" Γνωρίζετε ότι γράφω με αργό ρυθμό. Αυτό οφείλεται κυρίως στο ότι δεν είμαι ποτέ ικανοποιημένος έως ότου έχω πει όσο το δυνατόν περισσότερα με λίγες λέξεις, και η συνοπτική γραφή απαιτεί πολύ περισσότερο χρόνο από την εκτενή γραφή."

Carl Friedrich Gauss (1777-1855)

Μια Εισαγωγή στην Άλγεβρα

Δεύτερη Έκδοση

Δημήτριος Α. Βάρσος
Δημήτριος Ι. Δεριζιώτης
Ιωάννης Π. Εμμανουήλ
Μιχαήλ Π. Μαλιάκας
Ολυμπία Ταλέλλη

[PO,ΛE]2 [ΛO] [PE]
[῎E,῎O]

Πρόλογος

Αυτό το βιβλίο απευθύνεται κυρίως σε προπτυχιακούς φοιτητές των Μαθηματικών.

Διδάσκοντας επί σειρά ετών Μαθηματικά, βρεθήκαμε απέναντι σε ένα σημαντικό παιδαγωγικό πρόβλημα: Τα Μαθηματικά -και ειδικά η Άλγεβρα- είναι από τη φύση τους "αφαιρετικά". Εκεί έγκειται η δυναμική τους αλλά και η σχεδόν καθολική χρησιμότητά τους. Πώς λοιπόν επιτυγχάνεται σε ένα εισαγωγικό μάθημα Άλγεβρας μια ισορροπία του αφαιρετικού στοιχείου με το συγκεκριμένο; Οι προσπάθειές μας για το σκοπό αυτό αποτυπώνονται στο παρόν βιβλίο.

Κύριο χαρακτηριστικό της αποτύπωσης αυτής είναι ότι καταβλήθηκε ιδιαίτερη προσπάθεια έτσι ώστε αφενός η αφαίρεση να πραγματοποιείται σταδιακά, δηλαδή να παρέχονται κίνητρα που να δικαιολογούν την εισαγωγή νέων εννοιών, και αφετέρου να επεξηγούνται με όσο το δυνατόν απλό τρόπο οι σημαντικές τεχνικές που χρησιμοποιούνται στις αποδείξεις των αποτελεσμάτων. Για το σκοπό αυτό, στο παρόν βιβλίο υπάρχει ένας μεγάλος αριθμός επεξεργασμένων παραδειγμάτων και εφαρμογών. Επειδή δε πεποίθησή μας είναι ότι η μελέτη των Μαθηματικών δεν αρμόζει σε θεατές αλλά απαιτεί ενεργητική συμμετοχή, επιχειρήσαμε να παρεμβάλουμε μέσα στο κείμενο απλές ερωτήσεις, ώστε να επιβεβαιώνεται από τον αναγνώστη κατά πόσο έχει κατανοήσει τις προηγηθείσες των ερωτήσεων έννοιες. Επίσης, έχουν συμπεριληφθεί αρκετές ασκήσεις έτσι ώστε ο φοιτητής που μελετά το βιβλίο να ενθαρρύνεται να χρησιμοποιεί "χαρτί και μολύβι".

Η λέξη "Άλγεβρα" είναι μέρος του τίτλου ενός Αραβικού κειμένου του 800 μ.Χ. το οποίο αναφερόταν στους κανόνες για τη λύση των εξισώσεων και μέχρι περίπου τα μέσα του 19ου αιώνα η Άλγεβρα ήταν ο κλάδος των Μαθηματικών που ασχολείτο με τη μελέτη των εξισώσεων.

Δεν υπάρχει αμφιβολία ότι ο όρος "δομή" κατέχει μια από τις κυριότερες θέσεις στα σύγχρονα Μαθηματικά. Πράγματι, η σωστή κατανόηση και μελέτη των δομών θεωρείται θεμελιώδες εργαλείο για την προώθηση μιας ενοποιημένης ανάπτυξης των Μαθηματικών. Ένα από τα σημαντικότερα είδη δομών αποτελεί ένα σύνολο εφοδιασμένο με μία ή περισσότερες πράξεις. Σήμερα, η Άλγεβρα

είναι η μελέτη ακριβώς αυτών των δομών. Για το λόγο αυτό, μπορεί κανείς να πει δικαιολογημένα ότι η Άλγεβρα δεν αποτελεί μόνο ένα μέρος των Μαθηματικών, αλλά ότι παίζει για τα Μαθηματικά το ρόλο που αυτά έπαιξαν και παίζουν στην ανάπτυξη των θετικών επιστημών.

Είναι κοινή πεποίθηση ότι η νέα αντίληψη για το ρόλο της Άλγεβρας που επικράτησε στη δεκαετία του 1920, η οποία συνδέεται με τα ονόματα της Emmy Noether, των Emil Artin, B.L. Van der Waerden, Hermann Weyl και άλλων επιφανών μαθηματικών, βασίστηκε στη μελέτη θεμελιωδών δομών όπως οι Ομάδες, οι Δακτύλιοι, τα Πρότυπα και τα Σώματα. Αυτή η αντίληψη της "Σύγχρονης Άλγεβρας" (ονομασία που υιοθετήθηκε για αυτή τη νέα τάση) οδήγησε σε μια θεμελιώδη, καινοτόμο και εξαιρετικά αποδοτική ανάπτυξη της Άλγεβρας. Κύριο χαρακτηριστικό αυτής της ανάπτυξης είναι ότι πριν λίγα χρόνια λύθηκαν σημαντικές εικασίες των προηγούμενων αιώνων, που αναφέρονται σε κλασικά Μαθηματικά. Ως ένα τέτοιο παράδειγμα πρέπει να αναφέρουμε τη μνημειώδη εικασία του Fermat, σύμφωνα με την οποία η εξίσωση $x^n + y^n = z^n$ δεν έχει καμιά ακέραια λύση (x, y, z), με τα x, y, z όλα διάφορα του μηδενός, όταν το $n \geq 3$. Η εικασία αυτή αποδείχτηκε ότι ισχύει, από τον Wiles, έπειτα από 350 χρόνια. Άλλα χαρακτηριστικά παραδείγματα είναι το 10ο, 14ο και 17ο πρόβλημα του Hilbert, όπως επίσης και οι εικασίες του André Weil. Ένα δε από τα σημαντικότερα αποτελέσματα που έχει επιτευχθεί μέχρι σήμερα στην Άλγεβρα θεωρείται η απόδειξη της εικασίας των Burnside και Galois, που αναφέρεται στην ίδια τη Θεωρία Ομάδων, για την ύπαρξη της ταξινόμησης των απλών πεπερασμένων ομάδων. Αποδείχθηκε το 1980 και απασχόλησε τους μεγαλύτερους αλγεβριστές του περασμένου αιώνα, κυρίως της περιόδου 1950-1980.

Το βιβλίο αυτό είναι όσο το δυνατόν αυτοδύναμο και καλύπτει τη βασική θεωρία των δακτυλίων και των ομάδων. Η δομή των δακτυλίων εξετάζεται στις Ενότητες 2 και 3, ενώ στις Ενότητες 4 και 5 αναπτύσσεται η θεωρία των ομάδων. Οι Ενότητες 2 και 4 είναι έτσι δομημένες, ούτως ώστε να είναι ανεξάρτητες η μία της άλλης. Συνεπώς, ο φοιτητής είναι ελεύθερος να μελετήσει τους δακτυλίους πριν ή μετά τις ομάδες. Στην Ενότητα 1 μελετώνται οι βασικές ιδιότητες των ακεραίων, καθώς και η έννοια της μοναδικής παραγοντοποίησης σε γινόμενο πρώτων αριθμών. Ένας από τους στόχους της Ενότητας 3 είναι να καταδείξει την έννοια αυτή γενικότερα στους δακτυλίους μοναδικής παραγοντοποίησης και κατόπιν να την εφαρμόσει για την επίλυση συγκεκριμένων Διοφαντικών εξισώσεων. Στην Ενότητα 1 μελετάται επίσης η αριθμητική των ισοτιμιών, ένα θεμελιώδες παράδειγμα που αναπτύσσεται γενικότερα στις Ενότητες 2 και 4. Στην Ενότητα 4 μελετάται η έννοια της συμμετρίας, που οδηγεί φυσιολογικά στην έννοια της ομάδας. Στη συνέχεια, αναπτύσσεται η βασική θεωρία των ομάδων και η νέα αυτή γνώση εφαρμόζεται για να ληφθούν αποτελέσματα στη στοιχειώδη θεω-

ρία αριθμών. Τέλος, στην Ενότητα 5 αναπτύσσεται η έννοια της δράσης μιας ομάδας, η οποία ουσιαστικά γενικεύει την έννοια της συμμετρίας. Ως βασική εφαρμογή αυτής της έννοιας, αποδεικνύουμε τα θεωρήματα του Sylow, που είναι από τα πιο σημαντικά αποτελέσματα της θεωρίας των πεπερασμένων ομάδων.

Επειδή πιστεύουμε ότι ένα εισαγωγικό βιβλίο οφείλει να παρέχει κατευθύνσεις στον ενδιαφερόμενο αναγνώστη για μια περαιτέρω εμβάθυνση, υπάρχουν στο κείμενο αρκετές παραπομπές σε θέματα της Θεωρίας Αριθμών, της Μεταθετικής Άλγεβρας, της Θεωρίας Ομάδων, κ.ά.

Εκφράζουμε τις θερμές ευχαριστίες μας στις κυρίες Ρόζα Γαρδέρη και Πόπη Μπολιώτη για την ταχεία και αποτελεσματική δακτυλογράφηση του κειμένου στο σύστημα LaTeX. Επίσης, ευχαριστούμε το φοιτητή Βασίλη Πασχάλη του Τμήματός μας που συνέβαλε στη διαμόρφωση των σχημάτων.

Οι κύριες αλλαγές στη δεύτερη αυτή έκδοση, πέρα από τη διόρθωση όλων των παροραμάτων τα οποία υπέπεσαν στην αντίληψή μας, είναι οι εξής: Η Ενότητα 2 της πρώτης έκδοσης διασπάστηκε σε δύο Ενότητες, καθώς οι τέσσερις τελευταίες Παράγραφοί της αποτελούν τώρα την Ενότητα 3. Επιπλέον, άλλαξε η σειρά των Παραγράφων §2.7 και §2.8 και προστέθηκε η Παράγραφος §2.9 (Επεκτάσεις Σωμάτων και Γεωμετρικές Κατασκευές). Αναμορφώθηκε η ανάπτυξη της ύλης της Ενότητας 3 της πρώτης έκδοσης (που αποτελεί τώρα την Ενότητα 4), με αποτέλεσμα να συγχωνευθούν οι Παράγραφοι §3.3 και §3.4 της πρώτης έκδοσης (στην Παράγραφο §4.3), οι Παράγραφοι §3.5 και §3.8 της πρώτης έκδοσης (στην Παράγραφο §4.5) και να διασπαστεί η Παράγραφος §3.9 της πρώτης έκδοσης (στις Παραγράφους §4.7 και §4.8).

Οι συγγραφείς Αθήνα, Σεπτέμβριος 2005

Περιεχόμενα

1 Ακέραιοι

Στην Ενότητα αυτή θα μελετήσουμε ιδιότητες του συνόλου των ακεραίων αριθμών, $\mathbb{Z}$. Ο σκοπός μας είναι διττός. Αφενός θα μελετήσουμε τις ιδιότητες του $\mathbb{Z}$ που θα χρησιμοποιήσουμε σε επόμενες Ενότητες και αφετέρου θα εισάγουμε μέσω του $\mathbb{Z}$ μερικές θεμελιώδεις έννοιες της Άλγεβρας. Έτσι, δίνεται η ευκαιρία στον αναγνώστη να μελετήσει αρκετές από τις έννοιες της Άλγεβρας, που εμφανίζονται παρακάτω, στην ειδική περίπτωση των ακεραίων. Σε καμιά περίπτωση η Ενότητα αυτή δεν αποτελεί εισαγωγή στον πλούσιο κλάδο της Θεωρίας Αριθμών.

Θα θεωρήσουμε γνωστές τις πλέον στοιχειώδεις ιδιότητες της πρόσθεσης και του πολλαπλασιασμού ακεραίων όπως και της διάταξης, $... < -1 < 0 < 1 < ...$, που υπάρχει στο $\mathbb{Z}$ με τις οποίες είμαστε εξοικειωμένοι από τα πρώτα μαθητικά μας χρόνια. Οι τεχνικές των αποδείξεων που θα δούμε εδώ είναι τυπικές για την Άλγεβρα, πράγμα που θα διαπιστώσουμε παρακάτω όταν μελετήσουμε δακτυλίους, σώματα και ομάδες.

Στο βιβλίο αυτό θα χρησιμοποιούμε τους παρακάτω συμβολισμούς.

$\mathbb{N} = \{0, 1, 2, \dots\}$ Το σύνολο των φυσικών αριθμών.
$\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$ Το σύνολο των ακεραίων αριθμών.
$\mathbb{Q}$ Το σύνολο των ρητών αριθμών.
$\mathbb{R}$ Το σύνολο των πραγματικών αριθμών.
$\mathbb{C}$ Το σύνολο των μιγαδικών αριθμών.
$\mathbb{Z}_{>0}$ Το σύνολο των θετικών ακεραίων.
$\mathbb{Q}_{>0}$ Το σύνολο των θετικών ρητών αριθμών.
$\mathbb{R}_{>0}$ Το σύνολο των θετικών πραγματικών αριθμών.

1.1 Μαθηματική Επαγωγή, Διωνυμικοί Συντελεστές

Στην Παράγραφο αυτή θα υπενθυμίσουμε τη μέθοδο απόδειξης που ονομαζεται Μαθηματική Επαγωγή. Επίσης θα ασχοληθούμε με τους διωνυμικούς συντελεστές. Η αφετηρία μας είναι το επόμενο αξίωμα.

1.1.1 Αξίωμα (*Αξίωμα Ελαχίστου*). *Κάθε μη κενό σύνολο φυσικών αριθμών περιέχει ελάχιστο στοιχείο.*

Σημειώνουμε ότι αντίστοιχη ιδιότητα δεν ισχύει στους πραγματικούς ή ρητούς αριθμούς. Για παράδειγμα, το σύνολο $\{1, 1/2, 1/3, 1/4, ...\}$ δεν περιέχει ελάχιστο στοιχείο αν και είναι υποσύνολο των θετικών ρητών αριθμών.

Από τη διάταξη που υπάρχει στο $\mathbb{Z}$, παρατηρούμε ότι κάθε μη κενό σύνολο φυσικών αριθμών περιέχει μοναδικό ελάχιστο στοιχείο.

1.1.2 Θεώρημα (*Μαθηματική Επαγωγή*). *Έστω ότι για κάθε φυσικό αριθμό n δίνεται μια πρόταση $P(n)$, που αφορά τον n, τέτοια ώστε*

1) η $P(0)$ αληθεύει, και

2) για κάθε n, αν η $P(n)$ αληθεύει, τότε η $P(n+1)$ αληθεύει.

Τότε η $P(n)$ αληθεύει για κάθε φυσικό αριθμό n.

Απόδειξη. Έστω A το υποσύνολο του $\mathbb{N}$ που αποτελείται από τους n για τους οποίους η πρόταση $P(n)$ δεν αληθεύει,

$$A = \{n \in \mathbb{N} | P(n) \text{ δεν αληθεύει}\}.$$

Θα δείξουμε ότι το A είναι κενό. Ας υποθέσουμε ότι $A \neq \emptyset$. Τότε από το Αξίωμα Ελαχίστου το A περιέχει ελάχιστο στοιχείο, έστω m. Από την υπόθεση 1) έχουμε $m > 0$. Από τον ορισμό του m έπεται ότι η πρόταση $P(m-1)$ αληθεύει. Τότε όμως η υπόθεση 2) δίνει ότι η $P(m)$ αληθεύει. Αυτό είναι άτοπο. ⊤

Είδαμε ότι το προηγούμενο Θεώρημα έπεται από το Αξίωμα Ελαχίστου. Μπορεί να αποδειχθεί ότι το Θεώρημα της Μαθηματικής Επαγωγής είναι ισοδύναμο με το Αξίωμα Ελαχίστου (Άσκηση 8). Η υπόθεση 1) στο προηγούμενο Θεώρημα συνήθως ονομάζεται "αρχικό βήμα της επαγωγής" ενώ η υπόθεση 2) "επαγωγικό βήμα." Πριν προχωρήσουμε σε παραδείγματα, αναφέρουμε μια παραλλαγή που διαφέρει στο αρχικό βήμα της επαγωγής.

1.1.3 Θεώρημα (*Μαθηματική Επαγωγή με αρχικό βήμα από το* m). *Έστω $m \in \mathbb{N}$. Έστω ότι για κάθε φυσικό αριθμό n με $n \geq m$ δίνεται μια πρόταση $P(n)$, που αφορά τον n, τέτοια ώστε*

1) *η* $P(m)$ *αληθεύει, και*

2) *για κάθε* $n \geq m$*, αν η* $P(n)$ *αληθεύει, τότε η* $P(n+1)$ *αληθεύει.*

Τότε η $P(n)$ *αληθεύει για κάθε* $n \in \mathbb{N}$ *με* $n \geq m$*.*

Απόδειξη. Η απόδειξη είναι παρόμοια με την προηγούμενη και αφήνεται σαν άσκηση. ⊤

1.1.4 Παραδείγματα.

1) $1 + 2 + \cdots + n = \dfrac{1}{2}n(n+1)$ για κάθε θετικό ακέραιο n.
Χρησιμοποιούμε επαγωγή. *Αρχικό βήμα:* Για $n = 1$, η αποδεικτέα σχέση είναι $1 = \dfrac{1}{2}1(1+1)$, που ισχύει. *Επαγωγικό βήμα:* Έστω ότι ισχύει

$$1 + 2 + \cdots + n = \frac{1}{2}n(n+1). \qquad P(n)$$

Θα αποδείξουμε ότι ισχύει

$$1 + 2 + \cdots + (n+1) = \frac{1}{2}(n+1)(n+2). \qquad P(n+1)$$

Το αριστερό μέλος της $P(n+1)$ γράφεται με τη βοήθεια της $P(n)$

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

Το δεξιό μέλος της παραπάνω ισότητας είναι $\dfrac{1}{2}(n+1)(n+2)$, που είναι το ζητούμενο.

2) $2^n > n^2$ για κάθε ακέραιο $n \geq 5$.
Χρησιμοποιούμε επαγωγή. Για $n = 5$ η αποδεικτέα σχέση είναι η $2^5 > 5^2$, που ισχύει. Υποθέτουμε τώρα ότι ισχύει

$$2^n > n^2, \qquad P(n)$$

όπου $n \geq 5$, και θα αποδείξουμε ότι

$$2^{n+1} > (n+1)^2. \qquad P(n+1)$$

Από την $P(n)$ έχουμε ότι $2^{n+1} = 2 \cdot 2^n > 2n^2$. Επιπλέον ισχύει $2n^2 = n^2 + n \cdot n \geq n^2 + 3n$ (γιατί $n \geq 3$), και $n^2 + 3n \geq n^2 + 2n + 1 = (n+1)^2$. Από τις προηγούμενες σχέσεις προκύπτει το ζητούμενο.

3) Έστω A ένα πεπερασμένο σύνολο που έχει n στοιχεία. Τότε το πλήθος των υποσυνόλων του A είναι 2^n.
Χρησιμοποιούμε επαγωγή. Για $n = 0$, η πρόταση αληθεύει καθώς το κενό σύνολο έχει $2^0 = 1$ υποσύνολα. Υποθέτουμε τώρα ότι η πρόταση αληθεύει για κάθε σύνολο με $n \in \mathbb{N}$ στοιχεία. Έστω ότι το A έχει $n+1$ στοιχεία και $\alpha \in A$. Το σύνολο $B = A - \{\alpha\}$ έχει n στοιχεία και συνεπώς το πλήθος των υποσυνόλων του είναι 2^n. Θα μετρήσουμε το πλήθος των υποσυνόλων του A. Έστω $\Gamma \subseteq A$. Διακρίνουμε δύο περιπτώσεις. 1) Έστω $\alpha \notin \Gamma$. Τότε $\Gamma \subseteq B$ και συνεπώς το πλήθος των Γ είναι 2^n. 2) Έστω $\alpha \in \Gamma$. Τότε $\Gamma = \Delta \cup \{\alpha\}$ με $\Delta \subseteq B$, οπότε συμπεραίνουμε ότι το πλήθος των Γ είναι πάλι 2^n. Συνολικά, υπάρχουν $2^n + 2^n = 2^{n+1}$ υποσύνολα του A, που είναι το ζητούμενο.

4) **Θεώρημα de Moivre**. Έστω $\theta \in \mathbb{R}$. Τότε για τον μιγαδικό αριθμό $\sigma\upsilon\nu\theta + i\eta\mu\theta$ ισχύει $(\sigma\upsilon\nu\theta + i\eta\mu\theta)^n = \sigma\upsilon\nu(n\theta) + i\eta\mu(n\theta)$ για κάθε $n \in \mathbb{N}$. Για $n = 0$ η αποδεικτέα σχέση είναι προφανής. Υποθέτουμε ότι αυτή ισχύει για n. Χρησιμοποιώντας τις γνωστές τριγωνομετρικές ταυτότητες $\sigma\upsilon\nu(\theta+\varphi) = \sigma\upsilon\nu\theta\sigma\upsilon\nu\varphi - \eta\mu\theta\eta\mu\varphi$ και $\eta\mu(\theta+\varphi) = \eta\mu\theta\sigma\upsilon\nu\varphi + \eta\mu\varphi\sigma\upsilon\nu\theta$, έχουμε

$$\begin{aligned}(\sigma\upsilon\nu\theta + i\eta\mu\theta)^{n+1} &= (\sigma\upsilon\nu\theta + i\eta\mu\theta)^n(\sigma\upsilon\nu\theta + i\eta\mu\theta)\\ &= (\sigma\upsilon\nu(n\theta) + i\eta\mu(n\theta))(\sigma\upsilon\nu\theta + i\eta\mu\theta)\\ &= \sigma\upsilon\nu(n\theta)\sigma\upsilon\nu\theta - \eta\mu(n\theta)\eta\mu\theta\\ &\quad + i(\sigma\upsilon\nu(n\theta)\eta\mu\theta + \eta\mu(n\theta)\sigma\upsilon\nu\theta)\\ &= \sigma\upsilon\nu(n\theta+\theta) + i\eta\mu(n\theta+\theta)\\ &= \sigma\upsilon\nu((n+1)\theta) + i\eta\mu((n+1)\theta).\end{aligned}$$

Υπάρχει μία άλλη μορφή της μαθηματικής επαγωγής που είναι χρήσιμη.

1.1.5 Θεώρημα (*Δεύτερη Μορφή της Μαθηματικής Επαγωγής*). *Έστω ότι για κάθε φυσικό αριθμό n δίνεται μια πρόταση $P(n)$, που αφορά τον n, τέτοια ώστε*

1) *η $P(0)$ αληθεύει, και*

2) *για κάθε n, αν η $P(k)$ αληθεύει για κάθε φυσικό αριθμό k με $0 \leq k \leq n$, τότε η $P(n+1)$ αληθεύει.*

Τότε η $P(n)$ αληθεύει για κάθε φυσικό αριθμό n.

Απόδειξη. Αρκεί να αποδειχθεί ότι το σύνολο $A = \{n \in \mathbb{N} | P(n) \text{ δεν αληθεύει}\}$ είναι κενό. Έστω ότι το A δεν είναι κενό. Τότε λόγω του Αξιώματος 1.1.1, το A περιέχει ελάχιστο στοιχείο, έστω m. Από την υπόθεση 1) έχουμε ότι $m \geq 1$. Από τον ορισμό του m προκύπτει ότι η πρόταση $P(k)$ αληθεύει για κάθε $k \leq m-1$. Από την υπόθεση 2) προκύπτει ότι η $P(m)$ αληθεύει, που είναι άτοπο. ⊺

Σημείωση. Στη Δεύτερη Μορφή της Μαθηματικής επαγωγής είναι δυνατόν το αρχικό βήμα να μην είναι το 0 αλλά οποιοσδήποτε $m \in \mathbb{N}$. Σύγκρινε με το Θεώρημα 1.1.3.

Διωνυμικοί συντελεστές

Στη συνέχεια θα ασχοληθούμε με το διωνυμικό ανάπτυγμα που θα χρησιμοποιηθεί στα επόμενα. Έστω $i \leq n$ φυσικοί αριθμοί. Με $\binom{n}{i}$ συμβολίζουμε τον συντελεστή του x^i στο ανάπτυγμα του διωνύμου $(1+x)^n$. Για παράδειγμα, έχουμε $\binom{2}{0} = 1$, $\binom{2}{1} = 2$, $\binom{2}{2} = 1$, αφού $(1+x)^2 = 1 + 2x + x^2$. Όμοια έχουμε $\binom{3}{0} = 1$, $\binom{3}{1} = 3$, $\binom{3}{3} = 1$, αφού $(1+x)^3 = 1 + 3x + 3x^2 + x^3$. Έτσι γράφουμε εξ ορισμού

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n.$$

Στην περίπτωση που έχουμε $i > n$ συμφωνούμε ότι $\binom{n}{i} = 0$. Αυτό επιτρέπει κάποια ομοιομορφία στις διατυπώσεις προτάσεων που αφορούν τους διωνυμικούς συντελεστές. (Βλ. την πρώτη σχέση της παρακάτω πρότασης για $i = n+1$.)

1.1.6 Πρόταση. *1) Έστω i, n φυσικοί αριθμοί με $1 \leq i \leq n+1$. Τότε*

$$\binom{n+1}{i} = \binom{n}{i-1} + \binom{n}{i}.$$

2) Έστω i, n φυσικοί αριθμοί με $i \leq n$. Τότε

$$\binom{n}{i} = \frac{n!}{i!(n-i)!} \tag{1}$$

όπου θέτουμε $0! = 1$ και για κάθε θετικό ακέραιο n, $n! = 1 \cdot 2 \cdot \cdots \cdot n$.

Απόδειξη. 1) Θεωρούμε την ταυτότητα πολυωνύμων

$$(1+x)^{n+1} = (1+x)^n(1+x) = (1+x)^n + (1+x)^n x$$

και συγκρίνουμε τους συντελεστές του x^i στο αριστερό και δεξιό μέλος. Στο αριστερό μέλος ο εν λόγω συντελεστής είναι $\binom{n+1}{i}$, ενώ στο δεξιό είναι $\binom{n}{i}+\binom{n}{i-1}$.
2) Χρησιμοποιούμε επαγωγή στο n. Για $n=0$, οπότε $i=0$, η αποδεικτέα σχέση είναι προφανής. Υποθέτοντας την (1) θα αποδείξουμε ότι

$$\binom{n+1}{i} = \frac{(n+1)!}{i!(n+1-i)!}. \tag{2}$$

Αν $i=0$, εύκολα επαληθεύεται η (2). Έστω λοιπόν $0<i\leq n+1$, οπότε από το 1) της πρότασης και την ισότητα (1) έχουμε

$$\begin{aligned}\binom{n+1}{i} = \binom{n}{i-1}+\binom{n}{i} &= \frac{n!}{(i-1)!(n-i+1)!}+\frac{n!}{i!(n-i)!}\\ &= \frac{n!}{(i-1)!(n-i)!}\left(\frac{1}{n-i+1}+\frac{1}{i}\right)\\ &= \frac{n!}{(i-1)!(n-i)!}\frac{n+1}{(n-i+1)i}\\ &= \frac{(n+1)!}{i!(n+1-i)!}.\end{aligned}$$

και άρα η (2) ισχύει. ⊤

1.1.7 Εφαρμογή.
Έστω A ένα πεπερασμένο σύνολο με n στοιχεία. Τότε το πλήθος των υποσυνόλων του A που έχουν i στοιχεία είναι ίσο με $\binom{n}{i}$ για κάθε i με $0\leq i\leq n$.
Εφαρμόζουμε επαγωγή στο n. Αν $n=0$, τότε $i=0$ και το ζητούμενο είναι προφανές, αφού το κενό σύνολο έχει ακριβώς $\binom{0}{0}=1$ υποσύνολο. Έστω ότι κάθε πεπερασμένο σύνολο με n στοιχεία, $n>0$, έχει $\binom{n}{i}$ υποσύνολα με i στοιχεία. Έστω ότι το A έχει $n+1$ στοιχεία. Θα μετρήσουμε τώρα το πλήθος των υποσυνόλων του A που έχουν i στοιχεία. Έστω $a\in A$ και $B=A-\{\alpha\}$. Έστω Γ ένα υποσύνολο του A που έχει i στοιχεία. Όπως στο Παράδειγμα 1.1.4 3), διακρίνουμε δύο περιπτώσεις. 1) Έστω $\alpha\notin\Gamma$. Τότε $\Gamma\subseteq B$. Από την υπόθεση της επαγωγής έπεται ότι το πλήθος των Γ είναι $\binom{n}{i}$. 2) Έστω $\alpha\in\Gamma$. Τότε $\Gamma-\{\alpha\}\subseteq B$. Από την υπόθεση της επαγωγής έπεται ότι το πλήθος των

$\Gamma - \{\alpha\}$ (και επομένως το πλήθος των Γ) είναι $\binom{n}{i-1}$. Συνολικά υπάρχουν $\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}$ υποσύνολα του A που έχουν i στοιχεία.

Ασκήσεις 1.1

1) Αποδείξτε ότι $\dfrac{1}{1\cdot 2} + \dfrac{1}{2\cdot 3} + \cdots + \dfrac{1}{n(n+1)} = \dfrac{n}{n+1}$ για κάθε θετικό ακέραιο n.

2) Αποδείξτε ότι $1^3 + 2^3 + \cdots + n^3 = \dfrac{1}{4}n^2(n+1)^2 = (1 + 2 + \cdots + n)^2$ για κάθε θετικό ακέραιο n.

3) Αποδείξτε ότι

   i) $3n < n^3$ για κάθε $n \in \mathbb{N}$, $n \geq 2$.

   ii) $mn < n^m$ για κάθε $m, n \in \mathbb{N}$ με $m \geq 3$ και $n \geq 2$.
   Υπόδειξη: επαγωγή στο m.

