Θεμέλια Μαθηματικής Ανάλυσης

Πρόχειρες Σημειώσεις

Τμήμα Μαθηματικών
Πανεπιστήμιο Αθηνών
Αθήνα, 2020

Περιεχόμενα

Κεφάλαιο 1

Στοιχεία θεωρίας συνόλων

Η κεντρική έννοια αυτού του μαθήματος, η έννοια του **συνόλου**, είναι εξαιρετικά απλή. Σύνολο είναι οποιαδήποτε συλλογή ή ομάδα αντικειμένων. Έτσι, έχουμε το σύνολο όλων των φοιτητών που γράφτηκαν στο Τμήμα Μαθηματικών στη διάρκεια του 2020, το σύνολο όλων των άρτιων φυσικών αριθμών, το σύνολο όλων των σημείων του επιπέδου που έχουν απόσταση ίση με 1 από το σημείο $(0, 0)$, το σύνολο όλων των ροζ ελεφάντων.

Τα σύνολα δεν είναι αντικείμενα του πραγματικού κόσμου, όπως τα τραπέζια ή τα αστέρια. Είναι δημιουργήματα του μυαλού μας και όχι των χεριών μας. Ένα σακί γεμάτο με πατάτες δεν είναι ένα σύνολο από πατάτες, το σύνολο όλων των μορίων μιας σταγόνας νερού δεν είναι το ίδιο αντικείμενο με αυτή τη σταγόνα νερού. Ο ανθρώπινος νους έχει την ικανότητα της αφαίρεσης, μπορούμε να σκεφτόμαστε ότι ένα πλήθος διαφορετικών αντικειμένων συνδέονται μέσω κάποιας κοινής τους ιδιότητας και έτσι να θεωρούμε ένα σύνολο αντικειμένων που έχουν αυτή την ιδιότητα. Η ιδιότητα που συζητάμε δεν είναι τίποτε άλλο από την ικανότητά μας να σκεφτόμαστε αυτά τα αντικείμενα μαζί. Έτσι, υπάρχει ένα σύνολο που έχει ως στοιχεία του τους αριθμούς $2, 7, 12, 13, 29, 34$ και 11000, αν και είναι δύσκολο να δούμε τι είναι αυτό που συνδέει τους συγκεκριμένους εφτά αριθμούς. Αρκεί το γεγονός ότι τους φέραμε μαζί στο μυαλό μας. Ο Georg Cantor, ο οποίος θεμελίωσε τη θεωρία συνόλων στα τέλη του δέκατου ένατου αιώνα, περιέγραψε την έννοια του συνόλου ως εξής: «Σύνολο είναι μια συλλογή σε μία ολότητα συγκεκριμένων, διακεκριμένων αντικειμένων της διαίσθησης ή της σκέψης μας. Αυτά τα αντικείμενα λέγονται στοιχεία του συνόλου».

Στόχος αυτού του μαθήματος είναι να δούμε με ποιόν τρόπο η θεωρία συνόλων μπορεί να χρησιμεύσει ως βάση για τη θεμελίωση άλλων μαθηματικών θεωριών. Επομένως, δεν πρόκειται να ασχοληθούμε με σύνολα ανθρώπων ή μορίων, αλλά μόνο με σύνολα *μαθη-*

ματικών αντικειμένων, όπως οι αριθμοί, τα σημεία στο χώρο, οι συναρτήσεις, τα σύνολα. Όπως θα δούμε, είναι δυνατόν να ορίσουμε τις πρώτες τρεις έννοιες στα πλαίσια της θεωρίας συνόλων, σαν σύνολα με πρόσθετες ιδιότητες. Έτσι, όλα τα αντικείμενα με τα οποία θα ασχοληθούμε είναι σύνολα. Για να επεξηγήσουμε κάποια σημεία, θα μιλάμε για σύνολα αριθμών ή σημείων πριν δώσουμε τον ακριβή ορισμό αυτών των εννοιών. Αυτό όμως θα γίνεται μόνο στα παραδείγματα, τις ασκήσεις και τα προβλήματα, όχι στο κύριο σώμα της θεωρίας.

Σύνολα μαθηματικών αντικειμένων είναι, για παράδειγμα:

(α) Το σύνολο των πρώτων διαιρετών του 324.
(β) Το σύνολο όλων των φυσικών αριθμών που διαιρούνται με το 0.
(γ) Το σύνολο όλων των συνεχών συναρτήσεων $f : [0, 1] \to \mathbb{R}$.
(δ) Το σύνολο όλων των ελλείψεων με κύριο άξονα 5 και εκκεντρότητα 3.
(ε) Το σύνολο όλων των συνόλων που τα στοιχεία τους είναι φυσικοί αριθμοί μικρότεροι από τον 20.

Εξετάζοντας αυτά και πολλά άλλα όμοια παραδείγματα, διαπιστώνουμε ότι τα σύνολα με τα οποία δουλεύουν οι μαθηματικοί είναι σχετικά απλά. Μελετάμε τους φυσικούς αριθμούς και διάφορα υποσύνολά τους (όπως το σύνολο όλων των πρώτων αριθμών), καθώς και σύνολα ζευγών, τριάδων και γενικότερα n-άδων φυσικών αριθμών. Μπορούμε να ορίσουμε τους ακέραιους και τους ρητούς αριθμούς χρησιμοποιώντας μόνο τέτοια σύνολα. Κατόπιν, οι πραγματικοί αριθμοί ορίζονται ως σύνολα ακολουθιών ρητών αριθμών. Η μαθηματική ανάλυση ασχολείται με σύνολα πραγματικών αριθμών και πραγματικές συναρτήσεις (σύνολα διατεταγμένων ζευγών από πραγματικούς αριθμούς) και, μερικές φορές, μελετώνται σύνολα συναρτήσεων ή και σύνολα συνόλων συναρτήσεων. Οι «εργαζόμενοι μαθηματικοί» σπάνια συναντούν αντικείμενα πιο πολύπλοκα από αυτά.

1.1 Σύνολα

Τα αντικείμενα από τα οποία αποτελείται ένα σύνολο ονομάζονται **στοιχεία** του συνόλου. Λέμε ότι τα στοιχεία ενός συνόλου **ανήκουν** σε αυτό. Για να συμβολίσουμε ότι το στοιχείο x ανήκει στο σύνολο S γράφουμε

$$x \in S.$$

Εάν το x δεν ανήκει στο S γράφουμε

$$x \notin S.$$

Για να γνωρίζουμε ποιό σύνολο εξετάζουμε, πρέπει να γνωρίζουμε ακριβώς ποιά είναι τα στοιχεία του. Και αντίστροφα, εάν γνωρίζουμε ακριβώς τα στοιχεία ενός συνόλου, τότε

γνωρίζουμε το σύνολο. Ένα ζήτημα είναι ότι μπορούμε να περιγράψουμε το ίδιο σύνολο με διαφορετικούς τρόπους. Για παράδειγμα, εάν A είναι το σύνολο των ριζών της εξίσωσης

$$x^2 - 6x + 8 = 0$$

και B το σύνολο των άρτιων αριθμών μεταξύ του 1 και του 5, τότε το A και το B έχουν ακριβώς δύο στοιχεία, τους αριθμούς 2 και 4. Συνεπώς, το A και το B είναι το ίδιο σύνολο. Δύο σύνολα είναι **ίσα** εάν έχουν τα ίδια στοιχεία. Συμβολίζουμε την ισότητα των συνόλων S και T με

$$S = T,$$

ενώ όταν δεν είναι ίσα γράφουμε

$$S \neq T.$$

Ο απλούστερος τρόπος για να προσδιορίσουμε ένα σύνολο είναι να καταγράψουμε όλα τα στοιχεία του, εάν αυτό είναι δυνατό. Ο συνήθης συμβολισμός είναι να τα κλείνουμε σε αγκύλες $\{\ \}$. Όταν γράφουμε

$$S = \{1, 2, 3, 4, 5, 6\}$$

εννοούμε το σύνολο του οποίου τα στοιχεία είναι οι αριθμοί $1, 2, 3, 4, 5, 6$, και μόνον αυτοί.

Πρέπει να τονίσουμε δύο σημεία σχετικά με αυτό το συμβολισμό, συνέπειες και τα δύο της έννοιας της ισότητας για σύνολα. Πρώτον, η σειρά με την οποία γράφουμε τα στοιχεία είναι αδιάφορη:

$$\{5, 4, 3, 2, 6, 1\} = \{1, 2, 3, 4, 5, 6\}.$$

Δεύτερον, επαναλήψεις των στοιχείων στην καταγραφή δεν αλλάζουν το σύνολο:

$$\{1, 2, 3, 4, 6, 1, 3, 5\} = \{1, 2, 3, 4, 5, 6\}.$$

Για να προσδιορίσουμε κάποιο σύνολο, μπορεί να μην είναι πρακτικό, ή ούτε καν δυνατό να καταγράψουμε όλα τα στοιχεία του. Το σύνολο των πρώτων αριθμών περιγράφεται πολύ καλύτερα με αυτή τη φράση παρά με την απαρίθμηση μερικών πρώτων

$$\{2, 3, 5, 7, 11, 13, 17, 19, \ldots\}.$$

Θα μπορούσαμε να γράψουμε

$$P = \{\text{όλοι οι πρώτοι αριθμοί}\}.$$

Μια χρήσιμη παραλλαγή είναι

$$P = \{p \mid p \text{ είναι πρώτος αριθμός}\}.$$

Γενικότερα, ο συμβολισμός

$$Q = \{x \mid \text{«κάτι σχετικό με το } x\text{»}\}$$

διαβάζεται «Q είναι το σύνολο όλων των x για τα οποία ισχύει το κάτι σχετικό με το x». Για να προσδιορίσουμε, για παράδειγμα, το σύνολο των λύσεων της εξίσωσης $x^2 - 5x + 6 = 0$ θα μπορούσαμε να λύσουμε την εξίσωση και να γράψουμε $S = \{2, 3\}$, ή θα μπορούσαμε να γράψουμε

$$S = \{x \mid x^2 - 5x + 6 = 0\}.$$

Ο δεύτερος τρόπος προσδιορίζει το σύνολο χωρίς να μας δίνει ρητά τα στοιχεία του, αλλά και χωρίς να χρειάζεται να λύσουμε την εξίσωση.

Με αυτό το συμβολισμό υπάρχει κάποια ασάφεια. Εάν αναφερόμαστε στους φυσικούς αριθμούς, το σύνολο

$$\{x \mid 1 \leqslant x \leqslant 5\}$$

αποτελείται από τους αριθμούς $1, 2, 3, 4, 5$, αλλά εάν αναφερόμαστε στους πραγματικούς αριθμούς, τότε περιλαμβάνει και όλους τους υπόλοιπους πραγματικούς αριθμούς μεταξύ του 1 και του 5. Ο καλύτερος τρόπος να κάνουμε αυτή τη διάκριση είναι να προσδιορίσουμε το σύνολο Y από το οποίο επιλέγουμε τα x που ικανοποιούν το «κάτι σχετικό με το x». Ο συμβολισμός

$$X = \{x \in Y \mid \text{«κάτι σχετικό με το } x\text{»}\}$$

σημαίνει ότι «X είναι το σύνολο όλων των στοιχείων x του συνόλου Y για τα οποία ισχύει το κάτι σχετικό με το x».

Ένας πιο σοβαρός λόγος για να διευκρινίζουμε το σύνολο Y από το οποίο επιλέγουμε τα στοιχεία του X είναι για να εξασφαλίσουμε ότι το «κάτι σχετικό με το x» έχει νόημα για όλα τα $x \in Y$, είναι δηλαδή μια ιδιότητα που είναι σαφές εάν ισχύει ή δεν ισχύει για κάθε στοιχείο του Y, και τότε X είναι το σύνολο των στοιχείων του Y για τα οποία ισχύει αυτή η ιδιότητα.

Άσκηση 1.1.1. Εξετάστε αν οι παρακάτω προτάσεις είναι αληθείς ή ψευδείς. Εξηγήστε σύντομα την απάντησή σας.

(α) $1 \in \{1, 2\}$
(β) $3 \in \{1, 5, 2, 3\}$
(γ) $3 \in \{1, 5, 2\}$
(δ) $\{1, 3\} \in \{1, 3, 5, 2\}$
(ε) $\{5\} \in \{1, 3, 5, 2\}$
(στ) $2 \in \{x \in \mathbb{R} \mid x^2 - 3x + 2 = 0\}$
(ζ) $\{1, 4, 2, 3\} = \{2, 3, 1, 4, 3, 2\}$
(η) $\{a, d, b, d\} = \{a, b, d\}$
(θ) $\{a, b, d, d\} = \{a, b, a, d\}$
(ι) $\{x \in \mathbb{Q} \mid x^2 - 2x = 0\} = \{x \in \mathbb{R} \mid x^2 - 2x = 0\}$

1.2 Υποσύνολα

Ένα σύνολο B είναι **υποσύνολο** του συνόλου A άν κάθε στοιχείο του B είναι και στοιχείο του A. Τότε, λέμε επίσης ότι το B **περιέχεται** στο A και γράφουμε

$$B \subseteq A.$$

Πρόταση 1.2.1. *Εάν A και B είναι σύνολα, τότε $A = B$ εάν και μόνο εάν $A \subseteq B$ και $B \subseteq A$.*

Απόδειξη. Εάν $A = B$ τότε, εφόσον $A \subseteq A$, έπεται ότι $A \subseteq B$ και $B \subseteq A$. Αντιστρόφως, υποθέτουμε ότι $A \subseteq B$ και $B \subseteq A$. Τότε κάθε στοιχείο του A είναι στοιχείο του B και κάθε στοιχείο του B είναι στοιχείο του A. Άρα, τα A και B έχουν τα ίδια στοιχεία, και συνεπώς $A = B$. □

Πρόταση 1.2.2. *Εάν A, B, C είναι σύνολα, και $A \subseteq B$ και $B \subseteq C$, τότε $A \subseteq C$.*

Απόδειξη. Κάθε στοιχείο του A είναι στοιχείο του B και κάθε στοιχείο του B είναι στοιχείο του C. Άρα, κάθε στοιχείο του A είναι στοιχείο του C, και συνεπώς $A \subseteq C$. □

Είναι πολύ σημαντικό να διακρίνουμε υποσύνολα και στοιχεία. Τα στοιχεία του $\{1, 2\}$ είναι τα 1 και 2. Τα υποσύνολα του $\{1, 2\}$ είναι τα $\{1, 2\}$, $\{1\}$, $\{2\}$, και ακόμη ένα υποσύνολο, που προς το παρόν θα το συμβολίσουμε $\{\ \}$.

Η Πρόταση 1.2.2 δεν ισχύει αν αντικαταστήσουμε το $\subseteq$ με το $\in$. Τα στοιχεία ενός στοιχείου του συνόλου X δεν είναι απαραίτητα στοιχεία του X. Για παράδειγμα, εάν $A = 1$, $B = \{1, 2\}$ και $C = \{\{1, 2\}, \{3, 4\}\}$, τότε $A \in B$ και $B \in C$ αλλά τα στοιχεία του C είναι *τα σύνολα* $\{1, 2\}$ και $\{3, 4\}$, άρα το $A = 1$ δεν είναι στοιχείο του C.

Το σύνολο που συμβολίσαμε με $\{\ \}$ είναι ένα σύνολο το οποίο δεν περιέχει κανένα στοιχείο. Ένα τέτοιο σύνολο το λέμε **κενό**. Για παράδειγμα, το σύνολο

$$\{x \in \mathbb{Z} \mid x = x + 1\}$$

είναι κενό, αφού η εξίσωση $x = x + 1$ δεν έχει λύσεις στο $\mathbb{Z}$. Ένα κενό σύνολο έχει κάποιες αξιοπρόσεκτες ιδιότητες. Εάν E είναι ένα κενό σύνολο και X είναι οποιοδήποτε σύνολο, τότε $E \subseteq X$. Ας δούμε γιατί. Πρέπει να δείξουμε ότι κάθε στοιχείο του E είναι στοιχείο του X. Για να μην ισχύει αυτό, θα πρέπει να υπάρχει κάποιο στοιχείο του E που να μην ανήκει στο X. Αφού όμως το E είναι κενό, δεν υπάρχει κανένα τέτοιο στοιχείο.

Εάν E και F είναι δύο κενά σύνολα, από τη συζήτηση που προηγήθηκε έχουμε ότι $E \subseteq F$ και $F \subseteq E$. Άρα, $E = F$. Όλα τα κενά σύνολα είναι ίσα. Άρα, υπάρχει ένα μοναδικό κενό σύνολο. Δίνουμε σε αυτό το σύνολο ένα ειδικό σύμβολο: με

$$\varnothing$$

θα συμβολίζουμε το *μοναδικό* κενό σύνολο.

Άσκηση 1.2.3. Εξετάστε αν οι παρακάτω προτάσεις είναι αληθείς ή ψευδείς. Εξηγήστε σύντομα την απάντησή σας.

(α) $1 \subseteq \{1, 2\}$
(β) $\{3, 1\} \subseteq \{1, 5, 2, 3\}$
(γ) $\{3\} \subseteq \{1, 5, 2\}$
(δ) $\{1, 3\} \in \{1, 3, 5, 2\}$
(ε) $\{5\} \in \{1, 3, 5, 2\}$
(στ) $2 \subseteq \{x \in \mathbb{R} \mid x^2 - 3x + 2 = 0\}$
(ζ) $\{1, 4, 2, 3\} \subseteq \{2, 3, 1, 4, 3, 2\}$
(η) $\{a, d, b, d\} \subseteq \{a, b, a, d\}$
(θ) $\{b \in \mathbb{N} \mid b > 2\} = \{a \in \mathbb{N} \mid a > 2\}$
(ι) $\{b \in \mathbb{N} \mid b > 2\} \subseteq \{a \in \mathbb{N} \mid a > 2\}$
(ια) $\{2\} \subseteq \{1, \{2\}\}$
(ιβ) $\{2\} \in \{1, \{2\}\}$
(ιγ) $\{b \in \mathbb{N} \mid b \geqslant 2\} \subseteq \{a \in \mathbb{N} \mid a > 2\}$
(ιδ) $\{x \in \mathbb{Q} \mid x^2 - 2 = 0\} = \varnothing$

1.3 Το παράδοξο του Russell

Όπως υπάρχει το κενό σύνολο, που δεν περιέχει κανένα στοιχείο, μπορούμε να αναρωτηθούμε εάν υπάρχει ένα σύνολο που να περιέχει τα πάντα. Θα δούμε ότι αυτή η ιδέα είναι παρατραβηγμένη.

Ας θεωρήσουμε τη συλλογή Ω όλων των συνόλων. Εάν αυτή η συλλογή Ω είναι σύνολο, τότε το ίδιο το Ω θα πρέπει να είναι στοιχείο του εαυτού του:

$$\Omega \in \Omega.$$

Τα συνηθισμένα σύνολα που έχουμε συναντήσει, όπως το σύνολο $\mathbb{N}$, δεν είναι στοιχεία του εαυτού τους. Μπορείτε να αφιερώσετε λίγη ώρα προσπαθώντας να φανταστείτε κάποιο σύνολο που είναι στοιχείο του εαυτού του.

Τώρα μπορούμε να θεωρήσουμε το υποσύνολο S του Ω που αποτελείται από τα σύνολα που δεν είναι στοιχεία του εαυτού τους,

$$S = \{A \in \Omega \mid A \notin A\}.$$

Αφού $S \subseteq \Omega$, το S είναι επίσης σύνολο, και μπορούμε να αναρωτηθούμε εάν το S είναι στοιχείο του εαυτού του. Τώρα όμως έχουμε το εξής παράδοξο.

- Εάν $S \in S$, τότε $S \in \Omega$ αλλά το S δεν ικανοποιεί την ιδιότητα που χαρακτηρίζει τα στοιχεία του S, και συνεπώς $S \notin S$.

- Εάν $S \notin S$, τότε $S \in \Omega$ και το S ικανοποιεί την ιδιότητα που χαρακτηρίζει τα στοιχεία του S, συνεπώς $S \in S$.

Οποιαδήποτε από τις δύο υποθέσεις για το S οδηγεί σε αντίφαση.

Αυτό το παράδοξο, γνωστό με το όνομα παράδοξο του Russell, προέκυψε επειδή θεωρήσαμε ότι συλλογές όπως η S ή η Ω είναι σύνολα. Η αρχική μας περιγραφή ενός συνόλου ως μιας *οποιασδήποτε* συλλογής δεν είναι επαρκής. Σε πιο προχωρημένα μαθήματα Θεωρίας Συνόλων θα δούμε πώς ξεπερνιούνται τα παράδοξα, με κατάλληλο περιορισμό της έννοιας του συνόλου. Προς το παρόν, θα προσέχουμε τα σύνολα που εξετάζουμε να είναι σαφώς προσδιορισμένα, και να γνωρίζουμε ακριβώς ποια στοιχεία ανήκουν στο σύνολο και ποια όχι.

Η μη ύπαρξη ενός συνόλου των πάντων είναι ακόμη ένας λόγος για τον οποίο ο συμβολισμός

$$\{x \in Y \mid P(x)\},$$

όπου Y είναι ένα γνωστό σύνολο, και $P(x)$ «κάτι σχετικό με το x», είναι απαραίτητος εκτός αν το Y συνάγεται από τα συμφραζόμενα. Έχοντας προσδιορίσει το Y, μπορούμε να εξετάσουμε την ιδιότητα $P(x)$ και να βεβαιωθούμε ότι έχει νόημα για όλα τα στοιχεία του Y, πριν επιλέξουμε αυτά για τα οποία είναι αληθής.

Αλλιώς είναι σαν να θεωρούμε το $\{x \in \Omega \mid P(x)\}$, κάτι που όπως είδαμε μπορεί να οδηγήσει σε παράδοξα. Παρατηρήστε ότι εάν θεωρήσουμε κάποιο συγκεκριμένο σύνολο που αποτελείται από σύνολα, η ιδιότητα $X \notin X$ δεν παρουσιάζει κανένα πρόβλημα. Για παράδειγμα, εάν $T = \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, τότε

$$\{X \in T \mid X \notin X\} = \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\},$$

και προφανώς $T \notin T$.

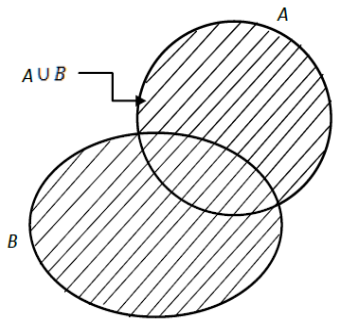
1.4 Ένωση και Τομή

Δύο σημαντικές μέθοδοι για να δημιουργούμε νέα σύνολα είναι η ένωση και η τομή. Η **ένωση** δύο συνόλων A και B είναι το σύνολο του οποίου τα στοιχεία είναι τα στοιχεία του A και τα στοιχεία του B και μόνον αυτά. Εάν

$$A = \{1, 2, 3\} \qquad B = \{3, 4, 5\}$$

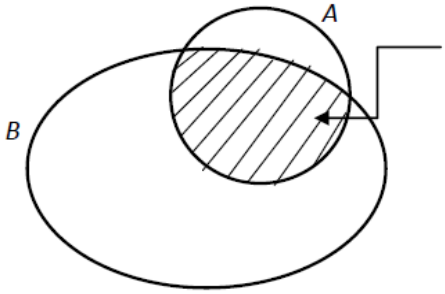
τότε η ένωση είναι το $\{1, 2, 3, 4, 5\}$. Συμβολίζουμε την ένωση των συνόλων A και B με $A \cup B$:

$$A \cup B = \{x \mid x \in A \text{ ή } x \in B \text{ (ή και τα δύο)}\}.$$



Η **τομή** δύο συνόλων A και B είναι το σύνολο του οποίου τα στοιχεία είναι όλα τα κοινά στοιχεία των A και B. Για τα σύνολα A και B του προηγούμενου παραδείγματος η τομή είναι το σύνολο $\{3\}$, γιατί μόνο το 3 ανήκει και στα δύο σύνολα. Συμβολίζουμε την τομή των συνόλων A και B με $A \cap B$:

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



Άσκηση 1.4.1. Προσδιορίστε τα παρακάτω σύνολα:

(α) $\{1, 2, \{4\}\} \cup \{2, 3, 6\}$.
(β) $\{1, \{2\}, 4\} \cap \{2, 3, 6\}$.
(γ) $A \cup B$, όπου $A = \{x \in \mathbb{Z} \mid |x| \geqslant 3\}$ και $B = \{y \in \mathbb{Z} \mid y \leqslant -3\}$.
(δ) $C \cap D$, όπου $C = \{x \in \mathbb{Z} \mid |x| \geqslant 3\}$ και $D = \{y \in \mathbb{Z} \mid y \leqslant 3\}$.

Πρόταση 1.4.2. *Εάν A, B, C είναι σύνολα, τότε*

1. $A \cup \varnothing = A$

2. $A \cup A = A$

3. $A \cup B = B \cup A$

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

Απόδειξη. Μόνο το 4 παρουσιάζει κάποια δυσκολία. Υποθέτουμε ότι $x \in (A \cup B) \cup C$. Τότε $x \in A \cup B$ είτε $x \in C$. Εάν $x \in C$, τότε $x \in B \cup C$, άρα $x \in A \cup (B \cup C)$. Εάν $x \notin C$, τότε $x \in A$ είτε $x \in B$. Σε κάθε περίπτωση έχουμε $x \in A \cup (B \cup C)$. Έχουμε δείξει ότι εάν $x \in (A \cup B) \cup C$ τότε $x \in A \cup (B \cup C)$, δηλαδή

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

Με ένα παρόμοιο επιχείρημα δείχνουμε ότι

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

Από την Πρόταση 1.2.1 έχουμε το ζητούμενο. □

Παρόμοια αποτελέσματα ισχύουν για τις τομές.

Πρόταση 1.4.3. *Εάν A, B, C είναι σύνολα, τότε*

1. $A \cap \varnothing = \varnothing$

2. $A \cap A = A$

3. $A \cap B = B \cap A$

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

Απόδειξη. Οι αποδείξεις είναι ανάλογες με αυτές της Πρότασης 1.4.2. □

Άσκηση 1.4.4. Συμπληρώστε τις αποδείξεις των Προτάσεων 1.4.2 και 1.4.3.

Τέλος υπάρχουν δύο ταυτότητες που συνδέουν ενώσεις και τομές.

Πρόταση 1.4.5. *Εάν τα A, B, C είναι σύνολα, τότε*

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

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

Απόδειξη. Εάν $x \in A \cup (B \cap C)$, τότε $x \in A$ είτε $x \in B \cap C$. Εάν $x \in A$ τότε $x \in A \cup B$ και $x \in A \cup C$, άρα $x \in (A \cup B) \cap (A \cup C)$. Αλλιώς, $x \in B \cap C$, κάτι που συνεπάγεται ότι $x \in B$ και $x \in C$. Άρα $x \in A \cup B$ και $x \in A \cup C$, συνεπώς $x \in (A \cup B) \cap (A \cup C)$. Αυτό δείχνει ότι

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

Αντίστροφα, υποθέτουμε ότι $y \in (A \cup B) \cap (A \cup C)$. Τότε $y \in A \cup B$ και $y \in A \cup C$. Θα εξετάσουμε δύο περιπτώσεις: όταν $y \in A$ και όταν $y \notin A$. Στην πρώτη περίπτωση έχουμε $y \in A \cup (B \cap C)$. Στη δεύτερη περίπτωση, εφόσον $y \in A \cup B$, πρέπει να ισχύει $y \in B$, και παρόμοια $y \in C$. Έπεται ότι $y \in B \cap C$, και συνεπώς, και σε αυτή την περίπτωση έχουμε ότι $y \in A \cup (B \cap C)$. Άρα,

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

Τα δύο αποτελέσματα δίνουν τη ζητούμενη ταυτότητα. Η απόδειξη του 2 είναι ανάλογη. □

Άσκηση 1.4.6. Συμπληρώστε την απόδειξη της Πρότασης 1.4.5.

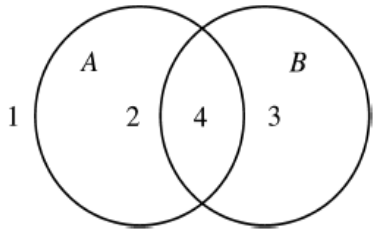
Η Πρόταση 1.4.5 μας δίνει δύο *επιμεριστικούς* νόμους, ανάλογους με τον επιμεριστικό κανόνα για τον πολλαπλασιασμό ως προς την πρόσθεση:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

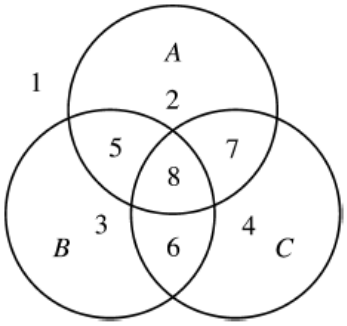
Προσέξτε ότι στην περίπτωση των αριθμητικών πράξεων δεν ισχύει η επιμεριστική ιδιότητα εάν αντιστρέψουμε τις πράξεις: η πρόσθεση δεν είναι επιμεριστική ως προς τον πολλαπλασιασμό.

Τα λεγόμενα **διαγράμματα Venn** προσφέρουν έναν τρόπο να παραστήσουμε αυτές τις συνολοθεωρητικές ταυτότητες.

Τέτοια σχήματα συχνά βοηθούν στην κατανόηση των σχέσεων μεταξύ των διαφόρων συνόλων, αλλά πρέπει να σχεδιαστούν προσεκτικά για να παριστάνουν τη γενικότερη κάθε φορά περίπτωση. Εάν έχουμε ένα σύνολο, στο διαγραμμα Venn εμφανίζονται δύο περιοχές: τα σημεία που ανήκουν στο σύνολο και εκείνα που δεν ανήκουν στο σύνολο.



Με δύο σύνολα έχουμε τέσσερεις περιοχές, ενώ με τρία σύνολα οκτώ περιοχές. Είναι εύκολο να σχεδιάσουμε τρεις κύκλους ώστε να διακρίνονται οι οκτώ περιοχές που παριστάνουν τη γενική περίπτωση για τρία σύνολα.



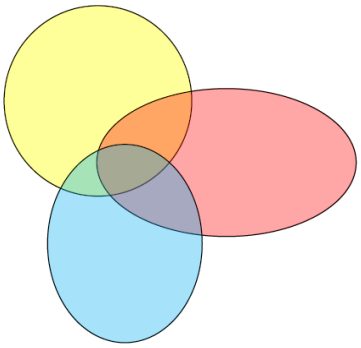
Για τέσσερα σύνολα, το ανάλογο σχήμα δεν μπορεί να γίνει με κύκλους. Μπορείτε να το καταφέρετε με τρεις κύκλους και ένα ελεύθερο σχήμα;

Τα διαγράμματα αποτελούν σημαντικό βοήθημα για την κατανόηση της κατάστασης. Όμως σε αυτό το στάδιο των σπουδών σας, όταν σας ζητείται να αποδείξετε μια σχέση μεταξύ συνόλων, μπορείτε να χρησιμοποιήσετε επικουρικά το διάγραμμα, αλλά είναι απαραίτητο να γράψετε την απόδειξη χρησιμοποιώντας με προσοχή τον σωστό μαθηματικό συυμβολισμό και ακριβείς μαθηματικές διατυπώσεις.

Άσκηση 1.4.7. Σχεδιάστε τα διαγράμματα Venn στις ακόλουθες περιπτώσεις:

(α) Έχουμε δύο σύνολα A και B που ικανοποιούν τις $A \cup B \subseteq B$ και $B \nsubseteq A$.

(β) Έχουμε τρία σύνολα A, B και C που ικανοποιούν τις $A \cap B \cap C = \varnothing$, $A \cap B \neq \varnothing$, $A \cap C \neq \varnothing$ και $B \cap C \neq \varnothing$.



Πρόταση 1.4.8. *Εάν A και B είναι δύο σύνολα, οι επόμενες ιδιότητες είναι ισοδύναμες:*

1. $A \subseteq B$
2. $A \cap B = A$
3. $A \cup B = B$.

Με τον όρο «ισοδύναμες» εννοούμε ότι κάθε μία από τις τρεις ιδιότητες ισχύει εάν και μόνο εάν ισχύουν και οι άλλες δύο. Συμβολικά,

$$(A \subseteq B) \iff (A \cap B = A) \iff (A \cup B = B).$$

Απόδειξη. Υποθέτουμε ότι $A \subseteq B$ και θέλουμε να δείξουμε ότι $A \cap B = A$. Γνωρίζουμε ότι $A \cap B \subseteq A$. Εάν $x \in A$, τότε, αφού $A \subseteq B$, έχουμε $x \in B$, άρα $x \in A \cap B$. Δηλαδή, $A \subseteq A \cap B$. Άρα, $A \cap B = A$.

Αντίστροφα, υποθέτουμε ότι $A \cap B = A$ και θέλουμε να δείξουμε ότι $A \subseteq B$. Εάν $x \in A$, τότε $x \in A \cap B$, άρα $x \in B$. Συνεπώς, $A \subseteq B$.

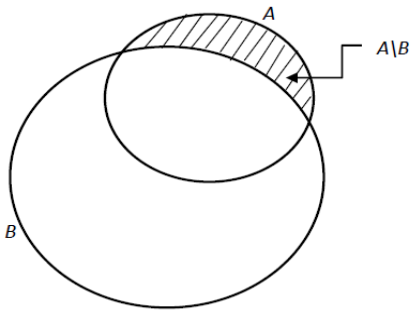
Έτσι, έχουμε δείξει ότι τα 1 και 2 είναι ισοδύναμα.

Για την ισοδυναμία των 1 και 3, παρατηρούμε ότι το 3 μας λέει ότι εάν βάλουμε τα στοιχεία του A μαζί με τα στοιχεία του B, παίρνουμε το σύνολο B. Συμπληρώστε πιο αναλυτικά την απόδειξη, όπως κάναμε για την προηγούμενη ισοδυναμία. □

1.5 Συμπληρώματα

Εάν A και B είναι σύνολα, η συνολοθεωρητική **διαφορά** $A \setminus B$ ορίζεται ως το σύνολο όλων των στοιχείων του A που δεν ανήκουν στο B:

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



Άσκηση 1.5.1. Εάν $A = \{1, 2, 3\}$ και $B - \{1, 5, 6, 7\}$, βρείτε τα σύνολα $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$ και $(A \cup B) \setminus (A \cap B)$.

Εάν το B είναι υποσύνολο του A, ονομάζουμε το $A \setminus B$ **συμπλήρωμα του B ως προς το A**.

Δεν μπορούμε να ξεχάσουμε το A και να ορίσουμε το συμπλήρωμα του B ως το σύνολο όλων όσα δεν ανήκουν στο B, γιατί τότε η ένωση του B και του υποτιθέμενου συμπληρώματος θα ήταν το σύνολο Ω των πάντων, το οποίο όπως είδαμε δεν μπορεί να υπάρχει.

Σε συγκεκριμένες περιπτώσεις μπορεί να υπάρχει ένα σύνολο που περιέχει όλα τα αντικείμενα που εξετάζουμε. Τότε ονομάζουμε αυτό το σύνολο **χώρο**. Όταν αναφερόμαστε σε ακεραίους αριθμούς, ο χώρος μπορεί να είναι το σύνολο $\mathbb{Z}$ των ακεραίων. Όταν έχουμε στο νου μας κάποιο συγκεκριμένο χώρο U, ορίζουμε το **συμπλήρωμα** B^c κάθε υποσυνόλου του U να είναι το

$$B^c = U \setminus B,$$

δηλαδή το συμπλήρωμα του B ως προς το χώρο U. Στην επόμενη πρόταση δίνουμε κάποιες ιδιότητες του συμπληρώματος:

Πρόταση 1.5.2. *Εάν τα A και B είναι υποσύνολα του χώρου U, ισχύουν τα ακόλουθα:*

1. $\varnothing^c = U$
2. $U^c = \varnothing$
3. $(A^c)^c = A$
4. *Εάν $A \subseteq B$ τότε $B^c \subseteq A^c$.*

Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι **κανόνες De Morgan** για τη σχέση του συμπληρώματος με τις ενώσεις και τις τομές:

Πρόταση 1.5.3. *Εάν A και B είναι υποσύνολα του χώρου U, τότε ισχύουν τα ακόλουθα:*

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

Απόδειξη. Εάν $x \in (A \cup B)^c$, τότε $x \notin A \cup B$. Αυτό σημαίνει ότι $x \notin A$ και $x \notin B$, άρα $x \in A^c$ και $x \in B^c$, και συνεπώς $x \in A^c \cap B^c$. Επομένως,

$$(A \cup B)^c \subseteq A^c \cap B^c.$$

Για να αποδείξουμε τον αντίθετο εγκλεισμό, αντιστρέφουμε τα βήματα της προηγούμενης απόδειξης. Έτσι αποδεικνύεται η 1.

Για να αποδείξουμε την 2 μπορούμε να ακολουθήσουμε ανάλογα βήματα. Ένας άλλος τρόπος είναι να αντικαταστήσουμε το A με το A^c και το B με το B^c στην 1, που δίνει

$$(A^c \cup B^c)^c = A^{cc} \cap B^{cc} = A \cap B.$$

Κατόπιν παίρνουμε συμπληρώματα και έχουμε

$$(A \cap B)^c = (A^c \cup B^c)^{cc} = A^c \cup B^c,$$

που είναι η 2. □

Άσκηση 1.5.4. Απλοποιήστε τις ακόλουθες εκφράσεις:
(α) $(D^c \cup F)^c \cup (D \cap F)$.
(β) $((X^c \cup Y) \cap (X^c \cup Y^c))^c$.

