Η κατασκευή των μιγαδικών αριθμών.

Στο καρτεσιανό γινόμενο

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$$

ορίζουμε δύο πράξεις ως εξής:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

και

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1).$$

Μπορούμε εύκολα να ελέγξουμε ότι οι δύο πράξεις είναι καλά ορισμένες (ιδέ Άσκηση $7.3.4_1$).

Πρόταση 7.3.1. *Το σύνολο* $(\mathbb{R}^2, +\cdot)$ *είναι σώμα.*

Απόδειξη. Ο έλεγχος ότι το σύνολο $(\mathbb{R}^2, +, \cdot)$ είναι σώμα είναι εύκολος.

Με ουδέτερο ως προς την πρόσθεση το $(0, 0)$ και ουδέτερο ως προς τον πολλαπλασιασμό το $(1, 0)$.

Η μόνη, ίσως, δυσκολία είναι η απόδειξη της ύπαρξης αντιστρόφου για ένα

$$(a, b) \neq (0, 0).$$

Ας προσπαθήσουμε. Έστω $(a, b) \neq (0, 0)$, αναζητούμε (αν υπάρχει) ένα $(x, y) \in \mathbb{R}^2$ ούτως ώστε

$$(a, b) \cdot (x, y) = (1, 0).$$

Κάνοντας τον πολλαπλασιασμό έχουμε

$$(ax - by, ay + bx) = (1, 0),$$

οπότε προκύπτει το σύστημα

$$\begin{cases} ax - by = 1 \\ ay + bx = 0 \end{cases}$$

Εύκολα βλέπουμε ότι η (μοναδική) λύση του συστήματος είναι η

$$x = \frac{a}{a^2 + b^2}, y = \frac{-b}{a^2 + b^2}.$$

Άρα

$$(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right).$$

Τα υπόλοιπα αφήνονται ως άσκηση (Άσκηση $7.3.4_2$). ό.έ.δ.

Τώρα είμαστε σε θέση να δούμε ότι το σύνολο $\mathbb{C}$ με στοιχεία τις αυθαίρετες εκφράσεις $a + ib$ αποκτά Μαθηματική υπόσταση.

Πρόταση 7.3.2. *Η απεικόνιση:*

$$\varphi : \mathbb{R}^2 \longrightarrow \mathbb{C} \text{ με } \varphi((x, y)) = x + iy.$$

Είναι πράγματι καλά ορισμένη απεικόνιση και μάλιστα 1-1 και επί.

Επιπλέον, η φ "διατηρεί" τις πράξεις της πρόσθεσης και πολλαπλασιασμού. Δηλαδή, για $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$, ισχύει ότι

$$\varphi((x_1, y_1) + (x_2, y_2)) = \varphi((x_1, y_1)) \oplus \varphi((x_2, y_2))$$

και

$$\varphi((x_1, y_1) \cdot (x_2, y_2)) = \varphi((x_1, y_1)) \odot \varphi((x_2, y_2)).$$

Απόδειξη. Η απόδειξη είναι προφανής και αφήνεται ως άσκηση (Άσκηση 7.3.4$_3$). ό.έ.δ.

Η προηγούμενη πρόταση μας επιτρέπει την "ταύτιση" κάθε διατεταγμένου ζεύγους (a, b) με τον μιγαδικό αριθμό $a + ib$, οπότε το σύνολο $(\mathbb{C}, \oplus, \odot)$ αποκτά την δομή ενός σώματος με ουδέτερο ως προς την πρόσθεση τον μιγαδικό αριθμό

$$\varphi(0, 0) = 0 + i0$$ [9]

και ουδέτερο ως προς τον πολλαπλασιασμό τον μιγαδικό αριθμό

$$\varphi(1, 0) = 1 + i0.$$

Από την ταύτιση αυτή, για την φανταστική μονάδα, έχουμε ότι $i \leftrightarrow (0, 1)$, οπότε

$$i^2 \leftrightarrow (0, 1) \cdot (0, 1) = (-1, 0) = -(1, 0),$$

το αντίθετο του μοναδιαίου στοιχείου $(1, 0)$.

Επίσης, από την ταύτιση αυτή, ο αντίστροφος ενός μη μηδενικού μιγαδικού αριθμού $z = a + ib$ είναι ο

$$z^{-1} = \frac{a}{a^2 + b^2} + i\frac{-b}{a^2 + b^2}.$$

Έχοντας υπόψιν το πώς υπολογίζονται οι δυνάμεις i^n της φανταστικής μονάδας για κάθε φυσικό αριθμό n, είναι τώρα εύκολο να υπολογίζουμε τις δυνάμεις i^m για κάθε ακέραιο m. Για παράδειγμα

$$i^{-1} = i^3 = -i.$$

Ας δούμε τώρα τη σχέση του συνόλου των πραγματικών αριθμών και του συνόλου των μιγαδικών αριθμών.

Ορίζουμε την εξής απεικόνιση:

$$\vartheta : \mathbb{R} \longrightarrow \mathbb{C} \text{ με } \vartheta(x) = x + i0.$$

Είναι εύκολο να δούμε ότι η ϑ είναι πράγματι απεικόνιση και μάλιστα 1-1. Επιπλέον, η ϑ "διατηρεί" τις πράξεις της πρόσθεσης και του πολλαπλασιασμού. Πράγματι, για $x, y \in \mathbb{R}$ έχουμε

$$\vartheta(x + y) = \vartheta(x) + \vartheta(y) \text{ και } \vartheta(x \cdot y) = \vartheta(x) \cdot \vartheta(y).$$

Δηλαδή η ϑ είναι ένας μονομορφισμός σωμάτων (προσπαθήστε το!).

Υπ' αυτήν την έννοια οι πραγματικοί αριθμοί θεωρούνται υποσύνολο των μιγαδικών αριθμών (κάθε πραγματικός αριθμός έχει μηδενικό φανταστικό μέρος).

[9] Όπως έχουμε ήδη επισημάνει, αντί του ορθού $\varphi((x, y))$, γράφουμε $\varphi(x, y)$, δεδομένου ότι δεν δημιουργείται σύγχυση.

Παρατηρήσεις 7.3.3.

1. Όπως είδαμε κάθε "αυθαιρεσία" τώρα αίρεται. Αλλά δεν πρέπει να λησμονούμε ότι ιστορικά οι "αυθαιρεσίες" αυτές οδήγησαν τους Μαθηματικούς στο να ορίσουν τον πολλαπλασιασμό στο $\mathbb{R}^2$ κατ' αυτόν τον "παράξενο" τρόπο

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1).$$

2. Συνοψίζοντας, επανερχόμενοι στο αρχικό μας παράδειγμα, βλέπουμε ότι, ενώ δεν υπάρχουν πραγματικοί αριθμοί, οι οποίοι να ικανοποιούν τις σχέσεις

$$x \cdot y = 7 \text{ και } x + y = 4,$$

θεωρώντας τις σχέσεις αυτές στο "ευρύτερο περιβάλλον" των μιγαδικών αριθμών, έχουμε λύση[10].

Δεν ξεχνάμε ότι το ίδιο κάναμε (κατασκευάζοντας τους ακεραίους αριθμούς) για να αντιμετωπίσουμε το πρόβλημα της αφαίρεσης ενός φυσικού αριθμού από έναν μικρότερό του.

Το ίδιο κάναμε (κατασκευάζοντας τους ρητούς αριθμούς) για να αποκτήσει κάθε μη μηδενικός ακέραιος αντίστροφο.

Το ίδιο κάναμε (κατασκευάζοντας τους πραγματικούς αριθμούς) για να αποκτήσει κάθε θετικός ρητός αριθμός τετραγωνική ρίζα.

Τώρα, κάθε αρνητικός πραγματικός αριθμός απέκτησε τετραγωνική ρίζα.

3. Έχοντας αποδείξει ότι το σύνολο $(\mathbb{R}^2, +, \cdot)$ είναι σώμα, και μέσω του ισομορφισμού φ, ότι το σύνολο $(\mathbb{C}, \oplus, \odot)$ είναι σώμα, στο εξής θα αναφερόμαστε στο *σώμα* των Μιγαδικών Αριθμών. Μάλιστα δε, πλέον δεν υπάρχει λόγος να έχουμε διαφορετικούς συμβολισμούς για την πρόσθεση και τον πολλαπλασιασμό και θα συμβολίζουμε $(\mathbb{C}, +, \cdot)$.

7.3.1 Συζυγείς Μιγαδικοί αριθμοί

Έστω $z = a + ib$ ένας μιγαδικός αριθμός, τότε ο μιγαδικός αριθμός $a - ib$ θα ονομάζεται **ο συζυγής** του $z = a + ib$ και θα συμβολίζεται $\bar{z} = a - ib$. Παρατηρούμε ότι $z + \bar{z} = 2a$ και $z - \bar{z} = 2ib$, μια απλή, αλλά πολύ χρήσιμη παρατήρηση.

Η επομένη πρόταση περιλαμβάνει μερικές στοιχειώδεις, αλλά πολύ σημαντικές ιδιότητες των συζυγών μιγαδικών αριθμών.

Πρόταση 7.3.4. *Έστω $z_1, z_2, z \in \mathbb{C}$, τότε ισχύουν:*

1. $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$.
2. $\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$.
3. $\bar{\bar{z}} = z$.
4. $\bar{z} = z$ *αν και μόνο αν* $z \in \mathbb{R}$.

[10] Εδώ πρέπει να αναφερθεί ότι: *The shortest path between two truths in the real domain passes through the complex domain*. Jacques Hadamard (1865-1963).

Απόδειξη. Η απόδειξη είναι άμεση εφαρμογή του ορισμού και αφήνεται ως άσκηση (Άσκηση 7.3.4$_4$). ό.έ.δ.

Πόρισμα 7.3.5. *Η απεικόνιση* $\varrho : \mathbb{C} \longrightarrow \mathbb{C}$ *με* $\varrho(z) = \bar{z}$ *είναι αυτομορφισμός (δηλαδή ομομορφισμός 1-1 και επί) του* $\mathbb{C}$ *με τον περιορισμό του στο σώμα* $\mathbb{R}$ *των πραγματικών αριθμών να είναι ο ταυτοτικός ομομορφισμός.*

Πόρισμα 7.3.6. *Έστω* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, *ένα πολυώνυμο με πραγματικούς συντελεστές.*

Υποθέτουμε ότι ο μιγαδικός αριθμός $z = a + ib$ *είναι ρίζα του* $p(x)$. *Τότε και ο συζυγής* $\bar{z} = a - ib$ *είναι ρίζα του* $p(x)$.

Απόδειξη. Ως γνωστόν ο z είναι ρίζα του πολυωνύμου, αν

$$p(z) = a_n z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 = 0.$$

Η τιμή του πολυωνύμου $p(x)$ στην θέση $\bar{z}$ είναι ο μιγαδικός αριθμός

$$p(\bar{z}) = a_n \bar{z}^n + a_{n-1}\bar{z}^{n-1} + \cdots + a_1 \bar{z} + a_0.$$

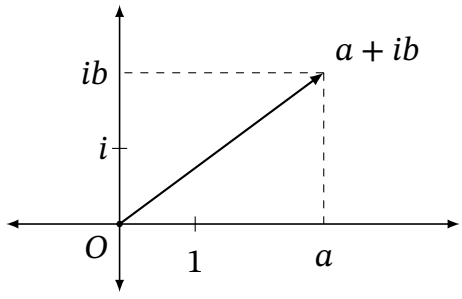
Από την προηγουμένη πρόταση, δεδομένου ότι $\bar{r} = r$, για όλους τους πραγματικούς αριθμούς r, έχουμε ότι

$$\begin{aligned} p(\bar{z}) &= a_n \bar{z}^n + a_{n-1}\bar{z}^{n-1} + \cdots + a_1 \bar{z} + a_0 \\ &= \overline{a_n z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0} \\ &= \overline{p(z)} = \bar{0} = 0. \end{aligned}$$

Επομένως, το $\bar{z}$ είναι ρίζα του πολυωνύμου $p(x)$. ό.έ.δ.

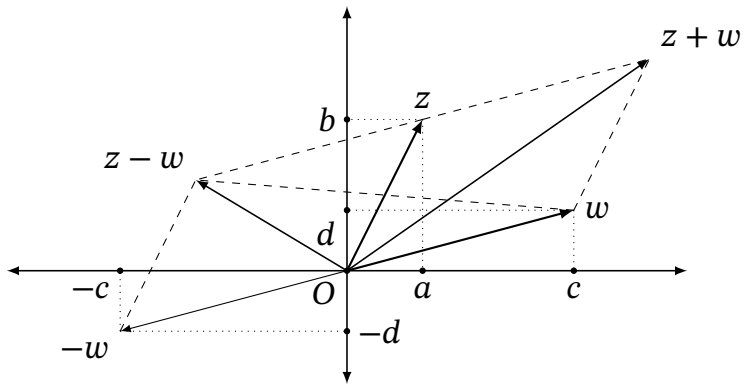
7.3.2 Γεωμετρική παράσταση των Μιγαδικών Αριθμών - Μέτρο Μιγαδικού Αριθμού

Όπως είδαμε στην σελίδα 287 κάθε μιγαδικός αριθμός μπορεί να αναπαρασταθεί με ένα διατεταγμένο ζεύγος στο Ευκλείδειο Επίπεδο και αντίστροφα. Αυτό μας επιτρέπει να αντιστοιχίσουμε κάθε μιγαδικό αριθμό $a + ib$ σε ένα διάνυσμα με αρχή την αρχή των αξόνων και πέρας το διατεταγμένο ζεύγος (a, b) όπως φαίνεται στο σχήμα 7.1. Η αναπαράσταση αυτή είναι πολύ χρήσιμη, τόσο για *εποπτικούς*, όσο και για λογιστικούς λόγους.



Σχήμα 7.1: *Γεωμετρική παράσταση του μιγαδικού αριθμού* $a + ib$.

Μπορούμε εύκολα να δούμε (προσπαθήστε το!) ότι το άθροισμα δύο μιγαδικών αντιστοιχεί στο άθροισμα των αντιστοίχων διανυσμάτων (*κανόνας του παραλληλογράμμου*). Όπως και η αφαίρεση μιγαδικών στην αφαίρεση (πρόσθεση του αντιθέτου) δύο διανυσμάτων. (Σχήμα 7.2)



Σχήμα 7.2: *Άθροισμα και διαφορά μιγαδικών αριθμών.*

Για τον λόγο αυτόν στο εξής θα ταυτίζουμε (και αυτό δεν θα προκαλεί σύγχυση) τις έννοιες Ευκλείδειο επίπεδο (το $\mathbb{R}^2$) και *Μιγαδικό επίπεδο* (το $\mathbb{C}$). Μάλιστα δε, τις περισσότερες φορές θα αναφέρουμε απλώς το επίπεδο[11].

Το μέτρο μιγαδικού αριθμού.

Έστω ο μιγαδικός αριθμός $z = a + ib$. Το αντίστοιχο διάνυσμα, που τον αναπαριστά, έχει αρχή το σημείο $(0, 0)$, την αρχή των αξόνων, και τέλος το σημείο (a, b). Επομένως, από το Πυθαγόρειο Θεώρημα, έχει μήκος ίσον με $\sqrt{a^2 + b^2}$. Το μέγεθος αυτό θα ονομάζεται **μέτρο** ή **απόλυτη τιμή** του μιγαδικού αριθμού $z = a+ib$ και συμβολίζεται

$$| z | = \sqrt{a^2 + b^2}.$$

Προφανώς το μέτρο μιγαδικού αριθμού είναι μη αρνητικός πραγματικός αριθμός ($| z | \geq 0$ και $| z | = 0$, αν και μόνο αν $z = 0$).

Για παράδειγμα, το μέτρο του μιγαδικού αριθμού $3 + i4$ ισούται με

$$\sqrt{3^2 + 4^2} = 5.$$

Η απόλυτη τιμή ενός μιγαδικού αριθμού επεκτείνει την γνωστή έννοια της απόλυτης τιμής ενός πραγματικού αριθμού (γιατί;).

Αν z, w είναι δύο μιγαδικοί αριθμοί, τότε το μέτρο

$$| z - w |$$

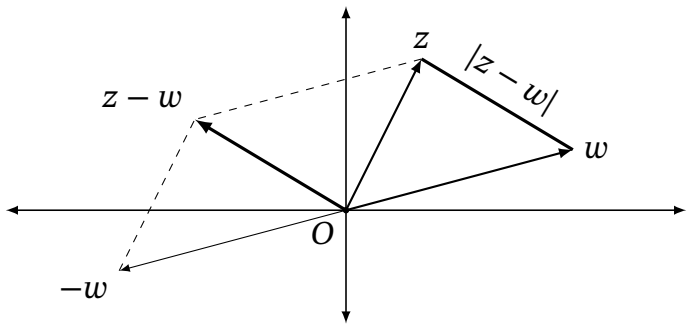
της διαφοράς τους καλείται **απόσταση** των δύο μιγαδικών αριθμών, διότι (ιδέ σχήμα 7.3) είναι ίσον με την (γεωμετρική) απόσταση των άκρων των διανυσμάτων που αντιστοιχούν στους δύο αυτούς μιγαδικούς αριθμούς. Μάλιστα δε, αν

$$z = a + ib \text{ και } w = c + id,$$

τότε

$$| z - w | = \sqrt{(a - c)^2 + (b - d)^2}.$$

[11] Στην βιβλιογραφία το μιγαδικό επίπεδο αναφέρεται και ως *διάγραμμα Argand*, από το όνομα του Γάλλου Μαθηματικού Argand, αν και, όπως οι ιστορικοί των Μαθηματικών αναφέρουν, για πρώτη φορά έγινε αντιστοίχιση των μιγαδικών αριθμών με τα σημεία του επιπέδου από τον Δανό Wessell το 1797.



Σχήμα 7.3: *Μέτρο διαφοράς μιγαδικών αριθμών.*

Πρόταση 7.3.7. *Έστω z, w δύο μιγαδικοί αριθμοί, τότε ισχύουν:*

i. $|z \cdot w| = |z| \cdot |w|$. Το μέτρο του γινομένου μιγαδικών αριθμών ισούται με το γινόμενο των μέτρων τους.

ii. $z \cdot \bar{z} = (|z|)^2$.

iii. $|\bar{z}| = |z|$.

iv. Στην περίπτωση, όπου $z \neq 0$, $|z^{-1}| = (|z|)^{-1}$.

Απόδειξη. Η απόδειξη είναι προφανής και στηρίζεται μόνο στον ορισμό του συζυγούς μιγαδικού αριθμού και στον ορισμό του μέτρου μιγαδικού αριθμού.

Εδώ θα αποδείξουμε μόνο την i. αφήνοντας τις υπόλοιπες ως άσκηση (Άσκηση 7.3.4$_5$).

i. Έστω $z = a + ib$ και $w = c + id$ δύο μιγαδικοί αριθμοί. Τότε, ως γνωστόν

$$z \cdot w = (ac - bd) + i(ad + bc),$$

οπότε για το μέτρο του γινομένου $z \cdot w$ έχουμε

$$|z \cdot w| = \sqrt{(ac - bd)^2 + (ad + bc)^2}.$$

Για το γινόμενο των μέτρων των δύο αυτών αριθμών έχουμε

$$|z| \cdot |w| = \sqrt{a^2 + b^2} \cdot \sqrt{c^2 + d^2}.$$

Συγκρίνοντας τις υπόριζες παραστάσεις στα δεύτερα μέλη των προηγουμένων σχέσεων με άμεσο υπολογισμό βλέπουμε ότι είναι ίσες. ό.έ.δ.

Όπως θα δούμε (ιδέ Θεώρημα 7.3.11) για το γινόμενο δύο μιγαδικών αριθμών ισχύει "κάτι περισσότερο".

Παρατηρήσεις 7.3.8.

1. Στην απόδειξη των ανωτέρω, συνήθως αποδεικνύουμε το ii., οπότε έπεται το iii.. Θα μπορούσατε να αποδείξετε (ανεξάρτητα) πρώτα το iii. και μετά να συνάγετε το ii.;

2. Από τα προηγούμενα έπεται μια άλλη έκφραση του αντιστρόφου ενός μη μηδενικού μιγαδικού αριθμού. Αν $0 \neq z \in \mathbb{C}$, τότε $z^{-1} = \bar{z}/|z|^2$. (Παράβαλλε με την εύρεση του αντιστρόφου ενός μιγαδικού αριθμού στην σελίδα 287).

3. Επίσης, από τα προηγούμενα, έπεται ότι μπορούμε (για λογιστικούς κυρίως λόγους), όταν έχουμε "κλάσματα" μιγαδικών αριθμών, να τα "απλοποιήσουμε" και να έχουμε κλάσματα με παρονομαστή πραγματικό αριθμό.

   Πράγματι, έστω $z = a+ib$ και $w = c+id$ δύο μιγαδικοί αριθμοί με $w \neq 0$. Το κλάσμα μιγαδικών αριθμών $\frac{z}{w}$ (στην πραγματικότητα το $\frac{z}{w}$ είναι άλλη έκφραση του $z \cdot w^{-1}$) ισούται με

$$\frac{z}{w} = \frac{z \cdot \bar{w}}{w \cdot \bar{w}} = \frac{z \cdot \bar{w}}{|\, w \,|^2}.$$

   Διαφορετικά

$$\frac{a+ib}{c+id} = \frac{(a+ib)(c-id)}{(c+id)(c-id)} = \frac{ac+bd}{c^2+d^2} + i\left(\frac{bc-ad}{c^2+d^2}\right)^{12}.$$

Πρόταση 7.3.9. ***(Η τριγωνική ιδιότητα)*** *Έστω z, w δύο μιγαδικοί αριθμοί, τότε ισχύουν:*

i. $|\, z + w \,| \leq |\, z \,| + |\, w \,|$.

ii. $||\, z \,| - |\, w \,|| \leq |\, z - w \,|$.

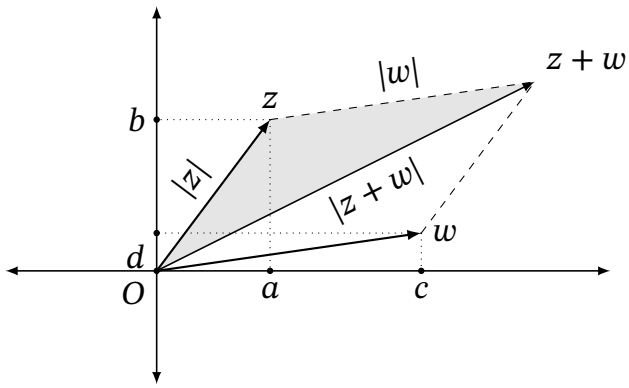
Απόδειξη. Υπάρχουν πολλές αποδείξεις για τις ανωτέρω ανισότητες. Εδώ θα δώσουμε δύο αποδείξεις για το i., μια Γεωμετρική και μια Αλγεβρική, αφήνοντας τα υπόλοιπα ως άσκηση (Άσκηση $7.3.4_6$).

1^{η} Απόδειξη:

Όπως έχουμε επισημάνει, για το άθροισμα δύο μιγαδικών αριθμών ισχύει ο κανόνας του *παραλληλογράμμου* (ιδέ σχήμα 7.4)

Θεωρούμε το τρίγωνο με κορυφές 0 (την αρχή των αξόνων), z και $z+w$. Η πλευρά με άκρα 0, z έχει μήκος ίσον με $|\, z \,|$ (Σχήμα 7.4), η πλευρά με άκρα 0, $z+w$ έχει μήκος ίσον με $|\, z+w \,|$, ενώ η τρίτη πλευρά, ως παράλληλη και ίση με την πλευρά, η οποία έχει άκρα 0, w, έχει μήκος ίσον με $|\, w \,|$, οπότε πράγματι ισχύει η σχέση

$$|\, z + w \,| \leq |\, z \,| + |\, w \,| \,.$$



Σχήμα 7.4: *Τριγωνική ανισότητα.*

[12] Εξ' ου και ο μνημονικός "κανόνας": *Μετατρέπουμε τους μιγαδικούς παρονομαστές σε πραγματικούς πολλαπλασιάζοντάς τους με τον αντίστοιχο συζυγή μιγαδικό αριθμό.*

2^{η} Απόδειξη:
Έστω $z = a + ib$ και $w = c + id$.
Γνωρίζουμε ότι στους πραγματικούς αριθμούς ισχύει η ανισότητα

$$2abcd \leq (ad)^2 + (bc)^2.$$

Προσθέτουμε και στα δύο μέλη την ποσότητα $(ac)^2 + (bd)^2$ και έχουμε

$$(ac)^2 + (bd)^2 + 2abcd \leq (ac)^2 + (bd)^2 + (ad)^2 + (bc)^2,$$

δηλαδή

$$(ac + bd)^2 \leq (a^2 + b^2)(c^2 + d^2).$$

Στην τελευταία σχέση παίρνουμε τις τετραγωνικές ρίζες και στα δύο μέλη και η ανισότητα διατηρείται (γιατί;). Άρα έχουμε

$$ac + bd \leq \sqrt{(a^2 + b^2)(c^2 + d^2)},$$

πολλαπλασιάζοντας και τα δύο μέλη της σχέσης αυτής με το 2 έχουμε

$$2ac + 2bd \leq 2\sqrt{(a^2 + b^2)(c^2 + d^2)} \qquad (*)$$

Προσθέτουμε και στα δύο μέλη της σχέσης αυτής το $a^2 + b^2 + c^2 + d^2$ και κάνουμε τις πράξεις, οπότε έχουμε

$$\begin{aligned}(a + c)^2 + (b + d)^2 &\leq (\sqrt{a^2 + b^2})^2 + (\sqrt{c^2 + d^2})^2 + 2\sqrt{(a^2 + b^2)(c^2 + d^2)} \\ &= (\sqrt{a^2 + b^2} + \sqrt{c^2 + d^2})^2.\end{aligned}$$

Στην τελευταία ανισότητα παίρνουμε τις τετραγωνικές ρίζες και στα δύο μέλη και έχουμε

$$\sqrt{(a + c)^2 + (b + d)^2} \leq \sqrt{a^2 + b^2} + \sqrt{c^2 + d^2}.$$

Δηλαδή την προς απόδειξη σχέση

$$| z + w | \leq | z | + | w | . \qquad \text{ό.έ.δ.}$$

Παρατήρηση 7.3.10. Η πρώτη απόδειξη είναι εποπτική και στηρίζεται στο "διαισθητικό" *Η ευθεία είναι η συντομοτέρα οδός*. Αυτό είμαστε σε θέση να το αποδείξουμε;

Η δεύτερη απόδειξη φαντάζει πολύπλοκη και "εξωπραγματική", καθότι γεννάται το ερώτημα: Πώς φανταστήκαμε να ξεκινήσουμε από την ανισότητα

$$2abcd \leq (ad)^2 + (bc)^2;$$

Σε αυτό μας οδηγεί η *ανάλυση* του προβλήματος.
Έστω $z = a + ib$ και $w = c + id$. Η προς απόδειξη σχέση

$$| z + w | \leq | z | + | w |$$

είναι ισοδύναμη με την

$$\sqrt{(a + c)^2 + (b + d)^2} \leq \sqrt{a^2 + b^2} + \sqrt{c^2 + d^2}.$$

Υψώνοντας στο τετράγωνο και τα δύο (μη αρνητικά) μέλη της σχέσης αυτής έχουμε την ισοδύναμη σχέση

$$(a+c)^2+(b+d)^2 \leq (a^2+b^2)+(c^2+d^2)+2\sqrt{(a^2+b^2)(c^2+d^2)},$$

στην τελευταία σχέση κάνουμε τις πράξεις και καταλήγουμε στην ισοδύναμη σχέση

$$2ac+2bd \leq 2\sqrt{(a^2+b^2)(c^2+d^2)}.$$

Δηλαδή στη σχέση $(*)$.

Εδώ πρέπει να επισημάνουμε ότι την τριγωνική ιδιότητα την έχουμε ήδη συναντήσει στους πραγματικούς αριθμούς (Πρόταση 7.1.31). Οπότε, η Πρόταση 7.1.31 θα μπορούσε να θεωρηθεί ως πόρισμα της προηγουμένης πρότασης.

Μπορείτε να συγκρίνετε την απόδειξη που εδόθη εκεί με τις αποδείξεις, οι οποίες δίνονται εδώ;

Όπως βλέπουμε, οι ανωτέρω ανισότητες εμφανίζονται μεταξύ μέτρων πραγματικών αριθμών. Γεννάται το ερώτημα:

"Μπορούμε να ορίσουμε μια διάταξη στο σύνολο $\mathbb{C}$ των μιγαδικών αριθμών;"

Όπως τίθεται το ερώτημα, η απάντηση είναι καταφατική (ιδέ Παρατήρηση 4.4.26).

Ας εξειδικεύσουμε το ερώτημα:

"Μπορούμε να ορίσουμε μια διάταξη στο σύνολο $\mathbb{C}$ των μιγαδικών αριθμών *παρόμοια* με την διάταξη των πραγματικών αριθμών;"

Στους πραγματικούς αριθμούς έχουμε ορίσει μια (ολική) διάταξη όπου ισχύει ότι: Αν $r, s, t \in \mathbb{R}$ με $r < s$, τότε $r+t < s+t$. Αν επιπλέον $t > 0$, τότε $rt < st$ (Θεώρημα 7.1.28).

Ας υποθέσουμε ότι έχουμε μια *παρόμοια* ολική διάταξη στους μιγαδικούς αριθμούς, τότε για την φανταστική μονάδα i θα ίσχυε ότι $i > 0$ ή $i < 0$. Έστω $i > 0$, τότε θα έπρεπε να έχουμε $i^2 = -1 > 0$, αυτό όμως είναι άτοπο.

Όμοια αποδεικνύεται ότι δεν είναι δυνατόν να ισχύει $i < 0$.

Εφαρμογές- Παραδείγματα.

Προς εμπέδωση των ανωτέρω, θα δούμε ορισμένα παραδείγματα και εφαρμογές.

1. Έστω ο μιγαδικός αριθμός $z = a+ib$. Έχουμε ορίσει τον συζυγή $\bar{z} = a-ib$.

   Γνωρίζουμε την γεωμετρική παράσταση του z (ιδέ σχήμα 7.1). Αν θελήσουμε να αναπαραστήσουμε τον συζυγή $\bar{z}$ στο επίπεδο. Ποία η θέση του σε σχέση με την θέση του z;

   Προφανώς, τα δύο σημεία z και $\bar{z}$ είναι συμμετρικά ως προς τον άξονα των πραγματικών αριθμών (γιατί;).

2. Έστω ο μη μηδενικός μιγαδικός αριθμός $z = a+ib$. Έχουμε ορίσει τον αντίστροφό του z^{-1}.

   Αν θελήσουμε να αναπαραστήσουμε τον αντίστροφο z^{-1} στο επίπεδο. Ποια η θέση του σε σχέση με την θέση του z;

   Δεν ξεχνάμε ότι

$$z^{-1} = \frac{a}{a^2+b^2} + i\frac{-b}{a^2+b^2},$$

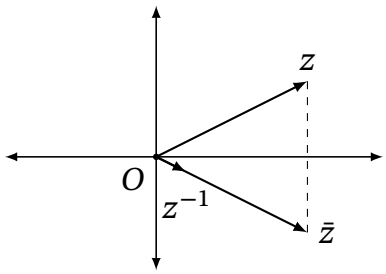
οπότε, θα έλεγε κάποιος, δεν έχουμε παρά να τον αναπαραστήσουμε στο επίπεδο με το ζεύγος

$$\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right).$$

Αλλά δεν ξεχνάμε ότι $z^{-1} = \bar{z}/\mid z \mid^2$ (ιδέ Παρατήρηση 7.3.8).

Επομένως, συμπεραίνουμε ότι η αναπαράσταση του z^{-1} στο επίπεδο είναι ένα σημείο το οποίο βρίσκεται στην ίδια ευθεία, που διέρχεται από την αρχή των αξόνων και διέρχεται από το σημείο $(a, -b)$. Δηλαδή στον φορέα, ο οποίος καθορίζεται από τον συζυγή μιγαδικό $\bar{z} = a - ib$ (ιδέ σχήμα 7.5).

Δεν έχουμε παρά να πειραματισθούμε επιλέγοντας συγκεκριμένους μιγαδικούς αριθμούς.



Σχήμα 7.5: *Αντίστροφος μιγαδικού αριθμού.*

3. Αναζητούμε (αν υπάρχει) έναν μιγαδικό αριθμό z, ώστε $z^2 = i$. Δηλαδή αναζητούμε την *τετραγωνική ρίζα* της φανταστικής μονάδας.

   Έστω $z = x + iy$ ο μιγαδικός αριθμός, που αναζητούμε. Τότε

   $$z^2 = (x + iy)(x + iy) = i.$$

   Αυτό σημαίνει ότι

   $$(x^2 - y^2) + i(2xy) = i.$$

   Δηλαδή

   $$x^2 = y^2 \text{ και } 2xy = 1.$$

   Επομένως, εύκολα έπεται ότι

   $$x = y = \frac{\sqrt{2}}{2} \text{ ή } x = y = -\frac{\sqrt{2}}{2}.$$

   Άρα υπάρχουν δύο τετραγωνικές ρίζες της φανταστικής μονάδας.

4. Σε συνέχεια των προηγουμένων, αν $z = a + ib$, αναζητούμε (αν υπάρχει) έναν μιγαδικό αριθμό $w = x+iy$, ώστε $w^2 = z$. Δηλαδή αναζητούμε την *τετραγωνική ρίζα* του (τυχαίου) μιγαδικού αριθμού z. Από την ισότητα

   $$(x + iy)(x + iy) = a + ib$$

   έχουμε ότι

   $$(x^2 - y^2) + i(2xy) = a + ib.$$

Επομένως, αναζητούμε πραγματικούς αριθμούς, οι οποίοι να ικανοποιούν τις ισότητες

$$x^2 - y^2 = a \text{ και } 2xy = b.$$

Οπότε, μπορούμε (;) να υπολογίσουμε τα ζητούμενα x και y.

Εδώ θα πρέπει να παρατηρήσουμε ότι ο υπολογισμός των x και y δεν είναι ακατόρθωτος, αλλά είναι χρονοβόρος. Υπάρχει κάποιος άλλος (πιο εύκολος) τρόπος να υπολογίζουμε την τετραγωνική ρίζα ενός μιγαδικού αριθμού; Επ' αυτού θα επανέλθουμε αργότερα (ιδέ σελ. 302).

Ο μοναδιαίος κύκλος.

Προφανώς οι αριθμοί $1, -1, i, -i$ έχουν μέτρο 1. Γεννάται το ερώτημα: Υπάρχουν και άλλοι μιγαδικοί αριθμοί, οι οποίοι έχουν μέτρο 1 και πώς μπορούμε να τους βρούμε όλους;

Προφανώς ένας μιγαδικός αριθμός $z = x + iy$ με μέτρο 1 ικανοποιεί τη σχέση

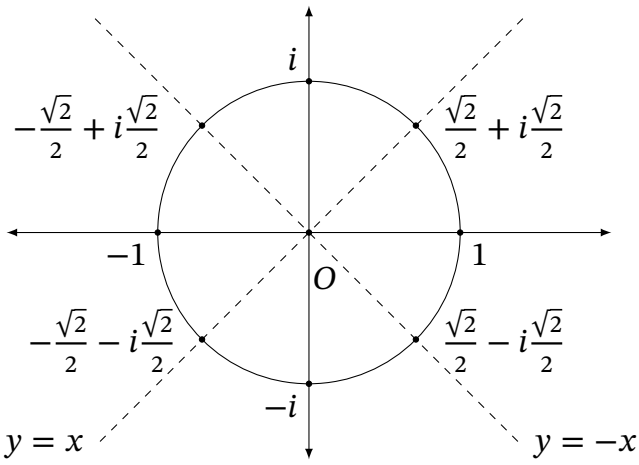
$$| x | = \sqrt{x^2 + y^2} = 1,$$

δηλαδή $x^2 + y^2 = 1$, απ' όπου έπεται ότι το σημείο με συντεταγμένες (x, y) βρίσκεται στην περιφέρεια ενός κύκλου με κέντρο την αρχή των αξόνων και ακτίνα ίση με 1. Προφανώς ισχύει και το αντίστροφο, κάθε σημείο (μιγαδικός αριθμός z) που ανήκει στην περιφέρεια αυτού του κύκλου έχει μέτρο ίσον με ένα ($| z | = 1$). Ο κύκλος αυτός ονομάζεται **μοναδιαίος κύκλος**. Προφανώς οι τέσσερις μιγαδικοί αριθμοί

$$\pm\sqrt{2}/2 \pm i\sqrt{2}/2,$$

(όπου τα πρόσημα + και - λαμβάνονται με όλους τους δυνατούς συνδυασμούς), έχουν απόλυτη τιμή ίση με ένα. Οι τέσσερις αυτοί αριθμοί προφανώς (;) είναι τα σημεία τομής του μοναδιαίου κύκλου με τις διαγώνιες ευθείες $y = x$ και $y = -x$ (ιδέ σχήμα 7.6).

Θα επανέλθουμε στον μοναδιαίο κύκλο, όταν μιλήσουμε για την (γεωμετρική) παράσταση του γινομένου δύο μιγαδικών αριθμών.

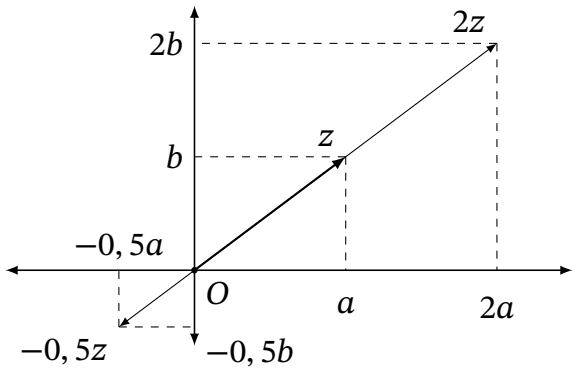


Σχήμα 7.6: *Σημεία τομής μοναδιαίου κύκλου με τις* $y = \pm x$.

Γεωμετρική παράσταση του γινομένου μιγαδικών αριθμών - Πολικές συντεταγμένες.

Πριν δούμε την γενική περίπτωση, θα δούμε δύο μερικά παραδείγματα.

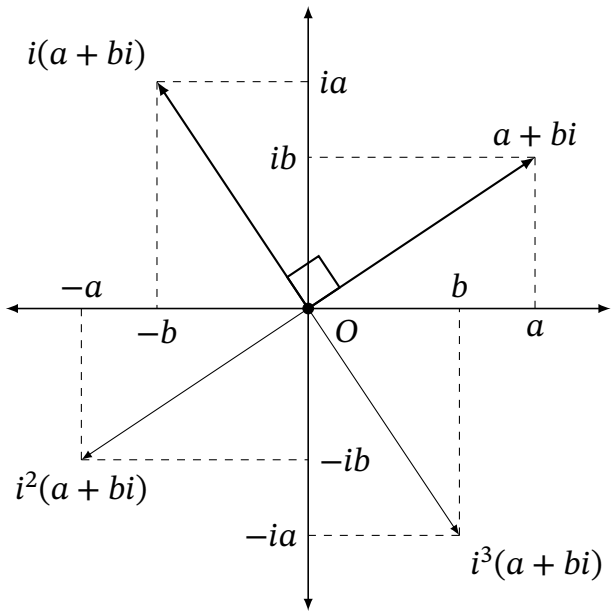
1. Έστω $z = a + ib$ ένας μιγαδικός αριθμός και r ένας πραγματικός αριθμός, τότε το γινόμενο
$$rz = (ra) + i(rb)$$
είναι ένας μιγαδικός αριθμός, ο οποίος γεωμετρικά παρίσταται από το ζεύγος
$$(ra, rb).$$
Δηλαδή βρίσκεται στην ίδια ευθεία που διέρχεται από την αρχή των αξόνων και το ζεύγος (a, b) (Βλέπε σχήμα 7.7), και προφανώς έχει μέτρο ίσον με
$$|\, r \,| \cdot |\, z \,| .$$



Σχήμα 7.7: *Γινόμενο μιγαδικού με πραγματικό.*

2. Έστω τώρα ο μιγαδικός αριθμός $z = a + ib$, τον οποίο θέλουμε να πολλαπλασιάσουμε με την φανταστική μονάδα i. Τότε έχουμε
$$iz = -b + ia.$$
Οι δύο μιγαδικοί αριθμοί z και iz προφανώς έχουν ίσα μέτρα. Αν παραστήσουμε στο επίπεδο τους δύο μιγαδικούς αριθμούς, (ιδέ σχήμα 7.8), z και iz, βλέπουμε ότι οι δύο ευθείες που ορίζονται από τα σημεία
$$0 \text{ και } (a, b) \text{ και } 0 \text{ και } (-b, a)$$
είναι κάθετες (γιατί;). Δηλαδή ο πολλαπλασιασμός με το i έχει επιφέρει μια στροφή (με κέντρο την αρχή των αξόνων και αριστερόστροφα) του σημείου z έως το σημείο iz κατά γωνία ίση με $\pi/2$.

Παρομοίως ο πολλαπλασιασμός του z με το $-i$ επιφέρει μια στροφή (με κέντρο την αρχή των αξόνων και δεξιόστροφα) του σημείου z έως το σημείο $-iz$.



Σχήμα 7.8: *Γινόμενο μιγαδικού με την φανταστική μονάδα.*

Γεννάται τώρα το ερώτημα: Αν έχουμε δύο (τυχαίους) μιγαδικούς αριθμούς

$$z = a + ib \text{ και } w = c + id,$$

ποια η γεωμετρική παράσταση του γινομένου zw σε σχέση με την γεωμετρική παράσταση των z και w;

Πριν προχωρήσουμε, θα δούμε έναν άλλο τρόπο παράστασης ενός μιγαδικού αριθμού ως σημείο στο επίπεδο $\mathbb{R}^2$.

Έστω ο μη μηδενικός μιγαδικός αριθμός $z = a+ib$. Μπορούμε να προσδιορίσουμε το σημείο (a, b) και με τον εξής τρόπο: Μετράμε την γωνία, έστω θ, που σχηματίζει ο θετικός ημιάξονας των x με την ημιευθεία με αρχή των αξόνων και η οποία διέρχεται από το σημείο (a, b). Θεωρούμε ως αρχική πλευρά της γωνίας αυτής τον θετικό ημιάξονα και κινούμενοι αριστερόστροφα θεωρούμε τελική πλευρά την ημιευθεία με αρχή των αξόνων και η οποία διέρχεται από το σημείο (a, b). Μετράμε την απόσταση r του σημείου (a, b) από την αρχή των αξόνων. Το σημείο (a, b) (άρα ο μιγαδικός αριθμός $z = a + ib$) είναι τώρα πλήρως καθορισμένος από την απόσταση r και την γωνία θ. Προφανώς η απόσταση r είναι το μέτρο

$$| z | = \sqrt{a^2 + b^2}.$$

Η γωνία θ ονομάζεται **όρισμα** του μιγαδικού αριθμού z και συμβολίζεται με

$$\theta = arg(z)\ ^{13}.$$

Το ζεύγος $(| z |, arg(z))$ ονομάζεται **πολικές συντεταγμένες** του μιγαδικού αριθμού z. Η σχέση που συνδέει τις καρτεσιανές συντεταγμένες (a, b) και τις πολικές συντεταγμένες $(| z |, arg(z))$ είναι προφανώς η εξής:

$$a = | z | \cdot \cos(\theta) \text{ και } b = | z | \cdot \sin(\theta) \text{ (γιατί;)}.$$

[13] Προσοχή! Για τον μηδενικό μιγαδικό αριθμό $0 = 0 + i0$ **δεν** ορίζεται όρισμα (γιατί;). Επομένως, όταν αναφερόμαστε στο όρισμα ενός μιγαδικού αριθμού, σιωπηλά, θα θεωρούμε ότι πρόκειται για μη μηδενικό μιγαδικό αριθμό.

Δηλαδή

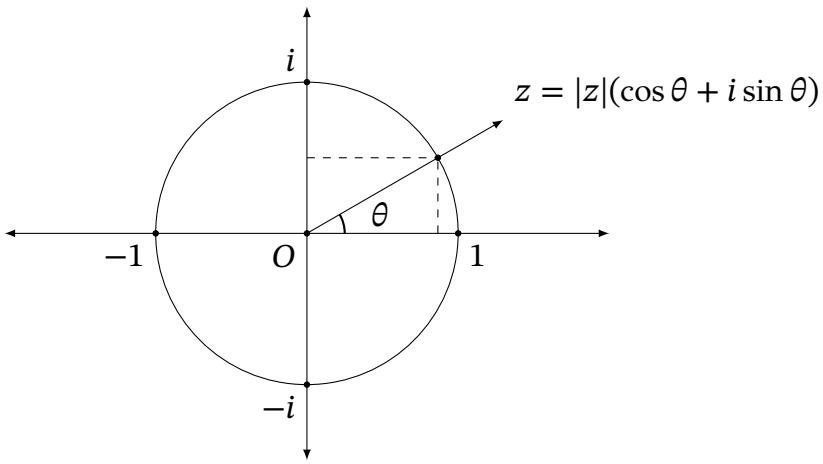
$$\begin{aligned} z &= a + ib \\ &= |\, z \,| \cdot \cos(\theta) + i(|\, z \,| \cdot \sin(\theta)) \\ &= |\, z \,| \cdot (\cos(\theta) + i \sin(\theta)) \ [14]. \end{aligned}$$

Ο μιγαδικός αριθμός

$$\cos(\theta) + i \sin(\theta)$$

έχει προφανώς μέτρο ίσον με 1 ($\cos(\theta)^2 + \sin(\theta)^2 = 1$). Η παρατήρηση αυτή μας οδηγεί στο:

Συμπέρασμα. Κάθε μιγαδικός αριθμός είναι το γινόμενο ενός πραγματικού αριθμού και ενός μιγαδικού, ο οποίος βρίσκεται επί του μοναδιαίου κύκλου (ιδέ σχήμα 7.9).



Σχήμα 7.9: *Τριγωνομετρική μορφή μιγαδικού αριθμού.*

Τώρα είμαστε σε θέση να απαντήσουμε στο προηγούμενο ερώτημα. Δηλαδή πώς σχετίζεται η γεωμετρική παράσταση του γινομένου zw με τις γεωμετρικές παραστάσεις των z και w.

Θεώρημα 7.3.11. ***(Θεώρημα De Moivre)*** *Έστω οι μιγαδικοί αριθμοί z και w με πολικές συντεταγμένες*

$$z = r_1(\cos(\theta_1) + i \sin(\theta_1)) \text{ και } w = r_2(\cos(\theta_2) + i \sin(\theta_2)),$$

τότε ισχύει

$$z \cdot w = r_1 r_2(\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)).$$

Δηλαδή το γινόμενο δύο μιγαδικών αριθμών έχει μέτρο ίσον με το γινόμενο των μέτρων τους και όρισμα ίσον με το άθροισμα των ορισμάτων τους (ιδέ σχήμα 7.10).

[14] Επισημαίνεται ότι: Λόγω του ότι $\cos(\theta) = \cos(\theta + 2k\pi)$ και $\sin(\theta) = \sin(\theta + 2k\pi)$, $k \in \mathbb{Z}$, για έναν μιγαδικό αριθμό υπάρχουν πολλά ορίσματα, αλλά για κάθε μιγαδικό αριθμό υπάρχει μοναδικό (γιατί;) όρισμα στο διάστημα $-\pi < \theta \leq \pi$. Οπότε, χωρίς βλάβη, θα μιλάμε για **το** όρισμα ενός (μη μηδενικού) μιγαδικού αριθμού.

Απόδειξη. Η απόδειξη είναι άμεση, αρκεί να θυμηθούμε τις γνωστές (;) από την τριγωνομετρία, σχέσεις

$$\cos(\theta+\phi) = \cos(\theta)\cos(\phi) - \sin(\theta)\sin(\phi)$$

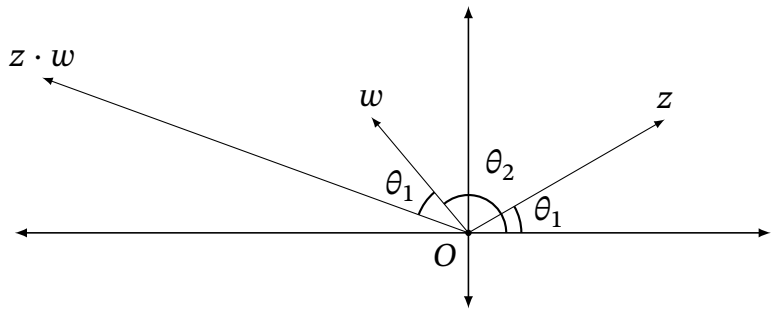
και

$$\sin(\theta+\phi) = \cos(\theta)\sin(\phi) + \sin(\theta)\cos(\phi)$$

Για το γινόμενο $z \cdot w$ έχουμε

$$\begin{aligned} z \cdot w &= (r_1(\cos(\theta_1) + i\sin(\theta_1))) \cdot (r_2(\cos(\theta_2) + i\sin(\theta_2))) \\ &= (r_1 r_2)(\cos(\theta_1) + i\sin(\theta_1)) \cdot (\cos(\theta_2) + i\sin(\theta_2)) \\ &= (r_1 r_2)(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)). \end{aligned}$$

ό.έ.δ.



Σχήμα 7.10: *Γινόμενο μιγαδικών αριθμών.*

Πόρισμα 7.3.12. *Έστω* $z = r(\cos(\theta) + i\sin(\theta))$, *τότε για κάθε θετικό ακέραιο* n *ισχύει:*

i. $z^n = r^n(\cos(n\theta) + i\sin(n\theta))$.

ii. $z^{-n} = r^{-n}(\cos(n\theta) - i\sin(n\theta))$.

Απόδειξη.

i. Για $n = 2$ από το προηγούμενο θεώρημα έχουμε

$$z^2 = r \cdot r(\cos(\theta+\theta) + i\sin(\theta+\theta)) = r^2(\cos(2\theta) + i\sin(2\theta)).$$

Οπότε, επαναληπτικά έπεται το αποτέλεσμα[15].

ii. Γνωρίζουμε γενικά ότι ο αντίστροφος ενός μιγαδικού αριθμού w ισούται με

$$w^{-1} = \frac{\bar{w}}{|\, w \,|^2},$$

[15]Εδώ πρέπει να είμαστε προσεκτικοί. Όταν λέμε επαναληπτικά, σημαίνει ότι εφαρμόζουμε την προσεταιριστική ιδιότητα του πολλαπλασιασμού μιγαδικών αριθμών $z^{n+1} = (z^n)\cdot z$. Δηλαδή, στο...βάθος εφαρμόζουμε επαγωγή.

οπότε

$$\begin{aligned} z^{-n} &= (z^n)^{-1} \\ &= \frac{\overline{z^n}}{|\, z^n \,|^2} && \text{(από το πρώτο ερώτημα)} \\ &= \frac{r^n(\cos(n\theta) - i\sin(n\theta)}{(r^n)^2} \\ &= r^{-n}(\cos(n\theta) - i\sin(n\theta)) \,. \end{aligned}$$

ό.έ.δ.

Από το προηγούμενο πόρισμα έπεται η γνωστή (;) τριγωνομετρική ισότητα:
Για κάθε ακέραιο αριθμό n ισχύει.

$$(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta).$$

(Την ισότητα αυτή την έχουμε ήδη συναντήσει, ιδέ Άσκηση 3.2.11$_{17}$). Στο προηγούμενο πόρισμα είδαμε πώς υπολογίζουμε δυνάμεις μιγαδικών αριθμών. Δηλαδή για $z \in \mathbb{C}$ και $n \in \mathbb{N}$ πώς επιλύεται η εξίσωση

$$x = z^n \text{ στο } \mathbb{C}.$$

Υπάρχει και το δυϊκό πρόβλημα:

Για $z \in \mathbb{C}$ και $n \in \mathbb{N}$ να επιλυθεί η εξίσωση

$$x^n = z \text{ στο } \mathbb{C}. \qquad (*)$$

Δηλαδή, πώς βρίσκουμε ρίζες μιγαδικών αριθμών;
Ας υποθέσουμε ότι

$$z = r(\cos(\theta) + i\sin(\theta)),$$

αναζητούμε έναν μιγαδικό αριθμό

$$w = s(\cos(\varphi) + i\sin(\varphi))$$

έτσι ώστε $w^n = z$, δηλαδή

$$s^n(\cos(n\varphi) + i\sin(n\varphi)) = r(\cos(\theta) + i\sin(\theta)).$$

Από την τελευταία σχέση έπεται ότι

$$s = \sqrt[n]{r},\ \cos(n\varphi) = \cos(\theta) \text{ και } \sin(n\varphi) = \sin(\theta).$$

Από τις σχέσεις αυτές έπεται ότι το όρισμα του ζητουμένου μιγαδικού w ισούται με

$$arg(w) = \varphi = \frac{\theta + 2k\pi}{n}$$

για $k = 0, 1, \ldots, n-1$. Δηλαδή υπάρχουν n το πλήθος (διακεκριμένοι) μιγαδικοί αριθμοί, οι οποίοι ικανοποιούν την εξίσωση $(*)$ και ονομάζονται **n-οστές ρίζες** του μιγαδικού αριθμού z.

Σχόλια 7.3.13. Προηγουμένως (ιδέ Παράδειγμα 7.3.2.2$_4$), είχαμε υπολογίσει την τετραγωνική ρίζα ενός μιγαδικού αριθμού, χωρίς την χρήση πολικών συντεταγμένων. Παρατηρήστε την διαφορά, ως προς την ευκολία, με την χρήση πολικών συντεταγμένων.

Επίσης, παρατηρήστε την "δυσκολία", που έχουμε να υπολογίσουμε το όρισμα του αθροίσματος δύο μιγαδικών αριθμών, όταν γνωρίζουμε τα ορίσματά τους.

n-οστές ρίζες της μονάδος

Στην ειδική περίπτωση, όπου έχουμε την εξίσωση

$$x^n = 1,\ n \in \mathbb{N},$$

θα μιλάμε για n-οστές ρίζες της μονάδος.

Σύμφωνα με τα προηγούμενα, δεδομένου ότι

$$1 = \cos(0) + i\sin(0),$$

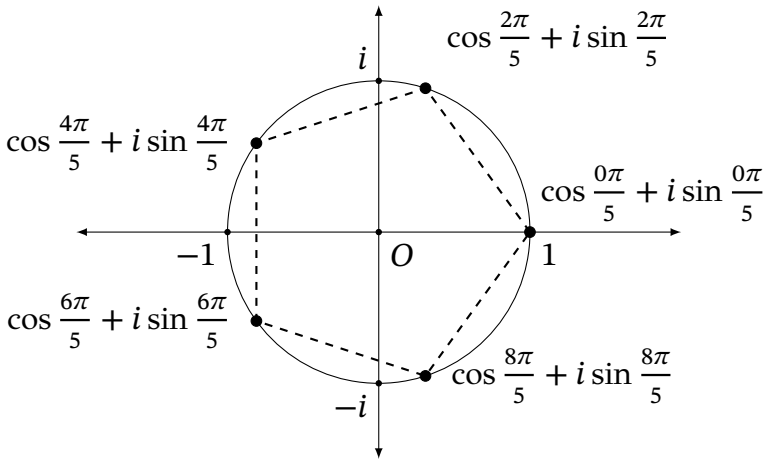
ένας μιγαδικός αριθμός που ικανοποιεί την εξίσωση $x^n = 1$ θα είναι της μορφής

$$z_k = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)$$

για $k = 0, 1, \ldots, n-1$.

Για παράδειγμα, όπως έχουμε επισημάνει από την αρχή (σελ. 285), οι 4-τες ρίζες της μονάδος είναι οι $1, i, -1, -i$.

Προφανώς κάθε n-οστή ρίζα της μονάδος έχει μέτρο ίσον με ένα και, στην γεωμετρική της παράσταση, βρίσκεται επί του μοναδιαίου κύκλου. Μάλιστα δε (σχηματικά) οι n-οστές ρίζες της μονάδος αποτελούν τις κορυφές ενός κανονικού n-γώνου εγγεγραμμένου στον μοναδιαίο κύκλο με την μια κορυφή να αποτελεί το σημείο με συντεταγμένες $(1, 0)$.



Σχήμα 7.11: *5-τες ρίζες της μονάδος.*

Ας εντρυφήσουμε περισσότερο στις n-οστές ρίζες της μονάδος.

Έστω

$$C_n = \{z_0 = 1, z_1, z_2, \ldots, z_{n-1}\}$$

το σύνολο όλων των n-οστών ριζών της μονάδος.

Παρατηρούμε ότι, για $z_i, z_j \in C_n$, ισχύει ότι

$$(z_i \cdot z_j)^n = z_i^n \cdot z_j^n = 1.$$

Επομένως, το σύνολο C_n είναι κλειστό ως προς την πράξη του πολλαπλασιασμού μιγαδικών αριθμών. Συνεπώς, αποτελεί ομάδα, ως προς αυτήν την πράξη (γιατί;).

Η ομάδα $(C_n, \cdot)$ θα ονομάζεται η ομάδα των n-οστών ριζών της μονάδος και προφανώς έχει τάξη ίση με n.

Επίσης, παρατηρούμε ότι

$$z_1^k = \left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)^k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = z_k,$$

για όλα τα $k = 0, 1, \ldots, n-1$. Μάλιστα δε η τάξη του στοιχείου z_1 είναι ίση με n.

Συνεπώς, η ομάδα $(C_n, \cdot)$ είναι κυκλική τάξης n [16].

Πρόταση 7.3.14. *Το σύνολο $C_n = \{z_0 = 1, z_1, z_2, \ldots, z_{n-1}\}$ των n-οστών ριζών της μονάδος αποτελεί κυκλική ομάδα με τάξη ίση με n, ως προς την πράξη του πολλαπλασιασμού μιγαδικών αριθμών.*

Απόδειξη. Η απόδειξη έχει προηγηθεί, με τις λεπτομέρειες να αφήνονται ως άσκηση (Άσκηση 7.3.4$_{22}$). ό.έ.δ.

Όπως γνωρίζουμε (ιδέ Θεώρημα Γ.1.8), ένα στοιχείο $z_r = z_1^r$ της κυκλικής ομάδας C_n είναι γεννήτορας, αν και μόνο αν $μ.κ.δ.(n, r) = 1$.

Ένας τέτοιος γεννήτορας θα ονομάζεται **πρωταρχική** n-οστή ρίζα της μονάδος. Επομένως, υπάρχουν $\varphi(n)$ το πλήθος πρωταρχικές ρίζες της μονάδος, όπου φ είναι η συνάρτηση του Euler (ιδέ Παράγραφο 6.1.2.5).

Ας επανέλθουμε στον υπολογισμό των n-οστών ριζών ενός τυχαίου μιγαδικού αριθμού.

Έστω $z = r(\cos(\theta) + i\sin(\theta))$, είχαμε δει ότι οι n-οστές ρίζες του z είναι οι

$$w_k = \sqrt[n]{r}\left(\cos\frac{\theta + 2k\pi}{n} + i\sin\frac{\theta + 2k\pi}{n}\right),$$

για $k = 0, 1, \ldots, n-1$. Για $k = 0$ έχουμε

$$w_0 = \sqrt[n]{r}(\cos\theta + i\sin\theta),$$

οπότε

$$w_k = w_0 \cdot z_1^k,$$

για $k = 0, 1, \ldots, n-1$,όπου

$$z_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

είναι (μια) πρωταρχική n-οστή ρίζα της μονάδας.

Συμπέρασμα: Για τον υπολογισμό όλων των n-οστών ριζών ενός μιγαδικού αριθμού, είναι αρκετό να υπολογίσουμε μόνο μία. Δεδομένου ότι γνωρίζουμε τις n-οστές ρίζες της μονάδος.

7.3.3 Η έκφραση των μιγαδικών αριθμών σε εκθετική μορφή - Η εξίσωση του Euler

Μέχρι τώρα έχουμε δει πώς ένας μιγαδικός αριθμός εκφράζεται σε καρτεσιανές και σε πολικές συντεταγμένες.

Έχει αποδειχθεί ότι κάθε μιγαδικός αριθμός μπορεί να εκφρασθεί ως δύναμη ενός συγκεκριμένου πραγματικού αριθμού.

[16] Για τον μη εξοικειωμένο αναγνώστη με την έννοια της ομάδας και ειδικότερα της κυκλικής ομάδας, παραπέμπουμε στην Παράγραφο Γ.1.1.

Η απόδειξη δεν είναι κατανοητή για έναν, ο οποίος δεν είναι εξοικειωμένος με την έννοια της δυναμοσειράς και την σύγκλιση δυναμοσειρών. Η έκφραση όμως ενός μιγαδικού αριθμού σε εκθετική μορφή διευκολύνει τον "χειρισμό" των μιγαδικών αριθμών και είναι πολύ χρήσιμη στις εφαρμογές.

Για τον λόγο αυτόν, εδώ θα παραθέσουμε ορισμένα αποτελέσματα, επικαλούμενοι (αυθαιρέτως) ότι ισχύουν κάποια άλλα αποτελέσματα και στηριζόμενοι στην διαίσθησή μας για το τι σημαίνουν ορισμένοι όροι[17].

Σκοπός μας είναι να παρουσιάσουμε την περίφημη ταυτότητα του Euler.

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

Τι είναι το e και τι σημαίνει δύναμη με εκθέτη τον φανταστικό αριθμό $i\theta$;

Έστω η ακολουθία

$$\left(\left(1+\frac{1}{n}\right)^n\right)_{n\in\mathbb{N}}.$$

Αποδεικνύεται[18] ότι η ακολουθία συγκλίνει μάλιστα δε ισχύει,

$$\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n = 1+1+\frac{1}{2!}+\frac{1}{3!}+\cdots+\frac{1}{n!}+\cdots = e = 2.718281828\cdots.$$

Ο πραγματικός αριθμός e αναφέρεται ως *αριθμός του Euler* ή ως βάση των *φυσικών* λογαρίθμων.

Για έναν πραγματικό αριθμό θ αποδεικνύεται ότι

$$e^{\theta} = 1+\frac{\theta}{1!}+\frac{\theta^2}{2!}+\frac{\theta^3}{3!}+\cdots+\frac{\theta^n}{n!}+\cdots \qquad (*)$$

Επίσης, αποδεικνύεται ότι η δυναμοσειρά

$$1-\frac{\theta^2}{2!}+\frac{\theta^4}{4!}-\frac{\theta^6}{6!}+\cdots$$

συγκλίνει μάλιστα δε ισχύει ότι

$$\cos\theta = 1-\frac{\theta^2}{2!}+\frac{\theta^4}{4!}-\frac{\theta^6}{6!}+\cdots.$$

Επίσης, αποδεικνύεται ότι

$$\sin\theta = \frac{\theta}{1!}-\frac{\theta^3}{3!}+\frac{\theta^5}{5!}-\frac{\theta^7}{7!}+\cdots.$$

Γνωρίζοντας ότι $i^{2n} = (-1)^n$ και $i^{2n+1} = i(-1)^n$, για $n\in\mathbb{N}$, οι ανωτέρω ισότητες λαμβάνουν την μορφή

$$\cos\theta = 1+\frac{(i\cdot\theta)^2}{2!}+\frac{(i\cdot\theta)^4}{4!}+\frac{(i\cdot\theta)^6}{6!}+\cdots+\frac{(i\cdot\theta)^{2n}}{(2n)!}+\cdots$$

[17] Έχοντας επίγνωση ότι η όλη παρουσίαση, όχι μόνο δεν αποτελεί τεκμηριωμένη απόδειξη, αλλά είναι μια "*υβριστική*" αντιμετώπιση του θέματος.