4) Αποδείξτε ότι για κάθε $k, m, n \in \mathbb{N}$ ισχύουν οι παρακάτω ταυτότητες.

   i) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n\binom{n}{n} = 0$,

   ii) $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$,

   iii) $\binom{2n}{n} = \binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2$,

   iii) $\binom{m+n}{k} = \binom{m}{0}\binom{n}{k} + \binom{m}{1}\binom{n}{k-1} + \cdots + \binom{m}{k}\binom{n}{0}$.

   Υπόδειξη: Για την πρώτη ταυτότητα χρησιμοποιήστε ότι $(1 + (-1))^n = 0$. Για την τρίτη, συγκρίνετε τους συντελεστές του x^n στην ταυτότητα $(1+x)^{2n} = (1+x)^n(1+x)^n$.

5) Έστω $f_0 = 0$, $f_1 = 1$ και $f_n = f_{n-1} + f_{n-2}$ για $n \geq 2$ (ακολουθία του Fibonacci).
   Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύουν:

   i) $f_0 + f_1 + \cdots + f_n = f_{n+2} - 1$.

   ii) $f_{n+2}f_n - f_{n+1}^2 = (-1)^{n+1}$.

iii) $f_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$, όπου $\alpha = \frac{1+\sqrt{5}}{2}$ και $\beta = \frac{1-\sqrt{5}}{2}$ (οι α, β ικανοποιούν την εξίσωση $x^2 - x - 1 = 0$).

iv) $f_{2n} = \binom{n}{0} f_0 + \binom{n}{1} f_1 + \cdots + \binom{n}{n} f_n$.
Υπόδειξη: Χρησιμοποιήστε το iii).

6) Για κάθε $r, n \in \mathbb{N}$ με $r \leq n$ αποδείξτε ότι $\binom{r}{r} + \binom{r+1}{r} + \cdots + \binom{n}{r} = \binom{n+1}{r+1}$.

7) Έστω $\theta \in \mathbb{R}$. Τότε για τον μιγαδικό αριθμό $\sigma\upsilon\nu\theta + i\eta\mu\theta$ ισχύει $(\sigma\upsilon\nu\theta + i\eta\mu\theta)^n = \sigma\upsilon\nu(n\theta) + i\eta\mu(n\theta)$ για κάθε $n \in \mathbb{Z}$.

8) Αποδείξτε ότι τα ακόλουθα είναι ισοδύναμα.

i) Αξίωμα 1.1.1 (Αξίωμα Ελαχίστου).

ii) Θεώρημα 1.1.2 (Μαθηματική Επαγωγή)

iii) Θεώρημα 1.1.5 (Δεύτερη μορφή της Μαθηματικής Επαγωγής).

1.2 Διαιρετότητα

Στην Παράγραφο αυτή θα μελετήσουμε την έννοια της διαιρετότητας στο $\mathbb{Z}$. Αφού αποδείξουμε τον Αλγόριθμο Διαίρεσης, θα αναπτύξουμε την έννοια του μέγιστου κοινού διαιρέτη με τη βοήθεια του οποίου θα αποδείξουμε το Θεμελιώδες Θεώρημα της Αριθμητικής, σύμφωνα με το οποίο κάθε ακέραιος αριθμός διάφορος των 0 και ± 1 γράφεται ως γινόμενο πρώτων κατά τρόπο ουσιαστικά μοναδικό.

Διαιρετότητα και πρώτοι αριθμοί

Έστω $a, b \in \mathbb{Z}$. Θα λέμε ότι ο a ***διαιρεί*** τον b (ή ότι ο a είναι ***διαιρέτης*** του b ή ότι ο b είναι ***πολλαπλάσιο*** του a) αν υπάρχει $c \in \mathbb{Z}$ με $b = ac$. Θα γράφουμε τότε $a|b$. Παρατηρούμε ότι κάθε ακέραιος είναι διαιρέτης του 0 ενώ το 0 είναι διαιρέτης μόνο του εαυτού του.

Έστω a, b, c τρεις ακέραιοι αριθμοί. Εύκολα διαπιστώνουμε ότι ισχύουν οι παρακάτω ιδιότητες, τις οποίες θα χρησιμοποιούμε στη συνέχεια χωρίς ιδιαίτερη μνεία.

- Αν $a|b$ και $a|c$, τότε $a|bx + cy$ για κάθε $x, y \in \mathbb{Z}$. Ιδιαίτερα, $a|b \pm c$.
- Αν $a|b$ και $b|a$, τότε $a = \pm b$.
- Αν $a|b$ και $b|c$, τότε $a|c$
- Αν $a|b$ και οι a, b είναι θετικοί, τότε $a \leq b$.

Ενδεικτικά αποδεικνύουμε την πρώτη ιδιότητα: από την υπόθεση, υπάρχουν ακέραιοι e, f τέτοιοι ώστε $b = ae$ και $c = af$. Αντικαθιστώντας έχουμε ότι $bx + cy = aex + afy = a(ex + fy)$. Συνεπώς, $a|bx + cy$.

Ένας θετικός ακέραιος $p \neq 1$ λέγεται ***πρώτος*** αριθμός αν οι μόνοι διαιρέτες του είναι οι ± 1 και $\pm p$. Για παράδειγμα, από τους $1, 2, 3, 4, 5, 6, 7, 8$ και 9 οι πρώτοι αριθμοί είναι οι $2, 3, 5$ και 7. Ο κύριος σκοπός μας στην Παράγραφο αυτή είναι να αποδείξουμε ότι κάθε ακέραιος αριθμός διάφορος των 0, ± 1 γράφεται ως γινόμενο πρώτων κατά τρόπο ουσιαστικά μοναδικό (Θεμελιώδες Θεώρημα της Αριθμητικής). Αντίστοιχο αποτέλεσμα θα συναντήσουμε στην Ενότητα 2, όταν μελετήσουμε πολυώνυμα. Επίσης η ιδέα της μοναδικής παραγοντοποίησης αναπτύσσεται πιο γενικά στην Ενότητα 3.

Στην διατύπωση της ακόλουθης Πρότασης δεχόμαστε ότι κάθε πρώτος αριθμός είναι γινόμενο πρώτων αριθμών κατά τετριμμένο τρόπο.

1.2.1 Πρόταση. *Κάθε θετικός ακέραιος διάφορος του 1 είναι γινόμενο πρώτων αριθμών.*

Απόδειξη. Έστω ότι η πρόταση δεν ισχύει και έστω M το σύνολο των ακεραίων $n > 1$ οι οποίοι δεν είναι γινόμενα πρώτων αριθμών. Τότε $M \neq \emptyset$ και από το Αξίωμα 1.1.1 υπάρχει ελάχιστο στοιχείο $m \in M$. Έχουμε $m > 1$ και ο m δεν είναι πρώτος (αφού κάθε πρώτος είναι κατά τετριμμένο τρόπο γινόμενο πρώτων). Συνεπώς $m = ab$ για κάποιους ακεραίους a, b όπου $1 < a < m$ και $1 < b < m$. Από τον ορισμό του m προκύπτει ότι $a \notin M$ και $b \notin M$, δηλαδή οι a, b είναι γινόμενα πρώτων αριθμών. Τότε όμως το ίδιο συμβαίνει για το γινόμενό τους $m = ab$, δηλαδή $m \notin M$. Αυτό είναι άτοπο. ⊤

Συνεπώς βλέπουμε ότι κάθε ακέραιος διάφορος των $0, \pm 1$ γράφεται στην μορφή $\pm p_1 \dots p_k$, όπου οι p_i είναι πρώτοι αριθμοί (όχι αναγκαστικά διακεκριμένοι).

1.2.2 Θεώρημα (*Ευκλείδης*). [1] *Υπάρχουν άπειροι πρώτοι αριθμοί.*

Απόδειξη. Έστω ότι το σύνολο των πρώτων αριθμών είναι πεπερασμένο και ότι είναι το $\{p_1, \dots, p_m\}$. Ο ακέραιος $p_1 p_2 \dots p_m + 1$ έχει έναν πρώτο διαιρέτη σύμφωνα με την Πρόταση 1.2.1, έστω p_i. Αφού $p_i | p_1 p_2 \dots p_m + 1$ και $p_i | p_1 p_2 \dots p_m$ συμπεραίνουμε ότι ο p_i διαιρεί τη διαφορά, δηλαδή $p_i | 1$. Αυτό είναι άτοπο. ⊤

Το επόμενο αποτέλεσμα περιγράφει μια από τις πιο σημαντικές ιδιότητες του $\mathbb{Z}$ και θα χρησιμοποιηθεί πολλές φορές στα παρακάτω.

1.2.3 Θεώρημα (*Αλγόριθμος Διαίρεσης ή Ευκλείδεια Διαίρεση*). *Έστω $a, b \in \mathbb{Z}$ με $a > 0$. Τότε υπάρχουν μοναδικοί $q, r \in \mathbb{Z}$ με τις ιδιότητες*

$$b = qa + r \quad \text{και} \quad 0 \leq r < a.$$

Απόδειξη. 1) *Ύπαρξη*: Θέτουμε $M = \{b - ta \geq 0 | t \in \mathbb{Z}\}$. Ισχύει $M \neq \emptyset$ (αρκεί να θεωρήσουμε $t < 0$ με $|t|$ αρκετά μεγάλο, όπου με $|t|$ συμβολίζουμε την απόλυτη τιμή του t), οπότε από το Αξίωμα 1.1.1 υπάρχει ελάχιστο στοιχείο $r \in M$. Έχουμε $r = b - qa$, για κάποιον ακέραιο q, και θα δείξουμε ότι $r < a$. Αν ίσχυε $r \geq a$, τότε αντικαθιστώντας θα είχαμε $b - (q+1)a \geq 0$, οπότε $b - (q+1)a \in M$. Αυτό είναι άτοπο από τον ορισμό του r, γιατί $r > r - a = b - (q+1)a$.
2) *Μοναδικότητα*: Έστω ότι είχαμε $b = qa + r$, $0 \leq r < a$, όπου $q, r \in \mathbb{Z}$ και $b = q'a + r'$, $0 \leq r' < a$, όπου $q', r' \in \mathbb{Z}$. Τότε λαμβάνουμε

$$(q - q')a = r' - r$$

[1] Η απόδειξη αυτή, όπως και ο Ευκλείδειος Αλγόριθμος, περιέχονται στο έργο *Στοιχεία* του Ευκλείδη.

και

$$-a < r' - r < a.$$

Άρα $-a < (q - q')a < a$ και συνεπώς (αφού $a > 0$) $-1 < q - q' < 1$. Επειδή $q - q \in \mathbb{Z}$, συμπεραίνουμε ότι $q - q' = 0$. Συνεπώς $r' - r = (q - q')a = 0$. ⊤

Σημειώσεις

1. Η απόδειξη της ύπαρξης των q και r στο προηγούμενο Θεώρημα συνίσταται στην αυστηρή διατύπωση της ακόλουθης απλής ιδέας. Ας υποθέσουμε για ευκολία ότι $b > 0$. Αφαιρούμε από τον b τα μη αρνητικά πολλαπλάσια του a, δηλαδή τα 0, a, $2a$, $3a, \ldots$, έτσι ώστε η διαφορά $b - ta$ να παραμένει μη αρνητική. Το τελευταίο τέτοιο πολλαπλάσιο είναι το qa και η διαφορά $b - qa$ είναι το r.

2. Αν παραλείψουμε το $a > 0$ από την υπόθεση του προηγούμενου Θεωρήματος και θεωρήσουμε $a \neq 0$, τότε το μόνο που αλλάζει είναι η ανισότητα του συμπεράσματος που πρέπει να είναι τώρα $0 \leq r < |a|$. (Η απόδειξη έπεται αμέσως από το Θεώρημα: αν ο a είναι αρνητικός, εφαρμόζουμε το Θεώρημα για $-a$ στη θέση του a).

3. Ο φυσικός αριθμός r του αλγορίθμου διαίρεσης ονομάζεται το ***υπόλοιπο*** της διαίρεσης του b με το a.

Μέγιστος κοινός διαιρέτης

Έστω $a, b \in \mathbb{Z}$ με τουλάχιστον έναν διάφορο του μηδενός. Ένας ***μέγιστος κοινός διαιρέτης*** των a και b (συμβολικά $\mu\kappa\delta(a, b)$ ή (a, b)) είναι ένας θετικός ακέραιος d που έχει τις ιδιότητες

1. $d|a$ και $d|b$

2. αν $c \in \mathbb{Z}$ με $c|a$ και $c|b$, τότε $c|d$.

Για παράδειγμα, έχουμε $\mu\kappa\delta(12, 30) = 6$. Παρατηρούμε ότι αν $d = \mu\kappa\delta(a, b)$, τότε κάθε άλλος κοινός διαιρέτης c των a και b είναι τέτοιος ώστε $c \leq d$ λόγω της συνθήκης 2 του ορισμού. Έτσι εξηγείται η ονομασία *μέγιστος* κοινός διαιρέτης.

Στο στάδιο αυτό δεν είναι τελείως σαφές ότι υπάρχει $\mu\kappa\delta$ για κάθε $a, b \in \mathbb{Z}$ με τουλάχιστον έναν διάφορο του μηδενός. Πέρα από την ύπαρξη, το παρακάτω αποτέλεσμα παρέχει μία σημαντική παράσταση του $\mu\kappa\delta$ που θα χρησιμοποιηθεί συχνά στα παρακάτω.

1.2.4 Θεώρημα. *Έστω $a, b \in \mathbb{Z}$ με τουλάχιστον έναν διάφορο του μηδενός. Τότε υπάρχει μοναδικός μέγιστος κοινός διαιρέτης των a και b. Επιπλέον υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $\mu\kappa\delta(a, b) = ax + by$.*

Απόδειξη. Ύπαρξη: Θέτουμε $M = \{ax + by | x, y \in \mathbb{Z} \text{ και } ax + by > 0\}$ και παρατηρούμε ότι $M \neq \emptyset$ (γιατί $a^2 + b^2 > 0$). Έστω d το ελάχιστο στοιχείο του M, το οποίο υπάρχει σύμφωνα με το Αξίωμα 1.1.1. Έχουμε $d = ax + by$ για κάποιους $x, y \in \mathbb{Z}$.

Θα αποδείξουμε ότι $d = \mu\kappa\delta(a,b)$. Για τον σκοπό αυτό, δείχνουμε πρώτα ότι $d|a$ και $d|b$. Από το Θεώρημα 1.2.3, υπάρχουν ακέραιοι q, r τέτοιοι ώστε $a = qd+r, 0 \leq r < d$. Έχουμε $r = a-qd = a-q(ax+by) = a(1-qx)+b(-qy)$. Αυτό σημαίνει ότι αν $r \neq 0$, τότε $r \in M$, που όμως είναι άτοπο λόγω του ελαχίστου του d. Άρα $r = 0$ και συνεπώς $d|a$. Όμοια αποδεικνύεται ότι $d|b$. Τώρα έστω $c|a$ και $c|b$. Επειδή έχουμε $d = ax + by$ συμπεραίνουμε ότι $c|d$. Άρα πράγματι ο d είναι ένας $\mu\kappa\delta$ των a και b.

Μοναδικότητα: Αν d και d' ήταν μέγιστοι κοινοί διαιρέτες των a, b, θα είχαμε $d|d'$ (γιατί ο d' είναι ένας $\mu\kappa\delta$ των a, b) και $d'|d$ (γιατί ο d είναι ένας $\mu\kappa\delta$ των a, b). Άρα $d = \pm d'$, και αφού $d, d' > 0$ παίρνουμε $d = d'$. ⊤

Η προηγούμενη απόδειξη παρέχει έναν τρόπο προσδιορισμού του $\mu\kappa\delta$ (ως το ελάχιστο του συνόλου M). Υπάρχει όμως ένας πιο πρακτικός τρόπος (Ευκλείδειος Αλγόριθμος) που περιγράφεται παρακάτω. Πριν από αυτό, όμως, θα αποδείξουμε το Θεμελιώδες Θεώρημα της Αριθμητικής. Για το σκοπό αυτό χρειαζόμαστε το ακόλουθο Λήμμα, που έπεται από το Θεώρημα 1.2.4.

1.2.5 Λήμμα. *Έστω $a, b, p \in \mathbb{Z}$ όπου ο p είναι πρώτος αριθμός. Αν ο p διαιρεί το γινόμενο ab, τότε ο p διαιρεί τουλάχιστον έναν από τους a και b.*

Απόδειξη. Έστω ότι ο p δεν διαιρεί τον a. Αφού ο p είναι πρώτος έχουμε $\mu\kappa\delta(a,p) = 1$. Σύμφωνα με το Θεώρημα 1.2.4 υπάρχουν ακέραιοι x και y τέτοιοι ώστε $1 = ax + py$. Άρα $b = abx + pyb$. Επειδή $p|abx$ και $p|pyb$ προκύπτει ότι $p|abx + pyb$, δηλαδή $p|b$. ⊤

1.2.6 Παρατηρήσεις.

1. Με επαγωγή μπορεί να γενικευθεί το προηγούμενο Λήμμα στην περίπτωση περισσοτέρων παραγόντων: Αν ο p είναι ένας πρώτος αριθμός που διαιρεί το γινόμενο $a_1 \ldots a_m$, $(a_i \in \mathbb{Z})$, τότε θα διαιρεί τουλάχιστον έναν από τους a_i. Η απόδειξη αφήνεται σαν άσκηση.

2. Το Λήμμα 1.2.5 είναι ιδιαίτερα χρήσιμο. Μια τυπική εφαρμογή του είναι η απόδειξη ότι ο αριθμός $\sqrt{2}$ είναι άρρητος. Πράγματι, έστω ότι $\sqrt{2} = \frac{m}{n}$, όπου οι m, n είναι θετικοί ακέραιοι. Μπορούμε να υποθέσουμε ότι $\mu\kappa\delta(m,n) = 1$, γιατί διαφορετικά απλοποιούμε το κλάσμα. Έχουμε $m^2 = 2n^2$. Αν $n \neq 1$, τότε σύμφωνα με την Πρόταση 1.2.1 υπάρχει πρώτος p με $p|n$. Τότε $p|m^2$ και άρα $p|m$, από το Λήμμα 1.2.5. Συνεπώς $p|\mu\kappa\delta(m,n)$, δηλαδή $p|1$, που είναι άτοπο. Άρα $n = 1$. Αλλά τότε $\sqrt{2} = m \in \mathbb{Z}$, που είναι άτοπο. Με παρόμοιο τρόπο μπορεί να αποδειχθεί ότι για κάθε θετικό ακέραιο a που δεν είναι τετράγωνο ακεραίου ο αριθμός $\sqrt{a}$ είναι άρρητος (Άσκηση 15).

1.2.7 Θεώρημα (*Θεμελιώδες Θεώρημα της Αριθμητικής*). *Κάθε ακέραιος $a > 1$ γράφεται ως γινόμενο πρώτων αριθμών, $a = p_1 \dots p_m$, p_i πρώτος. Η παράσταση αυτή είναι μοναδική με την εξής έννοια: αν $a = p_1 \dots p_m = q_1 \dots q_n$ (p_i, q_j πρώτοι), τότε $m = n$ και, μετά ενδεχομένως από κάποια αναδιάταξη, έχουμε $p_1 = q_1, \dots, p_m = q_m$.*

Απόδειξη. Έστω $a > 1$ ένας ακέραιος αριθμός. Στην Πρόταση 1.2.1 δείξαμε ότι υπάρχουν πρώτοι αριθμοί $p_1, \dots, p_m$ που έχουν την ιδιότητα $a = p_1 \dots p_m$. Θα δείξουμε τώρα τη μοναδικότητα της παράστασης αυτής. Έστω ότι $a = p_1 \dots p_m = q_1 \dots q_n$, όπου οι p_i, q_j είναι πρώτοι αριθμοί. Μπορούμε να υποθέσουμε ότι $m \leq n$, οπότε εφαρμόζουμε επαγωγή στο m. Για $m = 1$ έχουμε $p_1 = q_1 \dots q_n$ οπότε ο p_1 θα διαιρεί κάποιον από τους q_j σύμφωνα με την Παρατήρηση 1.2.6, έστω τον q_1. Επειδή ο q_1 είναι πρώτος παίρνουμε $p_1 = q_1$. Έτσι $1 = q_2 \dots q_n$, πράγμα που σημαίνει ότι $n = 1$.

Έστω τώρα $m > 1$. Από την ισότητα $p_1 \dots p_m = q_1 \dots q_n$ παίρνουμε όπως πριν, μετά ενδεχομένως από μια αναδιάταξη των q_j, ότι $p_2 \dots p_m = q_2 \dots q_n$. Το ζητούμενο προκύπτει τώρα από την επαγωγική υπόθεση. ⊤

Σύμφωνα με το προηγούμενο Θεώρημα, κάθε ακέραιος $a \neq 0, \pm 1$ έχει μοναδική παράσταση (χωρίς να λαμβάνεται υπόψη η σειρά των παραγόντων) της μορφής $a = \pm p_1^{a_1} \dots p_n^{a_n}$, όπου οι p_i είναι ανά δύο διάφοροι πρώτοι αριθμοί και οι a_i είναι θετικοί ακέραιοι. Η παραγοντοποίηση αυτή καλείται ***ανάλυση του a σε γινόμενο πρώτων*** και οι πρώτοι αριθμοί $p_1, \dots, p_n$ ονομάζονται ***πρώτοι παράγοντες*** του a.

Δύο ακέραιοι a,b ονομάζονται ***σχετικά πρώτοι*** αν $\mu\kappa\delta(a, b) = 1$. Ισοδύναμα, δύο ακέραιοι είναι σχετικά πρώτοι αν δεν έχουν κοινό πρώτο παράγοντα.

Ευκλείδειος Αλγόριθμος

Περιγράφουμε τώρα μία πρακτική διαδικασία που υπολογίζει το $\mu\kappa\delta(a, b)$ και επιπλέον προσδιορίζει ακεραίους x, y έτσι ώστε να ισχύει $\mu\kappa\delta(a, b) = ax + by$ σύμφωνα με το Θεώρημα 1.2.4. Ονομάζεται δε ***Ευκλείδειος αλγόριθμος*** και στηρίζεται στην επαναλαμβανόμενη εφαρμογή της ακόλουθης απλής παρατήρησης:

$$b = aq + r \Rightarrow \mu\kappa\delta(a, b) = \mu\kappa\delta(r, a). \tag{1}$$

Πράγματι, από την ισότητα $b = aq + r$ έπεται ότι $\mu\kappa\delta(a, b) | r$. Έχουμε δηλαδή $\mu\kappa\delta(a, b) | r$ και $\mu\kappa\delta(a, b) | a$, οπότε από τον ορισμό του $\mu\kappa\delta$ παίρνουμε $\mu\kappa\delta(a, b) | \mu\kappa\delta(r, a)$. Με παρόμοιο τρόπο αποδεικνύεται ότι $\mu\kappa\delta(r, a) | \mu\kappa\delta(a, b)$. Επειδή ο $\mu\kappa\delta$ είναι θετικός ακέραιος, από τις δύο τελευταίες σχέσεις προκύπτει ότι $\mu\kappa\delta(a, b) = \mu\kappa\delta(r, a)$.

Παράδειγμα

Έστω $a = 50$ και $b = 240$. Από την ταυτότητα διαίρεσης λαμβάνουμε διαδοχικά

$$\begin{aligned} 240 &= 4 \cdot 50 + 40 \\ 50 &= 1 \cdot 40 + 10 \\ 40 &= 4 \cdot 10 + 0 \end{aligned}$$

Εφαρμόζοντας την (1) σε κάθε μια από τις τρεις ισότητες, έχουμε

$$\mu\kappa\delta(50, 240) = \mu\kappa\delta(40, 50) = \mu\kappa\delta(10, 40) = \mu\kappa\delta(0, 10) = 10.$$

Για να προσδιορίσουμε ακεραίους x, y τέτοιους ώστε $10 = 50x + 240y$ ξεκινάμε από την τελευταία ταυτότητα διαίρεσης που έχει μη μηδενικό υπόλοιπο (την $50 = 1 \cdot 40 + 10$) και εκτελούμε διαδοχικές αντικαταστάσεις "εργαζόμενοι προς τα πάνω". (Η διαδικασία αυτή ονομάζεται ανταναίρεση).

$$\begin{aligned} 10 &= 50 - 1 \cdot 40 = \\ &= 50 - 1 \cdot (240 - 4 \cdot 50) = \\ &= 50 \cdot 5 + 240 \cdot (-1), \end{aligned}$$

οπότε $x = 5$ και $y = -1$.

Από το προηγούμενο παράδειγμα βλέπουμε ότι ο $\mu\kappa\delta$ δύο ακεραίων a και $b (a \neq 0)$ ισούται με το τελευταίο μη μηδενικό υπόλοιπο (r_n) που συναντάμε στον αντίστοιχο Ευκλείδειο αλγόριθμο:

$$\begin{aligned} b &= aq + r, \quad 0 \leq r < a \\ a &= rq_1 + r_1, \quad 0 \leq r_1 < r \\ r &= r_1q_2 + r_2, \quad 0 \leq r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, \quad 0 \leq r_3 < r_2 \\ &\cdots \\ r_{n-2} &= r_{n-1}q_n + r_n, \quad 0 \leq r_n < r_{n-1} \\ r_{n-1} &= r_nq_{n+1} + 0. \end{aligned}$$

Πράγματι, εφαρμόζοντας διαδοχικά την (1) έχουμε

$$\mu\kappa\delta(a, b) = \mu\kappa\delta(r, a) = \mu\kappa\delta(r_1, r) = \mu\kappa\delta(r_2, r_1) = \cdots$$

$$= \mu\kappa\delta(r_n, r_{n-1}) = \mu\kappa\delta(0, r_n) = r_n.$$

Εδώ υπάρχει το ερώτημα αν η διαδικασία των διαδοχικών διαιρέσεων τερματίζεται μετά από πεπερασμένο αριθμό επαναλήψεων. Η απάντηση είναι θετική, γιατί τα υπόλοιπα σχηματίζουν μια αυστηρά φθίνουσα ακολουθία φυσικών αριθμών με αρχή το a, δηλαδή έχουμε $a > r > r_1 > \cdots > r_n$.

Για να γράψουμε τον $\mu\kappa\delta(a,b)$ στη μορφή $ax+by$ πρώτα επιλύουμε τις παραπάνω εξισώσεις ως προς τα υπόλοιπα λαμβάνοντας

$$\begin{aligned} r &= b - aq \\ r_1 &= a - rq_1 \\ r_2 &= r - r_1q_2 \\ r_3 &= r_1 - r_2q_3 \\ &\cdots \\ r_{n-2} &= r_{n-4} - r_{n-3}q_{n-2} \\ r_{n-1} &= r_{n-3} - r_{n-2}q_{n-1} \\ r_n &= r_{n-2} - r_{n-1}q_n. \end{aligned}$$

Στη συνέχεια αντικαθιστούμε στην τελευταία εξίσωση τον r_{n-1} από την προτελευταία

$$r_n = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n = r_{n-2}(1 + q_{n-1}q_n) + r_{n-3}(-q_n).$$

Στη νέα εξίσωση αντικαθιστούμε την έκφραση που έχουμε για τον r_{n-2}.

$$r_n = r_{n-2}(1+q_{n-1}q_n)+r_{n-3}(-q_n) = (r_{n-4}-r_{n-3}q_{n-2})(1+q_{n-1}q_n)+r_{n-3}(-q_n).$$

Συνεχίζοντας κατά τον τρόπο αυτό φθάνουμε τελικά σε μια παράσταση της μορφής $r_n = ax + by$.

Παρατηρούμε ότι η παραπάνω μέθοδος παρέχει μια νέα απόδειξη της ύπαρξης του $\mu\kappa\delta(a,b)$ και της ύπαρξης $x, y \in \mathbb{Z}$ που έχουν την ιδιότητα $\mu\kappa\delta(a,b) = ax + by$.

Σημειώνουμε ότι οι x, y δεν είναι αναγκαστικά μοναδικοί , αφού $ax + by = a(x + b) + b(y - a)$. Ισχύει όμως $\mu\kappa\delta(x,y) = 1$ (Άσκηση 9).

Παρατηρήσεις στην ανάλυση ακεραίων σε γινόμενο πρώτων

1) Η ανάλυση ακεραίων σε γινόμενο πρώτων παρέχει έναν άλλο τρόπο υπολογισμού του $\mu\kappa\delta$. Έστω a, b θετικοί ακέραιοι και

$$a = p_1^{a_1} \cdots p_n^{a_n} \quad \text{και} \quad b = p_1^{b_1} \cdots p_n^{b_n} \tag{2}$$

όπου p_i είναι ανά δύο διάφοροι πρώτοι και $a_i, b_i \in \mathbb{N}$. (Και οι δύο παραγοντοποιήσεις περιέχουν τους ίδιους πρώτους $p_1, \ldots, p_n$ γιατί επιτρέπουμε εδώ μηδενικούς

εκθέτες). Παρατηρούμε ότι ισχύει

$$a|b \Leftrightarrow a_i \leq b_i \quad \text{για κάθε} \quad i. \tag{3}$$

Πράγματι, η απόδειξη της κατεύθυνσης '$\Leftarrow$' είναι άμεση. Αντίστροφα, έστω $a|b$ και έστω ότι $a_1 > b_1$. Τότε από την (2) παίρνουμε ότι ο $p_1^{a_1-b_1}p_2^{a_2}\dots p_n^{a_n}$ διαιρεί τον $p_2^{b_2}\dots p_n^{b_n}$. Από την Παρατήρηση 1.2.6 1. βλέπουμε ότι $p_1|p_i$ για κάποιο $i \neq 1$. Αυτό είναι άτοπο.