Άσκηση 1.5.5. Έστω A και B δύο υποσύνολα του χώρου U. Δείξτε ότι $A \setminus B = A \cap B^c$ και, χρησιμοποιώντας αυτή την ισότητα, δείξτε ότι, για κάθε $A, B, C \subseteq U$,
(α) $(A \setminus B) \setminus C = A \setminus (B \cup C)$.
(β) $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$.

Ορισμός 1.5.6. Η **συμμετρική διαφορά** $A \triangle B$ δύο συνόλων A και B ορίζεται να είναι το σύνολο

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

Άσκηση 1.5.7. Αποδείξτε ότι $A \triangle B = (A \cup B) \setminus (A \cap B)$.

Άσκηση 1.5.8. Αν A είναι ένα σύνολο, βρείτε τα σύνολα $A \triangle A$ και $A \triangle \varnothing$. Αποδείξτε ότι $A \triangle B = B \triangle A$.

Από τα προηγούμενα ίσως έχετε παρατηρήσει ότι οι κανόνες της θεωρίας συνόλων εμφανίζονται ανά ζεύγη: για κάθε κανόνα, εάν αλλάξουμε τις ενώσεις σε τομές και τις τομές σε ενώσεις, παίρνουμε έναν άλλον κανόνα. Ονομάζουμε αυτή την παρατήρηση **αρχή δυϊσμού του De Morgan**:

> Εάν σε μια συνολοθεωρητική ταυτότητα στην οποία εμφανίζονται μόνο οι πράξεις $\cup$ και $\cap$ αντικαταστήσουμε κάθε $\cup$ με $\cap$ και κάθε $\cap$ με $\cup$, προκύπτει μια νέα αληθής ταυτότητα.

Η γενική απόδειξη αυτού του αποτελέσματος βασίζεται σε μια κάπως περίπλοκη επαγωγή που κρύβει την απλότητα του βασικού επιχειρήματος. Θεωρούμε λοιπόν ένα χαρακτηριστικό παράδειγμα: γνωρίζουμε ότι ισχύει η ταυτότητα

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \tag{1.5.1}$$

Παίρνοντας τα συμπληρώματα και εφαρμόζοντας δύο φορές τους κανόνες De Morgan καταλήγουμε στην

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

Αυτή η ταυτότητα ισχύει για οποιαδήποτε σύνολα A, B, C, άρα ισχύει και για τα A^c, B^c, C^c, συνεπώς ισχύει η ταυτότητα

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

η οποία προκύπτει από την (1.5.1) αν εφαρμόσουμε την αρχή δυϊσμού του De Morgan.

1.6 Σύνολα από σύνολα

Μερικές φορές εξετάζουμε σύνολα τα στοιχεία των οποίων είναι επίσης σύνολα. Για παράδειγμα, μπορούμε να θεωρήσουμε το $S = \{A, B\}$, όπου $A = \{1, 2\}$ και $B = \{2, 3, 4\}$. Ένα άλλο παράδειγμα είναι το σύνολο όλων των υποσυνόλων ενός συνόλου X, το οποίο ονομάζεται **δυναμοσύνολο** του X και συμβολίζεται με $\mathbb{P}(X)$:

$$Y \in \mathbb{P}(X) \text{ εάν και μόνο εάν } Y \subseteq X.$$

Εάν $X = \{0, 1\}$ τότε $\mathbb{P}(X) = \{\varnothing, \{0\}, \{1\}, \{0, 1\}\}$.

Σε αυτές τις περιπτώσεις, όπου κάθε στοιχείο του S είναι σύνολο, μπορούμε να προχωρήσουμε ένα βήμα παραπέρα και να θεωρήσουμε τα στοιχεία των στοιχείων του S. Έτσι μπορούμε να γενικεύσουμε τις έννοιες της ένωσης και της τομής και να ορίσουμε

$$\bigcup S = \{x \mid x \in A \text{ για κάποιο } A \in S\},$$

και, εάν $S \neq \varnothing$,

$$\bigcap S = \{x \mid x \in A \text{ για κάθε } A \in S\}.$$

Το σύνολο $\bigcup S$ ονομάζεται **ένωση** του S και το $\bigcap S$ ονομάζεται **τομή** του S. Η ένωση του S αποτελείται από όλα τα στοιχεία των στοιχείων του S, ενώ η τομή του S αποτελείται από τα κοινά στοιχεία όλων των στοιχείων του S. Για παράδειγμα,

$$\bigcup\{\{1,2\},\{2,3,4\}\} = \{1,2,3,4\}$$

και

$$\bigcap\{\{1,2\},\{2,3,4\}\} = \{2\}.$$

Για κάθε σύνολο X ισχύει

$$\bigcup \mathbb{P}(X) = X \quad \text{και} \quad \bigcap \mathbb{P}(X) = \varnothing.$$

Αυτός ο συμβολισμός γενικεύει πράγματι την ένωση και την τομή δύο συνόλων. Εάν $S = \{A_1, A_2, \ldots, A_n\}$, χρησιμοποιούμε τον εναλλακτικό συμβολισμό

$$\bigcup S = \bigcup_{r=1}^{n} A_r$$

και

$$\bigcap S = \bigcap_{r=1}^{n} A_r.$$

Άσκηση 1.6.1. Βρείτε το δυναμοσύνολο του συνόλου $X = \{\alpha, \gamma, \omega\}$ και το δυναμοσύνολο του συνόλου $A = \{a, \{a, b\}\}$.

Άσκηση 1.6.2. Εάν S είναι το σύνολο των υποσυνόλων του $\mathbb{Z}$ στα οποία ανήκει το 0, βρείτε τα

$$\bigcup S \quad \text{και} \quad \bigcap S.$$

1.7 Ασκήσεις

1. Εξετάστε αν οι παρακάτω προτάσεις είναι αληθείς ή ψευδείς. Εξηγήστε σύντομα την απάντησή σας.

(α) $1 \subseteq \{1, 3, 5, 2\}$
(β) $\{1, 2\} \subseteq \{1, 3, 5, 2\}$
(γ) $\{x \in \mathbb{R} \mid x^2 - 3x + 2 = 0\} \subseteq \{1, 3, 5\}$
(δ) $\{x \in \mathbb{R} \mid x^2 - 3x + 2 = 0\} \in \mathbb{N}$
(ε) $\sqrt{2} \in \{x \in \mathbb{Q} \mid x^2 - 2 = 0\}$
(στ) $-3 \in \{a \in \mathbb{N} \mid a > 2\}$
(ζ) $\{1\} \in \{1, 2, 3\}$
(η) $\{1\} \subseteq \{1, 2, 3\}$
(θ) $1 \subseteq \{1, 2, 3\}$
(ι) $\{1, 2\} \subseteq \{1, \{2\}\}$
(ια) $\{\{2\}\} \in \{1, \{2\}\}$
(ιβ) $\{\{2\}\} \subseteq \{1, \{2\}\}$
(ιγ) $\varnothing \subseteq \varnothing$
(ιδ) $\varnothing \in \varnothing$
(ιε) $\varnothing \in \{\varnothing\}$
(ιστ) $\varnothing \subseteq \{\varnothing\}$.

2. Προσδιορίστε τα παρακάτω σύνολα:
(α) $A \cup \{A\}$, όπου $A = \{1, 2, 3\}$.
(β) $\varnothing \cup \{\varnothing\}$.
(γ) $\varnothing \cap \{\varnothing\}$.

3. Ποιά από τα παρακάτω σύνολα είναι ίσα;
$A = \{-1, 1, 2\}$.
$B = \{-1, 2, 1, 2\}$.
$C = \{n \in \mathbb{Z} \mid |n| \leqslant 2 \text{ και } n \neq 0\}$.
$D = \{-2, 2\} \cup \{1, -1\}$.

4. Αποδείξτε ότι, αν A, B, C είναι σύνολα, τότε:
(α) $A \cup \varnothing = A$ και $A \cap \varnothing = \varnothing$.
(β) $A \cup A = A$ και $A \cap A = A$.
(γ) $A \cup B = B \cup A$ και $A \cap B = B \cap A$.
(δ) $(A \cup B) \cup C = A \cup (B \cup C)$ και $(A \cap B) \cap C = A \cap (B \cap C)$.

5. Δίνονται τα σύνολα $A = \{1, 2, 3\}$ και $B = \{1, 5, 6, 7\}$. Βρείτε τα σύνολα $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$ και $(A \cup B) \setminus (A \cap B)$.

6. Αν $V = \{a, f, X\}$ και $W = \{1, f, \varnothing, \{\alpha\}\}$, βρείτε τα $V \setminus W$ και $W \setminus V$.

7. Αν $A = \{a, b, \{a, c\}, \varnothing\}$, βρείτε τα σύνολα:

$$A \setminus \{a\}, \quad A \setminus \varnothing, \quad A \setminus \{a, c\}, \quad A \setminus \{\{a, c\}\}, \quad A \triangle \{a, c\}, \quad \{a\} \setminus A.$$

8. Έστω $A = [2, 4]$, $B = (1, 3]$ και $C = [0, 5)$. Βρείτε τα σύνολα

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

9. Δίνονται τα σύνολα:

G = $\{n \in \mathbb{Z} \mid n = 2m$ για κάποιον $m \in \mathbb{Z}\}$
H = $\{n \in \mathbb{Z} \mid n = 3m$ για κάποιον $m \in \mathbb{Z}\}$
I = $\{n \in \mathbb{Z} \mid n^2$ περιττός$\}$
H = $\{n \in \mathbb{Z} \mid 0 \leqslant n \leqslant 10\}$.
Βρείτε τα σύνολα

$$G \cup I, G \cap I, G \cap H, J \setminus G, I \setminus H, J \cap (G \setminus H).$$

10. Δείξτε ότι η συμμετρική διαφορά έχει την προσεταιριστική ιδιότητα

$$(A \triangle B) \triangle C = A \triangle (B \triangle C).$$

11. Αποδείξτε ότι:
(α) $(A \triangle B) \triangle A = B$.
(β) $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$.

12. (α) Χρησιμοποιώντας την προηγούμενη άσκηση, δείξτε ότι: αν τα σύνολα A, B και C ικανοποιούν την $A \triangle B = A \triangle C$, τότε $B = C$.

(β) Δείξτε ότι: αν A και B είναι δύο σύνολα, τότε υπάρχει μοναδικό σύνολο X ώστε $A \triangle X = B$ (η «εξίσωση» $A \triangle X = B$ έχει μοναδική λύση).

13. Αν $X = X_1 \cup X_2$, δείξτε ότι

$$\bigcup X = \left(\bigcup X_1\right) \cup \left(\bigcup X_2\right).$$

14. Δίνονται τα σύνολα $A = \{\varnothing, \{\varnothing\}\}$ και $B = \{a, \{a\}, b\}$. Εξετάστε αν οι παρακάτω προτάσεις είναι αληθείς ή ψευδείς.
(α) $\varnothing \in \mathcal{P}(A)$.
(β) $\varnothing \subseteq \mathcal{P}(A)$.
(γ) $\{\varnothing\} \in \mathcal{P}(A)$.
(δ) $\{\{a\}\} \in \mathcal{P}(B)$.
(ε) $\{\{a\}\} \subseteq \mathcal{P}(B)$.
(στ) $\{\{a\}, b\} \subseteq \mathcal{P}(B)$.
(ζ) $\{\{a\}, \{\{a\}\}\} \subseteq \mathcal{P}(B)$.

15. Εξετάστε αν οι παρακάτω προτάσεις είναι αληθείς ή ψευδείς. Στην πρώτη περίπτωση δώστε απόδειξη, ενώ στην δεύτερη δώστε αντιπαράδειγμα.
(α) Αν A, B, C είναι σύνολα με $A \in B$ και $B \subseteq C$ τότε $A \in C$.
(β) Αν A, B, C είναι σύνολα με $A \in B$ και $B \subseteq C$ τότε $A \subseteq C$.

(γ) Αν A, B, C είναι σύνολα με $A \subseteq B$ και $B \in C$ τότε $A \subseteq C$.
(δ) Αν A, B, C είναι σύνολα με $A \in B$ και $B \in C$ τότε $A \in C$.

16. Βρείτε τα $\mathcal{P}(\varnothing)$, $\mathcal{P}(\mathcal{P}(\varnothing))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\varnothing)))$.

14. Αν A και B είναι δύο σύνολα, δείξτε ότι:
(α) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.
(β) $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$ αν και μόνο αν $A \subseteq B$ ή $B \subseteq A$.
(γ) $\mathcal{P}(A \setminus B) \subseteq (\mathcal{P}(A) \setminus \mathcal{P}(B)) \cup \{\varnothing\}$.

17. Δίνονται: ένα σύνολο X και ένα υποσύνολο $A \subseteq X$. Αν $Z = X \cup \mathcal{P}(X)$, δείξτε ότι $A \subseteq Z$ και $A \in Z$.

18. Δίνεται ένα σύνολο A με n στοιχεία. Πόσα στοιχεία έχει το δυναμοσύνολο $\mathcal{P}(A)$ του A;

19. Δείξτε ότι δεν υπάρχει σύνολο X με την ιδιότητα $\mathcal{P}(X) \subseteq X$. [*Υπόδειξη:* Θεωρώντας το σύνολο των υποσυνόλων Y του X για τα οποία $Y \notin Y$ θα οδηγηθείτε σε αντίφαση.]

20. Αν A και B είναι πεπερασμένα σύνολα και $|X|$ είναι το πλήθος των στοιχείων ενός συνόλου X, δείξτε ότι

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Σχεδιάστε κατάλληλο διάγραμμα Venn.

21. Αν A, B και C είναι πεπερασμένα σύνολα και $|X|$ είναι το πλήθος των στοιχείων ενός συνόλου X, δείξτε ότι

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|.$$

Σχεδιάστε κατάλληλο διάγραμμα Venn.

22. Για κάθε μία από τις παρακάτω προτάσεις, εξετάστε αν προκύπτει αληθής ή ψευδής πρόταση αν στη θέση του X βάλουμε καθένα από τα σύνολα $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ή $\mathbb{R}$:
(α) $\{x \in X \mid x^3 = 5\} \neq \varnothing$.
(β) $\{x \in X \mid -1 \leqslant x \leqslant 1\} = \{1\}$.
(γ) $\{x \in X \mid 2 < x^2 < 5\} \setminus \{x \in X \mid x > 0\} = \{-2\}$.
(δ) $\{x \in X \mid 1 < x \leqslant 4\} = \{x \in X \mid x^2 = 4\} \cup \{3, 4\}$.
(ε) $\{x \in X \mid 4x^2 = 1\} \setminus \{x \in X \mid x < 0\} = \{x \in X \mid 5x^2 = 3\} \cup \{x \in X \mid 2x = 1\} \neq \varnothing$.

23. Η εξίσωση $x + y = z$ έχει πολλές λύσεις $x, y, z \in \mathbb{N}$. Η εξίσωση $x^2 + y^2 = z^2$ έχει κι αυτή λύσεις στο $\mathbb{N}$ (για παράδειγμα, $x = 3$, $y = 4$, $z = 5$). Ορίζουμε

$$F = \{n \in \mathbb{N} \mid \text{υπάρχουν } x, y, z \in \mathbb{N} \text{ ώστε } x^n + y^n = z^n\}.$$

Πώς θα μπορούσατε να αποδείξετε ότι $F = \{1, 2\}$;

Κεφάλαιο 2

Διμελείς σχέσεις

2.1 Καρτεσιανό γινόμενο

Όπως έχουμε ήδη σημειώσει $\{a, b\} = \{b, a\}$. Σε κάποιες περιπτώσεις θέλουμε να αποκτήσει σημασία η σειρά με την οποία γράφονται τα στοιχεία ενός συνόλου. Για να μην προκύψουν ερωτήσεις της μορφής «τι είναι η σειρά;», τι θα πει γράφω «πρώτα» το a και «μετά» το b, κλπ., κάτι που μπορεί να μας οδηγήσει σε μια ατέλειωτη σειρά ορισμών αμφίβολης ακρίβειας, δίνουμε τον ακόλουθο ορισμό:

Ορισμός 2.1.1 (Kuratowski)**.** Ονομάζουμε **διατεταγμένο ζεύγος** των a, b (με πρώτο το a και δεύτερο το b) το σύνολο

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

Πρόταση 2.1.2. *Για τα διατεταγμένα ζεύγη (a, b) και (c, d) ισχύει η ισοδυναμία*

$$(a, b) = (c, d) \quad \textit{αν και μόνο αν} \quad a = c \ \textit{ και } \ b = d.$$

Απόδειξη. ($\Longrightarrow$) Η ισότητα $(a, b) = (c, d)$ ισοδυναμεί με την ισότητα των συνόλων

$$\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}, \tag{2.1.1}$$

απ¨ όπου προκύπτει ότι $\{a\} \in \{\{c\}, \{c, d\}\}$. Έχουμε δύο περιπτώσεις:

(i) $\{a\} = \{c\}$, άρα και $a = c$. Τότε η (2.1.1) γίνεται $\{\{a\}, \{a, b\}\} = \{\{a\}, \{a, d\}\}$, οπότε έχουμε τις υποπεριπτώσεις:

(α') $\{a, d\} = \{a\}$, δηλαδή $a = d$. Τότε

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

άρα $\{a,b\} = \{a\}$ και $a = b$, απ¨ όπου έπεται ότι $b = d$, είτε

(β΄) $\{a,d\} = \{a,b\}$. Από την τελευταία ισότητα παίρνουμε είτε $d = a$ οπότε $\{a,a\} = \{a,b\}$ και $a = b = d$, είτε $b = d$.

(ii) $\{a\} = \{c,d\}$, άρα $a = c = d$. Τότε η (2.1.1) γίνεται

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

απ΄ όπου έχουμε ότι $\{a,b\} = \{a\}$ και $b = a = d$.

($\Longleftarrow$) Προφανές. □

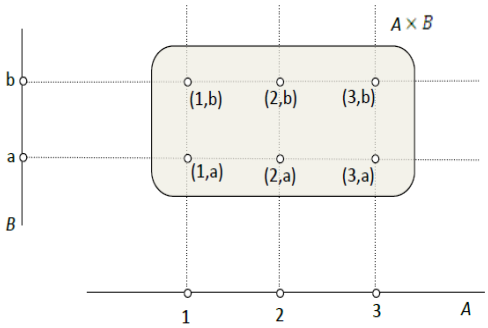
Ορισμός 2.1.3. Έστω A, B σύνολα. Ονομάζουμε **καρτεσιανό γινόμενο** των A και B το σύνολο

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

Ένας τρόπος να παραστήσουμε γραφικά το καρτεσιανό γινόμενο $A \times B$ των συνόλων A και B είναι να παραστήσουμε τα σύνολα A και B σαν δύο κάθετα ευθύγραμμα τμήματα πάνω στα οποία σημειώνονται τα στοιχεία τους, και το $A \times B$ σαν παραλληλόγραμμο, όπως φαίνεται στο επόμενο παράδειγμα:

$$\begin{aligned} A &= \{1,2,3\} \\ B &= \{a,b\} \\ A \times B &= \{(1,a),(2,a),(3,a),(1,b),2,b),(3,b)\} \end{aligned}$$

και το αντίστοιχο διάγραμμα είναι



Παρατηρούμε ότι

(α) Για κάθε σύνολο A ισχύει $A \times \varnothing = \varnothing \times A = \varnothing$.

(β) Για τυχόντα σύνολα A, B, C, εν γένει

$$A \times B \neq B \times A,$$
$$A \times (B \times C) \neq (A \times B) \times C.$$

Πρόταση 2.1.4. *Έστω A, B, C σύνολα. Τότε ισχύουν οι ισότητες:*

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

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

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

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

Απόδειξη. Αποδεικνύουμε δύο από τις ισότητες, οι υπόλοιπες αποδεικνύονται ανάλογα. Σε ό,τι ακολουθεί το «X ή Y» σημαίνει «είτε το X είτε το Y». Για την (i) έχουμε:

$$\begin{aligned}(x,y) \in A \times (B \cup C) &\iff x \in A \text{ και } y \in B \cup C \\ &\iff x \in A \text{ και } (y \in B \text{ ή } y \in C) \\ &\iff (x \in A \text{ και } y \in B) \text{ ή } (x \in A \text{ και } y \in C) \\ &\iff (x,y) \in A \times B \text{ ή } (x,y) \in A \times C \\ &\iff (x,y) \in (A \times B) \cup (A \times C).\end{aligned}$$

Για την (iv) έχουμε:

$$\begin{aligned}(x,y) \in (A \cap B) \times C &\iff x \in (A \cap B) \text{ και } y \in C \\ &\iff (x \in A \text{ και } x \in B) \text{ και } y \in C \\ &\iff (x \in A \text{ και } y \in C) \text{ και } (x \in B \text{ και } y \in C) \\ &\iff (x,y) \in A \times C \text{ και } (x,y) \in B \times C \\ &\iff (x,y) \in (A \times C) \cap (B \times C).\end{aligned}$$

□

Πρόταση 2.1.5. *Έστω A, B, C, D σύνολα. Τότε*

(i) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

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

Απόδειξη. (i) Παρατηρούμε ότι

$$\begin{aligned}(x,y) \in (A \times B) \cap (C \times D) &\iff (x,y) \in (A \times B) \text{ και } (x,y) \in (C \times D)\\ &\iff (x \in A \text{ και } y \in B) \text{ και } (x \in C \text{ και } y \in D)\\ &\iff (x \in A \text{ και } x \in C) \text{ και } (y \in B \text{ και } y \in D)\\ &\iff x \in A \cap C \text{ και } y \in B \cap D\\ &\iff (x,y) \in (A \cap C) \times (B \cap D).\end{aligned}$$

Για την (ii) παρατηρούμε ότι για κάθε $(x,y) \in (A \times B) \cup (C \times D)$ έχουμε $(x,y) \in (A \times B)$ ή $(x,y) \in (C \times D)$. Τότε,

- αν $(x,y) \in (A \times B)$, τότε $x \in A$ και $y \in B$, άρα $x \in A \cup C$ και $y \in B \cup D$, επομένως $(x,y) \in (A \cup C) \times (B \cup D)$.

- αν $(x,y) \in (C \times D)$, τότε $x \in C$ και $y \in D$, άρα $x \in A \cup C$ και $y \in B \cup D$, επομένως $(x,y) \in (A \cup C) \times (B \cup D)$.

Σε κάθε περίπτωση, από την $(x,y) \in (A \cup C) \times (B \cup D)$ συμπεραίνουμε ότι $(x,y) \in (A \cup C) \times (B \cup D)$. □

Η τελευταία σχέση εν γένει δεν είναι ισότητα. Για παράδειγμα, ας θεωρήσουμε τα σύνολα $A = \{a\}$, $B = \{b\}$, $C = \{c\}$ και $D = \{d\}$, όπου $a \neq c$ και $b \neq d$. Τότε

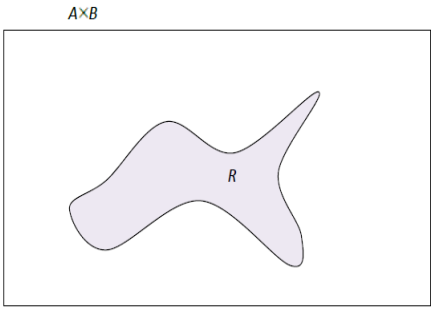
$$(A \times B) \cup (C \times D) = \{(a,b)\} \cup \{(c,d)\} = \{(a,b),(c,d)\},$$

ενώ

$$(A \cup C) \times (B \cup D) = \{a,c\} \times \{b,d\} = \{(a,b),(a,d),(c,b),(c,d)\}.$$

2.2 Διμελείς σχέσεις

Ορισμός 2.2.1. Έστω A, B σύνολα. Ονομάζουμε **(διμελή) σχέση** από το A στο B κάθε υποσύνολο R του $A \times B$.



Συμβολικά γράφουμε $x\,R\,y$ αντί για $(x,y)\in R$.

Παραδείγματα 2.2.2. (α) Έστω $A=B=X$. Η *σχέση της ισότητας* (από το X στο X) είναι το σύνολο

$$R=\{(x,y)\in X\times X : x=y\}=\{(x,x) : x\in X\}\subseteq X\times X.$$

Τότε

$$x\,R\,y \iff x=y.$$

Το ανωτέρω σύνολο $R=\{(x,x) : x\in X\}$ συχνά συμβολίζεται με Δ_X και ονομάζεται **διαγώνιος** του X.

(β) Έστω X σύνολο και $A=B=\mathcal{P}(X)$. Η *σχέση του εγκλεισμού* R από το $\mathcal{P}(X)$ στο $\mathcal{P}(X)$ είναι το σύνολο

$$R=\{(A,B) : A,B\subseteq X \text{ με } A\subseteq B\}\subseteq \mathcal{P}(X)\times\mathcal{P}(X).$$

Τότε

$$(A,B)\in R \iff A\subseteq B$$

(γ) Έστω A σύνολο και $B=\mathcal{P}(A)$. Θέτουμε

$$R=\{(x,C)\in A\times\mathcal{P}(A) : x\in C\}\subseteq A\times\mathcal{P}(A).$$

Τότε

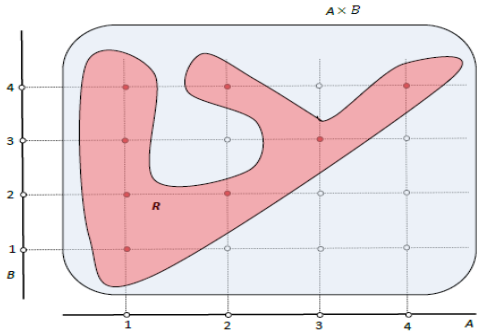
$$x\,R\,C \iff x\in C.$$

(δ) Έστω $A=\{1,2,3,4\}$. Θεωρούμε την σχέση $R\subseteq A\times A$ με

$$x\,R\,y \iff x\mid y \iff \frac{y}{x}\in\mathbb{Z}.$$

Τότε

$$R=\{(1,1),(1,2),(1,3),(1,4),(2,2),(2,4),(3,3),(4,4)\}.$$



Ορισμός 2.2.3. (i) Έστω $R \subseteq A \times B$ μια διμελής σχέση από το A στο B. Ονομάζουμε **αντίστροφη** της R την διμελή σχέση από το B στο A

$$R^{-1} = \{(b, a) \in B \times A : (a, b) \in R\}.$$

Παρατηρούμε ότι ισχύει η ισοδυναμία

$$(a, b) \in R \iff (b, a) \in R^{-1}.$$

(ii) Έστω $R \subseteq A \times B$, $X \subseteq A$ και $Y \subseteq B$. Ονομάζουμε **περιορισμό** της R στο $X \times Y$ την σχέση από το X στο Y

$$R|_{X \times Y} = \{(x, y) \in R : x \in X \text{ και } y \in Y\} = R \cap (X \times Y).$$

2.3 Σχέσεις ισοδυναμίας

Ορισμός 2.3.1. Έστω A ένα σύνολο. Μια διμελής σχέση $R \subseteq A \times A$ λέγεται **σχέση ισοδυναμίας** αν είναι

(i) *ανακλαστική* ή *αυτοπαθής*, δηλαδή $x \, R \, x$, για κάθε $x \in A$.

(ii) *συμμετρική*, δηλαδή ισχύει η συνεπαγωγή $x \, R \, y \Longrightarrow y \, R \, x$.

(iii) *μεταβατική*, δηλαδή ισχύει η συνεπαγωγή $x \, R \, y$ και $y \, R \, z \Longrightarrow x \, R \, z$.

Παρατήρηση 2.3.2. Για μια διμελή σχέση R από το A στο A, εύκολα βλέπουμε ότι

$$\begin{aligned} R \text{ ανακλαστική} &\iff \text{για κάθε } x \in A : (x, x) \in R \\ &\iff \Delta_A \subseteq R \end{aligned}$$

και ότι

$$R \text{ συμμετρική} \iff R = R^{-1}. \tag{2.3.1}$$

Στον παρακάτω πίνακα καταγράφονται διάφορες διμελείς σχέσεις από το $\mathbb{R}$ στο $\mathbb{R}$ και σημειώνονται οι ιδιότητες που έχουν.

Σχέση	Αυτοπαθής	Συμμετρική	Μεταβατική	Σχέση ισοδυναμίας
$x = y$	+	+	+	+
$x < y$	-	-	+	-
$x \geqslant y$	+	-	+	-
$\lvert x - y \rvert \leqslant 1$	+	+	-	-
$x - y \in \mathbb{Q}$	+	+	+	+
$x - y \notin \mathbb{Q}$	-	+	-	-
$x - y = 3$	-	-	-	-
$y = x^2$	-	-	-	-

Υπενθυμίζουμε και μερικά παραδείγματα σχέσεων ισοδυναμίας από την Ευκλείδεια γεωμετρία:

(α) Στο σύνολο των ευθειών ενός επιπέδου, η σχέση παραλληλίας ή ταύτισης.

(β) Στο σύνολο των τριγώνων ενός επιπέδου, η σχέση της ομοιότητας.

(γ) Στο σύνολο των κύκλων ενός επιπέδου η σχέση του να είναι δύο κύκλοι ομόκεντροι.

Ορισμός 2.3.3. Έστω R μια σχέση ισοδυναμίας στο X και $x \in X$. Ονομάζουμε κλάση ισοδυναμίας του x (ως προς την R) το σύνολο

$$[x] = \{y \in X : y \, R \, x\}.$$

Λήμμα 2.3.4. *Έστω R μια σχέση ισοδυναμίας στο X και $x, y \in X$. Τότε*

$$x \, R \, y \iff [x] = [y].$$

Απόδειξη. Έστω $x \, R \, y$. Για να δείξουμε ότι $[x] = [y]$, θα δείξουμε ότι $[x] \subseteq [y]$ και $[y] \subseteq [x]$. Πράγματι, έστω $w \in [x]$. Τότε $w \, R \, x$. Επειδή $x \, R \, y$ και η R είναι μεταβατική, παίρνουμε $w \, R \, y$, άρα $w \in [y]$. Ο εγκλεισμός $[y] \subseteq [x]$ αποδεικνύεται ανάλογα.

Αντίστροφα, έστω $[x] = [y]$. Λόγω της ανακλαστικής ιδιότητας της R, έχουμε $x \in [x]$ και $y \in [x] = [y]$. Από την $y \in [x]$ προκύπτει ότι $x \, R \, y$. □

Ορισμός 2.3.5. Έστω X ένα σύνολο. Μια **διαμέριση** του X είναι ένα σύνολο $\mathcal{D} \subseteq \mathcal{P}(X)$ με τις ακόλουθες ιδιότητες:

(i) Για κάθε $A \in \mathcal{D}$, $A \neq \varnothing$.

(ii) Αν $A, B \in \mathcal{D}$ με $A \cap B \neq \varnothing$, τότε $A = B$.

(iii) $\bigcup_{A \in \mathcal{D}} A = X$.

Θεώρημα 2.3.6. *Έστω $X \neq \varnothing$ ένα σύνολο. Τότε κάθε σχέση ισοδυναμίας στο X ορίζει μια διαμέριση του X και αντίστροφα.*

Απόδειξη. Έστω R μια σχέση ισοδυναμίας στο X. Συμβολίζουμε με $\mathcal{D}$ το σύνολο των κλάσεων ισοδυναμίας, δηλαδή

$$\mathcal{D} = \{[x] : x \in X\}.$$

Τότε το $\mathcal{D}$ είναι διαμέριση του X. Πράγματι,

(i) Για κάθε $[x] \in \mathcal{D}$ έχουμε ότι $x \in [x]$, άρα $[x] \neq \varnothing$.

(ii) Έστω $[x], [y] \in \mathcal{D}$ με $[x] \cap [y] \neq \varnothing$. Τότε

$$\begin{aligned} [x] \cap [y] \neq \varnothing &\implies \text{υπάρχει } z \in [x] \cap [y] \\ &\implies \text{υπάρχει } z \in X : x\,R\,z \text{ και } z\,R\,y \\ &\implies x\,R\,y. \end{aligned}$$

Από το Λήμμα 2.3.4 έπεται τώρα ότι $[x] = [y]$.

(iii) Αφού $[x] \subseteq X$, για κάθε $[x] \in \mathcal{D}$, έχουμε και για την ένωσή τους ότι

$$\bigcup_{[x] \in \mathcal{D}[x]} \subseteq X.$$

Δείχνουμε και τον αντίστροφο εγκλεισμό: Έστω $x_0 \in X$. Τότε $x_0 \in [x_0]$, άρα $x_0 \in \bigcup_{[x] \in \mathcal{D}} [x]$, δηλαδή

$$X \subseteq \bigcup_{[x] \in \mathcal{D}} [x].$$

Δείξαμε ότι κάθε σχέση ισοδυναμίας στο X διαμερίζει το X στις αντίστοιχες κλάσεις ισοδυναμίας.

Αντίστροφα, έστω $\mathcal{D}$ μια διαμέριση του X. Ορίζουμε στο X την ακόλουθη διμελή σχέση R:

$$x\,R\,y \iff \text{υπάρχει } A \in \mathcal{D} : x, y \in A.$$

Η R είναι σχέση ισοδυναμίας:

(i) Έστω $x \in X$. Επειδή $X = \bigcup_{A\in\mathcal{D}} A$, υπάρχει $A \in \mathcal{D}$ με $x \in A$, άρα $x, x \in A$ και $x\,R\,x$, δηλαδή η R είναι ανακλαστική.

(ii) Αν $x\,R\,y$, τότε υπάρχει $A \in \mathcal{D}$ με $x, y \in A$, άρα και $y, x \in A$, δηλαδή $y\,R\,x$ και η R είναι συμμετρική.

(iii) Έστω $x, y, z \in X$ με $x\,R\,y$ και $y\,R\,z$. Τότε υπάρχουν $A, B \in \mathcal{D}$ με $x, y \in A$ και $y, z \in B$. Επομένως $y \in A \cap B \neq \varnothing$ άρα $A = B$, οπότε $x, z \in A = B$, δηλαδή $x\,R\,z$ και η R είναι μεταβατική.

□

2.4 Ο δακτύλιος $\mathbb{Z}_m$

Θεωρούμε ένα $m \in \mathbb{N}$, σταθερό, και ορίζουμε την διμελή σχέση $R \subseteq \mathbb{Z} \times \mathbb{Z}$ με

$$\begin{aligned} x\,R\,y &\iff \text{ο } x - y \text{ είναι ακέραιο πολλαπλάσιο του } m \\ &\iff \text{υπάρχει } k \in \mathbb{Z} \,:\, x - y = km. \end{aligned}$$

Η σχέση R ονομάζεται *ισοτιμία modulo* m και συνήθως συμβολίζεται με $\equiv \pmod m$, δηλαδή

$$x \equiv y \,(\mathrm{mod} m) \iff \text{υπάρχει } k \in \mathbb{Z} \,:\, x - y = km.$$

Λήμμα 2.4.1. *Η ανωτέρω σχέση R είναι σχέση ισοδυναμίας.*

Απόδειξη. (i) Για κάθε $x \in \mathbb{Z}$, υπάρχει $k = 0 \in \mathbb{Z}$ με

$$x - x = 0 = 0m,$$

άρα $x\,R\,x$ και η R είναι ανακλαστική.

(ii) Ισχύουν οι συνεπαγωγές

$$\begin{aligned} x\,R\,y &\implies \text{υπάρχει } k \in \mathbb{Z} \,:\, x - y = km \\ &\implies \text{υπάρχει } -k \in \mathbb{Z} \,:\, y - x = (-k)m \\ &\implies y\,R\,x \end{aligned}$$

άρα η R είναι συμμετρική.