[18] Όπου εμφανίζεται η λέξη "αποδεικνύεται", εδώ πρόκειται για αυθαιρεσία και ο ενδιαφερόμενος αναγνώστης πρέπει να ανατρέξει σε στοιχειώδη, αλλά αξιοπρεπή, συγγράμματα Απειροστικού Λογισμού.

και

$$i \cdot \sin\theta = \frac{i\cdot\theta}{1!} + \frac{(i\cdot\theta)^3}{3!} + \frac{i\cdot\theta)^5}{5!} + \frac{(i\cdot\theta)^7}{7!} + \cdots + \frac{(i\cdot\theta)^{2n+1}}{(2n+1)!} + \cdots.$$

Προσθέτοντας (ή αφαιρώντας) κατά μέλη τις ανωτέρω ισότητες έχουμε:

$$\cos\theta \pm i\cdot\sin\theta = 1 \pm \frac{i\cdot\theta}{1!} + \frac{(i\cdot\theta)^2}{2!} \pm \frac{(i\cdot\theta)^3}{3!} + \frac{(i\cdot\theta)^4}{4!} \pm \frac{i\cdot\theta)^5}{5!} + \cdots + \frac{(i\cdot\theta)^{2n}}{(2n)!} \pm \frac{(i\cdot\theta)^{2n+1}}{(2n+1)!} + \cdots.$$

Αν "συγκρίνουμε" την τελευταία ισότητα με την ισότητα $(*)$, θα δούμε ότι "αντικαθιστώντας" τον πραγματικό αριθμό θ με τον φανταστικό αριθμό $i\cdot\theta$ δεν έχουμε παρά να παρατηρήσουμε ότι

$$e^{\pm i\theta} = \cos\theta \pm i\sin\theta.$$

Δηλαδή *αποδείξαμε;* την ταυτότητα του Euler.

Σχόλιο 7.3.15. Όπως προείπαμε, όλα τα ανωτέρω δεν αποτελούν (αυστηρή) απόδειξη. Βλέπουμε όμως ότι αποκτά νόημα η δύναμη πραγματικού αριθμού σε φανταστικό εκθέτη, κάτι που αποτελεί παράδοξο, ως προς την διαίσθησή μας[19].

Για παράδειγμα, όταν έχουμε e^5, αυτό σημαίνει ότι πολλαπλασιάζουμε τον πραγματικό αριθμό e με τον εαυτό του πέντε φορές ($e^5 = e\cdot e\cdot e\cdot e\cdot e$), κάτι που δεν μπορούμε να ισχυριστούμε για τον $e^{i\cdot 5}$.

Γνωρίζουμε ότι οι καρτεσιανές συντεταγμένες και οι πολικές συντεταγμένες ενός μιγαδικού αριθμού $z = a + ib$ συνδέονται ως εξής:

$$a = |z|\cdot\cos\theta \text{ και } b = |z|\cdot\sin\theta.$$

Δηλαδή

$$z = a + ib = |z|\cdot\cos\theta + i(|z|\cdot\sin\theta) = |z|\cdot(\cos\theta + i\sin\theta).$$

Τώρα μπορούμε να συνεχίσουμε

$$z = a + ib = |z|\cdot\cos\theta + i(|z|\cdot\sin\theta) = |z|\cdot(\cos\theta + i\sin\theta) = |z|e^{i\theta}.$$

Επομένως, οι n-οστές ρίζες της μονάδας, σε εκθετική μορφή, είναι οι

$$z_k = e^{i\frac{2k\pi}{n}},$$

για $k = 0, 1, 2, \ldots, n-1$.

Για τον πολλαπλασιασμό δύο μιγαδικών αριθμών

$$z = |z|e^{i\theta_1},\ w = |z|e^{i\theta_2},$$

έχουμε

$$\begin{aligned} z\cdot w &= (|z|e^{i\theta_1})\cdot(|w|e^{i\theta_2}) \\ &= |z|\cdot|w|e^{i\theta_1}e^{i\theta_2} \\ &= |z|\cdot|w|e^{i(\theta_1+\theta_2)} \\ &= |z|\cdot|w|(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)). \end{aligned}$$

[19]Πολλοί συγγραφείς, απλά ορίζουν ως $e^{i\theta} = \cos\theta + i\sin\theta$. Αυτό, εκτός του ότι είναι λογικά ακατανόητο, ανάγει ένα από τα μεγαλύτερα επιτεύγματα του Euler σε μια απλή ταυτολογία.

Τι παρατηρούμε; Αποδείξαμε πάλι το Θεώρημα 7.3.11 (**Θεώρημα De Moivre**).

Εδώ πρέπει να κάνουμε μια σημαντική παρατήρηση. Εκεί είχαμε επικαλεσθεί τις τριγωνομετρικές ισότητες

$$\cos(\theta+\phi) \;=\; \cos\theta\cdot\cos\phi - \sin\theta\cdot\sin\phi$$

και

$$\sin(\theta+\phi) \;=\; \cos\theta\cdot\sin\phi + \sin\theta\cdot\cos\phi.$$

Οι ισότητες αυτές αποδεικνύονται εύκολα με στοιχειώδη γεωμετρικά/τριγωνομετρικά επιχειρήματα.

Εδώ θα δούμε μια διαφορετική προσέγγιση.

Πρόταση 7.3.16. *Για κάθε πραγματικό αριθμό θ ισχύει ότι:*

i. $\cos\theta \;=\; \dfrac{e^{i\theta}+e^{-i\theta}}{2}.$

ii. $\sin\theta \;=\; \dfrac{e^{i\theta}-e^{-i\theta}}{2i}.$

Απόδειξη. Η απόδειξη είναι προφανής. Απλώς εφαρμόζουμε την ταυτότητα του Euler $e^{\pm i\theta} \;=\; \cos\theta \pm i\sin\theta$, με τις λεπτομέρειες να αφήνονται ως άσκηση (Άσκηση $7.3.4_{25}$). ό.έ.δ.

Πρόταση 7.3.17. *Για πραγματικούς αριθμούς θ, ϕ ισχύει ότι:*

$$\cos(\theta+\phi) \;=\; \cos\theta\cdot\cos\phi - \sin\theta\cdot\sin\phi$$

και

$$\sin(\theta+\phi) \;=\; \cos\theta\cdot\sin\phi + \sin\theta\cdot\cos\phi.$$

Απόδειξη. Θα αποδείξουμε την πρώτη ισότητα. Παρομοίως αποδεικνύεται και η άλλη ισότητα.

Θα ξεκινήσουμε από το δεύτερο μέλος.

Στην παράσταση $\cos\theta\cdot\cos\phi-\sin\theta\cdot\sin\phi$ αντικαθιστούμε τα $\cos\theta,\ \cos\phi,\ \sin\theta,\ \sin\phi$ με τα αντίστοιχα από την προηγουμένη πρόταση και έχουμε

$$\begin{aligned}\cos\theta\cdot\cos\phi-\sin\theta\cdot\sin\phi \;&=\; \frac{e^{i\theta}+e^{-i\theta}}{2}\cdot\frac{e^{i\phi}+e^{-i\phi}}{2} - \frac{e^{i\theta}-e^{-i\theta}}{2i}\cdot\frac{e^{i\phi}-e^{-i\phi}}{2i} \;=\; \cdots \;=\\ &=\; \frac{\cos(\theta+\phi)+i\sin(\theta+\phi)+\cos(-(\theta+\phi))+i\sin(-(\theta+\phi))}{2}.\end{aligned}$$

Αλλά γνωρίζουμε(;) ότι: "Αντίθετες γωνίες έχουν ίσα συνημίτονα και αντίθετα ημίτονα". Επομένως, συνεχίζοντας στην ανωτέρω ισότητα, έχουμε τελικά

$$\cos\theta\cdot\cos\phi-\sin\theta\cdot\sin\phi \;=\; \cos(\theta+\phi).$$

Να κάνετε τον έλεγχο τον πράξεων, συμπληρώνοντας τα κενά $\cdots$. ό.έ.δ.

Σχόλιο 7.3.18. Όπως βλέπουμε, θεωρώντας όλα τα προηγούμενα, "*ανακαλύψαμε τον τροχό*", δηλαδή την ισότητα

$$\cos(\theta + \phi) = \cos\theta \cdot \cos\phi - \sin\theta \cdot \sin\phi,$$

η οποία, όπως προείπαμε αποδεικνύεται με στοιχειώδη γεωμετρικά/τριγωνομετρικά επιχειρήματα.

Προσπαθήστε να την αποδείξετε στοιχειωδώς!!

Πιστεύοντας ότι όλα τα ανωτέρω ισχύουν[20], μπορούμε να επεκτείνουμε τον ορισμό της δύναμης του e σε φανταστικό εκθέτη σε δυνάμεις του e σε τυχαίο μιγαδικό αριθμό.

Έστω $z = a + ib$ ένας μιγαδικός, αριθμός, τότε, "κατ' αναλογίαν" με τις ιδιότητες που ισχύουν στις δυνάμεις πραγματικών αριθμών με πραγματικό εκθέτη, ορίζουμε

$$e^z = e^{a+ib} = e^a e^{ib} = e^a(\cos b + i \sin b).$$

Θα μπορούσαμε να επεκταθούμε ακόμη περισσότερο και να ορίσουμε δυνάμεις μιγαδικών με μιγαδικό εκθέτη.

Αλλά, φθάσαμε στο κατώφλι μιας ευρείας και πολύ σημαντικής περιοχής των Μαθηματικών, της Μιγαδικής Ανάλυσης, και εδώ δεν είναι ο σκοπός να το *διαβούμε*.

Θα κλείσουμε την αναφορά μας στους μιγαδικούς αριθμούς με μια από τις "*πλέον όμορφες*" ισότητες στα Μαθηματικά.

Στην ταυτότητα του Euler, αν θέσουμε $\theta = \pi$ έχουμε ότι

$$e^{i\pi} + 1 = 0$$

Όπως βλέπουμε, συνδυάζονται κατά "απίστευτο" τρόπο οι πέντε αριθμοί $e, \pi, i, 1, 0$ [21].

Εφαρμογές- Παραδείγματα.

Προς εμπέδωση των ανωτέρω, θα δούμε ορισμένα παραδείγματα και εφαρμογές.

1. Έστω z_1, z_2, z_3, z_4 τέσσερις μιγαδικοί αριθμοί με $|z_3| \neq |z_4|$. Δείξτε ότι

$$\frac{|z_1 + z_2|}{|z_3 + z_4|} \leq \frac{|z_1| + |z_2|}{||z_3| - |z_4||}.$$

   Η "βαρύγδουπη" αυτή ανισότητα είναι άμεση συνέπεια της τριγωνικής ανισότητας. Αρκεί να εφαρμόσουμε την γνωστή ιδιότητα, που ισχύει στους πραγματικούς αριθμούς (είναι η ιδιότητα 15 στο Θεώρημα 7.1.28).

   Για απλότητα θέτουμε

$$a = |z_1 + z_2|, b = |z_1| + |z_2|, \ c = |z_3 + z_4| \text{ και } d = ||z_3| - |z_4||.$$

   Οπότε, η προς απόδειξη ανισότητα γίνεται

$$\frac{a}{c} \leq \frac{b}{d}.$$

[20] Πράγματι ισχύουν, εμείς εδώ, τα περισσότερα, τα αποδεχθήκαμε χωρίς αποδείξεις.

[21] "...that is surely true, it is absolutely paradoxical; we cannot understand it, and we don't know what it means. But we have proved it, and therefore, we know it is the truth." Ο επίλογος από μια παρουσίαση της απόδειξης της ταυτότητας του Euler από τον Benjamin Peirce.

Από την τριγωνική ανισότητα έχουμε $a \leq b$ και $d \leq c$ (γιατί ισχύει η τελευταία ανισότητα;).

Όλα τα a, b, c, d είναι μη αρνητικοί πραγματικοί αριθμοί. Μάλιστα δε, από την υπόθεσή μας οι c και d είναι διάφοροι του μηδενός. Επομένως, από την $a \leq b$ έπεται ότι

$$\frac{a}{c} \leq \frac{b}{c}.$$

Από την σχέση $d \leq c$, έπεται ότι

$$\frac{b}{c} \leq \frac{b}{d}.$$

Οπότε, λόγω μεταβατικότητας, έχουμε την ζητουμένη ανισότητα.

2. Να υπολογίσετε την τετραγωνική ρίζα του $2i$.

Ας εκφράσουμε τον $2i$ σε πολικές συντεταγμένες. Έχουμε

$$2i = 2(0+i) = 2\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right).$$

Υποθέτουμε ότι η τετραγωνική ρίζα του $2i$ είναι ο

$$z = r(\cos\theta + i\sin\theta).$$

Τότε θα έχουμε $z^2 = 2i$. Δηλαδή

$$r^2(\cos\theta + i\sin\theta)^2 = 2\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right).$$

Από την τελευταία σχέση έπεται ότι $r = \pm\sqrt{2}$ και $2\theta = \frac{\pi}{2}$. Συνεπώς, οι δύο (διακεκριμένες) τετραγωνικές ρίζες του $2i$ ισούνται με

$$z = \pm\sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) = \pm(1+i)$$

(Συγκρίνατε με το Παράδειγμα 7.3.2.2$_3$).

3. Να υπολογίσετε τον $(-1+i)^7$. Εκφράζουμε τον $-1+i$ σε πολικές συντεταγμένες. Έχουμε

$$\sqrt{2}\cos\theta = 1 \text{ και } \sqrt{2}\sin\theta = 1$$

(γιατί; δεν ξεχνάμε πώς συνδέονται οι καρτεσιανές και πολικές συντεταγμένες).

Επομένως, $\cos\theta = -\frac{\sqrt{2}}{2}$, $\sin\theta = \frac{\sqrt{2}}{2}$, δηλαδή $\theta = \frac{3\pi}{4}$. Συνεπώς

$$-1+i = \sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right).$$

Στην συνέχεια έχουμε

$$(-1+i)^7 = \sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right)^7 = \cdots = -8(1+i)$$

(να κάνετε την επαλήθευση των πράξεων!).

4. Να υπολογίσετε όλα τα $w \in \mathbb{C}$ με $z^3 = -2$.

   Εφαρμόζοντας την ταυτότητα του Euler έχουμε ότι: $e^{i\pi} = -1$. Αυτό μας οδηγεί στο συμπέρασμα ότι ένας από τους ζητουμένους μιγαδικούς αριθμούς είναι ο

   $$w_1 = \sqrt[3]{2}e^{i\frac{\pi}{3}} \text{ (γιατί;)}.$$

   Επομένως, οι άλλοι δύο είναι οι

   $$w_2 = w_1 \cdot z_1,\ w_3 = w_1 \cdot z_1^2.$$

   Όπου $z_1 = e^{i\frac{2\pi}{3}}$ είναι η πρωταρχική τρίτη ρίζα της μονάδας (γιατί; Μα ισχύει το συμπέρασμα στην σελίδα 304).

7.3.4 Ασκήσεις

1. Δείξτε ότι οι πράξεις της πρόσθεσης και πολλαπλασιασμού, που ορίστηκαν στο σύνολο $\mathbb{R} \times \mathbb{R}$ στην σελίδα 287, είναι καλά ορισμένες.

2. Να συμπληρώσετε, με κάθε λεπτομέρεια, την απόδειξη της Πρότασης 7.3.1.

3. Να αποδείξετε, με κάθε λεπτομέρεια, την Πρόταση 7.3.2.

4. Να αποδείξετε, με κάθε λεπτομέρεια, την Πρόταση 7.3.4.

5. Να συμπληρώσετε, με κάθε λεπτομέρεια, την απόδειξη της Πρότασης 7.3.7.

6. Να συμπληρώσετε, με κάθε λεπτομέρεια, την απόδειξη της Πρότασης 7.3.9.

7. Έστω a, b, c τρεις θετικοί ακέραιοι αριθμοί, οι οποίοι αποτελούν *Πυθαγόρεια τριάδα*, δηλαδή αποτελούν τα μήκη των πλευρών ορθογωνίου τριγώνου. Αν c είναι το μήκος της υποτείνουσας, δείξτε ότι οι μιγαδικοί αριθμοί

   $$\pm\left(\frac{a}{c}\right) \pm i\left(\frac{b}{c}\right)$$

   βρίσκονται επί του μοναδιαίου κύκλου.

8. Να γράψετε υπό την μορφή $a + ib$ τους μιγαδικούς αριθμούς

   $$\frac{2+i3}{i(1+i)},\ \frac{(1+i)^2}{2-i\sqrt{3}},\ \frac{1}{1+\frac{i}{1+i}}.$$

9. Να υπολογίσετε το $|\,(2\bar{z}+5)(\sqrt{2}-i)\,|$ με δύο τρόπους. Πρώτον, εκτελώντας τις πράξεις και μετά υπολογίζοντας το μέτρο μιγαδικού αριθμού.

   Δεύτερον, εφαρμόζοντας πρώτα την ιδιότητα του μέτρου γινομένου μιγαδικών αριθμών και μετά κάνοντας επιμέρους πράξεις.

10. Να δώσετε ικανή και αναγκαία συνθήκη, ώστε στην τριγωνική ανισότητα να ισχύει ισότητα. Δηλαδή να ισχύει

    $$|\,z+w\,| = |\,z\,| + |\,w\,|\,.$$

11. Να δώσετε μια άλλη απόδειξη της τριγωνικής ανισότητας γνωρίζοντας ότι για κάθε μιγαδικό αριθμό z ισχύει $z\,\bar{z} = |\,z\,|^2$.

    Επομένως, $|\,z+w\,|^2 = \cdots$.

12. Να παραστήσετε στο επίπεδο όλους τους μιγαδικούς αριθμούς z με την ιδιότητα:

    i. $|\,z-(1+i)\,| = 2$,

    ii. $|\,z-1\,| = |\,z-i\,|$,

    iii. $|\,z+2+i\,| \geq 1$.

13. Δείξτε ότι, για όλα τα σημεία z του μοναδιαίου κύκλου, ο αριθμός

$$\frac{z-1}{z+1}$$

    είναι γνήσιος φανταστικός ή μηδέν.

14. Έστω $z \in \mathbb{C}$, αλλά όχι πραγματικός αριθμός. Υποθέτουμε ότι ο

$$z + \frac{1}{z}$$

    είναι πραγματικός αριθμός. Δείξτε ότι $|\,z\,| = 1$.

15. Να δείξετε την επιμεριστική ιδιότητα του πολλαπλασιασμού, ως προς την πρόσθεση, στους μιγαδικούς αριθμούς, χρησιμοποιώντας τις πολικές συντεταγμένες.

16. Να αποδείξετε, με κάθε λεπτομέρεια, τις Προτάσεις 7.3.4 και 7.3.7, χρησιμοποιώντας τις πολικές συντεταγμένες.

17. Να δείξετε ότι, για κάθε μιγαδικό αριθμό z, ο

$$\frac{1}{2}\left(\frac{z}{\bar{z}} + \frac{\bar{z}}{z}\right)$$

    είναι πραγματικός αριθμός. Να τον υπολογίσετε, αν $z = 1+i$.

18. Δείξτε ότι ο μιγαδικός αριθμός z ικανοποιεί την σχέση

$$\frac{|\,z-3\,|}{|\,z+3\,|} = 2$$

    αν και μόνο αν $|\,z+5\,| = 4$.

19. Να υπολογίσετε όλα τα $z \in \mathbb{C}$, ώστε $z^3 = -2+2i$.

20. Να συμπληρώσετε, με κάθε λεπτομέρεια, την απόδειξη της Πρότασης 7.3.14.

21. Να δείξετε ότι το άθροισμα όλων των n-οστών ριζών της μονάδος ισούται με μηδέν.

22. Να δώσετε ικανή και αναγκαία συνθήκη για έναν μιγαδικό αριθμό z, ώστε να υπάρχει ακέραιος αριθμός n με $z^n = 1$.

23. Να υπολογίσετε όλους τους μιγαδικούς αριθμούς z, για τους οποίους ισχύει

$$e^z = |\, 1 + i\sqrt{3}\,| \,.$$

24. Να γράψετε τον μιγαδικό αριθμό

$$\left(\frac{\sqrt{3}}{2} - i\frac{1}{2}\right)^{24}$$

στην μορφή $a + ib$.

25. Να αποδείξετε, με κάθε λεπτομέρεια, την Πρόταση 7.3.16.

26. Δίνονται οι μιγαδικοί αριθμοί z, w με

$$|\, z\,| = 0.9 \text{ και } arg(z) = \frac{\pi}{6}, \; |\, w\,| = 1.1 \text{ και } arg(w) = \frac{\pi}{6}.$$

Να παραστήσετε στο (ίδιο) μιγαδικό επίπεδο τις δυνάμεις

$$z^k,\, w^k \text{ για } k = 1, 2, \ldots, 6.$$

Ενώστε με μια τεθλασμένη γραμμή (κατά σειρά) όλα τα z^k. Όμοια ενώστε με μια τεθλασμένη γραμμή (κατά σειρά) όλα τα w^k. Τι παρατηρείτε;

Βιβλιογραφία

[1] E.D. Bloch. *The Real Numbers and Real Analysis*. Springer, 2011. ISBN: 978-03-8772-176-7.

[2] Herbert B. Enderton. *Elements of Set Theory*. Academic Press, 1977. ISBN: 978-01-2238-440-0.

[3] Steven G. Krantz. *The Elements of Advanced Mathematics*. Fourth Edition. Textbooks in mathematics. CRC Press Taylor and Francis Group, 2018. ISBN: 978-11-3850-631-2.

[4] M. Liebeck. *A Concise Introduction to Pure Mathematics*. Third Edition. Chapman Hall CRC Press, 2011. ISBN: 978-14-3983-598-2.

[5] I. Stewart & D. Tall. *The Foundations of Mathematics*. Second Edition. Oxford University Press, 2015.

ΠΑΡΑΡΤΗΜΑΤΑ

ΠΑΡΑΡΤΗΜΑ Α

ΟΙ ΦΥΣΙΚΟΙ ΑΡΙΘΜΟΙ

Οι φυσικοί αριθμοί είναι το πλέον (φαινομενικά) απλό και ταυτόχρονα το πλέον θεμελιώδες σύνολο αριθμών.

Όλοι έχουμε έρθει σε επαφή με τους φυσικούς αριθμούς από τα πρώτα βήματα της ανάπτυξης της σκέψης μας και τους θεωρούμε τόσο οικείους, ώστε να μην νιώθουμε την ανάγκη για περαιτέρω μελέτη τους.

Ήδη στο παρόν σύγγραμμα έχουμε δεχθεί την ύπαρξη και τις ιδιότητες των φυσικών αριθμών και τους έχουμε χρησιμοποιήσει κατά κόρον, τόσο σε παραδείγματα, όσο και στην αποδεικτική επιχειρηματολογία.

Αλλά, όταν παρουσιάσαμε την "Αρχή της Μαθηματικής επαγωγής", είχαμε επικαλεσθεί δύο "Θεωρήματα", το Θεώρημα 3.2.20 και το Θεώρημα 3.2.27 και είχαμε σχολιάσει ότι αυτά αποτελούν μέρος της αυστηρής θεμελίωσης των φυσικών αριθμών και είχαμε αναβάλει την λεπτομερή μελέτη τους.

Στο παρόν Παράρτημα θα επιχειρήσουμε μια αξιωματική παρουσίαση των φυσικών αριθμών και θα δούμε πώς αυτά τα θεωρήματα εντάσσονται στην όλη θεώρηση.

Α.1 Η Θεμελίωση των Φυσικών αριθμών κατά Peano.

Ένα "καλό" αξιωματικό σύστημα αποδέχεται (αυθαιρέτως) όσον το δυνατόν *λιγότερα*, από τα οποία μπορούν να αποδειχθούν όσον το δυνατόν *περισσότερα*.

Όσον αφορά τους φυσικούς αριθμούς, διαισθητικά γνωρίζουμε την ύπαρξη του στοιχείου 1, την πράξη της πρόσθεσης και του πολλαπλασιασμού, την έννοια του "επομένου" αριθμού, ο οποίος προκύπτει από την πρόσθεση στον αριθμό αυτόν του 1, την έννοια της "σύγκρισης" δύο φυσικών αριθμών (πότε ένας αριθμός είναι μικρότερος ενός άλλου). Θα δούμε ότι από αυτές τις έννοιες μόνο λίγες είναι απαραίτητο να θεωρηθούν ως αξιώματα και όλες οι άλλες απορρέουν από αυτές.

Τα αξιώματα του Peano.
Υπάρχει ένα σύνολο $\mathbb{N}$, ένα στοιχείο $1 \in \mathbb{N}$ και μια απεικόνιση $\sigma : \mathbb{N} \longrightarrow \mathbb{N}$, η οποία ικανοποιεί τις ακόλουθες ιδιότητες:

i. Δεν υπάρχει $n \in \mathbb{N}$, ώστε $\sigma(n) = 1$.

ii. Η απεικόνιση σ είναι 1-1.

iii. Έστω $S \subseteq \mathbb{N}$. Υποθέτουμε ότι $1 \in S$, και ότι, αν $s \in S$, τότε $\sigma(s) \in S$. Τότε $S = \mathbb{N}$.

Ένα σύνολο, το οποίο ικανοποιεί τα ανωτέρω αξιώματα, θα ονομάζεται **σύνολο των φυσικών αριθμών**.

Σχόλια Α.1.1.

1. Δεν είναι προφανές ότι υπάρχει μόνο ένα σύνολο, το οποίο να ικανοποιεί τα ανωτέρω αξιώματα. Στην συνέχεια (ιδέ Πρόταση Α.1.22) θα δούμε ότι υπάρχει μόνο ένα σύνολο φυσικών αριθμών.

2. Τα τρία αξιώματα είναι αναγκαία για τον ορισμό του συνόλου των φυσικών αριθμών.

   Πράγματι, έστω το σύνολο $M = \{1, a\}$ και $s : M \longrightarrow M$ με

   $$s(1) = a \text{ και } s(a) = a.$$

   Είναι προφανές ότι η τριάδα (M, s, 1) πληροί τα αξιώματα i. και iii., αλλά δεν πληροί το αξίωμα ii..

   Επίσης, για το ίδιο σύνολο $M = \{1, a\}$ και την απεικόνιση $\vartheta : M \longrightarrow M$ με

   $$\vartheta(1) = a \text{ και } \vartheta(a) = 1,$$

   είναι προφανές ότι η τριάδα (M, ϑ, 1) ικανοποιεί τα αξιώματα ii. και iii., αλλά όχι το i..

3. Το αξίωμα iii. είναι αναγκαίο, διότι αποτελεί το κύριο "συστατικό" στις αποδείξεις με την χρήση της "Αρχής της Επαγωγής".

   Για παράδειγμα, αν πάρουμε το σύνολο $\mathbb{N}$, αλλά αντί για την απεικόνιση σ, την απεικόνιση σ^2 (εδώ ως συνήθως $\sigma^2 = \sigma \circ \sigma$), τότε η τριάδα ($\mathbb{N}$, σ^2, 1) πληροί τα αξιώματα i. και ii., αλλά όχι το iii., διότι για το υποσύνολο

   $$S = \{1\} \cup \sigma^2(\mathbb{N})$$

   έχουμε ότι $1 \in S$ και για κάθε $s \in S$ ισχύει $\sigma^2(s) \in S$, αλλά $S \neq \mathbb{N}$.

   Επομένως, όταν μιλάμε για το σύνολο των φυσικών αριθμών $\mathbb{N}$, απαραίτητα (έστω και αν δεν το ομολογούμε) αναφερόμαστε, τόσο στην απεικόνιση σ, όσον και στην ύπαρξη του στοιχείου $1 \in \mathbb{N}$.

4. Συνήθως η εικόνα $\sigma(a)$ ενός $a \in \mathbb{N}$ ονομάζεται ο επόμενος του a και από το αξίωμα i. έπεται, διαισθητικά, ότι το $1 \in \mathbb{N}$, δεν έχει "προηγούμενο". Στην επομένη πρόταση θα δούμε ότι το 1 είναι ο μοναδικός φυσικός αριθμός, ο οποίος δεν έχει προηγούμενο.

Πρόταση Α.1.2. *Έστω $a \in \mathbb{N}$, υποθέτουμε ότι $1 \neq a$. Υπάρχει μοναδικός $b \in \mathbb{N}$, ώστε $a = \sigma(b)$.*

Απόδειξη. Ορίζουμε το εξής σύνολο

$$S = \{1\} \cup \{r \in \mathbb{N} \mid \text{υπάρχει } t \in \mathbb{N}, \text{ έτσι ώστε } \sigma(t) = r\}.$$

Προφανώς $1 \in S$. Έστω $a \in S$, τότε για το $r = \sigma(a)$ υπάρχει το $a \in \mathbb{N}$, έτσι ώστε $\sigma(a) = r$. Συνεπώς, από τον ορισμό του συνόλου S, έπεται ότι $r = \sigma(a) \in S$. Άρα, από το αξίωμα iii. έπεται ότι $S = \mathbb{N}$. Δηλαδή αποδείξαμε ότι κάθε φυσικός αριθμός είτε είναι το 1 είτε είναι ο επόμενος κάποιου φυσικού αριθμού.

Προφανώς, από το αξίωμα ii., έπεται ότι, αν υπάρχει $b \in \mathbb{N}$, ώστε $a = \sigma(b)$, τότε ο b είναι μοναδικός με αυτήν την ιδιότητα. ό.έ.δ.

Όπως προείπαμε, τα τρία αξιώματα του Peano είναι ικανά για να ορίσουμε και να αποδείξουμε τις ιδιότητες της πρόσθεσης και του πολλαπλασιασμού των φυσικών αριθμών.

Ορισμός Α.1.3. Στο σύνολο των φυσικών αριθμών ορίζουμε μια πρόσθεση

$$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

ως εξής:

1. $n + 1 = \sigma(n)$, για όλα τα $n \in \mathbb{N}$.

2. $n + \sigma(m) = \sigma(n + m)$, για όλα τα $n, m \in \mathbb{N}$.

Πρέπει να αποδείξουμε ότι η πράξη αυτή είναι καλά ορισμένη, δηλαδή είναι απεικόνιση. Επιλέγουμε και σταθεροποιούμε ένα $n \in \mathbb{N}$. Έστω

$$S_n = \{m \in \mathbb{N} \mid \text{όπου το άθροισμα } n + m \in \mathbb{N} \text{ είναι μοναδικό}\}.$$

Παρατηρούμε ότι το $1 \in S_n$, διότι $n + 1 = \sigma(n)$.

Έστω $m \in S_n$, τότε το άθροισμα $n + m$ είναι μοναδικό και από το 2. του ορισμού έπεται ότι το άθροισμα $n + \sigma(m) = \sigma(n + m)$ είναι μοναδικό (δεν ξεχνάμε ότι η σ είναι απεικόνιση), άρα $\sigma(m) \in S_n$. Συνεπώς, από το αξίωμα iii. έπεται ότι $S_n = \mathbb{N}$.

Το στοιχείο $n \in \mathbb{N}$ έχει επιλεγεί τυχαία. Συνεπώς, για κάθε $n \in \mathbb{N}$ το αντίστοιχο $S_n = \mathbb{N}$. Άρα πράγματι η πράξη της πρόσθεσης είναι απεικόνιση.

Ορισμός Α.1.4. Στο σύνολο των φυσικών αριθμών ορίζουμε (με την βοήθεια της πρόσθεσης) έναν πολλαπλασιασμό

$$\cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$ [1]

ως εξής:

α. $n \cdot 1 = n$, για όλα τα $n \in \mathbb{N}$.

β. $n \cdot \sigma(m) = n \cdot m + n$, για όλα τα $n, m \in \mathbb{N}$.

[1] Ως συνήθως, όταν δεν υπάρχει κίνδυνος σύγχυσης το σύμβολο του πολλαπλασιασμού παραλείπεται και αντί του $n \cdot m$ γράφουμε nm, δεν γράφουμε όμως 11 στην θέση του $1 \cdot 1$.

Όπως και για την πρόσθεση, πρέπει να αποδείξουμε ότι η πράξη αυτή είναι καλά ορισμένη.

Επιλέγουμε και σταθεροποιούμε ένα $n \in \mathbb{N}$. Έστω

$$S_n = \{ m \in \mathbb{N} \mid \text{όπου το γινόμενο } n \cdot m \in \mathbb{N} \text{ είναι μοναδικό} \}.$$

Παρατηρούμε ότι το $1 \in S_n$, διότι $n \cdot 1 = n$.

Έστω $m \in S_n$, τότε το γινόμενο $n \cdot m$ είναι μοναδικό και από το β) του ορισμού έπεται ότι το γινόμενο

$$n \cdot \sigma(m) = n \cdot m + n$$

είναι μοναδικό (δεν ξεχνάμε ότι η πρόσθεση είναι καλά ορισμένη), άρα $\sigma(m) \in S_n$. Συνεπώς, από το αξίωμα iii. έπεται ότι $S_n = \mathbb{N}$.

Το στοιχείο $n \in \mathbb{N}$ έχει επιλεγεί τυχαία. Συνεπώς, για κάθε $n \in \mathbb{N}$ το αντίστοιχο $S_n = \mathbb{N}$. Άρα πράγματι η πράξη του πολλαπλασιασμού είναι απεικόνιση.

Παρατηρήσεις Α.1.5.

1. Οι πράξεις της πρόσθεσης και του πολλαπλασιασμού φυσικών αριθμών είναι μοναδικές. Δηλαδή δεν μπορούμε να ορίσουμε μια "άλλη" πρόσθεση και έναν "άλλο" πολλαπλασιασμό, οι οποίες να πληρούν τις ανωτέρω ιδιότητες.

   Πράγματι, έστω μια άλλη πρόσθεση $\oplus : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, η οποία να πληροί τα (1) και (2) του ορισμού της πρόσθεσης.

   Έστω
   $$S = \{ x \in \mathbb{N} \mid n + x = n \oplus x, \text{ για όλα τα } n \in \mathbb{N} \}.$$
   Προφανώς το $1 \in S$ (γιατί;). Έστω $m \in S$, τότε
   $$n + m = n \oplus m,$$
   για όλα τα $n \in \mathbb{N}$. Από το (2) του ορισμού της πρόσθεσης έχουμε ότι
   $$n + \sigma(m) = \sigma(n + m) = \sigma(n \oplus m) = n \oplus \sigma(m),$$
   δηλαδή $\sigma(m) \in S$ και από το αξίωμα iii. έπεται ότι
   $$S = \mathbb{N}.$$
   Άρα πράγματι η πράξη της πρόσθεσης είναι μοναδική.

   Παρομοίως (αφήνοντάς το ως άσκηση) αποδεικνύεται ότι η πράξη του πολλαπλασιασμού είναι μοναδική.

2. Όπως βλέπουμε, τόσον η πράξη της πρόσθεσης, όσον και η πράξη του πολλαπλασιασμού, ορίζονται "αναδρομικά". Για παράδειγμα, πρώτα ορίζεται το άθροισμα $n + 1 = \sigma(n)$, μετά το άθροισμα $n + \sigma(1)$, και εφόσον έχει ορισθεί το $n + m$, ορίζεται το $n + \sigma(m) = \sigma(n + m)$. Παρομοίως για τον πολλαπλασιασμό.

Στην επομένη πρόταση είναι συγκεντρωμένες οι πλέον "οικείες" ιδιότητες της πρόσθεσης και του πολλαπλασιασμού φυσικών αριθμών, τις οποίες όλοι μας, "εκ γενετής", θεωρούσαμε ότι ισχύουν αυταπόδεικτα. Όλες μπορούν να αποδειχθούν με την χρήση (κυρίως) του αξιώματος iii.. Η σειρά με την οποία παρουσιάζονται είναι ενδεικτική και παραπέμπει στην τακτική: Άπαξ και μια ιδιότητα έχει αποδειχθεί, μπορεί να χρησιμοποιηθεί για την απόδειξη μιας άλλης (προσέχοντας πάντα να μην έχουμε αυτοεπικλήσεις).

Πρόταση Α.1.6. *Έστω $a, b, c \in \mathbb{N}$. Τότε ισχύουν οι εξής ιδιότητες:*

1. *Αν $a + c = b + c$, τότε $a = b$ (ο νόμος της διαγραφής στην πρόσθεση).*
2. *$(a + b) + c = a + (b + c)$ (η προσεταιριστική ιδιότητα της πρόσθεσης).*
3. *$1 + a = \sigma(a) = a + 1$.*
4. *$a + b = b + a$ (η πρόσθεση είναι μεταθετική).*
5. *$a + b \neq 1$.*
6. *$a + b \neq a$.*
7. *$a \cdot 1 = a = 1 \cdot a$ (ο πολλαπλασιασμός έχει ουδέτερο).*
8. *$(a + b)c = ac + bc$ (ο επιμερισμός του πολλαπλασιασμού ως προς την πρόσθεση).*
9. *$ab = ba$ (ο πολλαπλασιασμός είναι μεταθετικός).*
10. *$(ab)c = a(bc)$ (η προσεταιριστική ιδιότητα του πολλαπλασιασμού).*
11. *Αν $ac = bc$, τότε $a = b$ (ο νόμος της διαγραφής στον πολλαπλασιασμό).*
12. *$ab = 1$, αν και μόνο αν $a = b = 1$.*

Απόδειξη. Δεν θα αποδείξουμε όλες αυτές τις ιδιότητες. Θα αποδείξουμε τις (1), (2), (4), (6) και (12) αφήνοντας τις υπόλοιπες ως άσκηση.

(1). Έστω

$$S = \{ r \in \mathbb{N} \mid \text{ αν } x, y \in \mathbb{N} \text{ με } x + r = y + r \text{ τότε } x = y \}.$$

Θα δείξουμε ότι $S = \mathbb{N}$, δηλαδή την ιδιότητα που θέλουμε να αποδείξουμε.

Προφανώς το $1 \in S$. Πράγματι, έστω $x, y \in \mathbb{N}$ με $x + 1 = y + 1$, αυτό σημαίνει ότι

$$\sigma(x) = \sigma(y),$$

αλλά η απεικόνιση σ είναι 1-1 (από το αξίωμα ii.), συνεπώς $x = y$, το οποίο αποδεικνύει ότι το $1 \in S$.

Έστω $r \in S$, θα αποδείξουμε ότι $\sigma(r) \in S$. Υποθέτουμε ότι, για $x, y \in \mathbb{N}$, ισχύει

$$x + \sigma(r) = y + \sigma(y).$$

Η τελευταία ισότητα, από τον ορισμό της πρόσθεσης, γίνεται

$$\sigma(x + r) = \sigma(y + r),$$

αλλά, όπως προείπαμε, η σ είναι 1-1, συνεπώς $x + r = y + r$. Από την ισότητα αυτή, επειδή το $r \in S$, έχουμε ότι $x = y$. Άρα αποδείξαμε ότι $\sigma(r) \in S$, οπότε από το αξίωμα iii. έχουμε ότι $S = \mathbb{N}$.

(2). Έστω

$$T = \{ r \in \mathbb{N} \mid \text{αν } x, y \in \mathbb{N} \text{ τότε}, (x + y) + r = x + (y + r) \}.$$

Θα δείξουμε ότι $T = \mathbb{N}$, δηλαδή την ιδιότητα που θέλουμε να αποδείξουμε.

Προφανώς το $1 \in T$. Πράγματι, έστω $x, y \in \mathbb{N}$, από τον ορισμό της πρόσθεσης έχουμε,

$$(x + y) + 1 = \sigma(x + y) = x + \sigma(y) = x + (y + 1).$$

Έστω $r \in T$, θα αποδείξουμε ότι $\sigma(r) \in T$. Από τον ορισμό του T έχουμε

$$(x + y) + r = x + (y + r),$$

για όλα τα $x, y \in \mathbb{N}$. Τότε, πάλι από τον ορισμό της πρόσθεσης, έχουμε,

$$\begin{aligned} (x + y) + \sigma(r) &= \sigma((x + y) + r) = \\ &\sigma(x + (y + r)) \\ &= x + \sigma(y + r) \\ &= x + (y + \sigma(r)). \end{aligned}$$

Δηλαδή $\sigma(r) \in T$, οπότε από το αξίωμα iii. έχουμε ότι $T = \mathbb{N}$.

(4). Έστω

$$U = \{ r \in \mathbb{N} \mid \text{αν } x \in \mathbb{N} \text{ τότε } x + r = r + x \}.$$

Θα δείξουμε ότι $U = \mathbb{N}$, δηλαδή την ιδιότητα που θέλουμε να αποδείξουμε.

Επειδή ισχύει η ιδιότητα (3) (την οποία μπορούμε, και πρέπει να αποδείξουμε χωρίς την βοήθεια της προς απόδειξη ιδιότητας) έχουμε ότι $1 \in U$.

Έστω $r \in U$, θα αποδείξουμε ότι $\sigma(r) \in U$. Από τον ορισμό του U έχουμε

$$x + r = r + x,$$

για όλα τα $x \in \mathbb{N}$. Τότε, πάλι από τον ορισμό της πρόσθεσης, έχουμε,

$$\begin{aligned} x + \sigma(r) &= \sigma(x + r) \\ &= \sigma(r + x) \\ &= r + \sigma(x) \\ &= r + (x + 1) \\ &= r + (1 + x), \end{aligned}$$

βάσει της ιδιότητας (2) η τελευταία ισότητα συνεχίζεται

$$\begin{aligned} &= (r + 1) + x \\ &= \sigma(r) + x. \end{aligned}$$

Δηλαδή $\sigma(r) \in U$, οπότε από το αξίωμα iii. έχουμε ότι $U = \mathbb{N}$.

(6). Έστω

$$R = \{ r \in \mathbb{N} \mid \text{αν } x \in \mathbb{N} \text{ τότε } x + r \neq r \}.$$

Θα δείξουμε ότι $R = \mathbb{N}$, δηλαδή την ιδιότητα που θέλουμε να αποδείξουμε.

Επειδή ισχύει η ιδιότητα (5), έχουμε ότι $1 \in R$.

Έστω $r \in R$, θα αποδείξουμε ότι $\sigma(r) \in R$. Από τον ορισμό του R έχουμε $x+r \neq r$, για όλα τα $x \in \mathbb{N}$. Τότε, πάλι από τον ορισμό της πρόσθεσης, έχουμε,

$$x + \sigma(r) = \sigma(x+r) \neq \sigma(r)$$

(γιατί; μα αφού έχουμε ότι $x+r \neq r$ και η απεικόνιση σ είναι 1-1). Δηλαδή $\sigma(r) \in R$, οπότε από το αξίωμα iii. έχουμε ότι $R = \mathbb{N}$.

(12). Προφανώς, αν $a = b = 1$, τότε $ab = 1$.

Αντίστροφα, υποθέτουμε ότι $ab = 1$. Θα δείξουμε ότι $a = b = 1$. Υποθέτουμε ότι $b \neq 1$, τότε και το $a \neq 1$. Πράγματι, αν $a = 1$ και $b \neq 1$, τότε θα έχουμε

$$1 \cdot b = b = 1,$$

άτοπο. Άρα έχουμε ότι

$$ab = 1 \text{ με } a \neq 1 \text{ και } b \neq 1.$$

Από την Πρόταση A.1.2 έχουμε ότι υπάρχουν (μοναδικά) $c, d \in \mathbb{N}$, ώστε

$$a = \sigma(c) = c+1 \text{ και } b = \sigma(d) = d+1.$$

Τότε όμως από την ισότητα $ab = 1$ έχουμε ότι

$$(c+1) \cdot (d+1) = 1.$$

Λόγω της ιδιότητας (8), η τελευταία ισότητα γίνεται

$$cd + c + d + 1 = 1,$$

δηλαδή

$$\sigma(cd + c + d) = 1,$$

άτοπο. Άρα, από την ισότητα $ab = 1$, έπεται ότι $a = b = 1$. ό.έ.δ.

Στο Σχόλιο A.1.1$_4$, καθώς και στην Πρόταση A.1.2 είχαμε μιλήσει, διαισθητικά, για την έννοια του προηγουμένου ενός φυσικού αριθμού. Θα δούμε ότι μπορούμε να ορίσουμε μια μερική διάταξη στους φυσικούς αριθμούς, όπου οι έννοιες του προηγουμένου/επομένου στοιχείου αποκτούν Μαθηματική υπόσταση.

Ορισμός A.1.7. Στο σύνολο $\mathbb{N}$ των φυσικών αριθμών ορίζουμε μια σχέση $<$ ως εξής: Έστω $a, b \in \mathbb{N}$, τότε $a < b$, αν υπάρχει $k \in \mathbb{N}$, ώστε $b = a + k$. Επίσης, ορίζουμε μια σχέση $\leq$ ως εξής: Έστω $a, b \in \mathbb{N}$, τότε

$$a \leq b, \text{ αν } a < b, \text{ ή } a = b.$$

Ως συνήθως, για δύο φυσικούς αριθμούς a, b με $a < b$, μπορούμε ισοδυνάμως να γράφουμε $b > a$. Επίσης, αντί της έκφρασης "ο a προηγείται του b" χρησιμοποιούμε την έκφραση "ο a είναι μικρότερος του b".

Είναι εύκολο να δούμε (ιδέ Άσκηση A.1.1$_2$) ότι ο φυσικός αριθμός k στον προηγούμενο ορισμό είναι μοναδικός, συνήθως συμβολίζεται με $a - b$ και ονομάζεται η **διαφορά** του a από τον b.

Οι κυριότερες ιδιότητες των σχέσεων $<$ και $\leq$ περιλαμβάνονται στην επομένη πρόταση.

Πρόταση Α.1.8. *Έστω $a, b, c, d \in \mathbb{N}$. Τότε ισχύουν οι εξής ιδιότητες:*

1. $a \leq a$, $a \not< a$ *και* $a < \sigma(a) = a + 1$.
2. $1 \leq a$.
3. *Αν* $a < b$, $b < c$, *τότε* $a < c$.

   Αν $a \leq b$, $b < c$, *τότε* $a < c$.

   Αν $a < b$, $b \leq c$, *τότε* $a < c$.

   Αν $a \leq b$, $b \leq c$, *τότε* $a \leq c$.
4. $a < b$, *αν και μόνο αν* $a + c < b + c$.
5. $a < b$, *αν και μόνο αν* $ac < bc$.
6. *Ισχύει ακριβώς μια από τις σχέσεις* $a < b$, $a = b$, $b < a$ *(ο νόμος της τριχοτομίας).*
7. $a \leq b$ *ή* $b \leq a$.
8. *Αν* $a \leq b$ *και* $b \leq a$, *τότε* $a = b$.
9. *Δεν είναι δυνατόν να ισχύει* $a < b < a + 1$.
10. $a \leq b$, *αν και μόνο αν* $a < b + 1$.
11. $a < b$, *αν και μόνο αν* $a + 1 \leq b$.

Απόδειξη. Θα αποδείξουμε μόνο τις (2), (4), (6) και (9) αφήνοντας τις υπόλοιπες ως άσκηση.

(2). Αν $a = 1$, τότε προφανώς $1 \leq a$. Υποθέτουμε ότι $a \neq 1$, από την Πρόταση Α.1.2 έχουμε ότι υπάρχει $b \in \mathbb{N}$ με $a = b + 1$, δηλαδή $1 < a$ (από τον ορισμό της σχέσης $<$). Άρα τελικά $1 \leq a$.

(4). Υποθέτουμε ότι $a < b$, τότε υπάρχει $k \in \mathbb{N}$, ώστε $b = a + k$, τότε

$$b + c = (a + k) + c$$

(γιατί;). Επομένως

$$b + c = (a + c) + k$$

(δεν ξεχνάμε ότι ισχύει η προσεταιριστικότητα και η μεταθετικότητα στην πρόσθεση), συνεπώς $a + c < b + c$.

Αντίστροφα, υποθέτουμε ότι $a + c < b + c$, τότε υπάρχει $k \in \mathbb{N}$ με

$$(a + c) + k = b + c.$$

Από την ιδιότητα της διαγραφής στην πρόσθεση, έχουμε ότι $a + k = b$, δηλαδή $a < b$.

(6). Θα δείξουμε ότι δεν μπορούν δύο από τις σχέσεις $a < b$, $a = b$, $b < a$ να ισχύουν ταυτόχρονα.

Υποθέτουμε ότι ισχύει $a < b$ και $a = b$. Τότε έχουμε ότι $a < a$, που δεν ισχύει λόγω της (1).

Όμοια δεν ισχύει $a = b$, $b < a$.

Υποθέτουμε ότι $a < b$ και $b < a$. Από την (3) έπεται ότι $a < a$, άτοπο από την (1).

Θα δείξουμε ότι πράγματι τουλάχιστον ένα από τα $a < b$, $a = b$, $b < a$ ισχύει.

Έστω

$$S = \{ x \in \mathbb{N} \mid \text{ αν } y \in \mathbb{N} \text{ τότε } x < y, \text{ ή } x = y, \text{ ή } y < x \}.$$

Θα δείξουμε ότι $S = \mathbb{N}$.

Προφανώς $1 \in S$, διότι από την (2) έχουμε ότι για όλα τα $y \in \mathbb{N}$ ισχύει $1 \leq y$, δηλαδή $1 = y$ ή $1 < y$.

Υποθέτουμε ότι $x \in S$. Θα δείξουμε ότι $x + 1 \in S$. Επειδή $x \in S$, έχουμε ότι για $y \in \mathbb{N}$ θα ισχύει $x < y$ ή $x = y$ ή $y < x$.

Αν $x < y$, τότε έχουμε ότι υπάρχει $k \in \mathbb{N}$ με $x + k = y$, αν $k = 1$, τότε $x + 1 = y$ και συνεπώς $x + 1 \in S$. Αν $1 < k$, τότε $x + 1 < x + k$ (διότι ισχύει η (4)), οπότε

$$x + 1 < x + k = y,$$

άρα $x + 1 \in S$.

Αν $x = y$, τότε $y < x + 1$ (από την (1)) και συνεπώς $x + 1 \in S$.

Αν $y < x$, τότε $y < x < x + 1$, δηλαδή (από την (3)) έχουμε ότι $y < x + 1$, άρα $x + 1 \in S$.

Τελικά αποδείξαμε ότι, από την υπόθεση $x \in S$ έπεται ότι $x + 1 \in S$, άρα από το αξίωμα iii. έχουμε ότι $S = \mathbb{N}$, και η απόδειξη του ισχυρισμού είναι πλήρης.

(9). Υποθέτουμε ότι $a < b < a + 1$. Από τον ορισμό της ανισότητας $<$ έπεται ότι υπάρχουν $k, m \in \mathbb{N}$ με $b = a + k$ και $a + 1 = b + m$, δηλαδή

$$a + 1 = (a + k) + m = a + (k + m).$$

Οπότε, από τον νόμο της διαγραφής στην πρόσθεση έχουμε ότι $1 = k + m$, άτοπο από την (5) της Πρότασης A.1.6. ό.έ.δ.

Σχόλια A.1.9.

1. Από τις ιδιότητες (1), (8), (3) και (6) έπεται ότι η σχέση $\leq$ είναι σχέση ολικής διάταξης.

2. Όπως στην Πρόταση A.1.6, έτσι και στην προηγουμένη πρόταση οι "προφανείς" ιδιότητες στις ανισότητες των φυσικών αριθμών δεν είναι προφανείς και χρήζουν αποδείξεως.

3. Από την ιδιότητα (9) έπεται ότι οι φυσικοί αριθμοί είναι "διακριτοί".

4. Από την προηγουμένη πρόταση βλέπουμε, διαισθητικά, ότι οι φυσικοί αριθμοί "*συνεχώς αυξάνουν*", ενώ δεν μπορεί "*συνεχώς να φθίνουν*". Ας γίνουμε πιο συγκεκριμένοι.

Η αρχή του ελαχίστου στοιχείου.

Θεώρημα Α.1.10. *Για κάθε μη κενό υποσύνολο S των φυσικών αριθμών υπάρχει ελάχιστο στοιχείο. Δηλαδή υπάρχει $m \in S$, ώστε $m \leq s$, για όλα τα $s \in S$.*

Απόδειξη. Υποθέτουμε ότι δεν υπάρχει $m \in S$, ώστε $m \leq s$, για όλα τα $s \in S$. Θα καταλήξουμε σε άτοπο.

Θεωρούμε το σύνολο

$$A = \{\, a \in \mathbb{N} \mid a < x \text{ για κάθε } x \in S \,\}.$$

Προφανώς $A \cap S = \varnothing$ (γιατί;). Επίσης, $1 \in A$, διότι, διαφορετικά θα υπήρχε $x \in S$ με $x \leq 1$, δηλαδή $x = 1 \in S$, οπότε το S θα είχε ελάχιστο στοιχείο.

Υποθέτουμε ότι $a \in A$ και ότι το $a+1 \notin A$, τότε υπάρχει $x \in S$ με $x \leq a+1$. Αν $x \leq a$, τότε έχουμε άτοπο, από τον ορισμό του συνόλου A. Συνεπώς

$$a < x \leq a+1,$$

δηλαδή $x = a+1 \in S$. Υποθέτουμε ότι υπάρχει $x \in S$ με $x < a+1$, τότε $x \leq a$, άτοπο από τον ορισμό του συνόλου A. Πώς καταλήξαμε στο άτοπο αυτό; υποθέτοντας ότι $a+1 \notin A$. Συνεπώς, από την υπόθεση $a \in A$, έπεται ότι $a+1 \in A$. Οπότε, από το αξίωμα iii. έχουμε ότι $A = \mathbb{N}$. Δηλαδή το S είναι το κενό σύνολο, άτοπο και η απόδειξη ολοκληρώθηκε. ό.έ.δ.

Παρατηρήσεις Α.1.11.

1. Από το προηγούμενο θεώρημα έπεται ότι το σύνολο των φυσικών αριθμών είναι καλώς διατεταγμένο (ιδέ σελίδα 139, Ορισμός 4.4.18).

2. Η απόδειξη του προηγουμένου θεωρήματος στηρίζεται στο αξίωμα iii. (αρχή της Μαθηματικής επαγωγής). Όπως θα δούμε, ισχύει και το αντίστροφο. Δηλαδή, η αρχή της Μαθηματικής επαγωγής και η αρχή του ελαχίστου στοιχείου είναι ισοδύναμες έννοιες.

Θεώρημα Α.1.12. *Έστω $(N, \leq)$ ένα (μη κενό) καλώς διατεταγμένο σύνολο, με e να είναι το ελάχιστο στοιχείο του N και $s : N \longrightarrow N$ μια απεικόνιση με τις ιδιότητες:*

1. *Η s είναι 1-1.*
2. *Για κάθε $n \in N$ με $n \neq e$ υπάρχει $m \in N$, ώστε $n = s(m)$.*
3. *Για κάθε $n \in N$ ισχύει $n < s(n)$.*

Το ζεύγος $(N, \leq)$ ικανοποιεί τα αξιώματα του Peano.

Απόδειξη. Παρατηρούμε ότι για όλα τα $n \in N$ ισχύει ότι $e \leq n < s(n)$, συνεπώς δεν υπάρχει $n \in N$ με $s(n) = e$. Δηλαδή ισχύει το αξίωμα i..

Το αξίωμα ii. ικανοποιείται από την υπόθεση (1).

Έστω $S \subseteq N$, υποθέτουμε ότι το $e \in N$ και ότι αν $n \in S$, τότε $s(n) \in S$. Θα δείξουμε ότι $S = N$.

Υποθέτουμε ότι δεν ισχύει η ισότητα $S = N$, Τότε το σύνολο $U = N \setminus S$ είναι μη κενό και επειδή έχει υποτεθεί ότι το σύνολο N είναι καλώς διατεταγμένο, έπεται ότι υπάρχει $n \in U$ με $n \leq r$, για όλα τα $r \in U$. Το $e \notin U$, συνεπώς $n \neq e$, άρα, από την υπόθεση (2), υπάρχει $m \in N$ με $n = s(m)$. Από την υπόθεση (3) έπεται ότι $m < s(m) = n$. Επειδή το n έχει υποτεθεί ελάχιστο στοιχείο του U, έχουμε ότι $m \notin U$. Δηλαδή $m \in S$. Από την υπόθεσή μας έπεται ότι $s(m) = n \in S$. Αυτό είναι άτοπο. Γιατί καταλήξαμε σε άτοπο; Διότι υποθέσαμε ότι το σύνολο $U = N \setminus S$ είναι μη κενό. Άρα $S = N$ και ικανοποιείται το αξίωμα iii.. ό.έ.δ.

Η αρχή του ελαχίστου στοιχείου μας δίνει την δυνατότητα να δούμε μια εναλλακτική έκφραση του αξιώματος iii. του Peano.

Έστω $a, b \in \mathbb{N}$. Ως συνήθως, θα συμβολίζουμε

$$\{a, \dots, b\} = \{x \in \mathbb{N} \mid a \leq x \leq b\}.$$

Πρόταση Α.1.13. *Έστω $S \subseteq \mathbb{N}$. Υποθέτουμε ότι:*

α. $1 \in S$.

β. Αν $m \in \mathbb{N}$ *και* $\{1, \dots, m\} \subseteq S$, *τότε* $m+1 \in S$.

Τότε $S = \mathbb{N}$.

Απόδειξη. Υποθέτουμε ότι $S \neq \mathbb{N}$, θα καταλήξουμε σε άτοπο. Έστω $U = \mathbb{N} \setminus S$, από την υπόθεσή μας το σύνολο U είναι μη κενό. Από την αρχή του ελαχίστου (Θεώρημα A.1.10) έπεται ότι υπάρχει $n \in U$ με $n \leq r$, για όλα τα $r \in U$. Επειδή το $1 \in S$, το $1 \notin U$, συνεπώς $n \neq 1$, άρα, από την Πρόταση A.1.2, υπάρχει $m \in \mathbb{N}$ με $n = m+1$.

Έστω $k \in \{1, \dots, m\}$, τότε ισχύει ότι $k \leq m < m+1 = n$ και επειδή το n είναι το ελάχιστο στοιχείο του συνόλου U, έχουμε ότι $k \in S$. Αυτό συμβαίνει για το τυχαίο $k \in \{1, \dots, m\}$, δηλαδή αποδείξαμε ότι

$$\{1, \dots, m\} \subseteq S.$$

Από την υπόθεσή μας αυτό σημαίνει ότι

$$m+1 = n \in S,$$

άτοπο. Επομένως, $S = \mathbb{N}$. ό.έ.δ.

Υπάρχει μια ακόμη παραλλαγή του αξιώματος iii., όπου αυτό "*προσαρμόζεται*" για υποσύνολα των φυσικών αριθμών της μορφής $S_k = \{x \mid x \in \mathbb{N} \text{ με } x \geq k\}$, όπου k είναι ένας φυσικός αριθμός.

Πρόταση Α.1.14. *Έστω $U \subseteq \mathbb{N}$ και $k \in \mathbb{N}$. Υποθέτουμε ότι:*

α. $k \in U$.

β. Αν $n \in S_k$ *και* $n \in U$, *τότε* $n+1 \in U$.

Τότε $S_k \subseteq U$.

Απόδειξη. Παρατηρούμε ότι, αν $k = 1$, τότε $S_1 = \mathbb{N}$ και ο ανωτέρω ισχυρισμός είναι το αξίωμα iii..

Επομένως, μπορούμε να υποθέσουμε ότι $k \neq 1$. Από την Πρόταση A.1.2 έπεται ότι υπάρχει (μοναδικός) $b \in \mathbb{N}$, ώστε $k = b+1$. Θεωρούμε το σύνολο

$$T = \{1, \dots, b\} \cup U.$$

Θα εφαρμόσουμε το αξίωμα iii. για να αποδείξουμε ότι $T = \mathbb{N}$, Τότε εύκολα (γιατί;) έπεται ότι $S_k \subseteq U$.

Προφανώς $1 \in T$. Έστω $n \in T$, θα δείξουμε ότι $n+1 \in T$. Οπότε από το αξίωμα iii. έχουμε ότι $T = \mathbb{N}$.

Θα διακρίνουμε περιπτώσεις:

1. $n < b$. Τότε $n+1 \leq b$, δηλαδή
$$n+1 \in \{1, \dots, b\} \subseteq T.$$

2. $n = b$. Τότε
$$n+1 = b+1 = k \in U \subseteq T.$$

3. $n > b$. Τότε $n \notin \{1, \dots, b\}$ και επειδή $n \in T$, έπεται ότι $n \in U$. Επιπλέον, επειδή $n > b$, έχουμε ότι
$$n \geq b+1 = k.$$
Συνεπώς, $n \in S_k$. Τώρα από την υπόθεση (β), δεδομένου ότι $n \in U$, έχουμε ότι
$$n+1 \in U \subseteq T.$$ ό.έ.δ.

Έναν συνδυασμό των δύο προηγουμένων προτάσεων αποτελεί η πρόταση:

Πρόταση Α.1.15. *Έστω $U \subseteq \mathbb{N}$ και $r \in \mathbb{N}$. Υποθέτουμε ότι:*

α. $r \in U$.

β. Αν $k \in S_r$ και $\{r, \dots, k\} \subseteq U$, τότε $k+1 \in U$.

Τότε $S_r \subseteq U$.

Απόδειξη. Η απόδειξη αποτελεί συνδυασμό των επιχειρημάτων των δύο προηγουμένων αποδείξεων και αφήνεται ως άσκηση. ό.έ.δ.

Όπως αναφέραμε και στην αρχή του κεφαλαίου, στην Παράγραφο 3.2.10 είχαμε διατυπώσει δύο θεωρήματα, τα οποία χρησιμοποιούσαμε για να τεκμηριώσουμε Μαθηματικές αποδείξεις με την αρχή της Μαθηματικής επαγωγής. Τα παραθέτουμε πάλι εδώ για να κάνουμε τις αναγκαίες συγκρίσεις.

Θεώρημα Α.1.16. *(Είναι το Θεώρημα 3.2.20). Έστω οι Προτάσεις $P(n)$, $n \in \mathbb{N}$. Υποθέτουμε ότι:*

i. Η $P(1)$ είναι αληθής.

ii. Για κάθε $k \in \mathbb{N}$ αποδεικνύουμε την αλήθεια της συνεπαγωγής
$$P(k) \implies P(k+1)$$
(δηλαδή αν η Πρόταση $P(k)$ είναι αληθής, τότε και η Πρόταση $P(k+1)$ είναι αληθής).

Τότε η Πρόταση $P(n)$ είναι αληθής για όλα τα $n \in \mathbb{N}$.