Χρησιμοποιώντας την (3) και τον ορισμό του $\mu\kappa\delta$ μπορούμε να δούμε ότι

$$\mu\kappa\delta(a,b) = p_1^{d_1}\dots p_n^{d_n}, \quad \text{όπου για κάθε} \quad i \quad \text{είναι} \quad d_i = \min\{a_i, b_i\}. \tag{4}$$

Για παράδειγμα, αν $a = 2^5 \cdot 3^4 \cdot 5^0$ και $b = 2 \cdot 3^6 \cdot 5^2$, τότε $\mu\kappa\delta(a,b) = 2 \cdot 3^4 \cdot 5^0$. Από την (4) μπορούμε να συνάγουμε χρήσιμες σχέσεις, όπως για παράδειγμα την

$$\mu\kappa\delta(ca, cb) = c \cdot \mu\kappa\delta(a,b). \tag{5}$$

Σημειώνουμε ότι ο τρόπος υπολογισμού του $\mu\kappa\delta$ που δίνεται στην (4) δεν είναι πολύ πρακτικός για μεγάλους αριθμούς γιατί προϋποθέτει τη γνώση αναλύσεων σε γινόμενα πρώτων. Γενικά η εύρεση της ανάλυσης ενός μεγάλου αριθμού σε γινόμενο πρώτων είναι ένας χρονοβόρος υπολογισμός που πολλές φορές καθίσταται πρακτικά αδύνατος, ακόμα και αν χρησιμοποιηθούν ισχυροί υπολογιστές. Σε αυτό ακριβώς το γεγονός στηρίζεται μια αξιόπιστη και διαδεδομένη μέθοδος κρυπτογράφησης μηνυμάτων, η RSA. Την μέθοδο αυτή παρουσιάζουμε συνοπτικά στην Παράγραφο 1.6 παρακάτω.

2) Έστω a, b ακέραιοι από τους οποίους τουλάχιστον ένας είναι μη μηδενικός. Ένα ***ελάχιστο κοινό πολλαπλάσιο*** ($\epsilon\kappa\pi$) των a, b είναι ένας θετικός ακέραιος e που έχει τις ιδιότητες

- $a|e$ και $b|e$
- αν ο $c \in \mathbb{Z}$ είναι τέτοιος ώστε $a|c$ και $b|c$, τότε $e|c$.

Είναι σαφές ότι αν υπάρχει $\epsilon\kappa\pi$ των a, b τότε αυτό είναι μοναδικό. Ας θεωρήσουμε τις παραγοντοποιήσεις των a, b σε γινόμενα πρώτων, $a = \pm p_1^{a_1}\dots p_n^{a_n}$ και $b = \pm p_1^{b_1}\dots p_n^{b_n}$. Για κάθε i θέτουμε $e_i = \max\{a_i, b_i\}$ και ορίζουμε τον θετικό ακέραιο $e = p_1^{e_1}\dots p_n^{e_n}$. Για παράδειγμα, αν $a = 2^5 \cdot 3^4 \cdot 5^0$ και $b = 2 \cdot 3^6 \cdot 5^2$, τότε $e = 2^5 \cdot 3^6 \cdot 5^2$. Χρησιμοποιώντας την (3), βλέπουμε ότι ο e ικανοποιεί τις δύο συνθήκες στον ορισμό του $\epsilon\kappa\pi$. Συνεπώς το $\epsilon\kappa\pi$ των a, b υπάρχει και είναι μοναδικό. Συμβολίζεται δε με $\epsilon\kappa\pi(a,b)$.

Από τη δεύτερη ιδιότητα στον ορισμό του $\epsilon\kappa\pi$ είναι σαφές ότι ανάμεσα στους θετικούς ακεραίους που είναι κοινά πολλαπλάσια των a και b το $\epsilon\kappa\pi(a,b)$ είναι ο ελάχιστος.

Χρησιμοποιώντας τη σχέση $\min\{a_i,b_i\}+\max\{a_i,b_i\}=a_i+b_i$, εύκολα αποδεικνύεται ότι

$$\mu\kappa\delta(a,b)\epsilon\kappa\pi(a,b)=|ab|. \tag{6}$$

1.2.8 Παραδείγματα.

1. Έστω $a,b,c\in\mathbb{Z}$ με $a|bc$. Αν ισχύει $\mu\kappa\delta(a,b)=1$, τότε $a|c$. (Σύγκρινε με το Λήμμα 1.2.5).
   Επειδή ισχύει $\mu\kappa\delta(a,b)=1$, υπάρχουν $x,y\in\mathbb{Z}$ με $1=ax+by$ (Θεώρημα 1.2.4). Παίρνουμε $c=cax+cby$. Έχουμε $a|cax$ και από την υπόθεση έπεται ότι $a|cby$. Άρα ο a θα διαιρεί τον $cax+cby=c$. (Μια άλλη απόδειξη μπορεί να δοθεί χρησιμοποιώντας αναλύσεις σε γινόμενα πρώτων).

2. Έστω $a,m,n\in\mathbb{Z}$ με $m|a$ και $n|a$. Αν $\mu\kappa\delta(m,n)=1$, τότε $mn|a$.
   Επειδή έχουμε $m|a$ και $n|a$, παίρνουμε $e|a$, όπου $e=\epsilon\kappa\pi(m,n)$. Αλλά από την (6) έχουμε $\epsilon\kappa\pi(m,n)=|mn|$, γιατί $\mu\kappa\delta(m,n)=1$.

3. Αν $a,b\in\mathbb{Z}$ και $\mu\kappa\delta(a,b)=d$, τότε $\mu\kappa\delta(a/d,b/d)=1$.
   Αν ο ακέραιος c διαιρεί και τον a/d και τον b/d, τότε ο cd διαιρεί και τον a και τον b. Άρα ο cd θα διαιρεί τον $\mu\kappa\delta(a,b)=d$ που σημαίνει ότι $c=\pm1$.

4. Αν το γινόμενο δύο σχετικά πρώτων θετικών ακεραίων αριθμών a,b είναι τετράγωνο ακεραίου, τότε οι a,b είναι τετράγωνα ακεραίων.
   Έστω $ab=c^2$ και $a=p_1^{a_1}\dots p_r^{a_r}$, $b=p_1^{b_1}\dots p_r^{b_r}$, $c=p_1^{c_1}\dots p_r^{c_r}$ αναλύσεις σε γινόμενα πρώτων όπως στην (2). Επειδή $\mu\kappa\delta(a,b)=1$, βλέπουμε ότι για κάθε i το πολύ ένας από τους a_i,b_i είναι μη μηδενικός. Από τη σχέση $(p_1^{a_1}\dots p_r^{a_r})(p_1^{b_1}\dots p_r^{b_r})=p_1^{2c_1}\dots p_r^{2c_r}$ και τη μοναδικότητα της παραγοντοποίησης στο $\mathbb{Z}$ έχουμε ότι $a_i+b_i=2c_i$ για κάθε i. Συνεπώς κάθε a_i (και b_i) είναι ίσο είτε με 0 είτε με $2c_i$. Επομένως ο a (και ο b) είναι τετράγωνο ακεραίου.

5. Να βρεθεί ο $\mu\kappa\delta(n^6-1,n^{10}-1)$
   Από τις σχέσεις

$$\begin{aligned} n^{10}-1&=n^4(n^6-1)+n^4-1,\\ n^6-1&=n^2(n^4-1)+n^2-1,\\ n^4-1&=(n^2+1)(n^2-1), \end{aligned}$$

συνάγουμε ότι

$$\mu\kappa\delta(n^{10}-1, n^6-1) = \mu\kappa\delta(n^6-1, n^4-1) = \mu\kappa\delta(n^4-1, n^2-1) = n^2-1.$$

Γενικά ισχύει $\mu\kappa\delta(n^a-1, n^b-1) = n^d-1$, όπου $d = \mu\kappa\delta(a,b)$ (Άσκηση 17).

6. Έστω $\mu\kappa\delta(m,n) = 1$. Να βρεθούν οι δυνατές τιμές για τον $\mu\kappa\delta(m+n, m-n)$.
Θα δείξουμε ότι η απάντηση είναι 1 ή 2. Έστω $d = \mu\kappa\delta(m+n, m-n)$. Επειδή $d|m+n$ και $d|m-n$, παίρνουμε $d|(m+n)+(m-n)$ και $d|(m+n)-(m-n)$, δηλαδή $d|2m$ και $d|2n$. Άρα $d|\mu\kappa\delta(2m,2n)$. Όμως $\mu\kappa\delta(2m,2n) = 2\mu\kappa\delta(m,n)$ από την (;;) και άρα $d|2$, δηλαδή $d = 1$ ή 2. Αποδείξαμε ότι οι πιθανές τιμές του d είναι 1 και 2. Για $m = 2$, $n = 1$ έχουμε $d = 1$, ενώ για $m = 3$, $n = 1$ έχουμε $d = 2$. Συνεπώς οι δυνατές τιμές του d είναι 1 ή 2.

7. Έστω a, b, n θετικοί ακέραιοι. Τότε $a^n|b^n$ αν και μόνο αν $a|b$.
Έστω $a = p_1^{a_1}\dots p_r^{a_r}$ και $b = p_1^{b_1}\dots p_r^{b_r}$ όπου p_i είναι ανά δύο διάφοροι πρώτοι αριθμοί και $a_i, b_i \in \mathbb{N}$. Έχουμε

$$a^n = p_1^{na_1}\dots p_r^{na_r}, \quad b^n = p_1^{nb_1}\dots p_r^{nb_r}.$$

Από τη σχέση (3) παίρνουμε

$$a^n|b^n \Leftrightarrow na_i \le nb_i \ \text{ για κάθε } \ i \Leftrightarrow a_i \le b_i \ \text{ για κάθε } \ i \Leftrightarrow a|b.$$

8. Να βρεθούν όλοι οι θετικοί ακέραιοι m, n τέτοιοι ώστε $m^n = n^m$.
Θα δείξουμε ότι τα ζητούμενα ζεύγη (m,n) είναι τα εξής: (2,4), (4,2) και (m,m) όπου m είναι θετικός ακέραος. Μπορούμε να υποθέσουμε ότι $m \ge n \ge 2$. Τότε $n^n|n^m$ δηλαδή $n^n|m^n$. Από την προηγούμενη Εφαρμογή παίρνουμε $n|m$. Έστω $m = an$. Τότε αντικαθιστώντας στην αρχική εξίσωση και λαμβάνοντας n-στες ρίζες παίρνουμε $an = n^a$. Όμως είναι εύκολο να δειχθεί με επαγωγή στο a ότι $an < n^a$ για κάθε $a \ge 3$ και $n \ge 2$ (Άσκηση 1.1.3). Συνεπώς $a = 1$ ή 2. Για $a = 1$ έχουμε $m = n$ και για $a = 2$ έχουμε $2n = n^2$, οπότε $n = 2$.

9) Έστω b ένας ακέραιος με $b > 1$. Τότε κάθε θετικός ακέραιος n έχει μοναδική παράσταση της μορφής

$$n = a_k b^k + a_{k-1}b^{k-1} + \dots + a_1 b + a_0,$$

όπου $k, a_j \in \mathbb{N}$ με $0 \leq a_j \leq b-1$ για $j = 0, 1, \ldots, k$ και $a_k \neq 0$.
Πράγματι, εφαρμόζοντας διαδοχικά τον Αλγόριθμο Διαίρεσης έχουμε

$$\begin{aligned} n &= bq_0 + a_0, \quad 0 \leq a_0 \leq b-1 \\ q_0 &= bq_1 + a_1, \quad 0 \leq a_1 \leq b-1 \\ &\vdots \\ q_{k-2} &= bq_{k-1} + a_{k-1}, \quad 0 \leq a_{k-1} \leq b-1 \\ q_{k-1} &= b0 + a_k, \quad 0 < a_k \leq b-1. \end{aligned}$$

Έχουμε $q_0 > q_1 > \ldots$. Υποθέτουμε ότι q_k είναι το πρώτο πηλίκο που ισούται με 0. Στην πρώτη ισότητα $n = bq_0 + a_0$ αντικαθιστούμε το q_0 από τη δεύτερη, στη συνέχεια το q_1 από την τρίτη και ούτω καθ΄ εξής. Τελικά προκύπτει μία παράσταση της μορφής $n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$, όπου $0 \leq a_j \leq b-1$ για $j = 0, 1, \ldots, k$ και $a_k \neq 0$. Για την απόδειξη της μοναδικότητας χρησιμοποιούμε τη δεύτερη μορφή της Μαθηματικής Επαγωγής. Το ζητούμενο είναι προφανές για $n = 1$. Έστω $n > 1$. Υποθέτουμε ότι η μοναδικότητα ισχύει για κάθε θετικό ακέραιο μικρότερο του n. Έστω ότι έχουμε και την παράσταση

$$n = c_l b^l + c_{l-1} b^{l-1} + \cdots + c_1 b + c_0,$$

όπου $l, c_j \in \mathbb{N}$ με $0 \leq c_j \leq b-1$ για $j = 0, 1, \ldots, l$ και $c_l \neq 0$. Έχουμε $a_0 = c_0$, γιατί καθένα από αυτά είναι το υπόλοιπο της διαίρεσης του n με τον b. Το ζητούμενο προκύπτει αν εφαρμοστεί η υπόθεση της επαγωγής στον ακέραιο $(n - a_0)/b$.

Η παραπάνω ισότητα που αποδείξαμε ονομάζεται η ***παράσταση του*** n ***ως προς τη βάση*** b. Για $b = 10$ έχουμε τη συνήθη ***δεκαδική παράσταση*** του n. Για $b = 2$ έχουμε τη ***δυαδική παράσταση*** του n. Επισημαίνουμε ότι η απόδειξη της ύπαρξης που δώσαμε παρέχει έναν αλγόριθμο με τον οποίο μπορούμε να βρούμε τα ΄ψηφία΄ a_i στην παράσταση του n ως προς μια βάση b.

Ασκήσεις 1.2

1) Αν ο p είναι πρώτος αριθμός με $p|a^n$, αποδείξτε ότι $p^n|a^n$.
Υπόδειξη: Λήμμα 1.2.5

2) Αν ο p είναι πρώτος αριθμός με $p|a$ και $p|a^2 + b^2$, αποδείξτε ότι $p|b$.

3) Προσδιορίστε τον $\mu\kappa\delta(36, 210)$, όπως και ακεραίους x, y τέτοιους ώστε $\mu\kappa\delta(36, 210) = 36x + 210y$.

4) Να βρεθεί ο ακέραιος $a > 1$ αν $\mu\kappa\delta(a, a+3) = a$.

5) Αποδείξτε ότι $\mu\kappa\delta(m, n) = \mu\kappa\delta(m + kn, n)$ για κάθε $k \in \mathbb{N}$.

6) Αποδείξτε ότι $6|a$ αν και μόνο αν $\mu\kappa\delta(a, a+2) \neq 1$ και $\mu\kappa\delta(a, a+3) \neq 1$.

7) Αποδείξτε ότι $\mu\kappa\delta(m+n, mn) = 1$ αν $\mu\kappa\delta(m, n) = 1$.

8) Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει $\mu\kappa\delta(3n+1, 10n+3) = 1$.

9) Αν $d = \mu\kappa\delta(m, n)$ και $d = mx + ny$, αποδείξτε ότι $\mu\kappa\delta(x, y) = 1$.

10) Αποδείξτε τη σχέση (6).

11) Έστω $a, m \in \mathbb{Z}$ με $m > 0$ και $a \neq 1$. Αποδείξτε ότι
$\mu\kappa\delta\left(\dfrac{a^m - 1}{a-1}, a-1\right) = \mu\kappa\delta(a-1, m)$.
Υπόδειξη: $\dfrac{a^m - 1}{a-1} = (a^{m-1} - 1) + (a^{m-2} - 1) + \cdots + (a-1) + m$.

12) Αν $a_1, \ldots, a_n \in \mathbb{Z}$ (όχι όλοι μηδέν) ορίζουμε τον $\mu\kappa\delta(a_1, \ldots, a_n)$ ως έναν θετικό ακέραιο d που έχει τις ιδιότητες 1) $d|a_i$ για κάθε i, και 2) αν $c \in \mathbb{Z}$ με $c|a_i$ για κάθε i τότε $c|d$.

   i) Αποδείξτε ότι ο $\mu\kappa\delta(a_1, \ldots, a_n)$ υπάρχει, είναι μοναδικός και επιπλέον υπάρχουν $x_i \in \mathbb{Z}$ με $\mu\kappa\delta(a_1, \ldots, a_n) = a_1x_1 + \cdots + a_nx_n$.

   ii) Αποδείξτε ότι αν $a_i \neq 0$ για κάθε i και $n \geq 3$ τότε $\mu\kappa\delta(a_1, \ldots, a_n) = \mu\kappa\delta(a_1, \ldots, a_{n-2}, \mu\kappa\delta(a_{n-1}, a_n)) = \mu\kappa\delta(a_1, \mu\kappa\delta(a_2, \ldots, a_n))$.

   iii) Υπολογίστε τον $\mu\kappa\delta(135, 170, 205, 310)$.

   iv) Γενικεύστε τη σχέση (4).

13) Αν $a_1, \ldots, a_n \in \mathbb{Z}$ είναι μη μηδενικοί ακέραιοι, ορίζουμε το $\epsilon\kappa\pi(a_1, \ldots, a_n)$ ως έναν θετικό ακέραιο e που έχει τις ιδιότητες 1) $a_i|e$ για κάθε i, και 2) αν $c \in \mathbb{Z}$ με $a_i|c$ για κάθε i τότε $e|c$.

   i) Αποδείξτε ότι το $\epsilon\kappa\pi(a_1, \ldots, a_n)$ υπάρχει, είναι μοναδικό και ανάμεσα στα θετικά κοινά πολλαπλάσια των $a_1, \ldots, a_n$ είναι το ελάχιστο.

   ii) Αν τα a_i είναι μη μηδενικά και $n \geq 3$, αποδείξτε ότι $\epsilon\kappa\pi(a_1, \ldots, a_n) = \epsilon\kappa\pi(a_1, \ldots, a_{n-2}, \epsilon\kappa\pi(a_{n-1}, a_n)) = \epsilon\kappa\pi(a_1, \epsilon\kappa\pi(a_2, \ldots, a_n))$.

   iii) Αποδείξτε ότι $\epsilon\kappa\pi(a_1, a_2, a_3) = \dfrac{a_1a_2a_3\mu\kappa\delta(a_1, a_2, a_3)}{\mu\kappa\delta(a_1, a_2)\mu\kappa\delta(a_2, a_3)\mu\kappa\delta(a_1, a_3)}$
   Υπόδειξη: Για κάθε αριθμούς a, b, c ο $\max\{a, b, c\}$ είναι ίσος με
   $$a + b + c - \min\{a, b\} - \min\{b, c\} - \min\{a, c\} + \min\{a, b, c\}.$$

14) Προσδιορίστε όλους τους θετικούς ακεραίους m, n ώστε $\epsilon\kappa\pi(m,n) = 100$.

15) Αποδείξτε ότι για κάθε θετικό ακέραιο a που δεν είναι τετράγωνο ακεραίου το $\sqrt{a}$ είναι άρρητος.

16) Ποιά είναι τα ελάχιστα στοιχεία των παρακάτω συνόλων;

   i) $\{24a + 36b > 0 | a, b \in \mathbb{Z}\}$

   ii) $\{24a + 36b + 8c > 0 | a, b, c \in \mathbb{Z}\}$

   iii) $\{a > 0 | a$ είναι πολλαπλάσιο του 24 και του $36\}$.

17) Αποδείξτε ότι $\mu\kappa\delta(n^a - 1, n^b - 1) = n^d - 1$, όπου $d = \mu\kappa\delta(a, b)$, a, b, n είναι θετικοί ακέραιοι, $n > 1$.

18) Έστω $a, b \in \mathbb{Z}$, $a > 1$. Αποδείξτε ότι υπάρχουν μοναδικά $q, r \in \mathbb{Z}$ με $b = qa + r$ και $-a/2 \leq r < a/2$.

19) i) Αποδείξτε ότι κάθε πρώτος αριθμός διάφορος του 2 είναι της μορφής $4n + 1$ ή $4n + 3$, $n \in \mathbb{N}$.

   ii) Αποδείξτε ότι κάθε φυσικός αριθμός της μορφής $4n + 3$ έχει έναν τουλάχιστον πρώτο διαιρέτη της μορφής $4n + 3$.

   iii) Αποδείξτε ότι υπάρχουν άπειροι πρώτοι αριθμοί της μορφής $4n + 3$, όπου $n \in \mathbb{N}$.
   Υπόδειξη: Τροποποιήστε κατάλληλα την απόδειξη του Ευκλείδη ότι υπάρχουν άπειροι πρώτοι αριθμοί θεωρώντας τον αριθμό $4a_1 \ldots a_m + 3$, όπου $\{3, a_1, \ldots, a_m\}$ είναι το σύνολο των πρώτων της μορφής $4n+3$.
   Σημείωση: Ένα φημισμένο και δύσκολο θεώρημα της Θεωρίας Αριθμών είναι αυτό του Dirichlet, που λέει ότι σε κάθε αριθμητική πρόοδο $an + b$, $n \in \mathbb{N}$, όπου $\mu\kappa\delta(a, b) = 1$, υπάρχουν άπειροι πρώτοι αριθμοί.

20) Αν a, n είναι θετικοί ακέραιοι, τέτοιοι ώστε $n > 1$ και ο $a^n - 1$ είναι πρώτος, αποδείξτε ότι $a = 2$ και ο n είναι πρώτος.

21) Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ο ακέραιος $5^{2n+1} + 6^{2n+1}$ είναι πολλαπλάσιο του 11.

22) Να βρεθούν όλοι οι πρώτοι p ώστε ο $p + 5$ να είναι πρώτος.

23) Αποδείξτε ότι υπάρχει μοναδική τριάδα της μορφής $(p, p + 2, p + 4)$, όπου οι $p, p + 2, p + 4$ είναι πρώτοι αριθμοί.
Σημείωση. Παραμένει μέχρι σήμερα ανοικτό το ερώτημα αν υπάρχουν άπειρα ζεύγη της μορφής $(p, p + 2)$, όπου οι $p, p + 2$ είναι πρώτοι αριθμοί.

24) Η άσκηση αυτή δίνει ένα παράδειγμα υποσυνόλου του $\mathbb{N}$ όπου, ενώ κάθε στοιχείο γράφεται ως γινόμενο "πρώτων", η γραφή *δεν* είναι μοναδική, και έτσι δεν ισχύει σε αυτό το ανάλογο Θεμελιώδες Θεώρημα της Αριθμητικής. Έστω $2\mathbb{Z}$ το σύνολο των αρτίων ακεραίων. Ένα στοιχείο q του $2\mathbb{Z}$ ονομάζεται "πρώτο", αν δεν υπάρχουν $a, b \in 2\mathbb{Z}$ με $q = ab$. Για παράδειγμα, τα $2, 6, 10, 30$ είναι πρώτα στοιχεία του $2\mathbb{Z}$. Αποδείξτε ότι κάθε μη μηδενικό στοιχείο του $2\mathbb{Z}$ γράφεται ως γινόμενο πρώτων στοιχείων. Παρατηρήστε ότι το $60 = 2 \cdot 30 = 6 \cdot 10$ γράφεται κατά δύο διαφορετικούς τρόπους ως γινόμενο πρώτων στοιχείων του $2\mathbb{Z}$.

25) Αν $\mu\kappa\delta(m, n) = 1$, ποιές είναι οι δυνατές τιμές για τον $\mu\kappa\delta(m^2+n^2, m+n)$;

26) Εξετάστε ποιές από τις παρακάτω συνεπαγωγές είναι σωστές.
Έστω $a, b \in \mathbb{Z}$ και $n \in \mathbb{N}$.

- $a|b^n \Rightarrow a|b$
- $a^n|b^n \Rightarrow a|b$
- $a^n|b \Rightarrow a|b$
- $a^3|b^2 \Rightarrow a|b$

27) Έστω a, m, n θετικοί ακέραιοι με $m < n$.

i) Αποδείξτε ότι $a^{2^m} + 1 | a^{2^n} - 1$.

ii) Αποδείξτε ότι $\mu\kappa\delta(a^{2^m} + 1, a^{2^n} + 1) = 1$ ή 2.

iii) Χρησιμοποιώντας το ii) αποδείξτε ότι υπάρχουν άπειροι πρώτοι.

28) i) Αποδείξτε ότι η εξίσωση $x^2 - y^2 = 2$ δεν έχει λύση με $x, y \in \mathbb{Z}$.

ii) Λύστε την εξίσωση $\dfrac{1}{x} + \dfrac{1}{y} = \dfrac{1}{7}$ όπου $x, y \in \mathbb{Z}$.

(*Υπόδειξη*: Παραγοντοποιήστε).

29) Δείξτε ότι για κάθε $n \in \mathbb{N}$ υπάρχει p πρώτος με $n < p \leq n! + 1$ και κατά συνέπεια υπάρχουν άπειροι πρώτοι.

30) Δείξτε ότι για για κάθε $n \in \mathbb{N}$, $n \geq 2$, δεν υπάρχει πρώτος αριθμός p με $n! + 2 \leq p \leq n! + n$.

31) Για την ακολουθία Fibonacci (Άσκηση 1.1.5) δείξτε ότι $\mu\kappa\delta(f_n, f_{n+1}) = 1$ για κάθε $n \in \mathbb{N}$.

32) Για την ακολουθία Fibonacci (Άσκηση 1.1.5) αποδείξτε ότι το f_n διαιρείται με το 3 αν και μόνο αν το n διαιρείται με το 4.

33) Έστω m, n δύο θετικοί ακέραιοι. Αποδείξτε ότι
$\mu\kappa\delta(m,n) = \mu\kappa\delta(m+n, \epsilon\kappa\pi(m,n))$.

34) Αποδείξετε ότι για κάθε ακέραιο $n > 1$, ο ρητός αριθμός $1 + 1/2 + 1/3 + \cdots + 1/n$ δεν είναι ακέραιος.
Υπόδειξη: Έστω ότι $1+1/2+1/3+\cdots+1/n = q \in \mathbb{N}$. Έστω 2^α η μέγιστη δύναμη του 2 που είναι μικρότερη ή ίση από το n. Έστω r το γινόμενο των μέγιστων δυνάμεων των περιττών πρώτων που είναι μικρότερες ή ίσες από το n. Πολλαπλασιάστε με $2^{\alpha-1}r$ για να φθάσετε σε άτοπο.

35) Έστω $f(x) = a_0 + \cdots + a_n x^n$ ένα πολυώνυμο, όπου $a_i \in \mathbb{Z}$ και $n \geq 1$. Αν ένα τουλάχιστον από τα a_i δεν είναι μηδέν, δείξτε ότι υπάρχει $y \in \mathbb{Z}$ τέτοιος ώστε ο $f(y)$ δεν είναι πρώτος.

1.3 Ισοτιμίες

Συχνά συμβαίνει οι λύσεις προβλημάτων που αφορούν ακεραίους να εξαρτώνται μόνο από υπόλοιπα διαιρέσεων. Ας θεωρήσουμε ένα πολύ απλό παράδειγμα. Η απάντηση στο ερώτημα 'ποιά ημέρα της εδβομάδας θα είναι 7001 ημέρες από την επόμενη Κυριακή' φαίνεται αμέσως αν σκεφθούμε ότι οι ημέρες της εβδομάδας επαναλαμβάνονται με περίοδο 7 και ότι $7001 = 7 \cdot 1000 + 1$. Συνεπώς η απάντηση είναι Δευτέρα. Στην ίδια απάντηση θα φθάναμε αν στη θέση του 7001 είχαμε 8, 15 ή οποιονδήποτε φυσικό αριθμό της μορφής $7m + 1$.

1.3.1 Ορισμός. *Έστω m ένας ακέραιος. Δύο ακέραιοι a και b θα λέγονται* ***ισότιμοι*** *modulo m (ή* ***ισοϋπόλοιποι*** *modulo m) αν ο m διαιρεί τη διαφορά $a - b$. Στην περίπτωση αυτή γράφουμε $a \equiv b \mod m$, δηλαδή*[1]

$$a \equiv b \mod m \quad \Leftrightarrow \quad m|a - b.$$

Για παράδειγμα, έχουμε $7001 \equiv 1 \mod 7$ αφού ο 7 διαιρεί τον $7001 - 1 = 7000$. Επίσης $14 \equiv -2 \mod 8$ αφού ο 8 διαιρεί τον $14 - (-2) = 16$.

Επειδή ισχύει $m|a - b$ αν και μόνο αν $-m|a - b$, μπορούμε να θεωρήσουμε στον παραπάνω ορισμό ότι ο m είναι μη αρνητικός.

Παρατηρούμε ότι αν $m = 0$, τότε $a \equiv b \mod m$ αν και μόνο αν $0|a - b$, δηλαδή αν και μόνο αν $a = b$. Άρα δύο ακέραιοι είναι ισότιμοι modulo 0 αν και μόνο αν είναι ίσοι.

1.3.2 Πρόταση. *Έστω m ένας θετικός ακέραιος και a, b δύο ακέραιοι. Τότε:*

1) Ισχύει $a \equiv b \mod m$ αν και μόνο αν οι a και b αφήνουν το ίδιο υπόλοιπο όταν διαιρεθούν με το m.

2) Υπάρχει ακριβώς ένας ακέραιος r με $a \equiv r \mod m$ και $0 \leq r < m$.

Απόδειξη. 1) Από τον Αλγόριθμο Διαίρεσης έχουμε

$$a = mq_1 + r_1, \quad 0 \leq r_1 < m$$
$$b = mq_2 + r_2, \quad 0 \leq r_2 < m,$$

[1] Η έννοια της ισοτιμίας είναι εξαιρετικά χρήσιμη στη Θεωρία Αριθμών αλλά και στην Άλγεβρα όπου εμφανίζεται πιο γενικά υπό τη μορφή των δομών πηλίκο. Αναπτύχθηκε δε συστηματικά από τον Gauss στο έργο του *Disquitiones Arithmeticae* (1801). Εκεί εισήχθηκε ο συμβολισμός $a \equiv b \mod m$ ο οποίος επικράτησε από τότε. Είναι αξιοσημείωτο ότι, αν και έχουν περάσει περισσότερα από 200 χρόνια από την κυκλοφορία του *Disquitiones Arithmeticae*, το βιβλίο αυτό θεωρείται ' σύγχρονο ' και διαβάζεται με ευκολία.