(iii) Έστω $x\,R\,y$ και $y\,R\,z$. Τότε υπάρχουν $k, \lambda \in \mathbb{Z}$ με

$$x - y = km \text{ και } y - z = \lambda m.$$

Προσθέτοντας τις ισότητες κατά μέλη παίρνουμε

$$x - z = (k + \lambda)m$$

με $k + \lambda \in \mathbb{Z}$, άρα η R είναι μεταβατική. □

Θα μελετήσουμε τώρα πώς η δεδομένη σχέση ισοδυναμίας διαμερίζει το $\mathbb{Z}$ σε κλάσεις ισοδυναμίας. Έστω $x_1, x_2 \in \mathbb{Z}$ με $x_1 \, R \, x_2$. Θεωρώντας την διαίρεση των x, y με m, γνωρίζουμε ότι υπάρχουν μονοσήμαντα ορισμένοι $k_1, k_2, \upsilon_1, \upsilon_2 \in \mathbb{Z}$ με

$$x_i = k_i m + \upsilon_i, \quad i = 1, 2$$

και

$$0 \leqslant \upsilon_1, \upsilon_2 \leqslant m - 1.$$

Η σχέση $x_1 \, R \, x_2$ σημαίνει ότι η διαφορά

$$x_1 - x_2 = (k_1 - k_2)m + (\upsilon_1 - \upsilon_2)$$

είναι ακέραιο πολλαπλάσιο του m. Άρα και η διαφορά $\upsilon_1 - \upsilon_2$ είναι ακέραιο πολλαπλάσιο του m. Όμως οι ανισότητες $0 \leqslant \upsilon_1, \upsilon_2 \leqslant m - 1$ μας δίνουν

$$\left.\begin{array}{rcccl} 0 & \leqslant & \upsilon_1 & \leqslant & m-1 \\ -(m-1) & \leqslant & -\upsilon_2 & \leqslant & 0 \end{array}\right\} \implies -(m-1) \leqslant \upsilon_1 - \upsilon_2 \leqslant m - 1$$

και το μοναδικό ακέραιο πολλαπλάσιο του m μέσα στο ανωτέρω διάστημα είναι το 0. Άρα $\upsilon_1 = \upsilon_2$. Αποδείξαμε λοιπόν το επόμενο:

Λήμμα 2.4.2. *Έστω $x_1, x_2 \in \mathbb{Z}$. Τότε*

$$x_1 \equiv x_2 \,(\mathrm{mod} m) \iff x_1, x_2 \text{ διαιρούμενοι με } m \text{ δίνουν το ίδιο υπόλοιπο.}$$

Σαν αποτέλεσμα του προηγούμενου λήμματος, έχουμε ότι υπάρχουν ακριβώς τόσες κλάσεις ισοδυναμίας, όσα είναι τα δυνατά υπόλοιπα. Δηλαδή, το $\mathbb{Z}$ διαμερίζεται στις εξής (m το πλήθος) κλάσεις ισοδυναμίας:

$$\begin{aligned} [0]_m &= \{km : k \in \mathbb{Z}\} \\ [1]_m &= \{km + 1 : k \in \mathbb{Z}\} \\ [2]_m &= \{km + 2 : k \in \mathbb{Z}\} \\ &\vdots \\ [m-1]_m &= \{km + (m-1) : k \in \mathbb{Z}\} \end{aligned}$$

Συμβολίζουμε με $\mathbb{Z}_m$ το σύνολο των κλάσεων ισοδυναμίας, δηλαδή

$$\mathbb{Z}_m = \big\{[0]_m, [1]_m, \dots [m-1]_m\big\}.$$

Ορισμός 2.4.3. Στο $\mathbb{Z}_m$ ορίζουμε μια πράξη που ονομάζουμε **πρόσθεση του** $\mathbb{Z}_m$, ως εξής:

$$+ : \mathbb{Z}_m \times \mathbb{Z}_m \longrightarrow \mathbb{Z}_m : ([x]_m, [y]_m) \longmapsto [x]_m + [y]_m := [x+y]_m.$$

Παρατηρούμε ότι η πρόσθεση του $\mathbb{Z}_m$ είναι *καλά ορισμένη*, δηλαδή αν $[x]_m = [x']_m$ και $[y]_m = [y']_m$, τότε $[x+y]_m = [x'+y']_m$. Πράγματι:

$$\left.\begin{array}{lllll} [x]_m = [x']_m & \Longrightarrow & x \equiv x' \,(\mathrm{mod} m) & \Longrightarrow & \text{υπάρχει } k \in \mathbb{Z} : x - x' = km \\ [y]_m = [y']_m & \Longrightarrow & y \equiv y' \,(\mathrm{mod} m) & \Longrightarrow & \text{υπάρχει } \lambda \in \mathbb{Z} : y - y' = \lambda m \end{array}\right\} \Longrightarrow$$
$$(x+y) - (x'-y') = (k+\lambda)m,\ k+\lambda \in \mathbb{Z}$$
$$\Longrightarrow \ [x+y]_m = [x'+y']_m.$$

Ακόμη, η πρόσθεση έχει τις παρακάτω ιδιότητες:

(A1) Είναι *μεταθετική*: Πράγματι, για κάθε $[x]_m, [y]_m \in \mathbb{Z}_m$, έχουμε

$$[x]_m + [y]_m = [x+y]_m = [y+x]_m = [y]_m + [x]_m.$$

(A2) Είναι *προσεταιριστική*: Για κάθε $[x]_m, [y]_m, [z]_m \in \mathbb{Z}_m$ ισχύει

$$\begin{aligned}[x]_m + ([y]_m + [z]_m) &= [x]_m + [y+z]_m = [x + (y+z)]_m = [(x+y)+z]_m \\ &= [x+y]_m + [z]_m = ([x]_m + [y]_m) + [z]_m.\end{aligned}$$

(A3) *Υπάρχει ουδέτερο στοιχείο*, η κλάση $[0]_m \in \mathbb{Z}_m$:

$$[x]_m + [0]_m = [x+0]_m = [x]_m, \quad \text{για κάθε } \ [x]_m \in \mathbb{Z}_m.$$

(A4) Κάθε $[x]_m \in \mathbb{Z}_m$ *έχει αντίθετο*, την κλάση $[-x]_m$:

$$[x]_m + [-x]_m = [x + (-x)]_m = [0]_m.$$

Οι ιδιότητες (A1)–(A4) καθιστούν το ζεύγος $(\mathbb{Z}_m, +)$ **αβελιανή/μεταθετική ομάδα**.

Ορισμός 2.4.4. Ονομάζουμε **πολλαπλασιασμό στο** $\mathbb{Z}_m$ την πράξη

$$\cdot : \mathbb{Z}_m \times \mathbb{Z}_m \longrightarrow \mathbb{Z}_m : ([x]_m, [y]_m) \longmapsto [x]_m \cdot [y]_m := [xy]_m.$$

Όπως προηγουμένως, ο πολλαπλασιασμός στο $\mathbb{Z}_m$ είναι *καλά ορισμένος*, δηλαδή αν $[x]_m = [x']_m$ και $[y]_m = [y']_m$, τότε $[xy]_m = [x'y']_m$. Πράγματι, από την ισότητα $[x]_m = [x']_m$ προκύπτει ότι τα x και x' διαιρούμενα με m δίνουν το ίδιο υπόλοιπο υ_x. Άρα, $x = km + \upsilon_x$ και $x' = k'm + \upsilon_x$, με $k, k' \in \mathbb{Z}$. Παρόμοια από την ισότητα $[y]_m = [y']_m$ παίρνουμε ότι $y = \lambda m + \upsilon_y$ και $y' = \lambda' m + \upsilon_y$. Άρα

$$\begin{aligned} xy - x'y' &= (km + \upsilon_x)(\lambda m + \upsilon_y) - (k'm + \upsilon_x)(\lambda' m + \upsilon_y) \\ &= (k\lambda m^2 + km\upsilon_y + \lambda m\upsilon_x + \upsilon_x\upsilon_y) \\ &\quad - (k'\lambda' m^2 + k'm\upsilon_y + \lambda' m\upsilon_x + \upsilon_x\upsilon_y) \\ &= \big((k\lambda m + k\upsilon_y + \lambda\upsilon_x) - (k'\lambda' m + k'\upsilon_y + \lambda'\upsilon_x)\big)m \end{aligned}$$

άρα $[xy]_m = [x'y']_m$.

Ακόμη, ο πολλαπλασιασμός έχει τις παρακάτω ιδιότητες:

(Β1) Είναι *μεταθετικός*: Για κάθε $[x]_m, [y]_m \in \mathbb{Z}_m$, έχουμε

$$[x]_m \cdot [y]_m = [xy]_m = [yx]_m = [y]_m \cdot [x]_m.$$

(Β2) Είναι *προσεταιριστικός*: Για κάθε $[x]_m, [y]_m, [z]_m \in \mathbb{Z}_m$ είναι:

$$\begin{aligned} [x]_m \cdot ([y]_m \cdot [z]_m) &= [x]_m \cdot [yz]_m = [x(yz)]_m = [(xy)z]_m \\ &= [xy]_m \cdot [z]_m = ([x]_m \cdot [y]_m) \cdot [z]_m. \end{aligned}$$

(Β3) *Υπάρχει ουδέτερο στοιχείο*, η κλάση $[1]_m \in \mathbb{Z}_m$:

$$[1]_m \cdot [x]_m = [1x]_m = [x]_m, \quad \text{για κάθε } \ [x]_m \in \mathbb{Z}_m.$$

Τέλος, πρέπει να παρατηρήσουμε ότι:

(Γ1) Η πρόσθεση και ο πολλαπλασιασμός στο $\mathbb{Z}_m$ *συνδέονται με την επιμεριστική ιδιότητα*: Για κάθε $[x]_m, [y]_m, [x]_m \in \mathbb{Z}_m$, ισχύει

$$\begin{aligned} [x]_m \cdot ([y]_m + [z]_m) &= [x]_m \cdot [y + z]_m = [x(y + z)]_m = [xy + xz]_m \\ &= [xy]_m + [xz]_m = [x]_m \cdot [y]_m + [x]_m \cdot [z]_m. \end{aligned}$$

Οι ιδιότητες (Α1)–(Α4) μαζί με τις (Β1)–(Β3) και την (Γ1) καθιστούν την τριάδα $(\mathbb{Z}_m, +, \cdot)$ **μεταθετικό δακτύλιο με μονάδα**.

Αξίζει να σημειώσουμε ότι *ο δακτύλιος* $(\mathbb{Z}_m, +, \cdot)$ *είναι σώμα, δηλαδή κάθε μη μηδενικό στοιχείο του έχει αντίστροφο, αν και μόνο αν ο* m *είναι πρώτος αριθμός.*

2.5 Σχέσεις διάταξης

Ορισμός 2.5.1. Έστω ένα σύνολο $X \neq \varnothing$. Μια σχέση $R \subseteq X \times X$ λέγεται **διάταξη**, αν είναι:

(Δ1) **ανακλαστική**, δηλαδή για κάθε $x \in X \ : \ x\,R\,x$,

(Δ2) **αντισυμμετρική**, δηλαδή $x\,R\,y$ και $y\,R\,x \implies x = y$, και

(Δ3) **μεταβατική**, δηλαδή $x\,R\,y$ και $y\,R\,z \implies x\,R\,z$.

Παραδείγματα 2.5.2. (α) Η σχέση $x \leqslant y$ στο $\mathbb{R}$.
(β) Η σχέση $A \subseteq B$ στο $\mathcal{P}(X)$.
(γ) Η σχέση $a \mid b$ στο $\mathbb{N}$.

Στο προηγούμενο Παράδειγμα (α), παρατηρούμε ότι για κάθε ζεύγος αριθμών $x, y \in \mathbb{R}$, ισχύει $x \leqslant y$ είτε $y \leqslant x$. Τα επόμενα δύο παραδείγματα δεν έχουν αυτή την ιδιότητα. Πράγματι, στο (β), αν το σύνολο X έχει δύο ή περισσότερα στοιχεία, τότε υπάρχουν $a, b \in X$ με $a \neq b$. Σε αυτή την περίπτωση είναι $\{a\}, \{b\} \in \mathcal{P}(X)$, αλλά δεν ισχύει ούτε $\{a\} \subseteq \{b\}$ ούτε $\{b\} \subseteq \{a\}$. Στο (γ), έχουμε $5 \in \mathbb{N}$ και $6 \in \mathbb{N}$ αλλά δεν ισχύει ούτε $5 \mid 6$, ούτε $6 \mid 5$.

Ορισμός 2.5.3. Μια διάταξη R στο σύνολο $X \neq \varnothing$ λέγεται **ολική** αν
(ΟΔ) για κάθε $x, y \in X \ : \ x\,R\,y$ ή $y\,R\,x$.

Σύμφωνα με τον ορισμό της διάταξης, οι σχέσεις $<$ στο $\mathbb{R}$ και $\subsetneq$ στο $\mathcal{P}(X)$ **δεν** είναι διατάξεις: δεν είναι ανακλαστικές. Επίσης, αξίζει να παρατηρήσουμε ότι η υπόθεση στην αντισυμμετρική ιδιότητα δεν ικανοποιείται ποτέ. Για να περιλάβουμε στη μελέτη μας σχέσεις όπως αυτές, δίνουμε τον επόμενο ορισμό:

Ορισμός 2.5.4. Έστω ένα σύνολο $X \neq \varnothing$. Μια σχέση $S \subseteq X \times X$ λέγεται **αυστηρή διάταξη**, αν έχει τις επόμενες ιδιότητες:

(ΑΔ1) για κάθε $x \in X \ : \ (x, x) \notin S$.

(ΑΔ2) $(x, y) \in S \ \Rightarrow \ (y, x) \notin S$.

(ΑΔ3) $x\,S\,y$ και $y\,S\,z \ \Rightarrow \ x\,S\,z$ (μεταβατικότητα).

Συμβολίζουμε με Δ_X την **διαγώνιο** του X, δηλαδή το σύνολο

$$\Delta_X = \{(x, x) : x \in X\}.$$

Τότε, για μια διάταξη R ισχύει πάντοτε $\Delta_X \subseteq R$, ενώ για μια αυστηρή διάταξη S ισχύει $S \cap \Delta_X = \varnothing$. Η παρατήρηση αυτή μας οδηγεί στην επόμενη πρόταση:

Πρόταση 2.5.5. *Έστω ένα σύνολο $X \neq \varnothing$. Τότε:*

(i) *Κάθε διάταξη $R \subseteq X \times X$ ορίζει μια αυστηρή διάταξη, την $S = R \setminus \Delta_X$.*

(ii) *Κάθε αυστηρή διάταξη $S \subseteq X \times X$ ορίζει μια διάταξη, την $R = S \cup \Delta_X$.*

Απόδειξη. (i) Έστω R μια διάταξη στο X. Ορίζουμε την σχέση $S = R \setminus \Delta_X$, δηλαδή

$$x\,S\,y \iff (x,y) \in R \setminus \Delta_X \iff x\,R\,y \text{ και } x \neq y.$$

Θα δείξουμε ότι η S είναι αυστηρή διάταξη. Πράγματι:

(ΑΔ1) Για κάθε $x \in X$ έχουμε $(x,x) \in \Delta_X$, άρα $(x,x) \notin R \setminus \Delta_X = S$.

(ΑΔ2) Με άτοπο: Έστω $x\,S\,y$ και $y\,S\,x$. Τότε ($x\,R\,y$ και $x \neq y$) και ($y\,R\,x$ και $y \neq x$). Δηλαδή, $x\,R\,y$ και $y\,R\,x$ και $x \neq y$. Αλλά από την (Δ2) της R, οι $x\,R\,y$ και $y\,R\,x$ δίνουν $x = y$, άτοπο.

(ΑΔ3) Έστω $x\,S\,y$ και $y\,S\,z$. Τότε ($x\,R\,y$ και $x \neq y$) και ($y\,R\,z$ και $y \neq z$). Από τις $x\,R\,y$ και $y\,R\,z$, λόγω της μεταβατικότητας της R, έχουμε $x\,R\,z$. Επίσης είναι $x \neq z$. Πράγματι, αν $x = z$, τότε (βλέπε τις δύο αρχικές υποθέσεις) $x\,S\,y$ και $y\,S\,x$, άτοπο. Άρα $x\,R\,z$ με $x \neq z$, δηλαδή $x\,S\,z$.

(ii) Αντίστροφα, έστω S μια αυστηρή διάταξη στο X. Ορίζουμε την σχέση $R = S \cup \Delta_X$, δηλαδή

$$x\,R\,y \iff x\,S\,y \text{ ή } x = y.$$

Θα δείξουμε ότι η R είναι διάταξη. Πράγματι:

(Δ1) Για κάθε $x \in X$, ισχύει $(x,x) \in \Delta_X$, άρα $(x,x) \in S \cup \Delta_X = R$ και η R είναι ανακλαστική.

(Δ2) Έστω $x\,R\,y$ και $y\,R\,x$. Τότε

$$\begin{aligned} x\,R\,y \text{ και } y\,R\,x &\implies (x\,S\,y \text{ ή } x = y) \text{ και } (y\,S\,x \text{ ή } y = x) \\ &\implies (x\,S\,y \text{ και } y\,S\,x) \text{ ή } x = y. \end{aligned}$$

Η πρώτη συνθήκη δεν ικανοποιείται ποτέ, άρα $x = y$ και η R είναι αντισυμμετρική.

(Δ3) Έστω $x\,R\,y$ και $y\,R\,z$. Τότε

$$\begin{aligned} x\,R\,y \text{ και } y\,R\,z &\implies (x\,S\,y \text{ ή } x=y) \text{ και } (y\,S\,z \text{ ή } y=z)\\ &\implies (x\,S\,y \text{ και } y\,S\,z) \text{ ή } (x\,S\,y \text{ και } y=z)\\ &\quad \text{ ή } (x=y \text{ και } y\,S\,z) \text{ ή } (x=y \text{ και } y=z)\\ &\implies x\,S\,z \text{ ή } x\,S\,z \text{ ή } x\,S\,z \text{ ή } x=z\\ &\implies (x,z)\in S\cup\Delta_X = R, \end{aligned}$$

και η R είναι μεταβατική.

□

Μία αυστηρή διάταξη S στο σύνολο X λέγεται *τριχοτομία*, αν για κάθε $x,y\in X$ ισχύει ένα ακριβώς από τα παρακάτω:

$$x\,S\,y \quad \text{ή} \quad y\,S\,x \quad \text{ή} \quad x=y.$$

Άσκηση: Να ελεγχθεί αν ισχύει η ισοδυναμία: η διάταξη R είναι ολική εάν και μόνο εάν η αντίστοιχη αυστηρή διάταξη S είναι τριχοτομία.

Θα κλείσουμε αυτή την παράγραφο δίνοντας ένα παράδειγμα ολικής διάταξης στους μιγαδικούς αριθμούς.

Παράδειγμα 2.5.6. Έστω $z_1=x_1+iy_1, z_2=x_2+iy_2\in\mathbb{C}$. Θεωρούμε την εξής σχέση:

$$z_1\preceq z_2 \iff (x_1<x_2) \text{ ή } (x_1=x_2 \text{ και } y_1\leqslant y_2).$$

(Δ1) Για κάθε $z=x+iy$, είναι $x=x$ και $y\leqslant y$, άρα $z\preceq z$ και η σχέση είναι ανακλαστική.

(Δ2) Για την αντισυμμετρία παρατηρούμε ότι:

$$\begin{aligned} z_1\preceq z_2 \text{ και } z_2\preceq z_1 &\implies [x_1<x_2 \text{ ή } (x_1=x_2 \text{ και } y_1\leqslant y_2)]\\ &\quad \text{και } [x_2<x_1 \text{ ή } (x_1=x_2 \text{ και } y_2\leqslant y_1)]\\ &\implies [x_1<x_2 \text{ και } x_2<x_1]\\ &\quad \text{ ή } [x_1<x_2 \text{ και } (x_1=x_2 \text{ και } y_2\leqslant y_1)]\\ &\quad \text{ ή } [(x_1=x_2 \text{ και } y_1\leqslant y_2) \text{ και } x_2<x_1]\\ &\quad \text{ ή } [(x_1=x_2 \text{ και } y_1\leqslant y_2) \text{ και } (x_1=x_2 \text{ και } y_2\leqslant y_1)] \end{aligned}$$

Οι τρεις πρώτες συνθήκες δεν ισχύουν ποτέ, άρα

$$\begin{aligned} z_1 \preceq z_2 \text{ και } z_2 \preceq z_1 &\implies (x_1 = x_2 \text{ και } y_1 \leqslant y_2) \text{ και } (x_1 = x_2 \text{ και } y_2 \leqslant y_1) \\ &\implies x_1 = x_2 \text{ και } y_1 \leqslant y_2 \text{ και } y_2 \leqslant y_1 \\ &\implies x_1 = x_2 \text{ και } y_1 = y_2 \\ &\implies z_1 = z_2. \end{aligned}$$

(Δ3) Για την μεταβατικότητα παρατηρούμε ότι

$$\begin{aligned} z_1 \preceq z_2 \text{ και } z_2 \preceq z_3 &\implies [x_1 < x_2 \text{ ή } (x_1 = x_2 \text{ και } y_1 \leqslant y_2)] \\ &\quad \text{και } [x_2 < x_3 \text{ ή } (x_2 = x_3 \text{ και } y_2 \leqslant y_3)] \\ &\implies [x_1 < x_2 \text{ και } x_2 < x_3] \\ &\quad \text{ή } [x_1 < x_2 \text{ και } (x_2 = x_3 \text{ και } y_2 \leqslant y_3)] \\ &\quad \text{ή } [(x_1 = x_2 \text{ και } y_1 \leqslant y_2) \text{ και } x_2 < x_3] \\ &\quad \text{ή } [(x_1 = x_2 \text{ και } y_1 \leqslant y_2) \text{ και } (x_2 = x_3 \text{ και } y_2 \leqslant y_3)] \end{aligned}$$

Κάθε μία από τις τρεις πρώτες συνθήκες συνεπάγεται ότι $x_1 < x_3$ ενώ η τελευταία συνεπάγεται ότι $x_1 = x_3$ και $y_1 \leqslant y_3$. Άρα

$$\begin{aligned} z_1 \preceq z_2 \text{ και } z_2 \preceq z_3 &\implies x_1 < x_3 \text{ ή } (x_1 = x_3 \text{ και } y_1 \leqslant y_3) \\ &\implies z_1 \preceq z_3. \end{aligned}$$

(ΟΔ) Τέλος, η σχέση $\preceq$ είναι ολική διάταξη στο $\mathbb{C}$: Θεωρούμε δύο τυχόντες $z_1 = x_1 + iy_1$, $z_2 = x_2 + iy_2 \in \mathbb{C}$. Για τα $x_1, x_2 \in \mathbb{R}$ ισχύει $x_1 < x_2$ ή $x_1 = x_2$ ή $x_2 < x_1$. Αν $x_1 < x_2$, τότε $z_1 \preceq z_2$. Αν $x_2 < x_1$, τότε $z_2 \preceq z_1$. Αν $x_1 = x_2$, εξετάζουμε την σχέση των y_1 και y_2: θα ισχύει $y_1 \leqslant y_2$ είτε $y_2 \leqslant y_1$. Στην πρώτη περίπτωση $z_1 \preceq z_2$ ενώ στην δεύτερη $z_2 \preceq z_1$. Άρα τελικά, για κάθε $z_1, z_2 \in \mathbb{C}$, ισχύει είτε $z_1 \preceq z_2$ είτε $z_2 \preceq z_1$.

Παρατήρηση. Αν $z_1 \preceq z_2$ και $z \in \mathbb{C}$ τυχών, εύκολα βλέπει κανείς ότι $z_1 + z \preceq z_2 + z$. Όμως, αν $z_1 \preceq z_2$ και $0 \preceq z$ με $z \neq 0$, δεν εξασφαλίζεται ότι $z_1 z \preceq z_2 z$.

Άσκηση: (α) Βρείτε μια τριάδα μιγαδικών αριθμών z_1, z_2, z που ικανοποιούν τις $z_1 \preceq z_2$ και $0 \preceq z$ με $z \neq 0$, αλλά δεν ισχύει $z_1 z \preceq z_2 z$.

(β) Δείξτε ότι το $\mathbb{C}$ δεν μπορεί να εφοδιαστεί με ολική διάταξη που να ικανοποιεί τα αξιώματα (Π10)-(Π13) των πραγματικών αριθμών.

2.6 Συναρτήσεις

Ορισμός 2.6.1. Έστω A, B σύνολα. Μια διμελής σχέση $R \subseteq A \times B$ από το A στο B λέγεται **συνάρτηση** ή **απεικόνιση**, αν ισχύει η επόμενη συνθήκη:

$$\text{για κάθε } \ a \in A \ \text{ υπάρχει μοναδικό } \ b \in B \ : \ (a,b) \in R.$$

Ιδιαιτέρως για τις συναρτήσεις γράφουμε:

- f αντί R,
- $f : A \to B$ αντί $f \subseteq A \times B$,
- $f(a) = b$ αντί $(a,b) \in f$.

Ο ορισμός της συνάρτησης απαιτεί κάθε σημείο του A να συμμετέχει σε ένα ακριβώς διατεταγμένο ζεύγος (a,b) της σχέσης, αλλά δεν βάζει κανένα περιορισμό στα στοιχεία του B. Κάποια από αυτά μπορεί να εμφανίζονται σε περισσότερα διατεταγμένα ζεύγη και άλλα να μην εμφανίζονται καθόλου.

Ορισμός 2.6.2. Μια απεικόνιση $f : A \to B$ λέγεται **ενεικόνιση** (ή απλά **ένα προς ένα**) (συμβ. 1-1) αν ισχύει η συνεπαγωγή

$$a_1, a_2 \in A \text{ με } a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$$

ή, ισοδύναμα, η συνεπαγωγή

$$a_1, a_2 \in A \text{ με } f(a_1) = f(a_2) \implies a_1 = a_2.$$

Μια απεικόνιση $f : A \to B$ λέγεται **επεικόνιση** (ή απλά **επί**) αν

$$\text{για κάθε } b \in B \ \text{ υπάρχει } \ a \in A : f(a) = b.$$

Μια απεικόνιση που είναι και 1-1 και επί λέγεται **αμφιμονοσήμαντη**.

Όπως για κάθε διμελή σχέση, έτσι και για μια απεικόνιση $f : A \to B$ υπάρχει η αντίστροφη διμελής σχέση $f^{-1} \subseteq B \times A$.

Ορισμός 2.6.3. Μια απεικόνιση $f : A \to B$ λέγεται **αντιστρέψιμη** αν και η διμελής σχέση $f^{-1} \subseteq B \times A$ είναι απεικόνιση.

Ισχύει η επόμενη

Πρόταση 2.6.4. *Μια απεικόνιση $f : A \to B$ είναι αντιστρέψιμη εάν και μόνο εάν είναι αμφιμονοσήμαντη.*

Απόδειξη. Σύμφωνα με τους Ορισμούς 2.6.1 και 2.6.3,

$$\begin{aligned} f \text{ αντιστρέψιμη} &\iff f^{-1} \text{ απεικόνιση} \\ &\iff \text{για κάθε } b \in B \text{ υπάρχει μοναδικό } a \in A : (b, a) \in f^{-1} \\ &\iff f \text{ είναι αμφιμονοσήμαντη} \end{aligned}$$

□

Ορισμός 2.6.5. *Έστω $f : A \to B$ μια απεικόνιση, $X \subseteq A$ και $Y \subseteq B$. Ονομάζουμε* **εικόνα του X μέσω της f** *το σύνολο*

$$f(X) = \{f(x) : x \in X\} \subseteq B$$

και **αντίστροφη εικόνα του Y μέσω της f** *το σύνολο*

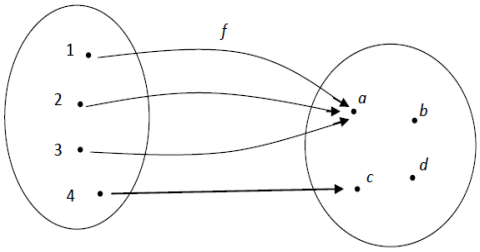
$$f^{-1}(Y) = \{x \in A : f(x) \in Y\} \subseteq A.$$

Παρατήρηση 2.6.6. (α) Η αντίστροφη *απεικόνιση* $f^{-1} : B \to A$ υπάρχει *μόνο* αν η f είναι αμφιμονοσήμαντη.

(β) Η αντίστροφη *εικόνα* $f^{-1}(X)$ ενός συνόλου υπάρχει *πάντοτε*.

Παράδειγμα 2.6.7. Θεωρούμε τα σύνολα $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$ και την απεικόνιση $f : A \to B$ με

$$f(1) = f(2) = f(3) = a \quad \text{και} \quad f(4) = c.$$



Η f δεν είναι ούτε 1-1 ούτε επί. Όμως, υπάρχει η αντίστροφη εικόνα $f^{-1}(X)$, για κάθε $X \subseteq B$. Για παράδειγμα,

$$\begin{aligned} f^{-1}(\varnothing) &= \varnothing \\ f^{-1}(\{b,c\}) &= \{4\} \\ f^{-1}(\{a,c\}) &= f^{-1}(B) = A \\ f^{-1}(\{a\}) &= f^{-1}(\{a,d\}) = \{1,2,3\} \end{aligned}$$

Η πρόταση που ακολουθεί είναι προφανής:

Πρόταση 2.6.8. *Έστω $f : A \to B$ μια απεικόνιση. Ισχύουν τα επόμενα:*

(i) *Αν $X_1 \subseteq X_2 \subseteq A$, τότε $f(X_1) \subseteq f(X_2) \subseteq B$.*

(ii) *Αν $Y_1 \subseteq Y_2 \subseteq B$, τότε $f^{-1}(Y_1) \subseteq F^{-1}(Y_2) \subseteq A$.*

(iii) *Για κάθε $X \subseteq A$ είναι*
$$X \subseteq f^{-1}(f(X)).$$

(iv) *Για κάθε $Y \subseteq B$ είναι*
$$f(f^{-1}(Y)) \subseteq Y.$$

(v) *Αν $X_1, X_2 \subseteq A$, τότε*
$$\begin{aligned} f(X_1 \cup X_2) &= f(X_1) \cup f(X_2) \\ f(X_1 \cap X_2) &\subseteq f(X_1) \cap f(X_2). \end{aligned}$$

(vi) *Αν $Y_1, Y_2 \subseteq B$, τότε*
$$\begin{aligned} f^{-1}(Y_1 \cup Y_2) &= f^{-1}(Y_1) \cup f^{-1}(Y_2) \\ f^{-1}(Y_1 \cap Y_2) &= f^{-1}(Y_1) \cap f^{-1}(Y_2). \end{aligned}$$

Ορισμός 2.6.9. Έστω $f : A \to B$ και $g : C \to D$ απεικονίσεις με $f(A) \subseteq C$. Τότε ορίζεται η απεικόνιση $g \circ f : A \to D$ με

$$(g \circ f)(x) = g(f(x)), \qquad \text{για κάθε } \ x \in A,$$

που ονομάζεται **σύνθεση** των f και g.

Η απόδειξη της επόμενης πρότασης είναι άμεση:

Πρόταση 2.6.10. *Έστω $f : A \to B$, $g : C \to D$ και $h : E \to F$ απεικονίσεις με $f(A) \subseteq C$ και $g(C) \subseteq E$. Τότε ορίζονται οι συνθέσεις*

$$h \circ (g \circ f) : A \longrightarrow F$$
$$(h \circ g) \circ f : A \longrightarrow E$$

και είναι ίσες. Άρα η σύνθεση απεικονίσεων είναι προσεταιριστική.

Πρόταση 2.6.11. *Έστω $f : A \to B$ και $g : B \to C$ δύο απεικονίσεις. Ισχύουν τα επόμενα:*

(i) *Αν οι f και g είναι* 1-1*, τότε η $g \circ f$ είναι* 1-1*.*

(ii) *Αν η $g \circ f$ είναι* 1-1*, τότε η f είναι* 1-1*.*

(iii) *Αν οι f και g είναι επί, τότε η $g \circ f$ είναι επί.*

(iv) *Αν η $g \circ f$ είναι επί, τότε η g είναι επί.*

Απόδειξη. (i) Υποθέτουμε ότι οι f και g είναι 1-1. Θα δείξουμε ότι η $g \circ f$ είναι 1-1. Έστω $x_1, x_2 \in A$ με $g \circ f(x_1) = g \circ g(x_2)$. Τότε $g(f(x_1)) = g(f(x_2))$. Επειδή η g είναι 1-1, $f(x_1) = f(x_2)$ και επειδή η f είναι 1-1, $x_1 = x_2$.

(ii) Υποθέτουμε ότι η $g \circ f$ είναι 1-1 και θα δείξουμε ότι η f είναι 1-1. Έστω $x_1, x_2 \in A$ με $f(x_1) = f(x_2)$. Εφαρμόζοντας την g στο στοιχείο $f(x_1) = f(x_2) \in B$ παίρνουμε $g(f(x_1)) = g(f(x_2))$. Επειδή η $g \circ f$ είναι 1-1, προκύπτει ότι $x_1 = x_2$.

(iii) Υποθέτουμε ότι οι f και g είναι επί. Θα δείξουμε ότι η $g \circ f$ είναι επί. Πράγματι, έστω $z \in C$. Επειδή η g είναι επί, υπάρχει $y \in B$ με $g(y) = x$. Επίσης, επειδή η f είναι επί, υπάρχει $x \in A$ με $f(x) = y$. Τότε $g \circ f(x) = g(f(x)) = g(y) = z$.

(iv) Τέλος υποθέτουμε ότι η $g \circ f$ είναι επί και δείχνουμε ότι η g είναι επί: Έστω $z \in C$. Επειδή η $g \circ f$ είναι επί, υπάρχει $x \in A$ με $g \circ f(x) = g(f(x)) = z$. Θέτοντας $y = f(x)$, έχουμε το ζητούμενο $y \in B$ με $g(y) = z$. □

Για κάθε σύνολο A η διμελής σχέση της ισότητας που αντιστοιχεί στη διαγώνιο Δ_A (βλέπε Παράδειγμα 2.5.2 (α)) είναι μια απεικόνιση $f : A \to A$ με $f(x) = x$ για κάθε $x \in A$, που την ονομάζουμε **ταυτοτική απεικόνιση** του συνόλου A και την συμβολίζουμε με id_A. Παρατηρούμε ότι για κάθε $f : A \to B$ και κάθε $g : C \to A$ ισχύει $f \circ id_A = f$ και $id_A \circ g = g$.

Αν η $f : A \to B$ είναι αμφιμονοσήμαντη και $f^{-1} : B \to A$ είναι η αντίστροφή της, προκύπτει αμέσως ότι

$$f^{-1} \circ f = id_A \quad \text{και} \quad f \circ f^{-1} = id_B.$$

Όπως φαίνεται από την επόμενη πρόταση, οι δύο προηγούμενες ισότητες είναι χαρακτηριστικές της αντίστροφης απεικόνισης.

Πρόταση 2.6.12. *Μια απεικόνιση $f : A \to B$ είναι αμφιμονοσήμαντη αν και μόνο αν υπάρχει μοναδική $g : B \to A$ με $g \circ f = id_A$ και $f \circ g = id_B$.*

Απόδειξη. ($\Longrightarrow$) Αν η f είναι αμφιμονοσήμαντη, τότε υπάρχει η $g = f^{-1}$ και ικανοποιεί τις ανωτέρω ισότητες. Για το μονοσήμαντο: Έστω ότι υπάρχουν $g, h : B \to A$ με

$$g \circ f = id_A, \quad f \circ g = id_B, \quad h \circ f = id_A, \quad f \circ h = id_B.$$

Τότε

$$g = g \circ id_B = g \circ (f \circ h) = (g \circ f) \circ h = id_A \circ h = h$$

δηλαδή $g = h = f^{-1}$.

($\Longleftarrow$) Αντίστροφα, έστω ότι υπάρχει μια $g : B \to A$ που ικανοποιεί τις δύο ισότητες. Επειδή οι ταυτοτικές απεικονίσεις είναι 1-1 και επί, από την $g \circ f = id_A$ προκύπτει ότι η f είναι 1-1 και από την $f \circ g = id_B$ ότι η f είναι επί. □

Ορισμός 2.6.13. Λέμε ότι μια απεικόνιση $f : A \to B$ **έχει αντίστροφη από αριστερά** αν υπάρχει μια $g : B \to A$ με $g \circ f = id_A$. Μια τέτοια g λέγεται **αριστερή αντίστροφη** της f.

Αντίστοιχα, λέμε ότι μια απεικόνιση $f : A \to B$ **έχει αντίστροφη από δεξιά** αν υπάρχει μια $h : B \to A$ με $f \circ h = id_B$. Μια τέτοια h λέγεται **δεξιά αντίστροφη** της f.

Πρόταση 2.6.14. *Μια $f : A \to B$ έχει αντίστροφη από αριστερά αν και μόνο αν η f είναι* 1-1.

Απόδειξη. ($\Longrightarrow$) Έστω ότι η $g : B \to A$ είναι αριστερή αντίστροφη της f. Τότε $g \circ f = id_A$. Επειδή η id_A είναι 1-1, η f είναι 1-1.

($\Longleftarrow$) Έστω ότι η f είναι 1-1. Σταθεροποιούμε ένα $a_0 \in A$ και ορίζουμε $g : B \to A$ ως εξής: αν $y \in f(A)$, υπάρχει ένα μοναδικό $x \in A$ με $f(x) = y$. Τότε θέτουμε $g(y) = x$. Αν $y \notin f(A)$, θέτουμε $g(y) = a_0$. Παρατηρούμε ότι για κάθε $x \in A$ έχουμε $y = f(x) \in f(A)$, άρα $g \circ f(x) = g(f(x)) = x$, δηλαδή $g \circ f = id_A$. □

Σημείωση: Αν η f δεν είναι επί, η απεικόνιση g που κατασκευάζουμε στην προηγούμενη πρόταση *δεν* είναι μονοσήμαντα ορισμένη, αλλά αλλάζει αν επιλεγεί άλλο a_0.

Πρόταση 2.6.15. *Μια απεικόνιση $f : A \to B$ έχει αντίστροφη από δεξιά αν και μόνο αν η f είναι επί.*

Απόδειξη. ($\Longrightarrow$) Έστω ότι η $h : B \to A$ είναι δεξιά αντίστροφη της f. Τότε $f \circ h = id_B$. Επειδή η id_A είναι επί, η f είναι επί.