Όπως βλέπουμε, το θεώρημα αυτό είναι αναδιατύπωση του αξιώματος iii.. Πράγματι, αν πάρουμε το σύνολο
$$S = \{n \in \mathbb{N} \mid \text{η πρόταση} P(n) \text{ είναι αληθής}\}.$$
Τότε βλέπουμε ότι έχουμε το αξίωμα iii..

Θεώρημα Α.1.17. *(Είναι το Θεώρημα 3.2.27) Έστω $r, k \in \mathbb{N}$ με $r \leq k$ και οι Προτάσεις $P(n)$ με $n \in \mathbb{N}$.*

Υποθέτουμε ότι η $P(r)$ είναι αληθής.

Υποθέτουμε ότι, αν οι Προτάσεις $P(j)$, για $r \leq j \leq k$ είναι αληθείς, τότε μπορούμε να αποδείξουμε ότι και η Πρόταση $P(k+1)$ είναι αληθής, δηλαδή η συνεπαγωγή

$$(P(r) \wedge P(r+1) \wedge \cdots \wedge P(k)) \Longrightarrow P(k+1)$$

είναι αληθής.

Τότε οι Προτάσεις $P(n)$ είναι αληθείς για κάθε $n \geq r$.

Όπως βλέπουμε, το θεώρημα αυτό είναι αναδιατύπωση της Πρότασης Α.1.15. Πράγματι, αρκεί στην πρόταση αυτή να θέσουμε

$$U = \{\, n \in \mathbb{N} \mid \text{η πρόταση } P(n) \text{ είναι αληθής} \,\}.$$

Παρατήρηση Α.1.18. Επισημαίνουμε ότι, τόσον το αξίωμα iii., όσον και οι παραλλαγές του είναι της μορφής $P(n) \Longrightarrow P(n+1)$ και η απόδειξη της συνεπαγωγής αυτής δεν συνίσταται στην απόδειξη της αληθείας της Πρότασης $P(n)$, ούτε στην απόδειξη της αληθείας της Πρότασης $P(n+1)$. Συγκεκριμένα, δεν θέλουμε να αποδείξουμε ότι $n \in S$ ούτε ότι $n+1 \in S$, αλλά την αλήθεια της συνεπαγωγής "Αν $n \in S$, τότε $n+1 \in S$".

Η απόδειξη με επαγωγή δεν αποδεικνύει ότι η $P(n)$ είναι αληθής για $n = \infty$ (αν αυτό σημαίνει κάτι), αλλά ότι η Πρόταση $P(n)$ είναι αληθής για άπειρο το πλήθος φυσικούς αριθμούς.

Ιδέ και την Παρατήρηση $3.2.21_1$.

Αναδρομικοί Ορισμοί.

Στην Παρατήρηση Α.1.5_2 είχαμε επισημάνει ότι οι πράξεις της πρόσθεσης και του πολλαπλασιασμού στους φυσικούς αριθμούς ορίζονται "αναδρομικά", όπου διαισθητικά ήμασταν ικανοποιημένοι. Αν όμως εντρυφήσουμε λίγο περισσότερο θα δούμε, για παράδειγμα, ότι το επιχείρημα

"...εφόσον έχει ορισθεί το $n+m$, ορίζεται το $n+\sigma(m) = \sigma(n+m)$..."

για την πρόσθεση "*πάσχει*" στο εξής σημείο: Από τον ορισμό των φυσικών αριθμών **δεν** απορρέει ότι, ξεκινώντας από το 1 και εφαρμόζοντας διαδοχικά την απεικόνιση

$$\sigma(1),\ \sigma(\sigma(1)),\ \ldots,\ \sigma(\cdots(\sigma(\sigma(1)\cdots)\ ^{[2]},$$

τελικά θα φθάσουμε στον φυσικό αριθμό m (αν πούμε "μετά από m βήματα" αμέσως αυτοαναιρούμαστε).

Γενικά συνηθίζουμε να γράφουμε για την επαναληπτική σύνθεση μιας απεικόνισης

$$f : A \longrightarrow A \quad f^n = \underbrace{f \circ \cdots \circ f}_{n}.$$

Μήπως θα ήταν ορθότερο να γράφουμε

"ορίζουμε *αναδρομικά* $f^1 = f$ και $f^n = f \cdot f^{(n-1)}$, για $n \geq 2$";

[2] Εδώ να επισημάνουμε τον συμβολισμό, που έχει καθιερωθεί για τους φυσικούς αριθμούς, $\sigma(1) = 1+1 = 2$, $\sigma(\sigma(1)) = \sigma(2) = 2+1 = 3$, ...

Ο σκοπός είναι να εξαλείψουμε εκφράσεις του τύπου "*και ούτω καθ' εξής*", "*μετά από ορισμένα βήματα*" ή αποσιωπητικά "...", όπου, διαισθητικά, παραπέμπουν σε κάτι, το οποίο θα έπρεπε να είναι στην θέση τους.

Πριν προχωρήσουμε, ας δούμε ένα παράδειγμα. Συνήθως, για έναν φυσικό αριθμό n γράφουμε

$$\Sigma_n = 1 + 2 + \cdots + n$$

για να δηλώσουμε το άθροισμα όλων των φυσικών αριθμών x με την ιδιότητα

$$1 \leq x \leq n.$$

Εδώ έχουμε τα εξής προβλήματα:

Πρώτον, μπορούμε να ορίσουμε επακριβώς τι σημαίνει το Σ_n, για τον κάθε φυσικό αριθμό n;

Δεύτερον, Εφόσον έχουμε ορίσει τι σημαίνει το Σ_n, για τον κάθε φυσικό αριθμό n, μπορούμε να το υπολογίσουμε;

Πρόκειται για δύο προβλήματα. Στο πρώτο θέλουμε να ορίσουμε κάτι και στο δεύτερο να αποδείξουμε ότι ισχύει κάτι.

Ως προς το πρώτο. Αν ορίσουμε

$$\begin{aligned} \Sigma_1 &= 1 \text{ και} \\ \Sigma_{n+1} &= (n+1) + \Sigma_n, \end{aligned}$$

για $n \geq 1$, τότε θα έχουμε επιτύχει έναν "*αναδρομικό*" ορισμό, ο οποίος με σαφήνεια; καθορίζει το Σ_n, για όλα τα $n \in \mathbb{N}$ (Επ' αυτού θα επανέλθουμε αργότερα, ιδέ Παράδειγμα A.1.26).

Ως προς το δεύτερο. Καλούμαστε να υπολογίσουμε τον φυσικό αριθμό Σ_n.

Πρόκειται για διαφορετικά προβλήματα.

Στο δεύτερο πρόβλημα έχουμε, κυρίως, δύο τρόπους αντιμετώπισης. Είτε με απ' ευθείας υπολογισμό ή να *εικάσουμε* το αποτέλεσμα και μετά να αποδείξουμε ότι η *εικασία* μας είναι σωστή.

Εικασίες, που πρέπει να αποδειχθούν για όλους τους φυσικούς αριθμούς (ή για υποσύνολα των φυσικών αριθμών της μορφής $S_k = \{x \mid x \in \mathbb{N} \text{με } x \geq k\}$, όπου $k \in \mathbb{N}$), αποδεικνύονται, συνήθως, με επαγωγικά επιχειρήματα.

Μετά το παράδειγμα αυτό, βλέπουμε ότι υπάρχουν δύο διαφορετικές έννοιες:

Η αναδρομή. και

Η επαγωγή.

Οι δύο αυτές έννοιες είναι στενώς συνδεδεμένες και πολλές φορές (κακώς) θεωρούνται ταυτόσημες, ενώ δεν είναι. Η ουσιώδης διαφορά τους είναι η εξής: Η επαγωγή χρησιμοποιείται για την απόδειξη πραγμάτων, τα οποία έχουν ήδη ορισθεί. Η αναδρομή χρησιμοποιείται για τον ορισμό πραγμάτων.

Θα διατυπώσουμε ένα θεώρημα, το οποίο "εγγυάται την εγκυρότητα" ενός αναδρομικού ορισμού.

Θεώρημα A.1.19. *Έστω A ένα σύνολο, $b \in A$ και $k : A \longrightarrow A$ μια απεικόνιση. Τότε υπάρχει μοναδική απεικόνιση $f : \mathbb{N} \longrightarrow A$, έτσι ώστε*

$$\begin{aligned} f(1) &= b \text{ και} \\ f(n+1) &= k(f(n)), \end{aligned}$$

για όλα τα $n \in \mathbb{N}$.

Απόδειξη. Η απόδειξη, αν και κατανοητή ως προς την σύλληψή της, είναι τεχνική και δεν κρίνεται σκόπιμο να παρατεθεί.

Εδώ θα παρουσιάσουμε μια σκιαγράφηση της απόδειξης.

Θα χρειαστεί να επικαλεστούμε τον ορισμό μιας απεικόνισης ως υποσύνολο ενός καρτεσιανού γινομένου (ιδέ τον Ορισμό 4.5.2).

Στην συγκεκριμένη περίπτωση αναζητούμε ένα $f \subseteq \mathbb{N} \times A$, το οποίο να πληροί τον ορισμό της απεικόνισης.

Δηλαδή για κάθε $n \in \mathbb{N}$ υπάρχει μοναδικό $y \in A$ με $(n, y) \in f$.

Επιπλέον, το υποσύνολο f, που αναζητούμε, πρέπει να πληροί και απαιτήσεις του (προς απόδειξη) Θεωρήματος. Δηλαδή,

i. $(1, b) \in f$ και,

ii. Αν $(n, x) \in f$, τότε $(n+1, k(x)) \in f$, για όλα τα $n \in \mathbb{N}$.

Προφανώς υπάρχει, τουλάχιστον ένα, υποσύνολο του $\mathbb{N} \times A$, το οποίο πληροί τις i. και ii. (για παράδειγμα το ίδιο το $\mathbb{N} \times A$). Το ερώτημα που προκύπτει είναι το εξής:

Υπάρχει κάποιο από αυτά, το οποίο είναι απεικόνιση;

Η ιδέα είναι η εξής:

Λαμβάνουμε ως f να είναι η τομή όλων των υποσυνόλων του $\mathbb{N} \times A$, τα οποία πληρούν τις i. και ii..

Τώρα η απόδειξη ότι η τομή αυτή είναι πράγματι απεικόνιση, είναι τεχνική και αυτό είναι που παραλείπεται, ώστε η απόδειξη να είναι ολοκληρωμένη.

Παρ' όλα ταύτα, συνιστάται να μελετηθεί σε μια δεύτερη ανάγνωση και παραπέμπουμε στα: [1] (Theorem 2.5.5 page 87) και [2] (Θεώρημα 5.6 σελ. 59). ό.έ.δ.

Για την κατανόηση του ανωτέρω θεωρήματος, θα δούμε κάποιες εφαρμογές.

Πρόταση Α.1.20. *(Ο ορισμός της πρόσθεσης). Υπάρχει μοναδική απεικόνιση*

$$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N},$$

η οποία ικανοποιεί τα εξής:

α. $n + 1 = \sigma(n)$, *για όλα τα* $n \in \mathbb{N}$.

β. $n + \sigma(m) = \sigma(n + m)$, *για όλα τα* $n, m \in \mathbb{N}$.

Απόδειξη. Έστω (τυχαίο) $p \in \mathbb{N}$. Παρατηρούμε ότι μπορούμε να εφαρμόσουμε το Θεώρημα Α.1.19 θέτοντας $A = \mathbb{N}$, $b = \sigma(p)$ και $k = \sigma : \mathbb{N} \longrightarrow \mathbb{N}$. Οπότε, υπάρχει μοναδική απεικόνιση $f_p : \mathbb{N} \longrightarrow \mathbb{N}$ με

$$f_p(1) = \sigma(p) \text{ και}$$
$$f_p(n+1) = \sigma(f_p(n)),$$

για όλα τα $n \in \mathbb{N}$. Ορίζουμε την απεικόνιση $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ ως εξής: $n + m = f_n(m)$, για όλα τα $(n, m) \in \mathbb{N} \times \mathbb{N}$. Παρατηρούμε ότι

$$n + 1 = f_n(1) = \sigma(n).$$

Δηλαδή ικανοποιείται το (α). Επίσης, ισχύει ότι

$$n + \sigma(m) = f_n(\sigma(m)) = \sigma(f_n(m)) = \sigma(n + m).$$

Δηλαδή ικανοποιείται το (β).

Η μοναδικότητα έχει αποδειχθεί στην Παρατήρηση Α.1.5$_1$. ό.έ.δ.

Πρόταση Α.1.21. *(Ο ορισμός του πολλαπλασιασμού) Υπάρχει μοναδική απεικόνιση*

$$\cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N},$$

η οποία ικανοποιεί τα εξής:

α. $n \cdot 1 = n$, *για όλα τα* $n \in \mathbb{N}$.

β. $n \cdot \sigma(m) = (n \cdot m) + n$, *για όλα τα* $n, m \in \mathbb{N}$.

Απόδειξη. Έστω $n \in \mathbb{N}$. Ορίζουμε την απεικόνιση $s_n : \mathbb{N} \longrightarrow \mathbb{N}$ με $s_n(m) = m + n$, για όλα τα $m \in \mathbb{N}$. Εφαρμόζουμε το Θεώρημα Α.1.19 για το σύνολο θέτοντας $A = \mathbb{N}$, το στοιχείο n και την απεικόνιση $k = s_n : \mathbb{N} \longrightarrow \mathbb{N}$. Οπότε, υπάρχει μοναδική απεικόνιση $f_n : \mathbb{N} \longrightarrow \mathbb{N}$ με

$$\begin{aligned} f_n(1) &= n \text{ και} \\ f_n(m+1) &= s_n(f_p(m)), \end{aligned}$$

για όλα τα $m \in \mathbb{N}$. Ορίζουμε την απεικόνιση $\cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ ως εξής: $n \cdot m = f_n(m)$. Παρατηρούμε ότι

$$n \cdot 1 = f_n(1) = n.$$

Δηλαδή ικανοποιείται το (α). Επίσης, ισχύει ότι

$$n \cdot \sigma(m) = f_n(\sigma(m)) = s_n(f_n(m)) = f_n(m) + n = (n \cdot m) + n.$$

Δηλαδή ικανοποιείται το (β).

Η μοναδικότητα της πράξης του πολλαπλασιασμού αφήνεται ως άσκηση. ό.έ.δ.

Στο Σχόλιο Α.1.1$_1$ είχαμε αναφέρει ότι το σύνολο των φυσικών αριθμών είναι μοναδικό. Ας δούμε την απόδειξη.

Πρόταση Α.1.22. *Υποθέτουμε ότι το σύνολο* $\mathbb{N}$ *με το στοιχείο* $1 \in \mathbb{N}$ *και την απεικόνιση* $\sigma : \mathbb{N} \longrightarrow \mathbb{N}$ *ικανοποιεί τα αξιώματα Peano. Υποθέτουμε ότι υπάρχει και ένα άλλο σύνολο* $\mathbb{M}$ *με ένα στοιχείο* $e \in \mathbb{M}$ *και μια απεικόνιση* $s : \mathbb{M} \longrightarrow \mathbb{M}$, *το οποίο ικανοποιεί τα αξιώματα Peano. Τότε υπάρχει μια απεικόνιση* $f : \mathbb{N} \longrightarrow \mathbb{M}$, *έτσι ώστε*

$$f(1) = e, \quad f \circ \sigma = s \circ f$$

και η οποία είναι 1-1 και επί.

(Υπ' αυτήν την έννοια, το σύνολο των φυσικών αριθμών είναι μοναδικό).

Απόδειξη. Από το Θεώρημα Α.1.19 έπεται ότι υπάρχει μια απεικόνιση $f : \mathbb{N} \longrightarrow \mathbb{M}$, έτσι ώστε

$$f(1) = e, \quad f \circ \sigma = s \circ f.$$

Απομένει να δειχθεί ότι η f είναι 1-1 και επί.

Έστω $S = f(\mathbb{N})$ το σύνολο τιμών της f. Παρατηρούμε ότι το $e = f(1) \in S$. Υποθέτουμε ότι $m \in S$, τότε υπάρχει $r \in \mathbb{N}$ με $m = f(r)$. Στα δύο μέλη της τελευταίας ισότητας εφαρμόζουμε την απεικόνιση s. Επομένως, έχουμε $s(m) = s(f(r))$. Από την υπόθεση έχουμε ότι $f \circ \sigma = s \circ f$. Οπότε, από την τελευταία ισότητα προκύπτει ότι

$$s(m) = f(\sigma(r)) \in S = f(\mathbb{N}).$$

Παρατηρούμε ότι το σύνολο S ικανοποιεί το αξίωμα iii., άρα $f(\mathbb{N}) = \mathbb{M}$. Δηλαδή η f είναι επί.

Έστω

$$A = \{ n \in \mathbb{N} \mid \text{υπάρχει } m \in \mathbb{N} \text{ με } n \neq m \text{ και } f(n) = f(m) \}.$$

Αν αποδείξουμε ότι το σύνολο A είναι το κενό σύνολο, θα έχουμε αποδείξει ότι η απεικόνιση είναι 1-1 (γιατί; Μα αυτός είναι ο ορισμός του 1-1). Θεωρούμε το σύνολο

$$U = \mathbb{N} \setminus A,$$

Υποθέτουμε ότι υπάρχει $u \in \mathbb{N}$ με $u \neq 1$ και $f(u) = f(1) = e$. Επειδή $u \neq 1$, έπεται ότι υπάρχει $v \in \mathbb{N}$ με $\sigma(v) = u$ (γιατί; Δεν ξεχνάμε την Πρόταση A.1.2). Τότε όμως, από την ισότητα $f(u) = f(1) = e$, θα έχουμε

$$f(\sigma(v)) = f(1) = e.$$

Οπότε, από την υπόθεση $f \circ \sigma = s \circ f$, έπεται ότι $s(f(v)) = e$. Αυτό είναι άτοπο (γιατί; Δεν ξεχνάμε ότι έχουμε υποθέσει ότι η τριάδα $(\mathbb{M}, e, s)$ ικανοποιεί τα αξιώματα του Peano, συνεπώς, από το αξίωμα i. δεν υπάρχει $f(v) \in \mathbb{M}$ με $s(f(v)) = e$). Κατά συνέπεια, δεν υπάρχει $u \in \mathbb{N}$ με $u \neq 1$ και $f(u) = f(1) = e$. Αυτό αποδεικνύει ότι $1 \notin A$, δηλαδή $1 \in U$.

Υποθέτουμε ότι $n \in U$ και $\sigma(n) \notin U$. Θα καταλήξουμε σε άτοπο. Από την υπόθεση $\sigma(n) \notin U$, έπεται ότι $\sigma(n) \in A$. Αυτό σημαίνει ότι υπάρχει $m \in \mathbb{N}$ με

$$\sigma(n) \neq m \text{ και } f(\sigma(n)) = f(m).$$

Το $m \neq 1$ (γιατί; Αν το $m = 1$, τότε θα είχαμε $f(\sigma(n)) = f(1)$ και από τα προηγούμενα θα είχαμε $\sigma(n) = 1$, το οποίο δεν ισχύει). Επομένως, έχουμε ότι

$$f(\sigma(n)) = f(m)$$

με το $m \neq 1$. Τώρα, από την Πρόταση A.1.2, έχουμε ότι υπάρχει $v \in \mathbb{N}$ με $\sigma(v) = m$, οπότε, αντικαθιστώντας στην σχέση $f(\sigma(n)) = f(m)$, έχουμε

$$f(\sigma(n)) = f(\sigma(v)).$$

Από την τελευταία σχέση και την υπόθεση $f \circ \sigma = s \circ f$ έπεται ότι

$$s(f(n)) = s(f(v)).$$

Η s, όμως είναι 1-1. Οπότε, έχουμε

$$f(n) = f(v).$$

Έχουμε όμως υποθέσει ότι $n \in U$, δηλαδή έχουμε

$$n = v.$$

Αυτό είναι άτοπο. (γιατί; Δεν ξεχνάμε ότι έχουμε υποθέσει ότι $\sigma(n) \neq m$ και ότι ισχύει ότι $\sigma(v) = m$ με την σ να είναι 1-1).

Τελικά δεν είναι δυνατόν να έχουμε $n \in U$ και $\sigma(n) \notin U$. Άρα με την υπόθεση $n \in U$ έπεται ότι $\sigma(n) \in U$. Οπότε, από το αξίωμα iii. έπεται ότι $U = \mathbb{N}$ και κατά συνέπεια $A = \emptyset$.

Τέλος. ό.έ.δ.

Θα δούμε ακόμη ένα παράδειγμα, πώς οι δύο έννοιες, αναδρομή και επαγωγή, συνδέονται μεν, διαφέρουν δε.

Παράδειγμα Α.1.23. Έστω το ερώτημα: Να "μελετήσετε" την ακολουθία, η οποία ορίζεται ως εξής:

$$\begin{aligned} a_1 &= 4 \\ a_{n+1} &= 3 + 2a_n, \end{aligned}$$

για όλα τα $n \in \mathbb{N}$.

Τις περισσότερες φορές, σχεδόν όλοι, θεωρούμε αυτονόητο ότι υπάρχει μια (μοναδική) τέτοια ακολουθία και προχωρούμε στην μελέτη της.

Στην πραγματικότητα εγείρεται το εξής ερώτημα: Υπάρχει πράγματι μια ακολουθία, η οποία "ικανοποιεί" την προηγουμένη περιγραφή;

Η διαίσθησή μας μας υπαγορεύει ότι πράγματι υπάρχει τέτοια ακολουθία, μάλιστα δε επιχειρηματολογούμε ως εξής: Γνωρίζουμε ότι $a_1 = 4$, υπολογίζουμε το

$$a_2 = 3 + 2a_1 = 3 + 2 \cdot 4 = 11.$$

Οπότε

$$a_3 = 3 + 2a_2 = 3 + 2a \cdot 11 = 25...$$

και ούτω καθ' εξής συνεχίζουμε....

Όμως, όπως έχουμε επισημάνει, η έκφραση "...και ούτω καθ' εξής συνεχίζουμε..." δεν αποτελεί Μαθηματικό επιχείρημα.

Σύμφωνα με το Θεώρημα Α.1.19, για το σύνολο $A = \mathbb{R}$, για $b = 4$ και για την απεικόνιση $k : \mathbb{R} \longrightarrow \mathbb{R}$ με

$$k(x) = 3 + 2x,$$

για $x \in \mathbb{R}$, υπάρχει μοναδική απεικόνιση $f : \mathbb{N} \longrightarrow \mathbb{R}$ με

$$\begin{aligned} f(1) &= 4 \text{ και} \\ f(n+1) &= 3 + f(n), \end{aligned}$$

για όλα τα $n \in \mathbb{N}$, οπότε, πράγματι υπάρχει η ακολουθία που περιγράψαμε προηγουμένως, απλώς θέτουμε $a_n = f(n)$.

Μέχρι τώρα ορίσαμε αναδρομικά την ακολουθία.

Το επόμενο ερώτημα είναι το εξής: Μπορούμε να βρούμε έναν τρόπο να υπολογίζουμε τον όρο a_n απ' ευθείας, για κάθε $n \in \mathbb{N}$;

Κάνοντας δοκιμές, υπολογίζοντας μερικούς από τους πρώτους όρους της ακολουθίας, καταλήγουμε στην εικασία: $a_n = 7 \cdot 2^{n-1} - 3$, για όλα τα $n \in \mathbb{N}$. Ενδέχεται κάποιος να μας υπαγορεύσει ότι $a_n = 7 \cdot 2^{n-1} - 3$. (Δεν έχει σημασία πώς καταλήξαμε στην εκτίμηση αυτή). Πρέπει να αποδείξουμε ότι πράγματι $a_n = 7 \cdot 2^{n-1} - 3$.

Θα εφαρμόσουμε την αρχή της Μαθηματικής επαγωγής.

Για $n = 1$, έχουμε ότι $a_1 = 7 \cdot 2^{1-1} - 3 = 4$ (το πρώτο βήμα).

Υποθέτουμε ότι για $n \in \mathbb{N}$ πράγματι $a_n = 7 \cdot 2^{n-1} - 3$ (η επαγωγική υπόθεση).

Θα δείξουμε ότι το αποτέλεσμα ισχύει και για $n + 1$ (το επαγωγικό βήμα).

Με απ' ευθείας υπολογισμό έχουμε

$$a_{n+1} = 3 + 2a_n = 3 + 2(7 \cdot 2^{n-1} - 3) = 3 + 7 \cdot 2^n - 6 = 7 \cdot 2^{(n+1)-1} - 3.$$

Οπότε, πράγματι, από την αρχή της Μαθηματικής επαγωγής, έχουμε ότι

$$a_n = 7 \cdot 2^{n-1} - 3.$$

Λίγα περί ακολουθιών.

Στα προηγούμενα έχουμε αναφερθεί πολλές φορές στην έννοια της ακολουθίας. Μάλιστα δε όσοι έχουν ασχοληθεί, έστω και στοιχειωδώς με τον "*Λογισμό πραγματικών αριθμών*" έχουν χρησιμοποιήσει κατά κόρον τις πραγματικές ακολουθίες.

Στην παράγραφο αυτή **δεν** θα προβούμε στην συστηματική μελέτη των ακολουθιών. Απλώς θα αναφέρουμε τους σχετικούς ορισμούς και, σε συνέχεια των προηγουμένων, θα εντρυφήσουμε περισσότερο, μέσω παραδειγμάτων, στις αναδρομικές ακολουθίες.

Ορισμός Α.1.24. Έστω A ένα μη κενό σύνολο, μια απεικόνιση $f : \mathbb{N} \longrightarrow A$ θα ονομάζεται **ακολουθία** με όρους από στο σύνολο A.

Όπως βλέπουμε, μια ακολουθία δεν είναι τίποτε άλλο από μια απεικόνιση, της οποίας το πεδίο ορισμού είναι το σύνολο των φυσικών αριθμών.

Έχει επικρατήσει την εικόνα $f(n)$ του φυσικού αριθμού n μέσω της απεικόνισης (ακολουθίας) f να την συμβολίζουμε με a_n, όπου το πρότυπο n εμφανίζεται ως δείκτης στην εικόνα του ($f(n) = a_n$).

Η διαίσθηση που έχουμε για την αλληλουχία των φυσικών αριθμών, όπου το 1 είναι ο πρώτος φυσικός αριθμός ακολουθούμενος από τον $\sigma(1) = 1+1$, ο $\sigma(1)$ ακολουθείται από τον $\sigma(\sigma(1))$ και ούτω καθ' εξής... μας επιτρέπει, διαισθητικά, να ομιλούμε για τον πρώτο όρο a_1, για τον δεύτερο όρο a_2 μιας ακολουθίας και ούτω καθ' εξής....

Συνήθως μια ακολουθία παριστάνεται ως εξής: $(a_n)_{n\in\mathbb{N}}$ ή ως $(a_1, a_2, \dots)$.

Εδώ πρέπει να προσέξουμε και να μην συγχέουμε το σύνολο τιμών μιας ακολουθίας, το οποίο, ως γνωστόν, είναι το σύνολο

$$f(\mathbb{N}) = \{ f(n) = a_n \in A \mid n \in \mathbb{N} \},$$

με την ακολουθία αυτή καθ' εαυτή.

Για παράδειγμα, η ακολουθία $f : \mathbb{N} \longrightarrow \mathbb{Z}$ με $f(n) = a_n = (-1)^n$, έχει άπειρο το πλήθος όρους $a_1 = (-1)^1 = -1$, $a_2 = (-1)^2 = 1$, ..., ενώ το σύνολο τιμών της είναι το $f(\mathbb{N}) = \{-1, 1\}$.

Το πρόβλημα με τις ακολουθίες, όπως με όλες τις απεικονίσεις, είναι αν μπορούμε να έχουμε έναν "εκπεφρασμένο τύπο"[3], όπου για κάθε στοιχείο του πεδίου ορισμού (εν προκειμένω για κάθε φυσικό αριθμό n), να μπορούμε να υπολογίσουμε την εικόνα του (εν προκειμένω τον n-οστό όρο της ακολουθίας).

Στο Θεώρημα A.1.19 βλέπουμε ότι σε μία ακολουθία, η οποία ορίζεται αναδρομικά, ο όρος a_{n+1} υπολογίζεται ως η τιμή μιας απεικόνισης k.

Στο Παράδειγμα A.1.23 βλέπουμε ότι, από τον αναδρομικό ορισμό της ακολουθίας, μπορούμε να υπολογίσουμε τον "τύπο" της ακολουθίας.

Αυτό γενικά δεν είναι εύκολο, μάλιστα δε τις περισσότερες φορές αυτό δεν είναι δυνατόν.

Ας δούμε το εξής παράδειγμα:

Παράδειγμα Α.1.25. Δίνεται η ακολουθία πραγματικών αριθμών, η οποία ορίζεται αναδρομικά ως εξής:

$$\begin{aligned} a_1 &= 5 \text{ και} \\ a_{n+1} &= 1 + 3(a_n)^2, \end{aligned}$$

για όλα τα $n \in \mathbb{N}$. Το Θεώρημα A.1.19 μας εξασφαλίζει ότι πράγματι μια τέτοια ακολουθία υπάρχει και είναι μοναδική, αλλά δεν είναι εύκολο να υπολογιστεί ο "τύπος" αυτής της ακολουθίας.

[3] Έχει επικρατήσει η έκφραση: *Αναζητούμε έναν κλειστό τύπο για την δοθείσα ακολουθία.*

Ας δούμε τώρα ένα άλλο παράδειγμα.

Παράδειγμα Α.1.26. Θεωρούμε την (γνωστή ιδέ σελ, 328) αναδρομική ακολουθία

$$\Sigma_n = 1 + 2 + \cdots + n,$$

για $n \in \mathbb{N}$. Όπως έχουμε ήδη επισημάνει, τα αποσιωπητικά "..." στο ανωτέρω άθροισμα δεν δίνουν έναν αυστηρό ορισμό της ακολουθίας αυτής. Αν όμως ορίσουμε

$$\begin{aligned} \Sigma_1 &= 1 \text{ και} \\ \Sigma_{n+1} &= (n+1) + \Sigma_n, \end{aligned}$$

τότε βλέπουμε ότι το Θεώρημα Α.1.19 δεν "καλύπτει" την περίπτωση αυτή, διότι για τον όρο Σ_{n+1} δεν υπάρχει απεικόνιση $k : \mathbb{R} \longrightarrow \mathbb{R}$, ώστε $\Sigma_{n+1} = k(\Sigma_n)$.

Το επόμενο θεώρημα μας "εγγυάται" ότι πράγματι η ακολουθία Σ_n είναι καλά ορισμένη και μοναδική.

Θεώρημα Α.1.27. *Έστω A ένα σύνολο, $e \in A$ και $r : A \times \mathbb{N} \longrightarrow A$ μια απεικόνιση. Τότε υπάρχει μοναδική απεικόνιση $g : \mathbb{N} \longrightarrow A$ με*

$$\begin{aligned} g(1) &= e \text{ και} \\ g(n+1) &= r(g(n), n), \end{aligned}$$

για όλα τα $n \in \mathbb{N}$.

Απόδειξη. Η απόδειξη στηρίζεται στο Θεώρημα Α.1.19.

Συγκεκριμένα εφαρμόζουμε το θεώρημα αυτό για το σύνολο $A \times \mathbb{N}$, για το στοιχείο $(e, 1)$ και για την απεικόνιση $k : A \times \mathbb{N} \longrightarrow A \times \mathbb{N}$ με

$$k(x, n) = (r(x, n), n+1), \quad \text{για όλα τα } (x, n) \in A \times \mathbb{N} \qquad (*)$$

Επομένως, υπάρχει μοναδική απεικόνιση $f : \mathbb{N} \longrightarrow A \times \mathbb{N}$ με

$$\begin{aligned} f(1) &= (e, 1) \text{ και} \\ f(n+1) &= k(f(n)), \end{aligned}$$

για όλα τα $n \in \mathbb{N}$.

Εμείς όμως θέλουμε μια απεικόνιση $g : \mathbb{N} \longrightarrow A$ με

$$\begin{aligned} g(1) &= e \text{ και} \\ g(n+1) &= r(g(n), n), \end{aligned}$$

για όλα τα $n \in \mathbb{N}$.

Η απεικόνιση $f : \mathbb{N} \longrightarrow A \times \mathbb{N}$ επάγει δύο απεικονίσεις "κατά συντεταγμένες". Δηλαδή, αν $f(n) = (f_1(n), f_2(n))$, τότε έχουμε τις απεικονίσεις

$$f_1 : \mathbb{N} \longrightarrow A \text{ και } f_2 : \mathbb{N} \longrightarrow \mathbb{N}.$$

Δεν έχουμε παρά να ορίσουμε την $g = f_1$. Τότε προφανώς

$$g(1) = e$$

και από την σχέση $f(n+1) = k(f(n))$ έχουμε

$$k(f(n)) = f(n+1) = (g(n+1), f_2(n+1)).$$

Επίσης, από την (∗), έχουμε ότι

$$k((f(n)) = k(g(n), f_2(n)) = (r((g(n), f_2(n))), f_2(n) + 1).$$

Συνεπώς

$$g(n+1) = r((g(n), f_2(n))) \text{ και } f_2(n+1) = f_2(n) + 1.$$

Από την τελευταία ισότητα $f_2(n+1) = f_2(n) + 1$ και το γεγονός ότι η απεικόνιση f είναι μοναδική (άρα και οι απεικονίσεις f_1, f_2 είναι μοναδικές) έπεται ότι η f_2 είναι η ταυτοτική απεικόνιση. Επομένως, από την ισότητα

$$g(n+1) = r((g(n), f_2(n)))$$

έπεται ότι τελικά

$$g(n+1) = r(g(n), n),$$

για όλα τα $n \in \mathbb{N}$. Όπως είχαμε απαιτήσει. ό.έ.δ.

Επανερχόμενοι στο προηγούμενο παράδειγμα, έχουμε την απεικόνιση

$$r : \mathbb{R} \times \mathbb{N} \longrightarrow \mathbb{R} \text{ με } r(x, n) = (n+1) + x.$$

Οπότε, η ακολουθία $(\Sigma_n)_{n\in\mathbb{N}}$ με

$$\begin{aligned} \Sigma_1 &= 1 \text{ και} \\ \Sigma_{n+1} &= r(\Sigma_n, n) = (n+1) + \Sigma_n \end{aligned}$$

ορίζεται καλά και είναι μοναδική. Οπότε, απ' ευθείας (ιδέ Άσκηση 3.2.3 $_8$) ή με επαγωγή (ιδέ Άσκηση 3.2.11$_1$) αποδεικνύουμε ότι

$$\Sigma_n = \frac{n(n+1)}{2}.$$

Θα συνεχίσουμε την αναφορά μας στις αναδρομικές ακολουθίες παρουσιάζοντας, εν συντομία, δύο χαρακτηριστικά παραδείγματα.

Οι αριθμοί Fibonacci και οι αριθμοί Lucas.

Ορίζουμε την εξής αναδρομική ακολουθία:

$$\begin{aligned} F_1 &= 1, F_2 = 1 \text{ και} \\ F_{n+2} &= F_{n+1} + F_n, \end{aligned}$$

για όλα τα $n \in \mathbb{N}$.

Η ακολουθία αυτή ονομάζεται **ακολουθία Fibonacci** και οι όροι της **αριθμοί Fibonacci**.

Όπως παρατηρούμε, η ακολουθία αυτή ορίζεται αναδρομικά *επικαλώντας* τους δύο προηγουμένους όρους. Αυτό είναι διαφορετικό από την περίπτωση όπου για να ορισθεί ο επόμενος όρος μιας ακολουθίας *αρκούσε* να γνωρίζουμε τον (αμέσως) προηγούμενο. Επομένως, δεν μπορούμε να συμπεράνουμε (αβασάνιστα), επικαλούμενοι το Θεώρημα A.1.19 (ούτε το Θεώρημα A.1.27) ότι πράγματι υπάρχει (και μάλιστα μοναδική) τέτοια ακολουθία.

Ας δούμε ορισμένες ιδιότητες αυτής της ακολουθίας.

Πρόταση Α.1.28. *Έστω $n \in \mathbb{N}$. Για την ακολουθία Fibonacci ισχύει:*

i. $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$.

ii. $F_1^2 + F_2^2 + \cdots + F_n^2 = F_n F_{n+1}$.

iii. Αν $n \geq 2$, τότε $F_n^2 - F_{n+1}F_{n-1} = (-1)^{n+1}$.

Απόδειξη. Θα αποδείξουμε μόνο το iii. αφήνοντας τα i. και ii. ως άσκηση (Άσκηση A.1.1$_{12}$).

Θα χρησιμοποιήσουμε επαγωγή. Παρατηρούμε ότι για $n = 2$ έχουμε ότι

$$F_2^2 - F_3F_1 = 1^2 - 2 \cdot 1 = 1 = (-1)^{2+1}.$$

Άρα ο ισχυρισμός ισχύει για $n = 2$. Υποθέτουμε ότι $n \geq 3$ και ότι ο ισχυρισμός ισχύει για όλα τα $k \in \{2, \ldots, n\}$. Χρησιμοποιούμε τον ορισμό $F_{n+2} = F_{n+1} + F_n$ και κάνοντας υπολογισμούς έχουμε ότι:

$$\begin{aligned} F_{n+1}^2 - F_{n+2}F_n &= (F_n + F_{n-1})^2 - (F_{n+1} + F_n)F_n \\ &= F_n^2 + 2F_nF_{n-1} + F_{n-1}^2 - F_{n+1}F_n - F_n^2 \\ &= F_{n-1}^2 + F_n(2F_{n-1} - F_{n+1}) \\ &= F_{n-1}^2 + F_n(2F_{n-1} - (F_n + F_{n-1})) \\ &= F_{n-1}^2 + F_n(F_{n-1} - F_n) \\ &= F_{n-1}^2 - F_nF_{n-2} = (-1)^{(n-1)+1} = (-1)^{(n+1)+1}. \end{aligned}$$

Όπου η (προ)τελευταία ισότητα ισχύει λόγω της επαγωγικής υπόθεσης. ό.έ.δ.

Πόρισμα Α.1.29. *Διαδοχικοί όροι στην ακολουθία Fibonacci είναι σχετικά πρώτοι. Δηλαδή μ.κ.δ. $(F_{n+1}, F_n) = 1$, για όλα τα $n \in \mathbb{N}$.*

Απόδειξη. Η απόδειξη είναι άμεση από την προηγουμένη Πρόταση.

Μπορείτε να δώσετε μια απόδειξη στηριζόμενοι μόνο στον ορισμό της ακολουθίας Fibonacci; ό.έ.δ.

Μια άλλη "εκδοχή" του αποτελέσματος, που μόλις αποδείξαμε είναι:

Πρόταση Α.1.30. *Για κάθε $n \in \mathbb{N}$ ισχύει:*

$$F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n.$$

Απόδειξη. Η απόδειξη μπορεί να στηριχθεί στην προηγουμένη πρόταση, αλλά μπορεί να αποδειχθεί και απ' ευθείας με επαγωγή. ό.έ.δ.

Από τον ορισμό της ακολουθίας Fibonacci έπεται αμέσως ότι για $n \in \mathbb{N}$ ισχύει ότι

$$F_{n+3} = F_{n+2} + F_{n+1} = 2F_{n+1} + F_n$$

και

$$F_{n+4} = F_{n+3} + F_{n+2} = 3F_{n+1} + 2F_n.$$

Οπότε, δοθέντος ενός $n \in \mathbb{N}$, εύκολα συμπεραίνουμε (με επαγωγή ως προς το $m \in \mathbb{N}$) ότι γενικά ισχύει

$$F_{n+(m+1)} = F_{m+1}F_{n+1} + F_mF_n \qquad (*)$$

Επιλέγοντας τώρα, ως m, ένα πολλαπλάσιο του n, συμπεραίνουμε ότι

$$\text{ο } F_{kn} \text{ είναι πολλαπλάσιο του } F_k \qquad (**)$$

Επομένως, παρατηρούμε ότι, στην ακολουθία Fibonacci, όλοι οι όροι της μορφής F_{3n} είναι άρτιοι, όλοι οι όροι της μορφής F_{4n} είναι πολλαπλάσια του 3... και συνεχίζουμε....

Οπότε, γεννάται το ερώτημα (σε συνδυασμό με το Πόρισμα A.1.29): Τι θα μπορούσαμε να πούμε γενικότερα επ' αυτού;

Θεώρημα A.1.31. *Έστω F_n, F_m δύο (τυχαίοι) αριθμοί Fibonacci και $d = μ.κ.δ.(n, m)$. Ένας θετικός ακέραιος δ είναι κοινός διαιρέτης των F_n και F_m, αν και μόνο αν ο δ διαιρεί τον F_d. Συγκεκριμένα, μ.κ.δ. $(F_n, F_m) = F_d$.*

Απόδειξη. Από την σχέση $(*)$ έπεται ότι κάθε κοινός διαιρέτης των F_n και F_m είναι διαιρέτης του F_{n+m} (γιατί;). Επίσης, από την ίδια σχέση, έχουμε ότι κάθε κοινός διαιρέτης των F_{n+m} και F_n είναι και διαιρέτης του $F_m F_{n+1}$ (γιατί;). Αλλά οι F_n και F_{n+1} είναι σχετικά πρώτοι, επομένως αναγκαστικά θα είναι διαιρέτης του F_m (γιατί;).

Άρα, προς το παρόν, έχουμε αποδείξει την ισοδυναμία:

Ο δ είναι κοινός διαιρέτης των F_n και F_m, αν και μόνο αν είναι κοινός διαιρέτης των F_{n+m} και F_m.

Τώρα, μπορούμε εύκολα να γενικεύσουμε και να αποδείξουμε, με επαγωγή, ότι:

Ο δ είναι κοινός διαιρέτης των F_n και F_m, αν και μόνο αν είναι κοινός διαιρέτης των F_{n+km} και F_m, για όλα τα $k \in \mathbb{N}$.

Επομένως, αν υ είναι το υπόλοιπο της διαίρεσης του n με τον m, έχουμε ότι:

Ο δ είναι κοινός διαιρέτης των F_n και F_m, αν και μόνο αν είναι κοινός διαιρέτης των F_υ και F_m.

Επαναλαμβάνοντας την ίδια διαδικασία, δηλαδή εφαρμόζοντας τον αλγόριθμο του Ευκλείδη, συμπεραίνουμε ότι

Ο δ είναι κοινός διαιρέτης των F_n και F_m, αν και μόνο αν είναι κοινός διαιρέτης των F_d και F_m.

Αλλά ο F_d διαιρεί τον F_m (γιατί; μα ισχύει η $(**)$).

Συνεπώς, η απόδειξη ολοκληρώθηκε. ό.έ.δ.

Όπως έχουμε αναφέρει, γενικά, όταν έχουμε μια αναδρομική ακολουθία, ενδιαφερόμαστε, αν μπορούμε να υπολογίσουμε τον n-οστό όρο της ακολουθίας απ' ευθείας. Θα δούμε πώς απαντούμε στο ερώτημα αυτό στην περίπτωση της ακολουθίας Fibonacci.

Θα ξεκινήσουμε δίνοντας την απάντηση.

Θεώρημα A.1.32. *Για κάθε $n \in \mathbb{N}$ ισχύει ότι*

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

Υπάρχουν πολλές αποδείξεις της ανωτέρω ισότητας. Πριν δούμε μια απόδειξη, θα κάνουμε μια ανάλυση του προβλήματος για να δούμε πώς εμφανίζεται η "ποσότητα" $\phi = \frac{1+\sqrt{5}}{2}$.

Στην Πρόταση A.1.30 είχαμε δει ότι:

Για κάθε $n \in \mathbb{N}$ ισχύει:

$$F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n.$$

Διαιρούμε και τα δύο μέλη της ισότητας αυτής με το F_n^2 και έχουμε

$$\left(\frac{F_{n+1}}{F_n}\right)^2 - \frac{F_{n+1}}{F_n} - 1 = \frac{(-1)^n}{F_n^2}.$$

Παρατηρούμε ότι, για *πολύ μεγάλες* τιμές του n, το δεξιό μέλος της ανωτέρω ισότητας *πλησιάζει* στο μηδέν, ενώ το αριστερό *προσιδιάζει* στο πολυώνυμο $x^2 - x - 1$. Επομένως, καθώς το n αυξάνει, ο λόγος $\frac{F_{n+1}}{F_n}$ *προσεγγίζει* μια από τις ρίζες του $x^2 - x - 1$, και καθώς $\frac{F_{n+1}}{F_n} > 1$, ο λόγος $\frac{F_{n+1}}{F_n}$ προσεγγίζει την θετική ρίζα

$$\phi = \frac{1+\sqrt{5}}{2}.$$

Η προηγουμένη διαισθητική προσέγγιση θα μπορούσε να παρουσιασθεί "τυπικά" με την έννοια του ορίου. Αν και δεν έχουμε αναφέρει την έννοια του ορίου, θεωρούμε ότι ο αναγνώστης είναι, έστω και στοιχειωδώς, εξοικειωμένος.

Θα δείξουμε ότι $\lim_{n\longrightarrow\infty} \frac{F_{n+1}}{F_n} = \phi$.

Υποθέτουμε ότι $\lim_{n\longrightarrow\infty} \frac{F_{n+1}}{F_n} = L$.

Τότε έχουμε

$$\begin{aligned} 1 + L &= \left(\lim_{n\longrightarrow\infty} \frac{F_n}{F_n}\right) + \left(\lim_{n\longrightarrow\infty} \frac{F_{n+1}}{F_n}\right) \\ &= \lim_{n\longrightarrow\infty} \frac{F_n + F_{n+1}}{F_n} \\ &= \lim_{n\longrightarrow\infty} \frac{F_{n+2}}{F_n} \\ &= \lim_{n\longrightarrow\infty} \left(\frac{F_{n+2}}{F_{n+1}} \cdot \frac{F_{n+1}}{F_n}\right) \\ &= \left(\lim_{n\longrightarrow\infty} \frac{F_{n+2}}{F_{n+1}}\right) \cdot \left(\lim_{n\longrightarrow\infty} \frac{F_{n+1}}{F_n}\right) = L^2. \end{aligned}$$

Δηλαδή $1 + L = L^2$. Επομένως, πράγματι $L = \phi$, δεδομένου ότι είναι η (θετική) ρίζα του πολυωνύμου $x^2 - x - 1$.

Απόδειξη. Απόδειξη του Θεωρήματος.

Θα χρησιμοποιήσουμε επαγωγή.

Θέτουμε

$$\phi = \frac{1+\sqrt{5}}{2} \text{ και } \bar{\phi} = \frac{1-\sqrt{5}}{2} = 1 - \phi.$$

Τα ϕ και $\bar{\phi}$, ως ρίζες του πολυωνύμου $x^2 - x - 1$, ικανοποιούν τις σχέσεις

$$\phi^2 = \phi + 1 \text{ και } \bar{\phi}^2 = \bar{\phi} + 1.$$

Παρατηρούμε ότι

$$F_1 = \frac{\phi^1 - \bar{\phi}^1}{\phi - \bar{\phi}} \text{ και } F_2 = \frac{\phi^2 - \bar{\phi}^2}{\phi - \bar{\phi}} \text{ (απλή επαλήθευση).}$$

Έστω $n \in \mathbb{N},\ n \geq 2$. Υποθέτουμε ότι

$$F_k = \frac{\phi^k - \bar{\phi}^k}{\phi - \bar{\phi}},$$

για όλα τα $k \leq n$.

Εκ του ορισμού της ακολουθίας Fibonacci έχουμε ότι $F_{n+1} = F_n + F_{n-1}$. Επομένως, από την υπόθεση έχουμε ότι

$$\begin{aligned} F_{n+1} &= F_n + F_{n-1} \\ &= \frac{\phi^n - \bar{\phi}^n}{\phi - \bar{\phi}} + \frac{\phi^{n-1} - \bar{\phi}^{n-1}}{\phi - \bar{\phi}} \\ &= \frac{(\phi^n - \bar{\phi}^n) + (\phi^{n-1} - \bar{\phi}^{n-1})}{\phi - \bar{\phi}} \\ &= \frac{\phi^{n-1}(\phi + 1) - \bar{\phi}^{n-1}(\bar{\phi} + 1)}{\phi - \bar{\phi}}. \end{aligned}$$

Αλλά $\phi^2 = \phi + 1$ και $\bar{\phi}^2 = \bar{\phi} + 1$, οπότε αντικαθιστώντας στην τελευταία ισότητα έχουμε ότι

$$F_{n+1} = \frac{\phi^{n-1}\phi^2 - \bar{\phi}^{n-1}\bar{\phi}^2}{\phi - \bar{\phi}} = \frac{\phi^{n+1} - \bar{\phi}^{n+1}}{\phi - \bar{\phi}}.$$ ό.έ.δ.

Πρόταση Α.1.33. *Για κάθε φυσικό αριθμό n ισχύει ότι*

$$\phi^{n-2} \leq F_n \leq \phi^{n-1}.$$

Απόδειξη. Η απόδειξη είναι εύκολη και μπορεί να προκύψει *λογιστικά* από το προηγούμενο θεώρημα ή εφαρμόζοντας επαγωγή. ό.έ.δ.

Θα κλείσουμε την σύντομη αναφορά στην ακολουθία Fibonacci παραθέτοντας ορισμένα σχόλια.

i. Στην αρχή είχαμε επισημάνει ότι τα Θεωρήματα Α.1.19 και Α.1.27 δεν εγγυώνται την ύπαρξη και την μοναδικότητα της ακολουθίας Fibonacci. Ισχύει ένα παρόμοιο θεώρημα, το οποίο παραθέτουμε ως άσκηση (Άσκηση Α.1.1_{21}).

ii. Ιστορικά φέρεται η ακολουθία αυτή να ορίστηκε από τον Fibonacci (ψευδώνυμο του Leonardo of Pisa, γεννημένος περίπου το 1175), αλλά είναι γνωστό ότι, πριν τον Fibonacci, οι Ινδοί Μαθηματικοί είχαν χρησιμοποιήσει την ακολουθία αυτή. Μάλιστα γίνεται ιδιαίτερη αναφορά στον Acharya Hemachandra (1089 – 1173), ο οποίος χρησιμοποίησε παρόμοια ακολουθία για την αποκρυπτογράφηση της Σανσκριτικής γραφής.

   Οι αριθμοί Fibonacci εμφανίζονται σε όλες τις επιστήμες και "ξεφυτρώνουν" απροσδόκητα. Δεν θα αναφερθούμε στις πράγματι σημαντικές και εντυπωσιακές εφαρμογές τους, δεδομένου ότι δεν είναι αυτός ο σκοπός μας.

   Απλώς επισημαίνουμε την, φαινομενικά απροσδόκητη, σχέση των αριθμών Fibonacci με τον αριθμό $\phi = \dfrac{1+\sqrt{5}}{2}$. Ο αριθμός αυτός, γνωστός ως **λόγος της χρυσής τομής** είναι γνωστός από την αρχαιότητα και έχει άμεση σχέση με το εξής πρόβλημα:

Δίνεται ένα ευθύγραμμο τμήμα AB μήκους 1. Να βρεθεί ένα σημείο Γ μεταξύ των A και B, ώστε, αν τα μήκη των τμημάτων $A\Gamma$ και ΓB είναι b και c αντίστοιχα, να ισχύει $\dfrac{1}{c} = \dfrac{c}{b}$.

Δεδομένου ότι πρέπει να ισχύει $b+c = 1$, έπεται ότι πρέπει να ισχύει $\dfrac{1}{c} = \dfrac{c}{1-c}$, εξού προκύπτει ότι $c^2 = 1-c$, δηλαδή το c είναι η (θετική) ρίζα του πολυωνύμου $x^2 + x - 1$, απ' όπου προκύπτει ότι $c = \phi - 1$[4].

iii. Ο (κλειστός) τύπος, όπου υπολογίζουμε τον n-οστό όρο της ακολουθίας Fibonacci απ' ευθείας (Θεώρημα A.1.32), ονομάζεται τύπος του Binet, αν και είναι γνωστό ότι οφείλεται στους L. Euler και D. Bernoulli.

Εδώ πρέπει να επισημάνουμε ότι στο Θεώρημα A.1.32 αποδείξαμε (επαγωγικά) ότι πράγματι ισχύει ο ισχυρισμός. Παραμένει όμως το ερώτημα πώς εικάστηκε το αποτέλεσμα, το οποίο αποδείξαμε. Υπάρχουν άλλες αποδείξεις, όπου υπολογίζεται απ' ευθείας ο n-οστός όρος της ακολουθίας Fibonacci. Για παράδειγμα, χρησιμοποιώντας δυναμοσειρές και γεννήτριες συναρτήσεις ή χρησιμοποιώντας ιδιότητες των πινάκων. Αυτά είναι πέραν των σκοπών του παρόντος.

iv. Στην προσπάθεια να αποδείξουμε ότι $\lim\limits_{n\longrightarrow\infty} \dfrac{F_{n+1}}{F_n} = \phi$ προβήκαμε σε ένα ατόπημα. Μπορείτε να το εντοπίσετε;[5]

v. Ορισμένοι συγγραφείς (για διαχειριστικούς κυρίως λόγους) ορίζουν η ακολουθία Fibonacci να αρχίζει από το μηδέν, δηλαδή

$$F_1 = 0, F_2 = 1, F_3 = 1, F_4 = 2, \dots,$$

αυτό δεν δημιουργεί κανένα πρόβλημα.

Μια άλλη αναδρομική ακολουθία, που θα μελετήσουμε εν συντομία, ορίζεται ως εξής:

$$\begin{aligned} L_1 &= 1, L_2 = 3 \text{ και} \\ L_{n+2} &= L_{n+1} + L_n, \end{aligned}$$

για όλα τα $n \in \mathbb{N}$.

Η ακολουθία αυτή ονομάζεται **ακολουθία Lucas** και οι όροι της **αριθμοί Lucas**.

Όπως και στην περίπτωση της ακολουθίας Fibonacci (ιδέ σχετικά σχόλια), η ακολουθία αυτή ορίζεται καλά και είναι μοναδική.

Παρατηρούμε ότι η ακολουθία Lucas *προσιδιάζει* με την ακολουθία Fibonacci. Ορίζονται και οι δύο με τον ίδιο αναδρομικό τρόπο, με μόνη διαφορά ότι $F_2 = 1$, ενώ $L_2 = 3$, η οποία όμως καθορίζει την πλήρη διαφοροποίηση σε όλους τους υπόλοιπους όρους.

Η ακολουθία Lucas έχει "παράλληλες" ιδιότητες με την ακολουθία Fibonacci.

---

[4] Παραμένει το ερώτημα: Μπορούμε να προσδιορίσουμε την θέση του σημείου Γ επάνω στο ευθύγραμμο τμήμα AB, χρησιμοποιώντας μόνο κανόνα και διαβήτη; Γνωρίζουμε στοιχειωδώς την Ευκλείδεια Γεωμετρία;

[5] Αυθαιρέτως δεχθήκαμε ότι υπάρχει το όριο, έστω L, και μετά αποδείξαμε ότι $L = \phi$. Πρώτα θα έπρεπε να εξασφαλίσουμε ότι πράγματι η εν λόγω ακολουθία έχει όριο. Εδώ αυτό το δεχόμαστε, διότι πράγματι έτσι είναι, αλλά η απόδειξη είναι πέραν του σκοπού μας. Γενικά πρέπει να είμαστε προσεκτικοί.

Θεώρημα Α.1.34. *Για κάθε $n \in \mathbb{N}$ ισχύει ότι*

i. $L_n = \phi^n + \bar{\phi}^n$, *όπου* $\phi = \dfrac{1+\sqrt{5}}{2}$ *και* $\bar{\phi} = \dfrac{1-\sqrt{5}}{2} = 1 - \phi$.

ii. $L_1 + L_2 + \cdots + L_n = L_{n+2} - 3$.

iii. $L_1^2 + L_2^2 + \cdots + L_n^2 = L_n L_{n+1} - 2$.

iv. Αν $n \geq 2$, *τότε* $L_n^2 - L_{n+1}L_{n-1} = 5(-1)^n$.

v. Αν $n \geq 2$, *τότε* $L_{n+1}^2 - L_n^2 = L_{n-1}L_{n+2}$.

Απόδειξη. Παρατηρήστε και εντοπίστε ομοιότητες και διαφορές με αντίστοιχες ιδιότητες που ισχύουν για την ακολουθία Fibonacci, οι οποίες αναφέρονται στο Θεώρημα Α.1.32 και στις Προτάσεις Α.1.28 και Α.1.30.

Η απόδειξη είναι παρόμοια με την απόδειξη, που κάναμε στις αντίστοιχες περιπτώσεις για την ακολουθία Fibonacci και αφήνεται ως άσκηση (Άσκηση Α.1.1_{18}). ό.έ.δ.

Μεταξύ των όρων των ακολουθιών Fibonacci και Lucas υπάρχουν αξιοσημείωτες σχέσεις. Μερικές αναφέρονται στην επομένη πρόταση.

Πρόταση Α.1.35. *Για κάθε $n \in \mathbb{N}$ ισχύει:*

i. $L_n = \dfrac{F_{2n}}{F_n} = F_n + 2F_{n-1} = F_{n+1} + F_{n-1} = 2F_{n+1} - F_n$.

ii. $F_n = \dfrac{2L_{n+1} - L_n}{5} = \dfrac{L_{n+1} + L_{n-1}}{5}$, *όπου στην δεύτερη ισότητα έχουμε* $n \geq 2$.

Απόδειξη. Θα αποδείξουμε μόνο την πρώτη ισότητα στην περίπτωση i., αφήνοντας τις υπόλοιπες περιπτώσεις ως άσκηση (Άσκηση Α.1.1_{20}).

Υπάρχουν δύο προσεγγίσεις για την απόδειξη της ισότητας

$$L_n = \frac{F_{2n}}{F_n}.$$

Μία εφαρμόζοντας ευθεία απόδειξη, και μία εφαρμόζοντας επαγωγή.

Θα εφαρμόσουμε ευθεία απόδειξη.

Γνωρίζουμε ότι για κάθε $m \in \mathbb{N}$ ισχύει

$$F_m = \frac{\phi^m - \bar{\phi}^m}{\phi - \bar{\phi}} \qquad \text{(Θεώρημα Α.1.32)}$$

και

$$L_m = \phi^m + \bar{\phi}^m \qquad \text{(Θεώρημα Α.1.34)}$$

Οπότε, με απλή αντικατάσταση έπεται το αποτέλεσμα.

Προσπαθήστε να αποδείξετε την ίδια ισότητα με επαγωγή. ό.έ.δ.

Δεν θα επεκταθούμε περισσότερο στις αναδρομικές ακολουθίες, καθ' ότι σκοπός μας είναι να γίνει κατανοητή η σύνδεση (διαφορές και ομοιότητες) μεταξύ των εννοιών "επαγωγή" και "αναδρομή".

Α.1.1 Ασκήσεις

1. Να αποδείξετε (εξ ολοκλήρου) την Πρόταση Α.1.6

2. Να δείξετε ότι στον ορισμό της ανισότητας $a < b$, αν υπάρχει $k \in \mathbb{N}$, ώστε $b = a + k$, το k είναι μοναδικό.

3. Να αποδείξετε (εξ ολοκλήρου) την Πρόταση Α.1.8.

4. Να αποδείξετε την Πρόταση Α.1.15.

5. Να δείξετε την μοναδικότητα της πράξης του πολλαπλασιασμού των φυσικών αριθμών.

6. Έστω $a, b \in \mathbb{N}$. Υποθέτουμε ότι $a + a = b + b$. Δείξτε ότι $a = b$.

7. Έστω $b \in \mathbb{N}$. Δείξτε ότι

$$\{n \in \mathbb{N} \mid 1 \leq n \leq b\} \cup \{n \in \mathbb{N} \mid b + 1 \leq n\} = \mathbb{N}.$$
$$\{n \in \mathbb{N} \mid 1 \leq n \leq b\} \cap \{n \in \mathbb{N} \mid b + 1 \leq n\} = \varnothing.$$

8. Έστω $a, b \in \mathbb{N}$ με $a < b$.

   i. Για τυχαίο $k \in \mathbb{N}$, δείξτε ότι υπάρχει μια απεικόνιση

   $$\alpha : \{a, \dots, b\} \longrightarrow \{a + k, \cdots, b + k\},$$

   η οποία είναι 1-1 και επί.

   ii. Έστω p ο (μοναδικός) φυσικός αριθμός, ώστε $b = a + p$. Δείξτε ότι υπάρχει μια απεικόνιση

   $$\beta : \{a, \dots, b\} \longrightarrow \{1, \cdots, p + 1\},$$

   η οποία είναι 1-1 και επί.

9. Ένα υποσύνολο $A \subseteq \mathbb{N}$ θα ονομάζεται *κλειστό*, αν $a \in A$ συνεπάγεται ότι $a + 1 \in A$.

   Υποθέτουμε ότι το $A \subseteq \mathbb{N}$ είναι κλειστό.

   i. Δείξτε ότι, αν $n \in \mathbb{N}$ και $a \in A$, τότε $a + n \in A$.

   ii. Δείξτε ότι, αν $a \in A$, τότε $\{x \in \mathbb{N} \mid x \geq a\} \subseteq A$.

10. Δείξτε ότι κάθε πεπερασμένο υποσύνολο των πραγματικών αριθμών έχει μέγιστο και ελάχιστο στοιχείο.

    Υπόδειξη: Εφαρμόστε το Θεώρημα Α.1.27.

11. Έστω $f : \mathbb{N} \longrightarrow \mathbb{N}$ μια απεικόνιση με την ιδιότητα $f(n) < f(n+1)$, για όλα τα $n \in \mathbb{N}$. Δείξτε ότι $n \leq f(n)$, για όλα τα $n \in \mathbb{N}$.

12. Δίνεται η αναδρομική ακολουθία $(a_n)_{n\in\mathbb{N}}$ με

$$a_1 = 1,\ a_2 = 1 \text{ και}$$
$$a_{n+2} = a_{n+1} + 3a_n.$$

Εικάστε ποιοι όροι της ακολουθίας αυτής είναι πολλαπλάσια του 4. Αποδείξτε την εικασία σας.

13. Να αποδείξετε πλήρως την Πρόταση A.1.28.

14. Να αποδείξετε πλήρως την Πρόταση A.1.30.

15. Να αποδείξετε τους ισχυρισμούς $(*)$ και $(**)$ στην σελίδα 337.

16. Να αποδείξετε πλήρως την Πρόταση A.1.33.

17. Δείξτε ότι για τους αριθμούς Fibonacci ισχύει:

i. $F_n \leq 2^{n-1}$.
ii. $F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}$.
iii. $F_2 + F_4 + F_6 + \cdots + F_{2n} = F_{2n+1} - 1$.
iv. $F_{n+k} = F_k F_{n+1} + F_{k-1} F_n$, για όλα τα $n, k \in \mathbb{N}$ με $k \geq 2$.
v. $\phi^n = F_n\phi + F_{n-1}$ και $\bar{\phi}^n = F_n\bar{\phi} + F_{n-1}$.