όπου $q_1, q_2, r_1, r_2 \in \mathbb{Z}$. Τότε

$$a - b = m(q_1 - q_2) + r_1 - r_2$$

και από τις ανισότητες παίρνουμε

$$|r_1 - r_2| < m.$$

Επειδή $m|m(q_1 - q_2)$, η προηγούμενη ισότητα δίνει: $m|a - b$ αν και μόνο αν $m|r_1 - r_2$. Επειδή όμως $|r_1 - r_2| < m$, παίρνουμε: $m|r_1 - r_2$ αν και μόνο αν $r_1 - r_2 = 0$. Τελικά, $m|a - b$ αν και μόνο αν $r_1 - r_2 = 0$.
2) Ένας r που ικανοποιεί τις συνθήκες της πρότασης είναι το υπόλοιπο της διαίρεσης του a με τον m. Για τη μοναδικότητα παρατηρούμε ότι αν $a \equiv r \mod m$, $0 \leq r < m$ και $a \equiv s \mod m$, $0 \leq s < m$, τότε από το 1) και τη μοναδικότητα του υπολοίπου διαίρεσης με το m προκύπτει $r = s$. ⊤

1.3.3 Σημείωση. *Παρατηρούμε ότι ισχύουν οι παρακάτω ιδιότητες.*

1) $a \equiv a \mod m$ για κάθε $a \in \mathbb{Z}$, αφού $m|a - a$ για κάθε $a \in \mathbb{Z}$.

2) αν $a \equiv b \mod m$, τότε $b \equiv a \mod m$, αφού από $m|a - b$ έπεται ότι $m| - (a - b)$, δηλαδή $m|b - a$.

3) αν $a \equiv b \mod m$ και $b \equiv c \mod m$, τότε $a \equiv c \mod m$, αφού από τις σχέσεις $m|a-b$ και $m|b-c$ έπεται ότι $m|(a-b)+(b-c)$, δηλαδή $m|a-c$.

Δείχνουμε τώρα ότι οι ισοτιμίες ‘ συμπεριφέρονται καλά ’ σε σχέση με την πρόσθεση και τον πολλαπλασιασμό του $\mathbb{Z}$.

1.3.4 Πρόταση. *Αν $a \equiv b \mod m$ και $c \equiv d \mod m$, τότε*

$$a + c \equiv b + d \mod m \quad \textit{και} \quad ac \equiv bd \mod m$$

Απόδειξη. Από την υπόθεση έχουμε $m|a-b$ και $m|c-d$. Επομένως, $m|(a-b)+(c-d)$, δηλαδή $m|(a+c)-(b+d)$ που σημαίνει ότι $a+c \equiv b+d \mod m$.

Για την άλλη σχέση, παρατηρούμε ότι $ac - bd = ac - bc + bc - bd = (a - b)c + b(c - d)$, που είναι πολλαπλάσιο του m αφού $m|a - b$ και $m|c - d$. Άρα $ac \equiv bd \mod m$. ⊤

1.3.5 Πόρισμα. *Αν $a \equiv b \mod m$, τότε*

$$a + c \equiv b + c \mod m, \quad ac \equiv bc \mod m \quad \textit{και} \quad a^n \equiv b^n \mod m$$

για κάθε φυσικό αριθμό n.

1.3.6 Σημείωση. Από τα προηγούμενα συνάγουμε ότι μπορούμε να χειριστούμε τις ισοτιμίες modulo m σαν ισότητες. Μπορούμε να πολλαπλασιάσουμε ή να προσθέσουμε κατά μέλη δύο ισοτιμίες. Επίσης μπορούμε να υψώσουμε τα μέλη μιας ισοτιμίας σε φυσική δύναμη. Όμως χρειάζεται προσοχή στη 'διαίρεση' όπως εξηγούμε αμέσως παρακάτω.

Νόμος Διαγραφής

Δεν αληθεύει γενικά ότι από $ac \equiv bc \mod m$ έπεται ότι $a = b \mod m$. Για πράδειγμα έχουμε $7 \cdot 2 \equiv 4 \cdot 2 \mod 6$, αλλά όχι $7 \equiv 4 \mod 6$. Αν όμως ισχύει $\mu\kappa\delta(c, m) = 1$, τότε από την ισοτιμία $ac \equiv bc \mod m$ συμπεραίνουμε ότι $a \equiv b \mod m$ σύμφωνα με το Παράδειγμα 1.2.8 1). Σχετικά ισχύει το εξής αποτέλεσμα.

1.3.7 Πρόταση.

1) Αν $ac \equiv bc \mod (cm)$, *όπου* c *είναι διάφορος του μηδενός, τότε*

$$a \equiv b \mod m.$$

2) Αν $ac \equiv bc \mod m$, *όπου τουλάχιστον ένας από τους* c, m *είναι μη μηδενικός, τότε*

$$a \equiv b \mod \frac{m}{d},$$

όπου $d = \mu\kappa\delta(c, m)$.

Απόδειξη. 1) Αν $ac - bc = ecm$ με $c \neq 0$, τότε $a - b = em$.
2) Από την υπόθεση έχουμε $m|c(a-b)$. Άρα $\frac{m}{d}\Big|\frac{c}{d}(a-b)$. Όμως $\mu\kappa\delta\left(\frac{m}{d}, \frac{c}{d}\right) = 1$ και άρα $\frac{m}{d}\Big|a - b$. ⊺

Είναι φανερό ότι ισχύουν τα αντίστροφα των 1) και 2) στην προηγούμενη Πρόταση, δηλαδή αν $a \equiv b \mod m$, τότε $ac \equiv bc \mod (cm)$, και αν $a \equiv b \mod \frac{m}{d}$, όπου $d = \mu\kappa\delta(c, m)$, τότε $ac \equiv bc \mod m$.

1.3.8 Εφαρμογές.

1. Θα αποδείξουμε ότι δεν υπάρχει ακέραιος της μορφής $4n + 3$ ($n \in \mathbb{N}$) που να είναι το άθροισμα δύο τετραγώνων ακεραίων.
   Έστω $a \in \mathbb{N}$ της μορφής $4n+3$ και έστω $x, y \in \mathbb{Z}$ με $a = x^2+y^2$. Από τον Αλγόριθμο Διαίρεσης με το 4, έπεται ότι κάθε ακέραιος είναι της μορφής $4n + r$, όπου $r = 0, 1, 2, 3$. Επειδή $4n + r \equiv r \mod 4$, παίρνουμε $x \equiv 0$ ή 1 ή 2 ή 3 $\mod 4$. Επομένως $x^2 \equiv 0$ ή 1 ή 4 ή 9 $\mod 4$. Αλλά $4 \equiv 0$

mod 4 και $9 \equiv 1 \mod 4$. Άρα $x^2 \equiv 0$ ή $1 \mod 4$. Όμοια έχουμε $y^2 \equiv 0$ ή $1 \mod 4$. Άρα έχουμε $x^2 + y^2 \equiv 0$ ή 1 ή $2 \mod 4$, δηλαδή $a \equiv 0$ ή 1 ή $2 \mod 4$. Αυτό όμως είναι άτοπο γιατί από την υπόθεση έχουμε $a \equiv 3 \mod 4$.
Στην Παράγραφο 2.12 αποδεικνύεται ένα Θεώρημα που χαρακτηρίζει τους φυσικούς αριθμους που είναι άθροισμα δύο τετραγώνων ακεραίων.

2. Για κάθε $n \in \mathbb{N}$, ο ακέραιος $3^{3n} - 5^n$ είναι πολλαπλάσιος του 11.
Επειδή $3^3 = 27 \equiv 5 \mod 11$, έχουμε $3^{3n} = (3^3)^n = 27^n \equiv 5^n \mod 11$. Άρα $3^{3n} - 5^n \equiv 0 \mod 11$.

3. Θα αποδείξουμε ότι δεν υπάρχουν ακέραιοι x, y με $x^2 - 5y^2 = 13$.
Έστω ότι υπάρχουν τέτοιοι ακέραιοι. Τότε έχουμε $x^2 - 5y^2 \equiv 13 \mod 5$. Όμως $5y^2 \equiv 0 \mod 5$ και $13 \equiv 3 \mod 5$. Άρα $x^2 \equiv 3 \mod 5$. Αυτό όμως είναι άτοπο, αφού για κάθε ακέραιο x έχουμε $x \equiv 0, 1, 2, 3$ ή $4 \mod 5$ και κατά συνέπεια $x^2 \equiv 0, 1, 4, 9$ ή $16 \mod 5$, δηλαδή $x^2 \equiv 0, 1$ ή $4 \mod 5$.

4. Να βρεθούν όλοι οι πρώτοι p ώστε οι $p + 10$ και $p + 14$ να είναι πρώτοι.
Δοκιμάζοντας μερικούς μικρούς πρώτους αριθμούς, βλέπουμε ότι για $p = 3$ οι 13 και 17 είναι πρώτοι. Θα δείξουμε τώρα ότι δεν υπάρχει άλλος p. Έστω p πρώτος με $p > 3$. Τότε $p \equiv 1$ ή $2 \mod 3$. Αν $p \equiv 1 \mod 3$, τότε $p + 14 \equiv 15 \mod 3$, δηλαδή $p + 14 \equiv 0 \mod 3$, και επομένως ο $p + 14$ δεν είναι πρώτος αφού είναι πολλαπλάσιο του 3 και διάφορος του 3. Αν $p \equiv 2 \mod 3$, τότε $p + 10 \equiv 12 \mod 3$, δηλαδή $p + 10 \equiv 0 \mod 3$, και κατά συνέπεια ο $p + 10$ δεν είναι πρώτος.

5. Για κάθε περιττό $n \in \mathbb{N}$ ο $1^n + 2^n + \cdots + (n-1)^n$ είναι πολλαπλάσιος του n.
Παρατηρούμε ότι το άθροισμα μπορεί να γραφεί

$$1^n+2^n+\cdots+(n-1)^n = \sum_{k=1}^{k=\frac{n-1}{2}} k^n + \sum_{k=1}^{k=\frac{n-1}{2}} (n-k)^n = \sum_{k=1}^{k=\frac{n-1}{2}} (k^n+(n-k)^n).$$

Έχουμε $n-k \equiv -k \mod n$ και άρα $(n-k)^n \equiv (-k)^n \equiv (-1)^n k^n \equiv -k^n \mod n$, γιατί ο n είναι περιττός. Αρα $k^n + (n-k)^n \equiv 0 \mod n$, και κατά συνέπεια $1^n + 2^n + \cdots + (n-1)^n \equiv 0 \mod n$.

6. **Πυθαγόρειες τριάδες**. Χρησιμοποιώντας τη μοναδικότητα της ανάλυσης ακεραίων σε γινόμενα πρώτων αλλά και απλές ιδιότητες ισοτιμιών θα προσδιορίσουμε όλους τους ακεραίους x, y, z που έχουν την ιδιότητα $x^2 + y^2 = z^2$.

Αν η τριάδα (x, y, z) είναι μια λύση της εξίσωσης $x^2 + y^2 = z^2$, τότε και οι $(\pm x, \pm y, \pm z)$ είναι λύσεις και επομένως μπορούμε να υποθέσουμε ότι οι x, y, z είναι μη αρνητικοί. Παρατηρούμε ότι αν $d = \mu\kappa\delta(x, y, z)$ (Άσκηση 1.2.12), τότε $(x/d)^2 + (y/d)^2 = (z/d)^2$ και $\mu\kappa\delta(x/d, y/d, z/d) = 1$. Επομένως κάθε λύση της αρχικής εξίσωσης θα είναι της μορφής (dx_0, dy_0, dz_0), όπου d είναι θετικός ακέραιος και (x_0, y_0, z_0) είναι μια λύση με $\mu\kappa\delta(x_0, y_0, z_0) = 1$. Από τώρα και στο εξής υποθέτουμε ότι $\mu\kappa\delta(x, y, z) = 1$. Στην περίπτωση αυτή, οι x, y, z είναι ανά δύο σχετικά πρώτοι. Ιδιαίτερα, ακριβώς ένας από τους x, y, z είναι άρτιος.

Παρατηρούμε ότι ο z δεν είναι άρτιος. Πράγματι, αν ο z ήταν άρτιος, τότε οι x, y θα ήταν περιττοί. Αυτό είναι άτοπο αφού από τη μια μεριά έχουμε $z^2 \equiv 0 \mod 4$ και από την άλλη $z^2 = x^2 + y^2 \equiv 1 + 1 \equiv 2 \mod 4$.

Συνεπώς μπορούμε να υποθέσουμε ότι: x περιττός, y άρτιος και z περιττός.

Έχουμε

$$y^2 = z^2 - x^2 = (z - x)(z + x).$$

Ισχυριζόμαστε ότι $\mu\kappa\delta(z-x, z+x) = 2$. Πράγματι, αν $d = \mu\kappa\delta(z-x, z+x)$, τότε $d|(z - x) + (z + x) = 2z$ και $d|(z - x) - (z + x) = -2x$, οπότε $d|\mu\kappa\delta(2z, 2x) = 2\mu\kappa\delta(z, x) = 2$. Επειδή όμως οι $z - x, z + x$ είναι άρτιοι, παίρνουμε $d = 2$.

Θέτουμε $a = (z + x)/2$, $b = y/2$, $c = (z - x)/2$ (που είναι μη αρνητικοί ακέραιοι) οπότε $b^2 = ac$. Επειδή $\mu\kappa\delta(z-x, z+x) = 2$, έχουμε $\mu\kappa\delta(c, a) = 1$, οπότε, σύμφωνα με την Εφαρμογή 1.2.8 4), οι a, c είναι τετράγωνα ακεραίων, $a = u^2$, $c = v^2$. Άρα $z + x = 2u^2$, $z - x = 2v^2$, $y^2 = (2u^2)(2v^2)$ και επομένως

$$x = u^2 - v^2, \quad y = 2uv, \quad z = u^2 + v^2.$$

Επιπλέον ισχύει $u \geq v$, $\mu\kappa\delta(u, v) = 1$, αφού $\mu\kappa\delta(x, y, z) = 1$.

Αποδείξαμε ότι κάθε λύση της αρχικής εξίσωσης $x^2+y^2 = z^2$ με $x, y, z \in \mathbb{N}$ (χωρίς τον περιορισμό $\mu\kappa\delta(x, y, z) = 1$) είναι της μορφής

$$x = d(u^2 - v^2)+, \quad y = 2duv, \quad z = d(u^2 + v^2),$$

όπου $d, u, v \in \mathbb{N}$, $u \geq v$ και $\mu\kappa\delta(u, v) = 1$. Αντίστροφα, με έναν εύκολο υπολογισμό επαληθεύεται ότι οι παραπάνω ακέραιοι x, y, z είναι λύσεις.

Οι τριάδες ακεραίων της μορφής $(d(u^2 - v^2), 2duv, d(u^2 + v^2))$, όπου $\mu\kappa\delta(u, v) = 1$, ονομάζονται '***Πυθαγόρειες τριάδες***'.

7. **Θεώρημα του Fermat[2] για $n = 4$**. Με τη βοήθεια των Πυθαγορείων τριάδων θα αποδείξουμε εδώ ότι δεν υπάρχουν μη μηδενικοί ακέραιοι x, y, z που έχουν την ιδιότητα $x^4 + y^4 = z^4$.
Για τον σκοπό αυτό θα αποδείξουμε ότι η εξίσωση

$$x^4 + y^4 = z^2 \qquad (*)$$

δεν έχει θετικές ακέραιες λύσεις. Αυτό αρκεί γιατί αν (a, b, c) είναι λύση της $x^4 + y^4 = z^4$, τότε (a, b, c^2) είναι λύση της $x^4 + y^4 = z^2$.

Έστω ότι υπάρχει λύση (x, y, z) της $(*)$ με $x, y, z > 0$ θετικοί ακέραιοι. Επιλέγουμε μια λύση με z ελάχιστο. Τότε $\mu\kappa\delta(x, y, z) = 1$ γιατί αν p είναι ένας πρώτος κοινός διαιρέτης των x, y, z ο p^4 διαιρεί τον $x^4 + y^4$ και άρα ο p^2 διαιρεί τον z. Αλλά τότε μία λύση της $(*)$ είναι η $(x/p, y/p, z/p^2)$, πράγμα άτοπο αφού $z/p^2 < z$.

Γράφοντας $(x^2)^2 + (y^2)^2 = z^2$, από την προηγούμενη Εφαρμογή παίρνουμε

$$x^2 = u^2 - \nu^2, \quad y^2 = 2u\nu, \quad z = u^2 + \nu^2$$

όπου u, ν είναι θετικοί ακέραιοι και $\mu\kappa\delta(u, \nu) = 1$. Επειδή $y^2 = 2u\nu$ έχουμε $4|y^2$ και άρα τουλάχιστον ένας από τους u, ν είναι άρτιος. Αν ο u είναι άρτιος, ο ν είναι περιττός και κατά συνέπεια $x^2 = u^2 - \nu^2 \equiv -1 \mod 4$, που είναι άτοπο (βλ. Εφαρμογή 1). Επομένως ο u είναι περιττός και ο ν άρτιος, $\nu = 2\nu'$. Επειδή $y^2 = 4u\nu'$ και $\mu\kappa\delta(u, \nu') = 1$, οι u, ν' είναι τετράγωνα ακεραίων: $u = a^2, \nu' = b^2$ (Παράδειγμα 1.1.8 4). Εφαρμόζουμε πάλι τις Πυθαγόρειες τριάδες, αυτή τη φορά στην εξίσωση $x^2 + \nu^2 = u^2$. Παρατηρούμε ότι ο ν είναι άρτιος και οι x, u περιττοί και ότι $\mu\kappa\delta(x, \nu, u) = 1$. Επομένως υπάρχουν θετικοί ακέραιοι c, d με $\mu\kappa\delta(c, d) = 1$ τέτοιοι ώστε

$$x = c^2 - d^2, \quad \nu = 2cd, \quad u = c^2 + d^2.$$

Επειδή $b^2 = \nu' = cd$, συμπεραίνουμε ότι οι c, d είναι τετράγωνα ακεραίων, $c = e^2$, $d = f^2$. Έχουμε

$$e^4 + f^4 = a^2,$$

[2] Σύμφωνα με το 'Θεώρημα του Fermat' , η εξίσωση $x^n + y^n = z^n$ δεν έχει θετικές ακέραιες λύσεις όταν $n \geq 3$. Ο Fermat (περί το 1637) πίστευε ότι βρήκε μια απόδειξη, αλλά δεν άφησε κανένα σχετικό γραπτό έργο. Σήμερα επικρατεί η άποψη ότι ο Fermat έκανε λάθος. Η προσπάθεια απόδειξης του ισχυρισμού του Fermat οδήγησε στην ανάπτυξη νέων σημαντικών κλάδων των Μαθηματικών όπως είναι η Αλγεβρική Θεωρία Αριθμών και η Μεταθετική Άλγεβρα. Τελικά ο ισχυρισμός του Fermat αποδείχτηκε από τον A. Wiles (1995). Η απόδειξη είναι εξαιρετικά δύσκολη και για την εργασία αυτή απενεμήθη στον Wiles το Cole Prize, που είναι μια από τις ανώτατες διακρίσεις στα Μαθηματικά.

δηλαδή μια λύση της αρχικής εξίσωσης είναι η (e, f, a). Αλλά έχουμε $z = u^2 + \nu^2 = a^4 + 4b^4 > a^4 \geq a$, δηλαδή $z > a$. Αυτό είναι άτοπο από τον ορισμό του z. Η απόδειξη είναι πλήρης.

Η τεχνική που ακολουθήσαμε στην παραπάνω απόδειξη, σύμφωνα με την οποία κατασκευάσαμε μια λύση που είναι 'μικρότερη' από μια 'ελάχιστη', οφείλεται στον Fermat και ονομάζεται η '***μέθοδος της καθόδου***'.

8. **Οι κωδικοί ISBN**. Κάθε δημοσιευμένο βιβλίο περιέχει έναν κωδικό, ο οποίος αποτελείται από 9 ψηφία και έναν ακέραιο μεταξύ 0 και 10. Ο κωδικός αυτός ονομάζεται ISBN (International Standard Book Number). Τα πρώτα 9 ψηφία παρέχουν πληροφορίες για το βιβλίο, όπως τον τόπο και χρόνο έκδοσης. Το τελευταίο ψηφίο χρησιμεύει να εντοπίζονται λάθη. Αν ο κωδικός ISBN είναι $a_1 a_2 \dots a_{10}$, όπου $a_1, \dots, a_9 \in \{0, \dots, 9\}$ και $a_{10} \in \{0, \dots, 10\}$ τότε πρέπει να ισχύει

$$a_1 + 2a_2 + \cdots + 9a_9 \equiv a_{10} \mod 11.$$

9. **ΑΦΜ**. Σε κάθε Έλληνα φορολογούμενο πολίτη αντιστοιχεί ένας εννιαψήφιος Αριθμός Φορολογικού Μητρώου (ΑΦΜ). Όπως και στο προηγούμενο παράδειγμα, το τελευταίο ψηφίο υπάρχει για να αποφεύγονται λάθη ή και να εντοπίζονται πλαστοί ΑΦΜ. Συγκεκριμένα, αν $a_1 \dots a_9$ είναι ο ΑΦΜ τότε πρέπει να ισχύει

$$2^8 a_1 + 2^7 a_2 + \cdots + 2a_8 \equiv a_9 \mod 11,$$

όταν το αριστερό μέλος δεν είναι ισοδύναμο με το 10 mod 11. Διαφορετικά, πρέπει να ισχύει $a_9 = 0$.

Ασκήσεις 1.3

1) Αποδείξτε ότι αν $a \equiv b \mod m$ και $n|m$ τότε $a \equiv b \mod n$.

2) Εξετάστε αν ισχύουν τα παρακάτω ισοτιμίες

   i) $2004 \equiv 1003 \mod 11$

   ii) $(7 - a)^2 \equiv a^2 \mod 7$ για κάθε $a \in \mathbb{Z}$

   iii) $(1 - 2n)^2 \equiv (4n + 1)^{10} \mod 4n$ για κάθε $n \in \mathbb{Z}$

   iv) $(6n + 5)^2 \equiv 1 \mod 4$ για κάθε $n \in \mathbb{Z}$

3) Αποδείξτε ότι

i) $a \equiv b \mod 2 \Rightarrow a^2 \equiv b^2 \mod 4$

ii) $a \equiv b \mod 3 \Rightarrow a^3 \equiv b^3 \mod 9$

4) Αποδείξτε ότι $a \equiv b \mod m$ αν και μόνο αν $a^2 + b^2 \equiv 2ab \mod m^2$.
Υπόδειξη: Εφαρμογή 1.2.8 7).

5) Αποδείξτε ότι για κάθε περιττό ακέραιο a ισχύει $a^2 \equiv 1 \mod 8$.

6) Αποδείξτε ότι για κάθε $a \in \mathbb{Z}$ ισχύει $a^2 \equiv 0, 1$ ή $4 \mod 8$. Κατά συνέπεια ο αριθμός 200340067085 δεν είναι τετράγωνο ακεραίου.

7) Αποδείξτε ότι κανένας ακέραιος της μορφής $3^m + 3^n + 1$, όπου m, n θετικοί ακέραιοι, δεν είναι τετράγωνο ακεραίου.
Υπόδειξη: Εργαστείτε $\mod 8$.

8) Αποδείξτε ότι δεν υπάρχει ακέραιος της μορφής $4n + 2$, όπου $n \in \mathbb{Z}$, που είναι διαφορά δύο τετραγώνων ακεραίων.

9) Για κάθε $n \in \mathbb{N}$ αποδείξτε ότι $4^n \equiv 1 + 3n \mod 9$.

10) Να βρεθούν όλοι οι ακέραιοι $0 \leq x \leq 101$ που ικανοποιούν $x^2 \equiv 1 \mod 101$.

11) Έστω p πρώτος αριθμός. Αποδείξτε ότι αν για τον ακέραιο x ισχύει $x^2 \equiv x \mod p$, τότε $x \equiv 0$ ή $1 \mod p$.

12) Ποιό είναι το υπόλοιπο της διαίρεσης του 100^{100} με το 11;

13) Αποδείξετε ότι κάθε ημερολογιακό έτος (δίσεκτο ή μη) έχει μία τουλάχιστον "Τρίτη και 13".
Υπόδειξη: Μετρήστε modulo 7 αρχίζοντας από την 13η Ιανουαρίου.

14) Αποδείξτε ότι $\mu\kappa\delta(a, m) = \mu\kappa\delta(b, m)$ αν $a \equiv b \mod m$. Εξετάστε αν αληθεύει το αντίστροφο.

15) Ένας ακέραιος αριθμός (σε δεκαδική γραφή) διαιρείται με το 9 αν και μόνο αν το άθροισμα των ψηφίων του, $\sum_i a_i$, διαιρείται με το 9.

16) Ένας ακέραιος αριθμός $a_k \cdots a_1 a_0$ (σε δεκαδική γραφή) διαιρείται με το 11 αν και μόνο αν ο αριθμός $\sum_i (-1)^i a_i$ διαιρείται με το 11.

17) Ένας ακέραιος αριθμός $a_k \cdots a_1 a_0$ (σε δεκαδική γραφή) διαιρείται με το 5 αν και μόνο αν ο αριθμός a_0 διαιρείται με το 5.

18) i) Έστω $a \equiv b \mod m$ και $a \equiv b \mod n$. Αποδείξτε ότι $a \equiv b \mod e$, όπου $e = \epsilon\kappa\pi(m,n)$.

ii) Να βρεθούν όλοι οι ακέραιοι x που ικανοποιούν $x \equiv 7 \mod 8$ και $x \equiv 7 \mod 9$

19) Να βρεθούν όλες οι τριάδες $(p, p+4, p+8)$ όπου οι $p, p+4, p+8$ είναι πρώτοι αριθμοί.

20) Αποδείξτε ότι δεν υπάρχουν ακέραιοι x, y με $7x^2 - 15y^2 = 1$.

21) Αποδείξτε ότι δεν υπάρχουν μη μηδενικοί ακέραιοι x, y, z με $x^2+y^2 = 3z^2$. *Υπόδειξη*:Μέθοδος της καθόδου: Έστω $(x, y, z) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ μια λύση με x θετικό και ελάχιστο. Από $x^2+y^2 = 3z^2$, συμπεράνατε ότι καθένα από τα x, y, z είναι πολλαπλάσιο του 3. Απλοποιώντας λαμβάνουμε μια νέα λύση (x_0, y_0, z_0) με $0 < x_0 < x$. Αυτό είναι άτοπο.

22) Αν ο $x^2 + y^2 + z^2$ είναι πολλαπλάσιο του 5 (όπου $x, y, z \in \mathbb{Z}$) αποδείξτε ότι ένα τουλάχιστον από τους x, y, z είναι πολλαπλάσιο του 5.

23) Αποδείξτε ότι αν ο $m \in \mathbb{N}$ είναι τετράγωνο ακεραίου και κύβος ακεραίου, τότε είναι της μορφής $7k$ ή $7k + 1$.

24) Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει $11|3^{3n+1} + 2^{4n+3}$.

25) Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει $21|4^{n+2} + 5^{2n+1}$.

26) Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει

i) $10^n + 3 \cdot 4^{n+2} \equiv 4 \mod 9$

ii) $(n+1)^{2n} + 4n^{2n+1}$ δεν είναι πολλαπλάσιο του 3.

27) Έστω $m, n \in \mathbb{N}$ με τον n περιττό. Τότε ο ακέραιος $i^n + (m-i)^n$ είναι πολλαπλάσιος του m για κάθε $i = 0, \ldots, m$.

28) Αποδείξτε ότι αν οι m, n είναι περιττοί τότε $1^m + 2^m + \cdots + (n-1)^m \equiv 0 \mod n$.

29) Έστω n περιττός φυσικός αριθμός. Αποδείξτε ότι κάθε ακέραιος είναι ισότιμος modulo n με ακριβώς έναν ακέραιο από τους $-\frac{n-1}{2}, -\frac{n-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{n-3}{2}, \frac{n-1}{2}$.

1.4 Οι Ακέραιοι modulo m

Στην προηγούμενη Παράγραφο διαπιστώσαμε ότι οι ισοτιμίες modulo m ικανοποιούν αριθμητικές ιδιότητες παρόμοιες με ιδιότητες των ακεραίων. Στην Παράγραφο αυτή θα κατασκευάσουμε ένα πεπερασμένο σύνολο $\mathbb{Z}_m$ και θα ορίσουμε κατά φυσικό τρόπο το άθροισμα και το γινόμενο δύο στοιχείων του. Θα δούμε ότι οι αριθμητική στο $\mathbb{Z}_m$ έχει άμεση σχέση με την αριθμητική ισοτιμιών modulo m. Το σύνολο $\mathbb{Z}_m$ με τις πράξεις αυτές παρουσιάζει ιδιαίτερο ενδιαφέρον, γιατί αφενός μεν οι υπολογισμοί σε αυτό επιτρέπουν συχνά την εξαγωγή με σύντομο και κομψό τρόπο χρήσιμων συμπερασμάτων που αφορούν ακεραίους, αφετέρου δε αυτό αποτελεί ένα σημαντικό παράδειγμα δύο γενικότερων εννοιών που θα μελετήσουμε στις επόμενες Ενότητες.

Σχέσεις ισοδυναμίας

Θα χρειαστούμε εδώ (αλλά και σε επόμενες Ενότητες) βασικά στοιχεία από τις ισοδυναμίες τα οποία θα υπενθυμίσουμε.

Μια ***σχέση*** σε ένα σύνολο A είναι ένα υποσύνολο του καρτεσιανού γινομένου $A \times A = \{(a, b) | a, b \in A\}$.

Έστω X μια σχέση στο A. Αντί να γράφουμε $(a, b) \in X$, συχνά χρησιμοποιούμε τον συμβολισμό $a \underset{X}{\sim} b$. Επίσης, πολλές φορές θα γράφουμε $a \sim b$, όταν είναι φανερό ποιο σύνολο X εννοούμε. Συνεπώς οι συμβολισμοί $(a, b) \in X$ και $a \sim b$ είναι ισοδύναμοι.

Μια σχέση στο μη κενό σύνολο A θα λέγεται ***σχέση ισοδυναμίας*** στο A αν ισχύουν οι παρακάτω ιδιότητες.

1) $a \sim a$ για κάθε $a \in A$ (ανακλαστική ιδιότητα)

2) αν $a \sim b$, τότε $b \sim a$ (συμμετρική ιδιότητα), και

3) αν $a \sim b$ και $b \sim c$, τότε $a \sim c$ (μεταβατική ιδιότητα).

1.4.1 Παραδείγματα.

1) Έστω A ένα μη κενό σύνολο. Θεωρούμε τη σχέση που ορίζεται ως εξής: $a \sim b$ αν και μόνο αν $a = b$. Τότε είναι σαφές ότι ορίζεται μια σχέση ισοδυναμίας στο A.