($\Longleftarrow$) Έστω ότι η f είναι επί. Τότε για κάθε $y \in B$ η αντίστροφη εικόνα $f^{-1}(\{y\})$ είναι μη κενή. Για κάθε $y \in B$, επιλέγουμε ένα $x_y \in f^{-1}(\{y\})$. Τότε $f(x_y) = y$. Θέτουμε $h : B \to A$ με $h(y) = x_y$, για κάθε $y \in B$, οπότε $f(h(y)) = f(x_y) = y$, δηλαδή $f \circ h = id_B$. □

Σημείωση: Αν η f δεν είναι 1-1, τότε η h που κατασκευάζουμε *δεν* είναι μονοσήμαντα ορισμένη, αλλά αλλάζει αν αλλάξουμε την επιλογή των x_y.

Πρόταση 2.6.16. *Έστω $f : A \to B$ μια απεικόνιση που έχει αριστερή αντίστροφη g και δεξιά αντίστροφη h. Τότε η f είναι αντιστρέψιμη και $g = h = f^{-1}$.*

Απόδειξη. Από τις προηγούμενες δύο προτάσεις, αφού η f έχει και αριστερή και δεξιά αντίστροφη, είναι 1-1 και επί, δηλαδή είναι αμφιμονοσήμαντη, άρα αντιστρέψιμη. Επειδή $g \circ f = id_A$ και $f \circ h = id_B$, παίρνουμε

$$g = g \circ id_B = g \circ (f \circ h) = (g \circ f) \circ h = id_A \circ h = h$$

και η ισότητα με την f^{-1} προκύπτει από την Πρόταση 2.6.15. □

2.7 Ασκήσεις

Καρτεσιανό γινόμενο

1. Κάποιος σας προτείνει τον εξής ορισμό του διατεταγμένου ζεύγους:

$$(x, y) = \{x, \{y\}\}.$$

Τι λέτε;

2. Εξετάστε αν ισχύουν οι ισότητες

$$\begin{aligned} (A \setminus B) \times C &= (A \times C) \setminus (B \times C) \\ (A \triangle B) \times C &= (A \times C) \triangle (B \times C). \end{aligned}$$

3. Δώστε παράδειγμα συνόλων A, B, C και D για τα οποία το $(A \times B) \cup (C \times D)$ είναι γνήσιο υποσύνολο του $(A \cup C) \times (B \cup D)$.

Σχέσεις

4. Ορίζουμε δύο σχέσεις $\boldsymbol{\rho}$ και $\boldsymbol{\sigma}$ στο $\mathbb{N}$ ως εξής:

$$(a, b) \in \rho \text{ αν και μόνο αν } a \mid b \text{ (ο } a \text{ είναι διαιρέτης του } b)$$

και

$$(a, b) \in \boldsymbol{\sigma} \text{ αν και μόνο αν } a^2 \mid b \text{ (ο } a^2 \text{ είναι διαιρέτης του } b).$$

Περιγράψτε με ιδιότητες διαιρετότητας τις σχέσεις $\boldsymbol{\rho} \cup \boldsymbol{\sigma}$, $\rho \cap \boldsymbol{\sigma}$, $\boldsymbol{\rho} \setminus \boldsymbol{\sigma}$, $\boldsymbol{\sigma} \setminus \boldsymbol{\rho}$.

5. Για καθεμιά από τις παρακάτω σχέσεις στο $\mathbb{R}$ εξετάστε αν είναι: (α) ανακλαστική, (β) συμμετρική, (γ) μεταβατική.

(i) $x < y$.

(ii) $x \geqslant y$.

(iii) $|x - y| \leqslant 1$.

(iv) $|x - y| \leqslant 0$.

(v) $x - y \in \mathbb{Q}$.

(vi) $x - y \notin \mathbb{Q}$.

6. Θεωρούμε δύο ανακλαστικές σχέσεις $\boldsymbol{\rho}$ και $\boldsymbol{\sigma}$ στο X. Δείξτε ότι οι σχέσεις $\boldsymbol{\rho} \cup \boldsymbol{\sigma}$ και $\boldsymbol{\rho} \cap \boldsymbol{\sigma}$ είναι επίσης ανακλαστικές.

7. Έστω $\boldsymbol{\rho}$ και $\boldsymbol{\sigma}$ δύο συμμετρικές σχέσεις στο σύνολο X. Εξετάστε αν οι σχέσεις $\boldsymbol{\rho} \cup \boldsymbol{\sigma}$, $\boldsymbol{\rho} \cap \boldsymbol{\sigma}$ και $\boldsymbol{\rho} \setminus \boldsymbol{\sigma}$ είναι επίσης συμμετρικές.

8. Ορίζουμε μια σχέση $\boldsymbol{\sigma}$ στο $\mathbb{N} \times \mathbb{N}$ (δηλαδή, $\boldsymbol{\sigma} \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$), ως εξής:

$$(m, n)\, \boldsymbol{\sigma}\, (r, s) \quad \text{αν} \quad m + s = r + n.$$

Δείξτε ότι η $\boldsymbol{\sigma}$ είναι σχέση ισοδυναμίας. Οι κλάσεις ισοδυναμίας αυτής της σχέσης αντιστοιχούν με φυσιολογικό τρόπο στα στοιχεία ενός γνωστού συνόλου. Ποιό είναι αυτό;

9. Ορίζουμε μια σχέση $\boldsymbol{\sigma}$ στο σύνολο $B = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : y \neq 0\}$ ως εξής:

$$(m, n)\, \boldsymbol{\sigma}\, (r, s) \quad \text{αν} \quad m \cdot s = n \cdot r.$$

Εξετάστε αν η $\boldsymbol{\sigma}$ είναι σχέση ισοδυναμίας.

10. Το επιχείρημα που ακολουθεί αποδεικνύει ότι αν μια σχέση $\sim$ είναι συμμετρική και μεταβατική, τότε είναι και ανακλαστική. Εξετάστε αν είναι σωστό, και αν όχι, εξηγήστε ποιό είναι το λάθος.

> Έστω $a \sim b$. Η $\sim$ είναι συμμετρική, συνεπώς $b \sim a$. Αφού η $\sim$ είναι μεταβατική, από τις $a \sim b$ και $b \sim a$ συμπεραίνουμε ότι $a \sim a$. Άρα, η $\sim$ είναι ανακλαστική.

11. Να αποδειχθεί ότι μια σχέση $\sim$ σε ένα σύνολο X είναι σχέση ισοδυναμίας αν και μόνο αν ισχύουν τα εξής: (α) η $\sim$ είναι συμμετρική και μεταβατική, και, (β) για κάθε $x \in X$ υπάρχει $y \in X$ ώστε $x \sim y$.

12. Στο $\mathbb{Z}$ θεωρούμε τις σχέσεις $\equiv_4$ και $\equiv_6$. Ποιά είναι η σχέση $\equiv_4 \cap \equiv_6$;

13. Πόσες διαφορετικές σχέσεις ισοδυναμίας μπορούμε να ορίσουμε στο σύνολο $A = \{1, 2, 3, 4\}$;

14. Έστω $\boldsymbol{\rho_1}$ και $\boldsymbol{\rho_2}$ δύο σχέσεις ισοδυναμίας στο ίδιο σύνολο X. Υποθέτουμε ότι $\boldsymbol{\rho_1} \subseteq \boldsymbol{\rho_2}$. Αν Δ_1 και Δ_2 είναι οι διαμερίσεις του X που αντιστοιχούν στις $\boldsymbol{\rho_1}, \boldsymbol{\rho_2}$, υπάρχει κάποια σχέση μεταξύ των Δ_1 και Δ_2;

15. Έστω X το σύνολο των ανθρώπων και έστω σ η σχέση: $x \sigma y$ αν και μόνο οι x και y έχουν τους ίδιους γονείς. Είναι η σ σχέση ισοδυναμίας· Αν ναι, βρείτε το σύνολο των κλάσεων ισοδυναμίας, δηλαδή τη διαμέριση που ορίζει η σ στο X.

Αν η φράση "τους ίδιους γονείς" αντικατασταθεί από τη φράση "τουλάχιστον έναν κοινό γονέα" είναι η σ σχέση ισοδυναμίας;

16. Έστω $\boldsymbol{\rho}$ μια διάταξη στο σύνολο X. Δείξτε ότι η αντίστροφη σχέση $\boldsymbol{\rho}^{-1}$ είναι επίσης διάταξη.

17. Στο σύνολο $A = \{\{0\}, \{0, 1\}, \{0, 1, 2\}, \{0, 1, 2, 3\}\}$ ορίζουμε σχέση $\boldsymbol{\rho}$ ως εξής: $x \boldsymbol{\rho} y$ αν $x \subseteq y$. Εξετάστε αν η $\boldsymbol{\rho}$ είναι ολική διάταξη.

18. Ορίζουμε μια σχέση $\boldsymbol{\rho}$ στο $\mathbb{N}$ ως εξής:

$$(a, b) \in \rho \text{ αν } a|b \text{ (ο } a \text{ είναι διαιρέτης του } b).$$

Είναι η $\boldsymbol{\rho}$ σχέση διάταξης; Αν ναι, είναι ολική διάταξη;

19. Ορίζουμε μια σχέση $\boldsymbol{\rho}$ στο $X = \{1, 2, 6, 30, 210\}$ ως εξής:

$$(a, b) \in \boldsymbol{\rho} \text{ αν } a \mid b \text{ (ο } a \text{ είναι διαιρέτης του } b).$$

Είναι η $\boldsymbol{\rho}$ σχέση διάταξης; Αν ναι, είναι ολική διάταξη;

20. Έστω ότι (A, R_1) και (B, R_2) είναι δύο ολικά διατεταγμένα σύνολα. Στο σύνολο $A \times B$ ορίζουμε τη σχέση R ως εξής:

$$(a, b)\, R\, (c, d) \quad \Longleftrightarrow \quad a\, R_1\, c \quad \text{και} \quad b\, R_2\, d\,.$$

Ελέγξτε αν η R είναι διάταξη. Αν ναι, είναι ολική διάταξη;

21. Στο $\mathbb{R}^2$ ορίζουμε σχέση $\boldsymbol{\rho}$ ως εξής: $(x_1, y_1)\,\boldsymbol{\rho}\,(x_2, y_2)$ αν είτε $y_1 < y_2$ ή $y_1 = y_2$ και $x_1 \leqslant x_2$. Εξετάστε αν η $\boldsymbol{\rho}$ είναι ολική διάταξη.

22. Έστω A ένα σύνολο με μια σχέση ολικής διάταξης R και έστω B ένα σύνολο με μια σχέση ολικής διάταξης T. Η *λεξικογραφική διάταξη* L στο $A \times B$ ορίζεται ως εξής: $(a, b)\ L\ (c, d)$ αν: είτε $a\,R\,c$ και $a \neq c$ ή $a = c$ και $b\,T\,d$. Ελέγξτε ότι η L είναι σχέση διάταξης και εξετάστε αν είναι ολική διάταξη. Γιατί λέγεται η L λεξικογραφική διάταξη;

Συναρτήσεις

23. Οι παρακάτω συναρτήσεις έχουν πεδίο τιμών το $\mathbb{R}$ και πεδίο ορισμού κάποιο υποσύνολο του $\mathbb{R}$. Βρείτε σε κάθε περίπτωση ποιό είναι το μεγαλύτερο δυνατό πεδίο ορισμού:

$$h(x) = \ln x, \qquad \alpha(v) = -v, \qquad j(\beta) = \frac{1}{\beta^2 - 1}, \qquad g(u) = \ln(\ln(\cos u)).$$

24. Οι παρακάτω συναρτήσεις έχουν πεδίο τιμών το $\mathbb{R}$ και πεδίο ορισμού κάποιο υποσύνολο του $\mathbb{R}$. Βρείτε σε κάθε περίπτωση ποιό είναι το μεγαλύτερο δυνατό πεδίο ορισμού:

$$V(t) = \ln(1 - t^2), \qquad y = \ln(\sin^2 x), \qquad \rho = \sqrt{(u-1)(u-2)(u-3)(u-4)}.$$

25. Προσδιορίστε την εικόνα για τις ακόλουθες συναρτήσεις $f : \mathbb{R} \to \mathbb{R}$:

(α) $f(x) = x^3$.

(β) $f(x) = x - 4$.

(γ) $f(x) = e^x + 3$.

(δ) $f(x) = \begin{cases} 1/x & \text{αν } x \neq 0 \\ 0 & \text{αν } x = 0 \end{cases}$

26. Για κάθε μία από τις συναρτήσεις της Άσκησης 25 εξετάστε αν (σαν συνάρτηση από το $\mathbb{R}$ στο $\mathbb{R}$) είναι: (α) $1-1$, (β) επί, (γ) $1-1$ και επί.

27. Προσδιορίστε την εικόνα για τις ακόλουθες συναρτήσεις $f, g : \mathbb{R} \to \mathbb{R}$:

(α) $f(x) = x^2 + 2x + 2$, $g(x) = x^2 + \cos x$.

(β) $f(x) = |x|$, $g(x) = 1/x$ αν $x \neq 0$ και $g(0) = 0$.

(γ) $f(x) = x^2 + x - |x|^2$, $g(x) = x^{16} + x$.

28. Για καθεμιά από τις συναρτήσεις της Άσκησης 27 εξετάστε αν (σαν συνάρτηση από το $\mathbb{R}$ στο $\mathbb{R}$) είναι: (α) $1-1$, (β) επί, (γ) $1-1$ και επί.

29. Δώστε παράδειγμα συνάρτησης $f : \mathbb{Z} \to \mathbb{Z}$ που να είναι:

(α) $1-1$ αλλά όχι επί.

(β) επί αλλά όχι $1-1$.

(γ) $1-1$ και επί.

(δ) ούτε $1-1$ ούτε επί.

30. Έστω S το σύνολο των δίσκων στο επίπεδο και έστω $f : S \to \mathbb{R}$ η συνάρτηση που ορίζεται ως εξής: $f(x)$ =το εμβαδόν του x. Εξετάστε αν (α) η f είναι ένα προς ένα, (β) η f είναι επί.

31. Έστω T το σύνολο των κύκλων με κέντρο την αρχή των αξόνων στο επίπεδο και έστω $g : T \to \mathbb{R}^+$ η συνάρτηση που ορίζεται ως εξής: $g(x)$ =το μήκος της περιφέρειας του x. Εξετάστε αν (α) η g είναι ένα προς ένα, (β) η g είναι επί.

32. Αν $A = \{1, 2\}$ και $B = \{a, b, c\}$, πόσες διαφορετικές συναρτήσεις υπάρχουν από το A στο B; Πόσες από το B στο A; Σε κάθε περίπτωση, πόσες από αυτές είναι $1-1$ και πόσες από αυτές είναι επί; Πόσες είναι $1-1$ και επί;

33. Έστω A ένα σύνολο με m στοιχεία και B ένα σύνολο με n στοιχεία ($m, n \in \mathbb{N}$). Να βρεθεί το πλήθος των συναρτήσεων από το A στο B.

34. Αν $A = \varnothing$ και $B \neq \varnothing$, δείξτε ότι υπάρχει ακριβώς μία συνάρτηση από το A στο B και ότι δεν υπάρχει συνάρτηση από το B στο A. Υπάρχει συνάρτηση από το $\varnothing$ στο $\varnothing$;

35. Δίνονται οι συναρτήσεις f, g και $h : \mathbb{N} \to \mathbb{N}$ που ορίζονται ως εξής:

(α) $f(n) = n + 1$.

(β) $g(n) = 2n$.

(γ) $h(n) = \begin{cases} 0 & \text{αν ο } n \text{ είναι άρτιος} \\ 1 & \text{αν ο } n \text{ είναι περιττός} \end{cases}$

Προσδιορίστε τις συναρτήσεις $f \circ f$, $f \circ g$, $g \circ f$, $g \circ h$, $h \circ g$ και $(f \circ g) \circ h$.

36. Δίνονται συναρτήσεις f και g τέτοιες ώστε να ορίζεται η σύνθεση $g \circ f$. Δείξτε ότι:

(α) Αν η $g \circ f$ είναι επί, τότε η g είναι επί.

(β) Αν η $g \circ f$ είναι $1-1$, τότε η f είναι $1-1$.

Δώστε παραδείγματα συναρτήσεων f και g που να δείχνουν ότι δεν ισχύουν οι αντίστροφες συνεπαγωγές: μπορεί η g να είναι επί ενώ η $g \circ f$ όχι, μπορεί η f να είναι $1-1$ αλλά η $g \circ f$ όχι.

37. Αν οι $f : A \to B$ και $g : B \to C$ είναι $1-1$ και επί, δείξτε ότι η $g \circ f : A \to C$ είναι $1-1$ και επί.

38. Αν $f : A \to B$ είναι συνάρτηση, $U, V \subseteq A$ και $X, Y \subseteq B$, δείξτε ότι:

(α) $f(\varnothing) = \varnothing, \qquad f^{-1}(\varnothing) = \varnothing, \qquad f^{-1}(B) = A.$

(β) $f(U \cap V) \subseteq f(U) \cap f(V)$.

(γ) Αν η f είναι $1-1$, τότε $f(U \cap V) = f(U) \cap f(V)$.

(δ) $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$.

(ε) $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$.

(στ) $f^{-1}(B \setminus X) = A \setminus f^{-1}(X)$.

39. Για τις παρακάτω συναρτήσεις ελέγξτε αν υπάρχει δεξιό αντίστροφο ή/και αριστερό αντίστροφο. Αν υπάρχει, βρείτε το.

(α) $f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = 4x + 2.$

(β) $g : \mathbb{R} \to \mathbb{R}^+, \qquad g(x) = x^2.$

40. Για τις συναρτήσεις f και g της Άσκησης 39 βρείτε τα σύνολα $f([-1,1])$, $f^{-1}([0,2])$, $g([-3,-2])$ και $g^{-1}([2,4])$.

41. Βρείτε το μεγαλύτερο υποσύνολο του $\mathbb{R} \times \mathbb{R}$ στο οποίο ορίζεται η συνάρτηση δύο μεταβλητών

$$f(x,y) = \frac{x^2 + 3xy}{(x-1)y}.$$

42. Βρείτε την ένωση και την τομή των παρακάτω οικογενειών συνόλων με σύνολο δεικτών A.

(α) $A = \{1, 2, 3, \ldots, n\}, \qquad S_a = [0, a+1].$

(β) $A = \mathbb{N}, \qquad S_a = \left(0, \frac{1}{n}\right) = \{x \in \mathbb{R} \mid 0 < x < 1/n\}.$

43. Δίνεται η συνάρτηση $f : \mathbb{R} \to \mathbb{R}$ με $f(x) = (x+1)^2$.

(α) Σχεδιάστε το γράφημα της f.

(β) Προσδιορίστε τα σύνολα $B = f(\mathbb{R})$, $f^{-1}([-1,4])$, $f^{-1}(\{-2\})$, $f^{-1}([-2,0))$.

(γ) Βρείτε δύο διαφορετικά δεξιά αντίστροφα της $f : \mathbb{R} \to f(\mathbb{R})$.

(δ) Βρείτε δύο υποσύνολα A_1 και A_2 του $\mathbb{R}$ τέτοια ώστε $A_1 \cup A_2 = \mathbb{R}$ και οι συναρτήσεις $f|_{A_1}$, $f|_{A_2}$ να είναι ένα προς ένα. Βρείτε ένα αριστερό αντίστροφο της $f|_{A_i} : A_i \to \mathbb{R}$, $i = 1, 2$.

44. Ορίζουμε τις παρακάτω διμελείς πράξεις στο $\mathbb{Z}$:

(α) $x \circ y = x - y$.

(β) $x \circ y = |x - y|$.

(γ) $x \circ y = x + y + xy$.

(δ) $x \circ y = \frac{1}{2}\left(x + y + \frac{1}{2}((-1)^{x+y} + 1) + 1\right)$.

Επαληθεύστε ότι είναι διμελείς πράξεις στο $\mathbb{Z}$, δηλαδή συναρτήσεις από το $\mathbb{Z} \times \mathbb{Z}$ στο $\mathbb{Z}$. Σε κάθε περίπτωση, ελέγξτε αν η πράξη είναι μεταθετική και προσεταιριστική.

45. Μια ακολουθία συνόλων $(A_n)_{n\in\mathbb{N}}$ λέγεται φθίνουσα αν για κάθε $n \in \mathbb{N}$ ισχύει

$$A_{n+1} \subseteq A_n.$$

(α) Αποδείξτε ότι αν η $(A_n)_{n\in\mathbb{N}}$ είναι φθίνουσα, τότε για κάθε $k \in \mathbb{N}$ ισχύει

$$\bigcap_{n=0}^{\infty} A_n = \bigcap_{n=k}^{\infty} A_n.$$

(β) Αποδείξτε ότι αν οι $(A_n)_{n\in\mathbb{N}}$, $(B_n)_{n\in\mathbb{N}}$ είναι φθίνουσες, τότε

$$\bigcap_{n=0}^{\infty} (A_n \cup B_n) = \left(\bigcap_{n=0}^{\infty} A_n\right) \cup \left(\bigcap_{n=0}^{\infty} B_n\right).$$

46. Έστω $f : X \to Y$ και έστω $(A_t)_{t\in T}$ οικογένεια υποσυνόλων του X. Αποδείξτε ότι:

$$f\left(\bigcup_{t\in T} A_t\right) = \bigcup_{t\in T} f(A_t) \quad \text{και} \quad f\left(\bigcap_{t\in T} A_t\right) \subseteq \bigcap_{t\in T} f(A_t).$$

Αν η f είναι ένα προς ένα, δείξτε ότι

$$f\left(\bigcap_{t\in T} A_t\right) = \bigcap_{t\in T} f(A_t).$$

Κεφάλαιο 3

Φυσικοί και ακέραιοι αριθμοί

3.1 Απόδειξη με επαγωγή

Ας υποθέσουμε ότι θέλουμε να αποδείξουμε την ακόλουθη ταυτότητα.

Πρόταση 3.1.1. *Το άθροισμα των φυσικών αριθμών από* 1 *έως* n *είναι ίσο με* $\frac{1}{2}n(n+1)$.

Είναι πολύ απλό να ελέγξουμε ότι η ισότητα ισχύει όταν $n = 1$. Το άθροισμα είναι ίσο με 1 και $\frac{1}{2}1(1+1)) = 1$.

Ας υποθέσουμε τώρα ότι η ισότητα ισχύει για κάποιον $k \geqslant 1$, δηλαδή

$$1 + 2 + \cdots + k = \frac{1}{2}k(k+1).$$

Τότε, προσθέτοντας τον $k+1$ και στα δύο μέλη έχουμε

$$\begin{aligned} 1 + 2 + \cdots + k + (k+1) &= \frac{1}{2}k(k+1) + (k+1) = (k+1)\Big(\frac{k}{2} + 2\Big) \\ &= (k+1)\frac{k+2}{2} = \frac{1}{2}(k+1)(k+2). \end{aligned}$$

Άρα, η ισότητα αληθεύει και για τον $k+1$.

Μοιάζει αρκετά λογικό να θεωρήσουμε ότι με αυτόν τον τρόπο εξασφαλίζεται ότι η ισότητα $1+2+\cdots+n = \frac{1}{2}n(n+1)$ για κάθε φυσικό αριθμό n. Το επιχείρημα βασίζεται σε αυτό που θα λέγαμε «και ούτω καθ' εξής». Εξασφαλίζουμε την αλήθεια της πρότασης για $n = 1$ και το γενικό βήμα, το οποίο από την ισχύ της πρότασης για τον k εξασφαλίζει ότι η πρόταση ισχύει για τον $k+1$. Εφαρμόζοντας το γενικό βήμα με $k = 1$ εξασφαλίζουμε ότι η πρόταση ισχύει για τον 2. Κατόπιν, εφαρμόζοντας το γενικό βήμα με $k = 2$ εξασφαλίζουμε

ότι η πρόταση ισχύει για τον $k = 3$. Αν θέλουμε να αποδείξουμε ότι η πρόταση ισχύει για τον 2020 μπορούμε να επαναλάβουμε αυτή τη διαδικασία 2019 φορές. Όσο μεγαλύτερος είναι ο n τόσο περισσότερες είναι οι επαναλήψεις του γενικού βήματος που απαιτούνται για να φτάσουμε στον n και να βεβαιωθούμε ότι η πρόταση ισχύει γι' αυτόν. Το πρόβλημα είναι ότι δεν είναι δυνατόν να καλύψουμε όλους τους φυσικούς αριθμούς, να αποδείξουμε δηλαδή την ισότητα για όλους τους n, με μια απόδειξη που να αποτελείται από πεπερασμένο αριθμό βημάτων.

Παρ' όλα αυτά, οι περισσότεροι θα συμφωνούσαν ότι η ταυτότητα της Πρότασης 3.1.1 ισχύει για κάθε n. Η λύση είναι να εφοδιάσουμε τον ίδιο τον ορισμό των φυσικών αριθμών με μια ιδιότητα που θα εμπεριέχει το «ούτω καθ' εξής» το οποίο μοιάζει να απαιτεί νομιμοποίηση ώστε να είναι αποδεκτές αποδείξεις αυτού του τύπου.

3.2 Οι φυσικοί αριθμοί

Στόχος μας είναι να περιγράψουμε το σύνολο των φυσικών αριθμών και αυτό δεν μπορούμε να το κάνουμε καταγράφοντας, το ένα μετά το άλλο, όλα τα στοιχεία του. Η προσέγγιση που θα ακολουθήσουμε είναι να προσπαθήσουμε να εκφράσουμε με συνολοθεωρητικό τρόπο την διαισθητική έννοια της απαρίθμησης. Αρχίζουμε με το 1, ακολουθεί το 2, μετά είναι το 3, και συνεχίζουμε δίνοντας κάθε φορά ένα όνομα στον επόμενο φυσικό αριθμό. Μπορούμε δε να συνεχίσουμε αυτή τη διαδικασία, όσο θέλουμε. Αυτή η διαδικασία της απαρίθμησης μπορεί να τυποποιηθεί αν θεωρήσουμε τον «επόμενο φυσικό αριθμό» ως μια συνάρτηση στο σύνολο $\mathbb{N}$ των φυσικών αριθμών,

$$\varepsilon : \mathbb{N} \to \mathbb{N},$$

με κατάλληλες ιδιότητες που να περιγράφουν το ότι «ο $\varepsilon(n)$ είναι ο επόμενος φυσικός από τον n», δηλαδή $\varepsilon(1) = 2$, $\varepsilon(2) = 3$, κλπ. Δύο τέτοιες ιδιότητες είναι οι ακόλουθες:

- Η ε δεν είναι επεικόνιση επί του $\mathbb{N}$, αφού $1 \neq \varepsilon(n)$ για κάθε $n \in \mathbb{N}$.
- Η ε είναι ενεικόνιση, δηλαδή, αν $m \neq n$ τότε $\varepsilon(m) \neq \varepsilon(n)$.

Προσθέτουμε όμως μια τρίτη, επιθυμητή ιδιότητα, η οποία θα μας επιτρέπει να αποδεικνύουμε προτάσεις όπως αυτή της προηγούμενης παραγράφου:

- Αν υποθέσουμε ότι κάποιο $S \subseteq \mathbb{N}$ έχει τις ιδιότητες
  (α) $1 \in S$ και (β) εάν $n \in S$ τότε $\varepsilon(n) \in S$,
  τότε $S = \mathbb{N}$.

Δηλαδή, εάν ένα σύνολο φυσικών αριθμών περιέχει το 1 και κάθε φορά που περιέχει κάποιον n περιέχει και τον $\varepsilon(n)$, τότε αυτό το σύνολο περιέχει όλους τους φυσικούς αριθμούς.

Όπως θα δούμε παρακάτω, για να προσεγγίσουμε αξιωματικά την Αριθμητική αρκεί να δεχτούμε (ή να απαιτήσουμε) την ύπαρξη ενός συνόλου που έχει αυτές τις τρεις ιδιότητες. Αυτά είναι τα λεγόμενα *αξιώματα του Peano*, ενός Ιταλού μαθηματικού που ανέπτυξε αυτή την προσέγγιση των φυσικών αριθμών στο τέλος του 19ου αιώνα.

Πριν διατυπώσουμε συστηματικά τα αξιώματα του Peano, ας σημειώσουμε ότι για πρακτικούς λόγους είναι προτιμότερο να συμπεριλάβουμε τον 0 στο σύνολο των φυσικών αριθμών. Αν θέλουμε οι φυσικοί αριθμοί να εκφράζουν το πλήθος των στοιχείων των πεπερασμένων συνόλων, τότε ο 0 είναι ο φυσικός αριθμός που εκφράζει το πλήθος των στοιχείων του κενού συνόλου $\varnothing$. Αλλά και στην αριθμητική, ο αριθμός 0 είναι πολύ συχνά χρήσιμος. Γι' αυτούς τους λόγους ξεκινάμε με το 0 στο αξιωματικό μας σύστημα και χρησιμοποιούμε το σύμβολο $\mathbb{N}_0$ για να δηλώσουμε το σύνολο των φυσικών αριθμών που περιέχει το 0.

Θεωρούμε λοιπόν ένα σύνολο $\mathbb{N}_0$ και μια συνάρτηση $\varepsilon : \mathbb{N}_0 \to \mathbb{N}_0$ με τις παρακάτω ιδιότητες:

(Φ1) Η συνάρτηση ε δεν είναι επεικόνιση επί του $\mathbb{N}_0$: υπάρχει κάποιο στοιχείο $0 \in \mathbb{N}_0$ τέτοιο ώστε, για κάθε $n \in \mathbb{N}_0$, $\varepsilon(n) \neq 0$.

(Φ2) Η συνάρτηση ε είναι ενεικόνιση: εάν $m, n \in \mathbb{N}_0$ και $\varepsilon(m) = \varepsilon(n)$ τότε $m = n$.

(Φ3) Εάν $S \subseteq \mathbb{N}_0$ είναι ένα σύνολο τέτοιο ώστε $0 \in S$ και για κάθε $n \in \mathbb{N}_0$ ισχύει η συνεπαγωγή

$$n \in S \implies \varepsilon(n) \in S,$$

τότε $S = \mathbb{N}_0$.

Αυτό που θα κάνουμε είναι να θεωρήσουμε την ύπαρξη ενός συνόλου με αυτές τις ιδιότητες ως ένα από τα αξιώματα στα οποία θα βασιστούν τα Μαθηματικά μας.

Αξίωμα ύπαρξης του συνόλου των φυσικών αριθμών. Υπάρχουν ένα σύνολο $\mathbb{N}_0$ και μια συνάρτηση $\varepsilon : \mathbb{N}_0 \to \mathbb{N}_0$ που ικανοποιούν τα αξιώματα (Φ1), (Φ2) και (Φ3).

Όπως θα δούμε, από αυτά τα αξιώματα μπορούμε να αποδείξουμε όλα τα αποτελέσματα της Αριθμητικής, να κατασκευάσουμε τους ακεραίους και, στο επόμενο κεφάλαιο, τους ρητούς και τους πραγματικούς αριθμούς. Επίσης, όπως έχουμε ήδη αναφέρει, το αξίωμα (Φ3), το οποίο λέγεται **αρχή της επαγωγής**, θα μας δώσει τη δυνατότητα της απόδειξης προτάσεων με επαγωγή. Ένα πρώτο παράδειγμα μας δίνει η επόμενη πρόταση.

Πρόταση 3.2.1. *Εάν $n \in \mathbb{N}_0$, $n \neq 0$, τότε υπάρχει μοναδικό στοιχείο m του $\mathbb{N}_0$ τέτοιο ώστε $n = \varepsilon(m)$.*

Απόδειξη. Θεωρούμε το σύνολο

$$S = \{n \in \mathbb{N}_0 \mid n = 0 \text{ ή } n = \varepsilon(m) \text{ για κάποιο } m \in \mathbb{N}_0\}.$$

Αυτό το οποίο θέλουμε να δείξουμε είναι ότι $S = \mathbb{N}_0$. Παρατηρούμε ότι:

1. Από τον ορισμό του S έχουμε $0 \in S$.
2. Εάν $n \in S$, τότε από τον ορισμό του S έχουμε ότι $\varepsilon(n) \in S$.

Συνεπώς, από το αξίωμα (Φ3), $S = \mathbb{N}_0$. Αυτό δείχνει ότι για κάθε $n \in \mathbb{N}_0 \setminus \{0\}$ υπάρχει $m \in \mathbb{N}_0$ τέτοιο ώστε $n = \varepsilon(m)$. Τέλος, εφαρμόζοντας το αξίωμα (Φ2) παίρνουμε τη μοναδικότητα: εάν $n = \varepsilon(m)$ και $n = \varepsilon(m')$ για κάποιους $m, m' \in \mathbb{N}_0$, τότε $\varepsilon(m) = \varepsilon(m')$ και από το (Φ2) έχουμε ότι $m = m'$. □

Σύμφωνα με την Πρόταση 3.2.1 το 0 είναι το μοναδικό στοιχείο του $\mathbb{N}_0$ το οποίο δεν είναι *επόμενο* κάποιου άλλου στοιχείου του $\mathbb{N}_0$. Μπορούμε τώρα να ορίσουμε το σύνολο $\mathbb{N} = \mathbb{N}_0 \setminus \{0\}$. Ορίζουμε επίσης $1 := \varepsilon(0)$. Τότε, $1 \in \mathbb{N}$.

Η απόδειξη της Πρότασης 3.2.1 ακολούθησε τα εξής τα βήματα: ορίσαμε κάποιο σύνολο $S \subseteq \mathbb{N}_0$ και δείξαμε ότι:

1. $0 \in S$,
2. εάν $n \in S$ τότε $\varepsilon(n) \in S$.

Από το αξίωμα (Φ3) συμπεράναμε ότι $S = \mathbb{N}_0$.

Όλες οι *επαγωγικές αποδείξεις* έχουν αυτή τη δομή. Κάθε φορά, το σύνολο S είναι της μορφής

$$S = \{n \in \mathbb{N}_0 \mid P(n)\},$$

όπου $P(n)$ είναι μια πρόταση που είναι αληθής ή ψευδής για κάθε $n \in \mathbb{N}_0$. Τότε, τα βήματα της απόδειξης είναι τα εξής:

(α) Δείχνουμε ότι η πρόταση $P(0)$ είναι αληθής.

(β) Δείχνουμε ότι εάν η πρόταση $P(n)$ είναι αληθής τότε και η πρόταση $P(\varepsilon(n))$ είναι αληθής.

Επικαλούμαστε τότε το αξίωμα (Φ3) για να συμπεράνουμε ότι η πρόταση $P(n)$ είναι αληθής για κάθε $n \in \mathbb{N}_0$. Αυτό που κάνουμε στην πράξη είναι να αιτιολογήσουμε τα βήματα (α) και (β) και στη συνέχεια λέμε ότι «με επαγωγή η $P(n)$ αληθεύει για κάθε n». Η έκφραση «με επαγωγή» υποδηλώνει ότι επικαλούμαστε κάποιο αξίωμα, το *αξίωμα της επαγωγής*. Στο

βήμα (β) η απόδειξη της $P(n) \implies P(\varepsilon(n))$ ονομάζεται *επαγωγικό βήμα* και η υπόθεση ότι η $P(n)$ είναι αληθής ονομάζεται *επαγωγική υπόθεση*.

Η «απόδειξη» που περιγράψαμε για την Πρόταση 3.1.1 είχε ακριβώς αυτή τη δομή, με μόνη διαφορά ότι ξεκινήσαμε από την πρόταση $P(1)$ και όχι κάποια $P(0)$. Η διαφορά αυτή δεν είναι ουσιαστική: στη συνέχεια θα δούμε διάφορες παραλλαγές της «επαγωγικής απόδειξης». Συνεπώς, τώρα πια, η απόδειξη της Πρότασης 3.1.1 που περιγράψαμε είναι ένα τυπικό παράδειγμα απόδειξης με επαγωγή.

3.2.1 Αναδρομικοί ορισμοί

Θέλουμε να ορίσουμε την πράξη της πρόσθεσης φυσικών αριθμών ξεκινώντας από την συνάρτηση ε του επόμενου. Για κάθε $m \in \mathbb{N}_0$ θέτουμε

$$m + 0 = m$$

και στη συνέχεια ορίζουμε τον $m + \varepsilon(n)$ χρησιμοποιώντας τον $m + n$ και θέτοντας

$$m + \varepsilon(n) = \varepsilon(m + n).$$

Το επόμενο βασικό θεώρημα εξασφαλίζει ότι μπορούμε όντως να ορίζουμε συναρτήσεις χρησιμοποιώντας μια τέτοια αναδρομική διαδικασία.

Θεώρημα 3.2.2 (θεώρημα αναδρομής)**.** *Έστω X ένα σύνολο, $f : X \to X$ μια συνάρτηση και $c \in X$. Τότε, υπάρχει μοναδική συνάρτηση $\varphi : \mathbb{N}_0 \to X$ τέτοια ώστε*

(α) $\varphi(0) = c$,

(β) $\varphi(\varepsilon(n)) = f(\varphi(n))$ *για κάθε* $n \in \mathbb{N}_0$.

Απόδειξη. Μια συνάρτηση $\varphi : \mathbb{N}_0 \to X$ είναι ένα υποσύνολο $\varphi \subseteq \mathbb{N}_0 \times X$ με τις εξής ιδιότητες:

(i) Για κάθε $n \in \mathbb{N}_0$ υπάρχει $x \in X$ τέτοιο ώστε $(n, x) \in \varphi$,

(ii) Εάν $(n, x) \in \varphi$ και $(n, y) \in \varphi$ τότε $x = y$.