18. Να αποδείξετε πλήρως το Θεώρημα A.1.34.

19. Δείξτε ότι για τους αριθμούς Lucas ισχύει ότι

i. $L_1 + L_3 + L_5 + \cdots + L_{2n-1} = L_{2n} - 2$.
ii. $L_2 + L_4 + L_6 + \cdots + L_{2n} = L_{2n+1} - 1$.

20. Να αποδείξετε πλήρως την Πρόταση A.1.35.

21. Έστω A ένα (μη κενό) σύνολο, $a, b \in A$ και $\pi : A \times A \longrightarrow A$ μια απεικόνιση. Υπάρχει μοναδική απεικόνιση $f : \mathbb{N} \longrightarrow A$, ούτως ώστε

$$f(1) = a,\ f(2) = b \text{ και}$$
$$f(n+2) = \pi(\,(f(n), f(n+1))\,),$$

για όλα τα $n \in \mathbb{N}$.

Σχόλιο: Η άσκηση αυτή στην πραγματικότητα είναι ένα άλλο θεώρημα (πέραν των Θεωρημάτων A.1.19 καιA.1.27), το οποίο αποδεικνύεται *παρομοίως*, η απόδειξή του όμως είναι πέραν των σκοπών του παρόντος.

Βιβλιογραφία

[1] E.D. Bloch. *Proofs and Fundamentals: A first course in Abstract Mathematics*. Second Edition, Springer, 2011. ISBN: 978-14-4197-126-5.

[2] Γιάννης Ν. Μοσχοβάκης. *Σημειώσεις στη Συνολοθεωρία*. Προκαταρκτική 2η έκδοση. http://www.math.ucla.edu/~ynm/lectures/g.pdf, 2014.

[3] P. Halmos. *Naive Set Theory*. Springer, 1974. ISBN: 978-0-387-90104-6.

[4] T. Jech. *Set Theory*. Springer, 2003. ISBN: 978-3540440857.

[5] Steven G. Krantz. *The Elements of Advanced Mathematics*. Fourth Edition. Textbooks in mathematics. CRC Press Taylor and Francis Group, 2018. ISBN: 978-11-3850-631-2.

[6] Αντώνης Τσολομύτης. *Σύνολα και αριθμοί*. Leader Books, 2004. ISBN: 978-96-0790-147-7.

ΠΑΡΑΡΤΗΜΑ Β

Η ΠΛΗΘΙΚΟΤΗΤΑ ΤΩΝ ΣΥΝΟΛΩΝ

Στο πρώτο κεφάλαιο είχαμε ασχοληθεί με την έννοια του συνόλου, αλλά δεν είχαμε αναφερθεί (συστηματικά/αυστηρά) στο "*μέγεθος*" ενός συνόλου. Επίσης, στο τρίτο κεφάλαιο είχαμε ασχοληθεί με τις σχέσεις μεταξύ συνόλων, όπου είχαμε μελετήσει τις απεικονίσεις μεταξύ συνόλων και είχαμε αναφέρει συνθήκες για το πότε μια απεικόνιση είναι 1-1, επί ή 1-1 και επί. Πάλι όμως δεν είχαμε αναφερθεί στο μέγεθος των συνόλων, πολύ δε περισσότερο δεν είχαμε αναφερθεί στην σύγκριση των μεγεθών δύο συνόλων.

Διαισθητικά όμως έχουμε την έννοια του πεπερασμένου συνόλου και του συνόλου με άπειρο το πλήθος στοιχεία. Μάλιστα δε χρησιμοποιούμε αυτές τις έννοιες στην καθημερινότητά μας χωρίς(;) ιδιαίτερα προβλήματα. Αν όμως θελήσουμε να εντρυφήσουμε περισσότερο, θα δούμε ότι εγείρονται προβλήματα, για τα οποία η διαίσθησή μας δεν αρκεί για να τα αντιμετωπίσουμε.

Για παράδειγμα, όταν έχουμε δύο πεπερασμένα σύνολα (ακόμη δεν έχουμε ορίσει αυστηρά την έννοια του πεπερασμένου συνόλου), τότε μπορούμε να απαριθμήσουμε τα στοιχεία του κάθε συνόλου και να αποφανθούμε για το μέγεθός τους. Τι γίνεται όμως αν έχουμε σύνολα με άπειρο το πλήθος στοιχεία; Υπάρχουν σύνολα με άπειρο το πλήθος στοιχεία, τα οποία δεν είναι "ισομεγέθη";

Για αρκετούς αιώνες υπήρχε η αίσθηση ότι όλα τα σύνολα με άπειρο το πλήθος στοιχεία είναι ισομεγέθη.

Πρώτος ο Cantor (ο θεμελιωτής της σύγχρονης θεωρίας συνόλων) επισήμανε την διαφορά μεταξύ των εννοιών "πλήθος" των στοιχείων ενός συνόλου και "μέγεθος" ενός συνόλου[1].

Πριν προχωρήσουμε, ας δούμε ένα κλασικό(;) παράδειγμα.

Υποθέτουμε ότι έχουμε ένα σύνολο με σφαιρίδια και ένα σύνολο, του οποίου τα

[1] Όπως προείπαμε, και θα δούμε συστηματικά στα επόμενα, οι δύο έννοιες ταυτίζονται στην περίπτωση των πεπερασμένων συνόλων.

στοιχεία είναι κουτιά. Θέλουμε να τοποθετήσουμε σε κάθε κουτί μόνο ένα σφαιρίδιο. Το ερώτημα που τίθεται είναι το εξής: Θα γεμίσουν τα κουτιά και θα περισσέψουν σφαιρίδια, θα χωρέσουν όλα τα σφαιρίδια και θα παραμείνουν άδεια κουτιά ή θα γεμίσουν όλα τα κουτιά και δεν θα περισσέψουν σφαιρίδια;

Η απάντηση, θα έλεγε κάποιος, είναι προφανής. Μετρούμε τον αριθμό των σφαιριδίων και τον αριθμό των κουτιών και αμέσως αποφαινόμαστε, συγκρίνοντας τους δύο (πληθικούς) αριθμούς, ποιο από τα τρία ενδεχόμενα ισχύει (προφανώς δεν μπορούν να ισχύουν ταυτόχρονα δύο ενδεχόμενα).

Ας δούμε, όμως μια άλλη προσέγγιση του προβλήματος **χωρίς** να μετρήσουμε τα στοιχεία των δύο συνόλων.

Λαμβάνουμε τα δύο σύνολα, τα τοποθετούμε δίπλα-δίπλα και αρχίζουμε να τοποθετούμε ένα-ένα τα σφαιρίδια σε αντίστοιχα κουτιά, μέχρι να εξαντληθούν τα στοιχεία ενός από τα δύο σύνολα. Ανάλογα με του ποιου συνόλου τα στοιχεία θα εξαντληθούν πρώτα έχουμε και την απάντηση.

Η δεύτερη προσέγγιση, αν και πιο επίπονη, έχει ένα μεγάλο πλεονέκτημα. Μπορεί να εφαρμοστεί και σε σύνολα με άπειρο το πλήθος στοιχεία. Όπου εδώ εμφανίζεται, όπως προείπαμε, η διαφορά μεταξύ του πλήθους στοιχείων ενός συνόλου και του μεγέθους ενός συνόλου. Πώς επιτυγχάνεται αυτό; Μα φυσικά επικαλούμενοι την έννοια της απεικόνισης.

Μετά από αυτά, ας γίνουμε πιο συστηματικοί.

Ορισμός Β.0.1. Έστω A, B δύο σύνολα. Τα A και B θα ονομάζονται **ισοπληθικά** ή ότι έχουν την ίδια πληθικότητα, αν υπάρχει μια απεικόνιση $f : A \longrightarrow B$, η οποία να είναι 1-1 και επί. Δύο ισοπληθικά σύνολα θα συμβολίζονται ως

$$A \sim B \text{ [2]}.$$

Όπως βλέπουμε, ο ανωτέρω ορισμός αναφέρεται στην *σύγκριση* δύο συνόλων και δεν αναφέρεται στην πληθικότητα κάθε ενός συνόλου ξεχωριστά.

Πρόταση Β.0.2. *Έστω A, B, C τρία σύνολα, τότε ισχύουν τα εξής:*

i. $A \sim A$.

ii. *Αν* $A \sim B$, *τότε* $B \sim A$.

iii. *Αν* $A \sim B$ *και* $B \sim C$, *τότε* $A \sim C$.

Απόδειξη. Η απόδειξη αποτελεί απλή εφαρμογή του ορισμού και των ιδιοτήτων των απεικονίσεων (ιδέ το Θεώρημα 4.5.32) και αφήνεται ως άσκηση. ό.έ.δ.

Σχόλιο Β.0.3. Παρατηρούμε ότι η ανωτέρω σχέση μας θυμίζει την σχέση ισοδυναμίας, η οποία ορίζεται σε ένα σύνολο. Πρέπει να είμαστε προσεκτικοί. Η σχέση $\sim$ εδώ δεν είναι σχέση ισοδυναμίας, διότι θα πρέπει να αναφερθούμε στο *σύνολο όλων των συνόλων*, κάτι, που όπως έχουμε αναφέρει στο πρώτο κεφάλαιο, οδηγεί σε παράδοξα.

Παρ' όλα ταύτα, έχει επικρατήσει δύο ισοπληθικά σύνολα να αναφέρονται και ως **ισοδύναμα** σύνολα.

Πριν προχωρήσουμε, ας δούμε μερικά παραδείγματα.

[2] Γνώμη μας είναι ότι πιο δόκιμο θα ήταν να ονομάζονται **ισομεγέθη**, δεδομένου ότι υπάρχουν σύνολα, τα οποία έχουν άπειρο το πλήθος στοιχεία, αλλά δεν είναι ισοπληθικά. Διατηρούμε την καθιερωμένη ορολογία, καθ' ότι στην συνέχεια θα δούμε ότι υπάρχουν πολλών ειδών *άπειρα*.

Παραδείγματα Β.0.4.

1. Το σύνολο των φυσικών αριθμών είναι ισοπληθικό με το σύνολο των ακεραίων αριθμών.

   Πράγματι, αν θεωρήσουμε την απεικόνιση $\phi : \mathbb{N} \longrightarrow \mathbb{Z}$ με

   $$\phi(n) = \begin{cases} \dfrac{n}{2} & \text{αν n είναι άρτιος} \\ -\dfrac{n-1}{2} & \text{αν n είναι περιττός} \end{cases}$$

   τότε είναι εύκολο να διαπιστώσουμε (κάντε το!) ότι η απεικόνιση ϕ είναι 1-1 και επί.

   Στην παράγραφο 4.5.2, όπου μιλούσαμε για τις απεικονίσεις, είχαμε δει την Άσκηση $4.5.3_6$

   "Δείξτε ότι η απεικόνιση $f : \mathbb{N} \longrightarrow \mathbb{Z}$ με

   $$f(n) = \frac{(-1)^n(2n-1)+1}{4}$$

   είναι 1-1 και επί."

   Δηλαδή από τότε είχαμε αποδείξει ότι τα δύο σύνολα $\mathbb{N}$ και $\mathbb{Z}$ είναι ισοπληθικά, μόνο που τότε δεν είχαμε τον σχετικό ορισμό.

2. Έστω $a, b, c, d \in \mathbb{R}$ με $a < b$ και $c < d$, Θα δείξουμε ότι τα κλειστά διαστήματα $[a, b]$ και $[c, d]$ είναι ισοπληθικά.

   Ορίζουμε την απεικόνιση $f : [a, b] \longrightarrow [c, d]$ ως εξής:

   $$f(x) = \frac{d-c}{b-a} \cdot (x-a) + c.$$

   Είναι πολύ εύκολο να ελέγξουμε (κάντε το!) ότι η απεικόνιση f είναι 1-1 και επί.

   Προσαρμόζοντας κατάλληλα τα ίδια επιχειρήματα είναι εύκολο να διαπιστώσουμε ότι τα ανοικτά διαστήματα (a, b) και (c, d) είναι ισοπληθικά. Επίσης, τα ημιάνοικτα διαστήματα $[a, b)$ και $[c, d)$ είναι ισοπληθικά.

3. Το σύνολο $\mathbb{R}$ των πραγματικών αριθμών είναι ισοπληθικό με το ανοικτό διάστημα $(-1, 1)$.

   Είναι εύκολο να δούμε ότι η απεικόνιση $f : \mathbb{R} \longrightarrow (-1, 1)$ με

   $$f(x) = \begin{cases} \dfrac{x^2}{x^2+1} & \text{αν x≥0} \\ \dfrac{-x^2}{x^2+1} & \text{αν x} < 0 \end{cases}$$

   είναι 1-1 και επί.

   Είναι η Άσκηση $4.5.3_7$. Αν δεν είχατε απαντήσει τότε, απαντήστε τώρα.

   Παρατηρήστε ότι η ανωτέρω απεικόνιση απεικονίζει κάθε ρητό αριθμό σε ρητό αριθμό και κάθε άρρητο αριθμό σε άρρητο αριθμό.

Συνδυάζοντας τα δύο τελευταία παραδείγματα έχουμε ότι:

Το σύνολο των πραγματικών αριθμών είναι ισοπληθικό με το ανοικτό διάστημα (a, b), για κάθε $a, b \in \mathbb{R}$ με $a < b$.

Στα προηγούμενα παραδείγματα βλέπουμε ότι υπάρχουν σύνολα, τα οποία είναι ισοπληθικά με γνήσια υποσύνολά τους, κάτι που έρχεται σε αντίθεση με την αίσθησή μας ότι ένα γνήσιο υποσύνολο ενός συνόλου πρέπει να περιέχει *λιγότερα* στοιχεία.

Στο σημείο αυτό ας λεπτολογήσουμε περισσότερο στο πρώτο παράδειγμα.

Ως συνήθως παριστάνουμε τους ακεραίους (κατ' αύξουσα σειρά) ως εξής:

$$\dots, -2, -1, 0, 1, 2, \dots,$$

όπου δεν υπάρχει "αρχικός ακέραιος". Η απεικόνιση $\phi : \mathbb{N} \longrightarrow \mathbb{Z}$ με

$$\phi(n) = \begin{cases} \dfrac{n}{2} & \text{αν n είναι άρτιος} \\ -\dfrac{n-1}{2} & \text{αν n είναι περιττός} \end{cases}$$

"αναδιατάσει" τους ακεραίους (όχι κατ' αύξουσα σειρά) ως εξής:

$$0, 1, -1, 2, -2, \dots,$$

όπου έχουμε πλέον "αρχικό στοιχείο".

Από τα προηγούμενα προκύπτει ότι είναι αναγκαίο να προβούμε σε μια (αυστηρή) διάκριση μεταξύ της έννοιας του πεπερασμένου συνόλου και του απείρου συνόλου, καθώς και μια γενικότερη θεώρηση για την σημασία της πληθικότητας του συνόλου των φυσικών αριθμών στην μελέτη της πληθικότητας άλλων συνόλων.

Για κάθε φυσικό αριθμό n έστω

$$N_n = \{k \in \mathbb{N} \mid 1 \leq k \leq n\} = \{1, 2, \cdots, n\}.$$

Ορισμός Β.0.5.

i. Ένα σύνολο θα ονομάζεται **πεπερασμένο**, αν είναι είτε το κενό σύνολο ή είναι ισοπληθικό με ένα N_n, για κάποιο $n \in \mathbb{N}$.

ii. Ένα σύνολο θα ονομάζεται **άπειρο**, αν δεν είναι πεπερασμένο.

iii. Ένα σύνολο θα ονομάζεται **απείρως αριθμήσιμο**, αν είναι ισοπληθικό με το σύνολο των φυσικών αριθμών.

iv. Ένα σύνολο θα ονομάζεται **αριθμήσιμο**, αν είναι πεπερασμένο ή απείρως αριθμήσιμο.

v. Ένα σύνολο θα ονομάζεται **υπεραριθμήσιμο**, αν δεν είναι αριθμήσιμο.

Προφανώς, υπάρχουν πεπερασμένα, απείρως αριθμήσιμα και αριθμήσιμα σύνολα. Άρα στον προηγούμενο ορισμό, τα i., iii. και iv. δεν είναι κενού περιεχομένου.

Για τα ii. και v. δεν είναι προφανές ότι δεν είναι κενού περιεχομένου.

Η διαίσθησή μας λέει ότι το σύνολο των φυσικών αριθμών είναι άπειρο (δεν είναι πεπερασμένο), αλλά χρήζει αποδείξεως.

Πρόταση Β.0.6. *Το σύνολο* $\mathbb{N}$ *είναι άπειρο.*

Υπάρχουν πολλές αποδείξεις γι' αυτό το, φαινομενικά, προφανές αποτέλεσμα.

Αναβάλλουμε προς το παρόν την απόδειξη για να εστιαστούμε πρώτα στα πεπερασμένα σύνολα, και μετά θα επανέλθουμε (ιδέ σελίδα 358).

Β.1 Πεπερασμένα σύνολα

Ορισμός Β.1.1. Έστω A ένα πεπερασμένο σύνολο. Στο σύνολο A προσάπτουμε έναν μη αρνητικό ακέραιο αριθμό, τον οποίο θα ονομάζουμε **πληθικό αριθμό** και θα τον συμβολίζουμε ως $|A|$ ή ως $card(A)$ [3].

Συγκεκριμένα: Αν $A = \emptyset$, ορίζουμε $|A| = 0$.

Αν $A \neq \emptyset$, τότε, εξ ορισμού, υπάρχει ένας φυσικός αριθμός n, ώστε $A \sim N_n$. Στην περίπτωση αυτή ορίζουμε $|A| = n$.

Αν παρατηρήσουμε τον προηγούμενο Ορισμό, θα δούμε ότι δεν μας εξασφαλίζει ότι σε ένα πεπερασμένο μη κενό σύνολο μπορούμε να προσάψουμε έναν μοναδικό πληθικό αριθμό. Πράγματι, στον ορισμό του πεπερασμένου συνόλου (Ορισμός Β.0.1) κανείς δεν μας εξασφαλίζει ότι ένα σύνολο είναι ισοπληθικό με ένα N_n, για μοναδικό $n \in \mathbb{N}$.

Δηλαδή ενδέχεται να έχουμε $N_n \sim N_m$ για δύο διαφορετικούς φυσικούς αριθμούς n και m.

Αυτό "μεταφράζεται" στο ότι ενδέχεται να υπάρχει απεικόνιση $f : N_n \longrightarrow N_m$, η οποία να είναι 1-1 και επί, ενώ $n \neq m$.

Διαισθητικά "φαντάζει" προφανές ότι δεν είναι δυνατόν να ισχύει. Συγκεκριμένα ισχύει η πρόταση.

Πρόταση Β.1.2. *Έστω $n, m \in \mathbb{N}$. Τότε ισχύει*

$$N_m \sim N_n \text{ αν και μόνο αν } n = m.$$

Ο ισχυρισμός της πρότασης δεν είναι προφανής και χρήζει αποδείξεως[4].

Σκοπός μας είναι να εξασφαλίσουμε ότι η έννοια του πληθικού αριθμού ενός πεπερασμένου συνόλου είναι καλά ορισμένη και συμβαδίζει με την διαίσθησή μας.

Επίσης, μέσω αυτής της αποδεικτικής διαδικασίας θα αναδειχθεί η (Μαθηματική) διαφοροποίηση μεταξύ πεπερασμένων και απείρων συνόλων.

Πρόταση Β.1.3. *Έστω A, B δύο ισοδύναμα (μη κενά) σύνολα. Υποθέτουμε ότι το σύνολο A είναι πεπερασμένο, τότε και το σύνολο B είναι πεπερασμένο, μάλιστα δε μπορούμε να του προσάψουμε τον ίδιο πληθικό αριθμό.*

Απόδειξη. Αφού το σύνολο A είναι πεπερασμένο, εξ ορισμού, υπάρχει ένα $n \in \mathbb{N}$, ώστε $A \sim N_n$. Από την Πρόταση Β.0.2 έχουμε ότι $B \sim N_n$. Οπότε, από τον Ορισμό Β.0.5, έπεται ότι το σύνολο B είναι πεπερασμένο και από τον Ορισμό Β.1.1 έπεται ότι και στο σύνολο B μπορούμε να προσάψουμε τον ίδιο πληθικό αριθμό με τον πληθικό αριθμό, που προσάψαμε στο σύνολο A. ό.έ.δ.

Προσοχή! Στην διατύπωση της προηγουμένης πρότασης. Δεν λέμε ότι τα δύο σύνολα έχουν τον ίδιο πληθικό αριθμό, αλλά ότι μπορούμε να τους προσάψουμε τον ίδιο πληθικό αριθμό, δεδομένου ότι δεν έχουμε εξασφαλίσει ότι σε ένα πεπερασμένο σύνολο μπορούμε να του προσάψουμε μοναδικό πληθικό αριθμό Άλλωστε αυτός είναι ο σκοπός μας (ιδέ Πρόταση Β.1.2, της οποίας η απόδειξη εκκρεμεί).

---

[3] Τον συμβολισμό $|A|$, συνήθως, τον χρησιμοποιούμε για πεπερασμένα σύνολα, ενώ τον συμβολισμό $card(A)$ τον χρησιμοποιούμε για άπειρα σύνολα.

[4] Ερώτημα: Πόσοι από τους *χρισμένους* Μαθηματικούς έχουν συνειδητοποιήσει ότι η πρόταση αυτή χρήζει αποδείξεως; Δεν μιλάμε, για το πώς αποδεικνύεται.

Πρόταση Β.1.4. *Έστω n ένας φυσικός αριθμός και A ένα σύνολο. Υποθέτουμε ότι $A \subseteq N_n$. Τότε το σύνολο A είναι πεπερασμένο. Μάλιστα δε υπάρχει μια απεικόνιση $g : N_n \longrightarrow \mathbb{N}_n$, η οποία είναι 1-1 και επί, με την ιδιότητα $g(A) = N_r$ και $r \leq n$. Στην περίπτωση δε όπου το σύνολο A είναι γνήσιο υποσύνολο του N_n, ισχύει ότι $r < n$.*

Απόδειξη. Για την απόδειξη θα εφαρμόσουμε την αρχή της Μαθηματικής επαγωγής.

Αν $n = 1$ και $A \subseteq N_1 = \{1\}$, τότε $A = \emptyset$ ή $A = \{1\}$ και ο ισχυρισμός ισχύει κατά προφανή τρόπο.

Έστω ένα $n \in \mathbb{N}$. Υποθέτουμε ότι ο ισχυρισμός ισχύει για όλα τα υποσύνολα $B \subseteq N_n$. Θα δείξουμε ότι ο ισχυρισμός ισχύει για όλα τα υποσύνολα $A \subseteq N_{n+1}$.

Έστω ένα $A \subseteq N_{n+1}$. Διακρίνουμε δύο περιπτώσεις:

i. $A \subseteq N_n$. Τότε, από την υπόθεση της επαγωγής, υπάρχει μια απεικόνιση

$$g : N_n \longrightarrow N_n,$$

η οποία είναι 1-1 και επί, με την ιδιότητα $g(A) = N_r$ και $r \leq n$. Στην περίπτωση αυτή επεκτείνουμε την g στην απεικόνιση $\hat{g} : N_{n+1} \longrightarrow N_{n+1}$ ορίζοντας

$$\hat{g}(x) = g(x), \text{ αν } x \in N_n \text{ και } \hat{g}(n+1) = n+1.$$

Προφανώς (γιατί;) η απεικόνιση $\hat{g}$ πληροί όλες τις προϋποθέσεις του ισχυρισμού για τον φυσικό αριθμό $n+1$ και απεδείχθη το επαγωγικό βήμα στην περίπτωση αυτή. Μάλιστα δε, στην περίπτωση αυτή το σύνολο A είναι γνήσιο υποσύνολο του N_{n+1} και προφανώς $r < n+1$.

ii. $A \nsubseteq N_n$.

Στην περίπτωση αυτή $n+1 \in A$ και $A = \mathrm{B} \cup \{n+1\}$, όπου $B = A \setminus \{n+1\}$ (γιατί;). Τότε όμως θα έχουμε $B \subseteq N_n$ και από την υπόθεση της επαγωγής έχουμε ότι υπάρχει μια απεικόνιση $g : N_n \longrightarrow \mathrm{N}_n$, η οποία είναι 1-1 και επί, με $g(B) = N_r$ και $r \leq n$.

Διακρίνουμε δύο υποπεριπτώσεις:

α. Αν $r = n$, τότε επεκτείνουμε την απεικόνιση g στην απεικόνιση

$$\hat{g} : N_{n+1} \longrightarrow N_{n+1}$$

με

$$\hat{g}(x) = g(x), \text{ αν } x \in N_n \text{ και } \hat{g}(n+1) = n+1.$$

Προφανώς η απεικόνιση $\hat{g}$ είναι 1-1 και επί (γιατί;). Οπότε

$$\hat{g}(A) = \hat{g}(\mathrm{B} \cup \{n+1\}) = \hat{g}(\mathrm{B}) \cup \hat{g}(\{n+1\}) = N_n \cup \{n+1\} = N_{n+1}.$$

Επομένως, απεδείχθη το επαγωγικό βήμα στην περίπτωση αυτή και ο ισχυρισμός ισχύει.

β. Αν $r < n$, τότε $r+1 \leq n$ και επεκτείνουμε την απεικόνιση g στην απεικόνιση

$$\hat{g} : N_{n+1} \longrightarrow N_{n+1}$$

με

$$\begin{aligned}\hat{g}(n+1) &= r+1,\\ \hat{g}(r+1) &= n+1 \text{ και}\\ \hat{g}(x) &= g(x), \text{ αν } x \in N_n \text{ και } x \neq r+1.\end{aligned}$$

Και στην περίπτωση αυτή, η απεικόνιση $\hat{g}$ είναι 1-1, επί και ισχύει

$$\hat{g}(A) \subseteq N_{r+1} \text{ με } r+1 \leq n+1 \text{ (γιατί;).}$$

Επομένως, απεδείχθη το επαγωγικό βήμα και στην περίπτωση αυτή και ο ισχυρισμός ισχύει.

Οπότε, ο ισχυρισμός ισχύει σε όλες τις περιπτώσεις και η απόδειξη ολοκληρώθηκε. ό.έ.δ.

Τώρα είμαστε σε θέση να αποδείξουμε την Πρόταση B.1.2.

Απόδειξη. Προφανώς, αν $n = m$ τότε $N_n \sim N_m$.

Αντίστροφα, υποθέτουμε ότι $N_m \sim N_n$. Θα δείξουμε ότι $n = m$.

Εφόσον $N_m \sim N_n$, εξ' ορισμού, υπάρχει μια απεικόνιση $f : N_m \longrightarrow N_n$, η οποία είναι 1-1 και επί.

Θα εφαρμόσουμε επαγωγή επί του n (προσοχή! το n αφορά, το πεδίον τιμών της απεικόνισης).

Αν $n = 1$, τότε θα έχουμε την απεικόνιση $f : N_m \longrightarrow N_1 = \{1\}$, (με το m, προς το παρόν, τυχαίο), η οποία είναι 1-1 και επί. Στην περίπτωση αυτή αναγκαστικά (γιατί;) $m = 1$ και ο ισχυρισμός ισχύει για $n = 1$.

Υποθέτουμε ότι ο ισχυρισμός ισχύει για ένα $n \in \mathbb{N}$. Έστω $f : \mathbb{N}_m \longrightarrow N_{n+1}$ μια απεικόνιση, η οποία είναι 1-1 και επί, θα δείξουμε ότι $m = n+1$.

Επειδή $n+1 > 1$, έπεται ότι το $m > 1$ (γιατί;). Επομένως, υπάρχει (μοναδικό) $k \in \mathbb{N}$, ώστε $m = k+1$ (γιατί; μα ισχύει το αξίωμα του Peano).

Τότε προφανώς(;)

$$N_m = N_k \cup \{k+1\}$$

Διακρίνουμε δύο περιπτώσεις:

i. $f(k+1) = n+1$.

   Αν πάρουμε τον περιορισμό $\bar{f}$ της f επί του (υπο)συνόλου N_k, προφανώς η $\bar{f} : N_k \longrightarrow N_n$ είναι 1-1 και επί. Οπότε, από την επαγωγική υπόθεση έχουμε ότι $k = n$ και συνεπώς $m = k+1 = n+1$. Άρα απεδείχθη το επαγωγικό βήμα στην περίπτωση αυτή και ο ισχυρισμός ισχύει.

ii. $f(k+1) = s$ με $s < n+1$. Στην περίπτωση αυτή θα κατασκευάσουμε μια άλλη (βοηθητική) απεικόνιση, η οποία θα είναι 1-1 και επί.

   Ορίζουμε $\hat{f} : N_{k+1} \longrightarrow N_{n+1}$ ως εξής:

$$\hat{f}(s) = f(k+1),\ \hat{f}(k+1) = n+1,\ \hat{f}(x) = f(x),$$

   για όλα τα υπόλοιπα $x \in N_{k+1} \setminus \{s, m\}$.

   Επειδή η f είναι 1-1 και επί είναι εύκολο (;) να δούμε ότι και η $\hat{f}$ είναι 1-1 και επί.

Αν πάρουμε τον περιορισμό της $\hat{f}$ επί του (υπο)συνόλου N_k, παρατηρούμε ότι

$$\hat{f}(N_k) = N_n.$$

Άρα αναγόμαστε στην πρώτη περίπτωση, απ' όπου συμπεραίνουμε ότι $k = n$ και συνεπώς $m = k+1 = n+1$. Επομένως, απεδείχθη το επαγωγικό βήμα και στην περίπτωση αυτή και ο ισχυρισμός ισχύει.

Συνεπώς, η απόδειξη ολοκληρώθηκε. ό.έ.δ.

Μετά την απόδειξη της πρότασης αυτής, βλέπουμε ότι ο πληθικός αριθμός ενός πεπερασμένου συνόλου είναι μοναδικός και επομένως ο Ορισμός B.1.1 είναι "καλός".

Πόρισμα B.1.5.

i. Έστω A ένα μη κενό πεπερασμένο σύνολο και $x \notin A$. Τότε το σύνολο

$$B = A \cup \{x\}$$

είναι πεπερασμένο και $|B| = |A| + 1$.

ii. Έστω A ένα πεπερασμένο σύνολο και $x \in A$. Τότε το σύνολο

$$B = A \setminus \{x\}$$

είναι πεπερασμένο και $|B| = |A| - 1$.

Απόδειξη.

i. Επειδή το σύνολο A είναι πεπερασμένο, υπάρχει (μοναδικός) $n \in \mathbb{N}$, ώστε $A \sim N_n$, άρα υπάρχει απεικόνιση $f : A \longrightarrow N_n$, η οποία είναι 1-1 και επί.

Ορίζουμε την *απεικόνιση*

$$\hat{f} : B = A \cup \{x\} \longrightarrow N_{n+1} = N_n \cup \{n+1\}$$

με

$$\hat{f}(a) = f(a), \text{ για όλα τα } a \in A \text{ και } \hat{f}(x) = n+1.$$

Είναι εύκολο και αφήνεται ως άσκηση (Άσκηση B.2.4$_2$) να δούμε ότι η $\hat{f}$ είναι πράγματι απεικόνιση και μάλιστα 1-1 και επί.

ii. Η απόδειξη μπορεί να γίνει απ' ευθείας. Αλλά μπορεί να στηριχθεί στο i. θέτοντας

$$A = (A \setminus \{x\}) \cup \{x\}.$$

Σε κάθε περίπτωση αφήνεται ως άσκηση. ό.έ.δ.

Πόρισμα B.1.6. *Έστω S ένα πεπερασμένο σύνολο και $A \subseteq S$. Το σύνολο A είναι πεπερασμένο και $|A| \leq |S|$.*

Απόδειξη. Η απόδειξη είναι προφανής και αφήνεται ως άσκηση (Άσκηση B.2.4$_3$). ό.έ.δ.

Πόρισμα B.1.7. *Η τομή πεπερασμένων συνόλων είναι πεπερασμένο σύνολο.*

Πόρισμα Β.1.8. *Ένα πεπερασμένο σύνολο δεν είναι ισοπληθικό με κάθε ένα από τα γνήσια υποσύνολά του.*

Απόδειξη. Έστω B ένα σύνολο και A ένα γνήσιο υποσύνολό του. Τότε υπάρχει ένα $x \in B$ με $x \notin A$. Επομένως $A \subseteq (B \setminus \{x\})$. Από το Πόρισμα Β.1.6 έχουμε ότι

$$|A| \leq |B \setminus \{x\}| = |B| - 1.$$

Άρα, από την Πρόταση Β.1.3, έχουμε ότι $A \nsim B$. ό.έ.δ.

Το τελευταίο πόρισμα είναι μια πρώτη "ένδειξη" της σημαντικής διαφοράς μεταξύ πεπερασμένων και απείρων συνόλων. Συγκρίνατε με τα Παραδείγματα Β.0.4.

Πρόταση Β.1.9. *Έστω A, B δύο πεπερασμένα σύνολα.*

i. Αν τα A και B είναι ξένα μεταξύ τους, τότε η ένωση $A \cup B$ είναι πεπερασμένο σύνολο. Μάλιστα δε ισχύει ότι $|A \cup B| = |A| + |B|$.

ii. Αν $C \subseteq A$, τότε ισχύει $|A| = |C| + |A \setminus C|$.

iii. Γενικά ισχύει ότι $|A \cup B| = |A| + |B| - |A \cap B|$.

Απόδειξη.

i. Αν τουλάχιστον ένα από τα δύο σύνολα είναι το κενό σύνολο, τότε το συμπέρασμα είναι προφανές. Επομένως, υποθέτουμε ότι και τα δύο σύνολα είναι μη κενά.

   Θα εφαρμόσουμε την αρχή της Μαθηματικής επαγωγής επί του πληθικού αριθμού του συνόλου B.

   Αν το σύνολο B είναι μονοσύνολο, τότε το συμπέρασμα έπεται από το Πόρισμα Β.1.5, οποιοσδήποτε και να είναι ο πληθικός αριθμός του συνόλου A.

   Υποθέτουμε ότι το συμπέρασμα ισχύει για κάθε σύνολο B με $|B| = n$, ξένο προς το σύνολο A και για οποιονδήποτε πληθικό αριθμό και αν έχει το σύνολο A. Δηλαδή ισχύει ότι $|A \cup B| = |A| + |B|$.

   Έστω B ένα σύνολο, ξένο προς το σύνολο A, με $|B| = n+1$ και $x \in B$. Τότε το σύνολο $\Gamma = B \setminus \{x\}$ έχει πληθικό αριθμό

   $$|\Gamma| = |B| - 1 = (n+1) - 1 = n$$

   και είναι ξένο προς το σύνολο A.

   Το σύνολο $A \cup \Gamma$, από την υπόθεση της επαγωγής, έχει πληθικό αριθμό

   $$|A \cup \Gamma| = |A| + |\Gamma|.$$

   Προφανώς $A \cup B = (A \cup \Gamma) \cup \{x\}$ και

   $$|A \cup B| = |A \cup \Gamma| + 1 = |A| + |\Gamma| + 1 = |A| + n + 1 = |A| + |B|.$$

   Συνεπώς, η απόδειξη ολοκληρώθηκε.

ii. Προφανώς $C \cap (A \setminus C) = \emptyset$, οπότε ο ισχυρισμός ισχύει, βάσει του i..

iii. Η απόδειξη είναι συνδυασμός των i. και ii..

Συγκεκριμένα, επειδή $B \subseteq A \cup B$, έχουμε ότι

$$|A \cup B| = |(A \cup B) \setminus B| + |B|.$$

Επίσης, επειδή $A \cap B \subseteq A$, έχουμε ότι

$$|A| = |(A \cap B)| + |A \setminus (A \cap B)|.$$

Αλλά ισχύει ότι

$$(A \cup B) \setminus B = A \setminus (A \cap B)$$

(γιατί; ιδέ Άσκηση 1.1.3$_{5_\alpha}$). Επομένως, η πρώτη ισότητα γίνεται

$$|A \cup B| = |(A \cup B) \setminus B| + |B| = |A \setminus (A \cap B)| + |B| = |A| - |(A \cap B)| + |B|.$$

Συνεπώς, η απόδειξη ολοκληρώθηκε. ό.έ.δ.

Σχόλιο Β.1.10. Η ανωτέρω πρόταση αναφέρεται ως **Ο νόμος της πρόσθεσης** στα (πεπερασμένα) σύνολα (ή προσθετική αρχή). Μάλιστα δε, επειδή διαισθητικά είναι κάτι το προφανές[5], θεωρείται ότι *αυταπόδεικτα* ισχύει. Όπως βλέπουμε, μπορεί (και πρέπει) να αποδειχθεί.

Μπορούμε να γενικεύσουμε την προηγουμένη πρόταση ως εξής:

Πρόταση Β.1.11. *Έστω A, B, C τρία πεπερασμένα σύνολα, τότε ισχύει ότι:*

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Απόδειξη. Η απόδειξη αποτελεί εφαρμογή της προηγουμένης πρότασης, δεδομένου ότι

$$A \cup B \cup C = (A \cup B) \cup C$$

και αφήνεται ως άσκηση ό.έ.δ.

Παράδειγμα Β.1.12. Να βρεθεί το πλήθος των φυσικών αριθμών των μικροτέρων ή ίσων του 20, οι οποίοι δεν διαιρούνται από το 3 ή το 5 ή το 13. Δηλαδή να βρεθεί ο πληθικός αριθμός του συνόλου

$$X = \{n \in \mathbb{N} \mid 1 \leq n \leq 20 \text{ και } n \text{ δεν είναι διαιρετός με το 3 ή το 5 ή το 13}\}.$$

Η απάντηση είναι απλή αρκεί να παρατηρήσουμε ότι

$$X = \{1, 2, 4, 7, 8, 11, 13, 16, 17, 19\}.$$

Αν θέσουμε όμως το ίδιο πρόβλημα για φυσικούς αριθμούς μεταξύ του 1 και του 1.000.000, τότε ένας έλεγχος για κάθε έναν αριθμό είναι ατελέσφορος. Θα εφαρμόσουμε την προηγουμένη πρόταση.

Έστω

$$\begin{aligned} X &= \{n \in \mathbb{N} \mid 1 \leq n \leq 1.000.000 \text{ και } n \text{ δεν είναι διαιρετός με το 3 ή το 5, ή το 13}\},\\ B_3 &= \{n \in X \mid n \text{ είναι διαιρετός με το 3}\},\\ B_5 &= \{n \in X \mid n \text{ είναι διαιρετός με το 5}\},\\ B_{13} &= \{n \in X \mid n \text{ είναι διαιρετός με το 13}\}. \end{aligned}$$

[5] Μια διαισθητική "απόδειξη" είναι άμεση παρατηρώντας το διάγραμμα του Venn της τομής δύο συνόλων, ιδέ Παράγραφο 1.1.4.1.

Επειδή σε κάθε τρεις διαδοχικούς φυσικούς αριθμούς μόνο ένας διαιρείται με το 3, έπεται ότι το πλήθος των φυσικών αριθμών μεταξύ του 1 και του 1.000.000, οι οποίοι είναι διαιρετοί με το 3, θα είναι ο μεγαλύτερος φυσικός αριθμός, ο οποίος είναι μικρότερος ή ίσος του $\frac{1.000.000}{3}$. Συνεπώς $|\, B_3 \,| = 333.333$.

Όμοια, επειδή σε κάθε πέντε διαδοχικούς φυσικούς αριθμούς μόνο ένας διαιρείται με το 5, έπεται ότι το πλήθος των φυσικών αριθμών μεταξύ του 1 και του 1.000.000, οι οποίοι είναι διαιρετοί με το 5 θα είναι ο μεγαλύτερος φυσικός αριθμός, ο οποίος είναι μικρότερος ή ίσος του $\frac{1.000.000}{5}$. Συνεπώς $|\, B_5 \,| = 200.000$.

Με το ίδιο σκεπτικό έχουμε ότι

$$\begin{aligned} |\, B_{13} \,| &= 76.923, \\ |\, B_3 \cap B_5 \,| &= 66.666 \leq \frac{1.000.000}{15}, \\ |\, B_3 \cap B_{13} \,| &= 25.641 \leq \frac{1.000.000}{39}, \\ |\, B_5 \cap B_{13} \,| &= 15.384 \leq \frac{1.000.000}{65}, \\ |\, B_3 \cap B_5 \cap B_{13} \,| &= 5.128 \leq \frac{1.000.000}{195}. \end{aligned}$$

Συνεπώς, ο αριθμός, που αναζητούμε, ισούται με τον

$$|\, X \setminus (B_3 \cap B_5 \cap B_{13}) \,| = \text{, βάσει της προηγουμένης πρότασης, } = \ldots = 492.307$$

(Να κάνετε τον έλεγχο).

Πρόταση Β.1.13. *Έστω A, B δύο πεπερασμένα σύνολα με $|\, A \,| = n$ και $|\, B \,| = m$. Το καρτεσιανό γινόμενο $A \times B$ είναι πεπερασμένο και $|\, A \times B \,| = |\, A \,| \cdot |\, B \,|$.*

Απόδειξη. Για κάθε στοιχείο $a \in A$ θεωρούμε το σύνολο

$$B_a = \{(a, b) \mid b \in B\}.$$

Προφανώς κάθε $B_a \sim B$ (γιατί;). Επίσης, για $a_1, a_2 \in A$ με $a_1 \neq a_2$, ισχύει ότι

$$B_{a_1} \cap B_{a_2} = \emptyset \text{ (γιατί;)}.$$

Έστω $(a, b) \in A \times B$, τότε

$$(a, b) \in B_a \subseteq \bigcup_{a \in A} B_a.$$

Αντίστροφα, έστω $(x, y) \in \bigcup_{a \in A} B_a$, τότε $(x, y) \in B_a$ για κάποιο $a \in A$. Συνεπώς $(x, y) = (a, b)$ με $b \in B$ και επομένως

$$\bigcup_{a \in A} B_a \subseteq A \times B.$$

Επομένως, $A \times B = \bigcup_{a \in A} B_a$ και από την Πρόταση Β.1.9 έχουμε ότι

$$|\, A \times B \,| = \sum_{a \in A} |\, B_a \,| = |\, A \,| \cdot |\, B \,|. \qquad \text{ό.έ.δ.}$$

Η προηγουμένη απόδειξη είναι απλή και μας εξασφαλίζει ότι υπάρχει μια απεικόνιση $f : A \times B \longrightarrow N_{nm}$, η οποία είναι 1-1 και επί.

Εκ πρώτης όψεως δεν είναι εύκολο να βρούμε μια τέτοια απεικόνιση.

Θα δούμε πώς μπορούμε να ορίσουμε μια τέτοια απεικόνιση.

Επειδή $A \sim N_n$ και $B \sim N_m$, χωρίς βλάβη της γενικότητας, ορίζουμε μια απεικόνιση

$$f : N_n \times N_m \longrightarrow N_{nm}$$

ως εξής:

$$f(i, j) = (i-1)m + j, \text{ για } (i, j) \in N_n \times N_m.$$

Η f είναι 1-1. Πράγματι, υποθέτουμε ότι $f(i, j) = f(r, s)$, τότε

$$(i-1)m + j = (r-1)m + s.$$

Από την τελευταία σχέση έχουμε ότι

$$(i-r)m = s - j.$$

Αυτό όμως ισχύει μόνο αν $i = r$ και $s = j$ (γιατί; δεν ξεχνάμε ότι $1 \leq s, j \leq m$).

Η f είναι επί. Έστω $y \in N_{nm}$, από την ταυτότητα της διαίρεσης με το m έχουμε ότι

$$y = \pi m + \upsilon \text{ με } 0 \leq \upsilon < m$$

και, επειδή $1 \leq y \leq nm$, αναγκαστικά $0 \leq \pi \leq n$. Τότε όμως για $x = (\pi + 1, \upsilon)$ έχουμε ότι

$$f(x) = f(\pi + 1, \upsilon) = ((\pi + 1 - 1)m + \upsilon = \pi m + \upsilon = y.$$

Θα κλείσουμε την αναφορά μας στα πεπερασμένα σύνολα συνοψίζοντας όλα τα προηγούμενα σε ένα θεώρημα.

Θεώρημα Β.1.14. Η αρχή του περιστεριώνα *Έστω A, B δύο πεπερασμένα σύνολα.*

i. Αν $|A| > |B|$, τότε κάθε απεικόνιση $f : A \longrightarrow B$ δεν είναι 1-1.

ii. Αν $|A| < |B|$, τότε κάθε απεικόνιση $g : A \longrightarrow B$ δεν είναι επί.

Απόδειξη.

i. Υποθέτουμε ότι υπάρχει μια απεικόνιση $f : A \longrightarrow B$, η οποία είναι 1-1. Τότε, ως γνωστόν(;), η απεικόνιση $g : A \longrightarrow f(A)$ με

$$g(a) = f(a),$$

για όλα τα $a \in A$, είναι 1-1 και επί. Επομένως, εξ ορισμού $A \sim f(A)$ με το $f(A) \subseteq B$. Τότε όμως έχουμε

$$|A| = |f(A)| \leq |B|$$

(γιατί ισχύει η ανισότητα στην προηγουμένη σχέση; μα ισχύει το Πόρισμα Β.1.6). Αυτό είναι άτοπο, διότι εξ υποθέσεως έχουμε ότι $|A| > |B|$.

ii. Με παρόμοια επιχειρήματα αποδεικνύεται και αυτός ο ισχυρισμός και αφήνεται ως άσκηση. ό.έ.δ.

Στην προηγουμένη απόδειξη (σκόπιμα) επιλέξαμε την μέθοδο της αντιθετοαντιστροφής (ιδέ παρ. 3.2.5), διότι το ανωτέρω θεώρημα το συναντάμε και στην εξής εκδοχή.

Θεώρημα Β.1.15. *Έστω A, B δύο πεπερασμένα σύνολα και $f : A \longrightarrow B$ μια απεικόνιση.*

i. Αν η $f : A \longrightarrow B$ είναι 1-1, τότε $|A| \leq |B|$.

ii. Αν η $f : A \longrightarrow B$ είναι επί, τότε $|A| \geq |B|$.

Σχόλια Β.1.16. Το ανωτέρω θεώρημα (σε οποιαδήποτε μορφή), από πολλούς θεωρείται, ως κάτι, το οποίο *αξιωματικά/αυταπόδεικτα ισχύει*. Όπως βλέπουμε, μπορεί (και πρέπει) να αποδειχθεί.

Δεν χρειάζεται ιδιαίτερο σχόλιο για τον χαρακτηρισμό *Η αρχή του περιστεριώνα*. Ο καθένας μπορεί να φανταστεί την εικόνα με περιστέρια (ή σφαιρίδια) και φωλιές (και κουτιά), όπου, συγκρίνοντας το πλήθος των στοιχείων των δύο συνόλων, μπορούμε να αποφανθούμε για την αντιστοιχία/απεικόνιση μεταξύ των δύο συνόλων.

Η αρχή του περιστεριώνα είναι πάρα πολύ χρήσιμη σε διαφόρους κλάδους των Μαθηματικών, όπως η Συνδυαστική, τα Διακριτά Μαθηματικά κ.λ.π., αλλά και σε περιοχές όπου δεν το φανταζόμαστε.

Ας δούμε ένα παράδειγμα.

Παράδειγμα Β.1.17. Έστω A ένα (τυχαίο) υποσύνολο του συνόλου $\{1, 2, \ldots, 100\}$, το οποίο περιέχει 10 το πλήθος στοιχεία. Υπάρχουν δύο (μη κενά) υποσύνολα του συνόλου A, ξένα μεταξύ τους, με την ιδιότητα: Το άθροισμα των στοιχείων του ενός να ισούται με το άθροισμα των στοιχείων του άλλου.

Το άθροισμα των στοιχείων του συνόλου A δεν μπορεί να υπερβαίνει τον αριθμό

$$10 \cdot 100 = 1000$$

(γιατί;), επομένως και για κάθε υποσύνολο $X \subseteq A$ το άθροισμα των στοιχείων του δεν μπορεί να υπερβαίνει το 1000.

Επίσης, το πλήθος των υποσυνόλων του συνόλου A είναι ίσον με 2^{10} (γιατί; ιδέ την Πρόταση 1.1.44 ή το Θεώρημα 3.2.9.

Ορίζουμε την εξής απεικόνιση

$$\mathcal{P}(A) \longrightarrow \{0, 1, 2, \ldots, 1000\},$$

η οποία απεικονίζει κάθε υποσύνολο X του A στο άθροισμα των στοιχείων του.

Παρατηρούμε ότι

$$|\mathcal{P}(A)| = 2^{10} = 1.024 > 1001 = |\{0, 1, 2, \ldots, 1000\}|,$$

επομένως, από το Θεώρημα Β.1.14,έχουμε ότι η f δεν είναι 1-1. Συνεπώς, υπάρχουν δύο διαφορετικά υποσύνολα του συνόλου A, των οποίων τα αθροίσματα των στοιχείων τους είναι ίσα.

Ερώτημα: Γιατί τα δύο αυτά υποσύνολα μπορούν να υποτεθούν ξένα μεταξύ τους;

Όπως βλέπουμε στο προηγούμενο παράδειγμα, η απόδειξη είναι "υπαρξιακή". Δεν χρειάστηκε να παραθέσουμε όλα τα υποσύνολα του συνόλου A και να τα συγκρίνουμε ως προς το άθροισμα των στοιχείων τους.

Β.2 Άπειρα σύνολα

Στην αρχή (μετά τον Ορισμό Β.0.5) είχαμε προβληματιστεί κατά πόσο υπάρχουν άπειρα σύνολα. Μάλιστα δε, είχαμε διατυπώσει την Πρόταση Β.0.6, την απόδειξη της οποίας είχαμε αναβάλει.

Στην παράγραφο αυτή θα ασχοληθούμε με την ύπαρξη απείρων συνόλων και, εν συντομία, με δύο *είδη* απείρων συνόλων. Τα αριθμήσιμα και τα υπεραριθμήσιμα.

Πρόταση Β.2.1. *Ένα σύνολο A είναι άπειρο, αν και μόνο αν περιέχει ένα γνήσιο άπειρο υποσύνολο.*

Απόδειξη. Υποθέτουμε ότι το σύνολο A είναι άπειρο. Έστω $x \in A$. Θέτουμε

$$B = A \setminus \{x\}.$$

Το σύνολο B είναι γνήσιο υποσύνολο του A.

Αν το B ήταν πεπερασμένο, τότε $B \sim N_n$ για κάποιο $n \in \mathbb{N}$. Επομένως, από το Πόρισμα Β.1.5, θα έχουμε ότι το σύνολο $A = B \cup \{x\}$ είναι πεπερασμένο, άτοπο.

Αντίστροφα, υποθέτουμε ότι το σύνολο A περιέχει ένα υποσύνολο B, το οποίο είναι άπειρο. Τότε το σύνολο A δεν μπορεί να είναι πεπερασμένο, από το Πόρισμα Β.1.6. ό.έ.δ.

Πρόταση Β.2.2. *(Είναι η Πρόταση Β.0.6) Το σύνολο $\mathbb{N}$ είναι άπειρο.*

Απόδειξη. Αν το $\mathbb{N}$ ήταν πεπερασμένο, δεν θα μπορούσε να είναι ισοπληθικό με ένα γνήσιο υποσύνολό του. Αλλά το $\mathbb{N}$ είναι ισοπληθικό με το υποσύνολό του

$$D = \{2n \mid n \in \mathbb{N}\},$$

το οποίο περιέχει όλους τους άρτιους φυσικούς αριθμούς (γιατί;) ό.έ.δ.

Β.2.1 Αριθμήσιμα σύνολα

Σε κάθε μη κενό πεπερασμένο σύνολο είχαμε προσάψει έναν φυσικό αριθμό, τον πληθικό του αριθμό, ο οποίος το χαρακτηρίζει ως προς το μέγεθός του. Στην περίπτωση των απείρων συνόλων δεν μπορούμε να προσάψουμε έναν φυσικό αριθμό, ο οποίος να τα χαρακτηρίζει ως προς το "μέγεθός" τους.

Στην περίπτωση του συνόλου των φυσικών και κάθε ισοπληθικού τους συνόλου, δηλαδή σε κάθε απείρως αριθμήσιμο σύνολο, προσάπτουμε έναν "πληθικό αριθμό" (ή πληθικότητα), το $\aleph_0$ και θα συμβολίζουμε

$$card(\mathbb{N}) = \aleph_0.$$

Οπότε,

$$card(\mathbb{Z}) = \aleph_0.$$

Πρόταση Β.2.3.

i. Έστω A ένα απείρως αριθμήσιμο σύνολο, τότε το σύνολο $A \cup \{x\}$ είναι απείρως αριθμήσιμο.

ii. Έστω A ένα απείρως αριθμήσιμο σύνολο και $x \in A$, τότε το σύνολο $A \setminus \{x\}$ είναι απείρως αριθμήσιμο.

Απόδειξη.

i. Προφανώς μπορούμε να υποθέσουμε ότι το $x \notin A$. Επειδή το A είναι ισοπληθικό με το σύνολο $\mathbb{N}$, υπάρχει μια απεικόνιση $f : \mathbb{N} \longrightarrow A$, η οποία είναι 1-1 και επί.

Ορίζουμε την εξής απεικόνιση $g : \mathbb{N} \longrightarrow A \cup \{x\}$ ως εξής:

$$g(n) = \begin{cases} x & \text{αν } n = 1 \\ f(n-1) & \text{αν } n > 1 \end{cases}$$

Είναι πολύ εύκολο να ελέγξουμε (ιδέ Άσκηση B.2.4$_{10}$) ότι η απεικόνιση g είναι 1-1 και επί.

ii. Όπως στο πρώτο μέρος, μπορούμε να ορίσουμε μια κατάλληλη απεικόνιση

$$h : \mathbb{N} \longrightarrow A \setminus \{x\},$$

η οποία είναι 1-1 και επί (κάντε το). ό.έ.δ.

Πόρισμα B.2.4. *Έστω A ένα απείρως αριθμήσιμο σύνολο και B ένα πεπερασμένο σύνολο. Το σύνολο $A \cup B$ είναι απείρως αριθμήσιμο.*

Απόδειξη. Η απόδειξη αποτελεί μια εφαρμογή της Μαθηματικής επαγωγής και αφήνεται ως άσκηση (Άσκηση B.2.4$_{10}$). ό.έ.δ.

Παρατηρήστε την (ουσιώδη) διαφορά μεταξύ του Πορίσματος B.1.5 και της Πρότασης B.2.3.

Πρόταση B.2.5. *Έστω A, B δύο απείρως αριθμήσιμα σύνολα, τα οποία είναι ξένα μεταξύ τους. Η ένωση $A \cup B$ είναι απείρως αριθμήσιμο σύνολο.*

Απόδειξη. Επειδή τα σύνολα A και B έχουν υποτεθεί απείρως αριθμήσιμα, υπάρχουν απεικονίσεις $f : \mathbb{N} \longrightarrow A$ και $g : \mathbb{N} \longrightarrow B$, οι οποίες είναι 1-1 και επί.

Ορίζουμε την απεικόνιση $h : \mathbb{N} \longrightarrow A \cup B$ ως εξής:

$$h(n) = \begin{cases} f\left(\dfrac{n+1}{2}\right) & \text{αν ο } n \text{ είναι περιττός} \\ \\ g\left(\dfrac{n}{2}\right) & \text{αν ο } n \text{ είναι άρτιος} \end{cases}$$

Η h είναι πράγματι απεικόνιση και μάλιστα είναι 1-1 και επί.

Θα δείξουμε ότι είναι επί αφήνοντας τα υπόλοιπα ως άσκηση (Άσκηση B.2.4$_{11}$).

Έστω $y \in A \cup B$. Τα A, B έχουν υποτεθεί ξένα μεταξύ τους, επομένως είτε $y \in A$ ή $y \in B$.

Υποθέτουμε ότι $y \in A$, τότε υπάρχει $n \in \mathbb{N}$, ώστε $f(n) = y$. Αν ο $n = 2k$, τότε για $x = 4k - 1$ έχουμε ότι

$$h(x) = h(4k-1) = f\left(\frac{(4k-1)+1}{2}\right) = f(2k) = f(n) = y.$$

Αν ο $n = 2k + 1$, τότε για $x = 4k + 1$ έχουμε ότι

$$h(x) = h(4k+1) = f\left(\frac{(4k+1)+1}{2}\right) = f(2k+1) = f(n) = y.$$

Υποθέτουμε ότι $y \in B$, τότε υπάρχει $n \in \mathbb{N}$, ώστε $g(n) = y$. Αν ο $n = 2k$, τότε για $x = 4k$ έχουμε ότι

$$h(x) = h(4k) = g\left(\frac{4k}{2}\right) = g(2k) = g(n) = y.$$

Αν ο $n = 2k + 1$, τότε για $x = 4k + 2$ έχουμε ότι

$$h(x) = h(4k + 2) = g\left(\frac{4k + 2}{2}\right) = g(2k + 1) = g(n) = y.$$

Επομένως, για το τυχαίο $y \in A \cup B$, πάντα υπάρχει ένα $x \in \mathbb{N}$, ώστε $h(x) = y$. Άρα η h είναι επί. ό.έ.δ.

Προφανώς, η ανωτέρω πρόταση γενικεύεται στην περίπτωση, όπου έχουμε την ένωση πεπερασμένου το πλήθος αριθμησίμων συνόλων (ιδέ Άσκηση B.2.4$_{12}$).

Εδώ θέλουμε να επισημάνουμε ότι μπορούμε να γενικεύσουμε ακόμη περισσότερο και να αποδείξουμε την εξής πρόταση:

Πρόταση B.2.6. *Έστω $(A_i)_{i\in I}$ μια οικογένεια αριθμησίμων συνόλων. Υποθέτουμε ότι το σύνολο δεικτών I είναι αριθμήσιμο σύνολο, τότε η ένωση $\bigcup_{i\in I} A_i$ είναι αριθμήσιμο σύνολο.*

Απόδειξη. Η ιδέα της απόδειξης είναι απλή και στηρίζεται στην ιδέα της απόδειξης της προηγουμένης πρότασης, αλλά είναι τεχνική και είναι πέραν του σκοπού μας.

Παρ' όλα ταύτα, συνιστάται να μελετηθεί σε μια δεύτερη ανάγνωση και παραπέμπουμε στο [1] (Theorem 6.6.9 page 236). ό.έ.δ.

Πρόταση B.2.7. *Έστω A ένα αριθμήσιμο σύνολο. Κάθε υποσύνολο $B \subseteq A$ είναι αριθμήσιμο.*

Απόδειξη. Αν το υποσύνολο B είναι πεπερασμένο, τότε, εξ ορισμού, είναι αριθμήσιμο. Υποθέτουμε ότι το B είναι άπειρο, τότε και το σύνολο A είναι άπειρο και, ως αριθμήσιμο, είναι απείρως αριθμήσιμο. Επομένως, μπορούμε να υποθέσουμε (εξ αρχής) ότι $A = \mathbb{N}$ (γιατί;).

Θα ορίσουμε μια απεικόνιση $f : \mathbb{N} \longrightarrow B$ και θα αποδείξουμε ότι είναι 1-1 και επί, οπότε έπεται το ζητούμενο.

Ο ορισμός της απεικόνισης θα γίνει αναδρομικά.

Το σύνολο B, ως υποσύνολο των φυσικών αριθμών, έχει ένα (μοναδικό) ελάχιστο στοιχείο, έστω b_1 (Δεν ξεχνάμε την Αρχή του ελαχίστου στοιχείου Θεώρημα A.1.10). Ορίζουμε

$$f(1) = b_1.$$

Το σύνολο $B \setminus \{b_1\}$ είναι μη κενό (γιατί;), επομένως έχει ελάχιστο στοιχείο, έστω b_2. Ορίζουμε

$$f(2) = b_2.$$

Για κάθε $n \in \mathbb{N}$ το σύνολο $B \setminus \{b_1, b_2, \ldots, b_n = f(n)\}$ είναι μη κενό (γιατί;), επομένως έχει ελάχιστο στοιχείο, έστω b_{n+1}. Οπότε, ορίζουμε

$$f(n + 1) = b_{n+1}.$$

Επομένως, η f είναι καλώς ορισμένη.

Επίσης, από τον τρόπο ορισμού της f, ισχύει ότι $f(r) < f(r+1)$, για όλα τα $r \in \mathbb{N}$ (γιατί;). Επομένως, $n \leq f(n)$, για όλα τα $n \in \mathbb{N}$ (ιδέ Άσκηση A.1.1$_{11}$).

Θα δείξουμε ότι η f είναι 1-1. Έστω $r, s \in \mathbb{N}$ με $r < s$, τότε

$$f(r) \in \{ f(1), f(2), \ldots, f(s-1) \},$$

αλλά $f(s-1) < f(s)$. Αυτό σημαίνει ότι $f(r) \neq f(s)$. Επομένως η f είναι 1-1.

Θα δείξουμε ότι η f είναι επί. Έστω $b \in B$ με $b \neq f(n)$, για όλα τα $n \in \mathbb{N}$. Έχουμε ήδη παρατηρήσει ότι $b \leq f(b)$, συνεπώς $b < f(b)$. Το στοιχείο $f(b)$, από τον τρόπο ορισμού της απεικόνισης f, είναι το ελάχιστο στοιχείο του συνόλου

$$B \setminus \{ f(1), f(2), \ldots, f(b-1) \}.$$

Επίσης, από την υπόθεση

$$b \in B \setminus \{ f(1), f(2), \ldots, f(b-1) \}.$$

Αυτό σημαίνει ότι $f(b) \leq b$, άτοπο. Πώς καταλήξαμε σε άτοπο; Διότι υποθέσαμε ότι $b \neq f(n)$, για όλα τα $n \in \mathbb{N}$.

Άρα η f είναι και επί. Συνεπώς, η απόδειξη ολοκληρώθηκε. ό.έ.δ.

Πόρισμα Β.2.8. *Κάθε άπειρο υποσύνολο των φυσικών αριθμών είναι απείρως αριθμήσιμο.*

Πόρισμα Β.2.9. *Η τομή αριθμησίμων συνόλων είναι αριθμήσιμο σύνολο.*

Για να αποδείξουμε ότι ένα σύνολο είναι αριθμήσιμο, συνήθως διακρίνουμε περιπτώσεις, αν είναι πεπερασμένο ή απείρως αριθμήσιμο. Το επόμενο θεώρημα μας επιτρέπει μια ενιαία αντιμετώπιση.

Θεώρημα Β.2.10. *Έστω A ένα (μη κενό) σύνολο. Οι ακόλουθες προτάσεις είναι ισοδύναμες.*

i. Το σύνολο A είναι αριθμήσιμο.

ii. Υπάρχει μια απεικόνιση $f : A \longrightarrow \mathbb{N}$, η οποία είναι 1-1.

iii. Υπάρχει μια απεικόνιση $g : \mathbb{N} \longrightarrow A$, η οποία είναι επί.