2) Έστω A το σύνολο των σημείων του πραγματικού επιπέδου. Θεωρούμε τη σχέση που ορίζεται ως εξής: $P \sim Q$ αν και μόνο αν τα σημεία P, Q ισαπέχουν από την αρχή των αξόνων. Τότε ορίζεται μια σχέση ισοδυναμίας στο A.

3) Έστω $A = \mathbb{R}$. Θεωρούμε τη σχέση στο $\mathbb{R}$ που ορίζεται ως εξής: $a \sim b$ αν και μόνο αν $a - b \in \mathbb{Z}$. Εύκολα διαπιστώνεται ότι ορίζεται μια σχέση ισοδυναμίας στο $\mathbb{R}$.

Έστω X μια σχέση ισοδυναμίας στο σύνολο A. Αν $a, b \in A$ με $a \sim b$, θα λέμε ότι το a είναι ***ισοδύναμο*** με το b (ή ότι τα a και b είναι ισοδύναμα, πράγμα που μπορούμε να πούμε λόγω της συμμετρικής ιδιότητας). Το σύνολο

$$[a] = \{x \in A | x \sim a\},$$

δηλαδή το σύνολο των στοιχείων του A που είναι ισοδύναμα με το a, ονομάζεται ***κλάση ισοδυναμίας*** του a. Προφανώς έχουμε $a \in [a]$ αφού $a \sim a$.

1.4.2 Παραδείγματα. (συνέχεια)
Η αρίθμηση εδώ αναφέρεται στα προηγούμενα παραδείγματα.

1) Για κάθε $a \in A$, ισχύει $[a] = \{a\}$,

2) Για κάθε σημείο P, η κλάση ισοδυναμίας $[P]$ είναι το σύνολο των σημείων του κύκλου που διέρχεται από το P και έχει κέντρο την αρχή των αξόνων.

3) Για κάθε $a \in \mathbb{R}$, ισχύει $[a] = \{a + m \in \mathbb{R} | m \in \mathbb{Z}\}$. Ειδικά έχουμε $[k] = \mathbb{Z}$ για κάθε $k \in \mathbb{Z}$.

Η επόμενη Πρόταση περιγράφει τις ιδιότητες των κλάσεων ισοδυναμίας που θα χρειαστούμε.

1.4.3 Πρόταση. *Έστω X μια σχέση ισοδυναμίας στο σύνολο A και $a, b \in A$. Τότε*

1. *$[a] = [b]$ αν και μόνο αν τα a, b είναι ισοδύναμα.*

2. *$[a] \cap [b] = \emptyset$ αν και μόνο τα a, b δεν είναι ισοδύναμα.*

3. *Το σύνολο A μπορεί να παρασταθεί ως ξένη ένωση κλάσεων ισοδυναμίας.*

Απόδειξη. 1. Έστω $[a] = [b]$. Τότε $a \in [a] = [b]$, οπότε $a \sim b$, από τον ορισμό της κλάσης ισοδυναμίας. Αντίστροφα, έστω $a \sim b$ και $x \in A$. Αν $x \in [a]$, τότε $x \sim a$. Επειδή $a \sim b$, η μεταβατική ιδιότητα δίνει $x \sim b$, οπότε έχουμε $x \in [b]$. Συνεπώς $[a] \subseteq [b]$. Με παρόμοιο τρόπο αποδεικνύεται ότι $[b] \subseteq [a]$. Άρα $[a] = [b]$.
2. Έστω ότι τα a και b δεν είναι ισοδύναμα και έστω $x \in [a] \cap [b]$. Από τη σχέση $x \in [a]$ συμπεραίνουμε ότι $a \sim x$. Όμοια, έχουμε ότι $x \sim \beta$. Επομένως έχουμε $a \sim b$, που είναι άτοπο. Τέλος αν τα a, b είναι ισοδύναμα, τότε $[a] = [b]$, όπως

είδαμε προηγουμένως, οπότε $[a] \cap [b] = [a] = [b] \neq \emptyset$.
3. Είναι φανερό ότι $A = \bigcup_{a \in A} [a]$. Η ένωση αυτή δεν είναι αναγκαστικά ξένη. Έστω ότι το σύνολο των διακεκριμένων κλάσεων ισοδυναμίας είναι το $\{[b] | b \in B\}$ για κάποιο $B \subseteq A$. Τότε έχουμε $A = \bigcup_{b \in B} [b]$ και επιπλέον από το 2 συμπεραίνουμε ότι $[b] \cap [b'] = \emptyset$, για κάθε $b, b' \in B$ με $b \neq b'$. ⊤

Έστω X μια σχέση ισοδυναμίας στο σύνολο A και $a \in A$. Κάθε στοιχείο της κλάσης ισοδυναμίας $[a]$ ονομάζεται ***αντιπρόσωπος*** της κλάσης $[a]$. Από την προηγούμενη Πρόταση έπεται ότι ένα $b \in A$ είναι αντιπρόσωπος της κλάσης $[a]$, αν και μόνο αν $[a] = [b]$, δηλαδή αν και μόνο αν $a \sim b$. Έστω ότι το σύνολο των διακεκριμένων κλάσεων ισοδυναμίας είναι το $\{[b] | b \in B\}$ για κάποιο $B \subseteq A$. Κάθε τέτοιο σύνολο B ονομάζεται ένα ***πλήρες σύστημα αντιπροσώπων*** της σχέσης ισοδυναμίας X.

Το σύνολο $\mathbb{Z}_m$
Θα εφαρμόσουμε τώρα τα παραπάνω σε μία ενδιαφέρουσα περίπτωση. Έστω m ένας φυσικός αριθμός. Στο σύνολο $\mathbb{Z}$ θεωρούμε τη σχέση που ορίζεται ως εξής

$$a \sim b \Leftrightarrow a \equiv b \mod m \tag{1}$$

Στη Σημείωση 1.3.3 είδαμε ότι η παραπάνω σχέση είναι μια σχέση ισοδυναμίας. Η κλάση ισοδυναμίας του $a \in \mathbb{Z}$ είναι

$$\begin{aligned} [a] &= \{x \in \mathbb{Z} | x \equiv a \mod m\} \\ &= \{x \in \mathbb{Z} | m \text{ διαιρεί τον } x - a\} \\ &= \{x \in \mathbb{Z} | x - a = km, \text{ για κάποιο } k \in \mathbb{Z}\} \\ &= \{a + km \in \mathbb{Z} | k \in \mathbb{Z}\}. \end{aligned} \tag{2}$$

Δηλαδή, τα στοιχεία του συνόλου $[a]$ είναι της μορφής $a + km$, $k \in \mathbb{Z}$. Για τον λόγο αυτό συνηθίζεται ο συμβολισμός $[a] = a + m\mathbb{Z}$. Όταν θέλουμε να δηλώσουμε την εξάρτηση του συνόλου $[a]$ από το m, συνήθως χρησιμοποιούμε τον συμβολισμό $[a]_m$, ή $a \mod m$.

Από την Πρόταση 1.4.3 έχουμε ότι

$$[a] = [b] \Leftrightarrow a \equiv b \mod m. \tag{3}$$

Το σύνολο των κλάσεων ισοδυναμίας που ορίζονται από την σχέση ισοδυναμίας (1) συμβολίζεται με $\mathbb{Z}_m$,

$$\mathbb{Z}_m = \{[a] \,|\, a \in \mathbb{Z}\}.$$

Για παράδειγμα, έστω $m = 2$. Τότε από τη (2) παίρνουμε $[0] = \{x \in \mathbb{Z} | x \text{ άρτιος}\}$ και $[1] = \{x \in \mathbb{Z} | x \text{ περιττός}\}$. Επειδή οι ακέραιοι $\ldots, -4, -2, 0, 2, 4,$

$\ldots$ είναι ισότιμοι $\mod 2$ έχουμε, λόγω της (3), ότι $\ldots = [-4] = [-2] = [0] = [2] = [4] = \ldots$. Επίσης, αφού οι ακέραιοι $\ldots, -3, -1, 1, 3, \ldots$ είναι ισότιμοι $\mod 2$, έχουμε $\ldots = [-3] = [-1] = [1] = [3] = \ldots$. Άρα $\mathbb{Z}_2 = \{[0], [1]\}$. Παρατηρούμε ότι $\mathbb{Z}_2 = \{[-4], [-3]\} = \{[-4], [1]\} = \ldots$ και γενικά

$$\mathbb{Z}_2 = \{[a_0], [a_1]\}, \quad \text{όπου} \quad a_i \equiv i \mod 2.$$

Έστω τώρα $m = 3$. Τότε από τη (2) παίρνουμε $[0] = \{x \in \mathbb{Z} | x = 3k, k \in \mathbb{Z}\}$, $[1] = \{x \in \mathbb{Z} | x = 3k + 1, k \in \mathbb{Z}\}$ και $[2] = \{x \in \mathbb{Z} | x = 3k + 2, k \in \mathbb{Z}\}$. Δηλαδή, $[0] = \{\ldots, -3, 0, 3, ...\}$, $[1] = \{\ldots, -2, 1, 4, \ldots\}$ και $[2] = \{\ldots, -1, 2, 5, \ldots\}$. Από τη σχέση (3) έχουμε ότι $\ldots = [-3] = [0] = [3] = \ldots$ όπως επίσης $\ldots = [-2] = [1] = [4] = \ldots$ και $\ldots = [-1] = [2] = [5] = \ldots$. Άρα $\mathbb{Z}_3 = \{[0], [1], [2]\}$. Παρατηρούμε ότι έχουμε $\mathbb{Z}_3 = \{[-3], [-2], [-1]\} = \{[-3], [1], [2]\} = \ldots$ και γενικά

$$\mathbb{Z}_3 = \{[a_0], [a_1], [a_2]\} \quad \text{όπου} \quad a_i \equiv i \mod 3.$$

1.4.4 Πρόταση. *Για κάθε θετικό ακέραιο m έχουμε $\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$. Πιο γενικά έχουμε $\mathbb{Z}_m = \{[a_0], [a_1], \ldots, [a_{m-1}]\}$, όπου οι a_i είναι ακέραιοι τέτοιοι ώστε $a_i \equiv i \mod m$ για κάθε i.*

Απόδειξη. Παρατηρούμε ότι οι κλάσεις ισοδυναμίας $[a_i]$, $i = 0, \ldots, m-1$ είναι διακεκριμένες. Πράγματι, αν $[a_i] = [a_j]$ με $0 \leq i, j \leq m-1$, τότε από την (3) έχουμε $i \equiv j \mod m$, οπότε από την Πρόταση 1.3.2 2) έχουμε $i = j$. Κάθε κλάση ισοδυναμίας $[a]$ ανήκει στο σύνολο $\{[a_0], [a_1], \ldots, [a_{m-1}]\}$. Πράγματι, από τον αλγόριθμο διαίρεσης έχουμε $\alpha = qm + r$, όπου $0 \leq r \leq m-1$, οπότε $a \equiv r \mod m$ και άρα $[a] = [r] = [a_r]$. Συνεπώς αποδείξαμε ότι $\mathbb{Z}_m \subseteq \{[a_0], [a_1], \ldots, [a_{m-1}]\}$. Επομένως $\mathbb{Z}_m = \{[a_0], [a_1], \ldots, [a_{m-1}]\}$. ⊤

Το $\mathbb{Z}_m$ ονομάζεται το σύνολο ***των ακεραίων*** modulo $\boldsymbol{m}$ και τα στοιχεία του ονομάζονται ***κλάσεις ισοτιμίας*** modulo $\boldsymbol{m}$, ή ***κλάσεις υπολοίπων*** modulo $\boldsymbol{m}$.

Παρατηρήσεις

1) Ένας διαισθητικός τρόπος να σκεφτόμαστε το σύνολο $\mathbb{Z}_m$ είναι ο εξής. Γύρω από έναν κύκλο με μήκος περιφέρειας m τυλίγουμε τον άξονα των πραγματικών αριθμών. Τότε τα σημεία $\ldots, -m, 0, m, 2m, \ldots$ του άξονα θα ταυτιστούν πάνω στον κύκλο. Ομοίως θα ταυτιστούν τα σημεία $\ldots, -m+1, 1, m+1, 2m+1, \ldots$.

2) Στην προηγούμενη Πρόταση είχαμε υποθέσει ότι ο m είναι θετικός. Αν $m = 0$, τότε από τη σχέση (1) έχουμε $a \sim b$ αν και μόνο αν $a = b$. Συνεπώς η κλάση ισοδυναμίας του a αποτελείται από ένα μόνο στοιχείο, $[a] = \{a\}$. Τότε, ταυτίζοντας το σύνολο $\{a\}$ με το στοιχείο a, μπορούμε να θεωρήσουμε ότι το σύνολο των κλάσεων υπολοίπων modulo 0 είναι το $\mathbb{Z}$.

3) Αν $m = 1$, τότε από τη σχέση (1) έχουμε $a \sim b$ για κάθε δύο ακεραίους a, b. Συνεπώς η κλάση ισοδυναμίας ενός ακεραίου a είναι όλο το σύνολο $\mathbb{Z}$ και άρα το σύνολο των κλάσεων υπολοίπων modulo 1 είναι ένα μονοσύνολο.

Η πρόσθεση και ο πολλαπλασιασμός στο $\mathbb{Z}_m$

Κατασκευάσαμε το σύνολο $\mathbb{Z}_m$ με τη βοήθεια μιας σχέσης ισοδυναμίας στο σύνολο $\mathbb{Z}$. Στο $\mathbb{Z}$, όμως, γνωρίζουμε πως να προσθέτουμε και να πολλαπλασιάζουμε στοιχεία. Συνεπώς είναι εύλογο το ερώτημα αν μπορούμε να προσθέτουμε και να πολλαπλασιάζουμε στοιχεία του $\mathbb{Z}_m$ με ανάλογο τρόπο.

Η πρόσθεση (αντίστοιχα, ο πολλαπλασιασμός) ακεραίων αντιστοιχεί σε *κάθε* ζεύγος (a, b) ακεραίων *μοναδικό* ακέραιο, τον $a+b$ (αντίστοιχα, τον ab). Δηλαδή έχουμε απεικονίσεις

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (a, b) \mapsto a + b$$
$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (a, b) \mapsto ab.$$

Με τη βοήθεια αυτών, ορίζουμε τις αντιστοιχίες,

$$+ : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m, ([a], [b]) \mapsto [a + b]$$
$$\cdot : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m, ([a], [b]) \mapsto [ab].$$

Αποδεικνύουμε τώρα ότι οι αντιστοιχίες αυτές είναι απεικονίσεις. Πρέπει να δείξουμε ότι: αν $([a], [b]) = ([c], [d])$, δηλαδή αν $[a] = [c]$ και $[b] = [d]$, τότε έπεται ότι $[a+b] = [c+d]$ και $[ab] = [cd]$. Με άλλα λόγια, αν $a \equiv c \mod m$ και $b \equiv d \mod m$, τότε $a + b \equiv c + d \mod m$ και $ab \equiv cd \mod m$. Όμως αυτό ισχύει από την Πρόταση 1.3.4.

Για παράδειγμα, στο $\mathbb{Z}_3$ έχουμε $[4] + [2] = [6] = [0]$, $[2][2] = [4] = [1]$. Στο $\mathbb{Z}_{10}$ έχουμε $[4] + [7] = [11] = [1]$, $[4][7] = [28] = [8]$, $[5][6] = [30] = [0]$. Βλέπουμε ότι η πρόσθεση και ο πολλαπλασιασμός κλάσεων υπολοίπων ανάγονται στη πρόσθεση και στον πολλαπλασιασμό αντιπροσώπων τους, δηλαδή ακεραίων.

Για την πρόσθεση και τον πολλαπλασιασμό που ορίσαμε στο $\mathbb{Z}_m$ ισχύουν οι παρακάτω ιδιότητες που θυμίζουν γενικές ιδιότητες της Αριθμητικής. Για κάθε $[a], [b], [c] \in \mathbb{Z}_m$ έχουμε ότι:

1. $([a] + [b]) + [c] = [a] + ([b] + [c])$

2. $[a]+[0]=[0]+[a]$
3. $[a]+[-a]=[-a]+[a]=[0]$
4. $[a]+[b]=[b]+[a]$
5. $([a][b])[c]=[a]([b][c])$
6. $[a]([b]+[c])=[a][b]+[a][c]$
7. $([a]+[b])[c]=[a][c]+[b][c]$
8. $[a][b]=[b][a]$
9. $[a][1]=[1][a]=[a]$

Οι αποδείξεις είναι απλές και παραλείπονται.

Οι ιδιότητες 1-9 θα εφαρμόζονται στα παρακάτω χωρίς ιδιαίτερη μνεία.

Παρατήρηση Πρέπει να τονιστεί εδώ, ότι αν και η πρόσθεση και ο πολλαπλασιασμός στοιχείων του $\mathbb{Z}_m$ έχουν ιδιότητες που θυμίζουν την πρόσθεση και τον πολλαπλασιασμό ακεραίων, υπάρχουν σημαντικές διαφορές. Για παράδειγμα, στο $\mathbb{Z}$ το γινόμενο δύο μη μηδενικών στοιχείων είναι μη μηδενικό. Στο $\mathbb{Z}_6$, όμως, έχουμε $[2][3]=[0]$. Επίσης, αν οι ακέραιοι a,b,c είναι τέτοιοι ώστε $ac=bc$ και $c\neq 0$, τότε $a=b$. Στο $\mathbb{Z}_6$, όμως, έχουμε $[1][3]=[5][3]$ με $[3]\neq[0]$ και $[1]\neq[5]$.

Αντιστρέψιμα στοιχεία στο $\mathbb{Z}_m$

Στη μελέτη της Αριθμητικής του $\mathbb{Z}_m$ (δηλαδή των ιδιοτήτων της πρόσθεσης και του πολλαπλασιασμού του $\mathbb{Z}_m$) είναι φυσικό να θεωρήσουμε πολυωνυμικές εξισώσεις στο $\mathbb{Z}_m$, δηλαδή πολυωνυμικές εξισώσεις με συντελεστές στοιχεία του $\mathbb{Z}_m$. Μία από τις απλούστερες από αυτές τις εξισώσεις είναι η $[a][x]=[b]$. Στην περίπτωση που υπάρχει κλάση $[a']\in\mathbb{Z}_m$ με την ιδιότητα $[a'][a]=[1]$ μπορούμε εύκολα να λύσουμε την εξίσωση πολλαπλασιάζοντάς την με την $[a']$,

$$[a][x]=[b]\Rightarrow[a']([a][x])=[a'][b]\Rightarrow[x]=[a'b].$$

Όμως δεν υπάρχει πάντα τέτοια κλάση $[a']$. Για παράδειγμα, έστω $[2]\in\mathbb{Z}_6$. Αν υπήρχε $[a']\in\mathbb{Z}_6$ με $[2][a']=[1]$, τότε $[2a']=[1]$ και άρα $2a'\equiv 1 \mod 6$, δηλαδή $2a'=1+6n, n\in\mathbb{Z}$, που είναι άτοπο. Οδηγούμαστε έτσι στον επόμενο ορισμό.

Ένα στοιχείο $[a]\in\mathbb{Z}_m$ λέγεται ***αντιστρέψιμο*** αν υπάρχει $[a']\in\mathbb{Z}_m$ με την ιδιότητα $[a][a']=[1]$, δηλαδή αν υπάρχει ακέραιος a' τέτοιος ώστε $aa'\equiv 1 \mod m$. Στην περίπτωση αυτή, το στοιχείο $[a']$ ονομάζεται αντίστροφο του $[a]$. Επίσης θα λέμε ότι ένα ***αντίστροφο modulo m*** του ακεραίου a είναι ο ακέραιος

a'. Για παράδειγμα, στο $\mathbb{Z}_6$ το$[5]$ είναι αντιστρέψιμο αφού $[5][5] = [1]$, ενώ το $[2]$ δεν είναι, όπως είδαμε πριν. Μάλιστα, τα μόνα αντιστρέψιμα στοιχεία του $\mathbb{Z}_6$ είναι τα $[1], [5]$. Στο $\mathbb{Z}_7$ το$[2]$ είναι αντιστρέψιμο αφού $[2][4] = [1]$.

Το σύνολο των αντιστρέψιμων στοιχείων του $\mathbb{Z}_m$ συμβολίζεται με $U(\mathbb{Z}_m)$.

Έστω $[a]$ ένα αντιστρέψιμο στοιχείο του $\mathbb{Z}_m$. Τότε υπάρχει μοναδικό στοιχείο $[a'] \in \mathbb{Z}_m$ με την ιδιότητα $[a][a'] = [1]$. Πράγματι, αν είχαμε $[a][a'] = [1]$ και $[a][a''] = [1]$, τότε $[a'] = [a'][1] = [a']([a][a'']) = ([a'][a])[a''] = ([a'][a])[a''] = [1][a''] = [a'']$.

Στην επόμενη Πρόταση προσδιορίζοντα τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_m$.

1.4.5 Πρόταση. *Το στοιχείο $[a] \in \mathbb{Z}_m$ είναι αντιστρέψιμο αν και μόνο αν $\mu\kappa\delta(a, m) = 1$.*

Απόδειξη. Έστω ότι $[a][b] = 1$. Τότε $ab \equiv 1 \mod m$, δηλαδή $ab = mn + 1$ για κάποιο $n \in \mathbb{Z}$. Από την τελευταία σχέση προκύπτει ότι $\mu\kappa\delta(a, m) = 1$. Αντίστροφα, έστω $\mu\kappa\delta(a, m) = 1$. Τότε υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $ax + my = 1$ (Θεώρημα 1.2.4). Έχουμε

$$\begin{aligned}[ax + my] = [1] &\Rightarrow [ax] + [my] = [1] \\ &\Rightarrow [a][x] + [m][y] = [1] \\ &\Rightarrow [a][x] + [0][y] = [1] \\ &\Rightarrow [a][x] = [1],\end{aligned}$$

δηλαδή το $[a]$ είναι αντιστρέψιμο. ⊤

Σημείωση Η παραπάνω απόδειξη περιέχει έναν πρακτικό τρόπο υπολογισμού του αντιστρόφου (εφόσον αυτό υπάρχει)του $[a]$. Με το συμβολισμό της απόδειξης, το αντίστροφο του $[a]$ είναι το $[x]$. Ένας τέτοιος ακέραιος x μπορεί να βρεθεί χρησιμοποιώντας τον Ευκλείδειο αλγόριθμο, όπως γνωρίζουμε από την Παράγραφο 1.2. Θα δούμε αμέσως παρακάτω ένα σχετικό παράδειγμα.

1.4.6 Εφαρμογή. Θα βρεθούν όλοι οι ακέραιοι x τέτοιοι ώστε $8x \equiv 11 \mod 15$. Εργαζόμενοι στο $\mathbb{Z}_{15}$ έχουμε $[8x] = [11]$, δηλαδή

$$[8][x] = [11]. \tag{1}$$

Επειδή $\mu\kappa\delta(8, 15) = 1$, το στοιχείο $[8]$ είναι αντιστρέψιμο στο $\mathbb{Z}_{15}$ σύμφωνα με την προηγούμενη Πρόταση. Έστω $[8][y] = [1]$. Πολλαπλασιάζοντας την (1) με $[y]$ παίρνουμε

$$[x] = [11y],$$

και συνεπώς αρκεί να προσδιορίσουμε έναν ακέραιο y. Χρησιμοποιώντας τον Ευκλείδειο αλγόριθμο για το ζεύγος $(8, 15)$ έχουμε $15 = 1 \cdot 8 + 7, 8 = 1 \cdot 7 + 1$.

Άρα $1 = 8 - 1 \cdot 7 = 8 - 1 \cdot (15 - 1 \cdot 8) = 8 \cdot 2 + 15(-1)$. Συνεπώς $[1] = [8 \cdot 2] + [15 \cdot (-1)] = [8][2]$ και άρα μπορούμε να θέσουμε $y = 2$. Τελικά $[x] = [11 \cdot 2] = [22] = [7]$, δηλαδή

$$x = 15n + 7, \quad n \in \mathbb{Z}.$$

Το σύνολο των αντιστρέψιμων στοιχείων του $\mathbb{Z}_m$ έχει ενδιαφέρουσες ιδιότητες ως προς τον πολλαπλασιασμό του $\mathbb{Z}_m$. Για παράδειγμα, ισχύει $[a]^k = [1]$ για κάθε $[a] \in U(\mathbb{Z}_m)$, όπου k είναι το πλήθος των στοιχείων του $U(\mathbb{Z}_m)$. Αυτό θα αποδειχθεί στην Παράγραφο 1.6. Εδώ θα αποδείξουμε την ειδική περίπτωση που ο $m = p$ είναι πρώτος. Στην περίπτωση αυτή, από την Πρόταση 1.4.4 και την Πρόταση 1.4.5 έχουμε ότι $k = p - 1$.

1.4.7 Θεώρημα (*Μικρό Θεώρημα του* Fermat). *Έστω $a \in \mathbb{Z}$ και p ένας πρώτος αριθμός. Τότε*

$$a^p \equiv a \mod p.$$

Αν επιπλέον ο p δεν διαιρεί τον a, τότε

$$a^{p-1} \equiv 1 \mod p.$$

Απόδειξη. Για να δείξουμε την πρώτη σχέση, θεωρούμε αρχικά την περίπτωση $a \in \mathbb{N}$ και χρησιμοποιούμε επαγωγή στον a. Για $a = 0$, η σχέση είναι προφανής. Υποθέτοντας ότι ισχύει η ισοτιμία για τον a, θα την αποδείξουμε για τον $a + 1$. Από το διωνυμικό ανάπτυγμα έχουμε

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1.$$

Ισχυριζόμαστε ότι οι ακέραιοι $\binom{p}{i} = \dfrac{(p-i+1)\cdots(p-1)p}{1.2\ldots i}$ είναι πολλαπλάσιοι του p όταν $i = 1, 2, \ldots, p-1$. Πράγματι, γράφοντας $(p-i+1)\ldots(p-1)p = \binom{p}{i}1 \cdot 2 \cdot \cdots \cdot i$ παρατηρούμε ότι ο p διαιρεί το αριστερό μέλος και άρα το δεξιό. Αφού ο p είναι πρώτος θα διαιρεί έναν τουλάχιστον παράγοντα λόγω της Παρατήρησης 1.2.6 1. Όμως ο p δεν διαιρεί κανένα από τους $1, 2, \ldots i$, οπότε διαιρεί τον $\binom{p}{i}$. Επομένως έχουμε ότι

$$(a+1)^p \equiv a^p + 1 \mod p.$$

Από την επαγωγική υπόθεση ισχύει $a^p \equiv a \mod p$ και συνεπώς $(a+1)^p \equiv a+1 \mod p$, που είναι το ζητούμενο.

Έχουμε αποδείξει την πρώτη σχέση για $a \in \mathbb{N}$. Έστω τώρα $a \in \mathbb{Z}$, $a < 0$. Αν ο p είναι περιττός έχουμε $a^p = -(-a)^p \equiv -(-a) \mod p$ από την περίπτωση της ισοτιμίας που αποδείξαμε πριν. Άρα $a^p \equiv a \mod p$. Άν $p = 2$, τότε $a^2 = (-a)^2 \equiv -a \mod 2$. Αλλά $-a \equiv a \mod 2$ και κατά συνέπεια $a^2 \equiv a \mod 2$.

Θα αποδείξουμε τώρα τη δεύτερη σχέση. Επειδή έχουμε $\mu\kappa\delta(p, a) = 1$, το στοιχείο $[a]$ είναι αντιστρέψιμο στο $\mathbb{Z}_p$ (Πρόταση 1.4.5). Έστω $[b][a] = [1]$. Πολλαπλασιάζοντας τη σχέση $[a^p] = [a]$ με $[b]$ προκύπτει ότι $[a^{p-1}] = [1]$. ⊤

1.4.8 Παρατήρηση. Από τη δεύτερη ισοτιμία στο Μικρό Θεώρημα του Fermat έχουμε ότι αν ο p είναι πρώτος και ο $a \in \mathbb{Z}$ δεν διαιρείται με τον p, τότε το αντίστροφο του $[a]$ στο $\mathbb{Z}_p$ είναι το $[a^{p-2}]$.

1.4.9 Παραδείγματα.

1) Το Μικρό Θεώρημα του Fermat μας διευκολύνει να υπολογίσουμε υπόλοιπα διαιρέσεων μεγάλων αριθμών με πρώτους. Για παράδειγμα, ας υπολογίσουμε το υπόλοιπο της διαίρεσης του 222^{555} με το 7. Επειδή έχουμε $222 = 31 \cdot 7 + 5$ παίρνουμε $222 \equiv 5 \mod 7$. Άρα

$$222^{555} \equiv 5^{555} \mod 7.$$

Από τη σχέση $555 = 92 \cdot 6 + 3$ παίρνουμε $5^{555} = (5^6)^{92} \cdot 5^3$. Από το Μικρό Θεώρημα του Fermat έχουμε $5^6 \equiv 1 \mod 7$. Συνεπώς

$$5^{555} \equiv 5^3 \mod 7.$$

Αλλά $5^3 \equiv (-2)^3 \equiv -8 \equiv 6 \mod 7$. Το ζητούμενο υπόλοιπο είναι 6.

2) Έστω p ένας πρώτος αριθμός και $a, b \in \mathbb{Z}$ με $a^p \equiv b^p \mod p$. Τότε $a^p \equiv b^p \mod p^2$
Πράγματι, χρησιμοποιώντας το Μικρό Θεώρημα του Fermat, από την υπόθεση συμπεραίνουμε ότι $a \equiv b \mod p$. Συνεπώς $b = a + kp$, $k \in \mathbb{Z}$. Τότε χρησιμοποιώντας το διωνυμικό ανάπτυγμα έχουμε

$$\begin{aligned} b^p - a^p &= (a + kp)^p - a^p \\ &= \binom{p}{1} a^{p-1}(kp) + \binom{p}{2} a^{p-2}(kp)^2 + \cdots + \binom{p}{p} (kp)^p. \end{aligned}$$

Είναι προφανές ότι στο δεξιό μέλος κάθε προσθετέος διαιρείται με τον p^2.