Συνεπώς, για να βρούμε μια συνάρτηση φ που να ικανοποιεί τις απαιτήσεις του θεωρήματος, πρέπει να προσδιορίσουμε $\varphi \subseteq \mathbb{N}_0 \times X$ με αυτές τις ιδιότητες, το οποίο επίπλεον να ικανοποιεί τα ακόλουθα:

(α) $(0, c) \in \varphi$,

(β) Εάν $(n, x) \in \varphi$ τότε $(\varepsilon(n), f(x)) \in \varphi$.

Ένα υποσύνολο του $\mathbb{N}_0 \times X$ που ικανοποιεί τα (α) και (β) είναι το ίδιο το $\mathbb{N}_0 \times X$. Αυτό που θα δείξουμε είναι ότι η τομή όλων των $U \subseteq \mathbb{N}_0 \times X$ που ικανοποιούν τα (α) και (β) ικανοποιεί επίσης τα (i) και (ii), άρα είναι η ζητούμενη συνάρτηση.

Θεωρούμε το σύνολο $\mathcal{T}$ όλων των $U \subseteq \mathbb{N}_0 \times X$ που έχουν τις ιδιότητες

$$(0, c) \in U$$

και

$$(n, x) \in U \implies (\varepsilon(n), f(x)) \in U.$$

Έχουμε $\mathcal{T} \neq \varnothing$, διότι $\mathbb{N}_0 \times X \in \mathcal{T}$. Ορίζουμε

$$\varphi = \bigcap \mathcal{T}.$$

Εύκολα ελέγχουμε ότι το σύνολο φ ικανοποιεί τα (α) και (β). Μάλιστα, είναι το μικρότερο σύνολο που ικανοποιεί αυτές τις ιδιότητες. Μένει να δείξουμε ότι οι (i) και (ii) ισχύουν για το φ, δηλαδή ότι το σύνολο φ είναι συνάρτηση.

Θεωρούμε το σύνολο

$$S = \{n \in \mathbb{N}_0 \mid \text{υπάρχει } x \in X \text{ ώστε } (n, x) \in \varphi\}.$$

Από το (α) έχουμε $0 \in S$, και από το (β) έχουμε ότι εάν $n \in S$ τότε $\varepsilon(n) \in S$. Επαγωγικά, συμπεραίνουμε ότι $S = \mathbb{N}_0$, άρα η (i) ικανοποιείται από το φ.

Θεωρούμε τώρα το σύνολο

$$M = \{n \in \mathbb{N}_0 \mid \text{υπάρχει μόνο ένα } x \in X \text{ ώστε } (n, x) \in \varphi\}.$$

Γνωρίζουμε ότι $(0, c) \in \varphi$. Ας υποθέσουμε ότι υπάρχει $d \neq c$ τέτοιο ώστε $(0, d) \in \varphi$. Τότε, ορίζουμε $\varphi_1 = \varphi \setminus \{(0, d)\}$. Παρατηρούμε ότι το φ_1 ικανοποιεί το (α) διότι $(0, c) \in \varphi_1$. Επίσης, εάν $(n, x) \in \varphi_1$ τότε $(\varepsilon(n), f(x)) \in \varphi$ και $(\varepsilon(n), f(x)) \neq (0, d)$ διότι $\varepsilon(n) \neq 0$, άρα $(\varepsilon(n), f(x)) \in \varphi_1$. Αυτό αποδεικνύει ότι το φ_1 ικανοποιεί και το (β). Όμως, το φ_1 είναι γνήσιο υποσύνολο του φ, άρα έχουμε καταλήξει σε άτοπο. Έτσι, συμπεραίνουμε ότι $0 \in M$.

Για το επαγωγικό βήμα, υποθέτουμε ότι $n \in M$, δηλαδή υπάρχει μοναδικό $x \in X$ τέτοιο ώστε $(n, x) \in \varphi$. Γνωρίζουμε ότι $(\varepsilon(n), f(x)) \in \varphi$ και για να δείξουμε ότι $\varepsilon(n) \in M$ αρκεί να δείξουμε ότι δεν υπάρχει $y \neq f(x)$ στο X τέτοιο ώστε $(\varepsilon(n), y) \in \varphi$. Εάν υποθέσουμε ότι υπάρχει τέτοιο $(\varepsilon(n), y) \in \varphi$, θεωρούμε το $\varphi_2 = \varphi \setminus \{(\varepsilon(n), y)\}$. Παρατηρούμε ότι το φ_2 ικανοποιεί το (α) διότι $(0, c) \in \varphi$ και $(0, c) \neq (\varepsilon(n), y)$. Για να δείξουμε ότι το φ_2 ικανοποιεί το (β) πρέπει να ελέγξουμε ότι η συνεπαγωγή

$$(m, z) \in \varphi_2 \implies (\varepsilon(m), f(z)) \in \varphi_2$$

ισχύει για κάθε $m \in \mathbb{N}_0$. Για $m = n$ αυτό ισχύει, διότι υπάρχει μοναδικό $x \in X$ τέτοιο ώστε $(n, x) \in \varphi$ και γι' αυτό το x έχουμε $(\varepsilon(n), f(x)) \in \varphi$ και δεν ισχύει $(\varepsilon(n), f(x)) = (\varepsilon(n), y)$ διότι $y \neq f(x)$. Για $m \neq n$ έχουμε $(\varepsilon(m), f(z)) \in \varphi$ και $\varepsilon(m) \neq \varepsilon(n)$, άρα $(\varepsilon(m), f(x)) \neq (\varepsilon(n), y)$, άρα $(\varepsilon(m), f(z)) \in \varphi_2$. Είδαμε ότι, σε όλες τις περιπτώσεις, το φ_2 ικανοποιεί το (β), και αφού το φ_2 είναι γνήσιο υποσύνολο του φ έχουμε καταλήξει σε άτοπο. Επαγωγικά, συμπεραίνουμε ότι $M = \mathbb{N}_0$, άρα το σύνολο φ ικανοποιεί και το (ii). □

Εφαρμόζοντας το θεώρημα αναδρομής μπορούμε να δώσουμε τους παρακάτω ορισμούς:

Πρόσθεση: Για κάθε $m \in \mathbb{N}_0$ ορίζουμε αναδρομικά συνάρτηση $\varphi_m : \mathbb{N}_0 \to \mathbb{N}_0$ με

$$\varphi_m(0) = m \quad \text{και} \quad \varphi_m(\varepsilon(n)) = \varepsilon(\varphi_m(n)).$$

Σε αυτή την περίπτωση εφαρμόζουμε το θεώρημα αναδρομής με $X = \mathbb{N}_0$, $c = m$ και $f = \varepsilon$. Τέλος, ορίζουμε

$$m + n := \varphi_m(n).$$

Πολλαπλασιασμός: Για κάθε $m \in \mathbb{N}_0$ ορίζουμε αναδρομικά συνάρτηση $\mu_m : \mathbb{N}_0 \to \mathbb{N}_0$ με

$$\mu_m(0) = 0 \quad \text{και} \quad \mu_m(\varepsilon(n)) = \mu_m(n) + m.$$

Σε αυτή την περίπτωση εφαρμόζουμε το θεώρημα αναδρομής με $X = \mathbb{N}_0$, $c = 0$ και $f(r) = r + m$. Τέλος, ορίζουμε

$$mn := \mu_m(n).$$

Δυνάμεις: Για κάθε $m \in \mathbb{N}$ ορίζουμε αναδρομικά συνάρτηση $\pi_m : \mathbb{N}_0 \to \mathbb{N}$ με

$$\pi_m(0) = 1 \quad \text{και} \quad \pi_m(\varepsilon(n)) = \pi_m(n)m.$$

Σε αυτή την περίπτωση εφαρμόζουμε το θεώρημα αναδρομής με $X = \mathbb{N}$, $c = 1$ και $f(r) = rm$. Τέλος, ορίζουμε

$$m^n := \pi_m(n).$$

Επαναλαμβανόμενη σύνθεση: Για κάθε συνάρτηση $g : A \to A$ ορίζουμε

$$g^0(x) = x$$
$$g^{\varepsilon(n)}(x) = g(g^n(x))$$

για κάθε $x \in A$. Εδώ $X = A^A$, το σύνολο των συναρτήσεων από το A στο A, $c = id_A$ και $F : A^A \to A^A$ η συνάρτηση με $F(h) = g \circ h$, για κάθε $h \in A^A$.

3.2.2 Κανόνες της Αριθμητικής

Στόχος μας σε αυτή την ενότητα είναι να αποδείξουμε ότι οι πράξεις της πρόσθεσης και του πολλαπλασιασμού, όπως έχουν οριστεί, ικανοποιούν τους γνωστούς κανόνες της αριθμητικής. Το βασικό εργαλείο μας θα είναι η επαγωγή.

Γνωρίζουμε, από τον ορισμό, ότι η πρόσθεση έχει τις ιδιότητες

(Π1) $m + 0 = m$,

(Π2) $m + \varepsilon(n) = \varepsilon(m + n)$,

και ο πολλαπλασιασμός έχει τις ιδιότητες

(Γ1) $m0 = 0$,

(Γ2) $m\varepsilon(n) = mn + m$.

Από τις (Π1) και (Π2) βλέπουμε ότι

$$m + \varepsilon(0) = \varepsilon(m + 0) = \varepsilon(m).$$

Συμβολίζουμε το $\varepsilon(0)$ με 1, συνεπώς μπορούμε να γράφουμε $\varepsilon(m) = m + 1$.

Λήμμα 3.2.3. *Για κάθε $m \in \mathbb{N}_0$ ισχύουν τα ακόλουθα:*

1. $0 + m = m$.
2. $1 + m = \varepsilon(m)$.
3. $0m = 0$.
4. $1m = m$.

Απόδειξη. Με επαγωγή ως προς m. Ενδεικτικά, δίνουμε το επιχείρημα για το πρώτο. Θεωρούμε το σύνολο

$$S = \{m \in \mathbb{N}_0 \mid 0 + m = m\}.$$

Από την (Π1) έχουμε $0 \in S$. Εάν $m \in S$ τότε $0 + m = m$, άρα από την (Π2) έχουμε $0 + \varepsilon(m) = \varepsilon(0 + m) = \varepsilon(m)$, δηλαδή $\varepsilon(m) \in S$. Από το (Φ3) συμπεραίνουμε ότι $S = \mathbb{N}_0$. □

Θεώρημα 3.2.4. *Για κάθε $m, n, p \in \mathbb{N}_0$ ισχύουν τα ακόλουθα:*

1. *Προσεταιριστική ιδιότητα της πρόσθεσης:*

$$(m + n) + p = m + (n + p).$$

2. *Μεταθετική ιδιότητα της πρόσθεσης:*

$$m + n = n + m.$$

3. *Προσεταιριστική ιδιότητα του πολλαπλασιασμού:*

$$(mn)p = m(np).$$

4. *Μεταθετική ιδιότητα του πολλαπλασιασμού:*

$$mn = nm.$$

5. *Επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση:*

$$m(n + p) = mn + mp.$$

Απόδειξη. Η προσεταιριστική ιδιότητα της πρόσθεσης αποδεικνύεται με επαγωγή ως προς p. Σταθεροποιούμε τους $m, n \in \mathbb{N}_0$ και θεωρούμε το σύνολο

$$S = \{p \in \mathbb{N}_0 \mid (m + n) + p = m + (n + p)\}.$$

Παρατηρούμε ότι

$$\begin{aligned} (m + n) + 0 &= m + n && \text{από την (Π1)} \\ &= m + (n + 0) && \text{από την (Π1)} \end{aligned}$$

Συνεπώς, $0 \in S$.
Υποθέτουμε τώρα ότι $p \in S$, δηλαδή

$$(m + n) + p = m + (n + p). \tag{3.2.1}$$

Χρησιμοποιώντας τρεις φορές την (Π2) βλέπουμε ότι

$$\begin{aligned} (m + n) + \varepsilon(p) &= \varepsilon((m + n) + p) && \text{από την (Π2)} \\ &= \varepsilon(m + (n + p)) && \text{από την Επαγωγική Υπόθεση (3.2.1)} \\ &= m + \varepsilon(n + p) && \text{από την (Π2)} \\ &= m + (n + \varepsilon(p)) && \text{από την (Π2)} \end{aligned}$$

άρα $\varepsilon(p) \in S$. Επαγωγικά, συμπεραίνουμε ότι $S = \mathbb{N}_0$.

Η μεταθετική ιδιότητα της πρόσθεσης αποδεικνύεται με επαγωγή ως προς n. Σταθεροποιούμε τον $m \in \mathbb{N}_0$ και θεωρούμε το σύνολο

$$S = \{n \in \mathbb{N}_0 \mid m + n = n + m\}.$$

Από το Λήμμα 3.2.3 (1) έχουμε ότι $0 \in S$. Εάν $n \in S$, τότε

$$m + n = n + m, \tag{3.2.2}$$

και

$$\begin{aligned}
m + \varepsilon(n) &= \varepsilon(m + n) && \text{από την (Π2)} \\
&= \varepsilon(n + m) && \text{από την Επαγωγική Υπόθεση (3.2.2)} \\
&= n + \varepsilon(m) && \text{από την (Π2)} \\
&= n + (1 + m) && \text{από το Λήμμα 3.2.3 (2)} \\
&= (n + 1) + m && \text{από το Θεώρημα 3.2.4 (1)} \\
&= \varepsilon(n) + m,
\end{aligned}$$

άρα $\varepsilon(n) \in S$. Επαγωγικά, συμπεραίνουμε ότι $S = \mathbb{N}_0$.

Αποδεικνύουμε τώρα την επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση, χρησιμοποιώντας επαγωγή ως προς p. Σταθεροποιούμε τους $m, n \in \mathbb{N}_0$ και θεωρούμε το σύνολο

$$S = \{p \in \mathbb{N}_0 \mid m(n + p) = mn + mp\}.$$

Τότε,

$$\begin{aligned}
m(n + 0) &= mn && \text{από την (Π1)} \\
&= mn + 0 && \text{από την (Π1)} \\
&= mn + m0 && \text{από την (Γ1)}
\end{aligned}$$

άρα $0 \in S$. Εάν $p \in S$, τότε

$$m(n + p) = mn + mp, \tag{3.2.3}$$

άρα

$$\begin{aligned} m(n+\varepsilon(p)) &= m\varepsilon(n+p) && \text{από την (Π2)} \\ &= m(n+p)+m && \text{από την (Γ2)} \\ &= (mn+mp)+m && \text{από την Επαγωγική Υπόθεση (3.2.3)} \\ &= mn+(mp+m) && \text{από το Θεώρημα 3.2.4 (1)} \\ &= mn+m\varepsilon(p) && \text{από την (Γ2)} \end{aligned}$$

και αυτό αποδεικνύει ότι $\varepsilon(p) \in S$. Επαγωγικά, συμπεραίνουμε ότι $S = \mathbb{N}_0$.

Παραλείπουμε την απόδειξη της προσεταιριστικής ιδιότητας του πολλαπλασιασμού, η οποία είναι παρόμοια με τις προηγούμενες, και αποδεικνύουμε την μεταθετική ιδιότητα του πολλαπλασιασμού με επαγωγή ως προς n. Θεωρούμε το σύνολο

$$S = \{n \in \mathbb{N}_0 \mid mn = nm, \text{ για κάθε } m \in \mathbb{N}_0\}.$$

Από το Λήμμα 3.2.3 (3) έχουμε ότι $0 \in S$. Εάν $n \in S$ τότε, για κάθε $m \in \mathbb{N}_0$,

$$mn = nm, \tag{3.2.4}$$

και έχουμε

$$\begin{aligned} m\varepsilon(n) &= mn+m && \text{από την (Γ2)} \\ &= nm+m && \text{από την (3.2.4).} \end{aligned}$$

Αυτό που πρέπει να δείξουμε είναι ότι $nm+m = \varepsilon(n)m$. Θα χρησιμοποιήσουμε μία ακόμη επαγωγή, αυτή τη φορά ως προς m. Σταθεροποιούμε το n και θεωρούμε το σύνολο

$$M = \{m \in \mathbb{N}_0 \mid nm+m = \varepsilon(n)m\}.$$

Παρατηρήστε ότι $0 \in M$. Εάν $m \in M$ τότε

$$nm+m = \varepsilon(n)m \tag{3.2.5}$$

και

$$\begin{aligned}
n\varepsilon(m)+\varepsilon(m) &= n(m+1)+(m+1) \\
&= (nm+n)+(m+1) && \text{από την Επαγωγική Υπόθεση (3.2.5)} \\
&= nm+(n+(m+1)) && \text{από το Θεώρημα 3.2.4 (1)} \\
&= nm+((n+m)+1) && \text{από το Θεώρημα 3.2.4 (1)} \\
&= nm+((m+n)+1) && \text{από το Θεώρημα 3.2.4 (2)} \\
&= nm+(m+(n+1)) && \text{από το Θεώρημα 3.2.4 (1)} \\
&= (nm+m)+(n+1) && \text{από το Θεώρημα 3.2.4 (1)} \\
&= \varepsilon(n)m+\varepsilon(n) && \text{από την Επαγωγική Υπόθεση (3.2.5)} \\
&= \varepsilon(n)\varepsilon(m) && \text{από την (Γ2),}
\end{aligned}$$

άρα $\varepsilon(m) \in M$. Επαγωγικά, συμπεραίνουμε ότι $M = \mathbb{N}_0$. Επιστρέφοντας στην προηγούμενη επαγωγή, έχουμε τώρα ότι $\varepsilon(n) \in S$, άρα τελικά $S = \mathbb{N}_0$ και η απόδειξη της μεταθετικής ιδιότητας του πολλαπλασιασμού είναι πλήρης. □

Έχοντας στη διάθεσή μας το Θεώρημα 3.2.4 μπορούμε πλέον να εφαρμόζουμε ελεύθερα τους κανόνες της αριθμητικής. Αντικαθιστούμε τον $\varepsilon(n)$ με $n+1$ και γράφουμε το αξίωμα (Φ3) της επαγωγής στη συνηθισμένη του μορφή:

> Εάν το $S \subseteq \mathbb{N}_0$ είναι τέτοιο ώστε $0 \in S$ και $(n \in S \implies n+1 \in S)$, τότε $S = \mathbb{N}_0$.

Το αξίωμα (Φ2) παίρνει τη μορφή

$$m+1 = n+1 \implies m = n,$$

και επαγωγικά μπορούμε να επεκτείνουμε αυτή την πρόταση ως εξής.

Πρόταση 3.2.5. *Για κάθε $m, n, q \in \mathbb{N}_0$ ισχύουν τα ακόλουθα:*

1. $m+q = n+q \implies m = n$.
2. *Εάν $q \neq 0$ και $mq = nq$ τότε $m = n$.*

Απόδειξη. Για τον πρώτο ισχυρισμό χρησιμοποιούμε επαγωγή ως προς q. Θεωρούμε το σύνολο

$$S = \{q \in \mathbb{N}_0 \mid \text{για κάθε } m, n \in \mathbb{N}_0, \text{ ισχύει η συνεπαγωγή : } m+q = n+q \implies m = n\}.$$

Παρατηρούμε ότι $0 \in S$. Εάν $q \in S$, υποθέτουμε ότι, για κάποια $m, n \in \mathbb{N}_0$, ισχύει

$$(m + (q + 1) = n + (q + 1)$$

και από το Θεώρημα 3.2.4 έχουμε

$$(m + q) + 1 = (n + q) + 1,$$

οπότε το αξίωμα (Φ2) μας δίνει

$$m + q = n + q,$$

και από την υπόθεση ότι $q \in S$ συμπεραίνουμε ότι

$$m = n.$$

Άρα, $q + 1 \in S$ και επαγωγικά συμπεραίνουμε ότι $S = \mathbb{N}_0$.

Για τον δεύτερο ισχυρισμό χρησιμοποιούμε επαγωγή ως προς m. Θεωρούμε το σύνολο

$$S = \{m \in \mathbb{N}_0 \mid \text{για κάθε } n \in \mathbb{N}_0,\ q \in \mathbb{N},\ \text{ισχύει η συνεπαγωγή :}\ mq = nq \implies m = n\}.$$

Για να δείξουμε ότι $0 \in S$, υποθέτουμε ότι για κάποιους $n, q \in \mathbb{N}_0$ με $q \neq 0$ ισχύει

$$nq = 0q = 0.$$

Έχουμε $q = p + 1$ για κάποιον $p \in \mathbb{N}_0$. Εάν $n \neq 0$ τότε έχουμε επίσης $n = r + 1$ για κάποιον $r \in \mathbb{N}_0$, άρα $nq = (pr + p + r) + 1 \neq 0$, άτοπο. Συνεπώς, $n = 0$. Έπεται ότι $0 \in S$.

Έστω τώρα ότι $m \in S$ και ότι, για για κάποιους $n, q \in \mathbb{N}_0$ με $q \neq 0$, ισχύει

$$(m + 1)q = nq.$$

Όπως πριν, βλέπουμε ότι $n \neq 0$ άρα $n = r + 1$ για κάποιον $r \in \mathbb{N}_0$. Τότε, $mq + q = rq + q$. Από τον πρώτο ισχυρισμό της πρότασης έχουμε ότι $mq = rq$, και από την επαγωγική υπόθεση παίρνουμε $m = r$. Συνεπώς, $m + 1 = r + 1 = n$. Αυτό ολοκληρώνει την απόδειξη. □

Αφαίρεση. Μπορούμε τώρα να συζητήσουμε την πράξη της *αφαίρεσης*. Εάν $p = r + q$ τότε από την Πρόταση 3.2.5(1) ο r προσδιορίζεται μονοσήμαντα από τους p και q, μπορούμε λοιπόν να τον συμβολίζουμε με

$$p - q.$$

Για κάθε $m, n \in \mathbb{N}_0$ ορίζουμε

$$m \geqslant n \ \text{ αν και μόνο αν υπάρχει } \ r \in \mathbb{N}_0 : m = r + n.$$

Για δεδομένους $m, n \in \mathbb{N}_0$, η *διαφορά* $m - n$ ορίζεται μόνο όταν $m \geqslant n$. Εύκολα επαληθεύουμε τους παρακάτω κανόνες για την αφαίρεση:

(α) Εάν $m \geqslant n \geqslant r$ τότε $m - (n - r) = (m - n) + r$.

(β) Εάν $n \geqslant r$ τότε $m + (n - r) = (m + n) - r$.

(γ) Εάν $n \geqslant r$ τότε $m(n - r) = mn - mr$.

Για παράδειγμα, αποδεικνύουμε το (γ): Έχουμε $n \geqslant r$, άρα μπορούμε να γράψουμε $n = s + r$ όπου $s = n - r$. Τότε,

$$mn = m(s + r) = ms + mr,$$

και από τον ορισμό της διαφοράς παίρνουμε

$$mn - mr = ms = m(n - r).$$

Διαίρεση. Μπορούμε επίσης να συζητήσουμε την πράξη της *διαίρεσης*: Στην περίπτωση που $m = rn$ για κάποιον $n \in \mathbb{N}$, συμβολίζουμε τον r με m/n.

3.2.3 Διάταξη των φυσικών αριθμών

Στην προηγούμενη ενότητα ορίσαμε την σχέση $\geqslant$ στο $\mathbb{N}_0$:

$$m \geqslant n \iff \text{υπάρχει } r \in \mathbb{N}_0 \text{ ώστε } m = r + n.$$

Ορίζουμε τώρα την αντίστροφη σχέση $\leqslant$:

$$m \leqslant n \iff n \geqslant m,$$

καθώς και τις $>$ και $<$:

$$m > n \iff m \geqslant n \text{ και } m \neq n,$$
$$m < n \iff n > m.$$

Θα δείξουμε ότι οι σχέσεις $\geqslant$ και $\leqslant$ είναι σχέσεις διάταξης, οπότε οι $>$ και $<$ είναι οι αντίστοιχες αυστηρές διατάξεις. Ξεκινάμε από την $\geqslant$. Είναι φανερό ότι αυτή είναι ανακλαστική αφού $m = 0 + m$ για κάθε $m \in \mathbb{N}_0$. Δείχνουμε τώρα ότι είναι μεταβατική και αντισυμμετρική.

Πρόταση 3.2.6. *Για κάθε $m, n, p \in \mathbb{N}_0$ ισχύει ότι: εάν $m \geqslant n$ και $n \geqslant p$ τότε $m \geqslant p$.*

Απόδειξη. Υπάρχουν r και s στο $\mathbb{N}_0$ τέτοιοι ώστε $m = r + n$ και $n = s + p$. Τότε,

$$m = r + (s + p) = (r + s) + p,$$

συνεπώς $m \geqslant p$. □

Πρόταση 3.2.7. *Για κάθε $m, n \in \mathbb{N}_0$ ισχύει ότι: εάν $m \geqslant n$ και $n \geqslant m$ τότε $m = n$.*

Απόδειξη. Υπάρχουν $r, t \in \mathbb{N}_0$ τέτοιοι ώστε $m = r + n$ και $n = t + m$, άρα $m = r + t + m$. Από την Πρόταση 3.2.5 (1) έπεται ότι $r + t = 0$. Εάν $t \neq 0$ τότε $t = q + 1$ για κάποιον $q \in \mathbb{N}_0$, άρα $0 = (r + q) + 1$, το οποίο είναι άτοπο από το αξίωμα (Φ1). Συνεπώς, $t = 0$ και έχουμε $n = m$. □

Η επόμενη πρόταση δείχνει ότι η $\geqslant$ συμπεριφέρεται καλά ως προς τις πράξεις της πρόσθεσης και του πολλαπλασιασμού στο $\mathbb{N}_0$.

Πρόταση 3.2.8. *Για κάθε $m, n, p, q \in \mathbb{N}_0$ ισχύουν τα ακόλουθα:*

1. *Εάν $m \geqslant n$ και $p \geqslant q$ τότε $m + p \geqslant n + q$.*
2. *Εάν $m \geqslant n$ και $p \geqslant q$ τότε $mp \geqslant nq$.*

Απόδειξη. Για τον πρώτο ισχυρισμό παρατηρούμε ότι υπάρχουν $r, s \in \mathbb{N}_0$ τέτοιοι ώστε $m = r+n$ και $p = s+q$, οπότε παίρνουμε $m+p = (r+s)+(n+q)$ και έτσι έχουμε $m+p \geqslant n+q$. Για τον δεύτερο ισχυρισμό, με τον ίδιο τρόπο βλέπουμε ότι $mp = nq + (rs + ns + rq)$, άρα $mp \geqslant nq$. □

Ο 0 είναι το μικρότερο στοιχείο του $\mathbb{N}_0$, με την ακόλουθη έννοια:

Λήμμα 3.2.9. *Εάν $m \in \mathbb{N}_0$ τότε $m \geqslant 0$.*

Απόδειξη. Παρατηρούμε ότι $m = m + 0$. □

Ο 1 είναι το αμέσως επόμενο μικρότερο στοιχείο του $\mathbb{N}_0$:

Λήμμα 3.2.10. *Εάν $m \in \mathbb{N}_0$ και $m > 0$ τότε $m \geqslant 1$.*

Απόδειξη. Εάν $m \neq 0$ τότε $m = q + 1$ για κάποιον $q \in \mathbb{N}_0$, άρα $m \geqslant 1$. □

Γενικότερα, ισχύει η ακόλουθη πρόταση.

Πρόταση 3.2.11. *Εάν $m, n \in \mathbb{N}_0$ και $m > n$ τότε $m \geqslant n + 1$.*

Απόδειξη. Έχουμε $m = r + n$ για κάποιον $r \in \mathbb{N}_0$ και $r \neq 0$ από την υπόθεση ότι $m > n$ (άρα $m \neq n$). Συνεπώς, $r = q + 1$ για κάποιον $q \in \mathbb{N}_0$, απ' όπου παίρνουμε ότι $m = q + (n + 1)$ και συνεπώς $m \geqslant n + 1$. □

Μπορούμε τώρα να δείξουμε ότι η $\geqslant$ είναι ολική διάταξη.

Πρόταση 3.2.12. *Η σχέση $\geqslant$ είναι ολική διάταξη στο $\mathbb{N}_0$.*

Απόδειξη. Έχουμε ήδη αποδείξει ότι η $\geqslant$ είναι ανακλαστική, μεταβατική και αντισυμμετρική. Αρκεί λοιπόν να δείξουμε ότι για κάθε $m, n \in \mathbb{N}_0$ ισχύει μία από τις $m \geqslant n$ ή $n \geqslant m$ ή και οι δύο.

Σταθεροποιούμε το $m \in \mathbb{N}_0$, θεωρούμε το σύνολο

$$S(m) = \{n \in \mathbb{N}_0 \mid m \geqslant n \text{ ή } n \geqslant m\}$$

και δείχνουμε ότι $S(m) = \mathbb{N}_0$: Από την $m \geqslant 0$ βλέπουμε άμεσως ότι $0 \in S(m)$. Υποθέτουμε τώρα ότι $n \in S(m)$. Τότε είτε $m \geqslant n$ είτε $n \geqslant m$. Εάν $n \geqslant m$ τότε $n + 1 \geqslant m$, Εάν $m \geqslant n$ τότε είτε $m = n$ και έχουμε $n+1 \geqslant m$, είτε $m > n$ οπότε $m \geqslant n+1$ από την Πρόταση 3.2.11. Σε κάθε περίπτωση, $n + 1 \in S(m)$ και επαγωγικά συμπεραίνουμε ότι $S(m) = \mathbb{N}_0$. □

Έπεται ότι η σχέση $>$ είναι αυστηρή διάταξη και ικανοποιεί την τριχοτομία:

Για κάθε $m, n \in \mathbb{N}_0$ αληθεύει ακριβώς μία από τις $m > n$ ή $m = n$ ή $n > m$.

Τέλος, αποδεικνύουμε το εξής.

Πρόταση 3.2.13. *Για κάθε $m, n, q \in \mathbb{N}_0$ ισχύουν τα ακόλουθα:*

1. $m + q > n + q \implies m > n$.
2. *Εάν $q \neq 0$ και $mq > nq$ τότε $m > n$.*

Απόδειξη. Για τον πρώτο ισχυρισμό παρατηρούμε ότι εάν δεν ισχύει η $m > n$ τότε από την τριχοτομία έχουμε $m \geqslant n$. Όμως τότε, από την Πρόταση 3.2.8 έχουμε ότι $m+q \leqslant n+q$ για κάθε $q \in \mathbb{N}_0$, το οποίο αντιφάσκει προς την υπόθεση. Ο δεύτερος ισχυρισμός αποδεικνύεται με παρόμοιο τρόπο. □

Ανάλογη πρόταση ισχύει, και αποδεικνύεται με τον ίδιο τρόπο, εάν αντικαταστήσουμε την σχέση $>$ με την σχέση $\geqslant$.

3.2.4 Παραλλαγές της επαγωγής

Πολύ χρήσιμες είναι οι ακόλουθες παραλλαγές της αρχής της επαγωγής:

(i) Έστω $m \in \mathbb{N}_0$ και έστω $S \subseteq \mathbb{N}_0$ με τις εξής ιδιότητες: (α) $m \in S$ και (β) για κάθε $n \geqslant m$ που ανήκει στο S έχουμε ότι $n + 1 \in S$. Τότε, $S \supseteq \{n \in \mathbb{N}_0 : n \geqslant m\}$.

(ii) **Ισχυρή μορφή της επαγωγής.** Έστω $S \subseteq \mathbb{N}_0$ με τις εξής ιδιότητες: $0 \in S$ και οποτεδήποτε $0, 1, \ldots, n \in S$ έχουμε και ότι $n + 1 \in S$. Τότε, $S = \mathbb{N}_0$.

Για την απόδειξη της (ii) θεωρούμε το σύνολο

$$T = \{n \in \mathbb{N} : 0 \in S, 1 \in S, \ldots, n \in S\}$$

και αποδεικνύουμε, με την κλασική επαγωγική μέθοδο, ότι $T = \mathbb{N}_0$. Παρατηρήστε ότι $T \subseteq S$, άρα έπεται άμεσα ότι $S = \mathbb{N}_0$.

Ισοδύναμα, έχουμε τα εξής:

(i) Έστω $\Pi(n)$, $n \in \mathbb{N}_0$ προτάσεις, όπου κάθε $\Pi(n)$ εξαρτάται από τον φυσικό n. Αν η $\Pi(m)$ αληθεύει για κάποιον $m \in \mathbb{N}_0$ και αν για κάθε $k \geqslant m$ ισχύει η συνεπαγωγή

$$\Pi(k) \text{ αληθεύει } \implies \Pi(k+1) \text{ αληθεύει,}$$

τότε η $\Pi(n)$ αληθεύει για κάθε φυσικό $n \geqslant m$.

(ii) Έστω $\Pi(n)$, $n \in \mathbb{N}_0$ προτάσεις, όπου κάθε $\Pi(n)$ εξαρτάται από τον φυσικό n. Αν η $\Pi(1)$ αληθεύει και αν για κάθε $k \in \mathbb{N}_0$ ισχύει η συνεπαγωγή

$$\text{οι } \Pi(1), \ldots, \Pi(k) \text{ αληθεύουν } \implies \Pi(k+1) \text{ αληθεύει,}$$

τότε η $\Pi(n)$ αληθεύει για κάθε $n \in \mathbb{N}_0$.

Με τη βοήθεια της ισχυρής μορφής της επαγωγής μπορούμε να αποδείξουμε μια άλλη σημαντική ιδιότητα των φυσικών αριθμών, η οποία χρησιμοποιείται συχνά σε αποδείξεις εναλλακτικά προς την αρχή της επαγωγής.

Θεώρημα 3.2.14 (Αρχή του ελαχίστου)**.** *Κάθε μη κενό υποσύνολο M του $\mathbb{N}_0$ έχει ένα ελάχιστο στοιχείο, δηλαδή υπάρχει στοιχείο του $\mathbb{N}_0$ που ανήκει στο M και είναι μικρότερο ή ίσο από κάθε στοιχείο του M.*

Απόδειξη. Θεωρούμε $M \subseteq \mathbb{N}_0$, $M \neq \varnothing$ και θέλουμε να δείξουμε ότι υπάρχει $a \in M$ τέτοιος ώστε $a \leqslant m$ για κάθε $m \in M$.

Υποθέτουμε ότι δεν υπάρχει τέτοιος a και θα καταλήξουμε σε αντίφαση. Θεωρούμε το σύνολο

$$T = \{n \in \mathbb{N}_0 \mid n \notin M\} = \mathbb{N}_0 \setminus M.$$

Παρατηρούμε ότι $0 \in T$. Πράγματι, αν είχαμε $0 \notin T$ τότε θα είχαμε $0 \in M$ και θα καταλήγαμε σε άτοπο διότι ο 0 θα ήταν το ελάχιστο στοιχείο του M.

Υπθέτουμε ότι, για κάποιον $n \in \mathbb{N}_0$, ισχύει $k \in T$ για κάθε $k \leqslant n$. Δηλαδή, για κάθε $k \leqslant n$, ισχύει $k \notin M$. Εάν $n+1 \in M$ τότε ο $n+1$ είναι το ελάχιστο στοιχείο του M και οδηγούμαστε σε αντίφαση. Συνεπώς, $n+1 \notin M$. Δηλαδή, $n+1 \in T$.

Από την ισχυρή μορφή της επαγωγής έπεται ότι $T = \mathbb{N}_0$, συνεπώς $M = \varnothing$ και έχουμε αντίφαση προς την υπόθεση του θεωρήματος. Άρα, το M έχει ελάχιστο στοιχείο. □

3.3 Ακέραιοι αριθμοί

3.3.1 Το σύνολο των ακεραίων

Για να κατασκευάσουμε τους ακέραιους αριθμούς από τους φυσικούς, πρέπει να ορίσουμε με κάποιον τρόπο τους αρνητικούς ακέραιους. Η ιδέα είναι να θεωρήσουμε διαφορές $m-n$ φυσικών αριθμών, όμως ως τώρα έχουμε μιλήσει για τον $m-n$ μόνο στην περίπτωση όπου $m \geqslant n$, οπότε ο $m-n$ είναι ο μοναδικός $r \in \mathbb{N}_0$ για τον οποίο ισχύει $m = n + r$.

Παρατηρούμε ότι αν $m, n, r, s \in \mathbb{N}_0$ και $m \geqslant n$, $r \geqslant s$ τότε

$$m - n = r - s \iff m + s = n + r.$$

Η δεξιά ισότητα έχει νόημα χωρίς να υποθέσουμε ότι $m \geqslant n$ και $r \geqslant s$, δηλαδή χωρίς κανένα περιορισμό στους m, n, r, s. Η ιδέα που θα χρησιμοποιήσουμε για να ορίσουμε τους ακέραιους αριθμούς ως διαφορές $m-n$ είναι να θεωρήσουμε το σύνολο $\mathbb{N}_0 \times \mathbb{N}_0$ των διατεταγμένων ζευγών (m, n), όπου $m, n \in \mathbb{N}_0$, και να ορίσουμε σε αυτό την σχέση

$$(m, n) \sim (r, s) \iff m + s = r + n. \tag{3.3.1}$$

Είναι εύκολο (και αφήνεται ως άσκηση) να δείξουμε το ακόλουθο λήμμα.

Λήμμα 3.3.1. *Η* (3.3.1) *είναι σχέση ισοδυναμίας στο* $\mathbb{N}_0 \times \mathbb{N}_0$.

Ορίζουμε τώρα $\mathbb{Z}$ να είναι το σύνολο των κλάσεων ισοδυναμίας που ορίζει η σχέση $\sim$. Η κλάση ισοδυναμίας ενός ζεύγους (m, n) αντιστοιχεί στην διαισθητική μας ιδέα για την διαφορά $m - n$ (η οποία τώρα μπορεί να είναι και «αρνητική»).