Απόδειξη. $(i) \Longrightarrow (ii)$ Η συνεπαγωγή αυτή είναι προφανής. Καθ' ότι, αν το A είναι πεπερασμένο, τότε υπάρχει απεικόνιση $h : A \longrightarrow N_n$, για κάποιο $n \in \mathbb{N}$, η οποία είναι 1-1 και επί, οπότε η σύνθεση της απεικόνισης αυτής με την εμφύτευση $j : N_n \longrightarrow \mathbb{N}$ μας δίνει την ζητουμένη απεικόνιση f.

Αν το A είναι απείρως αριθμήσιμο, τότε, εξ ορισμού, υπάρχει μια απεικόνιση $f : A \longrightarrow \mathbb{N}$, η οποία είναι 1-1 και επί.

$(ii) \Longrightarrow (i)$ Για την απεικόνιση $f : A \longrightarrow \mathbb{N}$, η οποία είναι 1-1, ισχύει ότι $A \sim f(A)$ (γιατί;). Αλλά $f(A) \subseteq \mathbb{N}$, επομένως, από την προηγουμένη πρόταση, έχουμε ότι το $f(A)$, άρα και το A, είναι αριθμήσιμο.

$(ii) \Longrightarrow (iii)$ Υποθέτουμε ότι υπάρχει μια απεικόνιση $f : A \longrightarrow \mathbb{N}$, η οποία είναι 1-1. Από το Θεώρημα 4.5.35 έπεται ότι υπάρχει μια αριστερή αντίστροφη απεικόνιση της f, έστω $g : \mathbb{N} \longrightarrow A$, η οποία είναι επί.

Παρομοίως αποδεικνύεται και η κατεύθυνση

$(iii) \Longrightarrow (ii)$ ό.έ.δ.

Πρόταση Β.2.11. *Το καρτεσιανό γινόμενο* $\mathbb{N}\times\mathbb{N}$ *είναι απείρως αριθμήσιμο σύνολο.*

Απόδειξη. Ορίζουμε την απεικόνιση $f : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$ ως εξής:

$$f(n, m) = 2^n 3^m.$$

Προφανώς (γιατί;) η f είναι απεικόνιση και μάλιστα 1-1. Επομένως, από το προηγούμενο θεώρημα έχουμε ότι το καρτεσιανό γινόμενο είναι αριθμήσιμο σύνολο και επειδή είναι άπειρο σύνολο είναι απείρως αριθμήσιμο. Δηλαδή ισοπληθικό με το σύνολο $\mathbb{N}$. ό.έ.δ.

Στην προηγουμένη πρόταση αποδείξαμε ότι $\mathbb{N}\times\mathbb{N} \sim \mathbb{N}$. Αλλά δεν βρήκαμε μια απεικόνιση $g : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$, η οποία να είναι 1-1 και επί (η απεικόνιση f είναι 1-1, αλλά όχι επί). Στην Άσκηση Β.2.4$_{13}$ δίνεται μια τέτοια απεικόνιση.

Πόρισμα Β.2.12. *Έστω* $A_1, A_2, \ldots, A_n$ *αριθμήσιμα σύνολα. Το καρτεσιανό γινόμενο* $A_1\times A_2\times\ldots\times A_n$ *είναι αριθμήσιμο σύνολο.*

Απόδειξη. Η απόδειξη στηρίζεται στις Προτάσεις Β.1.13, Β.2.11 και εφαρμόζοντας επαγωγή επί του πλήθους n των συνόλων. ό.έ.δ.

Θεώρημα Β.2.13. *Το σύνολο* $\mathbb{Q}$ *των ρητών αριθμών είναι απείρως αριθμήσιμο.*

Απόδειξη. Υπάρχουν πολλές αποδείξεις για το σημαντικό αυτό αποτέλεσμα. Εδώ θα δούμε μερικές.

$1^η$. Έχουμε αποδείξει ότι $\mathbb{Z} \sim \mathbb{N}$ (Παράδειγμα Β.0.4). Έχουμε αποδείξει ότι

$$\mathbb{Z}^* = \mathbb{Z}\setminus\{0\} \sim \mathbb{N}$$

(Πρόταση Β.2.3). Έχουμε αποδείξει ότι

$$N\times\mathbb{N} \sim \mathbb{N}$$

(Πρόταση Β.2.11). Συνεπώς

$$\mathbb{N} \sim \mathbb{Z}\times\mathbb{Z}^*.$$

Δηλαδή υπάρχει μια απεικόνιση $f : \mathbb{N} \longrightarrow \mathbb{Z}\times\mathbb{Z}^*$, η οποία είναι 1-1 και επί.

Από τον ορισμό των ρητών αριθμών (Ορισμός 6.2.2), έπεται ότι υπάρχει μια απεικόνιση (η φυσική απεικόνιση) $\varphi : \mathbb{Z}\times\mathbb{Z}^* \longrightarrow \mathbb{Q}$, η οποία είναι επί.

Επομένως, η σύνθεση $\varphi\circ f$ είναι επί. Οπότε, σύμφωνα με το Θεώρημα Β.2.10, το σύνολο των ρητών αριθμών είναι απείρως αριθμήσιμο.

$2^η$. Ως γνωστόν(;) κάθε θετικός ρητός αριθμός παρίσταται (μοναδικά) ως ένα ανάγωγο κλάσμα m/n με $m, n \in \mathbb{N}$. Έστω $\mathbb{Q}^+$ το σύνολο των θετικών ρητών αριθμών και $\mathbb{Q}^-$ το σύνολο των αρνητικών ρητών αριθμών.

Ορίζουμε την εξής απεικόνιση $g : \mathbb{Q}^+ \longrightarrow \mathbb{N}$ ως εξής:

$$g(m/n) = 2^m 3^n$$

προφανώς(;) η g είναι 1-1 (συγκρίνατε με την απόδειξη της Πρότασης Β.2.11). Επομένως, σύμφωνα με το Θεώρημα Β.2.10, το σύνολο των θετικών ρητών αριθμών είναι απείρως αριθμήσιμο.

Προφανώς $\mathbb{Q}^+ \sim \mathbb{Q}^-$ και $\mathbb{Q} = \mathbb{Q}^-\cup\{0\}\cup Q^+$, οπότε $\mathbb{Q} \sim \mathbb{N}$ (γιατί; δεν ξεχνάμε την Πρόταση Β.2.5).

3^{η}. Για κάθε φυσικό αριθμό n ορίζουμε το σύνολο

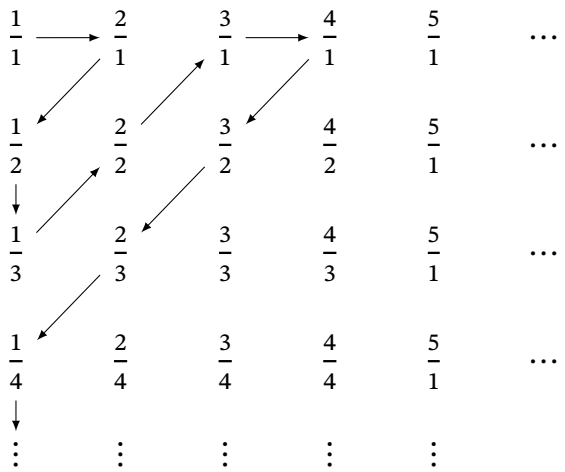
$$A_n = \{\frac{(n+1)-i}{i} \mid i = 1, 2, \dots, n\}.$$

Προφανώς κάθε A_n είναι πεπερασμένο σύνολο. Παρατηρούμε ότι για κάθε θετικό ρητό αριθμό της μορφής κ/λ ισχύει ότι

$$\kappa/\lambda = \frac{(\kappa+\lambda-1)+1-\lambda}{\lambda} \in A_m,$$

όπου $m = \kappa+\lambda-1$. Επομένως $\mathbb{Q}^+ \subseteq \bigcup_{n\in\mathbb{N}} A_n$. Το σύνολο $\bigcup_{n\in\mathbb{N}} A_n$ είναι αριθμήσιμο (γιατί; ιδέ Πρόταση B.2.6). Συνεπώς, το σύνολο $\mathbb{Q}^+$ είναι απείρως αριθμήσιμο, οπότε συνεχίζουμε ως ανωτέρω. ό.έ.δ.

Σχόλιο B.2.14. Σκόπιμα αποφύγαμε να αναφέρουμε την ευρέως γνωστή διαισθητική απόδειξη ότι το σύνολο των θετικών ρητών αριθμών είναι αριθμήσιμο, όπως παρουσιάζεται στο σχήμα B.1. Μπορείτε, παρατηρώντας το σχήμα να επιχειρηματο-



Σχήμα B.1: *Η πρώτη διαγώνιος μέθοδος του Cantor.*

λογήσετε, γιατί το σύνολο των θετικών ακεραίων αριθμών είναι απείρως αριθμήσιμο;

Θα κλείσουμε την παράγραφο αποδεικνύοντας ότι κάθε αριθμήσιμο σύνολο μπορεί να διαταχθεί καλώς (Ορισμός 4.4.18).

Έχουμε δει ότι το σύνολο των φυσικών αριθμών είναι καλώς διατεταγμένο (Θεώρημα A.1.10).

Έχουμε δει ότι το σύνολο των ακεραίων αριθμών (με την γνωστή διάταξη) δεν είναι καλώς διατεταγμένο. Αλλά το σύνολο των ακεραίων είναι αριθμήσιμο σύνολο (Παράδειγμα $B.0.4_1$).

Μάλιστα δε, η απεικόνιση $\phi : \mathbb{N} \longrightarrow \mathbb{Z}$ με

$$\phi(n) = \begin{cases} \frac{n}{2} & \text{αν n είναι άρτιος} \\ -\frac{n-1}{2} & \text{αν n είναι περιττός} \end{cases}$$

"αναδιατάσσει" τους ακεραίους (όχι κατ' αύξουσα σειρά) ως εξής:

$$0, 1, -1, 2, -2, \dots,$$

όπου έχουμε πλέον "αρχικό στοιχείο". Επομένως, στο σύνολο των ακεραίων αριθμών, θα μπορούσαμε να ορίσουμε μια νέα διάταξη $\prec$ ως εξής:

$$0 \prec 1 \prec -1 \prec 2 \prec -2 \prec \cdots.$$

Ως προς αυτήν την διάταξη το σύνολο $(\mathbb{Z}, \prec)$ είναι καλώς διατεταγμένο.

Θεώρημα Β.2.15. *Έστω S ένα απείρως αριθμήσιμο σύνολο. Στο σύνολο S μπορούμε να ορίσουμε μια διάταξη, ως προς την οποία να είναι καλώς διατεταγμένο σύνολο.*

Απόδειξη. Εξ ορισμού, υπάρχει μια απεικόνιση $\varphi : A \longrightarrow \mathbb{N}$, η οποία είναι 1-1 και επί.

Το σύνολο των φυσικών αριθμών $\mathbb{N}$ είναι καλώς διατεταγμένο, ως προς την συνήθη διάταξη $<$.

Στο σύνολο S ορίζουμε μια σχέση $\prec$ ως εξής:

$$a \prec b, \text{ αν και μόνο αν } \varphi(a) < \varphi(b).$$

Το σύνολο $(A, \prec)$ είναι ένα καλώς διατεταγμένο σύνολο.

Πράγματι, είναι ρουτίνα να ελέγξουμε ότι η $\prec$ είναι μια σχέση διάταξης.

Επίσης, αν S είναι ένα μη κενό υποσύνολο του A, τότε το σύνολο $\varphi(S) \subseteq \mathbb{N}$ έχει ελάχιστο στοιχείο, έστω m αυτό το στοιχείο. Επειδή η φ είναι 1-1 και επί, υπάρχει μοναδικό $s \in S$ με $\varphi(a) = m$.

Είναι εύκολο να ελέγξουμε ότι το s είναι το ελάχιστο στοιχείο του συνόλου S (Άσκηση B.2.4$_{24}$). ό.έ.δ.

Β.2.2 Υπεραριθμήσιμα σύνολα

Στην αρχή του Παραρτήματος αυτού (ιδέ σελ. 348) είχαμε προβληματιστεί, αν υπάρχουν υπεραριθμήσιμα σύνολα. Θα δούμε ότι πράγματι υπάρχουν τέτοια σύνολα.

Ορισμός Β.2.16. (Επέκταση του Ορισμού B.0.1)

Έστω A, B δύο σύνολα. Τα A και B θα ονομάζονται **ισοπληθικά** ή ότι έχουν την ίδια πληθικότητα, αν υπάρχει μια απεικόνιση $f : A \longrightarrow B$, η οποία είναι 1-1 και επί. Δύο ισοπληθικά σύνολα θα συμβολίζονται ως $A \sim B$ ή ως $card(A) = card(B)$.

Στην περίπτωση, όπου υπάρχει μια απεικόνιση $f : A \longrightarrow B$, η οποία είναι 1-1, τότε συμβολίζουμε

$$card(A) \leq card(B) \text{ ή } A \preceq B.$$

Στην περίπτωση, όπου υπάρχει μια απεικόνιση $f : A \longrightarrow B$, η οποία είναι 1-1, αλλά δεν υπάρχει απεικόνιση από το A στο B, η οποία είναι 1-1 και επί, τότε συμβολίζουμε

$$card(A) < card(B) \text{ ή } A \prec B.$$

Παρατήρηση Β.2.17. Εδώ πρέπει να παρατηρήσουμε ότι στην περίπτωση των πεπερασμένων συνόλων ισχύει η αρχή του περιστεριώνα. Εκεί είχαμε τα Θεωρήματα B.1.14 και B.1.15 (όπως έχουμε επισημάνει, πρόκειται για το ίδιο θεώρημα), όπου είχαμε δει πώς συγκρίνονται πληθικοί αριθμοί πεπερασμένων συνόλων με την βοήθεια απεικονίσεων.

Είναι αυτό που εδώ τίθεται ως ορισμός, αλλά αναφέρεται σε όλα τα σύνολα και μας επιτρέπει "σύγκριση" πληθικοτήτων συνόλων. Επ' αυτού θα επανέλθουμε αργότερα (ιδέ Παράγραφο B.2.3).

Θεώρημα Β.2.18. *Έστω A ένα σύνολο. Τότε*

$$card(A) < card(\mathcal{P}(A)) \quad (A \prec \mathcal{P}(A)).$$

Απόδειξη. Προφανώς, αν $A = \emptyset$, τότε

$$0 = card(A) < card(\mathcal{P}(A)) = card(\{\emptyset\} = 1.$$

Υποθέτουμε ότι $A \neq \emptyset$ και ότι υπάρχει μια απεικόνιση $f : A \longrightarrow \mathcal{P}(A)$, η οποία είναι 1-1 και επί. Τότε, επειδή η f είναι επί, για κάθε υποσύνολο του συνόλου A υπάρχει (μοναδικό) $a \in A$, ούτως ώστε το υποσύνολο αυτό να ισούται με την εικόνα $f(a)$.

Για $a \in A$ έχουμε ότι είτε $a \in f(a)$ ή $a \notin f(a)$. Ορίζουμε το εξής σύνολο:

$$S = \{s \in A \mid s \notin f(s)\}.$$

Προφανώς $S \subseteq A$, επομένως υπάρχει (μοναδικό) $a \in A$ με $S = f(a)$.

Υποθέτουμε ότι $a \in S = f(a)$. Από τον ορισμό του συνόλου S αυτό είναι άτοπο.

Υποθέτουμε ότι $a \notin S = f(a)$. Από τον ορισμό του συνόλου S, έχουμε ότι

$$a \in f(a) = S,$$

πάλι άτοπο.

Επομένως, σε όλες τις περιπτώσεις οδηγούμαστε σε άτοπο. Συνεπώς, δεν υπάρχει απεικόνιση από το σύνολο A στο σύνολο $\mathcal{P}(A)$, η οποία να είναι επί.

Υπάρχει όμως η προφανής απεικόνιση $g : A \longrightarrow \mathcal{P}(A)$ με

$$g(a) = \{a\},$$

η οποία είναι 1-1. Συνεπώς $A \prec \mathcal{P}(A)$. ό.έ.δ.

Πόρισμα Β.2.19. *Το δυναμοσύνολο $\mathcal{P}(\mathbb{N})$ των φυσικών αριθμών είναι υπεραριθμήσιμο.*

Το προηγούμενο θεώρημα, στην περίπτωση των πεπερασμένων συνόλων, το είχαμε συναντήσει ως την Πρόταση 1.1.44 (ή ως το Θεώρημα 3.2.25), όπου είχαμε δει ότι σε ένα πεπερασμένο σύνολο, με n το πλήθος στοιχεία, το πλήθος των υποσυνόλων του ισούται με 2^n.

Οπότε, κατ' αναλογίαν, συμβολίζουμε

$$card(\mathcal{P}(\mathbb{N})) = 2^{\aleph_0}.$$

Από το προηγούμενο θεώρημα έπεται ότι μπορούμε να *ιεραρχήσουμε* τις πληθικότητες των απείρων συνόλων, ξεκινώντας από τους φυσικούς αριθμούς, ως εξής:

$$\mathbb{N} \prec \mathcal{P}(\mathbb{N}) \prec \mathcal{P}(\mathcal{P}(\mathbb{N})) \prec \cdots .$$

Επομένως, υπάρχει μια απειρία διαφορετικών "ειδών απείρου".

Πρόταση Β.2.20. *Έστω A ένα σύνολο και $B \subseteq A$. Υποθέτουμε ότι το υποσύνολο B είναι υπεραριθμήσιμο. Το σύνολο A είναι υπεραριθμήσιμο.*

Απόδειξη. Η πρόταση αυτή αποτελεί την δυϊκή της Πρότασης Β.2.7 και η απόδειξή της αφήνεται ως άσκηση (ιδέ Άσκηση Β.2.4_{16}). ό.έ.δ.

Πριν διατυπώσουμε και αποδείξουμε την επομένη πρόταση, θα αναφέρουμε το γνωστό(;), αλλά όχι και τόσο εύκολο να αποδειχθεί, αποτέλεσμα.

> "Κάθε (θετικός) πραγματικός αριθμός a μπορεί να παρασταθεί σε δεκαδική μορφή ως εξής:
>
> $$a = m.a_1a_2a_3\cdots,$$
>
> όπου m είναι ένας μη αρνητικός ακέραιος αριθμός και τα (δεκαδικά ψηφία) $0 \leq a_i \leq 9$".

Σε μόνο μια περίπτωση ένας (θετικός) πραγματικός αριθμός μπορεί να παρασταθεί σε δεκαδική μορφή με περισσοτέρους του ενός τρόπους.

> "Ένας πραγματικός αριθμός της μορφής
>
> $$a = m.a_1a_2a_3\cdots a_k999\cdots,$$
>
> όπου από ένα ψηφίο και πέρα εμφανίζεται μια απειρία μόνο από το ψηφίο 9 ($a_k \neq 9$), είναι ίσος με τον
>
> $$a = m.a_1a_2a_3\cdots b_k000\cdots,$$
>
> όπου $b_k = a_k + 1$."

Για παράδειγμα, $0.2345999\cdots = 0.2346000\cdots$[6].

Επομένως, μπορούμε να μιλάμε για (μοναδική) **κανονική** δεκαδική παράσταση ενός πραγματικού αριθμού, όταν η παράστασή του $a = m.a_1a_2a_3\cdots$ στο τέλος δεν έχει μια απειρία ψηφίων 9.

Πρόταση Β.2.21. *Το διάστημα* $(0, 1) = \{x \in \mathbb{R} \mid 0 < x < 1\}$ *είναι υπεραριθμήσιμο σύνολο.*

Απόδειξη. Προφανώς (γιατί;) το διάστημα $(0, 1)$ είναι άπειρο σύνολο.

Υποθέτουμε ότι υπάρχει μια απεικόνιση $f : \mathbb{N} \longrightarrow (0, 1)$. Τότε θα μπορούσαμε να παραστήσουμε τις εικόνες $f(n)$, για $n \in \mathbb{N}$, σε κανονική δεκαδική μορφή ως εξής:

$$\begin{aligned}
f(1) &= 0.a_{11}a_{12}a_{13}\cdots a_{1k}\cdots\\
f(2) &= 0.a_{21}a_{22}a_{23}\cdots a_{2k}\cdots\\
f(3) &= 0.a_{31}a_{32}a_{33}\cdots a_{3k}\cdots\\
&\vdots\\
f(n) &= 0.a_{n1}a_{n2}a_{n3}\cdots a_{nk}\cdots\\
&\vdots
\end{aligned}$$

[6] 1. Αυτό είναι εύκολο να αποδειχθεί με την βοήθεια γεωμετρικών προόδων και, ίσως είναι γνωστό από τα "Γυμνασιακά Μαθηματικά".

2. Για διαχειριστικούς λόγους, όταν ένας δεκαδικός αριθμός είναι της μορφής

$$m.a_1a_2a_3\cdots a_kab\cdots cab\cdots c\cdots,$$

όπου το τμήμα $ab\cdots c$, στο τέλος επαναλαμβάνεται συνεχώς, τότε ο αριθμός συμβολίζεται ως $m.a_1a_2a_3\cdots a_k\overline{ab\cdots c}$, οπότε $0.2345\bar{9} = 0.2346\bar{0}$

Θα κατασκευάσουμε έναν πραγματικό αριθμό $b = 0.b_1b_2b_3\cdots b_k\cdots$ ως εξής:
Θέτουμε $b_1 = 1$, αν $a_{11} \neq 1$ και $b_1 = 2$, αν $a_{11} = 1$, δηλαδή

$$b_1 \neq a_{11}.$$

Θέτουμε $b_2 = 1$, αν $a_{22} \neq 1$ και $b_2 = 2$, αν $a_{22} = 1$, δηλαδή

$$b_2 \neq a_{22}.$$

Επαναλαμβάνουμε την ίδια διαδικασία για κάθε $k \in \mathbb{N}$ θέτοντας $b_k = 1$, αν $a_{kk} \neq 1$ και $b_k = 2$, αν $a_{kk} = 1$, δηλαδή

$$b_k \neq a_{kk}.$$

Ο πραγματικός αριθμός

$$b = 0.b_1b_2b_3\cdots b_k\cdots,$$

που κατασκευάσαμε με την ανωτέρω διαδικασία έχει την ιδιότητα

$$b \neq f(n),$$

για όλα τα $n \in \mathbb{N}$, διότι ο b και ο $f(n)$ διαφέρουν στο n-οστό δεκαδικό ψηφίο. Αλλά $b \in (0, 1)$. Συνεπώς η f δεν είναι επί. Δηλαδή δεν υπάρχει απεικόνιση

$$f : \mathbb{N} \longrightarrow (0, 1),$$

η οποία να είναι επί και επειδή το διάστημα $(0, 1)$ είναι άπειρο σύνολο, είναι υπεραριθμήσιμο. ό.έ.δ.

Θεώρημα Β.2.22. *Το σύνολο $\mathbb{R}$ των πραγματικών αριθμών είναι υπεραριθμήσιμο.*

Απόδειξη. Στο Παράδειγμα Β.0.4$_3$ είχαμε δει ότι $\mathbb{R} \sim (-1, 1)$. Από το Παράδειγμα Β.0.4$_2$, έπεται ότι $(-1, 1) \sim (0, 1)$. Οπότε, $\mathbb{R} \sim (0, 1)$, άρα είναι υπεραριθμήσιμο, βάσει της προηγουμένης πρότασης. ό.έ.δ.

Συνήθως συμβολίζουμε ως

$$\mathfrak{c} = card(\mathbb{R}).$$

Το επιχείρημα που χρησιμοποιήσαμε στην απόδειξη της Πρότασης Β.2.21 είναι γνωστό ως *"διαγώνιο επιχείρημα του Cantor"*, δεδομένου ότι πρώτος ο Cantor το επινόησε το 1874. Αν και η ιδέα είναι πολύ απλή (διαγωνίως αλλάζουμε ψηφία πραγματικών αριθμών), στηρίζεται στο αποτέλεσμα που προαναφέραμε, ότι κάθε πραγματικός αριθμός μπορεί να παρασταθεί μοναδικά σε κανονική δεκαδική μορφή. Ένα αποτέλεσμα, του οποίου η απόδειξη στηρίζεται στις ιδιότητες δυναμοσειρών, όπου στο... βάθος υπάρχει η "αρχή του ελαχίστου άνω φράγματος" στους πραγματικούς αριθμούς. Μια περαιτέρω συζήτηση επί του θέματος είναι πέραν του σκοπού του παρόντος.

Υπάρχει μια άλλη απόδειξη ότι το σύνολο των πραγματικών αριθμών είναι υπεραριθμήσιμο, η οποία οφείλεται, και αυτή, στον Cantor (μάλιστα είχε προηγηθεί του διαγωνίου επιχειρήματος).

Η απόδειξη αυτή στηρίζεται σε ένα σημαντικό θεώρημα της Ανάλυσης και γενικότερα της Τοπολογίας.

Για τον ενδιαφερόμενο αναγνώστη παραπέμπουμε στο [1] (Theorem 8.4.7 page 428 και Theorem 8.4.8 page 429).

Πρόταση Β.2.23. *Έστω* $irr\mathbb{R} = \mathbb{R} \setminus \mathbb{Q}$ *το σύνολο των αρρήτων πραγματικών αριθμών. Ισχύει ότι:*

$$irr\mathbb{R} \sim \mathbb{R}.$$

Απόδειξη. Γνωρίζουμε ότι ο $\sqrt{2}$ είναι άρρητος αριθμός (ιδέ Θεώρημα 3.2.8). Ορίζουμε το σύνολο

$$S = \{\sqrt{2}, 2\sqrt{2}, 3\sqrt{2}, \dots, n\sqrt{2}, \dots \mid n \in \mathbb{N}\}.$$

Προφανώς $S \subseteq irr\mathbb{R}$ και $S \sim \mathbb{N}$. Επομένως, το σύνολο $\mathbb{Q} \cup S$ είναι απείρως αριθμήσιμο (γιατί; ιδέ την Πρόταση Β.2.5 και το Θεώρημα Β.2.13). Συνεπώς

$$\mathbb{Q} \cup S \sim S.$$

Από γνωστές ιδιότητες των συνόλων έχουμε ότι

$$\mathbb{R} = \mathbb{Q} \cup irr\mathbb{R} = \mathbb{Q} \cup (S \cup (irr\mathbb{R} \setminus S)) = (\mathbb{Q} \cup S) \cup (irr\mathbb{R} \setminus S) \sim S \cup (irr\mathbb{R} \setminus S) = irr\mathbb{R}. \text{ ό.έ.δ.}$$

Από την προηγουμένη πρόταση συμπεραίνουμε ότι το σύνολο των ρητών αριθμών αποτελεί ένα *αμελητέο* (από άποψη μεγέθους) υποσύνολο των πραγματικών αριθμών.

Πρόταση Β.2.24. *Το σύνολο* $\mathbb{R} \times \mathbb{R}$ *είναι ισοπληθικό με το σύνολο* $\mathbb{R}$. *Οπότε,*

$$\mathbb{R}^n \sim \mathbb{R}, \text{ για όλα τα } n \in \mathbb{N}.$$

Απόδειξη. Από ό,τι έχει προηγηθεί είναι αρκετό να αποδείξουμε ότι

$$(0, 1) \times (0, 1) \sim (0, 1).^{7}$$

Στην Άσκηση B.2.4_{20} δίνεται μια υπόδειξη πώς αποδεικνύεται ο ισχυρισμός.

Οπότε, με επαγωγή αποδεικνύεται ότι

$$\mathbb{R}^n \sim \mathbb{R}, \text{ για όλα τα } n \in \mathbb{N}. \qquad \text{ό.έ.δ.}$$

Β.2.3 Ορισμένα επιπλέον σχόλια στην πληθικότητα συνόλων

Ως γνωστόν, αν $a, b \in \mathbb{N}$ με $a \leq b$ και $b \leq a$, τότε $a = b$.

Κάτι ανάλογο ισχύει και για τις πληθικότητες συνόλων.

Έστω A, B δύο πεπερασμένα σύνολα. Υποθέτουμε ότι υπάρχουν απεικονίσεις

$$f : A \longrightarrow B \text{ και } g : B \longrightarrow A,$$

οι οποίες είναι 1-1, τότε υπάρχει μια απεικόνιση

$$h : A \longrightarrow B,$$

η οποία είναι 1-1 και επί (γιατί; Μα ισχύει η αρχή του περιστεριώνα).

Με τον συμβολισμό του Ορισμού Β.2.16, έχουμε ότι,

$$\text{αν } A \preceq B \text{ και } B \preceq A, \text{ τότε } A \sim B.$$

Όπως είχαμε υπαινιχθεί στην Παρατήρηση Β.2.17, το ίδιο ισχύει για όλα τα σύνολα.

[7] Σε "Γεωμετρική γλώσσα". Το 1×1 τετράγωνο *καλύπτεται* από το διάστημα $(0, 1)$.

Θεώρημα Β.2.25. *(Cantor-Schroeder-Bernstein theorem) Έστω A, B δύο σύνολα. Υποθέτουμε ότι $A \preceq B$ και $B \preceq A$, τότε $A \sim B$.*

Απόδειξη. Πριν παρουσιάσουμε την απόδειξη, θα κάνουμε μια ανάλυση του προβλήματος, η οποία θα κάνει πιο κατανοητή την απόδειξη.

Από την υπόθεση υπάρχουν απεικονίσεις $f : A \longrightarrow B$, και $g : B \longrightarrow B$, οι οποίες είναι 1-1 και ισχύει ότι

$$g(f(A)) \subseteq g(B) \subseteq A.$$

(Σημειώστε ότι οι απεικονίσεις $f : A \longrightarrow B$ και $g : B \longrightarrow A$ δεν είναι, κατ' ανάγκη, η μία αντίστροφη της άλλης).

Αν μπορούσαμε να ορίσουμε μια απεικόνιση $\phi : A \longrightarrow g(B)$, η οποία να είναι 1-1 και επί, τότε θα είχαμε ότι $A \sim g(B)$, αλλά $B \sim g(B)$. Οπότε $A \sim B$ και θα είχαμε τελειώσει.

Μια πρώτη (φυσιολογική) σκέψη για τον ορισμό της απεικόνισης ϕ είναι η εξής: Ορίζουμε

$$\phi(x) = \begin{cases} (g \circ f)(x) & \text{αν } x \in A \setminus g(B) \\ x & \text{αν } x \in g(B) \end{cases}$$

Είναι εύκολο να δούμε ότι η ϕ είναι επί και *επιμέρους* 1-1. Δηλαδή, αν πάρουμε τους περιορισμούς της ϕ στο σύνολο $A \setminus g(B)$ και στο σύνολο $g(B)$, οι περιορισμοί αυτοί είναι 1-1, αλλά αυτό δεν σημαίνει ότι η ϕ είναι 1-1. Το πρόβλημα, που προκύπτει, οφείλεται στο ενδεχόμενο στα σύνολα τιμών $(g \circ f)(A \setminus g(B))$ και $g(B)$ να υπάρχει αλληλοκάλυψη (να έχουν μη κενή τομή).

Για να αρθεί το πρόβλημα αυτό ορίζουμε

$$\begin{aligned} T_0 &= A \setminus g(B), \\ T_1 &= (g \circ f)(T_0), \\ T_2 &= (g \circ f)(T_1) = (g \circ f)^2(T_0) \end{aligned}$$

και αναδρομικά

$$T_n = (g \circ f)^n(T_0).$$

Έστω $T = \bigcup_{n=0}^{\infty} T_n$. Προφανώς (γιατί;) $T \subseteq A$ και

$$(g \circ f)(T) = (g \circ f)(\bigcup_{n=0}^{\infty} T_n) = \bigcup_{n=0}^{\infty} (g \circ f)(T_n) = \bigcup_{n=0}^{\infty} T_{n+1} = \bigcup_{n=1}^{\infty} T_n \subseteq T$$

(εδώ εφαρμόσαμε την Πρόταση 4.5.26).

Επειδή $T_0 = A \setminus g(B) \subseteq T$ έχουμε ότι

$$A \setminus T \subseteq A \setminus T_0 = A \setminus (A \setminus g(B)) = g(B)$$

(γιατί ισχύει η τελευταία ισότητα; Ανατρέξτε στην Παράγραφο 1.1.2.2).

Τώρα ορίζουμε την απεικόνιση $\phi : A \longrightarrow g(B)$ ως εξής:

$$\phi(x) = \begin{cases} (g \circ f)(x) & \text{αν } x \in T \\ x & \text{αν } x \in A \setminus T \end{cases}$$

Προφανώς η ϕ είναι καλώς ορισμένη, δεδομένου ότι

$$(g \circ f)(T) \subseteq (g \circ f)(A) \subseteq g(B) \text{ και } A \setminus T \subseteq g(B).$$

Η ϕ είναι 1-1. Πράγματι, έστω $x, y \in A$ με $\phi(x) = \phi(y)$. Αν $x, y \in T$, τότε

$$\phi(x) = (g \circ f)(x),\ \phi(y) = (g \circ f)(y),$$

αλλά η σύνθεση $g \circ f$ είναι 1-1, συνεπώς $x = y$. Αν $x, y \in A \setminus T$, τότε η υπόθεση $\phi(x) = \phi(y)$ συνεπάγεται $x = y$. Υποθέτουμε ότι $x \in T$ και $y \in A \setminus T$, τότε η υπόθεση $\phi(x) = \phi(y)$ συνεπάγεται

$$(g \circ f)(x) = y \in (g \circ f)(T) \subseteq T,$$

άτοπο. Συνεπώς, δεν είναι δυνατόν να έχουμε $\phi(x) = \phi(y)$ με $x \in T$ και $y \in A \setminus T$. Συμμετρικά δεν είναι δυνατόν να έχουμε $\phi(x) = \phi(y)$ με $y \in T$ και $x \in A \setminus T$. Επομένως, σε όλες τις δυνατές περιπτώσεις η υπόθεση $\phi(x) = \phi(y)$ συνεπάγεται $x = y$, δηλαδή η ϕ είναι 1-1.

Η ϕ είναι επί. Έστω

$$b \in g(B) \subseteq A = (A \setminus T) \cup T.$$

Διακρίνουμε περιπτώσεις. Αν $b \in A \setminus T$, τότε, από τον ορισμό της ϕ έχουμε

$$\phi(b) = b.$$

Αν $b \in T$, επειδή

$$b \notin A \setminus g(B) = T_0,$$

έχουμε ότι $b \in T_n$ για κάποιο $n \geq 1$, αλλά τότε

$$b \in T_n = (g \circ f)(T_{n-1}),$$

αυτό σημαίνει ότι υπάρχει $a \in T_{n-1} \subseteq A$ με

$$b = (g \circ f)(a) = \phi(a).$$

Άρα πάντα υπάρχει $a \in A$ με $\phi(a) = b$, δηλαδή η ϕ είναι επί.

Συνεπώς, κατασκευάσαμε μια απεικόνιση

$$\phi : A \longrightarrow g(B),$$

η οποία είναι 1-1 και επί. Αυτό, όπως επισημάναμε στην αρχή της απόδειξης, αποδεικνύει τον ισχυρισμό του θεωρήματος. ό.έ.δ.

Σχόλιο Β.2.26. Το Θεώρημα Β.2.10 αποτελεί έναν "πρόδρομο", αλλά και ένα πόρισμα του προηγουμένου θεωρήματος. Μπορείτε να το διακρίνετε;

Το προηγούμενο θεώρημα είναι πολύ χρήσιμο για να αποδείξουμε ότι δύο σύνολα είναι ισοπληθικά χωρίς να είμαστε αναγκασμένοι να βρούμε μια απεικόνιση από το ένα σύνολο στο άλλο, η οποία να είναι 1-1 και επί, κάτι που είναι πολύ δύσκολο. Αλλά είναι ευκολότερο να βρούμε επιμέρους απεικονίσεις, οι οποίες να είναι απλώς 1-1.

Ως εφαρμογές του ανωτέρω θεωρήματος θα αναφέρουμε ορισμένες σημαντικές προτάσεις.

Πρόταση Β.2.27. *Έστω a, b πραγματικοί αριθμοί με $a < b$. Τότε ισχύει*

$$[a, b] \sim (a, b).$$

Απόδειξη. Από το Παράδειγμα B.0.4$_2$, έπεται ότι είναι αρκετό να αποδείξουμε τον ισχυρισμό για τα διαστήματα $[-1, 1]$ και $(-1, 1)$.

Ορίζουμε τις εξής απεικονίσεις: $f : (-1, 1) \longrightarrow [-1, 1]$ με

$$f(x) = x,$$

για όλα τα $x \in (-1, 1)$ και $g : [-1, 1] \longrightarrow (-1, 1)$ με

$$g(x) = x/2,$$

για όλα τα $x \in [-1, 1]$. Προφανώς οι f, g είναι 1-1. Συνεπώς

$$(-1, 1) \preceq [-1, 1] \text{ και } [-1, 1] \preceq (-1, 1),$$

οπότε από το προηγούμενο θεώρημα έπεται ότι $[-1, 1] \sim (-1, 1)$. ό.έ.δ.

Πρόταση Β.2.28. *Έστω a, b πραγματικοί αριθμοί με $a < b$. Τότε ισχύει*

$$[a, b) \sim (a, b).$$

Απόδειξη. Από το Παράδειγμα B.0.4$_2$, έπεται ότι είναι αρκετό να αποδείξουμε τον ισχυρισμό για τα διαστήματα $[0, 1)$ και $(0, 1)$.

Ορίζουμε τις εξής απεικονίσεις: $f : (0, 1) \longrightarrow [0, 1)$ με

$$f(x) = x,$$

για όλα τα $x \in (0, 1)$ και $g : [0, 1) \longrightarrow (0, 1)$ με

$$g(x) = \frac{1}{4} + \frac{x}{2},$$

για όλα τα $x \in [0, 1)$. Προφανώς οι f, g είναι 1-1. Συνεπώς

$$[0, 1) \preceq (0, 1) \text{ και } (0, 1) \preceq [0, 1),$$

οπότε από το προηγούμενο θεώρημα έπεται ότι $[0, 1) \sim (0, 1)$. ό.έ.δ.

Με παρόμοια επιχειρήματα μπορούμε να αποδείξουμε ότι όλα τα διαστήματα πραγματικών αριθμών

$$(a, b), (a, b], [a, b), [a, b], [-\infty, b), [-\infty, b], (a, \infty), [a, \infty) \text{ και } (-\infty, \infty) = \mathbb{R}$$

είναι, ανά δύο, ισοπληθικά.

Παρ' όλα ταύτα, αποτελεί "πρόκληση" να βρεθούν απεικονίσεις από διαστήματα της μορφής $[a, b]$ σε διαστήματα της μορφής $[a, b)$ ή από διαστήματα της μορφής $[a, b]$ σε διαστήματα της μορφής $(a, b]$ ή από διαστήματα της μορφής $[a, b]$ σε διαστήματα της μορφής $[a, b)$ ή από διαστήματα της μορφής (a, ∞) σε διαστήματα της μορφής (a, b), οι οποίες να είναι 1-1 και επί. Στην Άσκηση B.2.4$_{19}$ δίνονται τέτοιες απεικονίσεις.

Πρόταση Β.2.29. *Τα σύνολα* $\mathbb{R}$ *και* $\mathcal{P}(\mathbb{N})$ *έχουν την ίδια πληθικότητα* ($\mathbb{R} \sim \mathcal{P}(\mathbb{N})$, *συμβολικά* $2^{\aleph_0} = \mathfrak{c}$).

Απόδειξη. Έχουμε δει ότι $\mathbb{R} \sim (0, 1) \sim [0, 1)$, επομένως, αρκεί να αποδείξουμε ότι

$$\mathcal{P}(\mathbb{N}) \sim [0, 1).$$

Από το Θεώρημα των Cantor-Schroeder-Bernstein (Β.2.25) αρκεί να βρεθούν απεικονίσεις $f : [0, 1) \longrightarrow \mathcal{P}(\mathbb{N})$ και $g : \mathcal{P}(\mathbb{N}) \longrightarrow [0, 1)$, οι οποίες να είναι 1-1.

Για να ορίσουμε τις απεικονίσεις f και g θα χρησιμοποιήσουμε την κανονική δεκαδική παράσταση ενός πραγματικού αριθμού (κάτι ανάλογο κάναμε και στην Πρόταση Β.2.21).

Ορίζουμε την απεικόνιση $\phi : [0, 1) \longrightarrow \mathcal{P}(\mathbb{N} \cup \{0\})$ με

$$\phi(0) = \varnothing$$

και για $b = 0.b_1b_2b_3 \cdots b_k \cdots \in (0, 1)$ ορίζουμε

$$\phi(b) = \{ b_i 10^i \mid i \in \mathbb{N} \}.$$

Η ϕ είναι 1-1. Πράγματι, αν

$$b = 0.b_1b_2b_3 \cdots b_k \cdots \neq c = 0.c_1c_2c_3 \cdots b_k \cdots, \text{ τότε } b_i \neq c_i,$$

για τουλάχιστον έναν δείκτη i. Επομένως, $b_i 10^i \in \phi(b)$, αλλά $b_i 10^i \notin \phi(c)$. Συνεπώς

$$\phi(b) \neq \phi(c).$$

Τώρα, επειδή $\mathcal{P}(\mathbb{N} \cup \{0\}) \sim \mathcal{P}(\mathbb{N})$ (ιδέ Άσκηση Β.2.4_{21}) έπεται ότι υπάρχει απεικόνιση

$$f : [0, 1) \longrightarrow \mathcal{P}(\mathbb{N}),$$

η οποία είναι 1-1.

Ορίζουμε την απεικόνιση $g : \mathcal{P}(\mathbb{N}) \longrightarrow [0, 1)$ ως εξής:

$$g(\varnothing) = 0$$

και για κάθε μη κενό υποσύνολο $X \in \mathcal{P}(\mathbb{N})$ ορίζουμε

$$g(X) = 0.b_1b_2b_3 \cdots b_k \cdots,$$

όπου $b_i = 1$, αν $i \in X$ και $b_i = 0$, αν $i \notin X$.

Η g είναι 1-1. Πράγματι, αν $X \neq Y$, τότε υπάρχει τουλάχιστον ένας αριθμός k με $k \in X$ και $k \notin Y$. Τότε όμως

$$g(X) = 0.b_1b_2b_3 \cdots b_k \cdots \text{ και } g(Y) = 0.c_1c_2c_3 \cdots c_k \cdots$$

με $b_k = 1 \neq 0 = c_k$. Συνεπώς $g(X) \neq g(Y)$.

Άρα πληρούνται οι υποθέσεις του Θεωρήματος των Cantor-Schroeder-Bernstein, επομένως πράγματι $\mathbb{R} \sim \mathcal{P}(\mathbb{N})$. ό.έ.δ.

Για να κατανοήσουμε τον τρόπο ορισμού των απεικονίσεων ϕ και g, κάποια παραδείγματα, ίσως, είναι χρήσιμα.

$$\begin{aligned}
\phi(0.103) = \phi(0.10300\bar{0}) &= \{1 \cdot 10,\ 0 \cdot 10^2 \cdot 0,\ 3 \cdot 10^3,\ 0 \cdot 10^4,\ \dots\} \\
&= \{0,\ 10,\ 3000\}, \\
\phi(0.\bar{1}\cdots) &= \{10,\ 10^2,\ 10^3,\ \dots\}. \\
g(\{1,\ 2,\ 3\}) &= 0.111 = 0.111\bar{0}\cdots, \\
g(\{2,\ 4,\ 6,\ 8,\ \dots\}) &= 0.01010101\cdots, \\
g(\mathbb{N}) &= 0.\bar{1}\cdots.
\end{aligned}$$

Από το Θεώρημα B.2.18 έχουμε ότι

$$card(\mathbb{N}) < card(\mathcal{P}(\mathbb{N})).$$

Από την Πρόταση B.2.29 έχουμε ότι

$$card(\mathcal{P}(\mathbb{N})) = card(\mathbb{R}).$$

Επομένως, γεννάται το ερώτημα: Η πληθικότητα $\mathfrak{c} = card(\mathbb{R})$ είναι η *αμέσως μεγαλύτερη* της πληθικότητας $\aleph_0 = card(\mathbb{N})$; Δηλαδή

υπάρχει άπειρο σύνολο X με πληθικότητα γνησίως μεταξύ $\aleph_0$ και $\mathfrak{c}$

$$(\mathbb{N} \prec X \prec \mathbb{R});$$

Το ερώτημα αυτό ετέθη από τον Cantor περί το 1880. Προσπάθησε να βρει ένα τέτοιο σύνολο, αλλά εστάθη αδύνατον και είκασε ότι δεν υπάρχει σύνολο με την ανωτέρω ιδιότητα. Η εικασία αυτή έγινε γνωστή ως ***Υπόθεση του συνεχούς*** και αποτέλεσε ένα από τα περίφημα προβλήματα των σύγχρονων Μαθηματικών.

Με συνδυασμό των εργασιών των K. Goedel (1938) και P. Cohen (1963) αποδεικνύεται ότι η υπόθεση του συνεχούς είναι ανεξάρτητη από τα κλασικά αξιώματα της Θεωρίας Συνόλων (Zermelo-Fraenkel axioms)[8]. Αυτό σημαίνει ότι η υπόθεση του συνεχούς δεν μπορεί να αποδειχθεί ότι ισχύει, ούτε μπορεί να αποδειχθεί ότι δεν ισχύει με το αποδεκτό αξιωματικό σύστημα της Θεωρίας συνόλων. Επομένως, είτε πρέπει να αποδεχθούμε ότι δεν μπορούμε να απαντήσουμε στην εικασία αυτή ή πρέπει να επινοήσουμε μια άλλη αξιωματική θεμελίωση των συνόλων. Πάντως, επειδή είναι ανεξάρτητη από τα κλασικά αξιώματα της Θεωρίας Συνόλων, είτε την αποδεχθούμε ή την απορρίψουμε, δεν αποτελεί κάποια αντίφαση και για τον λόγο αυτόν, δεδομένου ότι το αποδεκτό αξιωματικό σύστημα της Θεωρίας Συνόλων "λειτουργεί καλά", η πλειονότητα της επιστημονικής κοινότητας απεφάσισε να συμβιώσει με την περίεργη κατάσταση σχετικά με την υπόθεση του συνεχούς.

B.2.4 Ασκήσεις

1. Να απαντήσετε, με κάθε λεπτομέρεια, στα (γιατί;), που αναφέρονται στην απόδειξη της Πρότασης B.1.4.

2. Να αποδείξετε, με κάθε λεπτομέρεια, το Πόρισμα B.1.5.

[8] Οι εργασίες των Goedel και Cohen δεν είναι κατανοητές από...*κοινούς Μαθηματικούς*.

3. Να αποδείξετε, με κάθε λεπτομέρεια, το Πόρισμα B.1.6.

4. i. Να αποδείξετε, με κάθε λεπτομέρεια, την Πρόταση B.1.11.

   ii. Να γενικεύσετε και να αποδείξετε το προηγούμενο ερώτημα. Συγκεκριμένα:

   Έστω $A_1, A_2, \ldots, A_n$ πεπερασμένα σύνολα. Το πλήθος των στοιχείων της ένωσης $A_1 \cup A_2 \cup \cdots \cup A_n$ μπορεί να υπολογισθεί προσθέτοντας το πλήθος όλων των τομών συνόλων από τα A_i με περιττό το πλήθος όρους και αφαιρώντας το πλήθος όλων των τομών συνόλων από τα A_i με άρτιο το πλήθος όρους.

   Να διατυπώσετε την ισότητα, η οποία περιγράφεται ανωτέρω και μετά να την αποδείξετε με επαγωγή επί του πλήθους n των συνόλων που μετέχουν στην ένωση[9].

5. Εφαρμόστε την αρχή του περιστεριώνα για να αποδείξετε τους ακόλουθους ισχυρισμούς:

   i. Σε οποιοδήποτε σύνολο ακεραίων αριθμών με $n+1$ το πλήθος στοιχεία υπάρχουν δύο στοιχεία των οποίων η διαφορά διαιρείται με το n.

   ii. Έστω $S = \{a_1, a_2, \ldots, a_n\}$ ένα σύνολο ακεραίων αριθμών. Υπάρχει μη κενό υποσύνολο του S, του οποίου το άθροισμα των στοιχείων του διαιρείται με το n.

   iii. Από το σύνολο $\{1, 2, 3, \ldots, 200\}$ επιλέγουμε 101 το πλήθος στοιχεία. Υπάρχουν, τουλάχιστον δύο, αριθμοί, όπου ο ένας είναι πολλαπλάσιο του άλλου.

   iv. Σε ένα σύνολο φυσικών με 7 στοιχεία υπάρχουν δύο στοιχεία των οποίων το άθροισμα ή η διαφορά διαιρείται με το 10.

   v. Σε μια επιφάνεια σφαίρας βρίσκονται τυχαία κατανεμημένα πέντε σημεία. Υπάρχει ένα ημισφαίριο, στο οποίο βρίσκονται τα τέσσερα από τα πέντε σημεία (Θεωρείται γνωστό τι σημαίνει ημισφαίριο και ότι σε ένα ημισφαίριο ανήκει ο μέγιστος κύκλος που το καθορίζει).

   vi. Δίνεται ένα τετράγωνο με πλευρά 1 μονάδα. Στο εσωτερικό του επιλέγουμε πέντε τυχαία σημεία. Τουλάχιστον δύο από αυτά απέχουν μεταξύ τους το πολύ $\frac{\sqrt{2}}{2}$ μονάδες.

6. Δείξτε ότι το Πόρισμα B.1.6, θα μπορούσε να (ανα)διατυπωθεί ως εξής:

   "Αν το σύνολο A είναι άπειρο και $A \subseteq B$, τότε το B είναι άπειρο."

7. Δείξτε ότι το Πόρισμα B.1.8, θα μπορούσε να (ανα)διατυπωθεί ως εξής:

   "Αν ένα σύνολο A είναι ισοπληθικό με ένα γνήσιο υποσύνολό του, τότε είναι άπειρο."

8. Δείξτε ότι στο Πόρισμα B.1.8 ισχύει και η αντίστροφη κατεύθυνση. Δηλαδή,

   Ένα σύνολο είναι πεπερασμένο, αν και μόνο αν δεν είναι ισοπληθικό με κάθε ένα από τα γνήσια υποσύνολά του.

[9] Η ισότητα αυτή αναφέρεται ως η "*Αρχή της ένταξης-αποκλεισμού*".

9. Έστω A, B δύο πεπερασμένα σύνολα και $f : A \longrightarrow B$ μια απεικόνιση.

   Δείξτε ότι κάθε δύο από τις ακόλουθες προτάσεις συνεπάγονται την τρίτη.

   i. Τα σύνολα A και B είναι ισοπληθικά.

   ii. Η απεικόνιση f είναι 1-1.

   iii. Η απεικόνιση f είναι επί.

10. Δείξτε, με κάθε λεπτομέρεια, την Πρόταση B.2.3 και το Πόρισμα B.2.4.

11. Να ολοκληρώσετε την απόδειξη της Πρότασης B.2.5.

12. Να αποδείξετε την εξής γενίκευση της Πρότασης B.2.5.

    Έστω $A_1, A_2, \ldots, A_n$ αριθμήσιμα σύνολα. Η ένωση $\bigcup_{i=1}^{n} A_i$ είναι αριθμήσιμο σύνολο.

13. Δείξτε ότι η απεικόνιση $g : \mathbb{N} \times \mathbb{N} \longrightarrow N$ με

$$g(m, n) = 2^{m-1}(2n - 1)$$

    είναι 1-1 και επί. Άρα έχουμε μια άλλη απόδειξη της Πρότασης B.1.13.

14. Να αποδείξετε, με κάθε λεπτομέρεια, το Πόρισμα B.2.12.

15. Έστω $\mathcal{F}$ το σύνολο όλων των πεπερασμένων υποσυνόλων του $\mathbb{N}$. Είναι το $\mathcal{F}$ αριθμήσιμο;

    Υπόδειξη. Έστω $p_1 < p_2 < \cdots < p_n < \cdots$, ακολουθία των πρώτων (κατά αύξουσα σειρά). Έστω $X = \{r_1, r_2, \ldots, r_k\}$ (με $r_i < r_{i+1}$) ένα στοιχείο του $\mathcal{F}$. Ορίζουμε την εξής απεικόνιση $f : \mathcal{F} \longrightarrow \mathbb{N}$ ως εξής:

$$f(X) = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} \text{ και } f(\emptyset) = 1.$$

    Εξετάστε αν η f είναι 1-1.

16. Να αποδείξετε, με κάθε λεπτομέρεια, την Πρόταση B.2.20.

17. Εξετάστε αν είναι σωστοί ή λάθος οι ακόλουθοι ισχυρισμοί:

    i. Έστω A, B, C σύνολα με τα A, C απείρως αριθμήσιμα και $A \subseteq B \subseteq C$. Το B είναι απείρως αριθμήσιμο.

    ii. Έστω A, B σύνολα με το A απείρως αριθμήσιμο και το B υπεραριθμήσιμο. Αν $A \subseteq B$, τότε το $B \setminus A$ είναι υπεραριθμήσιμο.

    iii. Έστω A, B σύνολα και $f : A \longrightarrow B$, $g : A \longrightarrow B$ με την f 1-1 και την g επί. Τότε υπάρχει $h : A \longrightarrow B$ απεικόνιση, η οποία είναι 1-1 και επί.

18. i. Δώστε ένα παράδειγμα συνόλων A, B, C με $A \sim B$, αλλά $A \cup C \nsim B \cup C$.

    ii. Έστω A, B, C με $A \sim B$ σύνολα με $A \cap C = \emptyset$ και $B \cap C = \emptyset$. Δείξτε ότι $A \cup C \sim B \cup C$.

    iii. Έστω A, B, C με $A \sim B$. Υποθέτουμε ότι $A \cup C \sim B \cup C$ και ότι $A \cap C = \emptyset$ και $B \cap C = \emptyset$. Είναι αληθές ότι $A \sim B$;

19. i. Θεωρούμε το σύνολο

$$S = \left\{ \frac{1}{n} \mid n \in \mathbb{N} \right\} \subset [0, 1].$$

Ορίζουμε την απεικόνιση $f : [0, 1] \longrightarrow [0, 1)$ με

$$f(x) = x, \text{ για } x \in [0, 1] \setminus S \text{ και } f\left(\frac{1}{n}\right) = \frac{1}{n+1}, \text{ για } \frac{1}{n} \in S.$$

Δείξτε ότι η f είναι 1-1 και επί. Συνεπώς, $[0, 1] \sim [0, 1)$.

ii. Θεωρούμε το σύνολο

$$T = \left\{ 1 - \frac{1}{n} \mid n \in \mathbb{N} \right\} \subset [0, 1).$$

Ορίζουμε την απεικόνιση $g : [0, 1) \longrightarrow (0, 1)$ με

$$g(x) = x, \text{ για } x \in [0, 1) \setminus T \text{ και } g\left(1 - \frac{1}{n}\right) = 1 - \frac{1}{n+1}, \text{ για } 1 - \frac{1}{n} \in T.$$

Δείξτε ότι η g είναι 1-1 και επί. Συνεπώς, $[0, 1) \sim (0, 1)$.

iii. Θεωρούμε την απεικόνιση $g \circ f : [0, 1] \longrightarrow (0, 1)$. Προφανώς η σύνθεση αυτή είναι 1-1 και επί. Συνεπώς, $[0, 1] \sim (0, 1)$.

iv. Δείξτε ότι

$$(0, \infty) \sim (0, 1),$$

αποδεικνύοντας ότι η απεικόνιση $g : (0, \infty) \longrightarrow (0, 1)$ με

$$g(x) = \frac{x}{x+1},$$

για όλα τα $x \in (0, \infty)$ είναι 1-1 και επί.

20. Έστω $S = (0, 1) \times (0, 1)$ και $T = (0, 1)$. Δείξτε ότι $S \sim T$.

Υπόδειξη. Έστω $(a, b) \in S$ με

$$a = 0.a_1a_2a_3 \cdots a_k \cdots \text{ και } b = 0.b_1b_2b_3 \cdots b_k \cdots$$

σε κανονική δεκαδική μορφή. Ορίζουμε την απεικόνιση $f : S \longrightarrow T$ ως εξής:

$$f(a, b) = 0.a_1b_1a_2b_2a_3b_3 \cdots a_kb_k \cdots.$$

Δείξτε ότι η f είναι 1-1, (αλλά όχι επί). Εφαρμόστε το Θεώρημα B.2.25.[10]

21. Έστω A, B δύο σύνολα. Αν $A \sim B$, τότε ισχύει ότι $\mathcal{P}(A) \sim \mathcal{P}(B)$.

22. Έστω A_n, $n \in \mathbb{N}$ το σύνολο των ριζών όλων των πολυωνύμων βαθμού n και με συντελεστές από το σώμα των ρητών αριθμών. Δείξτε ότι το A_n είναι απείρως αριθμήσιμο σύνολο (ιδέ Πόρισμα Γ.3.20).

23. Δείξτε ότι το σύνολο $B = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$ είναι ισοπληθικό με το $\mathbb{R}^2$.

24. Να συμπληρώσετε τα κενά στην απόδειξη του Θεωρήματος B.2.15.

[10] Το αποτέλεσμα αυτό απεδείχθη από τον G. Cantor και όταν το γνωστοποίησε, με επιστολή το 1877, στον R. Dedekind έγραψε "I see it but I do not believe it."

Βιβλιογραφία

[1] E.D. Bloch. *Proofs and Fundamentals: A first course in Abstract Mathematics*. Second Edition, Springer, 2011. ISBN: 978-14-4197-126-5.

[2] Herbert B. Enderton. *Elements of Set Theory*. Academic Press, 1977. ISBN: 978-01-2238-440-0.

[3] P. Halmos. *Naive Set Theory*. Springer, 1974. ISBN: 978-0-387-90104-6.

[4] Richard Hammack. *Book of Proof*. Edition 2.2. Virginia Commonwealth University Richard Hammack (publisher). Department of Mathematics and Applied Mathematics, 2013.

[5] Steven G. Krantz. *The Elements of Advanced Mathematics*. Fourth Edition. Textbooks in mathematics. CRC Press Taylor and Francis Group, 2018. ISBN: 978-11-3850-631-2.

[6] M. Liebeck. *A Concise Introduction to Pure Mathematics*. Third Edition. Chapman Hall CRC Press, 2011. ISBN: 978-14-3983-598-2.

[7] Γιάννης Ν. Μοσχοβάκης. *Σημειώσεις στη Συνολοθεωρία*. Προκαταρκτική 2η έκδοση. http://www.math.ucla.edu/~ynm/lectures/g.pdf, 2014.

ΠΑΡΑΡΤΗΜΑ Γ

ΜΙΑ ΕΚ ΝΕΟΥ "ΕΠΙΣΚΕΨΗ" ΣΤΙΣ ΟΜΑΔΕΣ ΚΑΙ ΤΟΥΣ ΔΑΚΤΥΛΙΟΥΣ

Στο πέμπτο Κεφάλαιο είχαμε αναφερθεί στην έννοια της ομάδας και του δακτυλίου, αλλά εκεί, πέραν των ορισμών, κάποιων στοιχειωδών ιδιοτήτων και κάποιων παραδειγμάτων δεν είχαμε επεκταθεί.

Εδώ θα αναφέρουμε κάποιες σημαντικές κατηγορίες ομάδων και δακτυλίων, όπως και κάποιες επιπλέον ιδιότητες.

Στο τέλος θα αναφερθούμε στους ομομορφισμούς ομάδων και στους ομομορφισμούς δακτυλίων.

Γ.1 Μερικές αξιοσημείωτες κατηγορίες ομάδων

Γ.1.1 Κυκλικές ομάδες

Ας ξεκινήσουμε με δύο παραδείγματα.

i. Έστω G μια ομάδα και $a \in G$. Το σύνολο $\langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$ είναι προφανώς υποομάδα της G.

   Είναι το Παράδειγμα 5.1.27$_6$. Εκεί είχαμε αναφέρει ότι:

   Η υποομάδα αυτή ονομάζεται η **κυκλική** υποομάδα η παραγομένη από το στοιχείο a.

ii. Έστω $(\mathbb{Z}, +)$ η προσθετική ομάδα των ακεραίων. Παρατηρούμε ότι, για κάθε ακέραιο αριθμό n, ισχύει $n = n \cdot 1$. Δηλαδή, κάθε ακέραιος αριθμός είναι πολλαπλάσιο του 1 (έχουμε τον προσθετικό συμβολισμό).

Και στα δύο αυτά παραδείγματα βλέπουμε ότι έχουμε ομάδες, για τις οποίες

υπάρχει ένα στοιχείο τους, ούτως ώστε κάθε άλλο στοιχείο τους να είναι δύναμη (πολλαπλάσιο) αυτού του στοιχείου.

Ορισμός Γ.1.1. Μία ομάδα G θα ονομάζεται **κυκλική**, αν υπάρχει ένα στοιχείο $a \in G$, ούτως ώστε, για κάθε $g \in G$, να υπάρχει ένας ακέραιος r με την ιδιότητα $g = a^r$ [1]. Το στοιχείο a θα ονομάζεται **γεννήτορας** της κυκλικής ομάδας G και θα συμβολίζουμε

$$G = \langle a \rangle.$$

Από τον ορισμό απορρέει ότι σε μια κυκλική ομάδα $\langle a \rangle$ τα στοιχεία της θα είναι της μορφής a^r με $r \in \mathbb{Z}$. Δηλαδή,

$$\langle a \rangle = \{\cdots a^{-2}, a^{-1}, a^0 = 1, a^1 = a, a^2, \cdots\}.$$

Το ερώτημα που προκύπτει είναι το εξής:

> Είναι όλες οι δυνάμεις a^r διαφορετικές μεταξύ τους; Ισοδύναμα, υπάρχουν $r, s \in \mathbb{Z}$ με $r \neq s$, αλλά $a^r = a^s$;

Ορισμός Γ.1.2. Έστω G μια ομάδα και $g \in G$. Ο μικρότερος θετικός ακέραιος n, αν υπάρχει τέτοιος αριθμός, με την ιδιότητα

$$g^n = 1_G$$

(με προσθετικό συμβολισμό $ng = 0$), θα ονομάζεται **τάξη** του στοιχείου g και θα συμβολίζεται $o(g)$. Στην περίπτωση, όπου δεν υπάρχει τέτοιος ακέραιος, τότε το στοιχείο g θα ονομάζεται άπειρης τάξης ($o(g) = \infty$).

Για παράδειγμα: Στην προσθετική ομάδα των ακεραίων αριθμών $(\mathbb{Z}, +)$ για κάθε μη μηδενικό στοιχείο a έχουμε ότι $na \neq 0$, για όλους του θετικούς ακεραίους. Συνεπώς, όλα τα μη μηδενικά στοιχεία της $(\mathbb{Z}, +)$ είναι άπειρης τάξης.

Προφανώς, σε μια ομάδα, το μόνο στοιχείο το οποίο έχει τάξη ίση με 1 είναι το ουδέτερο στοιχείο της ομάδας.