3) Για κάθε $n \in \mathbb{N}$ ισχύει $42|n^7 - n$.
Έχουμε $42 = 2 \cdot 3 \cdot 7$. Από το Παράδειγμα 1.2.8 2), αρκεί να αποδειχθεί ότι ισχύει κάθε μια από τις ισοτιμίες

$$\begin{aligned} n^7 &\equiv n \mod 7 \\ n^7 &\equiv n \mod 3 \\ n^7 &\equiv n \mod 2 \end{aligned}$$

Η πρώτη ισχύει από το Μικρό Θεώρημα του Fermat για $p = 7$. Για τη δεύτερη παρατηρούμε ότι εφαρμόζοντας δύο φορές το Μικρό Θεώρημα του Fermat για $p = 3$ έχουμε

$$n^7 = (n^3)^2 n \equiv n^2 n \equiv n \mod 3$$

Με παρόμοιο τρόπο (ή και άμεσα) αποδεικνύεται και η τρίτη ισοτιμία.

Ασκήσεις 1.4

1) Ποια είναι τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_{10}$; Για καθένα από αυτά υπολογίστε το αντίστροφο στοιχείο. Ποια από τα αντιστρέψιμα στοιχεία συμπίπτουν με το αντίστροφο τους;

2) Να βρεθούν όλοι οι ακέραιοι x τέτοιοι ώστε $12x \equiv 11 \mod 13$.

3) Να λυθεί στο $\mathbb{Z}_{127}$ η εξίσωση $[58][x] = [3]$.

4) Αληθεύει ότι η εξίσωση $[4][x] = [3]$ έχει λύση στο $\mathbb{Z}_6$;

5) Αποδείξτε ότι η εξίσωση $[a][x] = [b]$ έχει λύση στο $\mathbb{Z}_m$ αν και μόνο αν $\mu\kappa\delta(a, m)|b$.

6) Να λυθούν οι παρακάτω εξισώσεις

- $[x]^2 = [1]$ στο $\mathbb{Z}_8$
- $[x]^4 = [1]$ στο $\mathbb{Z}_5$
- $[x]^3 = [1]$ στο $\mathbb{Z}_5$
- $[x]^2 + [3][x] + [2] = [0]$ στο $\mathbb{Z}_6$
- $[x] + [x] + [x] = [0]$ στο $\mathbb{Z}_3$.

7) Αποδείξτε ότι ο ακέραιος p είναι πρώτος αν και μόνο αν το πλήθος των αντιστρέψιμων στοιχείων του $\mathbb{Z}_p$ είναι $p-1$.

8) Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει $n^5 \equiv n \mod 30$.

9) Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει $n^{49} \equiv n \mod 1547$.
Υπόδειξη: $1547 = 7 \cdot 13 \cdot 17$.

10) Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει $(n+1)^9 + 4n^5 \equiv 1 \mod 5$

11) Αποδείξτε ότι $n^{12} + 12^n \equiv 5 \mod 11$ αν και μόνο αν $n \equiv 2, 9 \mod 11$.

12) Ποιο είναι το υπόλοιπο της διαίρεσης του 100^{100} με το 13;

13) Ποια ημέρα της εβδομάδας θα είναι 333^{444} ημέρες από σήμερα;

14) Να βρεθεί ένα στοιχείο $[a]$ του $U(\mathbb{Z}_5)$ ώστε κάθε άλλο στοιχείο του $U(\mathbb{Z}_5)$ να είναι της μορφής $[a]^n$, $n \in \mathbb{N}$. Υπάρχει τέτοιο στοιχείο στο $U(\mathbb{Z}_8)$;

15) Έστω p πρώτος και $a \in \mathbb{Z}$ που δεν είναι πολλαπλάσιο του p. Αποδείξτε ότι ο ελάχιστος θετικός ακέραιος n για τον οποίο ισχύει στο $U(\mathbb{Z}_p)$ ότι $[a]^n = [1]$ είναι διαιρέτης του $p-1$.

16) Υπολογίστε το άθροισμα όλων των στοιχείων του $\mathbb{Z}_m$ όταν $m = 3, 4, 5, 6$. Αποδείξτε ότι αν ο m είναι περιττός, τότε το άθροισμα όλων των στοιχείων του $\mathbb{Z}_m$ είναι ίσο με $[0]$. Με τί ισούται το εν λόγω άθροισμα όταν ο m είναι άρτιος;

17) Έστω p πρώτος αριθμός με $p \equiv 3 \mod 4$. Αποδείξτε ότι δεν υπάρχει $[a] \in \mathbb{Z}_p$ με $[a]^2 = [-1]$.

18) Έστω $\mathbb{Z}_m = \{[a_1], \dots [a_m]\}$ και $[a] \in \mathbb{Z}_m$. Αποδείξτε ότι τα στοιχεία $[a] + [a_i]$, όπου $i = 1, \dots, m$, είναι διακεκριμένα και επομένως $\mathbb{Z}_m = \{[a + a_1], \dots, [a + a_m]\}$. Έστω επιπλέον ότι $[a] \neq [0]$. Αληθεύει ότι τα στοιχεία $[a][a_i]$, $i = 1, \dots, m$, είναι διακεκριμένα;

19) Εξετάστε αν αληθεύει ότι το άθροισμα δύο αντιστρέψιμων στοιχείων του $\mathbb{Z}_m$ είναι αντιστρέψιμο.

1.5 Διοφαντικές Εξισώσεις και Ισοτιμίες

Πολλά μαθηματικά προβλήματα που συναντάμε στην καθημερινή μας ζωή ανάγονται σε εξισώσεις στις οποίες επιζητούμε λύσεις που να είναι ακέραιοι αριθμοί. Οι εξισώσεις αυτής της μορφής παίζουν σημαντικό ρόλο στη Θεωρία Αριθμών και στην Άλγεβρα.

Μια εξίσωση της μορφής $f(x_1, \dots x_n) = 0$, όπου το $f(x_1, \dots x_n)$ είναι ένα πολυώνυμο των $x_1, \dots x_n$ με ακεραίους συντελεστές, ονομάζεται ***Διοφαντική*** όταν μας ενδιαφέρουν μόνο οι ακέραιες λύσεις της. Θα ασχοληθούμε εδώ με την πρώτη μη τετριμμένη Διοφαντική εξίσωση, $ax + by = c$, και θα περιγράψουμε πλήρως τις λύσεις της. Με τη χρήση αυτής θα λύσουμε την ισοτιμία $ax \equiv b \mod m$. Τέλος θα ασχοληθούμε με συστήματα ισοτιμιών (Κινεζικό Θεώρημα Υπολοίπων).

1.5.1 Θεώρημα. *Έστω $a, b, c \in \mathbb{Z}$ τέτοιοι ώστε τουλάχιστον ένας από τους a, b δεν είναι μηδεν. Θέτουμε $d = \mu\kappa\delta(a, b)$.*

1) *Αν ο d δεν διαιρεί τον c, τότε η Διοφαντική εξίσωση $ax + by = c$ δεν έχει λύσεις.*

2) *Αν ο d διαιρεί τον c, τότε η Διοφαντική εξίσωση έχει άπειρες λύσεις. Επιπλέον αν (x_0, y_0) είναι μία λύση, τότε κάθε άλλη λύση έχει τη μορφή*

$$x = x_0 + \frac{b}{d}n, \quad y = y_0 - \frac{a}{d}n, \quad n \in \mathbb{Z}. \tag{1}$$

Απόδειξη. 1) Υποθέτουμε ότι ο d δεν διαιρεί τον c. Έστω ότι υπάρχουν ακέραιοι x, y τέτοιοι ώστε $ax + by = c$. Αφού $d|a$ και $d|b$, παίρνουμε $d|c$, που είναι άτοπο.

2) Υποθέτουμε ότι ο d διαιρεί τον c. Επειδή $\mu\kappa\delta(a, b) = d$, υπάρχουν $s, t \in \mathbb{Z}$ με

$$d = as + bt \tag{2}$$

Αφού $d|c$, έχουμε $c = de$, όπου $e \in \mathbb{Z}$. Από την (2) παίρνουμε

$$c = de = a(se) + b(te),$$

που σημαίνει ότι μία λύση είναι η $x_0 = se$, $y_0 = te$.

Θα δείξουμε ότι η δοθείσα Διοφαντική εξίσωση έχει άπειρες λύσεις. Έστω $x = x_0 + \frac{b}{d}n$ και $y = y_0 - \frac{a}{d}n$, $n \in \mathbb{Z}$. Εύκολα επαληθεύεται με πράξεις ότι $ax + by = c$.

Τώρα θα δείξουμε ότι κάθε λύση είναι της μορφής (1). Έστω $x_0, y_0, x, y \in \mathbb{Z}$ με $ax + by = c$ και $ax_0 + by_0 = c$. Αφαιρώντας κατά μέλη παίρνουμε

$$a(x - x_0) = b(y_0 - y) \tag{3}$$

και άρα $\frac{a}{d}(x - x_0) = \frac{b}{d}(y - y_0)$. Αφού $\mu\kappa\delta\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, έχουμε ότι $\frac{a}{d} | y - y_0$. Άρα υπάρχει $n \in \mathbb{Z}$ με $y_0 - y = \frac{a}{d}n$, δηλαδή $y = y_0 - \frac{a}{d}n$.

Αν ο a δεν είναι μηδέν, τότε από την (3) παίρνουμε $x = x_0 + \frac{b}{d}n$. Η απόδειξη στην περίπτωση που ο b δεν είναι μηδέν είναι παρόμοια. ⊺

1.5.2 Παραδείγματα.

1) Η Διοφαντική εξίσωση $4x + 8y = 10$ δεν έχει λύσεις αφού $\mu\kappa\delta(4, 8) = 4$ που δεν διαιρεί τον 10.

2) Η Διοφαντική εξίσωση $21x + 14y = 70$ έχει άπειρες λύσεις αφού $\mu\kappa\delta(21, 14) = 7$ που διαιρεί το 70. Βρίσκουμε τις λύσεις ως εξής: Από τον Ευκλείδειο αλγόριθμο έχουμε $21 = 1 \cdot 14 + 7$, $14 = 2 \cdot 7 = 0$. Επομένως $7 = 1 \cdot 21 + (-1) \cdot 14$ και άρα $70 = 10 \cdot 21 + (-10) \cdot 14$. Έτσι μία λύση είναι η $x_0 = 10$, $y_0 = -10$. Επομένως κάθε λύση, σύμφωνα με το Θεώρημα 1.5.1, είναι της μορφής $x = 10 + 2n$ και $y = -10 - 3n$, όπου $n \in \mathbb{Z}$.

3) Θέλουμε να αγοράσουμε γραμματόσημα των 0.4 Ευρώ και 0.6 Ευρώ για μια επιστολή που κοστίζει 8 Ευρώ. Ποιος είναι ο ελάχιστος αριθμός γραμματοσήμων 0.4 Ευρώ που απαιτούνται;
Θα λύσουμε τη Διοφαντική εξίσωση $4x + 6y = 80$ και θα βρούμε τη λύση (x, y) όπου ο x είναι μη αρνητικός ακέραιος και ελάχιστος και $y \geq 0$. Αφού $\mu\kappa\delta(4, 6) = 2$ που διαιρεί το 80, υπάρχουν λύσεις. Από τον Ευκλείδειο Αλγόριθμο παίρνουμε $80 = (-40) \cdot 4 + 40 \cdot 6$ που σημαίνει ότι μία λύση είναι η $x_0 = -40$, $y_0 = 40$. Άρα κάθε λύση είναι της μορφής $x = -40 + 3n$, $y = 40 - 2n$. Επειδή $x \geq 0$ έχουμε $n \geq 14$. Άρα η ζητούμενη λύση προκύπτει για $n = 14$ και είναι η $x = 2$, $y = 12$.

Το προηγούμενο Θεώρημα μας βοηθά να μελετήσουμε ισοτιμίες.

1.5.3 Θεώρημα. *Έστω $a, b, m \in \mathbb{Z}$ με $m \neq 0$ και $d = \mu\kappa\delta(a, m)$. Για τις λύσεις της ισοτιμίας*

$$ax \equiv b \mod m$$

ισχύουν τα εξής:

1) αν $d \nmid b$, τότε δεν υπάρχουν λύσεις, και

2) αν $d|b$ τότε υπάρχουν ακριβώς d μη ισοδύναμες λύσεις modulo m.

Απόδειξη. Η ισοτιμία $ax \equiv b \mod m$ είναι ισοδύναμη με τη Διοφαντική εξίσωση $ax - my = b$. Οι λύσεις αυτής περιγράφονται από το Θεώρημα 1.5.1: αν $d \nmid b$ τότε δεν υπάρχουν λύσεις, ενώ αν $d|b$ τότε υπάρχουν άπειρες λύσεις που δίνονται από τις σχέσεις

$$x = x_0 + \frac{-m}{d}t, \quad y = y_0 - \frac{a}{d}t \quad (t \in \mathbb{Z}),$$

όπου (x_0, y_0) είναι μια συγκεκριμένη λύση της εξίσωσης.

Έστω $t_1, t_2 \in \mathbb{Z}$ και

$$x_1 = x_0 - \frac{m}{d}t_1 \quad \text{και} \quad x_2 = x_0 - \frac{m}{d}t_2,$$

Θα αποδείξουμε τώρα ότι

$$x_1 \equiv x_2 \mod m \Leftrightarrow t_1 \equiv t_2 \mod d.$$

Πράγματι, αν $x_1 \equiv x_2 \mod m$, τότε $\frac{m}{d}t_1 \equiv \frac{m}{d}t_2 \mod m$. Από την Πρόταση 1.3.7 προκύπτει ότι $t_1 \equiv t_2 \mod d$. Αντίστροφα, αν $t_1 \equiv t_2 \mod d$, τότε $\frac{m}{d}t_1 \equiv \frac{m}{d}t_2 \mod m$ και άρα $x_1 \equiv x_2 \mod m$.

Άρα αποδείξαμε ότι υπάρχουν ακριβώς d μη ισοδύναμες λύσεις modulo m. Μία επιλογή d μη ισοδυνάμων λύσεων modulo m δίνεται από τη σχέση

$$x = x_0 - \frac{m}{d}t, \tag{4}$$

για $t = 0, 1, \ldots, d-1$. ⊺

Σημειώσεις

1) Αν $c \in \mathbb{Z}$ είναι μια λύση της ισοτιμίας $ax \equiv b \mod m$ τότε κάθε $c' \in \mathbb{Z}$ με $c' \equiv c \mod m$ θα είναι λύση της ισοτιμίας λόγω της Πρότασης 1.3.4. Συνεπώς, από τώρα και στο εξής όταν λέμε ***λύση*** μιας ισοτιμίας $ax \equiv b \mod m$ εννοούμε μια ***κλάση υπολοίπων modulo m***, τέτοια ώστε κάθε στοιχείο x της κλάσης ικανοποιεί την ισοτιμία. Έτσι στη δεύτερη περίπτωση του προηγούμενου Θεωρήματος, θα λέμε ότι η ισοτιμία $ax \equiv b \mod m$ έχει ακριβώς d λύσεις.

2) Επειδή η ισοτιμία $ax \equiv b \mod m$ είναι ισοδύναμη με την εξίσωση $[a][x] = [b]$ στο $\mathbb{Z}_m$, βλέπουμε ότι μια πρωτοβάθμια εξίσωση στο $\mathbb{Z}_m$ μπορεί να μην έχει λύσεις, να έχει ακριβώς μια λύση ή να έχει περισσότερες λύσεις.

1.5.4 Παραδείγματα.

1) Θα προσδιορίσουμε τους $x \in \mathbb{Z}$ που έχουν την ιδιότητα $9x \equiv 12 \mod 15$. Έχουμε $d = \mu\kappa\delta(9, 15) = 3$ και $3|12$. Άρα υπάρχουν ακριβώς 3 κλάσεις υπολοίπων $\mod 15$ που είναι λύσεις. Για να βρούμε μια λύση της αντίστοιχης Διοφαντικής εξίσωσης $9x-15y = 12$ εφαρμόζουμε τον Ευκλείδειο αλγόριθμο

$$\begin{aligned} 15 &= 9 \cdot 1 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 3. \end{aligned}$$

Άρα $3 = 9-6\cdot 1 = 9-(15-9\cdot 1) = 9\cdot 2-15\cdot 1$ και πολλαπλασιάζοντας με 4 έχουμε $9 \cdot 8 - 15 \cdot 4 = 12$. Θέτουμε $(x_0, y_0) = (8, 4)$. Από την απόδειξη του Θεωρήματος 1.5.3, ισότητα (4), όλες οι λύσεις της αρχικής ισοτιμίας είναι

$$x \equiv 8 \mod 15, \quad x \equiv 3 \mod 15, \quad x \equiv 13 \mod 15.$$

2) Μπορούμε να λύσουμε την ισοτιμία $7x \equiv 22 \mod 10$ με την προηγούμενη μέθοδο ή εναλλακτικά να παρατηρήσουμε ότι αφού $\mu\kappa\delta(7, 10) = 1$, το 7 είναι αντιστρέψιμο modulo 10 (Πρόταση 1.4.5), έστω $7a \equiv 1 \mod 10$. Πολλαπλασιάζοντας την αρχική ισοτιμία με a παίρνουμε $x \equiv 22a \mod 10$. Με τον Ευκλείδειο αλγόριθμο (ή με όποιον άλλο τρόπο θέλουμε) βρίσκουμε το αντίστροφο του 7 modulo 10, $a \equiv 3 \mod 10$. Άρα $x \equiv 66 \equiv 6 \mod 10$ (δείτε και την Εφαρμογή μετά την Πρόταση 1.4.5).

Σημείωση Στο Παράδειγμα 1.5.4 1) μπορούμε να εργαστούμε και ως εξής. Η δοθείσα ισοτιμία είναι ισοδύναμη με την $3x \equiv 4 \mod 5$, που έχει ακριβώς μία λύση από το Θεώρημα 1.5.3, την $x \equiv 3 \mod 5$. Πώς σχετίζεται αυτή η λύση με τις τρεις λύσεις που βρήκαμε στο Παράδειγμα 1.5.4 1); Αν συμβολίσουμε την κλάση υπολοίπων $\mod m$ του a με $[a]_m$, τότε είναι εύκολο να δούμε ότι

$$[3]_5 = [3]_{15} \cup [8]_{15} \cup [13]_{15}.$$

Με άλλα λόγια βλέπουμε ότι έχουμε δύο περιγραφές του ιδίου συνόλου, δηλαδή του $\{x \in \mathbb{Z} | 9x \equiv 12 \mod 15\}$. Πιο γενικά, μπορεί να αποδειχθεί το εξής. Έστω d, m θετικοί ακέραιοι τέτοιοι ώστε $d|m$. Τότε για κάθε ακέραιο r έχουμε την ξένη ένωση

$$[r]_d = [r]_m \cup [r + d]_m \cup \cdots \cup \left[r + \left(\frac{m}{d} - 1\right) d\right]_m .$$

Η απόδειξη αφήνεται σαν άσκηση.

Συστήματα ισοτιμιών

Στη συνέχεια θα θεωρήσουμε συστήματα ισοτιμιών. Όταν λέμε λύση ενός συστήματος ισοτιμιών εννοούμε κάθε ακέραιο που ικανοποιεί όλες τις ισοτιμίες του συστήματος.

Αρχικά παρατηρούμε ότι είναι δυνατόν ένα σύστημα να μην έχει λύση αν και κάθε ισοτιμία του συστήματος έχει λύση. Ας θεωρήσουμε, για παράδειγμα, το σύστημα

$$\begin{aligned} x &\equiv 1 \mod 2 \\ x &\equiv 2 \mod 6. \end{aligned}$$

Αυτό δεν έχει λύση, γιατί από την πρώτη ισοτιμία παίρνουμε $2|x-1$ και από τη δεύτερη παίρνουμε $2|x-2$ και επομένως $2|1$.

Στην περίπτωση που υπάρχουν ακέραιοι x, x' που ικανοποιούν το σύστημα

$$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n \end{aligned}$$

παίρνουμε $x \equiv x' \mod m$ και $x \equiv x' \mod n$, δηλαδή $m|x-x'$ και $n|x-x'$, και επομένως $e|x-x'$, όπου $e = \epsilon\kappa\pi(m,n)$. Συνεπώς, αν υπάρχει λύση, αυτή είναι μοναδική $\mod e$. Στην ειδική περίπτωση που ισχύει $\mu\kappa\delta(m,n)=1$, τότε μπορούμε να δείξουμε ότι το προηγούμενο σύστημα έχει λύση (και είναι μοναδική $\mod e$, δηλαδή $\mod (mn)$). Σχετικό είναι το παρακάτω Θεώρημα.

1.5.5 Θεώρημα (*Κινεζικό Θεώρημα Υπολοίπων*). *Έστω $m_1, m_2, \ldots, m_r$ ανά δύο σχετικά πρώτοι θετικοί ακέραιοι. Τότε το σύστημα ισοτιμιών*

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ &\vdots \\ x &\equiv a_r \mod m_r \end{aligned}$$

έχει μοναδική λύση modulo $M = m_1 m_2 \ldots m_r$.

Απόδειξη. Ύπαρξη: Θέτουμε $M_k = \dfrac{M}{m_k}$ και παρατηρούμε ότι, λόγω της υπόθεσης, ισχύει $\mu\kappa\delta(M_k, m_k) = 1$. Επομένως το M_k είναι αντιστρέψιμο modulo m_k Έστω $M_k y_k \equiv 1 \mod m_k$. Θέτουμε

$$x = a_1 M_1 y_1 + \cdots + a_r M_r y_r \tag{5}$$

Επειδή για $i \neq k$ έχουμε $m_i | M_k$ η (5) δίνει $x \equiv a_k M_k y_k \mod m_k$, $k = 1, 2, \ldots, r$. Άρα $x \equiv a_k \mod m_k$, $k = 1, 2, \ldots, r$.

Μοναδικότητα: Έστω x και x' δύο λύσεις του αρχικού συστήματος. Τότε για κάθε $k = 1, 2, \ldots, r$ έχουμε $x \equiv x' \mod m_k$, δηλαδή $m_k | x - x'$. Από το Παράδειγμα 1.2.8 2) συμπεραίνουμε ότι $M | x - x'$, αφού οι m_k είναι ανά δύο σχετικά πρώτοι. ⊤

Τονίζουμε εδώ, ότι το σύνολο των ακεραίων που είναι λύσεις του συστήματος του προηγουμένου Θεωρήματος είναι η τομή των κλάσεων $[a_1]_{m_1}, \ldots, [a_r]_{m_r}$.

1.5.6 Παραδείγματα.

1) Για να λύσουμε το σύστημα

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 2 \mod 5 \\ x &\equiv 3 \mod 7 \end{aligned}$$

θέτουμε, σύμφωνα με την απόδειξη του Θεωρήματος 1.5.5, $M = 3 \cdot 5 \cdot 7 = 105$, $M_1 = \dfrac{105}{3} = 35$, $M_2 = \dfrac{105}{5} = 21$ και $M_3 = \dfrac{105}{7} = 15$. Για να βρούμε το y_1 λύνουμε την ισοτιμία $35y_1 \equiv 1 \mod 3$, δηλαδή την $2y_1 \equiv 1 \mod 3$. Έχουμε $y_1 \equiv 2 \mod 3$. Βρίσκουμε το y_2 από την $21y_2 \equiv 1 \mod 5$. Έχουμε $y_2 \equiv 1 \mod 5$. Βρίσκουμε το y_3 από την $15y_3 \equiv 1 \mod 7$. Έχουμε $y_3 \equiv 1 \mod 7$. Τελικά

$$x \equiv 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \mod 105,$$

δηλαδή $x \equiv 157 \equiv 52 \mod 105$.

2) Μπορούμε συχνά να λύσουμε συστήματα ισοτιμιών και με διαδοχικές αντικαταστάσεις. (Για τη μέθοδο αυτή δεν χρειάζονται τα moduli m_k να είναι ανά δύο σχετικά πρώτοι, αλλά στην περίπτωση αυτή δεν γνωρίζουμε εκ των προτέρων αν υπάρχει λύση). Για παράδειγμα έστω

$$\begin{aligned} x &\equiv 1 \mod 5 \\ x &\equiv 2 \mod 6 \\ x &\equiv 3 \mod 7 \end{aligned}$$

Γνωρίζουμε από το Κινεζικό Θεώρημα Υπολοίπων ότι το σύστημα έχει μοναδική λύση $\mod 210$ την οποία μπορούμε να βρούμε ως εξής. Από την πρώτη ισοτιμία έχουμε $x = 5t + 1$, $t \in \mathbb{Z}$. Αντικαθιστώντας στη δεύτερη έχουμε $5t \equiv 1 \mod 6$, την οποία λύνουμε για να βρούμε $t \equiv 5 \mod 6$. Άρα $t = 6u + 5$, $u \in \mathbb{Z}$. Συνεπώς $x = 5(6u + 5) + 1 = 30u + 26$.

Αντικαθιστώντας στην τρίτη ισοτιμία παίρνουμε $30u \equiv 5 \mod 7$. Η λύση είναι $u \equiv 6 \mod 7$. Άρα $u = 7v+6$, $v \in \mathbb{Z}$. Τελικά $x = 30(7v+6)+26 = 210v + 206$.
Συνεπώς $x \equiv 206 \mod 210$.

3) Με τη βοήθεια του Κινεζικού Θεωρήματος Υπολοίπων μπορούμε μερικές φορές να λύσουμε ισοτιμίες πιο πολύπλοκες από αυτές που μελετήσαμε στο Θεώρημα 1.5.3. Για παράδειγμα, ας θεωρήσουμε την $x^2 \equiv 1 \mod 77$. Επειδή $x^2 - 1 = (x+1)(x-1)$ και $77 = 7 \cdot 11$, εύκολα επαληθεύουμε ότι η εν λόγω ισοτιμία ισοδυναμεί με τα εξής 4 συστήματα ισοτιμιών

α) $x + 1 \equiv 0 \mod 77$

β) $x - 1 \equiv 0 \mod 77$

γ) $x + 1 \equiv 0 \mod 7$
$x - 1 \equiv 0 \mod 11$

δ) $x + 1 \equiv 0 \mod 11$
$x - 1 \equiv 0 \mod 7$.

Οι α) και β) λύνονται άμεσα ενώ στα γ) και δ) εφαρμόζουμε το Κινεζικό Θεώρημα Υπολοίπων. Βλέπουμε ότι οι λύσεις είναι: α) $x \equiv 76 \mod 77$, β) $x \equiv 1 \mod 77$, γ) $x \equiv 34 \mod 77$, δ) $x \equiv 43 \mod 77$.

4) Ας θεωρήσουμε το σύστημα

$$\begin{aligned} 2x &\equiv 1 \mod 3 \\ 5x &\equiv 2 \mod 7. \end{aligned}$$

Παρατηρούμε ότι σε αυτό δεν μπορούμε να εφαρμόσουμε άμεσα το Κινεζικό Θεώρημα Υπολοίπων. Επειδή το 2 είναι αντιστρέψιμο modulo 3 (και ένα αντίστροφό του είναι το 2), η πρώτη ισοτιμία του συστήματος είναι ισοδύναμη με την $x \equiv 2 \mod 3$. Με παρόμοιο τρόπο, βλέπουμε ότι η δεύτερη ισοτιμία είναι ισοδύναμη με την $x \equiv 6 \mod 7$. Συνεπώς το αρχικό σύστημα είναι ισοδύναμο με το

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 6 \mod 7. \end{aligned}$$

Το σύστημα αυτό μπορεί να λυθεί με το Κινεζικό Θεώρημα Υπολοίπων.

Ασκήσεις 1.5

1. Λύστε τις παρακάτω Διοφαντικές εξισώσεις.

   i) $5x + 8y = 99$

   ii) $6x + 4y = 100$

   iii) $6x + 4y = 99$

   iv) $110x + 150y = 30$

   v) $14x + 49y = 42$

2. Πόσα ζεύγη $(x, y) \in \mathbb{N} \times \mathbb{N}$ υπάρχουν τέτοια ώστε $2x + 3y = 70$;

3. Κατά πόσους διαφορετικούς τρόπους μπορεί να σχηματιστεί ένα ποσό 510 Ευρώ από χαρτονομίσματα των 20 και 50 Ευρώ;

4. Έστω $a, b, c \in \mathbb{Z} - \{0\}$ και $d \in \mathbb{Z}$.

   i) Αποδείξτε ότι η Διοφαντική εξίσωση $ax + by + cz = d$ έχει λύση αν και μόνο αν $\mu\kappa\delta(a, b, c)|d$.

   ii) Αποδείξτε ότι αν η Διοφαντική εξίσωση $ax + by + cz = d$ έχει μία λύση, τότε έχει άπειρες.

5. Λύστε τις Διοφαντικές εξισώσεις

   i) $2x + 3y + 4z = 79$
   Υπόδειξη: Θέστε $w = 3y + 4z$ και λύστε πρώτα την $2x + w = 79$.

   ii) $10x + 6y + 15z = 40$

6. Να βρεθούν οι ακέραιοι $x, y, z \in \mathbb{Z}$ που είναι λύσεις του συστήματος

$$x + y + z = 100$$
$$x + 8y + 50z = 156.$$

7. Είναι δυνατόν με συνολικά 50 νομίσματα των 2, 10 και 50 Ευρώ να σχηματιστεί ποσό 760 Ευρώ;

8. Ποιες από τις παρακάτω ισοτιμίες έχουν λύσεις; Βρείτε τις λύσεις (όπου υπάρχουν)

   i) $2x \equiv 6 \mod 12$

   ii) $101x \equiv 7 \mod 102$

iii) $14x \equiv 3 \mod 21$

iv) $9x \equiv 5 \mod 35$.

9. Ποια από τα παρακάτω συστήματα έχουν λύσεις; Βρείτε τις λύσεις (όπου υπάρχουν).

   i) $x \equiv 3 \mod 5$
   $x \equiv 5 \mod 6$
   $x \equiv 1 \mod 7$

   ii) $2x \equiv 1 \mod 7$
   $x \equiv 4 \mod 8$

   iii) $6x \equiv 2 \mod 9$
   $5x \equiv 1 \mod 10$

   iv) $4x \equiv 2 \mod 10$
   $3x \equiv 4 \mod 11$

10. Βρείτε τον ελάχιστο θετικό ακέραιο που όταν διαιρεθεί με τους 5, 7 και 9 αφήνει υπόλοιπα 1, 2, 3 αντίστοιχα.