Πιο αυστηρά, για κάθε $(m, n) \in \mathbb{N}_0 \times \mathbb{N}_0$ συμβολίζουμε με $\langle m, n\rangle$ την κλάση ισοδυναμίας στην οποία ανήκει το (m, n). Από τον ορισμό της $\sim$ έχουμε

$$\langle m, n\rangle = \langle r, s\rangle \iff m + s = n + r.$$

Για παράδειγμα,

$$\langle 2, 7\rangle = \langle 6, 11\rangle = \langle 23, 28\rangle$$

(και η κλάση αυτή θα παίξει πολύ σύντομα το ρόλο του -5).

Πρόσθεση και πολλαπλασιασμός στο $\mathbb{Z}$. Ορίζουμε τις πράξεις της πρόσθεσης και του πολλαπλασιασμού στο $\mathbb{Z}$ ως εξής: αν $\langle m, n\rangle$ και $\langle p, q\rangle$ είναι δύο στοιχεία του $\mathbb{Z}$, ορίζουμε

$$\langle m, n\rangle + \langle p, q\rangle = \langle m + p, n + q\rangle \tag{3.3.2}$$

και

$$\langle m,n\rangle\langle p,q\rangle = \langle mp+nq, mq+np\rangle. \tag{3.3.3}$$

Η λογική που κρύβεται πίσω από αυτούς τους ορισμούς είναι ότι σκεφτόμαστε το $\langle m,n\rangle$ ως $m-n$ και το $\langle p,q\rangle$ ως $p-q$, οπότε θα θέλαμε να ισχύουν οι

$$(m-n)+(p-q) = (m+p)-(n+q)$$

και

$$(m-n)(p-q) = (mp+nq)-(mq+np).$$

Πρέπει βέβαια αν ελέγξουμε ότι οι πράξεις που ορίστηκαν μέσω των (3.3.2) και (3.3.3) είναι καλά ορισμένες. Υποθέτουμε ότι $\langle m,n\rangle = \langle m_1,n_1\rangle$ και $\langle p,q\rangle = \langle p_1,q_1\rangle$, και το ερώτημα είναι αν

$$\langle m+p, n+q\rangle = \langle m_1+p_1, n_1+q_1\rangle.$$

όμως, $m+n_1 = n+m_1$ και $p+q_1 = p_1+q$, άρα

$$(m+p)+(n_1+q_1) = (m+n_1)+(p+q_1) = (n+m_1)+(p_1+q) = (m_1+p_1)+(n+q),$$

άρα, πράγματι, $\langle m+p, n+q\rangle = \langle m_1+p_1, n_1+q_1\rangle$.

Με τον ίδιο τρόπο ελέγχουμε ότι ο πολλαπλασιασμός είναι καλά ορισμένος: αν $\langle m,n\rangle = \langle m_1,n_1\rangle$ και $\langle p,q\rangle = \langle p_1,q_1\rangle$, τότε

$$\langle mp+nq, mq+np\rangle = \langle m_1p_1+n_1q_1, m_1q_1+n_1p_1\rangle.$$

Η επόμενη πρόταση δείχνει ότι οι πράξεις της πρόσθεσης και του πολλαπλασιασμού έχουν τις ιδιότητες που θέλουμε.

Πρόταση 3.3.2. *Οι πράξεις της πρόσθεσης και του πολλαπλασιασμού στο $\mathbb{Z}$ ικανοποιούν τα ακόλουθα:*

(Α1) *Για κάθε $a,b\in\mathbb{Z}$ ισχύει $a+b=b+a$.*

(Α2) *Για κάθε $a,b,c\in\mathbb{Z}$ ισχύει $a+(b+c)=(a+b)+c$.*

(Α3) *Υπάρχει κάποιο στοιχείο $\mathbf{0}$ του $\mathbb{Z}$ τέτοιο ώστε $\mathbf{0}+a=a$ για κάθε $a\in\mathbb{Z}$.*

(Α4) *Για κάθε $a\in\mathbb{Z}$ υπάρχει κάποιο στοιχείο $-a$ του $\mathbb{Z}$ τέτοιο ώστε $a+(-a)=(-a)+a=\mathbf{0}$.*

(Γ1) *Για κάθε $a,b\in\mathbb{Z}$ ισχύει $ab=ba$.*

(Γ2) *Για κάθε* $a, b, c \in \mathbb{Z}$ *ισχύει* $a(bc) = (ab)c$.

(Γ3) *Υπάρχει κάποιο στοιχείο* $\mathbf{1}$ *του* $\mathbb{Z}$ *τέτοιο ώστε* $\mathbf{1} \neq \mathbf{0}$ *και* $\mathbf{1}a = a$ *για κάθε* $a \in \mathbb{Z}$.

(Ε) *Για κάθε* $a, b, c \in \mathbb{Z}$ *ισχύει* $a + (b + c) = (a + b) + c$.

Απόδειξη. (Α1) Έστω $a = \langle m, n\rangle$ και $b = \langle p, q\rangle$ στο $\mathbb{Z}$. Έχουμε

$$\begin{aligned} a + b &= \langle m, n\rangle + \langle p, q\rangle = \langle m + p, n + q\rangle \\ &= \langle p + m, q + n\rangle = \langle p, q\rangle + \langle m, n\rangle = b + a, \end{aligned}$$

όπου χρησιμοποιήσαμε τις $m + p = p + m$ και $n + q = q + n$ που ισχύουν στο $\mathbb{N}_0$.

(Α2) Έστω $a = \langle m, n\rangle, b = \langle p, q\rangle$ και $c = \langle r, s\rangle$ στο $\mathbb{Z}$. Όπως πριν, χρησιμοποιώντας τώρα την προσεταιριστική ιδιότητα στο $\mathbb{N}_0$, έχουμε

$$\begin{aligned} a + (b + c) &= \langle m, n\rangle + (\langle p, q\rangle + \langle r, s\rangle) = \langle m, n\rangle + \langle p + r, q + s\rangle \\ &= \langle m + (p + r), n + (q + s)\rangle = \langle (m + p) + r, (n + q) + s\rangle \\ &= \langle m + p, n + q\rangle + \langle r, s\rangle = (\langle p, q\rangle + \langle m, n\rangle) + \langle r, s\rangle \\ &= (a + b) + c. \end{aligned}$$

(Α3) Θεωρούμε το $\mathbf{0} = \langle 0, 0\rangle \in \mathbb{Z}$ και παρατηρούμε ότι, για κάθε $a = \langle m, n\rangle \in \mathbb{Z}$,

$$\mathbf{0} + a = \langle 0, 0\rangle + \langle m, n\rangle = \langle m, n\rangle = a.$$

(Α4) Έστω $a = \langle m, n\rangle \in \mathbb{Z}$. Θεωρούμε το $-a = \langle n, m\rangle \in \mathbb{Z}$. Τότε,

$$a + (-a) = \langle m, n\rangle + \langle n, m\rangle = \langle m + n, n + m\rangle = \langle 0, 0\rangle = \mathbf{0}.$$

(Γ1) Έστω $a = \langle m, n\rangle$ και $b = \langle p, q\rangle$ στο $\mathbb{Z}$. Έχουμε

$$\begin{aligned} ab &= \langle m, n\rangle\langle p, q\rangle = \langle mp + nq, mq + np\rangle \\ &= \langle pm + qn, qm + pn\rangle = \langle p, q\rangle\langle m, n\rangle = ba, \end{aligned}$$

όπου χρησιμοποιήσαμε τις $mp + nq = pm + qn$ και $mq + np = qm + pn$ που ισχύουν στο $\mathbb{N}_0$.

(Γ2) Έστω $a = \langle m, n\rangle, b = \langle p, q\rangle$ και $c = \langle r, s\rangle$ στο $\mathbb{Z}$. Όπως πριν, χρησιμοποιώντας τώρα την προσεταιριστική ιδιότητα στο $\mathbb{N}_0$, έχουμε (μετά από κάποιες κουραστικές πράξεις!)

$$a(bc) = \langle m, n\rangle(\langle p, q\rangle\langle r, s\rangle) = (\langle p, q\rangle + \langle m, n\rangle) + \langle r, s\rangle = (ab)c.$$

(Γ3) Θεωρούμε το $\mathbf{1} = \langle 1, 0\rangle \in \mathbb{Z}$. Παρατηρούμε ότι $\langle 1, 0\rangle \neq \langle 0, 0\rangle$ και ότι

$$\langle 1, 0\rangle\langle m, n\rangle = \langle 1 \cdot m + 0 \cdot n, 1 \cdot n + 0 \cdot m\rangle = \langle m, n\rangle$$

για κάθε $\langle m, n\rangle \in \mathbb{Z}$.

(Ε) Έστω $a = \langle m, n\rangle, b = \langle p, q\rangle$ και $c = \langle r, s\rangle$ στο $\mathbb{Z}$. Χρησιμοποιώντας τώρα την επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση στο $\mathbb{N}_0$, έχουμε

$$\begin{aligned} a(b + c) &= \langle m, n\rangle(\langle p, q\rangle + \langle r, s\rangle) = \langle m, n\rangle\langle p + r, q + s\rangle \\ &= \langle m(p + r) + n(q + s), n(p + r) + m(q + s)\rangle \\ &= \langle (mp + nq) + (mr + ns), (np + mq) + (nr + ms)\rangle \\ &= \langle mp + nq, np + mq\rangle + \langle mr + ns, nr + ms\rangle \\ &= \langle m, n\rangle\langle p, q\rangle + \langle m, n\rangle\langle r, s\rangle = ab + ac. \end{aligned}$$

□

Διάταξη στο $\mathbb{Z}$. Μπορούμε να ορίσουμε διάταξη στο $\mathbb{Z}$ προσδιορίζοντας αρχικά το σύνολο των μη αρνητικών στοιχείων του. Ορίζουμε

$$\mathbb{Z}^+ = \{\langle m, n\rangle : m \geqslant n \text{ στο } \mathbb{N}_0\}.$$

Το σύνολο $\mathbb{Z}^+$ έχει τις ακόλουθες βασικές ιδιότητες (η απόδειξη αφήνεται ως άσκηση).

Πρόταση 3.3.3. *Το σύνολο* $\mathbb{Z}^+$ *ικανοποιεί τα ακόλουθα:*

(Σ1) *Αν* $a, b \in \mathbb{Z}^+$ *τότε* $a + b, ab \in \mathbb{Z}^+$.

(Σ2) *Για κάθε* $a \in \mathbb{Z}$ *έχουμε είτε* $a \in \mathbb{Z}^+$ *είτε* $-a \in \mathbb{Z}^+$.

(Σ3) *Αν* $a \in \mathbb{Z}^+$ *και* $-a \in \mathbb{Z}^+$ *τότε* $a = \mathbf{0}$.

Στη συνέχεια ορίζουμε την σχέση $\geqslant$ στο $\mathbb{Z}$ ως εξής:

$$\langle m, n\rangle \geqslant \langle p, q\rangle \iff \text{υπάρχει } \langle r, s\rangle \in \mathbb{Z}^+ \text{ ώστε } \langle m, n\rangle = \langle p, q\rangle + \langle r, s\rangle.$$

Η επόμενη πρόταση δείχνει ότι η σχέση $\geqslant$ είναι διάταξη (με κάποιες πρόσθετες καλές ιδιότητες σε σχέση με τις πράξεις).

Πρόταση 3.3.4. *Η σχέση* $\geqslant$ *στο* $\mathbb{Z}$ *ικανοποιεί τα ακόλουθα:*

(Δ1) *Έστω* $a, b, c \in \mathbb{Z}$. *Αν* $a \geqslant b$ *και* $b \geqslant c$ *τότε* $a \geqslant c$.

(Δ2) *Για κάθε* $a, b \in \mathbb{Z}$ *έχουμε είτε* $a \geqslant b$ *είτε* $b \geqslant a$.

(Δ3) *Έστω* $a, b \in \mathbb{Z}$. *Αν* $a \geqslant b$ *και* $b \geqslant a$ *τότε* $a = b$.

(Δ4) *Έστω* $a, b, c, d \in \mathbb{Z}$. *Αν* $a \geqslant b$ *και* $c \geqslant d$ *τότε* $a + c \geqslant b + d$.

(Δ5) *Έστω* $a, b, c, d \in \mathbb{Z}$. *Αν* $a \geqslant b \geqslant 0$ *και* $c \geqslant d \geqslant 0$ *τότε* $ac \geqslant bd$.

Απόδειξη. Αφήνεται ως άσκηση. □

Ορίζουμε τώρα και τις υπόλοιπες σχέσεις διάταξης στο $\mathbb{Z}$:

$$\begin{aligned} a > b &\iff a \geqslant b \text{ και } a \neq b, \\ a \leqslant b &\iff b \geqslant a, \\ a < b &\iff b > a. \end{aligned}$$

Η σχέση $>$ είναι αυστηρή διάταξη και ικανοποιεί την τριχοτομία:

Για κάθε $a, b \in \mathbb{Z}_0$ αληθεύει ακριβώς μία από τις $a > b$ ή $a = b$ ή $b > a$.

Το τελευταίο μας βήμα είναι να ανακτήσουμε τον συνήθη συμβολισμό για τους ακέραιους αριθμούς. Κάθε στοιχείο του $\mathbb{Z}^+$ είναι της μορφής $\langle m, n\rangle$ όπου $m \geqslant n$, συνεπώς μπορεί να γραφεί και ως $\langle m-n, 0\rangle$. Με άλλα λόγια, κάθε στοιχείο του $\mathbb{Z}^+$ είναι της μορφής $\langle r, 0\rangle$ για κάποιον $r \in \mathbb{N}_0$. Επίσης, η Πρόταση 3.3.3 (Σ2) μας λέει ότι για κάθε $a \in \mathbb{Z}$ είτε $a \in \mathbb{Z}^+$ είτε $-a \in \mathbb{Z}^+$, άρα είτε $a = \langle r, 0\rangle$ είτε $a = -\langle r, 0\rangle = \langle 0, r\rangle$.

Ορίζουμε την απεικόνιση $f : \mathbb{N}_0 \to \mathbb{Z}^+$ με $f(n) = \langle n, 0\rangle$. Μπορούμε τότε εύκολα να αποδείξουμε την ακόλουθη πρόταση.

Πρόταση 3.3.5. *Η* $f : \mathbb{N}_0 \to \mathbb{Z}^+$ *με* $f(n) = \langle n, 0\rangle$ *είναι αμφιμονοσήμαντη, και*

$$\begin{aligned} f(m+n) &= f(m) + f(n), \\ f(mn) &= f(m)f(n), \\ m \geqslant n &\iff f(m) \geqslant f(n). \end{aligned}$$

Η πρόταση αυτή δείχνει ότι τα $\mathbb{N}_0$ και $\mathbb{Z}^+$ είναι δύο διαφορετικοί τρόποι για να αναπαραστήσουμε την ίδια μαθηματική έννοια: τους μη αρνητικούς ακεραίους. Με αυτή την έννοια ταυτίζουμε τον $n \in \mathbb{N}_0$ με τον $\langle n, 0\rangle \in \mathbb{Z}^+$ και θεωρούμε το $\mathbb{N}_0$ ως υποσύνολο του $\mathbb{Z}$. Επίσης, στο εξής θα γράφουμε

$$\langle n, 0\rangle := n \quad \text{και} \quad \langle 0, n\rangle := -n.$$

Έχουμε πλέον το σύστημα αριθμών $\mathbb{N}_0$ ως «υποσύστημα» του συστήματος αριθμών $\mathbb{Z}$, και μάλιστα κάθε ακέραιος είναι είτε στοιχείο του $\mathbb{N}_0$ είτε ο αντίθετος κάποιου στοιχείου του $\mathbb{N}_0$.

3.3.2 Διαίρεση

Έστω $a, b \in \mathbb{Z}$. Λέμε ότι ο a *διαιρεί* τον b και γράφουμε $a \mid b$, αν υπάρχει $x \in \mathbb{Z}$ τέτοιος ώστε $b = ax$. Σε αυτή την περίπτωση θα λέμε ότι ο a είναι *διαιρέτης* του b ή ότι ο b είναι *πολλαπλάσιο* του a. Απλές συνέπειες του ορισμού είναι οι εξής:

(i) $a \mid a$ για κάθε $a \in \mathbb{Z}$.

(ii) $a \mid 0$ για κάθε $a \in \mathbb{Z}$.

(iii) $\pm 1 \mid a$ για κάθε $a \in \mathbb{Z}$.

(iv) $0 \mid a$ αν και μόνο αν $a = 0$.

(v) Αν $a \mid b$ και $b \mid c$ τότε $a \mid c$.

(vi) Αν $a \mid b$ και $a \mid c$ τότε $a \mid bx + cy$ για κάθε $x, y \in \mathbb{Z}$.

(vii) Αν $a, b \in \mathbb{Z}\backslash\{0\}$ και $a \mid b$ τότε $|a| \leqslant |b|$.

(viii) $a \mid \pm 1$ αν και μόνο αν $a = \pm 1$.

Η απόδειξη των (i) ως (viii) αφήνεται ως άσκηση.

Θεώρημα 3.3.6 (ταυτότητα της διαίρεσης)**.** *Υποθέτουμε ότι $a \in \mathbb{N}$ και $b \in \mathbb{Z}$. Τότε υπάρχουν μοναδικοί $q, r \in \mathbb{Z}$ τέτοιοι ώστε $b = aq + r$ και $0 \leqslant r < a$.*

«Γεωμετρική απόδειξη»: Ένας απλός γεωμετρικός τρόπος για να σκεφτόμαστε την ταυτότητα της διαίρεσης είναι ο εξής: φανταζόμαστε την πραγματική ευθεία πάνω στην οποία έχουμε σημειώσει με κουκίδες τους ακεραίους. Σημειώνουμε με πιο σκούρες κουκίδες τα πολλαπλάσια του a. Διαδοχικές σκούρες κουκίδες έχουν απόσταση ακριβώς ίση με a. Τότε ένα από τα ακόλουθα συμβαίνει:

(i) Ο ακέραιος b πέφτει πάνω σε κάποια από αυτές τις σκούρες κουκίδες, οπότε ο b είναι πολλαπλάσιο του a και $r = 0$.

(ii) Ο ακέραιος b βρίσκεται ανάμεσα σε δύο διαδοχικές σκούρες κουκίδες, δηλαδή ανάμεσα σε δύο διαδοχικά πολλαπλάσια του a, και η απόσταση r ανάμεσα στον b και το μεγαλύτερο πολλαπλάσιο του a που είναι μικρότερο από τον b είναι ένας θετικός ακέραιος που δεν ξεπερνάει τον $a - 1$.

Η αυστηρή απόδειξη που θα δώσουμε παρακάτω βασίζεται σε αυτή την ιδέα: θεωρούμε το σύνολο S των «αποστάσεων» $b - as$ του b από τις σκούρες κουκίδες που βρίσκονται αριστερά

του. Εξασφαλίζουμε ότι είναι μη κενό, άρα έχει ελάχιστο στοιχείο $b - aq$. Η κουκίδα aq είναι αυτή που βρίσκεται αμέσως πριν από τον b, και η απόσταση $r = b - aq$ πρέπει να είναι μικρότερη από a.

Απόδειξη του Θεωρήματος 3.3.6. Αποδεικνύουμε πρώτα την ύπαρξη αριθμών $q, r \in \mathbb{Z}$ που ικανοποιούν το ζητούμενο. Θεωρούμε το σύνολο

$$S = \{b - as : s \in \mathbb{Z}\} \cap \mathbb{Z}^+.$$

των μη αρνητικών ακεραίων της μορφής $b - as$. Το S είναι μη κενό. Πράγματι, αν $b \geqslant 0$ τότε $b - a \cdot 0 \in S$. Αν $b < 0$, επιλέγουμε $s = b$ και βλέπουμε ότι $b - ab = b(1 - a) \geqslant 0$.

Από την αρχή του ελαχίστου το S έχει ελάχιστο στοιχείο, το οποίο συμβολίζουμε με r. Από τον ορισμό του S έχουμε $r \geqslant 0$ και υπάρχει $q \in \mathbb{Z}$ τέτοιος ώστε $b - aq = r$. Μένει να δείξουμε ότι $r < a$. Ας υποθέσουμε ότι $r \geqslant a$. Τότε

$$b - a(q + 1) = b - aq - a = r - a \geqslant 0,$$

δηλαδή $b - a(q + 1) \in S$. Όμως $b - a(q + 1) = r - a < r$, το οποίο είναι άτοπο αφού ο r ήταν το ελάχιστο στοιχείο του S.

Αποδεικνύουμε τώρα τη μοναδικότητα των q και r. Ας υποθέσουμε ότι

$$b = aq_1 + r_1 = aq_2 + r_2, \tag{3.3.4}$$

όπου $0 \leqslant r_1, r_2 < a$. Χωρίς περιορισμό της γενικότητας υποθέτουμε ότι $r_1 \geqslant r_2$.

$$r_1 - r_2 = a(q_2 - q_1).$$

Αν $q_1 \neq q_2$, τότε $a(q_2 - q_1) \geqslant a$ ενώ $r_1 - r_2 < a$. Έχουμε αντίφαση, άρα $q_1 = q_2$ και από την (3.3.4) έπεται ότι $r_1 = r_2$. □

Παράδειγμα 3.3.7. Από το Θεώρημα 3.3.6, κάθε ακέραιος b γράφεται μονοσήμαντα στη μορφή $b = 2q + r$ για κάποιον $q \in \mathbb{Z}$ και κάποιον $r \in \{0, 1\}$. Λέμε ότι ο b είναι *άρτιος* αν $r = 0$. Αν $r = 1$, τότε λέμε ότι ο b είναι *περιττός*. Παρατηρήστε ότι οποιαδήποτε δύναμη περιττού ακεραίου είναι περιττός ακέραιος.

Σκοπός μας είναι να δείξουμε ότι αν οι ακέραιοι x, y, z ικανοποιούν την εξίσωση

$$x^3 + 2y^3 = 4z^3 \tag{3.3.5}$$

τότε $x = y = z = 0$.

Απόδειξη. Για κάθε λύση της (3.3.5) θεωρούμε το μη αρνητικό ακέραιο

$$d := \max\{|x|, |y|, |z|\}.$$

Ας υποθέσουμε ότι η εξίσωση (3.3.5) έχει μια μη τετριμμένη λύση (x_1, y_1, z_1) στο $\mathbb{Z}$, δηλαδή τουλάχιστον ένας από τους x_1, y_1, z_1 είναι μη μηδενικός ακέραιος. Τότε

$$d_1 = \max\{|x_1|, |y_1|, |z_1|\} > 0.$$

Παρατηρούμε ότι ο $x_1^3 = 4z_1^3 - 2y_1^3$ είναι άρτιος, άρα ο x_1 είναι άρτιος. Υπάρχει λοιπόν $x_2 \in \mathbb{Z}$ τέτοιος ώστε $x_1 = 2x_2$. Αντικαθιστώντας στην (1.2.5) παίρνουμε

$$8x_2^3 + 2y_1^3 = 4z_1^3 \Longrightarrow y_1^3 = 2z_1^3 - 4x_2^3. \tag{3.3.6}$$

Έπεται ότι ο y_1 είναι άρτιος, άρα γράφεται στη μορφή $y_1 = 2y_2$ για κάποιον $y_2 \in \mathbb{Z}$. Αντικαθιστώντας στην (3.3.6) παίρνουμε

$$8y_2^3 = 2z_1^3 - 4x_2^3 \Longrightarrow z_1^3 = 4y_2^3 + 2x_2^3.$$

Άρα ο z_1 είναι κι αυτός άρτιος και γράφεται στη μορφή $z_1 = 2z_2$ για κάποιον $z_2 \in \mathbb{Z}$. Παρατηρούμε ότι οι x_2, y_2 και z_2 ικανοποιούν την (3.3.5) και

$$0 < d_2 = \max\{|x_2|, |y_2|, |z_2|\} = \max\{|x_1|, |y_1|, |z_1|\}/2 = d_1/2 < d_1.$$

Συνεχίζοντας παρόμοια κατασκευάζουμε μια άπειρη γνησίως φθίνουσα ακολουθία φυσικών αριθμών $d_1 > d_2 > \cdots > d_n > d_{n+1} > \cdots$. Αυτό είναι άτοπο από την αρχή του ελαχίστου. Άρα η μόνη λύση της (3.3.5) στο $\mathbb{Z}$ είναι η τετριμμένη $x = y = z = 0$. □

Χρησιμοποιώντας την ταυτότητα της διαίρεσης και τη μέθοδο της μαθηματικής επαγωγής μπορούμε να αποδείξουμε την ύπαρξη και τη μοναδικότητα των m-αδικών αναπαραστάσεων των ακεραίων.

Θεώρημα 3.3.8. *Έστω $m \geqslant 2$ ένας ακέραιος. Κάθε φυσικός αριθμός n αναπαρίσταται κατά μοναδικό τρόπο στη μορφή*

$$n = a_0 + a_1 m + a_2 m^2 + \cdots + a_k m^k, \tag{3.3.7}$$

όπου k είναι ο μη αρνητικός ακέραιος για τον οποίο $m^k \leqslant n < m^{k+1}$, και $a_0, a_1, \ldots, a_k$ είναι ακέραιοι που ικανοποιούν τις $1 \leqslant a_k \leqslant m-1$ και $0 \leqslant a_i \leqslant m-1$ για κάθε $i = 0, 1, \ldots, k-1$.

Η (3.3.7) λέγεται *m-αδική αναπαράσταση* του n. Οι ακέραιοι a_i είναι τα *ψηφία* του n με *βάση* τον m.

Απόδειξη του Θεωρήματος 3.3.8. Θα χρησιμοποιήσουμε τη μέθοδο της μαθηματικής επαγωγής. Αν $1 \leqslant n < m$ τότε η $n = a_0$ είναι η μοναδική m-αδική αναπαράσταση (3.3.7) του n (εξηγήστε). Έστω $n \geq m$ και έστω ότι ο ισχυρισμός του θεωρήματος ισχύει για κάθε θετικό ακέραιο μικρότερο του n. Θα αποδείξουμε τον ίδιο ισχυρισμό για τον n. Από την ταυτότητα της διαίρεσης του n με τον m υπάρχουν ακέραιοι q και r με $0 \leqslant r < m$ έτσι ώστε

$$n = r + qm. \tag{3.3.8}$$

Από την υπόθεση $n \geq m$ έχουμε $q > 0$ και συνεπώς $0 < q < qm \leq qm + r = n$. Από την υπόθεση της επαγωγής ο q αναπαρίσταται στη μορφή

$$q = a_1 + a_2 m + \cdots + a_k m^{k-1} \tag{3.3.9}$$

για μοναδικούς ακεραίους a_i με $0 \leq a_i \leq m-1$ για $i = 1, 2, \ldots, k$ και $a_k > 0$. Από τις (3.3.8) και (3.3.9), θέτοντας $r = a_0$, προκύπτει ότι ο n αναπαρίσταται στη ζητούμενη μορφή

$$n = a_0 + a_1 m + \cdots + a_{k-1} m^{k-1} + a_k m^k.$$

Θα δείξουμε ότι αυτή η αναπαράσταση είναι μοναδική. Έστω

$$n = b_0 + b_1 m + \cdots + b_s m^s$$

μια άλλη m-αδική αναπαράσταση του n, όπου $0 \leqslant b_j \leqslant m-1$ για κάθε $j = 0, 1, \ldots, s$ και $b_s \geqslant 1$. Από την (1.2.15) έχουμε $n = r' + mq'$ όπου $r' = b_0$ και

$$q' = b_1 + b_2 m + \cdots + b_s m^{s-1} \tag{3.3.10}$$

είναι ακέραιοι με $0 \leq r' < m$. Από τη μοναδικότητα της διαίρεσης του n με το m προκύπτει ότι $r' = r$ και $q' = q$. Η πρώτη ισότητα δίνει $b_0 = a_0$ ενώ από την υπόθεση της επαγωγής για τη μοναδικότητα της m-αδική αναπαράστασης του $q = q'$ και τις (3.3.8) και (3.3.10) προκύπτει ότι $s = k$ και $b_i = a_i$ για $i = 1, 2, \ldots, k$, όπως το θέλαμε.

Τέλος, αν ο n είναι στη μορφή (3.3.7) τότε από τις σχέσεις $0 \leqslant a_i \leqslant m-1$ και $1 \leqslant a_k \leqslant m-1$ προκύπτει ότι $m^k \leq n \leq (m-1)(1+m+\cdots+m^k) = m^{k+1}-1 < m^{k+1}$. □

Παράδειγμα 3.3.9. Η 2-αδική αναπαράσταση του 100 είναι

$$100 = 1 \cdot 2^2 + 1 \cdot 2^5 + 1 \cdot 2^6,$$

και η 3-αδική αναπαράσταση του 100 είναι

$$100 = 1 + 2 \cdot 3^2 + 1 \cdot 3^4.$$

3.3.3 Μέγιστος κοινός διαιρέτης

Έστω a και b δύο φυσικοί αριθμοί. Οι a και b έχουν τουλάχιστον έναν κοινό διαιρέτη, τον 1. Σκοπός μας είναι να αποδείξουμε ότι υπάρχει μέγιστος φυσικός αριθμός d ο οποίος διαιρεί τους a και b. Η ιδέα πίσω από την απόδειξη που θα δώσουμε είναι να θεωρήσουμε το σύνολο I όλων των θετικών *ακεραίων συνδυασμών* $au + bv$ των a, b, όπου $u, v \in \mathbb{Z}$. Τέτοιοι θετικοί συνδυασμοί υπάρχουν: για παράδειγμα, $a = a \cdot 1 + b \cdot 0$. Η βασική παρατήρηση είναι ότι κάθε κοινός διαιρέτης k των a, b διαιρεί κάθε στοιχείο του I (ιδιότητα 6 της διαιρετότητας), άρα δεν ξεπερνάει το ελάχιστο στοιχείο του I. Αν δείξουμε ότι το ελάχιστο στοιχείο του I *είναι* κοινός διαιρέτης των a, b, τότε θα είναι ο «μέγιστος κοινός διαιρέτης» τους.

Θεώρημα 3.3.10. *Έστω $a, b \in \mathbb{N}$. Υπάρχει μοναδικός $d \in \mathbb{N}$ ο οποίος ικανοποιεί τα εξής.*

(i) $d \mid a$ *και* $d \mid b$.

(ii) *Αν για κάποιον $k \in \mathbb{N}$ έχουμε $k \mid a$ και $k \mid b$, τότε $k \mid d$. Ειδικότερα, $k \leqslant d$.*

Επιπλέον, υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $d = ax + by$.

Απόδειξη. Θεωρούμε το σύνολο

$$I = \{au + bv : u, v \in \mathbb{Z}\} \cap \mathbb{N}.$$

Είναι φανερό ότι το I είναι μη κενό, για παράδειγμα $a, b \in I$. Από την αρχή του ελαχίστου, το I έχει ελάχιστο στοιχείο d το οποίο γράφεται στη μορφή $d = ax + by$ για κάποιους $x, y \in \mathbb{Z}$.

Θα δείξουμε ότι ο d διαιρεί κάθε στοιχείο του I. Ας υποθέσουμε ότι $z = au + bv \in I$. Από το Θεώρημα 3.3.6 υπάρχουν $q, r \in \mathbb{Z}$ με $0 \leqslant r < d$ και $z = dq + r$. Παρατηρούμε ότι

$$r = z - dq = au + bv - (ax + by)q = a(u - xq) + b(v - yq) \in I.$$

Αν ήταν $0 < r < d$ τότε ο r θα ήταν στοιχείο του I μικρότερο από τον d, άτοπο από τον τρόπο ορισμού του d. Άρα $r = 0$, το οποίο αποδεικνύει ότι ο d διαιρεί τον z.

Αφού $a, b \in I$, ο d διαιρεί τους a και b. Αυτός είναι ο πρώτος ισχυρισμός του θεωρήματος. Για τον δεύτερο, παρατηρούμε ότι αν $k \mid a$ και $k \mid b$ τότε

$$k \mid ax + by = d.$$

Για τη μοναδικότητα του d παρατηρήστε ότι αν οι φυσικοί αριθμοί d_1 και d_2 ικανοποιούν τα (i) και (ii) τότε $d_1 \mid d_2$ και $d_2 \mid d_1$. Ειδικότερα $d_1 \leqslant d_2$ και $d_2 \leqslant d_1$, άρα $d_1 = d_2$. □

Ο αριθμός d που ορίζεται από το Θεώρημα 3.3.10 λέγεται *μέγιστος κοινός διαιρέτης* των a και b, και συμβολίζεται με $d = (a, b)$. Λέμε ότι δύο αριθμοί $a, b \in \mathbb{N}$ είναι *σχετικά πρώτοι* αν $(a, b) = 1$. Για παράδειγμα, οι 8 και 15 είναι σχετικά πρώτοι: $(8, 15) = 1$.

Παρατήρηση 3.3.11. Είναι χρήσιμο να θυμάται κανείς ότι ο μέγιστος κοινός διαιρέτης (a, b) των φυσικών αριθμών a και b είναι ο *ελάχιστος θετικός ακέραιος συνδυασμός* τους:

$$(a, b) = \min\{au + bv : u, v \in \mathbb{Z}\} \cap \mathbb{N}.$$

Ο *αλγόριθμος του Ευκλείδη* μας δίνει έναν πρακτικό τρόπο υπολογισμού του μέγιστου κοινού διαιρέτη δύο φυσικών αριθμών. Ξεκινάμε με δύο φυσικούς αριθμούς $a < b$. Από την ταυτότητα της διαίρεσης έχουμε

$$b = aq_1 + r_1$$

για κάποιους (μονοσήμαντα ορισμένους) $q_1 \in \mathbb{N}$ και $0 \leqslant r_1 < a$. Αν $r_1 = 0$ σταματάμε, αλλιώς γράφουμε την ταυτότητα της διαίρεσης του a με τον r_1:

$$a = r_1 q_2 + r_2,$$

για κάποιους (μονοσήμαντα ορισμένους) $q_2 \in \mathbb{N}$ και $0 \leqslant r_2 < r_1$. Συνεχίζουμε με τον ίδιο τρόπο. Η διαδικασία πρέπει κάποια στιγμή να καταλήξει σε υπόλοιπο $r_{n+1} = 0$. Αλλιώς, θα είχαμε μια άπειρη γνησίως φθίνουσα ακολουθία φυσικών αριθμών: $a > r_1 > r_2 > \cdots > r_n > r_{n+1} > \cdots$. Το επόμενο θεώρημα δείχνει ότι ο μέγιστος κοινός διαιρέτης των a και b είναι το τελευταίο μη μηδενικό υπόλοιπο: $(a, b) = r_n$ (αν $r_1 = 0$, τότε $a \mid b$ και $(a, b) = a$).

Θεώρημα 3.3.12. *Υποθέτουμε ότι $a, b \in \mathbb{N}$ και $a < b$. Ας υποθέσουμε ότι έχουμε βρεί $q_1, \ldots, q_{n+1} \in \mathbb{N}$ και $r_1, \ldots, r_n \in \mathbb{N}$ με $0 < r_n < r_{n-1} < \cdots < r_1 < a$ και*

$$\begin{aligned} b &= aq_1 + r_1, \\ a &= r_1 q_2 + r_2, \\ r_1 &= r_2 q_3 + r_3, \\ &\vdots = \vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, \\ r_{n-1} &= r_n q_{n+1}. \end{aligned}$$

Τότε $(a, b) = r_n$.

Απόδειξη. Θα δείξουμε ότι

$$(a, b) = (a, r_1).$$

Θέτουμε $d_1 = (a, b)$ και $d_2 = (a, r_1)$. Έχουμε $d_1 \mid a$ και $d_1 \mid b$, άρα $d_1 \mid b - aq_1 = r_1$. Αφού $d_1 \mid a$ και $d_1 \mid r_1$, το Θεώρημα 3.3.10 δείχνει ότι

$$d_1 \mid (a, r_1) = d_2. \tag{3.3.11}$$

Από την άλλη πλευρά, $d_2 \mid a$ και $d_2 \mid r_1$, άρα $d_2 \mid aq_1 + r_1 = b$. Αφού $d_2 \mid a$ και $d_2 \mid b$, το Θεώρημα 3.3.10 δείχνει ότι

$$d_2 \mid (a, b) = d_1. \tag{3.3.12}$$

Από τις (3.3.11) και (3.3.12) συμπεραίνουμε ότι $d_1 = d_2$. Επαναλαμβάνοντας το ίδιο επιχείρημα, παίρνουμε

$$(a, b) = (a, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n).$$

Όμως

$$(r_{n-1}, r_n) = (r_n q_{n+1}, r_n) = r_n,$$

δηλαδή $(a, b) = r_n$. □

Παράδειγμα 3.3.13. Θα υπολογίσουμε τον $(391, 2533)$. Με διαδοχικές διαιρέσεις παίρνουμε

$$\begin{aligned} 2533 &= 391 \cdot 6 + 187, \\ 391 &= 187 \cdot 2 + 17, \\ 187 &= 17 \cdot 11. \end{aligned}$$

Από το Θεώρημα 3.3.12 (με $a = 391$ και $b = 2533$) συμπεραίνουμε ότι $(391, 2533) = 17$. Παρατηρήστε ότι η ίδια διαδικασία μας επιτρέπει να βρούμε ακεραίους x και y για τους οποίους $17 = 391x + 2533y$. Έχουμε

$$\begin{aligned} 17 &= 391 - 187 \cdot 2 \\ &= 391 - (2533 - 391 \cdot 6) \cdot 2 \\ &= 391 \cdot 13 + 2533 \cdot (-2), \end{aligned}$$

δηλαδή $x = 13$ και $y = -2$.