Θεώρημα Γ.1.3. *Έστω G μια ομάδα και $g \in G$.*

Υποθέτουμε ότι το g έχει άπειρη τάξη. Τότε ισχύει

$$g^n = g^m, \text{ αν και μόνο αν } n = m.$$

Υποθέτουμε ότι το g έχει πεπερασμένη τάξη. Τότε

$$g^n = g^m, \text{ αν και μόνο αν η τάξη του } g \text{ διαιρεί την διαφορά } n - m.$$

Απόδειξη. Αν το g έχει άπειρη τάξη. Από την σχέση $g^n = g^m$ έπεται ότι $g^{n-m} = 1_G$. Αλλά το g έχει άπειρη τάξη, άρα, αναγκαστικά, $n - m = 0$, δηλαδή $n = m$.

Υποθέτουμε ότι το g έχει πεπερασμένη τάξη, έστω $o(g) = k$. Από τον αλγόριθμο της διαίρεσης ακεραίων αριθμών έχουμε ότι υπάρχουν ακέραιοι αριθμοί π και υ, ούτως ώστε $n - m = \pi k + \upsilon$ και $0 \leq \upsilon < k$.

Από την σχέση $g^n = g^m$ έχουμε ότι $g^{n-m} = 1_G$. Συνεπώς,

$$g^{n-m} = g^{\pi k + \upsilon} = g^{\pi k} \cdot g^{\upsilon} = (g^k)^{\pi} \cdot g^{\upsilon} = 1_G.$$

Δεδομένου ότι $g^k = 1_G$, έπεται ότι $g^{\upsilon} = 1_G$. Από την τελευταία σχέση έπεται ότι, αναγκαστικά, $\upsilon = 0$ (γιατί;). Άρα πράγματι η τάξη του στοιχείου g διαιρεί την διαφορά $n - m$. Το αντίστροφο είναι προφανές. ό.έ.δ.

[1] Χρησιμοποιούμε τον πολλαπλασιαστικό συμβολισμό. Στην περίπτωση του προσθετικού συμβολισμού θα έχουμε $g = ra$.

Πόρισμα Γ.1.4. *Έστω G μια ομάδα και $g \in G$ με πεπερασμένη τάξη $o(g) = k$. Τότε για την κυκλική υποομάδα την παραγομένη από το g έχουμε ότι*

$$\langle g \rangle = \{1_G, g, g^2 \cdots g^{k-1}\}.$$

Συνεπώς, $|\langle g \rangle| = o(g)$.

Απόδειξη. Για κάθε $a \in \langle g \rangle$ | υπάρχει ακέραιος r, ώστε $a = g^r$. Τα δυνατά υπόλοιπα της διαίρεσης του r με τον k είναι τα $0, 1, 2, \ldots, k-1$. Οπότε, πράγματι $a \in \{1_G, g, g^2 \cdots g^{k-1}\}$ (γιατί;). ό.έ.δ.

Παρατηρήσεις Γ.1.5. Από τα προηγούμενα έπεται ότι έχουμε δύο "είδη" κυκλικών ομάδων:

Τις πεπερασμένες κυκλικές ομάδες, οι οποίες είναι της μορφής

$$C_n = \langle a \mid a^n = 1 \rangle = \{a^0 = 1, a, a^2 \cdots a^{n-1}\},$$

όπου n είναι η τάξη του γεννήτορα a.

Τις άπειρες κυκλικές

$$C_\infty = \langle a \rangle = \{\cdots a^{-2}, a^{-1}, a^0 = 1, a^1 = a, a^2, \cdots\},$$

όπου ο γεννήτορας a είναι άπειρης τάξης.

Ένα παράδειγμα άπειρης κυκλικής ομάδας είναι η προσθετική ομάδα $(\mathbb{Z}, +)$ των ακεραίων αριθμών με γεννήτορα το 1. Καθότι για κάθε θετικό ακέραιο αριθμό n έχουμε ότι

$$n = n \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{n}.$$

Επίσης, από τα προηγούμενα, θεώρημα και πόρισμα, έπεται ότι η πράξη μεταξύ των στοιχείων μιας πεπερασμένης κυκλικής ομάδας $\langle a \mid a^n = 1 \rangle$ "μεταφέρεται" στην πρόσθεση εκθετών $mod\, n$. Δηλαδή

$$a^i a^j = a^{i+j} = a^k, \text{ όπου } i + j \equiv k mod\, n.$$

Για την "Αριθμητική $mod\, n$", θα αναφερθούμε διεξοδικά στην Παράγραφο Γ.2.1.

Όπως βλέπουμε, σε μια ομάδα, όταν έχουμε ένα στοιχείο a πεπερασμένης τάξης n, δεν χρειάζεται να χρησιμοποιούμε αρνητικούς εκθέτες, αφού ισχύει ότι

$$a^{-1} = a^{n-1}, a^{-2} = a^{n-2} \ldots \text{ (γιατί;)}.$$

Πρόταση Γ.1.6. *Έστω G μια ομάδα και $a \in G$ πεπερασμένης τάξης n, τότε για κάθε θετικό ακέραιο k ισχύει ότι:*

$$\langle a^k \rangle = \langle a^d \rangle \text{ και } o(a^k) = \frac{n}{d}, \text{ όπου } d = \text{μ.κ.δ.}(n, k).$$

Απόδειξη. Επειδή ο d διαιρεί τον k, έχουμε ότι $\langle a^k \rangle \subseteq \langle a^d \rangle$ (γιατί;). Από την Πρόταση 6.1.21 έχουμε ότι υπάρχουν ακέραιοι αριθμοί μ, ν, έτσι ώστε $d = \mu n + \nu k$. Επομένως,

$$a^d = a^{\mu n + \nu k} = (a^n)^\mu \cdot (a^k)^\nu = (a^k)^\nu \in \langle a^k \rangle.$$

Συνεπώς $\langle a^k \rangle \supseteq \langle a^d \rangle$. Άρα $\langle a^k \rangle = \langle a^d \rangle$.

Για το δεύτερο μέρος της πρότασης, παρατηρούμε ότι για κάθε διαιρέτη δ του n ισχύει ότι $o(a^\delta) = n/\delta$. Πράγματι, έχουμε ότι $(a^\delta)^{n/\delta} = 1$, άρα $o(a^\delta) \leq n/\delta$. Επίσης, έχουμε ότι

$$(a^\delta)^{o(a^\delta)} = 1,$$

δηλαδή $\delta \cdot o(a^\delta) \geq o(a) = n$ (γιατί;). Συνεπώς, σε συνδυασμό με την προηγουμένη ανισότητα, έχουμε ότι $o(a^\delta) = n/\delta$.

Οπότε, στην ειδική περίπτωση, όπου ο διαιρέτης του n είναι ο $d = \mu.κ.δ.(n, k)$, έπεται ότι

$$o(a^k) = |\langle a^k \rangle| = |\langle a^d \rangle| = o(a^d) = \frac{n}{d}.$$ ό.έ.δ.

Πόρισμα Γ.1.7. *Έστω a ένα στοιχείο μιας ομάδας G με $o(a) = n$. Τότε ισχύει*

$$\langle a^i \rangle = \langle a^j \rangle \text{ αν και μόνο αν } \mu.κ.δ.(n, i) = \mu.κ.δ.(n, j).$$

Απόδειξη. Από την προηγουμένη πρόταση έχουμε ότι

$$\langle a^i \rangle = \langle a^{\mu.κ.δ.(n,i)} \rangle$$

και

$$\langle a^j \rangle = \langle a^{\mu.κ.δ.(n,j)} \rangle.$$

Συνεπώς, πρέπει και αρκεί να αποδείξουμε ότι

$$\langle a^{\mu.κ.δ.(n,i)} \rangle = \langle a^{\mu.κ.δ.(n,j)} \rangle, \text{ αν και μόνο } \mu.κ.δ.(n, i) = \mu.κ.δ.(n, j).$$

Οπότε, πάλι από την προηγουμένη πρόταση, πρέπει και αρκεί να αποδείξουμε ότι

$$n/\mu.κ.δ.(n, i) = n/\mu.κ.δ.(n, j),$$

το οποίο ισχύει αν και μόνο αν

$$\mu.κ.δ.(n, i) = \mu.κ.δ.(n, j).$$ ό.έ.δ.

Μια σημαντική ειδική περίπτωση του προηγουμένου πορίσματος είναι το εξής:

Θεώρημα Γ.1.8. *Έστω a ένα στοιχείο μιας ομάδας G με $o(a) = n$. Τότε ισχύει*

$$\langle a \rangle = \langle a^k \rangle, \text{ αν και μόνο αν } o(a) = o(a^k), \text{ αν και μόνο αν } \mu.κ.δ.(n, k) = 1.$$

Η σημασία του προηγουμένου αποτελέσματος είναι μεγάλη (για τον λόγο αυτόν αναφέρεται ως θεώρημα), καθ' ότι σε μία πεπερασμένη κυκλική ομάδα, γνωρίζοντας έναν γεννήτορά της, μπορούμε να υπολογίσουμε όλους τους υπολοίπους.

Δηλαδή, το πρόβλημα για τον υπολογισμό των γεννητόρων μιας κυκλικής ομάδας με τάξη ίση με n είναι ισοδύναμο με τον υπολογισμό των θετικών ακεραίων $1 \leq k \leq n$, οι οποίοι είναι πρώτοι προς τον n.

Αλλά, ως γνωστόν (ιδέ Παράγραφο 6.1.2.5), το πλήθος των θετικών ακεραίων των μικροτέρων του n και πρώτων προς τον n είναι η τιμή $\varphi(n)$ της συνάρτησης του Euler.

Συνεπώς, βλέπουμε ότι ένα ομαδοθεωρητικό πρόβλημα είναι αλληλένδετο με ένα αριθμοθεωρητικό πρόβλημα. Επ' αυτού δεν θα επεκταθούμε περισσότερο. Απλώς θα αναφέρουμε μερικά σημαντικά αποτελέσματα υπό μορφή απλών ασκήσεων[2].

[2]Εδώ βλέπουμε, για άλλη μια φορά, ότι στα Μαθηματικά δεν ισχύει ο συσχετισμός "δύσκολο,...άρα σημαντικό".

Στην περίπτωση μιας άπειρης κυκλικής ομάδας

$$\langle a \rangle = \{\cdots, a^{-2}, a^{-1}, a^0 = 1, a, a^2, \cdots, \},$$

οι μόνοι γεννήτορες είναι οι a και a^{-1}. Πράγματι, αν a^k είναι ένας γεννήτορας της $\langle a \rangle$, τότε θα πρέπει $a = (a^k)^\mu$, για κάποιο ακέραιο μ, αλλά τότε αναγκαστικά $1 = k \cdot \mu$ (δεν ξεχνάμε το Θεώρημα Γ.1.3), άρα $k = \pm 1$.

Θα κλείσουμε την παράγραφο με ένα σημαντικό θεώρημα κατάταξης των υποομάδων μιας κυκλικής ομάδας.

Θεώρημα Γ.1.9. *Κάθε υποομάδα μιας κυκλικής ομάδας είναι κυκλική.*

Στην περίπτωση μιας άπειρης κυκλικής ομάδας, κάθε μη τετριμμένη υποομάδα είναι άπειρη κυκλική. Μάλιστα δε για κάθε θετικό ακέραιο αριθμό n υπάρχει μοναδική υποομάδα με δείκτη ίσον με n.

Στην περίπτωση μιας πεπερασμένης κυκλικής ομάδας τάξης n για κάθε διαιρέτη k του n υπάρχει μοναδική υποομάδα με τάξη ίση με k και δείκτη ίσον με n/k.

Απόδειξη. Έστω $G = \langle a \rangle$ και H μια υποομάδα της. Αν η H είναι τετριμμένη, τότε προφανώς είναι κυκλική. Υποθέτουμε ότι η H είναι μη τετριμμένη, τότε κάθε στοιχείο της είναι της μορφής a^r, αφού είναι και στοιχείο της κυκλικής ομάδας G. Δεδομένου δε ότι η H είναι ομάδα (άρα, αν περιέχει ένα στοιχείο, θα περιέχει και το αντίστροφό του), θα περιέχει στοιχεία της μορφής a^r με τον εκθέτη r θετικό ακέραιο. Έστω m ο μικρότερος θετικός ακέραιος, ώστε $a^m \in H$.

Ισχυρισμός: Κάθε άλλο στοιχείο της H είναι της μορφής a^k με το k πολλαπλάσιο του m.

Πράγματι, από τον αλγόριθμο της διαίρεσης έχουμε ότι υπάρχουν ακέραιοι π, υ με

$$k = \pi\, m + \upsilon \text{ και } 0 \leq \upsilon < m.$$

Επομένως έχουμε

$$a^\upsilon = a^{k+(-\pi)m} = a^k \cdot (a^m)^{-\pi} \in H$$

(γιατί;). Αυτό είναι άτοπο, εκτός εάν $\upsilon = 0$, διότι υποθέσαμε ότι ο m είναι ο μικρότερος θετικός ακέραιος, ώστε $a^m \in H$. Άρα απεδείχθη ο ισχυρισμός. Συνεπώς πράγματι, η H είναι κυκλική με $H = \langle a^m \rangle$.

Υποθέτουμε ότι η ομάδα $G = \langle a \rangle$ είναι άπειρη κυκλική, τότε, για κάθε θετικό ακέραιο αριθμό n, η υποομάδα $H = \langle a^n \rangle$ είναι μοναδική (δεν ξεχνάμε ότι στην περίπτωση των απείρων κυκλικών ομάδων $a^m = a^n$, αν και μόνο αν $m = n$). Επιπλέον, ο δείκτης της H στην G είναι ίσος με n. Δεδομένου ότι τα διαφορετικά σύμπλοκα της H στην G είναι τα $1 \cdot H$, $a \cdot H$, ..., $a^{n-1} \cdot H$ (Για τον ορισμό του δείκτη υποομάδας σε ομάδα και τον ορισμ;ο του συμπλόκου, ιδέ την Παράγραφο 5.1.2.3).

Υποθέτουμε ότι η ομάδα $G = \langle a \rangle$ είναι πεπερασμένη κυκλική με τάξη ίση με n. Έστω H μια υποομάδα της G, έχουμε ήδη αποδείξει ότι $H = \langle a^m \rangle$ με τον m να είναι ο μικρότερος θετικός ακέραιος, έτσι ώστε $a^m \in H$. Το αποτέλεσμα τώρα έπεται από την Πρόταση Γ.1.6, με τις λεπτομέρειες να αφήνονται ως άσκηση. ό.έ.δ.

Παράδειγμα Γ.1.10. Έστω $G = \langle a \rangle$ μια κυκλική ομάδα με τάξη ίση με 30. Οι θετικοί διαιρέτες του τριάντα είναι οι $1, 2, 3, 5, 6, 10, 15, 30$. Από το προηγούμενο θεώρημα έχουμε ότι υπάρχουν οκτώ υποομάδες της ομάδας G με τις αντίστοιχες τάξεις (συμπεριλαμβανομένων της τετριμμένης ομάδας και ομάδας G) και αντίστοιχους δείκτες $30, 15, 10, 6, 5, 3, 2, 1$.

Δεν θα επεκταθούμε περισσότερο στην μελέτη των κυκλικών ομάδων, διότι κάτι τέτοιο είναι πέραν του σκοπού αυτού του βιβλίου.

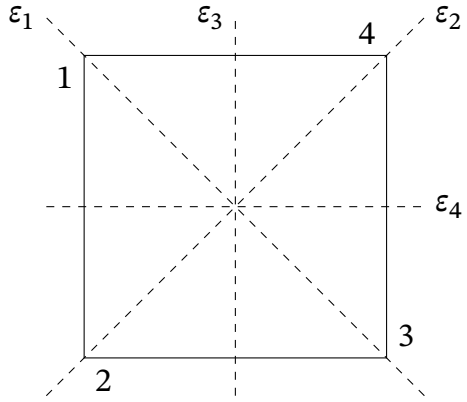
Γ.1.2 Ομάδες συμμετριών

Ας ξεκινήσουμε με ένα παράδειγμα. Υποθέτουμε ότι στο επίπεδο έχουμε ένα τετράγωνο και ότι μπορούμε να το μετακινούμε στον χώρο. Μετακινούμε το τετράγωνο και το επανατοποθετούμε στην αρχική του θέση. Ο σκοπός μας είναι να περιγράψουμε αποτελεσματικά όλους τους δυνατούς τρόπους, με τους οποίους μπορεί να επιτευχθεί αυτό. Προφανώς, κατά την επανατοποθέτηση του τετραγώνου στην αρχική του θέση οι κορυφές του τετραγώνου συμπίπτουν με τις θέσεις, όπου βρίσκονταν οι κορυφές του τετραγώνου. Συνεπώς, έχουμε ότι κάθε μετακίνηση του τετραγώνου και επανατοποθέτησή του αντιστοιχεί σε μια μετάθεση των τεσσάρων κορυφών του τετραγώνου. Άρα, θα έλεγε κάποιος, ότι έχουμε τόσες δυνατές επανατοποθετήσεις, όσες είναι και το πλήθος των μεταθέσεων σε τέσσερα σύμβολα (τις τέσσερις κορυφές). Ας εντρυφήσουμε περισσότερο.

Μια μετακίνηση και επανατοποθέτηση του τετραγώνου στην αρχική του θέση έχει τον εξής περιορισμό. "Διατηρεί τις αποστάσεις" μεταξύ των σημείων του. (Το τετράγωνο, κατά την επανατοποθέτησή του, δεν αλλάζει ούτε σχήμα, ούτε εμβαδόν). Τί σημαίνει αυτό; Ότι γειτονικές κορυφές παραμένουν γειτονικές. Επομένως, από όλες τις δυνατές μεταθέσεις των κορυφών δεν είναι όλες αποδεκτές.

Πριν προχωρήσουμε, κάθε επανατοποθέτηση του τετραγώνου στην αρχική του θέση, δηλαδή κάθε αποδεκτή μετάθεση των κορυφών του, θα την ονομάζουμε **συμμετρία** του τετραγώνου.

Για να περιγράψουμε όλες τις συμμετρίες του τετραγώνου ας αριθμήσουμε τις κορυφές του (βλέπε Σχήμα Γ.1).



Σχήμα Γ.1: *Συμμετρίες τετραγώνου.*

Η μετάθεση

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

προφανώς δεν είναι συμμετρία τετραγώνου (γιατί;)

Μια προφανής συμμετρία είναι η στροφή του τετραγώνου κατά 90^0 μοίρες. Η συμμετρία αυτή μπορεί να περιγραφεί από την μετάθεση

$$\vartheta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

Επίσης, οι στροφές κατά 180^0 και κατά 270^0 μοίρες είναι συμμετρίες του τετρα-

γώνου. Οι συμμετρίες αυτές περιγράφονται από τις μεταθέσεις

$$\vartheta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \text{ και} \vartheta_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

Πέραν αυτών των συμμετριών υπάρχουν και άλλες συμμετρίες;

Αν αναστρέψουμε[3] το τετράγωνο ως προς την ευθεία ϵ_1 (βλέπε Σχήμα Γ.1), τότε βλέπουμε ότι οι κορυφές 1 και 3 παραμένουν αμετακίνητες, ενώ οι κορυφές 2 και 4 εναλλάσσουν θέσεις. Αυτή η συμμετρία περιγράφεται από την μετάθεση

$$r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

Όμοια επιτυγχάνουμε συμμετρίες του τετραγώνου αν το ανατρέψουμε και ως προς τις ευθείες ϵ_2, ϵ_3, ϵ_4, οι οποίες περιγράφονται αντίστοιχα από τις μεταθέσεις

$$r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, r_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, r_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Επομένως, μέχρι τώρα έχουμε δει ότι σε ένα τετράγωνο έχουμε τις συμμετρίες

$$\vartheta_1, \vartheta_2, \vartheta_3, r_1, r_2, r_3, r_4.$$

Υπάρχουν άλλες συμμετρίες στο τετράγωνο; Υπάρχει ακόμη μία, αν θεωρήσουμε την ταυτοτική συμμετρία, όπου μετακινούμε και επανατοποθετούμε το τετράγωνο ακριβώς όπως ήταν στην αρχική του θέση. Η συμμετρία αυτή περιγράφεται από την ταυτοτική μετάθεση

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

Πέραν αυτών των συμμετριών δεν υπάρχουν άλλες συμμετρίες στο τετράγωνο. Πράγματι, όπως παρατηρήσαμε και προηγουμένως, η τελική θέση του τετραγώνου είναι πλήρως καθορισμένη από την θέση των τεσσάρων κορυφών του και του προσανατολισμού τους (άνω και κάτω όψη). Επομένως, υπάρχουν ακριβώς οκτώ συμμετρίες του τετραγώνου, αυτές που ήδη έχουμε περιγράψει.

Πρέπει να επισημάνουμε ότι αν συνδυάσουμε οποιεσδήποτε δύο από αυτές τις συμμετρίες προκύπτει μία από τις υπόλοιπες συμμετρίες.

Για παράδειγμα, αν συνδυάσουμε τις συμμετρίες ϑ_2 και r_2, δηλαδή πρώτα πραγματοποιούμε μια στροφή κατά 90^0 μοίρες και μετά μία αναστροφή ως προς την ευθεία ϵ_2, τότε θα προκύψει η συμμετρία r_4. Πράγματι, δεν έχουμε παρά να ελέγξουμε την σύνθεση των μεταθέσεων

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Εδώ πρέπει να επισημάνουμε ότι, αν πρώτα πραγματοποιήσουμε μια αναστροφή ως προς την ευθεία ϵ_2 και μετά μια στροφή κατά 90^0 μοίρες, τότε θα προκύψει η συμμετρία r_3 (γιατί;). Συνεπώς, δεν ισχύει η μεταθετικότητα στον συνδυασμό συμμετριών.

[3] Οι αναστροφές ως προς μια ευθεία ονομάζονται *ανακλάσεις ή κατοπτρισμοί* και η ευθεία *άξονας συμμετρίας*. Ιδέ και την γενική περίπτωση στην σελίδα 390.

Επίσης, η αντίστροφη κάθε μιας από τις συμμετρίες αυτές είναι και αυτή συμμετρία. Είναι εύκολο να διαπιστώσουμε ότι

$$\begin{aligned} r_1^{-1} &= r_1, & r_2^{-1} &= r_2, \\ r_3^{-1} &= r_3, & r_4^{-1} &= r_4, \\ \vartheta_1^{-1} &= \vartheta_3, & \vartheta_2 &= \vartheta_2. \end{aligned}$$

Επομένως, το σύνολο

$$D_4 = \{e, \vartheta_1, \vartheta_2, \vartheta_3, r_1, r_2, r_3, r_4\}$$

αποτελεί μια ομάδα με πράξη την σύνθεση μεταθέσεων. Η ομάδα αυτή ονομάζεται η ομάδα **συμμετριών** του τετραγώνου.

Όπως περιγράψαμε την ομάδα συμμετριών ενός τετραγώνου, ακριβώς με τον ίδιο τρόπο μπορούμε να περιγράψουμε την ομάδα συμμετριών ενός κανονικού πενταγώνου και γενικά ενός κανονικού n-γώνου.

Γενικότερα σε κάθε επίπεδο σχήμα ορίζεται η ομάδα συμμετριών του, η οποία περιγράφει την "κανονικότητα" του σχήματος αυτού. Για παράδειγμα, η ομάδα συμμετριών ενός σκαληνού τριγώνου είναι η τετριμμένη ομάδα, ενώ η ομάδα ενός ισοσκελούς, αλλά όχι ισοπλεύρου, τριγώνου έχει μόνο δύο στοιχεία, την ταυτοτική μετάθεση και την ανάκλαση ως προς τον άξονα, οποίος διέρχεται από την κορυφή του τριγώνου και είναι κάθετος στο μέσον της απέναντι πλευράς.

Η ομάδα συμμετριών ενός κανονικού n-γώνου ονομάζεται **διεδρική** ομάδα βαθμού n, έχει $2n$ το πλήθος στοιχεία και συμβολίζεται ως D_n.

Όπως ορίζονται οι ομάδες συμμετριών ενός επιπέδου σχήματος, έτσι ορίζονται και οι ομάδες συμμετριών Γεωμετρικών στερεών στον χώρο.

Η σύγχρονη κρυσταλλογραφία και κρυσταλλική Φυσική, για παράδειγμα, βασίζονται σε μεγάλο βαθμό στην γνώση ομάδων συμμετριών τρισδιάστατων σχημάτων.

Επίσης, οι ομάδες συμμετριών χρησιμοποιούνται ευρέως στην μελέτη της δομής των ηλεκτρονίων. Στην Στοιχειώδη Σωματιδιακή Φυσική οι ομάδες συμμετριών έχουν χρησιμοποιηθεί στην πρόβλεψη ύπαρξης στοιχειωδών σωματιδίων πριν αυτά ανακαλυφθούν πειραματικά.

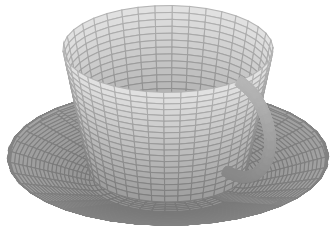
Πέραν αυτών, οι συμμετρίες και οι ομάδες τους είναι "παρούσες" παντού στην φύση, από τα πέταλλα των λουλουδιών και τις χιονονυφάδες έως και την κυτταρική διαίρεση και την τέχνη, από την ζωγραφική και την γλυπτική έως την μουσική.

Παρατηρήσεις Γ.1.11. Προηγουμένως, στην περιγραφή των συμμετριών ενός τετραγώνου "επιστρατεύσαμε" περισσότερο την διαίσθηση και εποπτεία, παρά την Μαθηματική αυστηρότητα. Στην περιγραφή της αναστροφής του τετραγώνου ως προς μια ευθεία θεωρήσαμε ως δεδομένο ότι μπορούμε να "κινηθούμε" στον τρισδιάστατο χώρο και με μία φυσική κίνηση, την αναστροφή, να επανατοποθετήσουμε το τετράγωνο στην αρχική του θέση στο επίπεδο.

Ας δούμε κάτι ανάλογο στον τρισδιάστατο χώρο. Ας φανταστούμε ότι έχουμε μια κούπα στον τρισδιάστατο χώρο. Η κούπα αυτή έχει μια συμμετρία ως προς το επίπεδο, το οποίο την "τέμνει", όπως στο Σχήμα Γ.2.

Αυτή δεν επιτυγχάνεται με φυσική κίνηση στον τρισδιάστατο χώρο, δεδομένου ότι δεν μπορούμε να "κινηθούμε" εκτός του τρισδιάστατου χώρου, όπως κάναμε με την αναστροφή του τετραγώνου που περιγράψαμε προηγουμένως.

Αν και αυτό δεν είναι δυνατόν να επιτευχθεί στην πράξη, είναι δυνατόν να περιγραφεί κομψά μέσω απεικονίσεων.



Σχήμα Γ.2: *Συμμετρία ως προς επίπεδο.*

Στα επόμενα απλώς θα αναφέρουμε μόνο μερικούς ορισμούς και απλές παρατηρήσεις για να δούμε, έστω και αδρά πώς όλα, όσα αναφέραμε προηγουμένως, εντάσσονται σε μια γενική θεώρηση.

Θα περιοριστούμε μόνο στο επίπεδο $\mathbb{R}^2$ και θα θεωρήσουμε γνωστά στοιχειώδεις έννοιες και αποτελέσματα από την Ευκλείδεια Γεωμετρία.

Θεωρούμε γνωστή (έστω και εμπειρικά)[4] την έννοια της απόστασης μεταξύ δύο σημείων $x = (x_1, x_2), y = (y_1, y_2) \in \mathbb{R}^2$.

Ορισμός Γ.1.12. Μια απεικόνιση $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ ονομάζεται **ισομετρία**, αν ισχύει

$$\| f(x) - f(y) \| = \| x - y \|,$$

για όλα τα $x, y \in \mathbb{R}^2$.

Προφανώς κάθε ισομετρία είναι μια απεικόνιση 1-1 (γιατί;).

Ένα φυσιολογικό ερώτημα είναι το εξής: Είναι κάθε ισομετρία επί; Δηλαδή οι ισομετρίες είναι αντιστρέψιμες απεικονίσεις;

Η απάντηση, διαισθητικά, είναι καταφατική, χρήζει όμως αποδείξεως (ιδέ Πρόταση Γ.1.14).

Προφανώς οι μεταφορές

$$T_{(a,b)} : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

(ιδέ Παράδειγμα 5.1.17$_9$) αποτελούν ισομετρίες (γιατί;).

Επίσης, η σύνθεση δύο ισομετριών αποτελεί ισομετρία.

Πράγματι, έστω $f, g : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ δύο ισομετρίες. Τότε για $x, y \in \mathbb{R}^2$ έχουμε

$$\begin{aligned} \| (f \circ g)(x) - (f \circ g)(y) \| &= \| f(g(x)) - f(g(y)) \| && \text{(επειδή η } f \text{ είναι ισομετρία)} \\ &= \| g(x) - g(y) \| && \text{(επειδή η } g \text{ είναι ισομετρία)} \\ &= \| x - y \| . \end{aligned}$$

Μπορούμε να κατατάξουμε τις ισομετρίες σε δύο μεγάλες κατηγορίες. Σ' αυτές που *σταθεροποιούν* σημεία και σε αυτές που δεν σταθεροποιούν σημεία.

[4] Πρόκειται για την γνωστή(;) Ευκλείδεια απόσταση

$$\| x - y \| = \sqrt{(x_1 - x_2)^2 + (x_2 - y_2)^2}.$$

Πρόταση Γ.1.13. *Κάθε ισομετρία μπορεί να αναλυθεί σε σύνθεση μιας μεταφοράς και μίας ισομετρίας, η οποία σταθεροποιεί την αρχή των αξόνων. Δηλαδή, για κάθε* $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ *ισομετρία υπάρχει μία μεταφορά* $T_{(a,b)} : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ *και μια ισομετρία* $f_0 : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ *με την ιδιότητα*

$$f_0(0,0) = (0,0) \text{ και } f = T_{(a,b)} \circ f_0.$$

Απόδειξη. Υποθέτουμε ότι

$$f(0,0) = (a,b).$$

Τότε η σύνθεση $T_{(-a,-b)} \circ f$ έχει την ιδιότητα

$$\begin{aligned}\left(T_{(-a,-b)} \circ f\right)(0,0) &= T_{(-a,-b)}(f(0,0)) \\ &= T_{(-a,-b)}(a,b) \\ &= (0,0).\end{aligned}$$

Οπότε, η απεικόνιση που αναζητούμε είναι η

$$f_0 = T_{(-a,-b)} \circ f.$$

ό.έ.δ.

Ας επικεντρωθούμε στις ισομετρίες, οι οποίες αφήνουν το σημείο $O = (0,0) \in \mathbb{R}^2$ σταθερό.

Έστω f μια τέτοια ισομετρία.

Η ισομετρία αυτή απεικονίζει κάθε σημείο του επιπέδου, το οποίο απέχει από την αρχή των αξόνων απόσταση έστω r, σε ένα σημείο, το οποίο και αυτό απέχει από την αρχή των αξόνων απόσταση ίση με r (γιατί;). Δηλαδή, η εικόνα του βρίσκεται στον κύκλο με κέντρο το σημείο $O = (0,0)$ και ακτίνα ίση με r.

Επομένως, χωρίς βλάβη της γενικότητας, μπορούμε να επικεντρωθούμε στην μελέτη των εικόνων των σημείων του μοναδιαίου κύκλου μέσω μιας ισομετρίας, η οποία σταθεροποιεί το σημείο $O = (0,0)$.

Έστω P, Q δύο σημεία του μοναδιαίου κύκλου και $f(P)$, $f(Q)$ οι αντίστοιχες εικόνες τους.

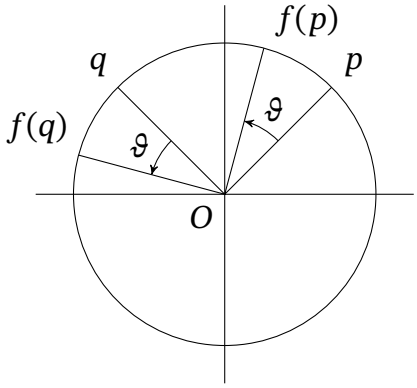
Ισχυρισμός: Η γωνία που σχηματίζουν τα διανύσματα με αρχή το σημείο O και πέρας τα σημεία P και Q είναι ίση με την γωνία που σχηματίζουν τα διανύσματα με αρχή το σημείο O και πέρας τα σημεία $f(P)$ και $f(Q)$ (γιατί;) Μα αφού πρόκειται για ισομετρία τα μήκη των ευθυγράμμων τμημάτων PQ και $f(P)f(Q)$ είναι ίσα. Άρα τα ισοσκελή τρίγωνα $\triangle(OPQ)$ και $\triangle(Of(P)f(Q))$ είναι ίσα.

Δηλαδή η ισομετρία f *διατηρεί τις γωνίες*.

Για την ισομετρία f διακρίνουμε δύο περιπτώσεις:

i. Η f δεν σταθεροποιεί κανένα σημείο του μοναδιαίου κύκλου. Στην περίπτωση αυτή, αν το σημείο P απεικονιστεί στη θέση $f(P)$ και η γωνία, που σχηματίζουν τα δύο διανύσματα (διαγράφοντας τον κύκλο αριστερόστροφα) $\overrightarrow{OP}$ και $\overrightarrow{Of(P)}$ είναι ίση με ϑ, τότε για οποιοδήποτε άλλο σημείο Q του κύκλου η γωνία των δύο διανυσμάτων $\overrightarrow{OQ}$ και $\overrightarrow{Of(Q)}$ είναι και αυτή (βάσει του προηγούμενου ισχυρισμού) ίση με ϑ.

   Η ισομετρία αυτή θα ονομάζεται **στροφή** κατά γωνία ϑ και θα την συμβολίζουμε ως R_ϑ (ιδέ Σχήμα Γ.3).



Σχήμα Γ.3: *Στροφή κατά γωνία* ϑ.

Προφανώς(;), η σύνθεση δύο στροφών είναι και αυτή στροφή. Μάλιστα δε, ισχύει ότι

$$R_\vartheta \circ R_\varphi = R_\varphi \circ R_\vartheta = R_{\vartheta+\varphi} \text{ (γιατί;)}$$

Επίσης, μια στροφή είναι αντιστρέψιμη απεικόνιση και ισχύει ότι

$$R_\vartheta^{-1} = R_{2\pi-\vartheta} = R_{-\vartheta}.$$

Εδώ επισημαίνουμε ότι στην ακραία περίπτωση, όπου η γωνία στροφής είναι ίση με την μηδενική γωνία, τότε πρόκειται για την ταυτοτική απεικόνιση (μηδενική στροφή). Είναι η μοναδική στροφή, η οποία σταθεροποιεί (όλα) τα σημεία του επιπέδου.

Προφανές είναι επίσης ότι δύο στροφές R_ϑ και R_φ είναι ίσες, αν και μόνο αν

$$\vartheta - \varphi = 2k\pi,\ k \in \mathbb{Z}.$$

Συνεπώς, οι διαφορετικές στροφές είναι οι R_ϑ, για $0 \leq \vartheta < 2\pi$.

Επομένως, το σύνολο

$$Rot = \{ R_\vartheta \mid 0 \leq \vartheta < 2\pi \}$$

είναι ομάδα.

ii. Η f σταθεροποιεί ένα σημείο, αλλά όχι όλα τα σημεία, του μοναδιαίου κύκλου.

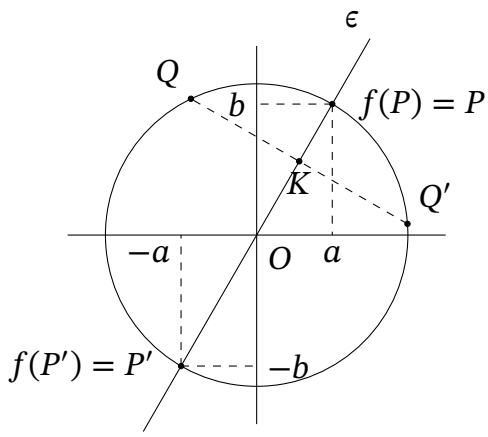
Υποθέτουμε ότι η f σταθεροποιεί το σημείο $P = (a, b)$ του μοναδιαίου κύκλου. Τότε, δεδομένου ότι είναι ισομετρία, θα σταθεροποιεί και το (αντιδιαμετρικό) σημείο $P' = (-a, -b)$ (γιατί;)

Ερώτημα: Υπάρχουν και άλλα σημεία του μοναδιαίου κύκλου, τα οποία σταθεροποιούνται από την f;

Έστω $Q = (r, s)$ ένα άλλο στοιχείο του μοναδιαίου κύκλου και

$$f(Q) = Q' = (r', s').$$

Επειδή η f είναι ισομετρία και $f(P) = P$ έχουμε ότι η χορδή με άκρα τα σημεία Q και Q' είναι κάθετη στην ευθεία ε που καθορίζεται από τα σημεία P και P' (γιατί;) Μάλιστα δε, το σημείο τομής της χορδής QQ' και της ευθείας ε είναι το μέσον της χορδής QQ' (γιατί;) (ιδέ σχήμα Γ.4).



Σχήμα Γ.4: *Ανάκλαση ή κατοπτρισμός ως προς άξονα.*

Αυτό ισχύει για όλα τα σημεία που δεν ανήκουν στην ευθεία ε, ενώ προφανώς όλα τα σημεία της ευθείας ε, και μόνο αυτά, παραμένουν σταθερά από την ισομετρία f.

Μια τέτοια ισομετρία θα ονομάζεται **ανάκλαση** ή **κατοπτρισμός**, η δε ευθεία ε θα ονομάζεται **άξονας** συμμετρίας της f.

Προφανώς (γιατί;) μια ανάκλαση f έχει την ιδιότητα $f \circ f = 1_{\mathbb{R}^2}$, η ταυτοτική απεικόνιση.

Ξεκινήσαμε με μία (μη σταθερή) ισομετρία ή οποία σταθεροποιεί το σημείο $O = (0, 0)$ και ένα ακόμη σημείο, το P, και είδαμε ότι η ισομετρία αυτή σταθεροποιεί μόνο τα σημεία της ευθείας που ορίζεται από τα σημεία O και P (σταθεροποιεί τον άξονα συμμετρίας της).

Αντίστροφα, για κάθε ευθεία ε, η οποία διέρχεται από την αρχή των αξόνων $O = (0, 0)$, μπορούμε να ορίσουμε μια ανάκλαση, της οποίας ο άξονας συμμετρίας είναι η δεδομένη ευθεία ε.

Πράγματι, αν ονομάσουμε (για καθαρά υπολογιστική ευκολία) την γωνία, που σχηματίζει η ευθεία ε με τον άξονα Ox ως $\vartheta/2$, τότε η απεικόνιση $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ με

$$f(x, y) = (\cos\vartheta \cdot x + \sin\vartheta \cdot y, \sin\vartheta \cdot x - \cos\vartheta \cdot y)$$

είναι μια ανάκλαση, της οποίας ο άξονας συμμετρίας είναι η δεδομένη ευθεία ε (γιατί;). Η ανάκλαση αυτή θα συμβολίζεται ως C_ε.

Από τα προηγούμενα έπεται η εξής σημαντική πρόταση:

Πρόταση Γ.1.14. *(Η Ευκλείδειος Ομάδα του επιπέδου)*
Το σύνολο όλων των ισομετριών του επιπέδου αποτελεί ομάδα με πράξη την σύνθεση απεικονίσεων.

Απόδειξη. Σύμφωνα με την Πρόταση Γ.1.13 κάθε ισομετρία $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ είναι η σύνθεση μιας μεταφοράς και μιας ισομετρίας, η οποία σταθεροποιεί την αρχή των αξόνων. Από τα προηγούμενα έπεται ότι μια τέτοια ισομετρία είναι είτε στροφή είτε ανάκλαση. Έχουμε δει ότι οι μεταφορές, οι στροφές και οι ανακλάσεις είναι αντιστρέψιμες απεικονίσεις. Επομένως, και η σύνθεσή τους είναι αντιστρέψιμη απεικόνιση. Άρα κάθε ισομετρία είναι αντιστρέψιμη απεικόνιση.

Επίσης, όπως είδαμε, η σύνθεση ισομετριών είναι ισομετρία, άρα πληρούνται τα κριτήρια του ορισμού της ομάδας.

Η ομάδα αυτή θα ονομάζεται **Ευκλείδεια** ομάδα του επιπέδου και θα συμβολίζεται ως E_2. ό.έ.δ.

Ορισμός Γ.1.15. Έστω S ένα μη κενό υποσύνολο του $\mathbb{R}^2$. Μια ισομετρία $f \in E_2$ θα ονομάζεται **συμμετρία** του S, αν $f(S) = S$.

Είναι εύκολο να δούμε (γιατί;) ότι το σύνολο όλων των συμμετριών ενός υποσυνόλου $S \subseteq \mathbb{R}^2$ αποτελεί ομάδα με πράξη την σύνθεση απεικονίσεων. Η ομάδα αυτή ονομάζεται Ομάδα **συμμετριών** του S και θα συμβολίζεται E_S.

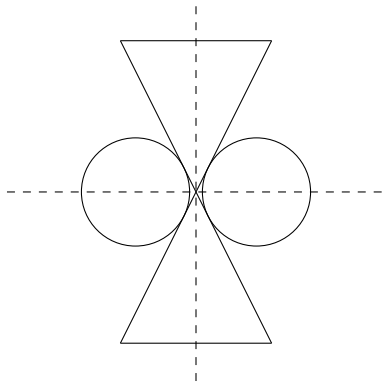
Παραδείγματα Γ.1.16.

1. Έχουμε ήδη περιγράψει την ομάδα συμμετριών του τετραγώνου, είναι η διεδρική ομάδα D_4.

   Παρόμοια μπορούμε να περιγράψουμε, όπως έχουμε προαναφέρει, τις ομάδες συμμετριών όλων των κανονικών n-γώνων, οι οποίες είναι οι διεδρικές D_n με $2n$ το πλήθος στοιχεία.

2. Ο κύκλος είναι από τα πλέον συμμετρικά σχήματα του επιπέδου. Πράγματι έχει "μεγάλη" ομάδα συμμετρίας. Για κάθε γωνία $0 \leq \vartheta < 2\pi$ η στροφή R_ϑ αποτελεί συμμετρία του κύκλου. Επίσης, κάθε ευθεία, η οποία διέρχεται από το κέντρο του κύκλου, αποτελεί και έναν άξονα συμμετρίας του κύκλου.

3. Το σχήμα Γ.5 έχει ομάδα συμμετρίας, η οποία αποτελείται από τέσσερα στοιχεία, μια στροφή κατά 180^o μοίρες, δύο ανακλάσεις ως προς τους σημειωμένους άξονες συμμετρίας και την ταυτοτική μετάθεση (η στροφή κατά 360^o μοίρες).



Σχήμα Γ.5: *Ομάδα συμμετρίας με τέσσερα στοιχεία.*

Πρόταση Γ.1.17. *Η ομάδα* $Tr = \{ T_{(a,b)} \mid (a, b) \in \mathbb{R}^2 \}$ *των μεταφορών (ιδέ Παράδειγμα* $5.1.17_9$*) είναι υποομάδα της ομάδας* E_2 *ισομετριών του επιπέδου.*

Η ομάδα των στροφών Rot είναι υποομάδα ομάδας E_2 *ισομετριών του επιπέδου.*

Το σύνολο όλων των ανακλάσεων δεν είναι ομάδα.

Απόδειξη. Η απόδειξη είναι προφανής, απλώς θέλουμε να τονίσουμε ότι σύνολα, τα οποία έχουμε αποδείξει ήδη ότι είναι ομάδες, μπορούν να θεωρηθούν υπομάδες άλλων ομάδων.

Για το ότι το σύνολο των ανακλάσεων δεν είναι ομάδα. αρκεί να παρατηρήσουμε ότι η σύνθεση δύο ανακλάσεων δεν είναι ανάκλαση (ιδέ Άσκηση $5.1.3_{26}$). ό.έ.δ.

Θα κλείσουμε την παράγραφο, επισημαίνοντας ότι: Αυτά που αναφέραμε για ισομετρίες και συμμετρίες στο επίπεδο ισχύουν και στον τρισδιάστατο χώρο (ακόμη και σε πολυδιάστατους χώρους). Εδώ ο σκοπός μας είναι, όπως προαναφέραμε, απλώς να πάρουμε μια γεύση πώς η έννοια της ομάδος έχει άμεση σχέση με την Γεωμετρία. Δεν θα επεκταθούμε περισσότερο.

Θα επανέλθουμε στις ομάδες αναφέροντας μερικές ιδιότητες επιπλέον των ομάδων, καθώς και τις "σχέσεις" των ομάδων μέσω ομομορφισμών ομάδων (ιδέ Παράγραφο Γ.3.1).

Γ.1.3 Ασκήσεις

1. Έστω G μια ομάδα και $a \in G$ πεπερασμένης τάξης. Δείξτε ότι $a^r = 1_G$, αν και μόνο αν η τάξη $o(a)$ διαιρεί τον ακέραιο r.

2. Δείξτε ότι σε μια πεπερασμένη ομάδα, όλα τα στοιχεία έχουν πεπερασμένη τάξη και η τάξη κάθε στοιχείου διαιρεί την τάξη της ομάδας.

3. Δείξτε ότι σε μια πεπερασμένη ομάδα G, για κάθε $g \in G$ ισχύει ότι $g^{|G|} = 1_G$.

4. Έστω G μια ομάδα με τάξη ίση με έναν πρώτο αριθμό. Δείξτε ότι η G είναι κυκλική.

5. Έστω G μια κυκλική ομάδα με τάξη ίση με 24 και $a \in G$ με $a^8 \neq 1$ και $a^{12} \neq 1$. Δείξτε ότι το a είναι γεννήτορας της G ($G = \langle a \rangle$).

6. Έστω G μια ομάδα και $a \in G$ με $o(a) = 24$. Να βρεθεί ένας γεννήτορας της τομής $\langle a^{21} \rangle \cap \langle a^{10} \rangle$.

7. Στην προσθετική ομάδα των ακεραίων έστω η υποομάδα $3\mathbb{Z} = \langle 3 \rangle$. Να βρείτε όλους τους γεννήτορες της $3\mathbb{Z}$.

8. Έστω G μια αβελιανή ομάδα και $a, b \in G$ στοιχεία πεπερασμένης τάξης. Δείξτε ότι το στοιχείο ab έχει πεπερασμένη τάξη.

9. Έστω G μια ομάδα και $a \in G$ πεπερασμένης τάξης. Να συμπληρώσετε την πρόταση:

   $o(a) = o(a^2)$, αν και μόνο αν η $o(a)$ είναι.....

10. Έστω a, b δύο στοιχεία μιας ομάδας. Υποθέτουμε ότι η τάξη του a είναι περιττός αριθμός και ότι ισχύει $a^{-1}ba = b^{-1}$. Δείξτε ότι $o(b) = 2$.

11. (Η Ορθογώνια ομάδα του επιπέδου)

    Στην Ευκλείδεια ομάδα E_2 των ισομετριών του επιπέδου, δείξτε ότι το σύνολο O_2 όλων των ισομετριών, οι οποίες σταθεροποιούν την αρχή των αξόνων $O = (0, 0)$ είναι υποομάδα.

    Δείξτε ότι στην ομάδα O_2 ισχύουν τα εξής:

    (α) Η σύνθεση δύο ανακλάσεων είναι μια στροφή.

    (β) Η σύνθεση μιας ανάκλασης και μιας στροφής είναι ανάκλαση.

    (γ) Η σύνθεση μιας στροφής και μιας ανάκλασης είναι ανάκλαση.

(δ) Αν C_ϵ είναι η ανάκλαση ως προς τον άξονα συμμετρίας ϵ, τότε για κάθε άλλη ανάκλαση $C_{\epsilon'}$ υπάρχει (μοναδική) στροφή R_ϑ, ώστε $C_{\epsilon'} = R_\vartheta \circ C_\epsilon$.

(ε) Η ομάδα Rot των στροφών είναι υποομάδα δείκτου 2 στην Ορθογώνια ομάδα O_2 ($[O_2 : Rot] = 2$).

(στ) Έστω R_ϑ μια στροφή κατά γωνία ϑ. Δείξτε ότι η ομάδα

$$\langle R_\vartheta \rangle = \{ R_\vartheta^k \mid k \in \mathbb{Z} \}$$

είναι πεπερασμένη, αν και μόνο αν $\vartheta = 2\pi/n$, όπου n είναι ένας θετικός ακέραιος.

Στην περίπτωση, όπου είναι πεπερασμένη, ποια είναι η τάξη της;

12. Να βρεθούν όλες οι μεταθέσεις $\pi \in S_4$, οι οποίες δεν είναι συμμετρίες του τετραγώνου.

13. Έστω R η στροφή στο τετράγωνο κατά 90^o μοίρες και C η ανάκλαση ως προς έναν άξονα συμμετρίας του τετραγώνου.

Δείξτε ότι η ομάδα συμμετριών του είναι η

$$D_4 = \{ 1, R, R^2, R^3, C, C \circ R, C \circ R^2, C \circ R^3 \}.$$

Γενικεύσατε για το τυχαίο κανονικό n-γωνο.

Γ.2 Μερικές αξιοσημείωτες κατηγορίες δακτυλίων

Στα μέχρι τώρα παραδείγματα δακτυλίων, που έχουμε δει, περιλαμβάνονται οι γνωστοί δακτύλιοι των ακεραίων, των ρητών και των πραγματικών αριθμών, καθώς και τις προφανείς "κατασκευές" δακτυλίων από άλλους δακτυλίους. Στα επόμενα θα αναφέρουμε δύο σημαντικές κατηγορίες δακτυλίων. Αυτές οι κατηγορίες δακτυλίων είναι πολύ σημαντικές και η επίδρασή τους διαχέεται σε όλα τα Μαθηματικά. Κάθε μια από αυτές τις κατηγορίες αποτελεί, από μόνη της, ένα αυτοτελές αντικείμενο μελέτης.

Εμείς εδώ απλώς θα προσπαθήσουμε να δώσουμε τους αναγκαίους ορισμούς και προφανείς ιδιότητες αυτών των δακτυλίων, καθώς και ερεθίσματα για περαιτέρω μελέτη, καθ' ότι έστω και μια μικρή προσπάθεια για επιπλέον εμβάθυνση, θα απέκλινε των σκοπών του παρόντος βιβλίου.

Γ.2.1 Ο δακτύλιος των ακεραίων mod m

Για να ορισθεί η κατηγορία αυτή των δακτυλίων, θα επικαλεσθούμε ένα γνωστό σε όλους, Μαθηματικούς και μη, βασικό θεώρημα (Είναι το Θεώρημα 6.1.19).

Θεώρημα Γ.2.1. *Έστω a, b ακέραιοι αριθμοί. Υποθέτουμε ότι ο b είναι μη μηδενικός και θετικός. Τότε υπάρχουν μοναδικοί ακέραιοι αριθμοί π (το πηλίκο) και υ (το υπόλοιπο), ώστε $a = \pi \cdot b + \upsilon$ με $0 \leq \upsilon < b$.*

Θα ξεκινήσουμε με το Παράδειγμα $5.1.35_1$.

Έστω $(\mathbb{Z}, +)$ η προσθετική ομάδα των ακεραίων αριθμών και m ένας θετικός ακέραιος, τότε τα σύμπλοκα της υποομάδας

$$m\mathbb{Z} = \{ mr \mid r \in \mathbb{Z} \},$$

ως προς την ομάδα $(\mathbb{Z}, +)$, είναι τα

$$0 + m\mathbb{Z},\ 1 + m\mathbb{Z},\ \dots,\ (m-1) + m\mathbb{Z}.$$

Για να προχωρήσουμε, θα υπενθυμίσουμε ότι στο συγκεκριμένο παράδειγμα η σχέση ισοδυναμίας που καθορίζει τα σύμπλοκα είναι η εξής:

$$a \sim b, \text{ αν } a - b \in m\mathbb{Z}.$$

Τι σημαίνει αυτό; Η διαφορά των ακεραίων αριθμών $a - b$ είναι πολλαπλάσιο του (θετικού) ακεραίου m, δηλαδή υπάρχει ακέραιος r, έτσι ώστε $a - b = mr$. Αν εφαρμόσουμε το προηγούμενο θεώρημα για τους ακεραίους a, m και b, m, θα έχουμε ότι

$$a = \pi_1 m + \upsilon_1 \text{ και } b = \pi_2 m + \upsilon_2,$$

για $\pi_1, \pi_2, \upsilon_1, \upsilon_2 \in \mathbb{Z}$ με $0 \leq \upsilon_1 < m$ και $0 \leq \upsilon_2 < m$. Από τις ισότητες αυτές, αν αφαιρέσουμε κατά μέλη, έχουμε ότι

$$a - b = (\pi_1 - \pi_2)m + (\upsilon_1 - \upsilon_2).$$

Αλλά έχουμε υποθέσει ότι η διαφορά είναι πολλαπλάσιο του m. Αυτό σημαίνει ότι

$$\upsilon_1 - \upsilon_2 = 0$$

(γιατί; δεν ξεχνάμε ότι $0 \leq \upsilon_1 < m$ και $0 \leq \upsilon_2 < m$).

Άρα αποδείξαμε ότι, αν $a \sim b$, τότε τα υπόλοιπα της διαίρεσης καθενός από αυτούς με τον m είναι ίσα. Προφανώς ισχύει και το αντίστροφο. Δηλαδή, αν οι ακέραιοι αριθμοί a και b διαιρούμενοι με τον ακέραιο m έχουν το ίδιο υπόλοιπο, τότε η διαφορά τους είναι πολλαπλάσιο του m, δηλαδή $a \sim b$.

Επομένως, βλέπουμε ότι η αρχική μας ισοδυναμία $a \sim b$, αν $a-b \in m\mathbb{Z}$, ισοδυνάμως εκφράζεται ως εξής: $a \sim b$, αν το υπόλοιπο της διαίρεσης του a με τον m ισούται με το υπόλοιπο της διαίρεσης του b με τον m.

Επίσης, παρατηρούμε ότι κάθε σύμπλοκο, δηλαδή κάθε κλάση ισοδυναμίας,

$$i + m\mathbb{Z} = \{\, i + mr \mid r \in \mathbb{Z} \,\},\ 0 \leq i \leq m-1$$

αποτελείται από όλους τους ακεραίους, οι οποίοι αφήνουν το ίδιο υπόλοιπο i, αν διαιρεθούν με τον m, άρα ως αντιπροσώπους των κλάσεων ισοδυναμίας μπορούμε να πάρουμε όλα τα δυνατά υπόλοιπα της διαίρεσης ενός ακεραίου με τον θετικό ακέραιο m.

Από το γεγονός αυτό έχει επικρατήσει δύο ισοδύναμοι ακέραιοι να ονομάζονται **ισοϋπόλοιποι** ή **ισότιμοι** με μέτρο m και αντί του συμβολισμού $a \sim b$ να χρησιμοποιούμε τον συμβολισμό

$$a \equiv b \bmod m.$$

Επίσης τα σύμπλοκα, δηλαδή οι κλάσεις ισοδυναμίας, αντί του $i + m\mathbb{Z}$ να συμβολίζονται ως $[i]_m$ ή στην περίπτωση, όπου δεν υπάρχει σύγχυση ως προς ποιον ακέραιο αναφερόμαστε, ως $[i]$ ή ως $\bar{i}$, ακόμη και ως i.

Το σύνολο πηλίκων, αντί του συμβολισμού $\mathbb{Z}/\sim$, θα συμβολίζεται στο εξής με $\mathbb{Z}_m$[5] και θα ονομάζεται το σύνολο των ακεραίων $\bmod m$.

[5] Δεν πρέπει να γίνεται σύγχυση με τον (υπο)δακτύλιο $m\mathbb{Z}$, ο οποίος αποτελείται από όλα τα πολλαπλάσια του m.

Πρόταση Γ.2.2. *Έστω m ένας θετικός ακέραιος αριθμός. Υποθέτουμε ότι για τους ακεραίους αριθμούς a_1, b_1, a_2, b_2 ισχύει ότι $a_1 \equiv b_1 mod\, m$ και $a_2 \equiv b_2 mod\, m$, τότε ισχύει ότι:*

$$(a_1 \pm a_2) \equiv (b_1 \pm b_2) mod\, m \quad \text{και} \quad (a_1 \cdot a_2) \equiv (b_1 \cdot b_2) mod\, m.$$

Επίσης, για κάθε ακέραιο αριθμό c ισχύει ότι

$$(c \cdot a_1) \equiv (c \cdot b_1) mod\, m.$$

Απόδειξη. Αρκεί να έχουμε συνειδητοποιήσει τι σημαίνει $a \equiv b mod\, m$.

Η "ισότητα" $a_1 \equiv b_1 mod\, m$ σημαίνει ότι υπάρχει $r \in \mathbb{Z}$, ώστε

$$a_1 - b_1 = m \cdot r.$$

Το ίδιο ισχύει και για την "ισότητα" $a_2 \equiv b_2 mod\, m$, δηλαδή υπάρχει $s \in \mathbb{Z}$, ώστε

$$a_2 - b_2 = m \cdot s.$$

Προσθέτοντας ή αφαιρώντας, κατά μέλη τις ισότητες αυτές έχουμε ότι

$$(a_1 \pm a_2) - (b_1 \pm b_2) = m(r \pm s).$$

Αυτό όμως σημαίνει ότι:

$$(a_1 \pm a_2) \equiv (b_1 \pm b_2) mod\, m.$$

Από την σχέση $a_1 - b_1 = m \cdot r$ έχουμε ότι

$$a_1 \cdot a_2 - b_1 \cdot a_2 = m \cdot r \cdot a_2$$

και από την σχέση $a_2 - b_2 = m \cdot s$ έχουμε ότι

$$b_1 \cdot a_2 - b_1 \cdot b_2 = m \cdot s \cdot b_1.$$

Προσθέτοντας κατά μέλη τις ισότητες

$$a_1 \cdot a_2 - b_1 \cdot a_2 = m \cdot r \cdot a_2 \quad \text{και} \quad b_1 \cdot a_2 - b_1 \cdot b_2 = m \cdot s \cdot b_1$$

έχουμε ότι

$$a_1 \cdot a_2 - b_1 \cdot b_2 = m \cdot (r \cdot a_2 + s \cdot b_2).$$

Αυτό σημαίνει ότι

$$(a_1 \cdot a_2) \equiv (b_1 \cdot b_2) mod\, m.$$

Προφανώς, για κάθε ακέραιο αριθμό c ισχύει ότι $(c \cdot a_1) \equiv (c \cdot b_1) mod\, m$. ό.έ.δ.

Στο σύνολο $\mathbb{Z}_m$ των ακεραίων $mod\, m$ θα ορίσουμε δύο πράξεις, μια πρόσθεση και έναν πολλαπλασιασμό, ως εξής:

$$[a] \oplus [b] = [a + b] \quad \text{και} \quad [a] \odot [b] = [a \cdot b].$$

Θα δείξουμε ότι οι πράξεις αυτές είναι "καλά ορισμένες". Δηλαδή δεν εξαρτώνται από την επιλογή των αντιπροσώπων από κάθε κλάση, αλλά από τις κλάσεις αυτές καθ' εαυτές.

Συνεπώς, πρέπει να δείξουμε ότι, αν $[a_1] = [a_2]$ και $[b_1] = [b_2]$, τότε ισχύει

$$[a_1] \oplus [b_1] = [a_2] \oplus [b_2] \quad \text{και} \quad [a_1] \odot [b_1] = [a_2] \odot [b_2],$$

δηλαδή πρέπει να δείξουμε ότι:

$$[a_1 + b_1] = [a_2 + b_2] \quad \text{και} \quad [a_1 \cdot b_1] = [a_2 \cdot b_2].$$

Η υπόθεση $[a_1] = [a_2]$ και $[b_1] = [b_2]$, σημαίνει ότι

$$a_1 \equiv b_1 mod\, m \quad \text{και} \quad a_2 \equiv b_2 mod\, m.$$

Οπότε, από την προηγουμένη πρόταση έχουμε ότι

$$(a_1 + a_2) \equiv (b_1 + b_2) mod\, m \quad \text{και} \quad (a_1 \cdot a_2) \equiv (b_1 \cdot b_2) mod\, m,$$

το οποίο σημαίνει ότι

$$[a_1 + b_1] = [a_2 + b_2] \quad \text{και} \quad [a_1 \cdot b_1] = [a_2 \cdot b_2].$$

Έχοντας αποδείξει ότι οι πράξεις που ορίσαμε στο σύνολο $\mathbb{Z}_m$ είναι καλά ορισμένες, μπορούμε να αποδείξουμε την εξής πρόταση:

Πρόταση Γ.2.3. *Έστω m ένας θετικός ακέραιος, το σύνολο $(Z_m, \oplus, \odot)$ είναι ένας μεταθετικός δακτύλιος με μονάδα*[6].

Απόδειξη. Δεδομένου ότι οι πράξεις της πρόσθεσης + και του πολλαπλασιασμού · στο σύνολο των ακεραίων είναι προσεταιριστικές, μεταθετικές και ισχύει η επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση, προφανώς από τον τρόπο ορισμού τους οι πράξεις

$$[a] \oplus [b] = [a + b] \quad \text{και} \quad [a] \odot [b] = [a \cdot b]$$

πληρούν τις αντίστοιχες ιδιότητες.

Επίσης, υπάρχει ουδέτερο ως προς την πρόσθεση και είναι η κλάση $[0]$ και υπάρχει ουδέτερο ως προς τον πολλαπλασιασμό και είναι η κλάση $[1]$.

Με τους προφανείς ελέγχους να αφήνονται ως άσκηση. Ποίο είναι το αντίθετο του στοιχείου $[a] \in \mathbb{Z}_m$; (Άσκηση Γ.2.3$_2$). ό.έ.δ.

Σχόλιο Γ.2.4. Για την πρόσθεση και τον πολλαπλασιασμό χρησιμοποιούμε τα σύμβολα $\oplus$ και $\odot$ αντίστοιχα, προς διάκριση από την πρόσθεση και τον πολλαπλασιασμό στους ακεραίους. Στη συνέχεια θα χρησιμοποιούμε τον ίδιο συμβολισμό, τόσο για τον δακτύλιο $\mathbb{Z}$, όσο και για τον δακτύλιο $\mathbb{Z}_m$, δεδομένου ότι στην ισότητα $[a] + [b] = [a + b]$ στο μεν πρώτο μέλος έχουμε πρόσθεση δύο κλάσεων ισοδυναμίας, ενώ στο δεύτερο πρόσθεση δύο ακεραίων. Αυτό, αν είμαστε προσεκτικοί, δεν προκαλεί σύγχυση. Εκείνο που δεν έχει νόημα είναι να γράφουμε $[a] + b$. Εδώ επισημαίνουμε ότι η γραφή $n[a]$ δεν σημαίνει πολλαπλασιασμό του (θετικού) ακεραίου n με την κλάση ισοδυναμίας $[a]$, αλλά είναι ο προσθετικός συμβολισμός

$$n[a] = \underbrace{[a] + [a] + \cdots + [a]}_{n}.$$

[6]Προφανώς (γιατί;), αν $m = 1$, τότε ο δακτύλιος Z_1 είναι ο τετριμμένος δακτύλιος, ο οποίος περιέχει μόνο ένα στοιχείο. Οπότε, όλα τα ανωτέρω (και όλα τα επόμενα) αποκτούν ενδιαφέρον, όταν $m > 1$. Για τον λόγο αυτόν, ο m θα υποτίθεται ότι είναι μεγαλύτερος του ένα, ακόμη και αν δεν αναφέρεται ρητά.