11. Λύστε το σύστημα

$$x \equiv 4 \mod 6$$
$$x \equiv 13 \mod 15$$

12. Ένας δορυφόρος που κινείται γύρω από την Γη έχει περίοδο t που είναι ακέραιο πολλαπλάσιο της μιας ώρας. Γνωρίζουμε ότι

   i) $t \leq 24$, και

   ii) ο δορυφόρος συμπληρώνει 11 περιστροφές σε χρονική περίοδο που αρχίζει όταν ένα 24ωρο ρολόι δείχνει 0 και λήγει (κάποιες ημέρες αργότερα) όταν το ρολόι δείχνει 17.
   Να βρεθεί ο t.

13. Βρείτε όλους τους $x \in \mathbb{Z}$ τέτοιους ώστε $x^2 \equiv 1 \mod 91$.

14. Έστω $m \in \mathbb{N}$ περιττός και $m = p_1^{m_1} \dots p_r^{m_r}$ η ανάλυσή του σε γινόμενο πρώτων με $p_i \neq p_j$ αν $i \neq j$. Αποδείξτε ότι η ισοτιμία $x^2 \equiv 1 \mod m$ έχει ακριβώς 2^r λύσεις $\mod m$.

15. Βρείτε όλους τους $x, y \in \mathbb{Z}$ ώστε το σύστημα

$$\begin{aligned} 2x + 4y &\equiv 3 \mod 11 \\ 3x + 2y &\equiv 5 \mod 11 \end{aligned}$$

να έχει λύση.

16. Θεωρούμε το σύστημα

$$\begin{aligned} ax + by &\equiv e \mod m \\ cx + dy &\equiv f \mod m \end{aligned}$$

και θέτουμε $\Delta = ad - bc$. Αποδείξτε ότι αν $\mu\kappa\delta(\Delta, m) = 1$, τότε υπάρχει μοναδική λύση $\mod m$ που δίνεται από

$$\begin{aligned} x &= \bar{\Delta}(de - bf) \mod m \\ y &= \bar{\Delta}(af - ce) \mod m, \end{aligned}$$

όπου $\bar{\Delta}$ είναι το αντίστροφο του Δ modulo m. (Συγκρίνατε με τον κανόνα του Cramer για τη λύση 2×2 γραμμικών συστημάτων επί του $\mathbb{R}$).

17. (Ένα αρχαίο Ινδικό πρόβλημα). Αν αφαιρεθούν τα αυγά από ένα καλάθι ανά 2, 3, 4, 5 και 6 τότε παραμένουν αντίστοιχα 1, 2, 3, 4, 5 αυγά. Όταν όμως αφαιρεθούν τα αυγά ανά 7 στο τέλος το καλάθι είναι άδειο. Ποιος είναι ο ελάχιστος αριθμός αυγών που θα μπορούσε να περιέχει το καλάθι;

18. Εξετάστε αν οι παρακάτω προτάσεις που αφορούν το $\mathbb{Z}_m$ είναι αληθείς ή ψευδείς

    i) Κάθε εξίσωση της μορφής $ax - b = 0$ $(a, b \in \mathbb{Z}_m, a \neq [0])$ έχει λύση στο $\mathbb{Z}_m$.

    ii) Κάθε εξίσωση της μορφής $ax - b = 0$ $(a, b \in \mathbb{Z}_m)$ έχει το πολύ μια λύση στο $\mathbb{Z}_m$.

    iii) Αν $x^2 = [1]$ στο $\mathbb{Z}_m$, τότε $x = [1]$ ή $x = [-1]$.

    iv) Αν $x^2 = [0]$ στο $\mathbb{Z}_m$, τότε $x = [0]$.

19. Έστω m ένας θετικός ακέραιος. Αποδείξτε ότι υπάρχουν m το πλήθος διαδοχικοί θετικοί ακέραιοι καθένας από τους οποίους διαιρείται με ένα τουλάχιστον τετράγωνο ακεραίου μεγαλυτέρου του 1.

20. Αποδείξτε ότι δεν υπάρχει ακέραιος αριθμός τέτοιος ώστε τα δύο τελευταία ψηφία του τετραγώνου του (στη συνήθη δεκαδική γραφή) να είναι 35.

21. Εξετάστε αν υπάρχει $b \in \mathbb{Z}$, $0 \leq b \leq 60$ τέτοιος ώστε το σύστημα

$$\begin{aligned} 12x &\equiv b \mod 30 \\ 22x &\equiv b \mod 11 \end{aligned}$$

να έχει λύση.

22. Βρείτε όλους τους ακεραίους x τέτοιους ώστε $x^3 + 2x^2 - x - 5 \equiv 0 \mod 105$.
Υπόδειξη: Έστω $f(x) = x^3 + 2x^2 - x - 5$. Με δοκιμές λύστε κάθε μία από τις ισοτιμές $f(x) \equiv 0 \mod 3$, $f(x) \equiv 0 \mod 5$, $f(x) \equiv 0 \mod 7$. Συνεχίστε εφαρμόζοντας το Κινεζικό Θεώρημα.

1.6 Η Συνάρτηση του Euler

Η συνάρτηση του Euler
Θα συμβολίζουμε με $\varphi(m)$ το πλήθος των στοιχείων του συνόλου $U(\mathbb{Z}_m)$ των αντιστρέψιμων στοιχείων του $\mathbb{Z}_m$. Τότε, ορίζεται μια συνάρτηση $\phi : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$, που ονομάζεται ***συνάρτηση του Euler***. Από την Πρόταση 1.4.5 έπεται ότι $\varphi(m)$ είναι το πλήθος των ακεραίων a, οι οποίοι είναι τέτοιοι ώστε

$$1 \leq a \leq m \quad \text{και} \quad \mu\kappa\delta(a, m) = 1.$$

Για παράδειγμα έχουμε $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$. Είναι φανερό ότι χρησιμοποιώντας τον ορισμό δεν είναι εύκολο να υπολογιστούν οι τιμές $\varphi(m)$ για μεγάλα m. Η παρακάτω Πρόταση παρέχει έναν διαφορετικό τρόπο υπολογισμού του ακεραίου $\varphi(m)$.

1.6.1 Πρόταση.

1) Για κάθε πρώτο p ισχύει $\varphi(p^i) = p^i - p^{i-1}$.

2) Αν $\mu\kappa\delta(m, n) = 1$, τότε $\varphi(mn) = \varphi(m)\varphi(n)$.

3) Αν η ανάλυση του n σε γινόμενο πρώτων είναι $n = p_1^{n_1} \dots p_s^{n_s}$, όπου οι p_i είναι διακεκριμένοι πρώτοι αριθμοί, τότε

$$\begin{aligned}\varphi(n) &= (p_1^{n_1} - p_1^{n_1-1})(p_2^{n_2} - p_2^{n_2-1}) \dots (p_s^{n_s} - p_s^{n_s-1}) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_s}\right).\end{aligned}$$

Απόδειξη. Υπενθυμίζουμε από την Παράγραφο 1.4 ότι

$$U(\mathbb{Z}_m) = \{[\alpha] \in \mathbb{Z}_m | \mu\kappa\delta(\alpha, m) = 1\}$$

1) Οι θετικοί ακέραιοι που είναι μικρότεροι του p^i και δεν είναι σχετικά πρώτοι με αυτόν είναι τα πολλαπλάσια του p της μορφής ap, όπου $1 \leq a \leq p^{i-1}$. Το πλήθος τους είναι p^{i-1}. Συνεπώς το πλήθος των θετικών ακεραίων που είναι μικρότεροι του p^i και σχετικά πρώτοι προς αυτόν είναι $p^i - p^{i-1}$.

2) Αρκεί να δείξουμε ότι υπάρχει 1-1 και επί απεικόνιση

$$\psi : U(\mathbb{Z}_{mn}) \to U(\mathbb{Z}_m) \times U(\mathbb{Z}_n).$$

Ορίζουμε $\psi([a]_{mn}) = ([a]_m, [a]_n)$, όπου με $[a]_k \in \mathbb{Z}_k$ παριστάνουμε την κλάση υπολοίπων modulo k του a. Η αντιστοιχία ψ είναι μια απεικόνιση, γιατί αν $[a]_{mn} = [b]_{mn}$, τότε $mn|a-b$, οπότε $m|a-b$ και $n|a-b$, δηλαδή $[a]_m = [b]_m$ και

$[a]_n = [b]_n$. Επιπλέον, αν $[a]_{mn} \in U(\mathbb{Z}_{mn})$ τότε $([a]_m, [a]_n) \in U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$, γιατί αν $\mu\kappa\delta(mn, a) = 1$, τότε $\mu\kappa\delta(m, a) = \mu\kappa\delta(n, a) = 1$. Η ψ είναι 1-1, γιατί αν $\psi(a) = \psi(b)$, τότε $[a]_m = [b]_m$ και $[a]_n = [b]_n$, οπότε $m|a-b$ και $n|a-b$. Επειδή όμως $\mu\kappa\delta(m, n) = 1$, έχουμε $mn|a-b$, δηλαδή $[a]_{mn} = [b]_{mn}$. Τέλος, για να δούμε ότι η ψ είναι επί, παρατηρούμε ότι δοθέντος του $([a]_m, [b]_n) \in U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$, από το Κινεζικό Θεώρημα Υπολοίπων υπάρχει ακέραιος x με $x \equiv a \mod m$ και $x \equiv b \mod n$. Για το x αυτό έχουμε $\mu\kappa\delta(x, m) = \mu\kappa\delta(a, m) = 1$ και $\mu\kappa\delta(x, n) = \mu\kappa\delta(b, n) = 1$. Συνεπώς, $\mu\kappa\delta(x, mn) = 1$ και άρα $[x]_{mn} \in U(\mathbb{Z}_{mn})$. Επίσης, $\psi([x]_{mn}) = ([x]_m, [x]_n) = ([a]_m, [b]_n)$.

3) Η σχέση αυτή προκύπτει από τις 1) και 2):

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{n_1} \dots p_s^{n_s}) = \\
&= \varphi(p_1^{n_1}) \dots \varphi(p_s^{n_s}) = \\
&= (p_1^{n_1} - p_1^{n_1-1}) \dots (p_s^{n_s} - p_s^{n_s-1}) = \\
&= p_1^{n_1} \dots p_s^{n_s} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_s}\right) = \\
&= n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_s}\right). \qquad \mathsf{T}
\end{aligned}$$

Η σχέση 3) είναι χρήσιμη για υπολογισμούς. Για παράδειγμα, έχουμε $\varphi(1000) = \varphi(2^3 5^3) = \varphi(2^3)\varphi(5^3) = (8-4)(125-25) = 400$.

Σημειώνουμε ότι η σχέση 2) στο προηγούμενο Θεώρημα μπορεί να αποδειχθεί χωρίς τη χρήση του Κινεζικού Θεωρήματος Υπολοίπων. Όμως η απόδειξη που δώσαμε εδώ παρουσιάζει ενδιαφέρον γιατί χρησιμοποιεί μια διασύνδεση μεταξύ των $U(\mathbb{Z}_{mn}), U(\mathbb{Z}_m), U(\mathbb{Z}_n)$ που θα μελετηθεί γενικότερα στην Ενότητα 2.

Θεώρημα του Euler

Από το Μικρό Θεώρημα του Fermat γνωρίζουμε ότι $a^{p-1} \equiv 1 \mod p$, όταν ο p είναι ένας πρώτος αριθμός με $\mu\kappa\delta(a, p) = 1$. Θα αποδείξουμε εδώ μια γενίκευση που λέει ότι $a^{\varphi(m)} \equiv 1 \mod m$, όπου $a, m \in \mathbb{Z}$, $m > 0$ και $\mu\kappa\delta(a, m) = 1$.

Έστω $[a], [b] \in U(\mathbb{Z}_m)$. Επειδή $\mu\kappa\delta(a, m) = \mu\kappa\delta(b, m) = 1$ έχουμε $\mu\kappa\delta(ab, m) = 1$. Πράγματι, κάθε πρώτος αριθμός που είναι κοινός διαιρέτης των ab και m θα διαιρεί έναν τουλάχιστον από τα a, b (Λήμμα 1.2.5) και κατά συνέπεια θα διαιρεί έναν τουλάχιστον από τους $\mu\kappa\delta(a, m), \mu\kappa\delta(b, m)$. Αυτό είναι άτοπο. Συνεπώς αποδείξαμε ότι

$$[a], [b] \in U(\mathbb{Z}_m) \Rightarrow [ab] \in U(\mathbb{Z}_m). \tag{1}$$

Έστω

$$U(\mathbb{Z}_m) = \{[a_1], \ldots, [a_k]\}, \quad k = \varphi(m). \tag{2}$$

Έστω $[a] \in U(\mathbb{Z}_m)$. Από το (1) έχουμε ότι $[aa_i] \in U(\mathbb{Z}_m)$, $i = 1, \ldots, k$. Επιπλέον τα στοιχεία αυτά είναι ανά δύο διάφορα, γιατί αν $[aa_i] = [aa_j]$, τότε $m|a(a_i - a_j)$, οπότε $m|a_i - a_j$, αφού $\mu\kappa\delta(a, m) = 1$, και άρα $[a_i] = [a_j]$. Επειδή τώρα το πλήθος των $[aa_i]$ είναι k, που είναι ο πληθάριθμος του $U(\mathbb{Z}_m)$, και επειδή το k είναι πεπερασμένο, παίρνουμε

$$U(\mathbb{Z}_m) = \{[aa_1], \ldots, [aa_k]\}. \tag{3}$$

Σχηματίζουμε το γινόμενο όλων των στοιχείων του $U(\mathbb{Z}_m)$. Από τις (3) και (2) παίρνουμε

$$\begin{aligned} &[aa_1] \ldots [aa_k] = [a_1] \ldots [a_k] \Rightarrow \\ &[a^k][a_1 \ldots a_k] = [a_1 \ldots a_k]. \end{aligned} \tag{4}$$

Από τη σχέση (1) έχουμε $[a_1 \ldots a_k] \in U(\mathbb{Z}_m)$. Πολλαπλασιάζοντας την (4) με το αντίστροφο του $[a_1 \ldots a_k]$ παίρνουμε

$$[a^k] = [1],$$

δηλαδή

$$a^{\varphi(m)} \equiv 1 \mod m.$$

Έχουμε αποδείξει το ακόλουθο αποτέλεσμα.

1.6.2 Θεώρημα (*Euler*). [1] *Έστω $a, m \in \mathbb{Z}$ και $m > 0$. Αν $\mu\kappa\delta(a, m) = 1$, τότε*

$$a^{\varphi(m)} \equiv 1 \mod m.$$

Από το Θεώρημα αυτό βλέπουμε ότι αν $\mu\kappa\delta(a, m) = 1$, τότε το αντίστροφο του $[a] \in \mathbb{Z}_m$ είναι το $[a^{\varphi(m)-1}]$.

Στην ειδική περίπτωση του Θεωρήματος του Euler που ο $m = p$ είναι πρώτος, έχουμε $\varphi(m) = p - 1$ και επιπλέον ισχύει $\mu\kappa\delta(a, p) = 1$ αν και μόνο αν ο p δεν διαιρεί τον a. Άρα προκύπτει μια άλλη απόδειξη για το Μικρό Θεώρημα του Fermat.

[1] Ο Euler (1707-1783) ξεκίνησε στις σπουδές του στο Πανεπιστήμιο του Basel της Ελβετίας όταν ήταν μόλις 13 χρονών και τρία χρόνια αργότερα απέκτησε master's στη Φιλοσοφία. Εργάστηκε δε σε πολλούς τομείς των Μαθηματικών αλλά και άλλων κλάδων, όπως είναι για παράδειγμα η Ναυπηγική, Υδροδυναμική και Μηχανική. Το επιστημονικό έργο του είναι τεράστιο και ο Euler θεωρείται ο πολυγραφότατος Μαθηματικός όλων των εποχών.

Το Θεώρημα του Euler μας επιτρέπει συχνά να υπολογίζουμε υπόλοιπα διαιρέσεων μεγάλων αριθμών. Για παράδειγμα, ας βρούμε το υπόλοιπο της διαίρεσης του 365^{2002} με το 24. Ισχύει $365 = 15 \cdot 24 + 5$ και άρα $365 \equiv 5 \mod 24$. Επίσης $\varphi(24) = \varphi(2^3 3) = (2^3 - 2^2)(3-1) = 8$ (Πρόταση 1.6.1). Καθώς $\mu\kappa\delta(5, 24) = 1$, από το Θεώρημα του Euler έχουμε $5^8 \equiv 1 \mod 24$. Επειδή $2002 = 250 \cdot 8 + 2$ έχουμε

$$365^{2002} = (365^8)^{250} \cdot 365^2 \equiv (5^8)^{250} \cdot 5^2 \equiv 1^{250} \cdot 5^2 \equiv 1 \mod 24.$$

1.6.3 Παραδείγματα.

1. Για κάθε ακέραιο a με $\mu\kappa\delta(a, 72) = 1$ ισχύει $a^{12} \equiv 1 \mod 72$.
   Αν εφαρμόσουμε άμεσα το Θεώρημα του Euler, λαμβάνουμε $a^{\varphi(72)} = a^{\varphi(8)\varphi(9)} = a^{24} \equiv 1 \mod 72$ που δεν είναι η ζητούμενη ισοτιμία. Για αυτό εργαζόμαστε κάπως διαφορετικά: Αρκεί να δείξουμε ότι $a^{12} \equiv 1 \mod 8$ και $a^{12} \equiv 1 \mod 9$, γιατί οι ακέραιοι 8,9 είναι σχετικά πρώτοι. Επειδή $\mu\kappa\delta(a, 72) = 1$ έχουμε ότι $\mu\kappa\delta(a, 8) = 1$ και άρα από το Θεώρημα του Euler ισχύει $a^{\varphi(8)} = a^4 \equiv 1 \mod 8$. Επομένως έχουμε $a^{12} = (a^4)^3 \equiv 1 \mod 8$. Όμοια αποδεικνύεται και η ισοτιμία $a^{12} \equiv 1 \mod 9$.

2. Έστω $a, m \in \mathbb{Z}$ με $m > 0$ και $\mu\kappa\delta(a, m) = 1$. Έστω k ο ελάχιστος θετικός ακέραιος τέτοιος ώστε $a^k \equiv 1 \mod m$ (τέτοιος k υπάρχει από το Θεώρημα του Euler και το Αξίωμα Ελαχίστου). Τότε $k | \varphi(m)$.
   Πράγματι, από τον Αλγόριθμο Διαίρεσης έχουμε $\varphi(m) = qk + r$, $0 \leq r < k$. Συνεπώς $a^{\varphi(m)} = (a^k)^q a^r$. Από το Θεώρημα του Euler και τον ορισμό του k παίρνουμε $1 \equiv a^r \mod m$. Λόγω του ελαχίστου του k παίρνουμε $r = 0$. Άρα $k | \varphi(m)$.

Η μέθοδος κρυπτογράφησης RSA

Η Κρυπτογραφία ασχολείται με την εύρεση και υλοποίηση μεθόδων αποστολής και λήψης μυστικών μηνυμάτων. Θα περιγράψουμε εδώ το σύστημα κρυπτογράφησης RSA.[2] Αυτό είναι από τα πιο διαδεδομένα συστήματα καθώς χρησιμοποιείται από κράτη και οργανισμούς για διπλωματικούς, στρατιωτικούς και οικονομικούς σκοπούς, όπως και από πολίτες σε καθημερινές οικονομικές συναλλαγές (π.χ. αγορές με πιστωτική κάρτα).

Το RSA συνίσταται στα επόμενα βήματα.

Βήμα 1: Ο προτιθέμενος παραλήπτης του μηνύματος επιλέγει δύο διακεκριμένους μεγάλους πρώτους αριθμούς (πχ της τάξης του 10^{100}). Στη συνέχεια θέτει $n = pq$ και επιλέγει έναν θετικό ακέραιο e σχετικά πρώτο με τον

[2] Το σύστημα RSA επινοήθηκε από τους Rivest, Shamir και Adleman το 1978.

$\varphi(n) = (p-1)(q-1)$. Το ζεύγος (e, n) γνωστοποιείται στον προτιθέμενο αποστολέα (κατά φανερό τρόπο).

Βήμα 2 (κρυπτογράφηση): Ο αποστολέας μετατρέπει το μήνυμα που θέλει να στείλει σε μια σειρά από ψηφία σύμφωνα με την 1-1 αντιστοιχία $A \mapsto 01, B \mapsto 02, \ldots, \Omega \mapsto 24$. Στη συνέχεια ομαδοποιεί τα ψηφία σε τετραψήφιους αριθμούς. Για καθέναν, X, από τους τετραψήφιους αυτούς αριθμούς υπολογίζει

$$Y(X) \equiv X^e \mod n, \quad 0 < Y(X) < n.$$

Δηλαδή, $Y(X)$ είναι το υπόλοιπο της διαίρεσης του X^e με τον n. Οι αριθμοί $Y(X)$ στέλνονται στον παραλήπτη (κατά φανερό τρόπο).

Βήμα 3 (αποκρυπτογράφηση): Καθώς από την υπόθεση είναι $\mu\kappa\delta(e, \varphi(n)) = 1$, η κλάση $[e]$ στο $\mathbb{Z}_{\varphi(n)}$ είναι αντιστρέψιμη (Πρόταση 1.4.5). Άρα υπάρχει $d \in \mathbb{N}$ με $de = k\varphi(n)+1$, για κάποιο $k \in \mathbb{Z}$. Ο παραλήπτης υπολογίζει ένα τέτοιο d (πχ με τον Ευκλείδειο Αλγόριθμο). Στη συνέχεια υψώνει κάθε $Y(X)$ στη δύναμη d και εφαρμόζει το Θεώρημα του Euler

$$Y(X)^d \equiv X^{ed} = X^{k\varphi(n)+1} = (X^{\varphi(n)})^k X \equiv X \mod n.$$

(Παρατηρούμε ότι η υπόθεση του Θεωρήματος του Euler, $\mu\kappa\delta(X, n) = 1$, ισχύει εδώ γιατί τα p, q είναι τουλάχιστον πενταψήφιοι αριθμοί ενώ οι X είναι τετραψήφιοι). Έτσι επανακτώνται οι αριθμοί X, δηλαδή το αρχικό μη κρυπτογραφημένο μήνυμα.

Για παράδειγμα, έστω $p = 43$ και $q = 59$. (Στην πράξη θα επιλέγαμε μεγάλους αριθμούς). Τότε $n = pq = 2537$ και $\varphi(n) = (p-1)(q-1) = 2436$. Έστω $e = 13$ οπότε $\mu\kappa\delta(13, 2436) = 1$. Ας υποθέσουμε ότι θέλουμε να στείλουμε το παρακάτω μήνυμα (χωρίς την τελεία)

ΤΑ ΜΑΘΗΜΑΤΙΚΑ ΕΙΝΑΙ ΧΡΗΣΙΜΑ.

Μετατρέπουμε το μήνυμα σε μια σειρά από ψηφία και ομαδοποιούμε σε τετραψήφιους αριθμούς λαμβάνοντας

1901 1201 0807 1201 1909 1001
0509 1301 1922 1707 1809 1201

σύμφωνα με το πρώτο τμήμα του Βήματος 2. (Αν στην τελευταία ομαδοποίηση είχαμε 2 ψηφία, θα προσθέταμε το "ανύπαρκτο γράμμα" 25 δύο φορές). Υπολογίζοντας τα $Y(X)$ βρίσκουμε[3]

0445 2224 1123 2224 0572 0304
2315 2326 2256 0155 2334 2224

[3]Οι συγκεκριμένοι υπολογισμοί έγιναν με το πρόγραμμα GAP

που είναι το κρυπτογραφημένο μήνυμα που στέλνουμε στον παραλήπτη.

Ο παραλήπτης υπολογίζει με τη βοήθεια του Ευκλείδειου αλγόριθμου ότι στο $\mathbb{Z}_{2436}$ το αντίστροφο του [13] είναι το [937] (βλ Εφαρμογή 1.4.6). Στη συνέχεια υπολογίζει τους X σύμφωνα με το Βήμα 3,

$$X \equiv Y(X)^{937} \mod 2537, \quad 0 \leq X < 2537,$$

εφόσον $\mu\kappa\delta(X, 2537) = 1$. (Ελέγχουμε ότι στο συγκεκριμένο παράδειγμα ικανοποιείται αυτή η συνθήκη για κάθε X. Αν είχαμε επιλέξει μεγάλα p, q τότε αυτός ο έλεγχος δεν θα ήταν απαραίτητος).

Παρατηρήσεις

1. Η ασφάλεια της μεθόδου RSA οφείλεται στο γεγονός ότι μέχρι σήμερα και παρά την ταχύτητα των υπολογιστών είναι εξαιρετικά χρονοβόρο - και άρα πρακτικά αδύνατο - να παραγοντοποιηθούν μεγάλοι αριθμοί. Αν η παραγοντοποίηση του n ήταν γνωστή (σε έναν υποκλοπέα του μηνύματος) τότε θα ήταν γνωστή η τιμή $\varphi(n)$ λόγω της Πρότασης 1.6.1. Συνεπώς θα μπορούσε να υπολογιστεί ο ακέραιος d και στη συνέχεια να γίνει η αποκρυπτογράφηση. Μέχρι σήμερα, είναι ανοικτό ερώτημα αν υπάρχει τρόπος αποκρυπτογράφησης μηνυμάτων που έχουν κρυπτογραφηθεί με το RSA, χωρίς να χρησιμοποιείται η παραγοντοποίηση του n.

2. Η εύρεση μεγάλων πρώτων αριθμών p, q δεν απαιτεί παρά ελάχιστα λεπτά σε υπολογιστές. Οι υπολογισμοί στα Βήματα 2 και 3 του RSA απαιτούν λίγα δευτερόλεπτα σε υπολογιστές όταν οι αριθμοί n, e, d έχουν το πολύ 200 ψηφία.

3. Ένας τρόπος επιλογής του e είναι η εύρεση ένος πρώτου μεγαλύτερου των p, q αφού τότε $\mu\kappa\delta(e, (p-1)(q-1)) = 1$. Πάντως, όπως και να επιλεγεί ο e θα πρέπει να ικανοποιεί την ανισότητα $101^e > n$ (ο αριθμός 101=0101 αντιστοιχεί στα γράμματα AA). Αν είχαμε $2424^e < n$ (ο αριθμός 2424 αντιστοιχεί στα γράμματα $\Omega\Omega$), τότε το κρυπτογραφημένο μήνυμα θα μπορούσε να αποκρυπτογραφηθεί απλά λαμβάνοντας ρίζες e-τάξης των $Y(X)$. Με άλλα λόγια, το e πρέπει να είναι αρκετά μεγάλο ώστε στο Βήμα 2 να συμβαίνει αναγωγή modulo n.

4. Η ομαδοποίηση στο Βήμα 2 θα μπορούσε να γίνει και σε εξάδες, οκτάδες κλπ.

Ασκήσεις 1.6

1. Βρείτε το υπόλοιπο της διαίρεσης του 5^{1000} με το 14.

2. Ποιά είναι τα τελευταία 2 ψηφία του 7^{100} στο δεκαδικό σύστημα;

3. Ποιά ένδειξη θα δείχνει ένα 24ωρο ρολόι 7^{19} ώρες μετά τις 1:00;

4. Έστω $a, b \in \mathbb{Z}$ σχετικά πρώτοι ακέραιοι. Αποδείξτε ότι $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \mod ab$.

5. Αποδείξτε ότι $a^7 \equiv a \mod 63$ αν $\mu\kappa\delta(a, 3) = 1$.

6. Έστω a, m θετικοί ακέραιοι με $\mu\kappa\delta(a, m) = \mu\kappa\delta(a-1, m) = 1$. Αποδείξτε ότι $1 + a + a^2 + \cdots + a^{\varphi(m)-1} \equiv 0 \mod m$.

7. i) Να βρεθεί ο ελάχιστος θετικός ακέραιος k ώστε $2^k \equiv 1 \mod 7$.

   ii) Έστω m ένας θετικός ακέραιος, $a \in \mathbb{Z}$, με $\mu\kappa\delta(a, m) = 1$, και k ο ελάχιστος θετικός ακέραιος ώστε $a^k \equiv 1 \mod m$. Αν $k > \varphi(m)/2$, αποδείξτε ότι $k = \varphi(m)$.

8. Αποδείξτε ότι η μοναδική λύση modulo M του συστήματος

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ &\vdots \\ x &\equiv a_r \mod m_r \end{aligned}$$

   όπου τα m_i είναι ανά δύο σχετικά πρώτοι ακέραιοι, δίνεται από

$$x \equiv a_1 M_1^{\varphi(m_1)} + \cdots + a_r M_r^{\varphi(m_r)} \mod M,$$

   όπου $M_i = M/m_i$, $M = m_1 m_2 \ldots m_r$.

9. Αποδείξτε ότι αν ο n διαιρείται με k διακεκριμένους περιττούς πρώτους, τότε $2^k | \varphi(n)$.

10. Αποδείξτε ότι

$$\varphi(2n) = \begin{cases} \varphi(n), & \text{αν } n \text{ περιττός} \\ 2\varphi(n), & \text{αν } n \text{ άρτιος} \end{cases}$$

11. Για κάθε θετικούς ακεραίους n, k αποδείξτε ότι $\varphi(n^k) = n^{k-1}\varphi(n)$.

12. Αποδείξτε ότι $\varphi(mn) = \dfrac{d}{\varphi(d)}\varphi(m)\varphi(n)$, όπου $d = \mu\kappa\delta(a, b)$.

13. Για ποια n ο $\varphi(n)$ είναι άρτιος;

14. Αποδείξτε ότι $\varphi(n)|n$ αν και μόνο αν $n = 1$, 2^a ή $2^a \cdot 3^b$, όπου a, b είναι θετικοί ακέραιοι.

15. Ένα κλάσμα $\frac{a}{b}$, όπου $a, b \in \mathbb{Z}-\{0\}$, ονομάζεται ανάγωγο αν $\mu\kappa\delta(a, b) = 1$. Αποδείξτε ότι το πλήθος των αναγώγων κλασμάτων $\frac{a}{b}$ με $1 \leq a < b \leq n$ είναι $\sum_{k=1}^{n} \varphi(k)$.