3.3.4 Βασικά λήμματα διαιρετότητας

Σε αυτή τη σύντομη παράγραφο αποδεικνύουμε κάποια στοιχειώδη αλλά πολύ βασικά λήμματα σχετικά με τη διαιρετότητα.

Λήμμα 3.3.14. *Αν $a, b \in \mathbb{N}$ και $d = (a, b)$ τότε έχουμε $a = du$ και $b = dv$ για ακεραίους $u, v \in \mathbb{N}$ με $(u, v) = 1$.*

Απόδειξη. Εφόσον $d \mid a$ και $d \mid b$ μπορούμε να γράψουμε $a = du$ και $b = dv$ με $u, v \in \mathbb{N}$. Από το Θεώρημα 3.3.10 υπάρχουν ακέραιοι x και y τέτοιοι ώστε $d = ax + by$ και συνεπώς $d = dux + dvy$ και $1 = ux + vy$. Από την τελευταία ισότητα προκύπτει ότι κάθε κοινός διαιρέτης των u και v θα πρέπει να διαιρεί το 1 και επομένως $(u, v) = 1$. □

Λήμμα 3.3.15. *Έστω $r_1, r_2 \in \mathbb{N}$ με $(r_1, r_2) = 1$. Αν $r_1 \mid r_2 m$ για κάποιον $m \in \mathbb{N}$, τότε $r_1 \mid m$.*

Απόδειξη. Υπάρχουν ακέραιοι x και y τέτοιοι ώστε $r_1 x + r_2 y = 1$. Άρα

$$r_1 mx + r_2 my = m.$$

Όμως $r_1 \mid r_1 mx$ και $r_1 \mid r_2 m \implies r_1 \mid r_2 my$. Άρα $r_1 \mid (r_1 mx + r_2 my) = m$. □

Παράδειγμα 3.3.16. Αν $8 \mid 3m$ τότε $8 \mid m$.

Λήμμα 3.3.17. *Έστω $r_1, r_2 \in \mathbb{N}$ με $(r_1, r_2) = 1$. Αν $r_1 \mid m$ και $r_2 \mid m$ για κάποιον $m \in \mathbb{N}$, τότε $r_1 r_2 \mid m$.*

Απόδειξη. Υπάρχουν ακέραιοι x και y τέτοιοι ώστε $r_1 x + r_2 y = 1$. Άρα

$$r_1 mx + r_2 my = m.$$

Αφού $r_2 \mid m$ έχουμε $r_1 r_2 \mid r_1 mx$ και αφού $r_1 \mid m$ έχουμε $r_1 r_2 \mid r_2 my$. Άρα $r_1 r_2 \mid (r_1 mx + r_2 my) = m$. □

Παράδειγμα 3.3.18. Για να δείξουμε ότι $24 \mid m$, αρκεί να δείξουμε ότι $8 \mid m$ και $3 \mid m$.

Ένα πολύ χρήσιμο αποτέλεσμα σχετικά με τη διαιρετότητα είναι το εξής.

Λήμμα 3.3.19. *Έστω $a, b, w \in \mathbb{N}$ με $(a, b) = 1$. Αν $w \mid ab$ τότε υπάρχουν μοναδικοί φυσικοί u, v τέτοιοι ώστε $w = uv$ και $u \mid a$, $v \mid b$. Επιπλέον έχουμε $(u, v) = 1$.*

Απόδειξη. Έστω $u = (w, a)$. Από το Λήμμα 3.3.14 μπορούμε να γράψουμε $w = uv$ και $a = uv'$ για φυσικούς αριθμούς v και v' με $(v, v') = 1$. Έχουμε $uv = w \mid ab = uv'b$ και συνεπώς $v \mid v'b$. Εφόσον $(v, v') = 1$ από το Λήμμα 3.3.15 προκύπτει ότι $v \mid b$. Ας δούμε γιατί $(u, v) = 1$: ο (u, v) διαιρεί τον u, άρα διαιρεί τον a. Ομοίως ο (u, v) διαιρεί τον v, άρα διαιρεί τον b. Έπεται ότι $(u, v) \mid (a, b) = 1$, οπότε $(u, v) = 1$.

Για τη μοναδικότητα, ας υποθέσουμε ότι $w = u_1v_1$, όπου $u_1 \mid a$ και $v_1 \mid b$. Από τις $u_1 \mid w$ και $u_1 \mid a$ βλέπουμε ότι $u_1 \mid (w, a) = u$. Επίσης από τις $u \mid a$, $v_1 \mid b$ και $(a, b) = 1$ συμπεραίνουμε όπως παραπάνω ότι $(u, v_1) = 1$. Επομένως από τη σχέση $u \mid w = u_1v_1$ και το Λήμμα 3.3.15 προκύπτει ότι $u \mid u_1$. Άρα $u_1 = u$ και συνεπώς $v_1 = v$. □

3.3.5 Ανάλυση σε γινόμενο πρώτων παραγόντων

Έστω $a > 1$ ένας φυσικός αριθμός. Θα λέμε ότι ο a είναι *πρώτος* αν έχει ακριβώς δύο θετικούς διαιρέτες, τον 1 και τον a. Αν ο a δεν είναι πρώτος, θα λέγεται *σύνθετος*. Για διάφορους λόγους είναι βολικό να μην κατατάξουμε τον 1 ούτε στους πρώτους ούτε στους σύνθετους αριθμούς.

Σε ότι ακολουθεί, με το σύμβολο p θα εννοούμε πάντα κάποιον πρώτο αριθμό. Το πρώτο μας αποτέλεσμα είναι απλή συνέπεια του Λήμματος 3.3.15.

Θεώρημα 3.3.20. *Έστω $a, b \in \mathbb{N}$ και p ένας πρώτος αριθμός. Αν $p \mid ab$ τότε $p \mid a$ ή $p \mid b$.*

Απόδειξη. Έστω ότι ο p δεν διαιρεί τον a. Αφού οι μόνοι διαιρέτες του p είναι ο 1 και ο p έχουμε $(a, p) = 1$. Από το Λήμμα 3.3.15 έπεται ότι $p \mid b$. □

Με επαγωγή ως προς k παίρνουμε την εξής γενίκευση.

Θεώρημα 3.3.21. *Έστω $a_1, \ldots, a_k \in \mathbb{N}$ και p ένας πρώτος αριθμός. Αν $p \mid a_1 \cdots a_k$ τότε $p \mid a_j$ για τουλάχιστον ένα $j \in \{1, \ldots, k\}$.*

Το *θεμελιώδες θεώρημα της αριθμητικής* μας λέει ότι κάθε φυσικός αριθμός αναλύεται (ουσιαστικά) μονοσήμαντα σε γινόμενο πρώτων παραγόντων.

Θεώρημα 3.3.22. *Κάθε φυσικός αριθμός $n > 1$ αναπαρίσταται σα γινόμενο πρώτων αριθμών. Η αναπαράσταση αυτή είναι μοναδική αν αγνοήσουμε τη διάταξη των παραγόντων του γινομένου.*

Σημείωση: Κάθε πρώτος θεωρείται γινόμενο πρώτων (με έναν όρο). Ένας βασικός λόγος που δεν θεωρούμε τον 1 πρώτο είναι για να εξασφαλίσουμε τη μοναδικότητα σε αυτό το θεώρημα (αλλιώς, θα είχαμε για παράδειγμα $6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3$).

Απόδειξη. Δείχνουμε πρώτα με επαγωγή ως προς n ότι κάθε ακέραιος $n \geqslant 2$ γράφεται σα γινόμενο πρώτων. Ο 2 είναι προφανώς γινόμενο πρώτων. Η επαγωγική υπόθεση είναι ότι κάθε $m \in \mathbb{N}$ με $2 \leqslant m < n$ γράφεται σα γινόμενο πρώτων. Αν ο n είναι πρώτος, δεν έχουμε τίποτα να δείξουμε. Αν ο n είναι σύνθετος, υπάρχουν $n_1, n_2 \in \mathbb{N}$ με $2 \leqslant n_1, n_2 < n$ τέτοιοι ώστε $n = n_1 n_2$. Από την επαγωγική υπόθεση, καθένας από τους n_1, n_2 αναπαρίσταται σα γινόμενο πρώτων, οπότε το ίδιο ισχύει και για τον $n = n_1 n_2$.

Δείχνουμε τώρα τη μοναδικότητα. Ας υποθέσουμε ότι

$$n = p_1 \cdots p_r = q_1 \cdots q_s, \tag{3.3.13}$$

όπου οι $p_1 \leqslant \cdots \leqslant p_r$ και $q_1 \leqslant \cdots \leqslant q_s$ είναι πρώτοι. Αφού $p_1 \mid q_1 \cdots q_s$, το Θεώρημα 3.3.21 δείχνει ότι υπάρχει $j \leqslant s$ τέτοιος ώστε $p_1 \mid q_j$. Αφού οι p_1 και q_j είναι πρώτοι, αναγκαστικά έχουμε $p_1 = q_j$. Ομοίως, αφού $q_1 \mid p_1 \cdots p_r$ υπάρχει $i \leqslant r$ τέτοιος ώστε $q_1 \mid p_i$, απ¨ όπου παίρνουμε $q_1 = p_i$. Παρατηρούμε ότι

$$p_1 = q_j \geqslant q_1 = p_i \geqslant p_1,$$

άρα $p_1 = q_1$. Τώρα η (3.3.13) παίρνει τη μορφή

$$p_2 \cdots p_r = q_2 \cdots q_s.$$

Επαναλαμβάνοντας την ίδια διαδικασία πεπερασμένες το πλήθος φορές, συμπεραίνουμε ότι $r = s$ και $p_i = q_i$ για κάθε $i = 1, \ldots, r$. □

Αν πάρουμε κατά ομάδες τους ίσους πρώτους που εμφανίζονται στην αναπαράσταση του Θεωρήματος 3.3.22, παίρνουμε αμέσως το εξής.

Θεώρημα 3.3.23. *Κάθε φυσικός αριθμός $n \geqslant 2$ αναπαρίσταται μονοσήμαντα στη μορφή*

$$n = p_1^{k_1} \cdots p_r^{k_r},$$

όπου $p_1 < \cdots < p_r$ είναι πρώτοι αριθμοί και $k_1, \ldots, k_r \in \mathbb{N}$.

Θα λέμε ότι η αναπαράσταση του Θεωρήματος 3.3.23 είναι η *κανονική αναπαράσταση* του φυσικού αριθμού n.

3.3.6 Η απειρία και το θεώρημα των πρώτων αριθμών

Η πρώτη σημαντική συνέπεια του θεμελιώδους θεωρήματος της αριθμητικής είναι το *θεώρημα του Ευκλείδη* για την απειρία των πρώτων αριθμών.

Θεώρημα 3.3.24. *Υπάρχουν άπειροι πρώτοι αριθμοί.*

Πρώτη απόδειξη. Το επιχείρημα είναι αυτό που χρησιμοποίησε ο Ευκλείδης. Ας υποθέσουμε ότι υπάρχουν πεπερασμένοι το πλήθος πρώτοι αριθμοί, οι $p_1 < \cdots < p_r$. Θεωρούμε τον φυσικό αριθμό

$$n = p_1 \cdots p_r + 1.$$

Ο n είναι μεγαλύτερος από 1, άρα έχει πρώτο διαιρέτη. Αφού το $\{p_1, \ldots, p_r\}$ είναι το σύνολο *όλων* των πρώτων αριθμών, υπάρχει $j \leqslant r$ τέτοιος ώστε $p_j \mid n$. Όμως $p_j \mid p_1 \cdots p_r$, άρα

$$p_j \mid (n - p_1 \cdots p_r) \quad \text{δηλαδή} \quad p_j \mid 1.$$

Αυτό είναι άτοπο, άρα υπάρχουν άπειροι πρώτοι. □

Η επόμενη απόδειξη χρησιμοποιεί τους *αριθμούς του Fermat*.

Δεύτερη απόδειξη. Για κάθε $n = 0, 1, 2, \ldots$ ορίζουμε

$$F_n = 2^{2^n} + 1.$$

Οι αριθμοί F_n λέγονται αριθμοί του Fermat. Αφού $F_n \geqslant 2$ για κάθε $n \geqslant 0$, κάθε F_n έχει τουλάχιστον έναν πρώτο διαιρέτη q_n. Θα δείξουμε ότι

$$n \neq m \Longrightarrow (F_n, F_m) = 1. \tag{3.3.14}$$

Οποιοιδήποτε δύο αριθμοί του Fermat είναι σχετικά πρώτοι, άρα

$$n \neq m \Longrightarrow q_n \neq q_m.$$

(γιατί;) Έπεται ότι οι q_n, $n \geqslant 0$, είναι διακεκριμένοι πρώτοι, το οποίο δείχνει την απειρία των πρώτων αριθμών.

Για την απόδειξη της (3.3.14) δείχνουμε πρώτα με επαγωγή το εξής: αν $n \geqslant 1$, τότε

$$\prod_{j=0}^{n-1} F_j = F_n - 2. \tag{3.3.15}$$

Η (3.3.15) ισχύει αν $n = 1$: $F_0 = 3 = 5 - 2 = F_1 - 2$. Αν δεχτούμε ότι ισχύει για $n = k$, τότε

$$\begin{aligned}\prod_{j=0}^{k} F_j &= \left(\prod_{j=0}^{k-1} F_j\right) \cdot F_k = (F_k - 2) \cdot F_k \\ &= (2^{2^k} - 1)(2^{2^k} + 1) = 2^{2^{k+1}} - 1 \\ &= F_{k+1} - 2,\end{aligned}$$

δηλαδή η (3.3.15) ισχύει για $n = k + 1$. Έστω τώρα $0 \leqslant m < n$ και έστω d ένας κοινός θετικός διαιρέτης των F_m και F_n. Τότε

$$d \mid F_m \mid \prod_{j=0}^{n-1} F_j = F_n - 2,$$

άρα $d \mid F_n$ και $d \mid (F_n - 2)$. Έπεται ότι $d \mid 2$, άρα $d = 1$ ή $d = 2$. Αφού όλοι οι αριθμοί του Fermat είναι περιττοί, ο d δεν μπορεί να ισούται με 2. Άρα $(F_n, F_m) = 1$. □

Η πρώτη απόδειξη (του Ευκλείδη) είναι πολύ πιο σύντομη και κομψή. Κοιτάζοντας όμως τη δεύτερη απόδειξη παρατηρούμε το εξής: αν $p_1 < p_2 < \cdots < p_n < p_{n+1} < \cdots$ είναι η άπειρη ακολουθία των πρώτων αριθμών, τότε

$$p_n \leqslant F_{n-1} = 2^{2^{n-1}} + 1$$

για κάθε $n \in \mathbb{N}$. Πράγματι, οι $F_0, F_1, \ldots, F_{n-1}$ έχουν n διακεκριμένους πρώτους διαιρέτες $p_{k_1}, \ldots, p_{k_n}$, άρα

$$p_n \leqslant \max\{p_{k_1}, \ldots, p_{k_n}\} \leqslant \max\{F_0, F_1, \ldots, F_{n-1}\} = F_{n-1}.$$

Η παρατήρηση αυτή μας οδηγεί στον ορισμό μιας συνάρτησης $\pi : \mathbb{R} \to \mathbb{R}$, με

$$\pi(x) = \text{ το πλήθος των πρώτων αριθμών } p \leqslant x.$$

Η π είναι αύξουσα, και βέβαια $\pi(x) = 0$ αν $x < 2$. Παρατηρούμε ότι αν $x \geqslant 2$ και αν $n = n(x)$ είναι ο μεγαλύτερος μη αρνητικός ακέραιος για τον οποίο $2^{2^n} + 1 \leqslant x$, τότε

$$\pi(x) \geqslant \pi\big(2^{2^n} + 1\big) \geqslant n + 1.$$

Από την άλλη πλευρά, $2^{2^{n+1}} \geqslant x$ άρα $\log_2(\log_2 x) \leqslant n + 1$. Έχουμε λοιπόν το εξής κάτω φράγμα για την $\pi(x)$.

Πρόταση 3.3.25. *Για κάθε πραγματικό αριθμό $x \geqslant 2$ ισχύει η ανισότητα*

$$\pi(x) \geqslant \log_2(\log_2 x).$$

Ειδικότερα, $\pi(x) \to +\infty$ καθώς το $x \to +\infty$, άρα υπάρχουν άπειροι πρώτοι. □

Με άλλα λόγια, η δεύτερη απόδειξη μας δίνει επιπλέον πληροφορίες για το πλήθος των πρώτων αριθμών σε ένα διάστημα της μορφής $[0, x]$, όπου x είναι ένας «μεγάλος» θετικός πραγματικός αριθμός.

Το πρόβλημα της ασυμπτωτικής συμπεριφοράς της συνάρτησης $\pi(x)$ καθώς το $x \to +\infty$ απασχόλησε έντονα τους μαθηματικούς κατά τον 19ο αιώνα. Ο Legendre (1798) έκανε την εικασία ότι για μεγάλα x ο αριθμός $\pi(x)$ είναι περίπου ίσος με

$$\pi(x) \simeq \frac{x}{\ln x - A},$$

όπου $A \simeq 1.08366$. Ο Gauss πρότεινε την προσέγγιση

$$\pi(x) \simeq \int_2^x \frac{1}{\ln t} dt. \tag{3.3.16}$$

Το ολοκλήρωμα στο δεξιό μέλος είναι ουσιαστικά ίσο με $x/\ln x$ για μεγάλα x, οπότε μια ισχυρή εικασία που προκύπτει από την (3.3.16) είναι η

$$\lim_{x\to\infty} \frac{\pi(x)\ln x}{x} = 1. \tag{3.3.17}$$

Ο Chebyshev (1848) έδειξε ότι αν το όριο στην (3.3.17) υπάρχει, τότε θα είναι υποχρεωτικά ίσο με 1. Λίγο αργότερα (1850) έδειξε ότι υπάρχουν δύο θετικές σταθερές c_1 και c_2 τέτοιες ώστε

$$c_1 \frac{x}{\ln x} \leqslant \pi(x) \leqslant c_2 \frac{x}{\ln x}$$

για κάθε $x \geqslant 2$. Δηλαδή, η σωστή τάξη μεγέθους του $\pi(x)$ είναι $x/\ln x$.

Πολύ νωρίτερα, ο Euler (1740) είχε εισαγάγει τη συνάρτηση

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

για πραγματικές τιμές της μεταβλητής s και είχε παρατηρήσει ότι αναπαρίσταται σαν απειρογινόμενο:

$$\zeta(s) = \prod_{p\in P} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Ο Riemann (1860) παρατήρησε ότι αυτή η ταυτότητα θα μπορούσε να οδηγήσει σε χρήσιμα συμπεράσματα για την κατανομή των πρώτων αριθμών αν θεωρούσε κανείς τη συνάρτηση ζ σαν συνάρτηση μιας μιγαδικής μεταβλητής s και χρησιμοποιούσε τις μεθόδους της μιγαδικής ανάλυσης. Ο συμβολισμός $\zeta(s)$ οφείλεται στον Riemann, και η συνάρτηση αυτή είναι γνωστή με το όνομα «συνάρτηση Ζήτα του Riemann».

Το 1896, οι Hadamard και de la Vallée Poussin έδειξαν ανεξάρτητα και σχεδόν ταυτόχρονα ότι το όριο στην (3.3.17) υπάρχει και είναι ίσο με 1. Το αποτέλεσμα αυτό είναι γνωστό ως το «Θεώρημα των πρώτων αριθμών». Από τη δουλειά του de la Vallée Poussin έπεται ότι το ολοκλήρωμα (3.3.17)) που πρότεινε ο Gauss δίνει καλύτερη προσέγγιση για την τιμή του $\pi(x)$ απ¨ ότι δίνει η (3.3.16), όποια τιμή κι αν δοκιμάσει κανείς για τη σταθερά A.

3.4 Ασκήσεις

1. Ορίσαμε τις δυνάμεις m^n για $m \in \mathbb{N}$ και $n \in \mathbb{N}_0$ αναδρομικά, θέτοντας $m^0 = 1$ και $m^{n+1} = m^n m$. Θεωρώντας γνωστές τις ιδιότητες της πρόσθεσης και του πολλαπλασιασμού, αποδείξτε με κατάλληλα επαγωγικά επιχειρήματα ότι

$$m^{n+r} = m^n m^r \quad \text{και} \quad (mq)^r = m^r n^r$$

για κάθε $m, q \in \mathbb{N}$ και $n, r \in \mathbb{N}_0$.

2. Αποδείξτε με επαγωγή ότι για κάθε $n \in \mathbb{N}$ ισχύουν τα ακόλουθα:

(α) $3 \mid (n^3 - n)$.

(β) $1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4} = (1 + 2 + \cdots + n)^2$.

(γ) $1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)! - 1$.

(δ) $\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$.

3. Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύουν τα ακόλουθα:

(α) $133 \mid (11^{n+1} + 12^{2n-1})$.

(β) $1 \cdot 2 + 2 \cdot 3 + \cdots + n \cdot (n+1) = \frac{1}{3} n(n+1)(n+2)$.

(γ) $q + q^2 + \cdots + q^n = q\frac{1-q^n}{1-q}$, όπου $q \in \mathbb{R}$, $q \neq 1$.

4. Να βρείτε τους φυσικούς αριθμούς για τους οποίους ισχύει κάθε μία από τις ανισότητες:

(α) $n < 2^n$, (β) $n! > n$, (γ) $2^n \geqslant n^3 + 1$, (δ) $2n^2 < 3^{n-1}$, (ε) $n! < \left(\frac{n+1}{2}\right)^n$.

5. Έστω $\alpha, \beta \in \mathbb{R}$ με $\alpha + \beta > 0$. Αποδείξτε ότι, για κάθε $n \in \mathbb{N}_0$,

$$\frac{\alpha^n + \beta^n}{2} \geqslant \left(\frac{\alpha + \beta}{2}\right)^n.$$

6. Ορίζουμε αναδρομικά το $n!$ θέτοντας $0! = 1$ και $(n+1)! = n!(n+1)$.

(α) Αποδείξτε με επαγωγή ότι ο $(n-r)!r!$ διαιρεί τον $n!$ για κάθε r με $0 \leqslant r \leqslant n$.

(β) Ορίζουμε τον διωνυμικό συντελεστή

$$\binom{n}{r} = \frac{n!}{(n-r)!r!}.$$

Αποδείξτε ότι

$$\binom{n}{0} = 1, \qquad \binom{n}{1} = n, \qquad \binom{n}{r} = \binom{n}{n-r}.$$

(γ) Αποδείξτε ότι

$$\binom{n}{r} + \binom{n}{r-1} = \binom{n+1}{r}.$$

(δ) Αποδείξτε με επαγωγή ότι

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{r}a^{n-r}b^r + \cdots + \binom{n}{n}b^n.$$

7. Αποδείξτε ότι

$$\binom{n}{1} + 2\binom{n}{2} + \cdots + n\binom{n}{n} = n \cdot 2^{n-1}$$

για κάθε $n \in \mathbb{N}$.

8. (α) Αποδείξτε ότι

$$2 \cdot 6 \cdot 10 \cdot 14 \cdots (4n-2) = \frac{(2n)!}{n!}$$

για κάθε $n \in \mathbb{N}$.

(β) Χρησιμοποιώντας το (α) αποδείξτε ότι $2^n(n!)^2 \leqslant (2n)!$ για κάθε $n \geqslant 1$.

9. Με τη μέθοδο της επαγωγής αποδείξτε ότι

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leqslant 2 - \frac{1}{n}$$

για κάθε $n \geqslant 1$.

10. Με τη μέθοδο της επαγωγής αποδείξτε ότι

$$2(\sqrt{n++1} - 1) \leqslant 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} \leqslant 2\sqrt{n} - 1.$$

για κάθε $n \geqslant 1$.

11. Με τη μέθοδο της επαγωγής αποδείξτε ότι

$$\frac{1}{\sqrt{n}} 2^{2n-1}(n!)^2 \leqslant (2n)! \leqslant 2^{2n-1}(n!)^2$$

για κάθε $n \geqslant 1$.

12. Με τη μέθοδο της επαγωγής αποδείξτε ότι

$$\frac{1}{2}\frac{3}{4}\frac{5}{6}\cdots\frac{2n-1}{2n} < \frac{1}{\sqrt{2n+1}}$$

για κάθε $n \geqslant 1$.

13. Με τη μέθοδο της επαγωγής αποδείξτε την ανισότητα Cauchy-Schwarz: για κάθε $n \geqslant 2$, αν $x_1, \ldots, x_n$ και $y_1, \ldots, y_n$ είναι πραγματικοί αριθμοί, τότε

$$(x_1y_1 + x_2y_2 + \cdots + x_ny_n)^2 \leqslant (x_1^2 + x_2^2 \cdots + x_n^2)(y_1^2 + y_2^2 + \cdots + y_n^2).$$

14. Οι αριθμοί Fibonacci (u_n) ορίζονται αναδρομικά ως εξής: $u_1 = 1$, $u_2 = 2$ και

$$u_{n+1} = u_n + u_{n-1}, \qquad n \geqslant 2.$$

Αποδείξτε ότι κάθε φυσικός αριθμός γράφεται ως άθροισμα αριθμών Fibonacci. Είναι αυτή η παράσταση μοναδική;

15. (α) Αποδείξτε ότι αν p/q είναι ανάγωγο κλάσμα τέτοιο ώστε $\frac{1}{n+1} < \frac{p}{q} < \frac{1}{n}$ για κάποιον $n \in \mathbb{N}$ τότε ο $\frac{p}{q} - \frac{1}{n+1}$ αν γραφτεί σε ανάγωγη μορφή έχει αριθμητή μικρότερο από p.
(β) Χρησιμοποιώντας το (α) αποδείξτε με επαγωγή ότι κάθε κλάσμα p/q με $p < q$ μπορεί να γραφτεί στη μορφή

$$\frac{p}{q} = \frac{1}{n_1} + \cdots + \frac{1}{n_k},$$

όπου $n_1, \ldots, n_k$ είναι φυσικοί αριθμοί.

16. Αποδείξτε ότι κάθε θετικός ακέραιος ο οποίος στο δεκαδικό σύστημα αποτελείται από 3^n όμοια ψηφία διαιρείται με το 3^n (π.χ. ο 777 διαιρείται με το 3, ο 222222222 διαιρείται με το 9 κλπ). *Υπόδειξη*: επαγωγή στο n.

17. Έστω $a, b \in \mathbb{N}$. Αν $(a, b) = ax + by$ για κάποιους $x, y \in \mathbb{Z}$, αποδείξτε ότι $(x, y) = 1$.

18. Έστω $a, b \in \mathbb{N}$ με $(a, b) = 1$.
(α) Ποιες είναι οι δυνατές τιμές του $(a + b, ab)$;
(β) Ποιες είναι οι δυνατές τιμές του $(a + b, a^2 + ab + b^2)$;
(γ) Ποιες είναι οι δυνατές τιμές του $(a + b, a^2 + b^2)$;

19. Αποδείξτε τις παρακάτω ιδιότητες του μέγιστου κοινού διαιρέτη.

(α) $(a, bc) = 1$ αν και μόνο αν $(a, b) = (a, c) = 1$.

(β) Αν $(a, b) = 1$ και $c \mid b$ τότε $(a, c) = 1$.

(γ) Αν $(a, b) = 1$ τότε $(a, bc) = (a, c)$.

(δ) $(a, b) = 1$ αν και μόνο αν $(a^2, b^2) = 1$.

Σε όλα τα ερωτήματα υποθέτουμε ότι $a, b, c \in \mathbb{N}$.

20. Έστω $d, n \in \mathbb{N}$. Αν $d \mid n$, τότε $(2^d - 1) \mid (2^n - 1)$. *Υπόδειξη:* Χρησιμοποιήστε την ταυτότητα $x^k - 1 = (x - 1)(x^{k-1} + x^{k-2} + \cdots + x + 1)$.

21. Αποδείξτε ότι το γινόμενο k διαδοχικών φυσικών διαιρείται με $k!$. *Υπόδειξη:* Αποδείξτε με επαγωγή ότι ο $\binom{n}{k}$ είναι ακέραιος.

22. (α) Αν ο n είναι πρώτος και ο k είναι ακέραιος με $1 \leq k \leq n - 1$ αποδείξτε ότι ο n διαιρεί το $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.
(β) Ισχύει το (α) χωρίς να υποθέσουμε ότι ο n είναι πρώτος;

23. Έστω $a, m, n \in \mathbb{N}$ με $a > 1$. Αποδείξτε ότι $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

24. Αποδείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $4n - 1$. *Υπόδειξη:* Μιμηθείτε το επιχείρημα του Ευκλείδη.

25. Υποθέτουμε ότι ο $2^n + 1$ είναι πρώτος για κάποιον $n \geqslant 2$ (οι πρώτοι αυτής της μορφής λέγονται *πρώτοι του Fermat*). Αποδείξτε ότι ο n είναι δύναμη του 2.

26. Υποθέτουμε ότι ο $2^n - 1$ είναι πρώτος για κάποιον $n \in \mathbb{N}$ (οι πρώτοι αυτής της μορφής λέγονται *πρώτοι του Mersenne*). Αποδείξτε ότι ο n είναι πρώτος.

27. Έστω p ένας πρώτος αριθμός. Αποδείξτε ότι ο $\sqrt{p}$ είναι άρρητος.

28. Αποδείξτε ότι ο $f(n) = n^2 + n + 41$ είναι πρώτος για $n = 0, 1, \ldots, 39$. Τι συμβαίνει όταν $n = 40$;

29. Αποδείξτε ότι δεν υπάρχει πολυώνυμο $f(x) = a_0 + a_2 x + \cdots + a_k x^k$, $k \geqslant 1$, $a_k \neq 0$, με συντελεστές ακεραίους, για το οποίο όλοι οι αριθμοί $|f(n)|$, $n \geqslant 0$ να είναι πρώτοι.

30. Έστω $n \geqslant 2$. Αποδείξτε ότι ο $(n+1)! + k$ είναι σύνθετος για κάθε $k = 2, \ldots, n+1$. Αυτό αποδεικνύει ότι υπάρχουν οσοδήποτε μακριά διαστήματα διαδοχικών σύνθετων αριθμών.

31. Αποδείξτε ότι $2^n \mid (n + 1)(n + 2) \cdots (2n)$ για κάθε $n \in \mathbb{N}$.

32. Αν $n \geqslant 2$ αποδείξτε ότι το άθροισμα

$$\sum_{k=1}^{n} \frac{1}{k}$$

δεν είναι ακέραιος.

Κεφάλαιο 4

Πληθάριθμοι

4.1 Ισοπληθικά σύνολα

Ορισμός 4.1.1 (ισοπληθικότητα)**.** Έστω A, B δύο μη κενά σύνολα. Τα A, B λέγονται *ισοπληθικά* αν υπάρχει μια συνάρτηση $f : A \to B$, η οποία είναι αμφιμονοσήμαντη. Λέμε τότε ότι έχουμε μια αντιστοιχία από το A στο B και γράφουμε $A \rightarrowtail B$.

Εάν τα σύνολα A και B είναι ισοπληθικά, γράφουμε $A =_c B$ ή $|A| = |B|$ ή και $A \sim B$.

Η επόμενη πρόταση μας λέει ότι η ισοπληθικότητα μεταξύ συνόλων είναι σχέση ισοδυναμίας στην *κλάση* όλων των συνόλων.

Πρόταση 4.1.2. *Έστω A, B, C μη κενά σύνολα. Τότε ισχύουν τα ακόλουθα:*
(α) $A \sim A$,
(β) *αν* $A \sim B$, *τότε* $B \sim A$ *και*
(γ) *αν* $A \sim B$ *και* $B \sim C$, *τότε* $A \sim C$.

Απόδειξη. (α) Για κάθε σύνολο A ισχύει $A \sim A$, αφού υπάρχει η ταυτοτική απεικόνιση $id_A : A \to A$ με $id_A(x) = x$ η οποία είναι αμφιμονοσήμαντη.

(β) Εάν $A \sim B$, τότε υπάρχει αμφιμονοσήμαντη απεικόνιση $f : A \to B$, άρα υπάρχει και η αμφιμονοσήμαντη απεικόνιση $f^{-1} : B \to A$, συνεπώς $B \sim A$.

(γ) Εάν $A \sim B$ και $B \sim C$, υπάρχουν αμφιμονοσήμαντες απεικονίσεις $f : A \to B$ και $g : B \to C$. Τότε η σύνθεση $g \circ f : A \to C$ είναι αμφιμονοσήμαντη, συνεπώς $A \sim C$. □

Παραδείγματα 4.1.3. (1) Το σύνολο $\mathbb{N}$ και το σύνολο $\mathbb{N}_0 = \{0, 1, 2, \dots\}$ είναι ισοπληθικά, μέσω της αντιστοιχίας

$$f : \mathbb{N} \rightarrowtail \mathbb{N}_0 : n \mapsto n - 1.$$

(2) Το σύνολο των φυσικών $\mathbb{N}$ είναι ισοπληθικό με το σύνολο των αρτίων φυσικών $A = \{2n : n \in \mathbb{N}\}$ μέσω της αντιστοιχίας

$$\mathbb{N} \rightarrowtail A : n \mapsto 2n.$$

(3) Το σύνολο $\mathbb{N}$ είναι ισοπληθικό με το σύνολο των αρνητικών ακέραιων $\{a \in \mathbb{Z} : a < 0\}$, αφού η απεικόνιση

$$\mathbb{N} \rightarrowtail \{a \in \mathbb{Z} : a < 0\} : n \mapsto -n$$

είναι αμφιμονοσήμαντη.

(4) Το σύνολο $\mathbb{N}$ είναι ισοπληθικό με το σύνολο των τετραγώνων των φυσικών, λόγω της αντιστοιχίας

$$\mathbb{N} \rightarrowtail \{n^2 : n \in \mathbb{N}\} : n \mapsto n^2$$

Αξίζει να παρατηρήσουμε ότι τα Παραδείγματα (1), (2) και (4) μας δείχνουν ότι ένα σύνολο μπορεί να είναι ισοπληθικό με *γνήσιο* υποσύνολο του.

(5) Τα ανοιχτά διαστήματα $(0, 1)$ και $(0, 2)$ είναι ισοπληθικά, μέσω της αντιστοιχίας

$$f : (0, 1) \rightarrowtail (0, 2) : f(x) = 2x.$$

Γενικότερα, κάθε ανοιχτό διάστημα $(a, b),\ a, b \in \mathbb{R},\ a < b$, είναι ισοπληθικό με το $(0, 1)$ μέσω της αντιστοιχίας

$$f : (0, 1) \rightarrowtail (a, b) : f(t) = (1 - t)a + tb.$$

Λόγω της μεταβατικής ιδιότητας της ισοπληθικότητας, παίρνουμε ότι για κάθε $a, b, c, d \in \mathbb{R}$ με $a < b$ και $c < d$, ισχύει

$$(a, b) \sim (c, d).$$

(6) Επειδή η απεικόνιση

$$\tan : (-\frac{\pi}{2}, \frac{\pi}{2}) \rightarrow \mathbb{R} : x \mapsto \tan x$$

είναι αμφιμονοσήμαντη, το $\mathbb{R}$ είναι ισοπληθικό με το διάστημα $(-\frac{\pi}{2}, \frac{\pi}{2})$, επομένως και με κάθε διάστημα (a, b).

(7) Το $\mathbb{R}$ είναι ισοπληθικό με τον (ανοιχτό) ημιάξονα $(0, +\infty)$, λόγω της αντιστοιχίας

$$\mathbb{R} \rightarrowtail (0, +\infty) : x \mapsto e^x.$$

Επίσης, $(0, +\infty) \sim (a, +\infty)$, για οποιοδήποτε $a \in \mathbb{R}$, αφού η

$$(0, +\infty) \rightarrowtail (a, +\infty) : x \mapsto x + a$$

είναι αμφιμονοσήμαντη. Άρα και

$$\mathbb{R} \sim (a, +\infty), \quad \forall\, a \in \mathbb{R}.$$

Εξάλλου, προφανώς, $(0, +\infty) \sim (-\infty, 0) \sim (-\infty, b)$, $b \in \mathbb{R}$. Συνοψίζοντας, έχουμε

$$\mathbb{R} \sim (a, b) \sim (c, +\infty) \sim (-\infty, c),$$

για κάθε $a, b, c \in \mathbb{R}$ με $a < b$.

Όλα τα διαστήματα που εμφανίζονται στα Παραδείγματα (5), (6) και (7) είναι *ανοιχτά*. Τί συμβαίνει αν «κλείσουμε» το ένα (τουλάχιστον) άκρο;

(8) Τα σύνολα $(0, 1)$ και $(0, 1]$ είναι ισοπληθικά. Πράγματι: θεωρούμε το σύνολο $A = \{\frac{1}{n} : n \in \mathbb{N}\}$, το οποίο είναι υποσύνολο του $(0, 1]$ και ορίζουμε τη συνάρτηση $f : (0, 1] \to (0, 1)$ με

$$f(x) = \begin{cases} \frac{1}{n+1}, & \text{αν } x \in A \text{ και } x = \frac{1}{n} \\ x, & \text{διαφορετικά} \end{cases}$$

Εύκολα ελέγχουμε ότι η f είναι αντιστοιχία.