Όπως σε κάθε δακτύλιο με μονάδα, έτσι και εδώ έχουμε την πολλαπλασιαστική ομάδα $U(\mathbb{Z}_m)$ (ιδέ Πρόταση 5.1.38).

Παραδείγματα Γ.2.5.

1. Το πρώτο παράδειγμα δεν μπορεί να είναι άλλο από την μέτρηση του χρόνου σε ώρες.

   Έχουμε δύο τύπους ωρολογίων. Αυτά που έχουν ως βάση μέτρησης το δωδεκάωρο και αυτά που έχουν ως βάση μέτρησης το εικοσιτετράωρο.

   Στην πρώτη περίπτωση εργαζόμαστε με μέτρο το 12 και στην δεύτερη περίπτωση εργαζόμαστε με μέτρο το 24.

   Στην πρώτη περίπτωση, όταν οι δείκτες του ωρολογίου μετρήσουν 12 ώρες, τότε η μέτρηση αρχίζει από την αρχή, δηλαδή έχουμε τον δακτύλιο $\mathbb{Z}_{12}$, όπου ισχύει $[0] = [12]$, $[1] = [13]$ και ούτω καθ' εξής.

   Στην δεύτερη περίπτωση, όταν οι δείκτες του ωρολογίου μετρήσουν 24 ώρες, τότε η μέτρηση αρχίζει από την αρχή, δηλαδή έχουμε τον δακτύλιο $\mathbb{Z}_{24}$, όπου ισχύει $[0] = [24]$, $[1] = [25]$ και ούτω καθ' εξής.

   Επομένως, αν αυτή την στιγμή το ωρολόγιο δείχνει ότι η ώρα είναι 2 και μας ρωτήσουν τι ώρα θα δείχνει το ωρολόγιο μετά από 62 ώρες, καθένας, ακόμη και αυτός που δεν γνωρίζει Μαθηματικά, θα σκεφθεί ως εξής: Πρώτα πρέπει να δούμε τι ωρολόγιο χρησιμοποιούμε, με 12-ωρη αρίθμηση ή με 24-ωρη αρίθμηση.

   Αν έχουμε 24-ωρη αρίθμηση, θα πούμε $2 + 62 = 64 = 2 \cdot 24 + 16$. Επομένως, το ωρολόγιο θα δείχνει 16. Στην πραγματικότητα έχουμε ότι $64 \equiv 16 mod\, 24$.

   Αν έχουμε 12-ωρη αρίθμηση, θα πούμε $2 + 62 = 64 = 5 \cdot 24 + 4$. Επομένως, το ωρολόγιο θα δείχνει 4. Στην πραγματικότητα έχουμε ότι $64 \equiv 4 mod\, 12$.

   Επίσης, ένα άλλο παράδειγμα με την μέτρηση του χρόνου (σε εβδομάδες) είναι το εξής: Σήμερα είναι Δευτέρα, τι μέρα της εβδομάδας θα έχουμε μετά από 153 ημέρες;

   Εδώ έχουμε τον δακτύλιο $\mathbb{Z}_7$ και παρατηρούμε ότι $153 = 21 \cdot 7 + 6$, επομένως η ημέρα που αναζητούμε είναι η Κυριακή.

   Στην πραγματικότητα έχουμε ότι $153 \equiv 6 mod\, 7$.

2. Ας μελετήσουμε τον δακτύλιο

$$\mathbb{Z}_{12} = \{[0], [1], \ldots, [10], [11]\}.$$

   Θέλουμε να βρούμε το αντίθετο ενός στοιχείου $[a] \in \mathbb{Z}_{12}$. Θα έλεγε κάποιος θα ελέγξουμε, με δοκιμές, ποιο στοιχείο $[b] \in \mathbb{Z}_{12}$ έχει την ιδιότητα:

$$[a] + [b] = [0]$$

   και αυτό να γίνει για όλα τα στοιχεία του $\mathbb{Z}_{12}$. Μα αυτό είναι επίπονο και μάλλον ατελέσφορο, όταν αντί του $\mathbb{Z}_{12}$ έχουμε γενικά τον δακτύλιο $\mathbb{Z}_m$.

   Θα το αντιμετωπίσουμε γενικά (ιδέ το ερώτημα στην απόδειξη της προηγουμένης πρότασης).

   Για ένα $[a] \in \mathbb{Z}_{12}$ αναζητούμε ένα $[b] \in \mathbb{Z}_{12}$, έτσι ώστε

$$[a] + [b] = [0] = [12].$$

Συνεπώς, για $b = 12 - a$ έχουμε πράγματι $[a] + [b] = [0]$. Οπότε,

$$-[1] = [11], -[2] = [10]$$

και ούτω καθ' εξής.

Ας υπολογίσουμε την πολλαπλασιαστική ομάδα $U(\mathbb{Z}_{12})$. Η ομάδα αυτή αποτελείται από όλα τα αντιστρέψιμα στοιχεία του δακτυλίου $\mathbb{Z}_{12}$. Προφανώς το $[1] \in \mathbb{Z}_{12}$. Ας εξετάσουμε αν το $[2] \in U(\mathbb{Z}_{12})$. Αναζητούμε, αν υπάρχει, κάποιο $[x] \in \mathbb{Z}_{12}$, ώστε $[2] \cdot [x] = [1]$, δηλαδή

$$[2 \cdot x] = [1].$$

Τι σημαίνει η τελευταία σχέση; Πρόκειται για ισότητα κλάσεων ισοδυναμίας, άρα πρέπει

$$2x \equiv 1 mod\, 12,$$

δηλαδή πρέπει το $2x - 1$ να είναι πολλαπλάσιο του 12. Αυτό όμως δεν μπορεί να συμβεί για κανέναν ακέραιο x (γιατί;). Επομένως, το στοιχείο $[2] \notin U(Z_{12})$.

Ας εξετάσουμε αν το $[5] \in \mathbb{Z}_{12}$ έχει αντίστροφο. Αναζητούμε, αν υπάρχει, κάποιο $[x] \in \mathbb{Z}_{12}$, ώστε $[5] \cdot [x] = [1]$, δηλαδή

$$[5 \cdot x] = [1].$$

Τι σημαίνει η τελευταία σχέση; Πρόκειται για ισότητα κλάσεων ισοδυναμίας, άρα πρέπει

$$5x \equiv 1 mod\, 12,$$

δηλαδή πρέπει το $5x - 1$ να είναι πολλαπλάσιο του 12. Παρατηρούμε ότι, για $x = 5$, έχουμε $[5] \cdot [5] = [1]$. Δηλαδή, το στοιχείο $[5] \in U(Z_{12})$.

Με τον ίδιο τρόπο θα μπορούσαμε να δοκιμάσουμε για όλα τα στοιχεία του δακτυλίου $\mathbb{Z}_{12}$. Προσπαθήστε το! Είναι επίπονο ή μάλλον ατελέσφορο, όταν αντί του $\mathbb{Z}_{12}$ έχουμε γενικά τον δακτύλιο $\mathbb{Z}_m$.

Επομένως, πρέπει να αναζητήσουμε μια γενική μέθοδο υπολογισμού της πολλαπλασιαστικής ομάδας $U(\mathbb{Z}_m)$ για τον τυχαίο θετικό ακέραιο m και όχι μόνο για $m = 12$.

Επ' αυτού θα επανέλθουμε αργότερα.

Επίσης, στον δακτύλιο $\mathbb{Z}_{12}$ παρατηρούμε ότι $[4] \cdot [3] = [0]$, δηλαδή, ενώ έχουμε δύο μη μηδενικά στοιχεία, το γινόμενό τους ισούται με μηδέν, κάτι που αντιβαίνει με τον "κανόνα" που ισχύει στον δακτύλιο των ακεραίων. "*Το γινόμενο δύο ακεραίων αριθμών ισούται με μηδέν, αν και μόνο αν τουλάχιστον ένας από τους παράγοντες είναι ίσος με μηδέν*".

Παρατήρηση Γ.2.6. Στο τελευταίο παράδειγμα, όπως και προηγουμένως, (ιδέ τις Ασκήσεις $5.1.5_{6,7}$) βλέπουμε ότι υπάρχουν δακτύλιοι με την ιδιότητα, το γινόμενο δύο μη μηδενικών στοιχείων τους να ισούται με μηδέν, δηλαδή υπάρχουν στοιχεία $0 \neq a$, $0 \neq b$ του δακτυλίου, ώστε $a \cdot b = 0$. Τα στοιχεία αυτά ονομάζονται **μηδενοδιαιρέτες** του δακτυλίου. Συγκεκριμένα, το a ονομάζεται αριστερός μηδενοδιαιρέτης και το b δεξιός μηδενοδιαιρέτης[7].

Επ' αυτού δεν θα επεκταθούμε περαιτέρω.

[7]Επειδή πάντα ισχύει ότι $0 \cdot a = a \cdot 0 = 0$ για όλα τα στοιχεία ενός δακτυλίου, το μηδέν δεν συγκαταλέγεται στους μηδενοδιαιρέτες ενός δακτυλίου.

Στο τελευταίο παράδειγμα είχαμε αντιμετωπίσει το πρόβλημα πώς υπολογίζουμε τα στοιχεία της πολλαπλασιαστικής ομάδας $U(\mathbb{Z}_{12})$ και γενικά της πολλαπλασιαστικής ομάδας $U(\mathbb{Z}_m)$.

Ας κάνουμε την "*ανάλυση*" του προβλήματος. Έστω $[a] \in \mathbb{Z}_m$. Αναζητούμε, αν υπάρχει, ένα $[x] \in \mathbb{Z}_m$, έτσι ώστε

$$[a] \cdot [x] = [1].$$

Τι σημαίνει η τελευταία σχέση; Πρόκειται για ισότητα κλάσεων ισοδυναμίας, άρα πρέπει και αρκεί

$$ax \equiv 1 mod\, m,$$

δηλαδή πρέπει και αρκεί το $ax - 1$ να είναι πολλαπλάσιο του m. Δηλαδή πρέπει και αρκεί να υπάρχει $k \in \mathbb{Z}$, ώστε $ax - 1 = km$, άρα πρέπει και αρκεί να υπάρχει $k \in \mathbb{Z}$, ώστε $ax + (-k)m = 1$. Από την τελευταία σχέση έπεται ότι πρέπει και αρκεί οι a και m να είναι σχετικά πρώτοι (γιατί; Ιδέ Πρόταση 6.1.21). Άρα αποδείξαμε την εξής πρόταση:

Πρόταση Γ.2.7. *Η πολλαπλασιαστική ομάδα του δακτυλίου $\mathbb{Z}_m$ είναι ίση με*

$$U(\mathbb{Z}_m) = \{[a] \in \mathbb{Z}_m \mid \text{μ.κ.δ.}(a, m) = 1\}.$$

Μάλιστα δε

$$| U(\mathbb{Z}_m) | = \varphi(m),$$

όπου φ είναι η συνάρτηση του Euler.

Απόδειξη. Η απόδειξη έχει προηγηθεί, με τις λεπτομέρειες να αφήνονται ως άσκηση. ό.έ.δ.

Ως γνωστόν (Ορισμός 5.1.41), σώμα είναι ένας μεταθετικός δακτύλιος με μονάδα, όπου όλα τα μη μηδενικά στοιχεία του έχουν αντίστροφο. Επομένως, για να απαντήσουμε στο ερώτημα, πότε ο δακτύλιος $\mathbb{Z}_m$ είναι σώμα, πρέπει και αρκεί να αποφανθούμε, πότε όλα τα μη μηδενικά στοιχεία έχουν αντίστροφο. Από την προηγουμένη πρόταση έχουμε ότι ένα στοιχείο $[a] \in \mathbb{Z}_m$ είναι αντιστρέψιμο, αν και μόνο αν

$$\text{μ.κ.δ.}(a, m) = 1.$$

Υποθέτουμε ότι ο ακέραιος αριθμός m είναι σύνθετος, τότε υπάρχουν θετικοί ακέραιοι αριθμοί r, s μεγαλύτεροι του 1, έτσι ώστε $m = r \cdot s$. Αλλά τότε τα στοιχεία $[r], [s] \in \mathbb{Z}_m$ δεν είναι αντιστρέψιμα (γιατί;). Άρα στην περίπτωση αυτή ο δακτύλιος $\mathbb{Z}_m$ δεν είναι σώμα.

Υποθέτουμε ότι ο ακέραιος αριθμός m είναι πρώτος, τότε για κάθε $k \in \mathbb{Z}$ με $1 \leq k \leq m - 1$ ισχύει ότι μ.κ.δ.$(k, m) = 1$ (γιατί;). Επομένως, στην περίπτωση αυτή έχουμε ότι όλα τα μη μηδενικά στοιχεία του δακτυλίου $\mathbb{Z}_m$ έχουν αντίστροφο. Δηλαδή ο δακτύλιος $\mathbb{Z}_m$ είναι σώμα.

Θεώρημα Γ.2.8. *Ο δακτύλιος $\mathbb{Z}_m$ είναι σώμα, αν και μόνο αν ο m είναι πρώτος αριθμός.*

Απόδειξη. Η απόδειξη έχει προηγηθεί, με τις λεπτομέρειες να αφήνονται ως άσκηση (Άσκηση $\Gamma.2.3_3$). ό.έ.δ.

Ως προς την προσθετική ομάδα του δακτυλίου $\mathbb{Z}_m$, προφανώς αυτή είναι κυκλική και ένας γεννήτοράς της είναι ο $[1]$, δεδομένου ότι, από τον ορισμό της πρόσθεσης, έχουμε ότι

$$[r] = [\underbrace{1+1+\cdots+1}_{r}] = \underbrace{[1]+[1]+\cdots+[1]}_{r} = r[1].$$

Συνεπώς, από το Θεώρημα Γ.1.8 και την Πρόταση Γ.2.7 έπεται η εξής πρόταση:

Πρόταση Γ.2.9. *Στον δακτύλιο $\mathbb{Z}_m$ οι γεννήτορες της προσθετικής ομάδας είναι ακριβώς τα στοιχεία της πολλαπλασιαστικής ομάδας $U(\mathbb{Z}_m)$.*

Απόδειξη. Η απόδειξη είναι απλός συνδυασμός των δύο αποτελεσμάτων που προαναφέραμε, με τις λεπτομέρειες να αφήνονται ως άσκηση (Άσκηση Γ.2.3$_4$). ό.έ.δ.

Γ.2.2 Ο δακτύλιος των πολυωνύμων

Η έννοια του πολυωνύμου είναι *οικεία*, σε όλους, από τα *Γυμνασιακά χρόνια*, παρ' όλα ταύτα, εκεί, συνήθως υπάρχουν ασάφειες και παρανοήσεις, οι οποίες μας *ακολουθούν* στα μετέπειτα.

Η μελέτη των πολυωνύμων με συντελεστές από έναν δακτύλιο αποτελεί έναν μεγάλο και ανεξάρτητο κλάδο των Μαθηματικών.

Εδώ θα προσπαθήσουμε να δώσουμε μια απλή παρουσίαση για να μπορούμε να χειριζόμαστε τα πολυώνυμα, όπου αυτά εμφανίζονται. Δεν θα επεκταθούμε περισσότερο καθότι μια, έστω και μικρή, απόπειρα εμβάθυνσης θα ήταν πέραν του σκοπού μας.

Ας ξεκινήσουμε "ανορθόδοξα" με ένα παράδειγμα.

Υποθέτουμε ότι θέλουμε να "επεκτείνουμε" τον δακτύλιο $\mathbb{Z}$ των ακεραίων σε έναν (μεγαλύτερο) δακτύλιο, ούτως ώστε να "συμπεριλάβουμε[8]" τον αριθμό $\pi = 3.14...$. Ένας τέτοιος "διευρυμένος" δακτύλιος, προφανώς (γιατί;), πέραν των ακεραίων και του αριθμού π, θα περιέχει και τους αριθμούς $-\pi$, $2\pi^2$, $3\pi^2+4\pi^3$, ... και γενικά κάθε *πολυωνυμική* έκφραση

$$a_0 + a_1\pi + a_2\pi^2 + \cdots a_n\pi^n,$$

όπου οι a_i είναι ακέραιοι αριθμοί.

Ας *πορευθούμε* αντίστροφα. Έστω

$$\mathbb{Z}[\pi] = \{a_0 + a_1\pi + a_2\pi^2 + \cdots a_n\pi^n \mid a_i \in \mathbb{Z},\ n \geq 0\}$$

το σύνολο όλων των πολυωνυμικών εκφράσεων του π. Προφανώς, το σύνολο αυτό είναι ένας υποδακτύλιος του δακτυλίου των πραγματικών αριθμών, δεδομένου ότι το άθροισμα και το γινόμενο δύο τέτοιων πολυωνυμικών εκφράσεων του π είναι και αυτό μια πολυωνυμική έκφραση του π.

Επομένως, ο "αμέσως μεγαλύτερος" δακτύλιος, που περιέχει τους ακεραίους και τον αριθμό π είναι ο $\mathbb{Z}[\pi]$.

Στο παράδειγμα αυτό, όπου στον δακτύλιο $\mathbb{Z}$ "προσαρτήσαμε" τον πραγματικό αριθμό π, έχουμε ένα πλεονέκτημα και ένα μειονέκτημα. Το πλεονέκτημα είναι ότι βρισκόμαστε εντός του δακτυλίου των πραγματικών αριθμών και οι σημειωμένες πράξεις στην έκφραση $a_0 + a_1\pi + a_2\pi^2 + \cdots a_n\pi^n$ δεν είναι τίποτε άλλο από τις πράξεις μεταξύ πραγματικών αριθμών. Το μειονέκτημα είναι ότι περιοριζόμαστε στον συγκεκριμένο αριθμό π και στον δακτύλιο των πραγματικών αριθμών, εντός του οποίου είμαστε υποχρεωμένοι να "κινηθούμε".

[8] Προς το παρόν χρησιμοποιούμε τις λέξεις "επεκτείνουμε", "συμπεριλάβουμε" εντελώς διαισθητικά.

Ας υποθέσουμε ότι έχουμε έναν δακτύλιο και θέλουμε να τον "επεκτείνουμε" σε έναν άλλο δακτύλιο, ώστε να συμπεριλάβουμε ένα ακόμη στοιχείο, το οποίο δεν ανήκει σε άλλον δακτύλιο. Το προηγούμενο παράδειγμα μας "κατευθύνει" πώς θα το επιτύχουμε.

Ορισμός Γ.2.10. Έστω R ένας μεταθετικός δακτύλιος με μονάδα[9] και x ένα αυθαίρετο σύμβολο. Μια τυπική έκφραση της μορφής

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

όπου $a_0, a_1, \ldots, a_n \in R,\ n \geq 0$ θα ονομάζεται **πολυώνυμο** ως προς x με συντελεστές από τον δακτύλιο R. Τα στοιχεία a_i θα ονομάζονται **συντελεστές** του πολυωνύμου και οι εκφράσεις a_ix^i θα ονομάζονται **όροι** ή **μονώνυμα** του πολυωνύμου. Το σύνολο όλων των πολυωνύμων θα συμβολίζεται με $R[x]$.

Πριν προχωρήσουμε, παραθέτουμε κάποιους επιπλέον ορισμούς και ορολογία.

Ένα πολυώνυμο συνήθως θα συμβολίζεται ως εξής:

$$r(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

και ως **βαθμό** του πολυωνύμου θα ορίσουμε τον μεγαλύτερο n, ώστε ο αντίστοιχος συντελεστής a_n να είναι διάφορος του μηδενός. Δηλαδή $a_n \neq 0$ και $a_i = 0$ για όλα τα $i > n$. Ο βαθμός ενός πολυωνύμου $r(x)$ θα συμβολίζεται με $deg\, r(x)$. Στην περίπτωση αυτή ο a_nx^n θα ονομάζεται **μεγιστοβάθμιος** όρος και το a_n συντελεστής του μεγιστοβαθμίου όρου. Στην περίπτωση, όπου ο συντελεστής του μεγιστοβαθμίου όρου ισούται με την μονάδα του δακτυλίου, το πολυώνυμο θα ονομάζεται **μονικό**.

Το πολυώνυμο, όπου όλοι οι συντελεστές του είναι ίσοι με μηδέν, δηλαδή το

$$0(x) = 0 + 0x + 0x^2 + \cdots$$

θα ονομάζεται το **μηδενικό** πολυώνυμο. Στο μηδενικό πολυώνυμο δεν προσάπτουμε βαθμό δεδομένου ότι, βάσει του ορισμού, δεν έχει μη μηδενικούς συντελεστές[10].

Το πολυώνυμο $p(x) = a_0$ με $a_0 \neq 0$ είναι το **σταθερό** πολυώνυμο, έχει μηδενικό βαθμό και δεν πρέπει να συγχέεται με το μηδενικό πολυώνυμο.

Δύο πολυώνυμα θα ονομάζονται **ίσα**, αν έχουν ίσους βαθμούς και τους αντίστοιχους συντελεστές ίσους. Δηλαδή, αν

$$r(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \quad \text{και} \quad s(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m,$$

τα $r(x)$ και $s(x)$ είναι ίσα, αν $n = m$ και $a_i = b_i$ για $i = 0, 1, 2, \ldots, n$.

Παρατηρήσεις Γ.2.11.

1. Όπως προαναφέραμε, το x είναι ένα αυθαίρετο σύμβολο και δεν πρέπει να το συγχέουμε με ένα άγνωστο στοιχείο ενός δακτυλίου, το οποίο καλούμαστε να "ανακαλύψουμε". Θα μπορούσαμε να το θεωρήσουμε ως ένα σύμβολο, όπου οι "δυνάμεις" x^n αποτελούν τους "δείκτες θέσης" των συντελεστών $a_0, a_1, a_2, \cdots$. Το σύμβολο x θα ονομάζεται **μεταβλητή**.

[9] Εδώ θα ορίσουμε τα πολυώνυμα ξεκινώντας από έναν μεταθετικό δακτύλιο με μονάδα. Πολυώνυμα μπορούν να ορισθούν και γενικά χωρίς να υποθέσουμε ότι ο δακτύλιος, τον οποίο έχουμε ως αφετηρία, είναι μεταθετικός με μονάδα, αλλά αυτό δεν θα μας απασχολήσει εδώ.

[10] Πολλοί συγγραφείς, για *διαχειριστικούς* λόγους στο μηδενικό πολυώνυμο προσάπτουν ως βαθμό το $-\infty$.

2. Ένα πολυώνυμο, συνήθως, το παριστάνουμε κατά τις "ανιούσες" δυνάμεις του x, ως
$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$
ή κατά τις "κατιούσες" δυνάμεις του x, ως
$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0.$$

3. Δεν πρέπει να συγχέουμε την έννοια του πολυωνύμου, όπως το ορίσαμε προηγουμένως, με την έννοια της πολυωνυμικής συνάρτησης/απεικόνισης. Σε μια απεικόνιση έχουμε πεδίο ορισμού και πεδίο τιμών. Στα πολυώνυμα δεν έχουμε αυτές τις έννοιες. Η σύγχυση προκύπτει, διότι τα πολυώνυμα, πολλές φορές, τα χρησιμοποιούμε για να ορίσουμε απεικονίσεις, όπου το x επιτρέπεται να λαμβάνει τιμές από έναν δακτύλιο E, ο οποίος περιέχει τον δακτύλιο των συντελεστών R και τα σημειούμενα σύμβολα (πρόσθεση και πολλαπλασιασμός) στην γραφή του πολυωνύμου να αποκτούν την πραγματική τους σημασία στον δακτύλιο E. Εξ' ου και το όνομα μεταβλητή για το x.

   Για παράδειγμα: Τα πολυώνυμα $f(x) = x^3, r(x) = x^5 \in \mathbb{Z}_3[x]$ είναι δύο διαφορετικά πολυώνυμα (βάσει του ορισμού της ισότητας πολυωνύμων), αλλά αν θεωρήσουμε τις απεικονίσεις $\bar{f} : \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$ και $\bar{r} : \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$ με "*τύπο*"
$$\bar{f}(t) = t^3 \quad \text{και} \quad \bar{r}(t) = t^5 \ [11],$$
   βλέπουμε ότι πρόκειται (γιατί;) για ίσες απεικονίσεις (Ορισμός 4.5.7).

   Επ' αυτού θα επανέλθουμε αργότερα.

Για να αποκτήσει το σύνολο των πολυωνύμων $R[x]$ δομή δακτυλίου, πρέπει να ορίσουμε μια πρόσθεση και έναν πολλαπλασιασμό πολυωνύμων.

Ορισμός Γ.2.12. Έστω R ένας μεταθετικός δακτύλιος με μονάδα. Στο σύνολο $R[x]$ όλων των πολυωνύμων με συντελεστές από τον δακτύλιο R ορίζουμε δύο πράξεις ως εξής:
Έστω $f(x) = a_0+a_1x+a_2x^2+\cdots+a_nx^n$, $g(x) = b_0+b_1x+b_2x^2+\cdots+b_mx^m \in R[x]$.
Ορίζουμε ως πρόσθεση των $f(x)$ και $g(x)$ το πολυώνυμο
$$\begin{aligned}(f+g)(x) &= f(x) + g(x)\\ &= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_{s-1} + b_{s-1})x^{s-1} + (a_s + b_s)x^s,\end{aligned}$$
όπου s ο μεγαλύτερος εκ των δύο βαθμών n και m και $a_i = 0$, για $i > n$ και $b_i = 0$, για $i > m$.
Ορίζουμε ως πολλαπλασιασμό των $f(x)$ και $g(x)$ το πολυώνυμο
$$(f \cdot g)(x) = f(x) \cdot g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n+m-1}x^{n+m-1} + c_{n+m}x^{n+m},$$
όπου
$$c_k = a_kb_0 + a_{k-1}b_1 + \cdots a_1b_{k-1} + a_0b_k = \sum_{k=i+j} a_ib_j,$$
για $k = 0, 1, 2, \ldots, n + m$.

[11] Σκόπιμα χρησιμοποιήσαμε τον συμβολισμό $\bar{f}$, $\bar{r}$, και το t για να κάνουμε την διάκριση μεταξύ πολυωνύμου και πολυωνυμικής απεικόνισης.

Προφανώς(;) οι πράξεις αυτές είναι καλά ορισμένες.

Πρέπει να επισημάνουμε ότι το σύμβολο + της πρόσθεσης μεταξύ των πολυωνύμων $f(x)+g(x)$ είναι το σύμβολο της πράξης της πρόσθεσης που ορίσαμε μεταξύ πολυωνύμων και δεν πρέπει να συγχέεται, ούτε με το σύμβολο +, που εμφανίζεται στην τυπική γραφή των πολυωνύμων, ούτε με το σύμβολο +, που εμφανίζεται μεταξύ των συντελεστών a_i+b_i και το οποίο δηλώνει την πράξη της πρόσθεσης μεταξύ στοιχείων του δακτυλίου R.

Το ίδιο ισχύει για το σύμβολο $\cdot$ μεταξύ των πολυωνύμων $f(x)\cdot g(x)$, που δηλώνει την πράξη του πολλαπλασιασμού που ορίσαμε μεταξύ πολυωνύμων.

Όλα αυτά, τόσο το σύμβολο +, όσο και το σύμβολο $\cdot$ αποκτούν "ενιαία" σημασία στο σύνολο $R[x]$, όπως θα δούμε στο επόμενο θεώρημα.

Θεώρημα Γ.2.13. *Έστω R ένας μεταθετικός δακτύλιος με μονάδα. Το σύνολο $(R[x],+,\cdot)$ των πολυωνύμων με συντελεστές από τον δακτύλιο R είναι μεταθετικός δακτύλιος με μονάδα με πράξεις την πρόσθεση και πολλαπλασιασμό, που ορίσαμε προηγουμένως.*[12]

Απόδειξη. Ο έλεγχος ότι πληρούνται οι ιδιότητες του Ορισμού 5.1.37 είναι εύκολος, όπου το ουδέτερο ως προς την πρόσθεση είναι το μηδενικό πολυώνυμο $0(x)$ και το ουδέτερο ως προς τον πολλαπλασιασμό το σταθερό πολυώνυμο 1.

Εδώ απλώς θα αποδείξουμε την προσεταιριστικότητα του πολλαπλασιασμού και τον επιμερισμό του πολλαπλασιασμού ως προς την πρόσθεση.

Έστω $\alpha(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$, $\beta(x)=b_0+b_1x+b_2x^2+\cdots+b_mx^m$, $\gamma(x)=c_0+c_1x+c_2x^2+\cdots+c_kx^k\in R[x]$. Τότε για το γινόμενο $\alpha(x)\cdot\beta(x)$ έχουμε ότι ισχύει

$$\alpha(x)\cdot\beta(x)=d_0+d_1x+d_2x^2+\cdots+d_{n+m-1}x^{n+m-1}+d_{n+m}x^{n+m},$$

όπου

$$d_\nu=\sum_{\nu=i+j}a_ib_j,$$

για $\nu=0,1,2,\ldots,n+m$. Επομένως,

$$\begin{aligned}&(\alpha(x)\cdot\beta(x))\cdot\gamma(x)=\\&=(d_0+d_1x+d_2x^2+\cdots+d_{n+m-1}x^{n+m-1}+d_{n+m}x^{n+m})\cdot(c_0+c_1x+c_2x^2+\cdots+c_kx^k)\\&=e_0+e_1x+e_2x^2+\cdots+e_{n+m+k}x^{n+m+k},\end{aligned}$$

όπου

$$e_\mu=\sum_{\mu=\nu+s}d_\nu c_s=\sum_{\mu=\nu+s}\Big(\sum_{\nu=i+j}a_ib_j\Big)c_s,$$

για $\mu=0,1,2,\ldots,n+m+k$. Από την τελευταία ισότητα (λόγω του επιμερισμού του πολλαπλασιασμού ως προς την πρόσθεση στον δακτύλιο R) έχουμε ότι

$$e_\mu=\sum_{\mu=i+j+s}a_ib_jc_s,$$

για $\mu=0,1,2,\ldots,n+m+k$.

[12] Όπως έχουμε προείπει, όταν αναφερόμαστε στον δακτύλιο των πολυωνύμων $R[x]$, πάντα ο δακτύλιος R θα θεωρείται μεταθετικός με μονάδα, έστω και αν αυτό δεν αναφέρεται ρητά.

Επαναλαμβάνοντας την ίδια διαδικασία, υπολογίζοντας πρώτα το γινόμενο $\beta(x)\cdot\gamma(x)$ και μετά το γινόμενο $\alpha(x)\cdot(\beta(x)\cdot\gamma(x))$ καταλήγουμε ότι ο συντελεστής του μ όρου είναι πάλι ο

$$e_\mu = \sum_{\mu=i+j+s} a_i b_j c_s,$$

για $\mu = 0, 1, 2, \dots, n+m+k$.

Άρα τελικά

$$\alpha(x)\cdot(\beta(x)\cdot\gamma(x)) = (\alpha(x)\cdot\beta(x))\cdot\gamma(x).$$

Για τον επιμερισμό του πολλαπλασιασμού ως προς την πρόσθεση έχουμε ότι

$$\begin{aligned}\alpha(x)\cdot(\beta(x)+\gamma(x)) &= (a_0+a_1x+a_2x^2+\cdots+a_nx^n)\cdot\\ &\quad\cdot[(b_0+c_0)+(b_1+c_1)x+(b_2+c_2)x^2+\cdots+(b_s+c_s)x^s]\\ &= d_0+d_1x+d_2x^2+\cdots+d_{n+s}x^{n+s},\end{aligned}$$

όπου

$$d_\nu = \sum_{\nu=i+j} a_i(b_j+c_j) = \sum_{\nu=i+j}(a_ib_j+a_ic_j) = (\sum_{\nu=i+j} a_ib_j)+(\sum_{\nu=i+j} a_ic_j),$$

για $\nu = 0, 1, 2, \dots, n+s$ και s ο μεγαλύτερος εκ των δύο βαθμών m και k.

Αλλά το άθροισμα $\sum_{\nu=i+j} a_ib_j$ είναι ο συντελεστής του ν-οστού όρου του γινομένου $\alpha(x)\cdot\beta(x)$ και το άθροισμα $\sum_{\nu=i+j} a_ic_j$ είναι ο συντελεστής του ν-οστού όρου του γινομένου $\alpha(x)\cdot\gamma(x)$.

Άρα πράγματι ισχύει ότι $\alpha(x)\cdot(\beta(x)+\gamma(x)) = \alpha(x)\cdot\beta(x)+\alpha(x)\cdot\gamma(x)$. ό.έ.δ.

Από τον τρόπο ορισμού της πρόσθεσης και του πολλαπλασιασμού πολυωνύμων, έπεται ότι

$$deg(f(x)+g(x)) \le \max\{deg(f(x)), deg(g(x))\}$$

και

$$deg(f(x)\cdot g(x)) \le deg(f(x)) + deg(g(x))$$

(γιατί;)

Ένα ερώτημα που προκύπτει είναι, αν μπορούμε να προσδιορίσουμε τα αντιστρέψιμα στοιχεία του δακτυλίου πολυωνύμων $R[x]$, όπου, όπως πάντα, ο δακτύλιος R είναι μεταθετικός με μονάδα.

Πρόταση Γ.2.14. *Έστω $\mathbb{F}$ ένα σώμα, τότε για $f(x), g(x)\in\mathbb{F}[x]$ ισχύει ότι:*

$$deg(f(x)\cdot g(x)) = deg(f(x)) + deg(g(x)) \quad \textit{και} \quad U(\mathbb{F}[x]) = U(\mathbb{F}).$$

Δηλαδή, τα μόνα αντιστρέψιμα πολυώνυμα είναι τα σταθερά πολυώνυμα.

Απόδειξη. Η απόδειξη είναι προφανής, δεδομένου ότι ο δακτύλιος των συντελεστών είναι σώμα. ό.έ.δ.

Παρατήρηση Γ.2.15. Η υπόθεση στην προηγουμένη πρόταση, ότι ο δακτύλιος των συντελεστών είναι σώμα, είναι καίρια.

Για παράδειγμα, το πολυώνυμο $2x+1\in\mathbb{Z}_4[x]$, αν και όχι σταθερό, είναι αντιστρέψιμο, μάλιστα δε, συμπίπτει με το αντίστροφό του, δεδομένου ότι

$$(2x+1)(2x+1) = 4x^2+4x+1 = 1\in\mathbb{Z}_4[x].$$

Η διαίρεση πολυωνύμων.

Κατά πάσα πιθανότητα, από τα μαθητικά χρόνια, είναι γνωστή η διαίρεση πολυωνύμων με συντελεστές ρητούς ή πραγματικούς αριθμούς. Εδώ θα δώσουμε μια γενική παρουσίαση για πολυώνυμα με συντελεστές από ένα τυχαίο σώμα.

Ο Αλγόριθμος διαίρεσης πολυωνύμων

Θεώρημα Γ.2.16. *Έστω* $\beta(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{m-1}x^{m-1} + b_mx^m$ *ένα μη μηδενικό πολυώνυμο με συντελεστές από ένα σώμα* $\mathbb{F}$. *Για κάθε πολυώνυμο*

$$\alpha(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n \in \mathbb{F}[x]$$

υπάρχουν μοναδικά πολυώνυμα $\pi(x), \upsilon(x) \in \mathbb{F}[x]$, *έτσι ώστε*

$$\alpha(x) = \beta(x) \cdot \pi(x) + \upsilon(x)$$

και

$$\upsilon(x) = 0 \text{ ή } deg(\upsilon(x)) < deg(\beta(x)).$$

Απόδειξη. Αν $\alpha(x) = 0$ ή $deg(\alpha(x)) < deg(\beta(x))$, τότε προφανώς, για $\pi(x) = 0$ και $\upsilon(x) = \alpha(x)$, έχουμε ότι

$$\alpha(x) = \beta(x) \cdot \pi(x) + \upsilon(x).$$

Υποθέτουμε ότι υπάρχουν πολυώνυμα $\alpha(x) \in \mathbb{F}[x]$, για τα οποία δεν υπάρχουν $\pi(x), \upsilon(x) \in \mathbb{F}[x]$, έτσι ώστε

$$\alpha(x) = \beta(x) \cdot \pi(x) + \upsilon(x) \quad \text{και} \quad \upsilon(x) = 0 \text{ ή } deg(\upsilon(x)) < deg(\beta(x)).$$

Επιλέγουμε ένα πολυώνυμο

$$\alpha(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n$$

με τον μικρότερο δυνατό βαθμό, το οποίο δεν ικανοποιεί τις ανωτέρω συνθήκες.

Από τα προηγούμενα, έπεται ότι για το πολυώνυμο $\alpha(x)$ θα ισχύει

$$deg(\alpha(x)) \geq deg(\beta(x)).$$

Κατασκευάζουμε το εξής πολυώνυμο

$$A(x) = \alpha(x) - b_m^{-1}a_nx^{n-m} \cdot \beta(x).$$

Επειδή τα πολυώνυμα $\alpha(x)$ και $b_m^{-1}a_nx^{n-m} \cdot \beta(x)$ είναι ομοβάθμια και έχουν αντίθετους μεγιστοβάθμιους συντελεστές (γιατί;) έπεται ότι το πολυώνυμο $A(x)$ έχει βαθμό γνήσια μικρότερο από τον βαθμό του $\alpha(x)$. Συνεπώς, για το πολυώνυμο $A(x)$ υπάρχουν $\pi_1(x), \upsilon_1(x) \in \mathbb{F}[x]$, έτσι ώστε

$$A(x) = \beta(x) \cdot \pi_1(x) + \upsilon_1(x)$$

και

$$\upsilon_1(x) = 0 \text{ ή } deg(\upsilon_1(x)) < deg(\beta(x))$$

(Δεν ξεχνάμε ότι το πολυώνυμο $\alpha(x)$ είναι ένα πολυώνυμο με τον μικρότερο βαθμό, το οποίο δεν ικανοποιεί τις ανωτέρω συνθήκες).

Από τον τρόπο ορισμού του $A(x)$ έχουμε ότι

$$\begin{aligned}\alpha(x) &= A(x) + b_m^{-1}a_n x^{n-m}\cdot\beta(x)\\ &= \beta(x)\cdot\pi_1(x) + \upsilon_1(x) + b_m^{-1}a_n x^{n-m}\cdot\beta(x)\\ &= \beta(x)\cdot(\pi_1(x) + b_m^{-1}a_n x^{n-m}) + \upsilon_1(x),\end{aligned}$$

οπότε θέτοντας $\pi(x) = \pi_1(x) + b_m^{-1}a_n x^{n-m}$ έχουμε ότι

$$\alpha(x) = \beta(x)\cdot\pi(x) + \upsilon_1(x).$$

Μα αυτό είναι άτοπο από την υπόθεση επιλογής του $\alpha(x)$. Συνεπώς, για όλα τα πολυώνυμα $\alpha(x)$ και $\beta(x)$, με το $\beta(x)$ μη μηδενικό, υπάρχουν πολυώνυμα

$$\pi(x), \upsilon(x) \in \mathbb{F}[x],$$

τα οποία πληρούν τις ανωτέρω συνθήκες.

Υποθέτουμε ότι υπάρχουν και άλλα δύο πολυώνυμα $p(x)$, $u(x) \in \mathbb{F}[x]$, τα οποία πληρούν τις ανωτέρω συνθήκες. Τότε θα έχουμε ότι

$$\alpha(x) = \beta(x)\cdot\pi(x) + \upsilon(x) \quad \text{και} \quad \alpha(x) = \beta(x)\cdot p(x) + u(x),$$

οπότε αφαιρώντας κατά μέλη έχουμε ότι

$$\beta(x)\cdot(\pi(x) - p(x)) + (\upsilon(x) - u(x)) = 0.$$

Αν $\pi(x) \neq p(x)$, τότε το πολυώνυμο $\beta(x)\cdot(\pi(x) - p(x)) + (\upsilon(x) - u(x))$ είναι μη μηδενικό (γιατί;).

Επομένως, αναγκαστικά $\pi(x) = p(x)$ και συνεπώς $\upsilon(x) = u(x)$. ό.έ.δ.

Παρατηρήσεις Γ.2.17.

1. Στο προηγούμενο Θεώρημα το πολυώνυμο $\beta(x)$ ονομάζεται **διαιρέτης** και το πολυώνυμο $\alpha(x)$ ονομάζεται **διαιρετέος**, ενώ τα πολυώνυμα $\pi(x)$ και $\upsilon(x)$ ονομάζονται **πηλίκο** και **υπόλοιπο** αντίστοιχα.

2. Οι εκφράσεις: "Το πολυώνυμο $\beta(x)$ διαιρεί το πολυώνυμο $\alpha(x)$", "Το πολυώνυμο $\alpha(x)$ είναι πολλαπλάσιο του πολυωνύμου $\beta(x)$", "Το πολυώνυμο $\beta(x)$ είναι παράγοντας του πολυωνύμου $\alpha(x)$" είναι Μαθηματικά ισοδύναμες και δηλώνουν ότι το υπόλοιπο της διαίρεσης του πολυωνύμου $\alpha(x)$ με το πολυώνυμο $\beta(x)$, είναι το μηδενικό πολυώνυμο.

   Στην περίπτωση αυτή χρησιμοποιούμε τον συμβολισμό $\beta(x) \mid \alpha(x)$.

3. Για να ισχύει το προηγούμενο θεώρημα, είναι αναγκαία η υπόθεση το πολυώνυμο $\beta(x)$ να είναι μη μηδενικό (γιατί;)

4. Η υπόθεση ότι οι συντελεστές των πολυωνύμων $\beta(x)$ και $\alpha(x)$ είναι από ένα σώμα είναι καίρια στο ότι έχουμε την δυνατότητα να "χρησιμοποιήσουμε" τον αντίστροφο του μεγιστοβαθμίου όρου του διαιρέτη $\beta(x)$ στην κατασκευή του πολυωνύμου $A(x)$.

5. Η κατασκευή του πολυωνύμου $A(x)$ στην απόδειξη του Θεωρήματος *υποδεικνύει* τον τρόπο με τον οποίο, σε διαδοχικά βήματα, μπορούμε να υπολογίσουμε το πηλίκο και το υπόλοιπο της διαίρεσης πολυωνύμων.

Παραδείγματα Γ.2.18.

1. Να βρεθεί το πηλίκο και το υπόλοιπο της διαίρεσης του πολυωνύμου

$$\alpha(x) = 2x^4 - 3x^3 + x^2 - 4x + 3$$

με το πολυώνυμο

$$\beta(x) = 3x^2 + x - 2,$$

θεωρούμενα ως πολυώνυμα με ρητούς συντελεστές.

Ακολουθούμε τον αλγόριθμο που "*υπαγορεύεται*" από την απόδειξη του θεωρήματος. Θέτουμε

$$\begin{aligned}\alpha_1(x) &= \alpha(x) - \frac{2}{3}x^{4-2}\cdot\beta(x)\\ &= 2x^4 - 3x^3 + x^2 - 4x + 3 - \frac{2}{3}x^2(3x^2 + x - 2)\\ &= -\left(3 + \frac{2}{3}\right)x^3 + \left(1 + \frac{4}{3}\right)x^2 - 4x + 3\\ &= -\frac{11}{3x}^3 + \frac{7}{3}x^2 - 4x + 3.\end{aligned}$$

Επειδή ο βαθμός του $\alpha_1(x)$ είναι μεγαλύτερος του βαθμού του $\beta(x)$, σημειώνουμε το (ενδιάμεσο) πηλίκο $\pi_1(x) = \frac{2}{3}x^2$ και συνεχίζουμε με το πολυώνυμο

$$\alpha_1(x) = -\frac{11}{3}x^3 + \frac{7}{3}x^2 - 4x + 3$$

στην θέση του $\alpha(x)$ και έχουμε

$$\begin{aligned}\alpha_2(x) &= \alpha_1(x) - \left(-\frac{11}{9}x\cdot\beta(x)\right)\\ &= -\frac{11}{3}x^3 + \frac{7}{3}x^2 - 4x + 3 + \frac{11}{3}x^3 + \frac{11}{9}x^2 - \frac{22}{9}x\\ &= \frac{32}{9}x^2 - \frac{58}{9}x + 3.\end{aligned}$$

Ο βαθμός του $\alpha_2(x)$ είναι ίσος με τον βαθμό του $\beta(x)$, οπότε σημειώνουμε το (δεύτερο ενδιάμεσο) πηλίκο $\pi_2(x) = -\frac{11}{9}x$ και συνεχίζουμε με το πολυώνυμο

$$\alpha_2(x) = \frac{32}{9}x^2 - \frac{58}{9}x + 3$$

στην θέση του $\alpha_1(x)$ και έχουμε

$$\begin{aligned}\alpha_3(x) &= \alpha_2(x) - \left(\frac{32}{27}\cdot\beta(x)\right)\\ &= \frac{32}{9}x^2 - \frac{58}{9}x + 3 - \frac{32}{9}x^2 - \frac{32}{27}x + \frac{64}{27}\\ &= -\left(\frac{58}{9} + \frac{32}{27}\right)x + \left(3 + \frac{64}{27}\right)\\ &= -\frac{206}{27}x + \frac{145}{27}.\end{aligned}$$

Παρατηρούμε ότι ο βαθμός του $\alpha_3(x)$ είναι μικρότερος από τον βαθμό του $\beta(x)$, οπότε σταματάμε σημειώνοντας το (τρίτο ενδιάμεσο) πηλίκο $\pi_3(x) = \frac{32}{27}$ και θέτουμε $\upsilon(x) = -\frac{206}{27}x + \frac{145}{27}$. Συνεπώς, τελικά έχουμε

$$\begin{aligned}\alpha(x) &= (\pi_1(x) + \pi_2(x) + \pi_3(x)) \cdot \beta(x) + \upsilon(x)\\ &= \left(\frac{2}{3}x^2 - \frac{11}{9}x + \frac{32}{27}\right) \cdot \beta(x) + \upsilon(x).\end{aligned}$$

2. Να βρεθεί το πηλίκο και το υπόλοιπο της διαίρεσης του πολυωνύμου

$$\alpha(x) = 2x^4 - 3x^3 + x^2 - 4x + 3$$

με το πολυώνυμο

$$\beta(x) = 3x^2 + x - 2,$$

θεωρούμενα ως πολυώνυμα με συντελεστές από το σώμα $\mathbb{Z}_5$.

Πρώτα απ' όλα $\alpha(x) = 2x^4 + 2x^3 + x^2 + x + 3$, $\beta(x) = 3x^2 + x + 3 \in \mathbb{Z}_5[x]$ (γιατί;)

Ακολουθούμε τον αλγόριθμο που "*υπαγορεύεται*" από την απόδειξη του θεωρήματος, αλλά με προσοχή, διότι οι πράξεις μεταξύ των συντελεστών γίνονται στο σώμα $\mathbb{Z}_5$. Θέτουμε

$$\begin{aligned}\alpha_1(x) &= \alpha(x) - 2 \cdot 3^{-1}x^{4-2} \cdot \beta(x)\\ &= 2x^4 + 2x^3 + x^2 + x + 3 - x^2(3x^2 + x + 3)\\ &= -(3+1)x^3 + (1+3)x^2 + x + 3\\ &= 3x^3 + 4x^2 + x + 3.\end{aligned}$$

Επειδή ο βαθμός του $\alpha_1(x)$ είναι μεγαλύτερος του βαθμού του $\beta(x)$, σημειώνουμε το (ενδιάμεσο) πηλίκο $\pi_1(x) = 4x^2$ και συνεχίζουμε με το πολυώνυμο

$$\alpha_1(x) = 3x^3 + 4x^2 + x + 3$$

στην θέση του $\alpha(x)$ και έχουμε

$$\begin{aligned}\alpha_2(x) &= \alpha_1(x) - (x \cdot \beta(x))\\ &= 3x^3 - x^2 + x + 3 + 2x^3 + 4x^2 + 2x\\ &= 3x^2 + 3x + 3.\end{aligned}$$

Ο βαθμός του $\alpha_2(x)$ είναι ίσος με τον βαθμό του $\beta(x)$, οπότε σημειώνουμε το (δεύτερο ενδιάμεσο) πηλίκο $\pi_2(x) = x$ και συνεχίζουμε με το πολυώνυμο $\alpha_2(x) = 3x^2 + 3x + 3$ στην θέση του $\alpha_1(x)$ και έχουμε

$$\alpha_3(x) = \alpha_2(x) - (4 \cdot \beta(x)) = 3x^2 + 3x + 3 + 2x^2 + x + 2 = -(2+1)x = 2x.$$

Παρατηρούμε ότι ο βαθμός του $\alpha_3(x)$ είναι μικρότερος από τον βαθμό του $\beta(x)$, οπότε σταματάμε σημειώνοντας το (τρίτο ενδιάμεσο) πηλίκο $\pi_3(x) = 1$ και θέτουμε $\upsilon(x) = 2x$. Συνεπώς τελικά έχουμε

$$\alpha(x) = (\pi_x + \pi_2(x) + \pi_3(x)) \cdot \beta(x) + \upsilon(x) = (4x^2 + x + 1) \cdot \beta(x) + \upsilon(x).$$

Στον δακτύλιο των πολυωνύμων θα επανέλθουμε αργότερα.

Γ.2.3 Ασκήσεις

1. Δείξτε ότι στον δακτύλιο $\mathbb{Z}_m$ υπάρχει ένα αντιστρέψιμο στοιχείο $[1] \neq [a]$, το οποίο συμπίπτει με το αντίστροφό του, δηλαδή $[a]^{-1} = [a]$.

   Επίσης, δείξτε ότι υπάρχει ακριβώς ένα $[a]$, το οποίο συμπίπτει με το αντίθετό του, αν και μόνο αν ο m είναι άρτιος αριθμός. (Παραβάλλετε με τις Ασκήσεις 5.1.3$_{16,17}$).

2. Να ολοκληρώσετε, με κάθε λεπτομέρεια, την απόδειξη της Πρότασης Γ.2.3.

3. Να ολοκληρώσετε, με κάθε λεπτομέρεια, την απόδειξη του Θεωρήματος Γ.2.8.

4. Να ολοκληρώσετε, με κάθε λεπτομέρεια, την απόδειξη της Πρότασης Γ.2.9.

5. Έστω $U(\mathbb{Z}_m)$ η πολλαπλασιαστική ομάδα του δακτυλίου $\mathbb{Z}_m$. Δείξτε ότι για κάθε $[a] \in U(\mathbb{Z}_m)$ ισχύει ότι $[a]^{\varphi(m)} = [1]$.

   Το Θεώρημα του Euler
   Έστω m ένας θετικός ακέραιος και a ένας ακέραιος πρώτος προς τον m. Δείξτε ότι $a^{\varphi(m)} \equiv 1 mod\, m$.

   Θεώρημα του Fermat
   Έστω p ένας πρώτος αριθμός. Δείξτε ότι για κάθε ακέραιο αριθμό a ισχύει ότι

   $$a^p \equiv a mod\, p.$$

6. Έστω $n = 9.000.000$. Στην προσθετική ομάδα $(\mathbb{Z}_n, +)$, να βρεθούν όλα τα στοιχεία με τάξη ίση με 9.

7. Σε ένα διαγώνισμα εδόθη το σύνολο

   $$\{[1], [9], [16], [22], [53], [74], [79], [81]\} \subseteq \mathbb{Z}_{91}$$

   και εζητείτο να αποδειχθεί ότι αποτελεί υποομάδα της πολλαπλασιαστικής ομάδας $U(\mathbb{Z}_{91})$. Κατά λάθος όμως είχε παραλειφθεί ένα στοιχείο. Στα μέσα του διαγωνίσματος έγινε αντιληπτή η παράλειψη και ο καθηγητής ξεκίνησε να τους πει ποιο στοιχείο λείπει. Τότε οι περισσότεροι εξεταζόμενοι του είπαν ότι δεν χρειάζεται να τους το πει, διότι ήδη το είχαν βρει, Μπορείτε να ανακαλύψετε ποίο στοιχείο είχε παραλειφθεί;

   Πριν το ανακαλύψετε, μπορείτε να εξηγήσετε γιατί πράγματι ένα στοιχείο είχε παραλειφθεί;

8. Οι αριθμοί $[5], [15] \in \mathbb{Z}_{56}$ ανήκουν σε μία υποομάδα της πολλαπλασιαστικής ομάδας $U(\mathbb{Z}_{56})$, η οποία περιέχει 12 στοιχεία. Μπορείτε να υπολογίσετε τα υπόλοιπα 10 στοιχεία;

9. Να κατασκευάσετε τον πολλαπλασιαστικό πίνακα της ομάδας $U(\mathbb{Z}_{12})$.

10. Να υπολογίσετε την πολλαπλασιαστική ομάδα $U(\mathbb{Z}_{15})$ και να δείξετε ότι για κάθε $[a] \in U(\mathbb{Z}_{15})$ ισχύει ότι $[a]^4 = [1]$.

11. Δίνεται το σύνολο $G = \{[4], [8], [12], [16]\} \subseteq \mathbb{Z}_{20}$. Δείξτε ότι το σύνολο αυτό με πράξη τον πολλαπλασιασμό $mod\, 20$ αποτελεί ομάδα. Είναι η ομάδα αυτή υποομάδα της πολλαπλασιαστικής ομάδας $U(\mathbb{Z}_{20})$;

12. Στην πολλαπλασιαστική ομάδα $U(\mathbb{Z}_{20})$ να υπολογίσετε τις κυκλικές υποομάδες $\langle [3] \rangle$ και $\langle [7] \rangle$.

13. Να υπολογίσετε όλους τους μηδενοδιαιρέτες του δακτυλίων $\mathbb{Z}_{20}$ και $\mathbb{Z}_{11}$.

    Τι παρατηρείτε; Μπορείτε (κάνοντας και άλλους πειραματισμούς) να εικάσετε έναν γενικό "κανόνα" για τους μηδενοδιαιρέτες του δακτυλίου $\mathbb{Z}_m$, για τυχαίο $m \geq 1$;

14. Δείξτε ότι το υποσύνολο $\{ [0], [2], [4], [6], [8] \} \subseteq \mathbb{Z}_{10}$ είναι υποδακτύλιος. Δείξτε ότι ο υποδακτύλιος αυτός έχει ουδέτερο ως προς τον πολλαπλασιασμό.

    (Είναι ένα παράδειγμα, όπου ο δακτύλιος και ο υποδακτύλιος δεν έχουν το ίδιο μοναδιαίο στοιχείο).

15. Δείξτε ότι στον δακτύλιο $\mathbb{Z}_{10}$ η "εξίσωση" $2 \cdot x = 4$ έχει περισσότερες από μία λύσεις, ενώ η "εξίσωση" $3 \cdot x = 4$ έχει ακριβώς μια λύση.

    Μπορείτε να εξηγήσετε πού οφείλεται η διαφορά.

16. Είναι ο δακτύλιος $\mathbb{Z}_6$ υποδακτύλιος του δακτυλίου $\mathbb{Z}_{12}$;

17. Στους δακτυλίους $\mathbb{Z}_{36}, \mathbb{Z}_{12}$ και $\mathbb{Z}_{13}$ να υπολογίσετε όλα τα μηδενοδύναμα στοιχεία και όλους τους μηδενοδιαιρέτες.

18. Έστω $\mathbb{F}$ ένα σώμα και $f(x), g(x), p(x) \in \mathbb{F}[x]$ με $deg(f(x)) < deg(p(x))$ και $deg(g(x)) < deg(p(x))$. Υποθέτουμε ότι υπάρχουν πολυώνυμα $r(x), s(x) \in \mathbb{F}[x]$, έτσι ώστε $f(x) + r(x) \cdot p(x) = g(x) + s(x) \cdot p(x)$. Δείξτε ότι $f(x) = g(x)$.

19. Έστω $\mathbb{F}$ ένα σώμα. Δείξτε ότι υπάρχουν $a, b \in \mathbb{F}$, έτσι ώστε το πολυώνυμο $x^2 + x + 1$ να διαιρεί το πολυώνυμο $x^{43} + ax + b$.

20. Να βρεθεί το υπόλοιπο της διαίρεσης του x^{51} με το πολυώνυμο $x + 4 \in \mathbb{Z}_7[x]$.

21. Να βρεθεί το πηλίκο της διαίρεσης του πολυωνύμου x^3+2 με το $2x^2+3x+4$, όταν θεωρηθούν πολυώνυμα που ανήκουν στον δακτύλιο $\mathbb{Z}_3[x]$ και όταν θεωρηθούν πολυώνυμα που ανήκουν στον δακτύλιο $\mathbb{Z}_5[x]$.

22. Έστω $\mathbb{F}$ σώμα και $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$. Δείξτε ότι το $x - 1$ διαιρεί το $f(x)$, αν και μόνο αν $a_n + a_{n-1} + \cdots + a_1 + a_0 = 0$.

23. Δείξτε ότι δεν υπάρχει ακέραιος m και $q(x) \in \mathbb{Z}[x]$, ώστε

$$6x^4 + 50 = (3x^2 + 4x + m)q(x).$$

24. Μια μεγάλη εταιρεία, θέλοντας να παροτρύνει τους μαθητές της χώρας για την ενασχόλησή τους με τα Μαθηματικά προκήρυξε με έπαθλο 10.000 ΕΥΡΩ την λύση του εξής προβλήματος:

    "Να βρεθούν τρεις διαφορετικοί ακέραιοι αριθμοί a, b, c και ένα πολυώνυμο $p(x)$ με ακεραίους συντελεστές, ώστε $p(a) = b$, $p(b) = c$, $p(c) = a$."

    Πολλοί μαθητές προσπάθησαν, αλλά κανείς δεν τα κατάφερε[13].

[13] Οι υπεύθυνοι της εταιρείας έδρασαν *εκ του ασφαλούς*. Το πρόβλημα δεν έχει λύση (γιατί;). Αλλά έδωσαν μια καλή ευκαιρία (σημαντικότερη των χρημάτων;!;!) να ασχοληθούν οι μαθητές με τα Μαθηματικά!

Γ.3 Ομομορφισμοί Αλγεβρικών δομών

Η έννοια του ομομορφισμού μεταξύ Αλγεβρικών δομών είναι θεμελιώδης στα Μαθηματικά δεδομένου ότι μέσω αυτών μπορούμε να μελετήσουμε "*άγνωστες*" Αλγεβρικές δομές, μέσω άλλων Αλγεβρικών δομών, τις οποίες "γνωρίζουμε καλύτερα".

Ένα από τα πλέον αντιπροσωπευτικά παραδείγματα, αποτελεί η "ταυτοποίηση" κάθε σημείου του επιπέδου με ένα ζεύγος πραγματικών αριθμών (τις συντεταγμένες του σημείου).

Ας γίνουμε πιο σαφείς.

Ορισμός Γ.3.1. Έστω $(A, *)$ και $(B, \circ)$ δύο σύνολα εφοδιασμένα με τις πράξεις $*$ και $\circ$ αντίστοιχα. Μια απεικόνιση $f : A \longrightarrow B$ θα ονομάζεται **ομομορφισμός** ή απλώς **μορφισμός** μεταξύ των αλγεβρικών δομών $(A, *)$ και $(B, \circ)$, αν

$$f(a * b) = f(a) \circ f(b), \text{ για όλα τα } a, b \in A.$$

Παρατηρήσεις Γ.3.2.

1. Έχει επικρατήσει η έκφραση: Μια απεικόνιση μεταξύ δύο αλγεβρικών δομών είναι ομομορφισμός, αν "διατηρεί" τις πράξεις.

2. Είναι λάθος να αναφερόμαστε για ομομορφισμούς μεταξύ συνόλων, χωρίς να διευκρινίζουμε ποιες πράξεις διατηρούν (δεν ξεχνάμε ότι ένα σύνολο μπορεί να είναι εφοδιασμένο με περισσότερες από μία πράξεις).

Στα επόμενα θα αναφερθούμε, εν συντομία, σε ομομορφισμούς μεταξύ ομάδων και ομομορφισμούς μεταξύ δακτυλίων.

Γ.3.1 Ομομορφισμοί Ομάδων

Όπως προαναφέραμε, ένας ομομορφισμός μεταξύ δύο ομάδων $(G_1, *)$ και $(G_2, \circ)$ είναι μια απεικόνιση $f : G_1 \longrightarrow G_2$, έτσι ώστε $f(a * b) = f(a) \circ f(b)$, για όλα τα $a, b \in G_1$[14].

Πριν δούμε παραδείγματα ομομορφισμού ομάδων, ας δούμε μερικές ιδιότητες των ομομορφισμών ομάδων, οι οποίες απορρέουν απ' ευθείας από τον ορισμό.

Πρόταση Γ.3.3. *Έστω $f : G \longrightarrow M$ ένας ομομορφισμός ομάδων.*

i. Αν 1_G είναι το ουδέτερο στοιχείο της ομάδας G και 1_M το ουδέτερο της ομάδας M, τότε ισχύει ότι $f(1_G) = 1_M$.

ii. $f(g^{-1}) = (f(g))^{-1}$, για όλα τα $g \in G$.

iii. $f(a) = f(b)$, αν και μόνο αν $f(ab^{-1}) = 1_M$.

Απόδειξη.

i. Υποθέτουμε ότι $f(1_G) = e \in M$, Τότε, για κάθε $g \in G$ έχουμε

$$1_M f(g) = f(1_G g) = f(1_G) f(g) = e f(g),$$

οπότε, $e = 1_M$ (γιατί; Δεν ξεχνάμε τον Νόμο της διαγραφής στις ομάδες (Άσκηση 5.1.3$_3$).)

[14] Όταν δεν υπάρχει σύγχυση, ως προς ποιες πράξεις τα σύνολα G_1, G_2 αποτελούν ομάδα, τότε, για τον ομομορφισμό f, απλώς γράφουμε $f(ab) = f(a)f(b)$.

ii. Προφανώς $f(g)(f(g))^{-1} = 1_M$. Αλλά

$$1_M = f(1_G) = f(gg^{-1}) = f(g)f(g^{-1}).$$

Συνεπώς $f(g)(f(g))^{-1} = f(g)f(g^{-1})$. Εξού το ζητούμενο $f(g^{-1}) = (f(g))^{-1}$.

iii. Το αποτέλεσμα είναι άμεση συνέπεια των προηγουμένων, οπότε αφήνεται ως άσκηση. ό.έ.δ.

Παραδείγματα Γ.3.4.