Εδώ αξίζει να παρατηρήσουμε ότι σε αντίθεση με όλες τις συναρτήσεις που ορίστηκαν στα παραδείγματα (5-7) μεταξύ (ανοιχτών) διαστημάτων, η συνάρτηση του Παραδείγματος (8) *δεν είναι συνεχής*. Μπορεί να βρεθεί συνεχής αμφιμονοσήμαντη απεικόνιση μεταξύ των $(0, 1)$ και $(0, 1]$;

Ορισμός 4.1.4. Έστω A, B δύο σύνολα. Λέμε ότι *το A έχει πληθάριθμο το πολύ ίσο με αυτόν του B,* αν υπάρχει 1-1 συνάρτηση $f : A \to B$. Γράφουμε $A \leqslant_c B$ ή $A \preceq B$. Ο συμβολισμός και η ορολογία δικαιολογούνται από το γεγονός ότι το A είναι ισοπληθικό με το $f(A)$ το οποίο είναι υποσύνολο του B.

Πρόταση 4.1.5. *Έστω A, B σύνολα. Οι επόμενες προτάσεις είναι ισοδύναμες:*
(i) $A \preceq B$.
(ii) *Υπάρχει συνάρτηση επί* $g : B \to A$.
(iii) *Υπάρχει* $C \subseteq B$ *με* $A \sim C$.

Απόδειξη. Γνωρίζουμε από την θεωρία συναρτήσεων ότι υπάρχει συνάρτηση 1-1 $f : A \to B$, εάν και μόνον εάν υπάρχει συνάρτηση επί $g : B \to A$. Άρα ισχύει $(i) \Leftrightarrow (ii)$.

Δείχνουμε ότι $(i) \Leftrightarrow (iii)$: Έστω ότι υπάρχει $f : A \to B$ που είναι 1-1. Θέτουμε $C := f(A) \subseteq B$. Τότε η $f : A \to C$ είναι αμφιμονοσήμαντη, άρα $A \sim C$. Έστω τώρα ότι

υπάρχει ένα σύνολο $C \subseteq B$ και μια 1-1 και επί συνάρτηση $f : A \to C$. Θεωρούμε και την *κανονική εμφύτευση*

$$i : C \longrightarrow B : x \longmapsto i(x) = x.$$

Τότε η συνάρτηση $i \circ f$ είναι 1-1, σαν σύνθεση δύο 1-1 συναρτήσεων. □

Στα προηγούμενα δείξαμε ότι η σχέση «$\sim$» είναι σχέση ισοδυναμίας στην κλάση όλων των συνόλων. Είναι φυσικό να γενηθεί το ερώτημα αν η σχέση $\preceq$ είναι (ολική) διάταξη. Είναι εύκολο να παρατηρήσουμε ότι:

(1) Για οποιοδήποτε σύνολο A, η ταυτοτική id_A είναι 1-1, άρα $A \preceq A$ και η σχέση είναι ανακλαστική.

(2) Αν A, B, C είναι σύνολα με $A \preceq B$ και $B \preceq C$, τότε υπάρχουν 1-1 συναρτήσεις $f : A \to B$ και $g : B \to C$, άρα υπάρχει και η συνάρτηση $g \circ f : A \to C$ που είναι 1-1 σαν σύνθεση τέτοιων. Άρα η σχέση είναι μεταβατική.

(3) Για να είναι αντισυμμετρική, θα έπρεπε να ισχύει η συνεπαγωγή

$$A \preceq B \text{ και } B \preceq A \Rightarrow A = B,$$

κάτι που σίγουρα δεν είναι σωστό (γιατί;). Θα περιμέναμε όμως ίσως να ισχύει στη θέση της η συνεπαγωγή

$$A \preceq B \text{ και } B \preceq A \Rightarrow A \sim B$$

το οποίο αντιστοιχεί στην επόμενη ερώτηση: *Έστω ότι υπάρχουν 1-1 απεικονίσεις $f : A \to B$ και $g : B \to A$. Μπορεί να εξασφαλιστεί η ύπαρξη μιας αμφιμονοσήμαντης $h : A \to B$;* Η απάντηση δίνεται στο επόμενο περιώνυμο και ενδιαφέρον

Θεώρημα 4.1.6 (Schröder–Bernstein). *Αν $X \preceq Y$ και $Y \preceq X$, τότε $X \sim Y$.*

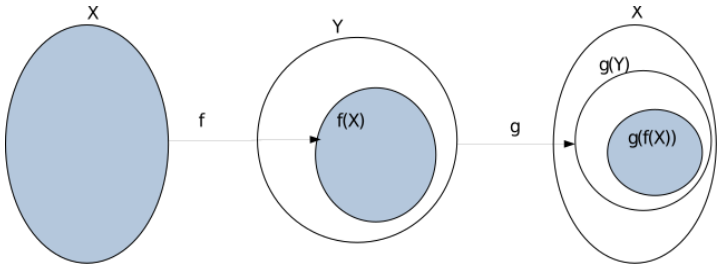
Απόδειξη. Από τις υποθέσεις προκύπτει ότι υπάρχουν δύο 1-1 συναρτήσεις $f : X \to Y$ και $g : Y \to X$. Σκοπός μας είναι να βρούμε μια 1-1 και επί συνάρτηση $h : X \to Y$. Θεωρούμε την σύνθεση

$$g \circ f : X \to X$$

που είναι 1-1, σαν σύνθεση τέτοιων, και παρατηρούμε ότι αν την θεωρήσουμε σαν απεικόνιση

$$g \circ f : X \to g(f(X)) \subseteq X$$

είναι αμφιμονοσήμαντη.



Δηλαδή έχουμε

$$g(f(X)) \subseteq g(Y) \subseteq X$$

με

$$g(f(X)) \sim X.$$

Επειδή $g(Y) \sim Y$, πρέπει να δείξουμε ότι $X \sim g(Y)$. Αυτό προκύπτει από το επόμενο

Λήμμα 4.1.7. *Αν $A_1 \subseteq B \subseteq A$ και $A_1 \sim A$, τότε $B \sim A$.*

Απόδειξη. Από την υπόθεση έχουμε την ύπαρξη μιας αμφιμονοσήμαντης $f : A \to A_1$. Θέτουμε $A_0 = A$, $B_0 = B$ και ορίζουμε αναδρομικά

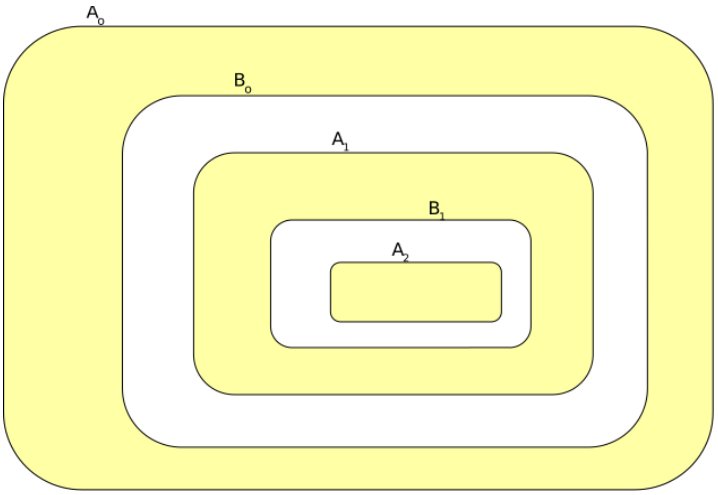
$$A_{n+1} = f(A_n), \qquad B_{n+1} = f(B_n), \quad \forall\, n \in \mathbb{N}_0.$$

Ο εγκλεισμός της υπόθεσης μας δίνει

$$\begin{aligned}
&A_0 \supseteq B_0 \supseteq A_1 \;\Rightarrow \\
&f(A_0) \supseteq f(B_0) \supseteq f(A_1) \;\Leftrightarrow\; A_1 \supseteq B_1 \supseteq A_2 \;\Rightarrow \\
&f(A_1) \supseteq f(B_1) \supseteq f(A_2) \;\Leftrightarrow\; A_2 \supseteq B_2 \supseteq A_3 \;\Rightarrow \\
&\dots
\end{aligned}$$

Προφανώς, συνεχίζοντας επαγωγικά παίρνουμε

$$A_n \supseteq B_n \supseteq A_{n+1}, \qquad \forall\, n \in \mathbb{N}_0.$$



Έτσι το αρχικό σύνολο $A = A_0$ χωρίζεται σε μια οικογένεια διαφορών $(C_n := A_n \setminus B_n)_{n\in\mathbb{N}_0}$, που φαίνεται στο ανωτέρω σχήμα χρωματισμένη και σε μια οικογένεια διαφορών $(B_n \setminus A_{n+1})_{n\in\mathbb{N}_0}$, που φαίνεται άχρωμη. Ονομάζουμε C το χρωματισμένο σύνολο, δηλ.

$$C := \bigcup_{n\in\mathbb{N}_0} C_n = \bigcup_{n\in\mathbb{N}_0} (A_n \setminus B_n)$$

Παρατηρούμε ότι

$$A \setminus C = B \setminus C.$$

Ισχυριζόμαστε τώρα ότι για κάθε $n \in \mathbb{N}_0$ ισχύει $f(C_n) = C_{n+1}$. Πράγματι, έστω $x \in C_n = A_n \setminus B_n$, δηλ. $x \in A_n$ και $x \notin B_n$. Τότε $f(x) \in f(A_n) = A_{n+1}$, και $f(x) \notin f(B_n) = B_{n+1}$, διότι αν $f(x) \in B_{n+1}$, υπάρχει $z \in B_n$ με $f(z) = f(x)$ όπου $B \ni z \neq x \notin B_n$, που είναι άτοπο, λόγω του 1-1 της f. Δηλ. $f(C_n) \subseteq C_{n+1}$. Επίσης η εικόνα $f(C_n)$ καλύπτει όλο το C_{n+1}. Πράγματι, έστω $y \in C_{n+1} = A_{n+1} \setminus B_{n+1}$. Επειδή $y \in A_{n+1}$, υπάρχει $x \in A_n$ με $f(x) = y$. Αν $x \in B_n$, τότε $y = f(x) \in B_{n+1}$, άτοπο, άρα $x \in A_n \setminus B_n = C_n$ και $y = f(x) \in f(C_n)$.

Συνεπώς, ο περιορισμός

$$f|_C : C = \bigcup_{n\in\mathbb{N}_0} C_n \longrightarrow f(C) = \bigcup_{n\in\mathbb{N}} C_n = B \cap C$$

είναι αμφιμονοσήμαντη απεικόνιση. Τώρα ορίζουμε

$$g : A = C \cup (A \setminus C) \longrightarrow B = (B \cap C) \cup (B \setminus C)$$
$$g(x) = \begin{cases} f(x), & x \in C \\ x, & x \in A \setminus C \end{cases}$$

Παρατηρούμε ότι η g είναι η ένωση των δύο αμφιμονοσήμαντων απεικονίσεων $f : C \to B \cap C$ και $id : A \setminus C \to A \setminus C = B \setminus C$ που ορίζονται σε δύο ξένα σύνολα και παίρνουν τιμές πάλι σε δύο ξένα σύνολα, άρα η g είναι και αυτή αμφιμονοσήμαντη. □

4.2 Αριθμήσιμα σύνολα

Συμβολισμός. Συμβολίζουμε με T_n το σύνολο των πρώτων n φυσικών, δηλαδή

$$T_n = \{1, 2, \dots n\}.$$

Ορισμός 4.2.1 (πεπερασμένα και άπειρα αριθμήσιμα σύνολα)**.** Έστω A σύνολο. Το A λέγεται

(α) *πεπερασμένο* αν $A = \emptyset$ ή αν υπάρχει $n \in \mathbb{N}$ με $A \sim T_n$,

(β) *άπειρο αριθμήσιμο* αν $A \sim \mathbb{N}$,

(γ) *αριθμήσιμο*, αν είναι πεπερασμένο ή άπειρο αριθμήσιμο.

Αν $A = \emptyset$, λέμε ότι ο *πληθάριθμος του A είναι* 0 ή ότι *το A έχει* 0 *στοιχεία.* Αν $A \sim T_n$, λέμε ότι ο *πληθάριθμος του A είναι* n ή ότι *το A έχει* n *στοιχεία.* Γράφουμε

$$\mathrm{card}(A) = n \ \ \textit{ή} \ \ \#A = n \ \ \textit{ή και} \ \ |A| = n, \quad n \in \mathbb{N}_o.$$

Του πληθάριθμο του $\mathbb{N}$ τον συμβολίζουμε με ω ή $\aleph_0$ (άλεφ 0). Έτσι, αν το σύνολο A είναι άπειρο αριθμήσιμο γράφουμε $|A| = \aleph_0$.

Λήμμα 4.2.2. *Κάθε $A \subseteq \mathbb{N}$ είναι αριθμήσιμο.*

Απόδειξη. Έστω $A \subseteq \mathbb{N}$. Τότε:

Αν $A = \emptyset$, τότε A είναι πεπερασμένο, άρα αριθμήσιμο. Αν $A \neq \emptyset$, τότε από την Αρχή Ελαχίστου (ΑΕ) υπάρχει ελάχιστο στοιχείο $\varphi(1) \in A$. Θεωρούμε το σύνολο $A \setminus \{\varphi(1)\}$.

Αν $A \setminus \{\varphi(1)\} = \emptyset$, τότε $A = \{\varphi(1)\} \sim \{1\} = T_1$, δηλ. A είναι πεπερασμένο, άρα αριθμήσιμο. Αν $A \setminus \{\varphi(1)\} \neq \emptyset$, τότε (πάλι από την ΑΕ) υπάρχει ελάχιστο $\varphi(2) \in A \setminus \{\varphi(1)\}$. Παρατηρούμε ότι $\varphi(1) < \varphi(2)$. Θεωρούμε το σύνολο $A \setminus \{\varphi(1), \varphi(2)\}$.

Αν $A \setminus \{\varphi(1), \varphi(2)\} = \emptyset$, τότε $A = \{\varphi(1), \varphi(2)\} \sim \{1, 2\} = T_2$, δηλ. A είναι πεπερασμένο, άρα αριθμήσιμο. Αν $A \setminus \{\varphi(1), \varphi(2)\} \neq \emptyset$, τότε (πάλι από την ΑΕ) υπάρχει ελάχιστο

στοιχείο $\varphi(3) \in A \setminus \{\varphi(1), \varphi(2)\}$. Παρατηρούμε ότι $\varphi(2) < \varphi(3)$. Θεωρούμε το σύνολο $A \setminus \{\varphi(1), \varphi(2), \varphi(3)\}$, και συνεχίζουμε επαγωγικά.

Αυτή η διαδικασία μπορεί να σταματήσει ή να μην σταματήσει:

Αν υπάρχει $n \in \mathbb{N}$ έτσι ώστε $A \setminus \{\varphi(1), \ldots, \varphi(n)\} = \emptyset$, τότε

$$A = \{\varphi(1), \ldots, \varphi(n)\} \sim \{1, \ldots, n\} = T_n,$$

δηλ. A είναι πεπερασμένο, άρα αριθμήσιμο.

Αν για κάθε $n \in \mathbb{N}$, $A \setminus \{\varphi(1), \ldots, \varphi(n)\} \neq \emptyset$, τότε ορίζεται η συνάρτηση

$$\varphi : \mathbb{N} \longrightarrow A : n \longmapsto \varphi(n).$$

Ισχυριζόμαστε ότι η φ είναι αμφιμονοσήμαντη. Πράγματι, επειδή $\varphi(n) < \varphi(n+1)$, για κάθε $n \in \mathbb{N}$, η $\varphi(n)$ είναι γνησίως αύξουσα. Επομένως είναι 1-1. Ιδιαιτέρως, είναι μια γνησίως αύξουσα ακολουθία φυσικών αριθμών, άρα $\varphi(n) \geqslant n$, για κάθε $n \in \mathbb{N}$ (απόδειξη: επαγωγικά).

Είναι και επί: Έστω $x \in A$. Τότε $x \in \mathbb{N}$ και $x \leqslant \varphi(x) < \varphi(x+1)$, άρα υπάρχει $n = x + 1 \in \mathbb{N}$ με $\varphi(n) > x$, δηλ. το σύνολο

$$A_x = \{n \in \mathbb{N} : \varphi(n) > x\}$$

είναι μη-κενό υποσύνολο του $\mathbb{N}$. Από την ΑΕ, έχει ελάχιστο στοιχείο, έστω το $m \in A_x$. Οπότε

$$x < \varphi(m) < \varphi(n), \quad \forall\, n \in A_x,\ n \neq m.$$

Θεωρούμε το $m-1$ και την εικόνα του $\varphi(m-1)$. Επειδή $m - 1 < m = \min A$, προκύπτει ότι $m - 1 \notin A$, άρα θα είναι $\varphi(m-1) \leqslant x$.

Αν $\varphi(m-1) < x$, τότε $x, \varphi(m) \in A \setminus \{\varphi(1), \varphi(2), \ldots, \varphi(m-1)\}$ με $x < \varphi(m)$, άρα $\varphi(m) \neq \min(A \setminus \{\varphi(1), \varphi(2), \ldots, \varphi(m-1)\})$, άτοπο. Άρα $\varphi(m-1) = x$, οπότε $x \in \varphi(\mathbb{N})$, που είναι το ζητούμενο. □

Από τον ορισμό των αριθμήσιμων συνόλων, παίρνουμε ότι κάθε αριθμήσιμο σύνολο είναι ισοπληθικό με κάποιο υποσύνολο του $\mathbb{N}$. Από την προηγούμενη πρόταση, κάθε υποσύνολο του $\mathbb{N}$ είναι αριθμήσιμο. Αρα

$$A \text{ αριθμήσιμο } \Leftrightarrow A \preceq \mathbb{N}.$$

Επομένως είναι προφανής η επόμενη

Πρόταση 4.2.3. *Έστω A ένα σύνολο. Τα παρακάτω είναι ισοδύναμα:*

(i) Το A είναι αριθμήσιμο.

(ii) Υπάρχει 1-1 απεικόνιση $f : A \to \mathbb{N}$.

(iii) Υπάρχει επί απεικόνιση $g : \mathbb{N} \to A$.

Παραδείγματα 4.2.4. (α) Το καρτεσιανό γινόμενο $\mathbb{N}\times\mathbb{N}$ είναι άπειρο αριθμήσιμο, δηλαδή

$$\mathbb{N}\times\mathbb{N}\sim\mathbb{N}.$$

Πράγματι, η απεικόνιση

$$f:\mathbb{N}\times\mathbb{N}\longrightarrow\mathbb{N}:f(m,n)=2^{m-1}(2n-1)$$

είναι αμφιμονοσήμαντη.
(β) Το σύνολο $\mathbb{Z}$ των ακεραίων είναι άπειρο αριθμήσιμο, δηλ.

$$\mathbb{Z}\sim\mathbb{N}.$$

Πράγματι, η απεικόνιση

$$g:\mathbb{N}_0\to\mathbb{Z}:g(n)=\begin{cases}k, & n=2k,\ k\in\mathbb{N}_0\\ -k, & n=2n-1,\ k\in\mathbb{N}\end{cases}$$

είναι αμφιμονοσήμαντη. Άρα $\mathbb{N}\sim\mathbb{N}_0\sim\mathbb{Z}$.
(γ) Το σύνολο $\mathbb{Q}$ των ρητών είναι άπειρο αριθμήσιμο, δηλ.

$$\mathbb{N}\sim\mathbb{Q}.$$

Πράγματι, η κανονική εμφύτευση

$$i:\mathbb{N}\to\mathbb{Q}:i(n)=n$$

είναι 1-1, άρα $\mathbb{N}\preceq\mathbb{Q}$. Επίσης η απεικόνιση

$$q:\mathbb{Z}\times\mathbb{N}\to\mathbb{Q}:q(a,n)=\frac{a}{n}$$

είναι επί. Επειδή το σύνολο $\mathbb{Z}\times\mathbb{N}$ είναι άπειρο αριθμήσιμο (γιατί;), προκύπτει $\mathbb{Q}\preceq\mathbb{Z}\times\mathbb{N}\sim\mathbb{N}$. Άρα το ζητούμενο είναι αποτέλεσμα του Θεωρήματος Schröder-Bernstein.

4.3 Υπεραριθμήσιμα σύνολα

Ορισμός 4.3.1 (υπεραριθμήσιμα σύνολα)**.** Ένα σύνολο A λέγεται:

(α) *υπεραριθμήσιμο*, αν δεν είναι αριθμήσιμο

(β) *άπειρο*, αν είναι άπειρο αριθμήσιμο ή υπεραριθμήσιμο.

Με άλλα λόγια, ένα σύνολο είναι άπειρο αν δεν είναι πεπερασμένο.

Ισχύει ο επόμενος χαρακτηρισμός των άπειρων συνόλων:

Πρόταση 4.3.2. *Ένα σύνολο A είναι άπειρο αν και μόνο αν υπάρχει 1-1 συνάρτηση $f : \mathbb{N} \to A$.*

Απόδειξη. Η απόδειξη είναι μια παραλαγή της απόδειξης της Πρότασης 4.2.2. Έστω A ένα άπειρο σύνολο. Τότε το A δεν είναι πεπερασμένο, ιδιαιτέρως δεν είναι κενό, άρα υπάρχει $a_1 \in A$. Θεωρούμε το το σύνολο $A \setminus \{a_1\}$. Αν $A \setminus \{a_1\} = \emptyset$, τότε $A = \{a_1\}$= πεπερασμένο, άτοπο. Άρα $A \setminus \{a_1\} \neq \emptyset$ και υπάρχει $a_2 \in A \setminus \{a_1\}$. Συνεχίζουμε επαγωγικά και ορίζουμε ακολουθία (a_n) στοιχείων του A. Παρατηρούμε ότι για κάθε $n < m$, ισχύει $a_m \in A \setminus \{a_1, \ldots, a_n, \ldots, a_{m-1}\}$, άρα $a_n \neq a_m$. Αυτό σημαίνει ότι η απεικόνιση

$$\varphi : \mathbb{N} \longrightarrow A : \varphi(n) = a_n$$

είναι 1-1.

Αντίστροφα, έστω ότι υπάρχει 1-1 συνάρτηση $f : \mathbb{N} \to A$. Αν το A είναι πεπερασμένο, τότε υπάρχουν $n \in \mathbb{N}$ και αμφιμονοσήμαντη $g : A \to T_n$. Αλλά τότε η σύνθεση $g \circ f : \mathbb{N} \to T_n$ είναι 1-1, άτοπο (γιατί;). □

Υπενθυμίζουμε ότι η ύπαρξη μιας 1-1 απεικόνισης $f : \mathbb{N} \to A$ είναι ισοδύναμη με την ύπαρξη μιας επί απεικόνισης $g : A \to \mathbb{N}$.

Παραδείγματα 4.3.3. (α) Τα σύνολα $\mathbb{N}$, $\mathbb{Z}$ και $\mathbb{Q}$ είναι άπειρα, αφού είναι άπειρα αριθμήσιμα.

(β) Το $\mathbb{R}$ είναι άπειρο, αφού η κανονική εμφύτευση $i : \mathbb{N} \to \mathbb{R}$ είναι 1-1. Και επειδή για κάθε $a, b \in \mathbb{R}$ με $a < b$ είναι $(a, b) \sim \mathbb{R}$, κάθε ανοιχτό διάστημα (a, b) και κάθε (μη τετριμμένο) κλειστό διάστημα $[a, b]$ είναι άπειρο σύνολο.

Σκοπός μας είναι να αποδείξουμε ότι υπάρχουν μη-αριθμήσιμα, δηλ. υπεραριθμήσιμα σύνολα. Αρκεί να δείξουμε ότι κάποιο γνωστό μας σύνολο δεν μπορεί να αντιστοιχισθεί αμφιμονοσήμαντα με το $\mathbb{N}$. Ένα τέτοιο σύνολο είναι το $\mathbb{R}$ και τα ισοπληθικά του. Αρκεί να δείξουμε ότι το διάστημα $[0, 1]$ είναι υπεραριθμήσιμο.

Πρόταση 4.3.4. *Το σύνολο $[0, 1]$ είναι υπεραριθμήσιμο.*

Απόδειξη Α. Για την απόδειξη που ακολουθεί, υπενθυμίζουμε ότι: (α) Κάθε πραγματικός αριθμός $x \geqslant 0$ έχει μια «δεκαδική παράσταση»:

$$x = a_0\,,\, a_1\, a_2\, a_3 \ldots, \quad \text{όπου } a_0 \in \mathbb{N}_0 \text{ και } a_i \in \{0, 1, \ldots, 9\}\ \forall\ i \in \mathbb{N}.$$

(β) Οι αριθμοί της μορφής

$$x = a_0\,,\, a_1\, a_2 \ldots a_n\, 0\, 0\, 0\, 0 \ldots$$

με $a_n \neq 0$ έχουν ακριβώς δύο δεκαδικές παραστάσεις: την ανωτέρω και την

$$x = a_0\,,\, a_1\, a_2\, \ldots\, (a_n - 1)\, 9\, 9\, 9\, 9\, \ldots$$

Π.χ. $1,7 = 1,70000\cdots = 1,699999\ldots$. Ολοι οι άλλοι μη αρνητικοί πραγματικοί αριθμοί έχουν μοναδική δεκαδική παράσταση.

Γράφουμε κάθε $x \in [0,1]$ με δεκαδική μορφή. Για τους αριθμούς που έχουν δύο δεκαδικές παραστάσεις, επιλέγουμε την μία, π.χ. την μορφή με τα άπειρα 0, ώστε η δεκαδική παράσταση όλων των αριθμών να είναι μονοσήμαντη.

Γνωρίζουμε ότι το διάστημα $[0,1]$ είναι άπειρο (βλ. 4.3.3 (β)). Έστω προς άτοπο ότι το $[0,1]$ είναι αριθμήσιμο. Τότε υπάρχει απεικόνιση επί $\varphi : \mathbb{N} \to [0,1]$, άρα $[0,1] = \varphi(\mathbb{N}) = \{\varphi_n : n \in \mathbb{N}\}$. Δηλ.

$$\forall\, x \in [0,1]\ \exists\, n \in \mathbb{N}\ :\ x = \varphi_n.$$

Γράφουμε όλα τα φ_n με την δεκαδική μορφή που επιλέξαμε:

$$\begin{array}{rcccccc}
\varphi_1 &=& 0\,,\, a_1^1 & a_2^1 & a_3^1 & \ldots\ a_n^1 & \ldots \\
\varphi_2 &=& 0\,,\, a_1^2 & a_2^2 & a_3^2 & \ldots\ a_n^2 & \ldots \\
\varphi_3 &=& 0\,,\, a_1^3 & a_2^3 & a_3^3 & \ldots\ a_n^3 & \ldots \\
\vdots & & \vdots & \vdots & \vdots & & \vdots \\
\varphi_n &=& 0\,,\, a_1^n & a_2^n & a_3^n & \ldots\ a_n^n & \ldots \\
\vdots & & \vdots & \vdots & \vdots & & \vdots
\end{array}$$

Θεωρούμε τώρα ένα $\xi = 0,\xi_1\xi_2\xi_3\ldots\xi_n\cdots \in [0,1]$ επιλέγοντας $\xi_k \neq a_k^k$ και $\xi_k \neq 9$, $k \in \mathbb{N}$. Τότε προφανώς για κάθε $n \in \mathbb{N}$ ισχύει $\xi \neq \varphi_n$ και η φ δεν είναι επί, άτοπο.

Απόδειξη Β. Το σύνολο $[0,1]$ είναι άπειρο. Όπως και στην προηγούμενη απόδειξη, θεωρούμε ότι είναι αριθμήσιμο, οπότε μπορούμε να γράψουμε $[0,1] = \{x_n\ :\ n \in \mathbb{N}\}$. Διαιρούμε το $[0,1]$ σε τρία διαδοχικά ισομήκη διαστήματα ως εξής: $[0,1] = [0,1/3] \cup [1/3,2/3] \cup [2/3,1]$. Τότε, τουλάχιστον ένα από αυτά τα τρία διαστήματα δεν περιέχει το x_1. Ονομάζουμε αυτό το διάστημα I_1 και το διαιρούμε σε τρία ισομήκη διαδοχικά κλειστά διαστήματα (μήκους 1/9). Τουλάχιστον ένα από αυτά δεν περιέχει το x_2. Ονομάζουμε αυτό το διάστημα I_2. Συνεχίζουμε με τον ίδιο τρόπο, οπότε παίρνουμε μια φθίνουσα ακολουθία κλειστών διαστημάτων $I_n = [a_n, b_n]$ με $x_n \notin I_n$ και $b_n - a_n = 3/n \to 0$. Από την Αρχή Κιβωτισμού ισχύει $\cap_{n\in\mathbb{N}} I_n = \{x\}$. Αφού $x \in [0,1]$, υπάρχει $m \in \mathbb{N}$ ώστε $x = x_m$. Ατοπο, διότι $x \in I_n$ για κάθε $n \in \mathbb{N}$, ενώ $x_m \notin I_m$. □

Πόρισμα 4.3.5. *Το σύνολο των πραγματικών αριθμών $\mathbb{R}$ και το σύνολο των αρρήτων $\mathbb{R} \setminus \mathbb{Q}$ είναι υπεραριθμήσιμα.*

Τον πληθάριθμο του $\mathbb{R}$ τον συμβολίζουμε με $\aleph_1$ (άλεφ 1). Επειδή $\mathbb{N} \subset \mathbb{R}$, έχουμε $\aleph_0 \preceq \aleph_1$, κι επειδή $\mathbb{N} \not\approx \mathbb{R}$, είναι $\aleph_0 \neq \aleph_1$, άρα $\aleph_0 \prec \aleph_1$. Προκύπτει φυσιολογικά η ερώτηση «*υπάρχει πληθάριθμος γνήσια ανάμεσα στα* $\aleph_0$ *και* $\aleph_1$*;*» Ισοδύναμα, «*υπάρχει σύνολο* X *με* $\aleph_0 \prec |X| \prec \aleph_1$*;*» Γνωρίζουμε σήμερα, ότι με τα αξιώματα που δεχόμαστε στην Θεωρία Συνόλων (Αξιώματα μαζί με το Αξίωμα της Επιλογής) δεν μπορεί να αποδειχθεί ούτε η ύπαρξη ούτε η ανυπαρξία τέτοιου συνόλου.

Θεώρημα 4.3.6 (Cantor)**.** *Για κάθε σύνολο* X*, ισχύει* $X \prec \mathcal{P}(X)$.

Απόδειξη. Παρατηρούμε πρώτα, ότι $|\emptyset| = 0 < 1 = |\mathcal{P}(\emptyset)| = |\{\emptyset\}|$. Έστω ένα $X \neq \emptyset$. Τότε ορίζουμε την απεικόνιση $f : X \to \mathcal{P}(X)$ με $f(x) = \{x\}$, που είναι 1-1, άρα $X \preceq \mathcal{P}(X)$.

Θα δείξουμε τώρα ότι δεν υπάρχει $\varphi : X \to \mathcal{P}(X)$ που να είναι 1-1 και επί. Προς άτοπο, έστω ότι υπάρχει τέτοια φ. Για κάθε $x \in X$, είναι $\varphi(x) \subseteq X$, άρα ισχύει ακριβώς μια από τις δύο σχέσεις

$$x \in \varphi(x) \;\text{ ή }\; x \notin \varphi(x).$$

Θέτουμε

$$B = \{x \in X \;:\; x \notin \varphi(x)\} \subseteq X.$$

Αφού η φ είναι επί, υπάρχει $x_o \in X$ με $\varphi(x_o) = B$. Για το x_o, τί από τα δύο ισχύει; $x_o \in B$ ή $x_o \notin B$; Παρατηρούμε ότι: Αν $x_o \in B$, τότε $x_o \notin B$, άτοπο. Αν $x_o \notin B$, τότε $x_o \in B$, άτοπο. Το άτοπο έχει προκύψει από την υπόθεση ότι η φ είναι επί. Άρα δεν υπάρχει τέτοια φ, και $X \prec \mathcal{P}(X)$. □

Σύμφωνα με το τελευταίο θεώρημα, $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$. Γνωρίζουμε επίσης ότι $|\mathbb{N}| < |\mathbb{R}|$. Από όσα είπαμε μέχρι τώρα δεν φαίνεται πώς διατάσσονται οι πληθάριθμοι $|\mathcal{P}(\mathbb{N})|$ και $|\mathbb{R}|$ μεταξύ τους. Αξίζει να αναφέρουμε ότι

$$|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|.$$

4.4 Ασκήσεις

1. Δείξτε ότι κάθε άπειρο σύνολο έχει άπειρο αριθμήσιμο υποσύνολο.

2. Δείξτε ότι κάθε άπειρο σύνολο A είναι ισοπληθικό με κάποιο γνήσιο υποσύνολό του.

3. Αν $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, δείξτε ότι η απεικόνιση $f : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ με

$$f(m, n) = 2^m(2n + 1) - 1$$

είναι 1-1 και επί, και συμπεράνατε ότι $\mathbb{N}_0 \times \mathbb{N}_0 \sim \mathbb{N}_0$

4. Είναι το $\mathbb{R} \setminus \mathbb{Q}$ αριθμήσιμο;

5. Μια ακολουθία $(t_1, t_2, \ldots, t_n, \ldots)$ φυσικών αριθμών λέγεται *αριθμητική πρόοδος* αν υπάρχει $d \in \mathbb{N}$ ώστε $t_{n+1} = t_n + d$ για κάθε $n \in \mathbb{N}$. Δείξτε ότι το σύνολο όλων των αριθμητικών προόδων είναι αριθμήσιμο.

6. Ορίστε μια αμφιμονοσήμαντη απεικόνιση $f : (0,1) \to \mathbb{R}$ η οποία να απεικονίζει τους ρητούς σε ρητούς και τους άρρητους σε άρρητους.

7. (α) Έστω A ένα σύνολο από κυκλικούς δίσκους στο επίπεδο, οι οποίοι ανά δύο δεν τέμνονται. Δείξτε ότι το A είναι αριθμήσιμο.

(β) Έστω A ένα σύνολο από κύκλους στο επίπεδο, οι οποίοι ανά δύο δεν τέμνονται. Είναι το A αναγκαστικά αριθμήσιμο;

(γ) Έστω A ένα σύνολο από οχτάρια στο επίπεδο, τα οποία ανά δύο δεν τέμνονται. Είναι το A αναγκαστικά αριθμήσιμο;

8. Έστω A ένα σύνολο θετικών πραγματικών αριθμών. Υποθέτουμε ότι υπάρχει $M > 0$ με την εξής ιδιότητα: για κάθε πεπερασμένο υποσύνολο B του A, το άθροισμα των στοιχείων του B είναι μικρότερο από M. Δείξτε ότι το A είναι αριθμήσιμο.

9. Ένας πραγματικός αριθμός x λέγεται *αλγεβρικός* αν υπάρχουν $m \in \mathbb{N}$ και ακέραιοι $a_0, a_1, \ldots, a_m$ (με $a_m \neq 0$) ώστε

$$(*) \qquad a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0 = 0.$$

Δείξτε ότι το σύνολο όλων των αλγεβρικών αριθμών είναι αριθμήσιμο. [*Υπόδειξη*: Για κάθε $N \in \mathbb{N}$, το πλήθος των εξισώσεων της μορφής $(*)$ με $m + |a_0| + \cdots + |a_m| = N$ είναι πεπερασμένο.]

10. Έστω A, B, C τρία μη κενά σύνολα. Αν X είναι το σύνολο όλων των συναρτήσεων $f : B \to C$, Y είναι το σύνολο όλων των συναρτήσεων $g : A \to X$ και Z είναι το σύνολο όλων των συναρτήσεων $h : A \times B \to C$, δείξτε ότι $Z \sim Y$.

11. Έστω A άπειρο σύνολο και έστω B αριθμήσιμο σύνολο. Δείξτε ότι $A \sim A \cup B$.

12. Δείξτε ότι το $\mathbb{N}$ έχει άπειρα το πλήθος ξένα ανά δύο άπειρα υποσύνολα.

13. (α) Δείξτε ότι υπάρχει οικογένεια $\{A_x : x \in \mathbb{R}\}$ άπειρων υποσυνόλων του $\mathbb{Q}$ με την εξής ιδιότητα: αν $x \neq y$ τότε το $A_x \cap A_y$ είναι πεπερασμένο.

(β) Δείξτε ότι υπάρχει οικογένεια $\{A_x : x \in \mathbb{R}\}$ άπειρων υποσυνόλων του $\mathbb{N}$ με την εξής ιδιότητα: αν $x \neq y$ τότε το $A_x \cap A_y$ είναι πεπερασμένο.

14. Έστω $\{I_a \mid a \in A\}$ οικογένεια ξένων ανά δύο ανοικτών διαστημάτων. Δείξτε ότι το A είναι αριθμήσιμο.

15. Έστω $f : [a, b] \to \mathbb{R}$ γνησίως αύξουσα συνάρτηση. Δείξτε ότι το σύνολο των $x \in [a, b]$ στα οποία η f είναι ασυνεχής είναι αριθμήσιμο.