1. Έστω G ομάδα, η ταυτοτική απεικόνιση $i : G \longrightarrow G$ με $i(g) = g$, για $g \in G$ προφανώς είναι ομομορφισμός ομάδων.

   Γενικότερα,

   Έστω G μια ομάδα και $K \leq G$. Η εμφύτευση $j : K \longrightarrow G$, με $j(k) = k$, για $k \in K$ είναι ομομορφισμός ομάδων.

2. Για κάθε δύο ομάδες G_1, G_2, η απεικόνιση $0 : G_1 \longrightarrow G_2$ με $0(x) = 1_{G_2}$, για όλα τα $x \in G_1$, προφανώς είναι ένας ομομορφισμός ομάδων (ο τετριμμένος ομομορφισμός).

3. Έστω $\mathbb{R}^*$ η ομάδα των μη μηδενικών πραγματικών αριθμών με πράξη τον πολλαπλασιασμό πραγματικών αριθμών. Η απεικόνιση $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ με $f(x) = \mid x \mid$ είναι προφανώς ένας ομομορφισμός ομάδων.

   (Δεν ξεχνάμε ότι η απόλυτη τιμή του γινομένου δύο πραγματικών αριθμών ισούται με το γινόμενο των αντιστοίχων απολύτων τιμών).

4. Η απεικόνιση $\varphi : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ με $\varphi(x) = x^2$ είναι ομομορφισμός ομάδων, διότι

$$\varphi(x \cdot y) = (x \cdot y)^2 = x^2 \cdot y^2 = \varphi(x) \cdot \varphi(y).$$

5. Έστω $\mathbb{R}$ η ομάδα όλων των πραγματικών αριθμών με πράξη την πρόσθεση πραγματικών αριθμών. Η απεικόνιση $h : \mathbb{R} \longrightarrow \mathbb{R}$ με $h(x) = x^2$ **δεν** είναι ομομορφισμός ομάδων, διότι

$$h(x + y) = (x + y)^2 \neq x^2 + y^2 = h(x) + h(y).$$

6. Έστω $\mathbb{Z}$ η προσθετική ομάδα των ακεραίων αριθμών και $\mathbb{Z}_m$, όπου m είναι ένας θετικός ακέραιος, η ομάδα των ακεραίων $mod\ m$ με πράξη την πρόσθεση $mod\ m$. Η απεικόνιση $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ με $\varphi(a) = [a]$ είναι ομομορφισμός ομάδων, διότι

$$\varphi(a + b) = [a + b] = [a] + [b] = \varphi(a) + \varphi(b)$$

   (γιατί; Μα ισχύει η Πρόταση Γ.2.2 και η Πρόταση Γ.2.3).

Στην πορεία θα δούμε και άλλα παραδείγματα ομομορφισμών ομάδων.

Σχόλιο Γ.3.5. Εδώ επισημαίνουμε ότι, όπως είναι φανερό και από τα Παραδείγματα 4 και 5 ανωτέρω, απεικονίσεις *φαινομενικά ίδιες*, στην πραγματικότητα είναι εντελώς διαφορετικές, ως προς την *συμπεριφορά τους*, όταν το πεδίο ορισμού και το πεδίο τιμών δεν είναι απλώς σύνολα, αλλά αλγεβρικές δομές.

Πριν προχωρήσουμε, παραθέτουμε μια σχετική ορολογία:

Έστω $f : G_1 \longrightarrow G_2$ ένας ομομορφισμός ομάδων. Αν η f, ως απεικόνιση είναι 1-1, θα ονομάζεται **μονομορφισμός**, αν είναι επί, θα ονομάζεται **επιμορφισμός**, αν είναι 1-1 και επί, θα ονομάζεται **ισομορφισμός**.

Στην περίπτωση όπου $G_1 = G_2$ (το πεδίο ορισμού συμπίπτει με το πεδίο τιμών), η f θα ονομάζεται **ενδομορφισμός**.

Ένας ενδομορφισμός ομάδων, ο οποίος είναι 1-1 και επί, θα ονομάζεται **αυτομορφισμός**.

Πρόταση Γ.3.6. *Έστω $f : G_1 \longrightarrow G_2$ ένας ομομορφισμός ομάδων, $H \leq G_1$ και $K \leq G_2$.*

Τότε ισχύουν τα εξής:

i. Το σύνολο $f(H) = \{ f(h) \mid h \in H \}$ είναι υποομάδα της G_2.

ii. Το σύνολο $f^{-1}(K) = \{ h \in G_1 \mid f(h) \in K \}$ είναι υποομάδα της G_1.

iii. Αν η υποομάδα H είναι κυκλική, τότε η $f(H)$ είναι κυκλική.

iv. Αν η υποομάδα H είναι αβελιανή, τότε η $f(H)$ είναι αβελιανή.

Πριν προχωρήσουμε, στην απόδειξη, παραπέμπουμε στην Παράγραφο 4.5.4 και ειδικότερα στον ορισμό 4.5.20 και στο Θεώρημα 4.5.24 για μια υπενθύμιση του τι σημαίνει εικόνα απεικόνισης και αντίστροφη εικόνα απεικόνισης.

Απόδειξη.

i. Προφανώς το σύνολο $f(H)$ είναι μη κενό (γιατί;). Επομένως, για να αποδείξουμε ότι είναι υποομάδα πρέπει και αρκεί να δείξουμε ότι για δύο στοιχεία $a, b \in f(H)$, το στοιχείο $a^{-1}b \in f(H)$ (γιατί; Μα αφού ισχύει η Πρόταση 5.1.24).

Έστω $a, b \in f(H)$. Αυτό σημαίνει ότι υπάρχουν $h, r \in H$, έτσι ώστε $a = f(h)$ και $b = f(s)$. Επομένως, έχουμε ότι

$$a^{-1}b = (f(h))^{-1}f(b) = f(h^{-1})f(s) = f(h^{-1}s) \in f(H).$$

Γιατί ισχύουν οι ανωτέρω ισότητες; Εδώ πρέπει να επικαλεσθούμε την Πρόταση Γ.3.3 και το γεγονός ότι η απεικόνιση f είναι ομομορφισμός.

ii. Έστω $a, b \in f^{-1}(K)$. Αυτό σημαίνει (ιδέ τον Ορισμό 4.5.20) ότι $f(a), f(b) \in K$. Η K όμως είναι υποομάδα, συνεπώς $f(a)^{-1}f(b) \in K$, δηλαδή

$$f(a^{-1})f(b) = f(a^{-1}b) \in K,$$

άρα $a^{-1}b \in f^{-1}(K)$. Επομένως, πράγματι $f^{-1}(K) \leq G_2$.

iii. Υποθέτουμε ότι η υποομάδα H είναι κυκλική, άρα υπάρχει ένας γεννήτορας $a \in H$. Τότε για κάθε άλλο στοιχείο $h \in H$, υπάρχει ένας ακέραιος αριθμός k, ώστε $h = a^k$.

Έστω $r \in f(H)$, τότε υπάρχει $h \in H$ με $f(h) = r$, συνεπώς $h = a^k$. Επομένως

$$r = f(h) = f(a^k) = (f(a))^k \in \langle f(a) \rangle.$$

Άρα $f(H) \leq \langle f(a) \rangle$. Οπότε, η $f(H)$ είναι κυκλική, ως υποομάδα κυκλικής.

Μάλιστα δε, επειδή προφανώς ισχύει και $\langle f(a) \rangle \leq f(H)$ (γιατί;), έχουμε αποδείξει κάτι πιο ισχυρό:

Η εικόνα ενός γεννήτορα της H, μέσω ενός ομομορφισμού, είναι γεννήτορας της $f(H)$.

iv. Ο ισχυρισμός είναι προφανής και αφήνεται ως άσκηση. ό.έ.δ.

Παρατηρήσεις Γ.3.7.

1. Έχουμε δει (Παρατήρηση Γ.1.5) ότι η προσθετική ομάδα $\mathbb{Z}$ των ακεραίων αριθμών είναι άπειρη κυκλική. Επίσης, έχουμε δει (σελίδα 400) ότι η προσθετική ομάδα των ακεραίων $\mathbb{Z}_m$ είναι κυκλική.

   Στο παράδειγμα Γ.3.4$_4$ είχαμε δει ότι η απεικόνιση $\mathbb{Z} \longrightarrow \mathbb{Z}_m$ είναι ομομορφισμός ομάδων. Επομένως, από την προηγουμένη Πρόταση συμπεραίνουμε (με έναν άλλο, πιο γενικό τρόπο) πάλι ότι η προσθετική ομάδα $\mathbb{Z}_m$ είναι κυκλική.

2. Το αντίστροφο του *iii)* στην προηγουμένη πρόταση δεν ισχύει. Πράγματι, έστω $G = \mathbb{Z} \times \mathbb{Z}$ το καρτεσιανό γινόμενο της προσθετικής ομάδας των ακεραίων με τον εαυτό της (ιδέ Άσκηση 5.1.3$_{19}$). Η απεικόνιση προβολή $\pi_1 : G \longrightarrow \mathbb{Z}$ με

$$\pi_1(a, b) = a,$$

   προφανώς(;) είναι ένας επιμορφισμός ομάδων. Η εικόνα $\pi_1(G) = \mathbb{Z}$ είναι κυκλική ομάδα, ενώ η ομάδα G δεν είναι κυκλική (γιατί;)

Γενικά, όταν έχουμε μια απεικόνιση $\vartheta : A \longrightarrow B$ μια απεικόνιση μεταξύ δύο συνόλων, εγείρεται το ερώτημα κατά πόσο η απεικόνιση αυτή είναι 1-1.

Στην ειδική περίπτωση των ομομορφισμών ομάδων θα δούμε τι επιπλέον μπορούμε να πούμε.

Ορισμός Γ.3.8. Έστω $f : G \longrightarrow M$ ένας ομομορφισμός ομάδων. Το σύνολο

$$Ker\, f = \{ a \in G \mid f(a) = 1_M \}$$

θα ονομάζεται **πυρήνας** του ομομορφισμού f.

Είναι εύκολο να δούμε ότι ο πυρήνας ενός ομομορφισμού ομάδων είναι υποομάδα του πεδίου ορισμού (ελέγξετε το!).

Πρόταση Γ.3.9. *Έστω $f : G \longrightarrow M$ ένας ομομορφισμός ομάδων. Η f είναι μονομορφισμός, αν και μόνο αν ο πυρήνας της f είναι η τετριμμένη υποομάδα της G.*

Απόδειξη. Η f είναι ομομορφισμός ομάδων, επομένως ισχύει ότι $f(1_G) = 1_M$. Υποθέτουμε ότι η f είναι μονομορφισμός. Επομένως, πράγματι $Ker\, f = \{1_G\}$.

Αντίστροφα, υποθέτουμε ότι $Ker\, f = \{1_G\}$. Έστω $a, b \in G$ με $f(a) = f(b)$. Επειδή η απεικόνιση f είναι ομομορφισμός ομάδων, έπεται ότι $f(a^{-1}b) = 1_M$. Δηλαδή, το στοιχείο

$$a^{-1}b \in Ker\, f = \{1_G\},$$

συνεπώς $a = b$. Άρα η f είναι 1-1. ό.έ.δ.

Ισχύει μια πιο γενική πρόταση, από την οποία απορρέει ως πόρισμα η προηγουμένη πρόταση.

Πρόταση Γ.3.10. *Έστω* $f : G \longrightarrow M$ *ένας ομομορφισμός ομάδων. Για* $a, b \in G$ *ισχύει ότι*

$$f(a) = f(b), \text{ αν και μόνο αν } aKer\, f = bKer\, f.$$

Απόδειξη. Στην ομάδα G ορίζεται μια σχέση ισοδυναμίας ως εξής:

$$a \sim b, \text{ αν } f(a) = f(b).$$

Έχουμε ήδη δει ότι η σχέση αυτή είναι σχέση ισοδυναμίας (ιδέ Πρόταση 4.5.28). Η κλάση ισοδυναμίας ενός στοιχείου $a \in G$ είναι η εξής:

$$\begin{aligned} C_a &= \{ b \in G \mid a \sim b \} \\ &= \{ b \in G \mid f(a) = f(b) \} \\ &= \{ b \in G \mid (f(b))^{-1} f(a) = 1_G \} \\ &= \{ b \in G \mid f(b^{-1}a) = 1_G \} \\ &= \{ b \in G \mid b^{-1}a \in Ker\, f \} = aKer\, f. \end{aligned}$$

Γιατί ισχύει η τελευταία ισότητα; Μα προφανώς διότι ισχύει η Πρόταση 5.1.30.

Οπότε, απεδείχθη ο ισχυρισμός. ό.έ.δ.

Παραδείγματα Γ.3.11.

1. Ας εξετάσουμε τους ομομορφισμούς, τους οποίους έχουμε δει στα Παραδείγματα $\Gamma.3.4_{3,4,6}$.

   Στο τρίτο παράδειγμα είχαμε τον ομομορφισμό $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ με $f(x) = \mid x \mid$. Προφανώς η f δεν είναι μονομορφισμός και

   $$Ker\, f = \{1, -1\}.$$

   Στο τέταρτο παράδειγμα είχαμε τον ομομορφισμό $\varphi : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ με $\varphi(x) = x^2$. Προφανώς η φ δεν είναι μονομορφισμός και

   $$Ker\, \varphi = \{1, -1\}.$$

   Στο έκτο παράδειγμα είχαμε τον ομομορφισμό $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ με $\varphi(a) = [a]$. Προφανώς η φ δεν είναι μονομορφισμός και

   $$Ker\, \varphi = m\mathbb{Z} = \{ mr \mid r \in \mathbb{Z} \} \text{ (γιατί;)}$$

2. Έστω $G = \mathbb{Z} \times \mathbb{Z}$ το καρτεσιανό γινόμενο της προθετικής ομάδας των ακεραίων με τον εαυτό της. Η απεικόνιση προβολή $\pi : G \longrightarrow \mathbb{Z}$ με $\pi(a, b) = a$ δεν είναι μονομορφισμός και προφανώς(;)

   $$Ker\, \pi = \{ (0, r) \in G \mid r \in \mathbb{Z} \} \text{ (γιατί;)}$$

3. Η απεικόνιση $\vartheta : \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ με $\vartheta(a) = (a, 0)$ προφανώς είναι ομομορφισμός και 1-1.

   Προσοχή! Στα δύο τελευταία παραδείγματα, αν και η σύνθεση $\pi \circ \vartheta : \mathbb{Z} \longrightarrow \mathbb{Z}$ είναι η ταυτοτική απεικόνιση, η μία απεικόνιση δεν είναι αντίστροφη της άλλης (γιατί; Ιδέ την Παράγραφο 4.5.6.1).

4. Έστω $\mathbb{Z}$ η προσθετική ομάδα των ακεραίων αριθμών και

$$G = \langle a \rangle = \{\dots, a^{-2}, a^{-1}, a^0 = 1, a^1 = a, a^2 \dots\}$$

μια άπειρη κυκλική ομάδα.

Ορίζουμε την απεικόνιση $\varphi : \mathbb{Z} \longrightarrow G$ ως εξής:

$\varphi(m) = a^m$. Είναι εύκολο να δούμε ότι η απεικόνιση αυτή είναι ένας ισομορφισμός ομάδων, δηλαδή ομομορφισμός, 1-1 και επί. Να κάνετε τον έλεγχο!

5. Έστω $\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$ η προσθετική ομάδα των ακεραίων αριθμών $mod\, n$ και

$$C_n = \langle a \mid a^n = 1 \rangle = \{a^0 = 1, a, a^2 \cdots a^{n-1}\}$$

μια πεπερασμένη κυκλική ομάδα τάξης n.

Ορίζουμε την απεικόνιση $\varphi : \mathbb{Z}_n \longrightarrow C_n$ ως εξής:

$$\varphi([k]) = a^k.$$

Είναι εύκολο να δούμε ότι η απεικόνιση αυτή είναι ένας ισομορφισμός ομάδων, δηλαδή ομομορφισμός, 1-1 και επί. Να κάνετε τον έλεγχο!

Παρατηρήσεις Γ.3.12.

1. Παρατηρήστε ότι στο πρώτο και δεύτερο παράδειγμα, αν και έχουμε διαφορετικούς ομομορφισμούς, οι ομομορφισμοί αυτοί έχουν ίσους πυρήνες.

2. Από τα δύο τελευταία παραδείγματα παρατηρούμε ότι στην πραγματικότητα έχουμε μόνο μια άπειρη κυκλική ομάδα, την προσθετική ομάδα των ακεραίων και για κάθε θετικό ακέραιο n μόνο μια κυκλική ομάδα τάξης n, την προσθετική ομάδα των ακεραίων $mod\, n$ (Παράβαλλε με το Θεώρημα Γ.1.3 και τις Παρατηρήσεις Γ.1.5).

   Γενικά η έννοια του ισομορφισμού διέπει όλα τα Μαθηματικά και μας επιτρέπει να "ταυτίζουμε" Μαθηματικά αντικείμενα και να θεωρούμε ότι πρόκειται για το ίδιο αντικείμενο.

   Εδώ ενδείκνυται να ανατρέξουμε στις ομάδες συμμετριών και να δούμε πώς προσδιορίσαμε την διεδρική ομάδα D_4 των συμμετριών ενός τετραγώνου. Αφ' ενός περιγράφοντας τα στοιχεία της ως "κατάλληλες" μεταθέσεις των τεσσάρων γωνιών του, αφ' ετέρου περιγράφοντας τα στοιχεία της γεωμετρικά ως στροφές και ανακλάσεις στο επίπεδο (ιδέ σελίδα 384 και την Άσκηση Γ.1.3$_{13}$.

3. Έστω $f\,; G \longrightarrow M$ ένας ομομορφισμός ομάδων και $K \leq G$, τότε, ως γνωστόν (ιδέ Θεώρημα 4.5.24), ισχύει ότι $K \leq f^{-1}(f(K))$. Επειδή η f είναι ομομορφισμός ομάδων, μπορούμε να αποδείξουμε ότι

$$f^{-1}(f(K)) = K \cdot Ker\, f$$

(ιδέ Άσκηση Γ.3.2$_5$).

Η σύνθεση ομομορφισμών.

Έστω δύο ομομορφισμοί ομάδων, των οποίων ορίζεται η σύνθεση, ως απεικονίσεις. Ένα φυσιολογικό ερώτημα, το οποίο προκύπτει, είναι κατά πόσον η σύνθεση αυτή είναι ομομορφισμός ομάδων.

Πρόταση Γ.3.13. *Έστω $f : G_1 \longrightarrow G_2$ και $g : G_2 \longrightarrow G_3$ δύο ομομορφισμοί ομάδων, όπου το πεδίο τιμών του πρώτου ομομορφισμού είναι ίσο με το πεδίο ορισμού του δεύτερου ομομορφισμού. Τότε η σύνθεση $g \circ f : G_1 \longrightarrow G_3$ είναι ομομορφισμός ομάδων.*

Απόδειξη. Έστω $a, b \in G_1$, επειδή η f είναι ομομορφισμός έχουμε ότι:

$$f(ab) = f(a)f(b) \in G_2.$$

Η g είναι ομομορφισμός, επομένως

$$g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a)(g \circ f)(b).$$

Από την πρώτη ισότητα έχουμε ότι

$$(g \circ f)(ab) = g(f(ab) = g(f(a)f(b)),$$

οπότε έχουμε

$$(g \circ f)(ab) = (g \circ f)(a)(g \circ f)(b). \qquad \text{ό.έ.δ.}$$

Προφανώς (γιατί;) ισχύει ότι $Ker\, f \leq Ker(g \circ f)$ και $(g \circ f)(G_1) \leq g(G_2)$.

Εδώ πρέπει να παρατηρήσουμε ότι ισχύουν όλες οι ιδιότητες, που αφορούν την σύνθεση απεικονίσεων. Ιδέ την Παράγραφο 4.5.6.

Έστω $f : G \longrightarrow M$ ένας ισομορφισμός ομάδων. Ως απεικόνιση 1-1 και επί, υπάρχει η αντίστροφή της $f^{-1} : M \longrightarrow G$. Είναι εύκολο να δούμε ότι η f^{-1} είναι ομομορφισμός ομάδων. Πράγματι, έστω $r, s \in M$, τότε, επειδή η f είναι επί, υπάρχουν $a, b \in G$, ώστε $r = f(a)$ και $s = f(b)$. Συνεπώς,

$$f^{-1}(rs) = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab.$$

Αλλά $a = f^{-1}(r)$ και $b = f^{-1}(s)$. Οπότε, αντικαθιστώντας στην προηγουμένη ισότητα, έχουμε $f^{-1}(rs) = f^{-1}(r)f^{-1}(s)$. Άρα η f^{-1} είναι ομομορφισμός ομάδων.

Έστω G μια ομάδα. Το σύνολο $(End(G), \circ)$ όλων των ενδομορφισμών της G, εφοδιασμένο με την πράξη της σύνθεσης απεικονίσεων, είναι ένα μονοειδές. Πράγματι, είναι προφανές ότι πληρούνται οι συνθήκες του Ορισμού 5.1.10.

Έστω G μια ομάδα, Το σύνολο $(Aut(G), \circ)$ όλων των αυτομορφισμών της G, εφοδιασμένο με την πράξη της σύνθεσης απεικονίσεων, είναι μια ομάδα. Πράγματι, είναι προφανές ότι πληρούνται οι συνθήκες του Ορισμού 5.1.16.

Γ.3.2 Ασκήσεις

1. Έστω $f : G \longrightarrow M$ ένας ομομορφισμός ομάδων. Δείξτε ότι ο πυρήνας $Ker\, f$ είναι υποομάδα της ομάδας G.

2. Έστω $f : \mathbb{Z}_{12} \longrightarrow \mathbb{Z}_{12}$ με $f([a]) = 3[a]$. Δείξτε ότι η f είναι ένας ομομορφισμός της προσθετικής ομάδας των ακεραίων $mod\, 12$. Να υπολογίσετε τον πυρήνα $Ker\, f$.

3. Έστω $exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \cdot)$ η "γνωστή" εκθετική συνάρτηση $exp(x) = e^x$ με πεδίο ορισμού την προσθετική ομάδα των πραγματικών αριθμών και πεδίο τιμών την πολλαπλασιαστική ομάδα των θετικών πραγματικών αριθμών. Δείξτε ότι η exp είναι ισομορφισμός ομάδων.

4. Δείξτε ότι δεν υπάρχει, μη τετριμμένος, ομομορφισμός $g : (\mathbb{Q}, +) \longrightarrow (\mathbb{Q}^+, \cdot)$ με πεδίο ορισμού την προσθετική ομάδα των ρητών αριθμών και πεδίο τιμών την πολλαπλασιαστική ομάδα των θετικών ρητών αριθμών.

   Υπόδειξη: Αν υπήρχε ένας τέτοιος ομομορφισμός ομάδων με $g(x) = a$, ποία θα ήταν η εικόνα $g(x/2)$;

5. Αποδείξτε τον ισχυρισμό που αναφέρεται στην Παρατήρηση Γ.3.12$_3$.

6. i. Δείξτε ότι η απεικόνιση $\varphi : \mathbb{C}^* \longrightarrow \mathbb{C}^*$, όπου $\mathbb{C}^*$ είναι η πολλαπλασιαστική ομάδα των μιγαδικών αριθμών με $\varphi(z) = z^4$ είναι ομομορφισμός ομάδων. Να υπολογίσετε τον πυρήνα του φ.

   ii. Έστω $H = \langle \cos 30^o + i \sin 30^o \rangle$ η κυκλική υποομάδα η παραγομένη από τον μιγαδικό αριθμό $z = \cos 30^o + i \sin 30^o$. Να υπολογίσετε την τάξη της και την εικόνα $\varphi(H)$ μέσω του ομομορφισμού του πρώτου ερωτήματος.

   Υπόδειξη: Εφαρμόστε τον γνωστό τύπο του De moivre.

7. Έστω $C_4 = \langle a \rangle$ και $C_5 = \langle b \rangle$ δύο κυκλικές ομάδες με τάξεις ίσες με 4 και 5 αντίστοιχα.

   Να βρεθούν όλοι οι ομομορφισμοί $\varphi : C_4 \longrightarrow C_5$ και $\vartheta : C_5 \longrightarrow C_4$.

8. Έστω $(G, \cdot)$ μια ομάδα. Επιλέγουμε και σταθεροποιούμε ένα στοιχείο $t \in G$. Στο σύνολο G ορίζουμε μια νέα πράξη $*$ ως εξής: $a * b = a \cdot t \cdot b$, για όλα τα $a, b \in$. Ως γνωστόν (;) (παράβαλλε με το Παράδειγμα 5.1.17$_3$) το σύνολο $(G, *)$ αποτελεί ομάδα.

   Δείξτε ότι οι ομάδες $(G, \cdot)$ και $(G, *)$ είναι ισόμορφες.

9. Έστω $(G, \circ)$ μια ομάδα και M ένα (τυχαίο) σύνολο. Έστω $f : G \longrightarrow M$ μια απεικόνιση, η οποία είναι 1-1 και επί. Στο σύνολο M ορίζουμε μια πράξη ως εξής: Για $a, b \in M$ ορίζουμε $a * b = f(x \circ y)$, όπου x, y είναι τα μοναδικά στοιχεία της ομάδας $(G, \circ)$ με την ιδιότητα $f(x) = a$, $f(y) = b$.

   Δείξτε ότι το σύνολο $(M, *)$ είναι ομάδα και ότι η απεικόνιση f είναι ισομορφισμός ομάδων.

10. Έστω $(G, +)$ μια αβελιανή ομάδα και $(End(G), \circ)$ η ημιομάδα των ενδομορφισμών της G. Στο σύνολο $End(G)$ ορίζουμε και μια άλλη πράξη ως εξής: Για $\varphi, \vartheta \in End(G)$ ορίζουμε $\varphi + \vartheta : G \longrightarrow G$ με

$$(\varphi + \vartheta)(x) = \varphi(x) + \vartheta(x)$$

   για $x \in G$. Δείξτε ότι η απεικόνιση $\varphi + \vartheta$ είναι ενδομορφισμός της G.

   Δείξτε ότι το σύνολο $(End(G), +, \circ)$ είναι δακτύλιος. Είναι ο δακτύλιος αυτός μεταθετικός;

Γ.3.3 Ομομορφισμοί δακτυλίων

Όπως στις ομάδες, μπορούμε να ορίσουμε την έννοια του ομομορφισμού δακτυλίων. Μόνο που εδώ, δεδομένου ότι ένας δακτύλιος είναι εφοδιασμένος με δύο πράξεις, πρέπει ένας ομομορφισμός να "διατηρεί" και τις δύο πράξεις.

Ορισμός Γ.3.14. Έστω $(R, +, \cdot)$ και $(S, \oplus, \odot)$ δύο δακτύλιοι. Μια απεικόνιση

$$\vartheta : R \longrightarrow S$$

θα ονομάζεται **ομομορφισμός** δακτυλίων, αν

$$\vartheta(x+y) = \vartheta(x) \oplus \vartheta(y) \text{ και } \vartheta(x \odot y) = \vartheta(x) \odot \vartheta(y), \text{ για όλα τα } x, y \in R.$$

Προφανώς, εκ του ορισμού, έπεται ότι ένας ομομορφισμός δακτυλίων, αν *αποσιωπήσουμε* την πράξη του πολλαπλασιασμού, είναι ένας ομομορφισμός των προσθετικών ομάδων των δύο δακτυλίων. Επομένως, πληροί όλες τις ιδιότητες των ομομορφισμών ομάδων, που έχουμε δει στην προηγουμένη παράγραφο.

Για παράδειγμα, έχουμε την έννοια του πυρήνα και ότι το μηδέν (το ουδέτερο ως προς την πρόσθεση) του πεδίου τιμών έχει εικόνα, μέσω ενός ομομορφισμού δακτυλίων, το μηδέν του πεδίου τιμών.

Όπως και στους ομομορφισμούς ομάδων, και εδώ έχουμε την έννοια του **μονομορφισμού**, του **επιμορφισμού** και του **ισομορφισμού δακτυλίων**.

Παραδείγματα Γ.3.15.

1. Η απεικόνιση $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ με $\varphi(r) = [r]$ είναι ένας ομομορφισμός δακτυλίων.

   Στο Παράδειγμα Γ.3.4$_6$ είχαμε δει ότι η απεικόνιση φ είναι ομομορφισμός μεταξύ των προσθετικών ομάδων των δύο δακτυλίων. Προφανώς η φ "διατηρεί" και τον πολλαπλασιασμό, δεδομένου ότι ισχύει

   $$\varphi(ab) = [ab] = [a][b] = \varphi(a)\varphi(b).$$

2. Είναι εύκολο να δούμε ότι η απεικόνιση $f : \mathbb{C} \longrightarrow \mathbb{C}$ με $f(a+bi) = a - bi$ είναι ομομορφισμός στον δακτύλιο των μιγαδικών αριθμών (γιατί;) Δεν ξεχνάμε τις γνωστές ιδιότητες των μιγαδικών αριθμών (Πρόταση 7.3.4).

3. Ας εξετάσουμε αν η απεικόνιση $\vartheta : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_{10}$ με $\vartheta(x) = 5x$ είναι ομομορφισμός δακτυλίων.

   Πριν προχωρήσουμε, πρέπει να επισημάνουμε ότι το στοιχείο x, ως στοιχείο στο πεδίο ορισμού, είναι η κλάση $x \bmod 4$, ενώ ως στοιχείο του πεδίου τιμών, είναι η κλάση $x \bmod 10$. Αυτό δεν πρέπει να μας δημιουργεί σύγχυση, αλλά πρέπει να είμαστε πολύ προσεκτικοί.

   Επομένως, για τον έλεγχο της ισότητας

   $$\vartheta(x+y) = 5(x+y) = 5x + 5y = \vartheta(x) + \vartheta(y),$$

   στο ένα μέλος έχουμε την πρόσθεση $\bmod 4$ και στο άλλο την πρόσθεση $\bmod 10$.

   Όμοια για τον έλεγχο της ισότητας

   $$\vartheta(xy) = 5(xy) = (5x)(5y) = \vartheta(x)\vartheta(y).$$

   Προσπαθήστε να κάνετε, με κάθε λεπτομέρεια, τον έλεγχο.

4. Η απεικόνιση $\varphi : \mathbb{R} \longrightarrow \mathbb{R}$ στον δακτύλιο των πραγματικών αριθμών με

$$\varphi(x) = x^2$$

δεν είναι ομομορφισμός δακτυλίων.

(γιατί; παράβαλλε με τα Παραδείγματα Γ.3.4$_{4,5}$).

5. Η απεικόνιση $\vartheta : \mathbb{Z} \longrightarrow 2\mathbb{Z}$ με $\varphi(x) = 2x$ προφανώς είναι ισομορφισμός μεταξύ των προσθετικών ομάδων των δύο δακτυλίων, αλλά δεν είναι ισομορφισμός δακτυλίων (γιατί;).

6. Έστω R ένας δακτύλιος με μονάδα. Η απεικόνιση $f : \mathbb{Z} \longrightarrow R$ με $f(n) = n \cdot 1_r$, είναι ένας ομομορφισμός δακτυλίων.

Για να το διαπιστώσουμε αυτό, αρκεί να ανατρέξουμε στην Άσκηση 5.1.5$_4$.

Παρατήρηση Γ.3.16. Γενικά, ενδέχεται να έχουμε δύο δακτυλίους, οι οποίοι να έχουν ουδέτερο ως προς τον πολλαπλασιασμό, αλλά ένας ομομορφισμός από τον έναν στον άλλο δεν απεικονίζει, κατ' ανάγκη, το ουδέτερο ως προς τον πολλαπλασιασμό του πεδίου ορισμού στο ουδέτερο ως προς τον πολλαπλασιασμό του πεδίου τιμών. Ιδέ στο τρίτο από τα αμέσως προηγούμενα παραδείγματα.

Επίσης, όπως έχουμε επισημάνει, ενδέχεται να έχουμε έναν δακτύλιο, έστω R, και έναν υποδακτύλιο, έστω K, οι οποίοι να έχουν διαφορετικά ουδέτερα ως προς τον πολλαπλασιασμό, κάτι που δεν συμβαίνει στις ομάδες.

Ρίζες πολυωνύμων.

Όλοι έχουμε "συναντήσει" την έννοια της ρίζας πολυωνύμου. Εδώ θα κάνουμε μια ανασκόπηση επισημαίνοντας ορισμένα σημεία.

Έστω E ένας μεταθετικός δακτύλιος με μονάδα και R ένας υποδακτύλιος του E με την ιδιότητα: Το ουδέτερο του πολλαπλασιασμού του E να ανήκει στον υποδακτύλιο R (δηλαδή οι δύο δακτύλιοι έχουν την ίδια μονάδα).

Επιλέγουμε ένα στοιχείο $r \in E$ και ορίζουμε την εξής απεικόνιση:

$$\varphi_r : R[x] \longrightarrow E.$$

Για $\sigma(x) = a_0 + a_1x + \cdots + a_nx^n$ ορίζουμε

$$\varphi_r(\sigma(x)) = \sigma(r) = a_0 + a_1r + \cdots + a_nr^n.$$

Η εικόνα $\sigma(r)$ του πολυωνύμου $\sigma(x)$ μέσω της απεικόνισης φ_r θα ονομάζεται η **τιμή** του $\sigma(x)$ στην θέση r.

Η απεικόνιση φ_r είναι ομομορφισμός δακτυλίων.

Πράγματι, από τον ορισμό της πρόσθεσης και του πολλαπλασιασμού πολυωνύμων (Ορισμός Γ.2.12) και την Παρατήρηση Γ.2.11$_3$ εύκολα προκύπτει ότι η απεικόνιση φ_r είναι ομομορφισμός δακτυλίων.

Έστω $\tau(x) \in R[x]$, αν υπάρχει $r \in E$, ούτως ώστε $\varphi_r(\tau(x)) = \tau(r) = 0$, τότε το r θα ονομάζεται **ρίζα** του πολυωνύμου $\tau(x)$.

Πριν προχωρήσουμε, θα επισημάνουμε δύο ερωτήματα που προκύπτουν.

i. Έστω $\sigma(x) \in R[x]$. Υπάρχει (τουλάχιστον) μια ρίζα r στον υπερδακτύλιο E του πολυωνύμου $\sigma(x)$;

ii. Έστω $r \in E$, υπάρχει πολυώνυμο $\sigma(x) \in R[x]$, του οποίου ρίζα να είναι το r;

Τα δύο αυτά ερωτήματα είναι δυϊκά. Στο πρώτο έχουμε ένα πολυώνυμο και αναζητούμε ρίζες του. Στο δεύτερο έχουμε ένα στοιχείο και αναζητούμε πολυώνυμο, του οποίου ρίζα να είναι το δοθέν στοιχείο.

Επίσης, πρέπει να επισημάνουμε ότι τα ερωτήματα αυτά είναι άμεσα συνδεδεμένα με τους δακτύλιους R και E.

Ας δούμε τα εξής παραδείγματα:

Έστω $\sigma(x) = x^2 - 2 \in \mathbb{Z}[x]$ και $E = \mathbb{Q}$ ο δακτύλιος των ρητών αριθμών. Εύκολα διαπιστώνουμε ότι δεν υπάρχει ρητός αριθμός, ο οποίος να είναι ρίζα του $x^2 - 2$. Αν όμως, αντί του δακτυλίου των ρητών αριθμών, θεωρήσουμε τον δακτύλιο $\mathbb{R}$ των πραγματικών αριθμών, τότε προφανώς το πολυώνυμο $x^2 - 2$ έχει ρίζες τους πραγματικούς αριθμούς $\sqrt{2},\ -\sqrt{2}$.

Έστω ο πραγματικός αριθμός $\pi = 3.14....$ Είναι γνωστό[15] ότι δεν υπάρχει πολυώνυμο με ρητούς συντελεστές, ούτως ώστε ο π να είναι ρίζα του. Αλλά υπάρχει το πολυώνυμο $x - \pi \in \mathbb{R}[x]$, του οποίου ρίζα είναι το π.

Παρατήρηση Γ.3.17. Θα μπορούσαμε να επιχειρηματολογήσουμε ως εξής: Ο ομομορφισμός $\varphi_r : R[x] \longrightarrow E$ έχει πυρήνα

$$Ker\,\varphi_r = \{\sigma(x) \in R[x] \mid \sigma(r), = 0 \in E\}.$$

Επομένως, το πρώτο ερώτημα αναδιατυπώνεται ως εξής:

> Δοθέντος ενός $\sigma(x) \in R[x]$, υπάρχει $r \in E$, ούτως ώστε $\sigma(x) \in Ker\,\varphi_r$;

Το δεύτερο ερώτημα αναδιατυπώνεται ως εξής:

> Δοθέντος ενός στοιχείου $r \in E$, μπορούμε να υπολογίσουμε τον πυρήνα $Ker\,\varphi_r$;

Επ' αυτών δεν θα επεκταθούμε περισσότερο.

Θα δούμε πώς συνδέεται η ύπαρξη ριζών πολυωνύμων με τον αλγόριθμο της διαίρεσης πολυωνύμων (ιδέ την Παράγραφο Γ.2.2.1).

Θεώρημα Γ.3.18. *Έστω $\mathbb{F}$ ένα σώμα, $a \in \mathbb{F}$ και $f(x) \in \mathbb{F}[x]$. Το υπόλοιπο της διαίρεσης του $f(x)$ με το $x - a$ είναι ίσον με το $f(a) \in \mathbb{F}$.*

Απόδειξη. Ως γνωστόν, από το Θεώρημα Γ.2.16, υπάρχουν μοναδικά πολυώνυμα $\pi(x), \upsilon(x) \in \mathbb{F}[x]$, ώστε

$$f(x) = \pi(x)(x - a) + \upsilon(x)$$

με

$$\upsilon(x) = 0 \text{ ή } \upsilon(x) = r \in \mathbb{F}.$$

Η απεικόνιση φ_a είναι ομομορφισμός δακτυλίων, επομένως έχουμε ότι

$$\varphi_a(f(x)) = \varphi_a(\pi(x)(x - a) + \upsilon(x)) = \pi(a)(a - a) + \upsilon(a) = \upsilon(a).$$

Αλλά αφ' ενός έχουμε $\varphi_a(f(x)) = f(a)$, αφ' ετέρου το $\upsilon(x)$ είναι το μηδενικό ή σταθερό πολυώνυμο. Επομένως, σε κάθε περίπτωση, έχουμε ότι $\upsilon(x) = f(a)$. ό.έ.δ.

[15] Είναι δύσκολο, σ' αυτό το επίπεδο, να αποδείξουμε αυτόν τον ισχυρισμό. Εδώ απλώς τον επικαλούμαστε ως "πληροφορία".

Πόρισμα Γ.3.19. *Με τις προηγούμενες υποθέσεις. Το πολυώνυμο $x-a$ διαιρεί το (είναι παράγοντας του) $f(x)$, αν και μόνο αν το στοιχείο a είναι ρίζα του $f(x)$.*

Πόρισμα Γ.3.20. *Ένα πολυώνυμο βαθμού n με συντελεστές από ένα σώμα, έστω $\mathbb{F}$, έχει το πολύ n το πλήθος ρίζες, οι οποίες ανήκουν στο σώμα $\mathbb{F}$.*

Απόδειξη. Αν το πολυώνυμο είναι σταθερό (δηλαδή βαθμού μηδέν), προφανώς δεν έχει ρίζες.

Αν το πολυώνυμο είναι βαθμού ένα, τότε είναι της μορφής $ax+b \in \mathbb{F}[x]$ και προφανώς έχει μοναδική ρίζα, την $-(a^{-1}b) \in \mathbb{F}$.

Υποθέτουμε ότι όλα τα πολυώνυμα με συντελεστές από το σώμα $\mathbb{F}$ και βαθμό $k \leq n-1$ έχουν το πολύ k το πλήθος ρίζες, οι οποίες ανήκουν στο σώμα $\mathbb{F}$. Έστω $\sigma(x) \in \mathbb{F}[x]$ με βαθμό ίσον με n. Αν το $\sigma(x)$ δεν έχει ρίζα, η οποία να ανήκει στο σώμα $\mathbb{F}$, έχει καλώς. Υποθέτουμε ότι το $\sigma(x)$ έχει μια ρίζα, έστω ρ, στο $\mathbb{F}$. Από το προηγούμενο πόρισμα έχουμε ότι $\sigma(x) = (x-\rho)\tau(x)$ με το $\tau(x) \in \mathbb{F}[x]$. Ο βαθμός του $\tau(x)$ είναι ίσος με $n-1$. Από την υπόθεση της επαγωγής το $\tau(x)$ έχει το πολύ $n-1$ το πλήθος ρίζες, οι οποίες ανήκουν στο σώμα $\mathbb{F}$. Άρα το $\sigma(x) = (x-\rho)\tau(x)$ έχει το πολύ n το πλήθος ρίζες, οι οποίες ανήκουν στο $\mathbb{F}$. ό.έ.δ.

Παρατήρηση Γ.3.21. Πρέπει να τονισθεί ότι το προηγούμενο πόρισμα δεν ισχύει αν δεν υποθέσουμε ότι ο δακτύλιος των συντελεστών του δοθέντος πολυωνύμου είναι σώμα.

Για παράδειγμα: Το πολυώνυμο $x^2+3x+2 \in \mathbb{Z}_6[x]$ έχει τέσσερις ρίζες εντός του δακτυλίου $\mathbb{Z}_6$. Πού οφείλεται αυτό; Δεν ξεχνάμε ότι ο Ευκλείδιος Αλγόριθμος της διαίρεσης (Θεώρημα Γ.2.16) ισχύει για πολυώνυμα με συντελεστές από ένα σώμα.

Γ.3.4 Ασκήσεις

1. Έστω $\varphi : \mathbb{Z}_m \longrightarrow \mathbb{Z}_n$ ένας ομομορφισμός δακτυλίων. Δείξτε ότι, αν $\varphi(1) = a$, τότε $a^2 = a$.

2. Εξετάστε αν η απεικόνιση $\vartheta : \mathbb{Z}_5 \longrightarrow \mathbb{Z}_{30}$ με $\vartheta(x \bmod 5) = 6(x \bmod 30)$ είναι ομομορφισμός δακτυλίων.

3. i. Να προσδιορίσετε όλους τους ενδομορφισμούς του δακτυλίου $\mathbb{Z}$.
   ii. Να προσδιορίσετε όλους τους ενδομορφισμούς του δακτυλίου $\mathbb{Z}_6$.
   iii. Να προσδιορίσετε όλους τους ενδομορφισμούς του δακτυλίου $\mathbb{Z}_m$.
   iv. Να προσδιορίσετε όλους τους ομομορφισμούς από τον δακτύλιο $\mathbb{Z}_6$ στον δακτύλιο $\mathbb{Z}_{10}$.
   v. Να προσδιορίσετε όλους τους ενδομορφισμούς του σώματος των ρητών αριθμών $\mathbb{Q}$.
   vi. Να προσδιορίσετε όλους τους ενδομορφισμούς του σώματος των πραγματικών αριθμών $\mathbb{R}$.

4. Έστω $\mathbb{F}$ ένα σώμα και $\vartheta : \mathbb{F} \longrightarrow R$ ένας ομομορφισμός δακτυλίων. Δείξτε ότι ο ϑ είτε είναι ο μηδενικός ομομορφισμός είτε είναι μονομορφισμός.

5. Θεωρώντας την δεκαδική παράσταση

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$$

ενός θετικού ακεραίου αριθμού, να υπολογίσετε τον πυρήνα του (φυσικού) επιμορφισμού $\mathbb{Z} \longrightarrow \mathbb{Z}_9$ (ιδέ Παράδειγμα Γ.3.15$_1$).

Μπορείτε να δώσετε ένα κριτήριο διαιρετότητας ενός ακεραίου αριθμού με το 9;

6. Μπορείτε να βρείτε το υπόλοιπο της διαίρεσης των αριθμών

$$(2 \cdot 10^{75} + 2)^{100} \text{ και } (10^{100} + 1)^{99}$$

με το τρία, χωρίς να χρησιμοποιήσετε "μολύβι και χαρτί";

7. Έστω R ένας μεταθετικός δακτύλιος με μονάδα.

   i. Δείξτε ότι η απεικόνιση $h : R[x] \longrightarrow R$ με

   $$h(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_0$$

   είναι επιμορφισμός δακτυλίων.

   Να προσδιορίσετε τον πυρήνα της.

   ii. Δείξτε ότι η απεικόνιση $g : R[x] \longrightarrow R$ με

   $$g(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_0 + a_1 + \cdots + a_n$$

   είναι επιμορφισμός δακτυλίων.

   Να προσδιορίσετε τον πυρήνα της.

8. Έστω R_1, R_2 δύο μεταθετικοί δακτύλιοι με μονάδα και $\varphi : R_1 \longrightarrow R_2$ ένας ομομορφισμός δακτυλίων.

   Ορίζουμε την απεικόνιση $\bar{\varphi} : R_1[x] \longrightarrow R_2[x]$ ως εξής: Αν

   $$\sigma(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in R_1[x],$$

   τότε

   $$\bar{\varphi}(\sigma(x)) = \varphi(a_0) + \varphi(a_1)x + \varphi(a_2)x^2 + \cdots + \varphi(a_n)x^n.$$

   Δείξτε ότι η απεικόνιση $\bar{\varphi}$ είναι ομομορφισμός δακτυλίων.

   Μπορείτε να περιγράψετε τον πυρήνα της;

   Δείξτε ότι: Η $\bar{\varphi}$ είναι μονομορφισμός, αν και μόνο αν η φ είναι μονομορφισμός.

   Η $\bar{\varphi}$ είναι επιμορφισμός, αν και μόνο αν η φ είναι επιμορφισμός.

9. Έστω $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ ο γνωστός επιμορφισμός δακτυλίων και

   $$\bar{\varphi} : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_m[x]$$

   ο επαγόμενος ομομορφισμός (σύμφωνα με την προηγουμένη άσκηση).

   Δείξτε ότι $\bar{\varphi}(\sigma(x)) = 0$, αν και μόνο αν κάθε συντελεστής του $\sigma(x)$ είναι πολλαπλάσιο του m.

   Στην περίπτωση, όπου ο m είναι πρώτος, δείξτε ότι

   $$\sigma(x)\tau(x) \in Ker\,\bar{\varphi}, \text{ αν } \sigma(x) \in Ker\,\bar{\varphi} \text{ ή } \tau(x) \in Ker\,\bar{\varphi}.$$

10. Έστω $f(x) \in \mathbb{R}[x]$ ένα πολυώνυμο με πραγματικούς συντελεστές. Υποθέτουμε ότι $z = a + bi$ είναι μια μιγαδική ρίζα του $f(x)$, δείξτε ότι και ο συζυγής μιγαδικός αριθμός $\bar{z} = a - bi$ είναι ρίζα του $f(x)$.

11. Δείξτε ότι το 1 είναι η μόνη ρίζα του $x^{25} - 1 \in \mathbb{Z}_{37}[x]$, η οποία ανήκει στο $\mathbb{Z}_{37}$.

12. Έστω $f(x) \in \mathbb{Z}[x]$ και $a \equiv b \mod m$. Δείξτε ότι $f(a) \equiv f(b) \mod m$.

    Υποθέτουμε ότι οι τιμές $f(0)$ και $f(1)$ είναι και οι δύο περιττοί αριθμοί. Δείξτε ότι το πολυώνυμο $f(x)$ δεν έχει ακέραιες ρίζες.

13. Έστω $\sigma(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x]$. Δείξτε ότι, αν το ανάγωγο κλάσμα r/s είναι ρίζα του $\sigma(x)$, τότε το r διαιρεί το a_0 και το s διαιρεί το a_n.

14. Έστω $\alpha(x), \beta(x), \gamma(x) \in \mathbb{Z}[x]$. Υποθέτουμε ότι $\alpha(x) = \beta(x) \cdot \gamma(x)$ και ότι υπάρχει ένας πρώτος p, ο οποίος διαιρεί κάθε συντελεστή του πολυωνύμου $\alpha(x)$. Δείξτε ότι ο p διαιρεί κάθε συντελεστή του $\beta(x)$ ή του $\gamma(x)$.

15. Έστω $\alpha(x) \in \mathbb{Z}[x]$. Υποθέτουμε ότι $\alpha(x) = \beta(x) \cdot \gamma(x)$, όπου $\beta(x), \gamma(x) \in \mathbb{Q}[x]$. Δείξτε ότι υπάρχουν $\mathrm{B}(x), \Gamma(x) \in \mathbb{Z}[x]$, τα οποία είναι ακέραια πολλαπλάσια των $\beta(x)$ και $\gamma(x)$ αντίστοιχα, ώστε $\alpha(x) = \mathrm{B}(x) \cdot \Gamma(x)$.

Βιβλιογραφία

[1] Joseph A. Gallian. *Contemporary Abstract Algebra*. Seventh Edition. Brooks/Cole, 2009. ISBN: 978-05-4716-509-7.

[2] Thomas W. Judson. *Abstract Algebra Theory and Applications*. Version 1.2, November. Copyright 2000,2001,2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA, 2002.

[3] Charles C. Pinter. *A Book of Abstract Algebra*. Second Edition. Dover Dover Publications, Inc., Mineola, New York Originally published: 2nd ed. New York: McGraw-Hill, 1990. ISBN: 978-04-8647-417-5.

[4] Στυλιανός Ανδρεαδάκης. *Εισαγωγή στην Άλγεβρα*. Εκδόσεις Συμμετρία, 1993.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Η παρατιθέμενη Βιβλιογραφία δεν είναι πλήρης. Απλώς είναι ενδεικτική και αποσκοπεί ώστε ο ενδιαφερόμενος αναγνώστης να *απεγκλωβιστεί* από την προσήλωση σε ένα μόνο βιβλίο.

Βιβλιογραφία

[1] Στυλιανός Ανδρεαδάκης. *Εισαγωγή στην Άλγεβρα*. Εκδόσεις Συμμετρία, 1993.

[2] Γιάννης Ν. Μοσχοβάκης. *Σημειώσεις στη Συνολοθεωρία*. Προκαταρκτική 2η έκδοση. http://www.math.ucla.edu/~ynm/lectures/g.pdf, 2014.

[3] Αντώνης Τσολομύτης. *Σύνολα και αριθμοί*. Leader Books, 2004. ISBN: 978-96-0790-147-7.

[4] Thomas Bieske. *An Introduction to Writing Mathematical Proofs: Shifting Gears from Calculus to Upper-Level Mathematics Classe*. Independently published, 2020. ISBN: 979-85-6123-065-3.

[5] E.D. Bloch. *Proofs and Fundamentals: A first course in Abstract Mathematics*. Second Edition, Springer, 2011. ISBN: 978-14-4197-126-5.

[6] E.D. Bloch. *The Real Numbers and Real Analysis*. Springer, 2011. ISBN: 978-03-8772-176-7.

[7] J. Cummings. *Proofs: A Long-Form Mathematics Textbook*. Independently published, 2021. ISBN: 979-85-9526-597-3.

[8] Herbert B. Enderton. *Elements of Set Theory*. Academic Press, 1977. ISBN: 978-01-2238-440-0.

[9] Joseph A. Gallian. *Contemporary Abstract Algebra*. Seventh Edition. Brooks/Cole, 2009. ISBN: 978-05-4716-509-7.

[10] D. Goldrei. *Classic Set Theory: For Guided Independent Study*. Chapman Hall CRC Press, 1996. ISBN: 978-04-1260-610-6.

[11] P. Halmos. *Naive Set Theory*. Springer, 1974. ISBN: 978-0-387-90104-6.

[12] Joel David Hamkins. *Proof and the Art of Mathematics*. MIT Press, 2020. ISBN: 978-02-6253-979-1.

[13] Richard Hammack. *Book of Proof*. Edition 2.2. Virginia Commonwealth University Richard Hammack (publisher). Department of Mathematics and Applied Mathematics, 2013.

[14] K. Houston. *How to Think Like a Mathematician*. Cambridge University Press, 2009. ISBN: 978-05-2189-546-0.

[15] K. Hrbacek-T. Jech. *Introduction to Set Theory*. Third Edition. Marcel Dekker Inc., 1999. ISBN: 08-2477-915-0.

[16] T. Jech. *Set Theory*. Springer, 2003. ISBN: 978-3540440857.

[17] Thomas W. Judson. *Abstract Algebra Theory and Applications*. Version 1.2, November. Copyright 2000,2001,2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA, 2002.

[18] Steven G. Krantz. *The Elements of Advanced Mathematics*. Fourth Edition. Textbooks in mathematics. CRC Press Taylor and Francis Group, 2018. ISBN: 978-11-3850-631-2.

[19] M. Liebeck. *A Concise Introduction to Pure Mathematics*. Third Edition. Chapman Hall CRC Press, 2011. ISBN: 978-14-3983-598-2.

[20] Charles C. Pinter. *A Book of Abstract Algebra*. Second Edition. Dover Dover Publications, Inc., Mineola, New York Originally published: 2nd ed. New York: McGraw-Hill, 1990. ISBN: 978-04-8647-417-5.

[21] Bernd S. W. Schröder. *Fundamentals of Mathematics: An Introduction to Proofs, Logic, Sets and Numbers*. First Edition Wiley, 2010. ISBN: 978-04-7055-138-7.

[22] C. Schumacher. *Chapter Zero: Fundamental Notions of Abstract Mathematics*. Second Edition. Addison-Wesley, 2021. ISBN: 02-0143-724-4.

[23] A. Stefanowitz. *Proofs and Mathematical Reasoning*. University of Birmingham, 2014.

[24] I. Stewart & D. Tall. *The Foundations of Mathematics*. Second Edition. Oxford University Press, 2015.

[25] John Stillwell. *Elements of Mathematics: From Euclid to Gödel*. First Edition. Princeton University Press, 2016. ISBN: 978-06-9117-168-5.

[26] John Stillwell. *The Story of Proof: Logic and the History of Mathematics*. Princeton University Press, 2022. ISBN: 978-06-9123-436-6.

[27] John Stillwell. *Mathematics and Its History*. Third Edition. Springer, 2010. ISBN: 978-14-4196-052-8.

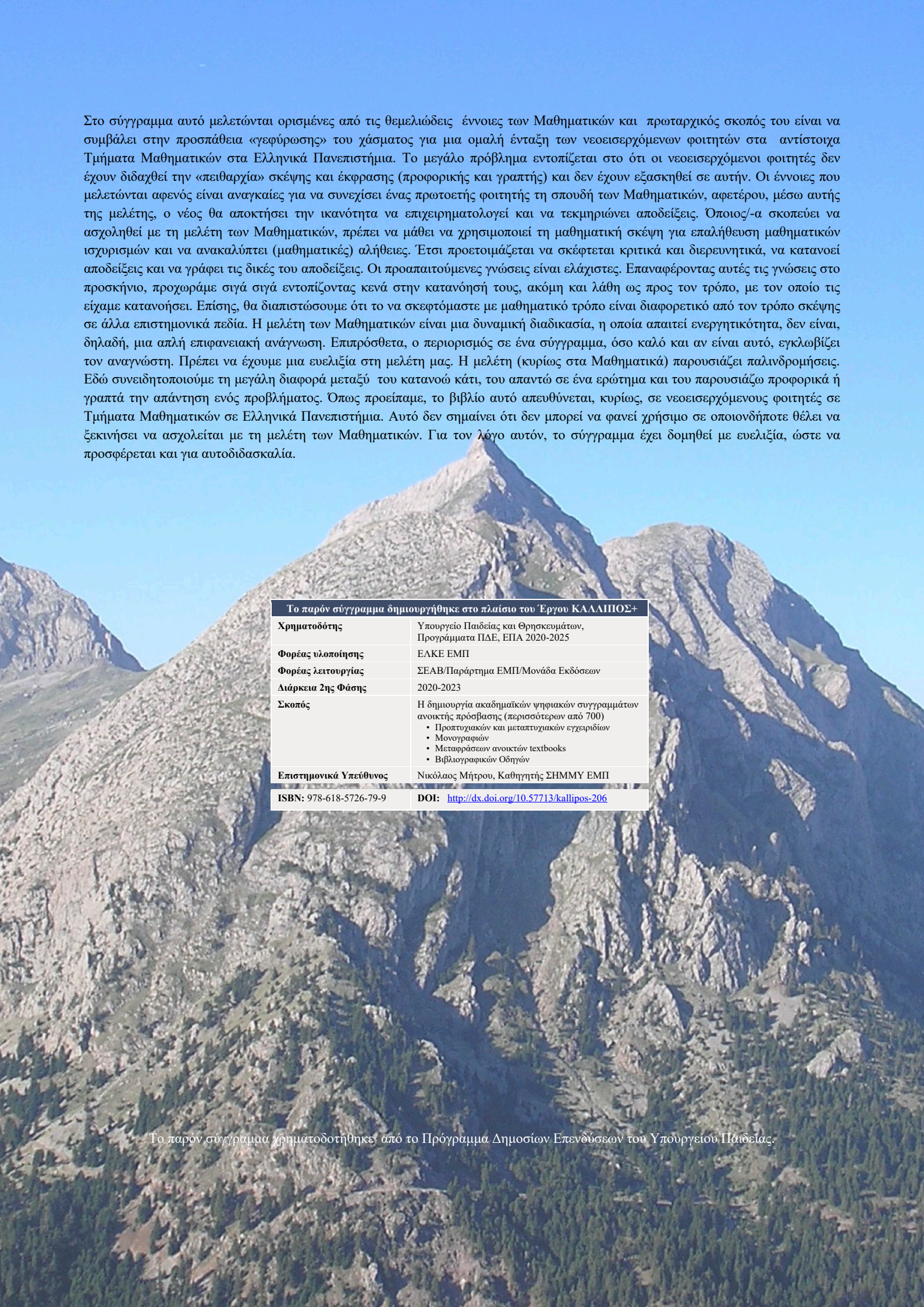
[28] John Stillwell. *The Real Numbers: An Introduction to Set Theory and Analysis*. First Edition. Springer, 2013. ISBN: 978-33-1934-726-4.

[29] T. Sundstrom. *Mathematical Reasoning, Writing and Proof*. Version 2.1 May 26. 2020.

[30] P. Suppes. *Introduction to Logic*. Dover Publications, 1999. ISBN: 978-04-8640-687-9.

ΕΥΡΕΤΗΡΙΟ

Στο σύγγραμμα αυτό μελετώνται ορισμένες από τις θεμελιώδεις έννοιες των Μαθηματικών και πρωταρχικός σκοπός του είναι να συμβάλει στην προσπάθεια «γεφύρωσης» του χάσματος για μια ομαλή ένταξη των νεοεισερχόμενων φοιτητών στα αντίστοιχα Τμήματα Μαθηματικών στα Ελληνικά Πανεπιστήμια. Το μεγάλο πρόβλημα εντοπίζεται στο ότι οι νεοεισερχόμενοι φοιτητές δεν έχουν διδαχθεί την «πειθαρχία» σκέψης και έκφρασης (προφορικής και γραπτής) και δεν έχουν εξασκηθεί σε αυτήν. Οι έννοιες που μελετώνται αφενός είναι αναγκαίες για να συνεχίσει ένας πρωτοετής φοιτητής τη σπουδή των Μαθηματικών, αφετέρου, μέσω αυτής της μελέτης, ο νέος θα αποκτήσει την ικανότητα να επιχειρηματολογεί και να τεκμηριώνει αποδείξεις. Όποιος/-α σκοπεύει να ασχοληθεί με τη μελέτη των Μαθηματικών, πρέπει να μάθει να χρησιμοποιεί τη μαθηματική σκέψη για επαλήθευση μαθηματικών ισχυρισμών και να ανακαλύπτει (μαθηματικές) αλήθειες. Έτσι προετοιμάζεται να σκέφτεται κριτικά και διερευνητικά, να κατανοεί αποδείξεις και να γράφει τις δικές του αποδείξεις. Οι προαπαιτούμενες γνώσεις είναι ελάχιστες. Επαναφέροντας αυτές τις γνώσεις στο προσκήνιο, προχωράμε σιγά σιγά εντοπίζοντας κενά στην κατανόησή τους, ακόμη και λάθη ως προς τον τρόπο, με τον οποίο τις είχαμε κατανοήσει. Επίσης, θα διαπιστώσουμε ότι το να σκεφτόμαστε με μαθηματικό τρόπο είναι διαφορετικό από τον τρόπο σκέψης σε άλλα επιστημονικά πεδία. Η μελέτη των Μαθηματικών είναι μια δυναμική διαδικασία, η οποία απαιτεί ενεργητικότητα, δεν είναι, δηλαδή, μια απλή επιφανειακή ανάγνωση. Επιπρόσθετα, ο περιορισμός σε ένα σύγγραμμα, όσο καλό και αν είναι αυτό, εγκλωβίζει τον αναγνώστη. Πρέπει να έχουμε μια ευελιξία στη μελέτη μας. Η μελέτη (κυρίως στα Μαθηματικά) παρουσιάζει παλινδρομήσεις. Εδώ συνειδητοποιούμε τη μεγάλη διαφορά μεταξύ του κατανοώ κάτι, του απαντώ σε ένα ερώτημα και του παρουσιάζω προφορικά ή γραπτά την απάντηση ενός προβλήματος. Όπως προείπαμε, το βιβλίο αυτό απευθύνεται, κυρίως, σε νεοεισερχόμενους φοιτητές σε Τμήματα Μαθηματικών σε Ελληνικά Πανεπιστήμια. Αυτό δεν σημαίνει ότι δεν μπορεί να φανεί χρήσιμο σε οποιονδήποτε θέλει να ξεκινήσει να ασχολείται με τη μελέτη των Μαθηματικών. Για τον λόγο αυτόν, το σύγγραμμα έχει δομηθεί με ευελιξία, ώστε να προσφέρεται και για αυτοδιδασκαλία.



Το παρόν σύγγραμμα δημιουργήθηκε στο πλαίσιο του Έργου ΚΑΛΛΙΠΟΣ+	
Χρηματοδότης	Υπουργείο Παιδείας και Θρησκευμάτων, Προγράμματα ΠΔΕ, ΕΠΑ 2020-2025
Φορέας υλοποίησης	ΕΛΚΕ ΕΜΠ
Φορέας λειτουργίας	ΣΕΑΒ/Παράρτημα ΕΜΠ/Μονάδα Εκδόσεων
Διάρκεια 2ης Φάσης	2020-2023
Σκοπός	Η δημιουργία ακαδημαϊκών ψηφιακών συγγραμμάτων ανοικτής πρόσβασης (περισσότερων από 700) • Προπτυχιακών και μεταπτυχιακών εγχειριδίων • Μονογραφιών • Μεταφράσεων ανοικτών textbooks • Βιβλιογραφικών Οδηγών
Επιστημονικά Υπεύθυνος	Νικόλαος Μήτρου, Καθηγητής ΣΗΜΜΥ ΕΜΠ
ISBN: 978-618-5726-79-9	**DOI:** http://dx.doi.org/10.57713/kallipos-206

Το παρόν σύγγραμμα χρηματοδοτήθηκε από το Πρόγραμμα Δημοσίων Επενδύσεων του Υπουργείου Παιδείας.