16. Έστω d, n θετικοί ακέραιοι με $d|n$. Θέτουμε $A_d = \{m \in \{1, \ldots, n\} | \mu\kappa\delta(m, n) = d\}$.

    1) Αποδείξτε ότι το σύνολο A_d περιέχει ακριβώς $\varphi(n/d)$ στοιχεία.
    2) Συμπεράνατε ότι $n = \sum_{d|n} \varphi(n/d)$ από την ξένη ένωση $\{1, \ldots, n\} = \bigcup_{d|n} A_d$.
    3) Άρα $n = \sum_{d|n} \varphi(d)$.

17. Έστω m, n θετικοί ακέραιοι και $a \in \mathbb{Z}$ με $\mu\kappa\delta(m, n) = \mu\kappa\delta(a, mn) = 1$. Αποδείξτε ότι $a^k \equiv 1 \mod mn$ για κάθε κοινό πολλαπλάσιο k των $\varphi(m)$ και $\varphi(n)$.

18. Αποκρυπτογραφήσετε το μήνυμα

    0456 1863 2228 1736 1588 2132 1134
    2225 1092 1593 1278 0095 1588 0739
    2495 0129 1157 0629 1786

    που κρυπτογραφήθηκε με τη μέθοδο RSA για $n = 43 \cdot 59 = 2537$ και $e = 13$. (Θα χρειαστείτε κάποιο υπολογιστικό πρόγραμμα γιατί διαφορετικά οι πράξεις θα είναι χρονοβόρες).

19. Γιατί στο Βήμα 2 του RSA έχουμε $0 < Y(X) < n$ και όχι $0 \leq Y(X) < n$;

2 Δακτύλιοι

Στην Ενότητα 1, κατασκευάσαμε το σύνολο, $\mathbb{Z}_n$, των ακεραίων modulo n, ορίσαμε δύο πράξεις σε αυτό και διαπιστώσαμε ότι αυτές έχουν αρκετές κοινές ιδιότητες με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού στο $\mathbb{Z}$ (βλέπε ιδιότητες 1-7 στην Παράγραφο 1.4). Από τη Γραμμική Άλγεβρα υπενθυμίζουμε ότι στο σύνολο $M_n(\mathbb{R})$ των $n \times n$ πραγματικών πινάκων οι πράξεις της πρόσθεσης και του πολλαπλασιασμού πινάκων ικανοποιούν τις ιδιότητες 1 - 7. Βλέπουμε, δηλαδή, ότι αν και τα σύνολα $\mathbb{Z}$, $\mathbb{Z}_n$, $M_n(\mathbb{R})$ διαφέρουν σημαντικά - για παράδειγμα το ένα είναι πεπερασμένο και τα άλλα άπειρα - οι παραπάνω πράξεις που ορίζονται σε αυτά έχουν αρκετές κοινές ιδιότητες. Θα δούμε στη συνέχεια και πολλά άλλα παραδείγματα συνόλων στα οποία ορίζονται κατά φυσιολογικό τρόπο δύο πράξεις που ικανοποιούν τις ιδιότητες 1 - 7. Συνεπώς είναι εύλογο να επιχειρήσουμε μια ενιαία μελέτη συνόλων εφοδιασμένων με πράξεις που έχουν ιδιότητες παρόμοιες με αυτές της πρόσθεσης και του πολλαπλασιασμού των $\mathbb{Z}$, $\mathbb{Z}_n$, και $M_n(\mathbb{R})$. Το όφελος από μια τέτοια αντιμετώπιση είναι ότι κάθε συμπέρασμα που θα αποδειχθεί δεν θα ισχύει μόνο στο $\mathbb{Z}$, $\mathbb{Z}_n$ και $M_n(\mathbb{R})$, αλλά σε κάθε σύνολο που είναι αντικείμενο της μελέτης. Επίσης, η μελέτη σε γενικότερο πλαίσιο πολλές φορές αποκαλύπτει νέες πτυχές των ειδικών περιπτώσεων. Οδηγούμαστε έτσι στη μελέτη δακτυλίων.

Η θεωρία δακτυλίων αποτελεί μια από τις πιο σημαντικές περιοχές της σύγχρονης Άλγεβρας και έχει πολλές εφαρμογές σε άλλες περιοχές των Μαθηματικών, όπως είναι για παράδειγμα η Θεωρία Αριθμών και η Αλγεβρική Γεωμετρία, αλλά και σε άλλα επιστημονικά αντικείμενα, όπως είναι η Κρυπτογραφία και η Θεωρία Κωδίκων.

2.1 Δακτύλιοι, Ακέραιες Περιοχές, Σώματα

Στην Παράγραφο αυτή θα ασχοληθούμε με τους ορισμούς και τις πλέον στοιχειώδεις ιδιότητες που αφορούν δακτυλίους.

Πράξεις

Στην Ενότητα 1 είδαμε ότι μπορούμε να "προσθέσουμε" και να "πολλαπλασιάσουμε" δύο στοιχεία του $\mathbb{Z}_n$,

$$[a] + [b] = [a + b]$$

$$[a][b] = [ab].$$

Και στις δύο περιπτώσεις αντιστοιχίσαμε σε κάθε ζεύγος στοιχείων του $\mathbb{Z}_n$ *μοναδικό* στοιχείο του $\mathbb{Z}_n$. Δηλαδή, είχαμε ορίσει δύο απεικονίσεις $\mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$, ή όπως λέμε, δύο "πράξεις" στο $\mathbb{Z}_n$.

Ορισμός *Μια* **πράξη** *σε ένα μη κενό σύνολο A είναι μια απεικόνιση της μορφής $A \times A \to A$.*

Παραδείγματα

1. Η πρόσθεση ακεραίων και ο πολλαπλασιασμός ακεραίων ορίζουν πράξεις στο $\mathbb{Z}$ και $\mathbb{N}$,

$$\mathbb{Z} \times \mathbb{Z} \ni (m, n) \mapsto m + n \in \mathbb{Z}, \quad \mathbb{Z} \times \mathbb{Z} \ni (m, n) \mapsto mn \in \mathbb{Z},$$

$$\mathbb{N} \times \mathbb{N} \ni (m, n) \mapsto m + n \in \mathbb{N}, \quad \mathbb{N} \times \mathbb{N} \ni (m, n) \mapsto mn \in \mathbb{N},$$

2. Η αφαίρεση ακεραίων ορίζει πράξη στο $\mathbb{Z}$

$$\mathbb{Z} \times \mathbb{Z} \ni (m, n) \mapsto m - n \in \mathbb{Z},$$

ενώ δεν ορίζει πράξη στο $\mathbb{N}$, γιατί το αποτέλεσμα $m - n$ ενδέχεται να μην είναι στοιχείο του $\mathbb{N}$.

3. Η διαίρεση ρητών αριθμών, ενώ δεν ορίζει πράξη στο $\mathbb{Q}$, γιατί ενδέχεται ο παρονομαστής να είναι μηδέν, ορίζει πράξη στο $\mathbb{Q} - \{0\}$,

$$(\mathbb{Q} - \{0\}) \times (\mathbb{Q} - \{0\}) \ni (r, s) \mapsto rs^{-1} \in \mathbb{Q} - \{0\}.$$

4. Έστω $m, n \in \mathbb{Z}$. Θέτουμε $\max(m, n) = m$ αν $m \geq n$ και $\max(m, n) = n$ αν $m < n$. Η αντιστοιχία $\mathbb{Z} \times \mathbb{Z} \ni (m, n) \mapsto \max(m, n) \in \mathbb{Z}$ είναι μία πράξη στο $\mathbb{Z}$.

5. Στο σύνολο $M_n(\mathbb{C})$ των $n \times n$ μιγαδικών πινάκων η συνήθης πρόσθεση πινάκων $(a_{ij})+(b_{ij}) = (c_{ij})$, $c_{ij} = a_{ij}+b_{ij}$, και ο συνήθης πολλαπλασιασμός $(a_{ij})(b_{kl}) = (c_{rs})$, $c_{rs} = \sum_{t=1}^{n} a_{rt}b_{ts}$, ορίζουν πράξεις.

6. Στο σύνολο $M_n(\mathbb{C})$ ορίζεται η πράξη

$$M_n(\mathbb{C}) \times M_n(\mathbb{C}) \to M_n(\mathbb{C}), ((a_{ij}), (b_{kl})) \mapsto (c_{rs}), \quad c_{rs} = a_{rs}b_{rs}$$

("πολλαπλασιασμός κατά στοιχείο").

Συνηθίζεται στην Άλγεβρα, στη θέση του συμβολισμού απεικονίσεων $f : A \times A \to A$ για μια πράξη στο A, να χρησιμοποιούμε συμβολισμούς όπως είναι οι $+$, $\cdot$, $*$, $\oplus$, $\otimes$ και η εικόνα του στοιχείου (a, b) να συμβολίζεται αντίστοιχα $a + b$, $a \cdot b$, $a * b$, $a \oplus b$, $a \otimes b$.

Σχόλια[1]

Η έννοια της πράξης είναι πολύ γενική: Σε κάθε μη κενό σύνολο A μπορεί να ορισθεί μία πράξη, για παράδειγμα η $A \times A \ni (a, b) \mapsto a \in A$. Εύκολα διαπιστώνουμε ότι αν το A αποτελείται από δύο στοιχεία, τότε μπορούν να ορισθούν σε αυτό 16 διαφορετικές πράξεις. Επίσης παρατηρούμε ότι σε σύνολα όπου έχουν ήδη ορισθεί πράξεις μπορούμε να ορίσουμε νέες πράξεις, όπως είναι για παράδειγμα οι

$$\mathbb{Z} \times \mathbb{Z} \ni (a, b) \mapsto a^2b - 3ab^5 + 1 \in \mathbb{Z},$$

$$\mathbb{Z}_n \times \mathbb{Z}_n \ni ([a], [b]) \mapsto [a][b] + [a] + [b] \in \mathbb{Z}_n.$$

Πρέπει να τονίσουμε εδώ ότι η Άλγεβρα δεν ασχολείται με την μελέτη της όποιας πράξης που μπορεί να επινοήσει κάποιος. Οι πράξεις που μελετάμε πηγάζουν από συγκεκριμένα προβλήματα των Μαθηματικών. Για παράδειγμα, στην μελέτη της αριθμητικής του $\mathbb{Z}$ σημαντικό ρόλο παίζουν οι ισοτιμίες modulo n και η αριθμητική τους και κατά συνέπεια οδηγούμαστε στην μελέτη του $\mathbb{Z}_n$ και των δύο πράξεων που ορίσαμε σε αυτό (βλ. Παράγραφο 1.4). Ένα άλλο χαρακτηριστικό παράδειγμα συναντάμε στη Γραμμική Άλγεβρα. Ο περίεργος τρόπος ορισμού του γινομένου δύο πινάκων δικαιολογείται από το γεγονός ότι ο πίνακας αυτός αντιστοιχεί στη σύνθεση δύο γραμμικών απεικονίσεων.

[1] Υπό τον τίτλο "Σχόλια" θα παραθέτουμε επεξηγήσεις ή διαισθητικές παρατηρήσεις που κρίνονται βοηθητικές για την κατανόηση του βιβλίου, έστω και αν αυτές δεν είναι διατυπωμένες με αυστηρό τρόπο.

Στη συνέχεια θα ασχοληθούμε με την περίπτωση που έχουν οριστεί δύο πράξεις σε ένα σύνολο οι οποίες ικανοποιούν ιδιότητες που μας θυμίζουν τις βασικές ιδιότητες της πρόσθεσης και του πολλαπλασιασμού στο $\mathbb{Z}$, $\mathbb{Z}_n$, και $M_n(\mathbb{R})$, δηλαδή τις ιδιότητες 1 - 7 της Παραγράφου 1.4.

2.1.1 Ορισμός. *Ένα σύνολο R εφοδιασμένο με δύο πράξεις, $+ : R \times R \to R$ και $\cdot : R \times R \to R$, ονομάζεται* ***δακτύλιος*** *αν ισχύουν οι παρακάτω ιδιότητες:*

1. $(a + b) + c = a + (b + c)$ *για κάθε* $a, b, c \in R$
2. *υπάρχει στοιχείο* $0_R \in R$ *τέτοιο ώστε* $a + 0_R = 0_R + a = a$ *για κάθε* $a \in R$
3. *για κάθε* $a \in R$ *υπάρχει στοιχείο* $a' \in R$ *τέτοιο ώστε* $a + a' = a' + a = 0_R$
4. $a + b = b + a$ *για κάθε* $a, b \in R$
5. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *για κάθε* $a, b, c \in R$
6. $a \cdot (b + c) = a \cdot b + a \cdot c$ *για κάθε* $a, b, c \in R$, *και*
7. $(a + b) \cdot c = a \cdot c + b \cdot c$ *για κάθε* $a, b, c \in R$.

Το στοιχείο 0_R ονομάζεται ***μηδενικό στοιχείο*** του δακτυλίου R και το στοιχείο a' ***αντίθετο*** του a. Θα δούμε παρακάτω ότι σε κάθε δακτύλιο R υπάρχει μοναδικό μηδενικό στοιχείο και ότι κάθε $a \in R$ έχει μοναδικό αντίθετο. Το αντίθετο του a θα το συμβολίζουμε συχνά με $-a$.

Αν στον δακτύλιο R ισχύει $a \cdot b = b \cdot a$, για κάθε $a, b \in R$, ο R θα λέγεται ***μεταθετικός***. Αν στο δακτύλιο R υπάρχει στοιχείο 1_R με την ιδιότητα $1_R \cdot r = r \cdot 1_R = r$, για κάθε $r \in R$, το 1_R θα ονομάζεται ***μοναδιαίο στοιχείο*** (ή ***μονάδα***) του R και θα λέμε ότι ο R είναι ***δακτύλιος με μοναδιαίο στοιχείο*** (ή με μονάδα). Θα δούμε παρακάτω ότι το μοναδιαίο στοιχείο (όταν υπάρχει) είναι μοναδικό.

Η πράξη $+$ (αντίστοιχα, $\cdot$) στον παραπάνω ορισμό συνήθως ονομάζεται η ***πρόσθεση*** (αντίστοιχα, ο ***πολλαπλασιασμός***) του δακτυλίου R.

Η ιδιότητα 1 (αντίστοιχα, η 5) συνήθως ονομάζεται η ***προσεταιριστική*** ιδότητα της πρόσθεσης (αντίστοιχα, του πολλαπλασιασμού). Οι ιδιότητες 6 και 7 συνήθως ονομάζονται ***επιμεριστικοί νόμοι***.

Σημειώσεις

1) Πολύ συχνά, θα χρησιμοποιούμε τον απλούστερο συμβολισμό ab στη θέση του $a \cdot b$. Επίσης, για το στοιχείο 0_R του R θα χρησιμοποιούμε συχνά το συμβολισμό $0_R = 0$ και, στην περίπτωση που ο R έχει μοναδιαίο στοιχείο 1_R, θα γράφουμε συχνά $1_R = 1$.

2) Αν θέλουμε να δηλώσουμε τον συμβολισμό των δύο πράξεων $+$ και $\cdot$ σε ένα δακτύλιο R, συνήθως τον παριστάνουμε σαν τριάδα $(R, +, \cdot)$.

2.1.2 Παραδείγματα.

1) Τα σύνολα $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ και $\mathbb{C}$ με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού μιγαδικών αριθμών είναι παραδείγματα μεταθετικών δακτυλίων με μονάδα.

2) **Ακέραιοι modulo n**
Το σύνολο $\mathbb{Z}_n$ με τις πράξεις που ορίσαμε στην Παράγραφο 1.4 είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Το μηδενικό στοιχείο είναι η κλάση $[0]$, το αντίθετο της κλάσης $[a]$ είναι η κλάση $[-a]$ και το μοναδιαίο στοιχείο είναι η κλάση $[1]$.

3) **$n \times n$ πίνακες**
Το σύνολο $M_n(\mathbb{C})$ των $n \times n$ μιγαδικών πινάκων με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού πινάκων είναι ένας δακτύλιος με μοναδιαίο στοιχείο τον ταυτοτικό $n \times n$ πίνακα

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Το μηδενικό στοιχείο είναι ο πίνακας του οποίου όλα τα στοιχεία είναι 0, ενώ το αντίθετο του $A = (a_{ij}) \in M_n(\mathbb{C})$ είναι το $-A = (-a_{ij})$. Ο $M_n(\mathbb{C})$ δεν είναι μεταθετικός αν $n \neq 1$, γιατί τότε υπάρχουν $A, B \in M_n(\mathbb{C})$ με $AB \neq BA$. Επίσης, το σύνολο $M_n(\mathbb{Z})$ των $n \times n$ πινάκων με στοιχεία ακεραίους αριθμούς (με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού πινάκων) είναι δακτύλιος.

Πιο γενικά, έστω R ένας δακτύλιος. Τότε στο σύνολο $M_n(R)$ των $n \times n$ πινάκων με στοιχεία από το R ορίζουμε δύο πράξεις ως εξής. Έστω $A, B \in M_n(R)$, $A = (a_{ij})$, $B = (b_{ij})$. Ορίζουμε $A + B = (a_{ij} + b_{ij})$και $AB = (c_{ij})$, όπου $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$. Ως προς τις πράξεις αυτές το σύνολο $M_n(R)$ είναι ένας δακτύλιος. Αν ο R έχει μοναιαίο στοιχείο, τότε και ο $M_n(R)$ έχει μοναδιαίο στοιχείο.

4) Το σύνολο $F(\mathbb{R}, \mathbb{R})$ όλων των απεικονίσεων $f : \mathbb{R} \to \mathbb{R}$ είναι ένας δακτύλιος ως προς τις πράξεις

$$+ : F(\mathbb{R}, \mathbb{R}) \times F(\mathbb{R}, \mathbb{R}) \to F(\mathbb{R}, \mathbb{R}), (f, g) \mapsto f + g,$$
$$\cdot : F(\mathbb{R}, \mathbb{R}) \times F(\mathbb{R}, \mathbb{R}), (f, g) \mapsto f \cdot g$$

όπου

$$f+g:\mathbb{R}\to\mathbb{R}, (f+g)(x)=f(x)+g(x), \quad \text{και}$$
$$f\cdot g:\mathbb{R}\to\mathbb{R}, (f\cdot g)(x)=f(x)g(x)$$

Ο δακτύλιος αυτός έχει μοναδιαίο στοιχείο την σταθερή απεικόνιση $\mathbb{R}\to\mathbb{R}$, $x\mapsto 1$, και είναι μεταθετικός.

Έστω X ένα μη κενό σύνολο και R ένας δακτύλιος. Στο σύνολο $F(X,R)$ όλων των απεικονίσεων $X\to R$ ορίζουμε πράξεις $+,\cdot$ με τρόπο παρόμοιο προς τον προηγούμενο. Δηλαδή αν $f,g\in F(X,R)$, ορίζουμε $f+g\in F(X,R)$ όπου $(f+g)(x)=f(x)+g(x)$ για κάθε $x\in X$, και $fg\in F(X,R)$, όπου $fg(x)=f(x)g(x)$ για κάθε $x\in X$. Ως προς τις πράξεις αυτές το $F(X,R)$ είναι ένας δακτύλιος.

5) Το σύνολο $C(\mathbb{R},\mathbb{R})$ όλων των συνεχών συναρτήσεων $f:\mathbb{R}\to\mathbb{R}$ με τις πράξεις του παραδείγματος 4 είναι ένας δακτύλιος. (Για να ορίζει η πρόσθεση και το γινόμενο απεικονίσεων πράξεις στο σύνολο $C(\mathbb{R},\mathbb{R})$, πρέπει να θυμηθούμε ότι το άθροισμα και το γινόμενο δύο συνεχών απεικονίσεων $\mathbb{R}\to\mathbb{R}$ είναι συνεχείς απεικονίσεις).

6) Το σύνολο των αρτίων ακεραίων με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού ακεραίων είναι ένας μεταθετικός δακτύλιος που δεν έχει μοναδιαίο στοιχείο. Το ίδιο αληθεύει για το σύνολο $m\mathbb{Z}=\{mk|k\in\mathbb{Z}\}$ με τις ίδιες πράξεις, όπου $m\in\mathbb{N}, m>1$.

7) **Ακέραιοι του Gauss**
Θεωρούμε το υποσύνολο των μιγαδικών αριθμών $\mathbb{Z}[i]=\{a+bi\in\mathbb{C}|a,b\in\mathbb{Z}\}$. Παρατηρούμε ότι το άθροισμα και το γινόμενο δύο μιγαδικών αριθμών που είναι στοιχεία του $\mathbb{Z}[i]$ ανήκουν στο $\mathbb{Z}[i]$. Με τις πράξεις αυτές, το $\mathbb{Z}[i]$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο.

8) Θεωρούμε το υποσύνολο των πραγματικών αριθμών $\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2}\in\mathbb{R}|a,b\in\mathbb{Q}\}$. Παρατηρούμε ότι το άθροισμα και το γινόμενο δύο πραγματικών αριθμών που είναι στοιχεία του $\mathbb{Q}[\sqrt{2}]$ είναι πάλι στοιχεία του $\mathbb{Q}[\sqrt{2}]$. Με τις πράξεις αυτές, το $\mathbb{Q}[\sqrt{2}]$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο.

9) Το σύνολο $\mathbb{N}$ με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού φυσικών αριθμών δεν είναι δακτύλιος. (Δεν ισχύει η ιδιότητα 3).

10) Στο σύνολο $\mathbb{Z}$ ορίζουμε τις πράξεις $\oplus : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $\bullet : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, όπου

$$a \oplus b = a + b - 1, \quad a \bullet b = ab - (a + b) + 2.$$

Μπορεί να αποδειχτεί ότι το $(\mathbb{Z}, \oplus, \bullet)$ είναι ένας δακτύλιος και μάλιστα μεταθετικός με μηδενικό στοιχείο το 1 και μοναδιαίο στοιχείο το 2. Η επαλήθευση των ιδιοτήτων σε αυτό το παράδειγμα δεν είναι τελείως άμεση. Από αυτές ενδεικτικά εξετάζουμε μία, για παράδειγμα την προσεταιριστική ιδιότητα της $\bullet$. Έχουμε

$$\begin{aligned}(a \bullet b) \bullet c &= (ab - (a + b) + 2) \bullet c \\ &= (ab - (a + b) + 2)c - (ab - (a + b) + 2 + c) + 2 \\ &= abc - ab - bc - ac + a + b + c\end{aligned}$$

και

$$\begin{aligned}a \bullet (b \bullet c) &= a \bullet (bc - (b + c) + 2) \\ &= a(bc - (b + c) + 2) - (a + bc - (b + c) + 2) + 2 \\ &= abc - ab - bc - ac + a + b + c.\end{aligned}$$

Άρα $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ για κάθε $a, b, c \in \mathbb{Z}$.

Το αντίθετο του a προσδιορίζεται από τη σχέση $a \oplus b = 1$, δηλαδή από την $a + b - 1 = 1$. Βλέπουμε ότι το αντίθετο του a το $2 - a$.

Το παράδειγμα αυτό δείχνει ότι είναι δυνατό ένα σύνολο να είναι δακτύλιος με πολλούς διαφορετικούς τρόπους.

11) **Δακτύλιος του Boole**
Έστω X ένα σύνολο και $P(X)$ το σύνολο των υποσυνόλων του X. Ορίζουμε δύο πράξεις στο $P(X)$: αν $A, B \in P(X)$, θέτουμε $A+B = A \cup B - A \cap B$ και $AB = A \cap B$. Το $P(X)$ με τις πράξεις αυτές είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο το X. (Μερικές από τις ιδιότητες δεν είναι τελείως άμεσες. Τα διαγράμματα Venn ίσως μας βοηθήσουν εποπτικά στην απόδειξή τους). Το μηδενικό στοιχείο είναι το κενό σύνολο και το αντίθετο του A είναι το ίδιο το A, δηλαδή $-A = A$.

12) Θεωρούμε το σύνολο $T_n(\mathbb{C})$ των μιγαδικών $n \times n$ άνω τριγωνικών πινάκων. Το άθροισμα και το γινόμενο δύο μιγαδικών $n \times n$ πινάκων που είναι άνω τριγωνικοί είναι πάλι άνω τριγωνικός. Το σύνολο $T_n(\mathbb{C})$ εφοδιασμένο με τις πράξεις αυτές είναι ένας δακτύλιος με μοναδιαίο στοιχείο, ο οποίος δεν είναι μεταθετικός ($n > 1$). Με ανάλογο τρόπο ορίζεται ο δακτύλιος $T_n(R)$ των $n \times n$ άνω τριγωνικών πινάκων με στοιχεία από ένα δακτύλιο R.

13) **Ευθύ γινόμενο δακτυλίων**
Έστω $(R,+,\cdot)$, $(S,\oplus,\odot)$ δύο δακτύλιοι. Μπορούμε να κατασκευάσουμε έναν νέο δακτύλιο ως εξής. Στο καρτεσιανό γινόμενο $R\times S=\{(r,s)|r\in R, s\in S\}$ ορίζουμε τις πράξεις $(r,s)+(r',s')=(r+r',s\oplus s')$ και $(r,s)(r',s')=(r\cdot r',s\odot s')$. Δηλαδή η πρόσθεση και ο πολλαπλασιασμός διατεταγμένων ζευγών ορίζονται κατά συντεταγμένη. Με τις πράξεις αυτές, το $R\times S$ είναι ένας δακτύλιος που ονομάζεται το ***ευθύ γινόμενο*** των R και S. Έχουμε $0_{R\times S}=(0_R,0_S)$ και $-(r,s)=(-r,-s)$.

Αν $R_1,\ldots,R_n$ είναι δακτύλιοι, το καρτεσιανό γινόμενο $R_1\times\cdots\times R_n$ είναι ένας δακτύλιος ως προς την πρόσθεση και τον πολλαπλασιασμό που ορίζονται κατά συντεταγμένη.

14) Έστω V ένας $\mathbb{R}$-διανυσματικός χώρος και $L(V,V)$ το σύνολο των γραμμικών απεικονίσεων $V\to V$. Αν $f,g\in L(V,V)$ ορίζουμε τις απεικονίσεις $f+g:V\to V$ και $f\circ g:V\to V$, όπου για κάθε $v\in V$ έχουμε $(f+g)(v)=f(v)+g(v)$ και $f\circ g(v)=f(g(v))$. Εύκολα αποδεικνύεται ότι $f+g, f\circ g\in L(V,V)$. Ως προς τις πράξεις αυτές το $L(V,V)$ είναι ένας δακτύλιος που έχει μοναδιαίο στοιχείο (την ταυτοτική απεικόνιση $I:V\to V$, $v\mapsto v$).

Ας δούμε τώρα μερικές άμεσες συνέπειες του ορισμού. Έστω R ένας δακτύλιος.

1. *Το στοιχείο $0_R\in R$ είναι μοναδικό ως προς την ιδιότητα 2.*
Πράγματι, αν υπήρχε και ένα άλλο, έστω $0'_R$, τότε αφενός $0_R=0_R+0'_R$ λόγω της ιδιότητας 2 για το $0'_R$, και αφετέρου $0_R+0'_R=0'_R$ λόγω της ίδιας ιδιότητας για το 0_R.

2. *Για κάθε $a\in R$, το a' της ιδιότητας 3 είναι μοναδικό.*
Πράγματι, αν υπήρχε και ένα άλλο, έστω a'', τότε χρησιμοποιώντας τις πρώτες τρεις ιδιότητες έχουμε
$$a''=a''+0_R=a''+(a+a')=(a''+a)+a'=0_R+a'=a'.$$

3. **Νόμος διαγραφής.** *Αν για τα $a,b,c\in R$ ισχύει $a+b=a+c$, τότε $b=c$.*
Πράγματι, προσθέτοντας κατά μέλη το $-a$ στην πρώτη σχέση και χρησιμοποιώντας τις πρώτες τρεις ιδιότητες παίρνουμε
$$\begin{aligned}-a+(a+b)=-a+(a+c)&\Rightarrow(-a+a)+b=(a+a)+c\\&\Rightarrow 0_R+b=0_R+c\Rightarrow b=c.\end{aligned}$$

4. *Αν για τα* $a, b \in R$ *ισχύει* $a + b = 0_R$*, τότε* $b = -a$.
   Αυτό προκύπτει αμέσως όταν εφαρμόσουμε τον νόμο της διαγραφής στη σχέση $a+b = a+(-a)$. (Επίσης προκύπτει από τη μοναδικότητα του $-a$).

5. *Για κάθε* $a \in R$ *ισχύει* $-(-a) = a$.
   Αυτό έπεται αμέσως από τη σχέση $a + (-a) = (-a) + a = 0_R$ (που λεει ότι το αντίθετο του $-a$ είναι το a).

6. *Για κάθε* $a, b \in R$ *ισχύει* $-(a + b) = (-a) + (-b)$.
   Πρώτα παρατηρούμε ότι ισχύει

$$(a + b) + ((-a) + (-b)) = 0_R. \tag{5}$$

   Πράγματι, έχουμε $(a + b) + ((-a) + (-b)) = ((a + b) + (-a)) + (-b) = ((b + a) + (-a)) + (-b) = (b + (a + (-a))) + (-b) = (b + 0_R) + (-b) = b + (-b) = 0_R$. Από την (5) προκύπτει το ζητούμενο.

7. *Για κάθε* $a \in R$ *ισχύει* $a0_R = 0_R a = 0_R$.
   Έχουμε $aa = a(a + 0_R) = aa + a0_R$. Έτσι $aa + 0_R = aa = aa + a0_R$ και από το νόμο της διαγραφής παίρνουμε $0_R = a0_R$. Όμοια αποδεικνύεται και η άλλη σχέση.

8. *Για κάθε* $a, b \in R$ *ισχύει* $a(-b) = (-a)b = -(ab)$.
   Έχουμε $0_R = a0_R = a(b + (-b)) = ab + a(-b)$. Από το 4 προκύπτει ότι $a(-b) = -(ab)$. Όμοια αποδεικνύεται και η άλλη σχέση.

9. *Για κάθε* $a, b \in R$ *ισχύει* $(-a)(-b) = ab$.
   Πράγματι, αυτό προκύπτει αν θέσουμε $-b$ στη θέση του b στην 8 και χρησιμοποιήσουμε ότι $-(-b) = b$.

10. *Αν ο* R *έχει μοναδιαίο στοιχείο, αυτό είναι μοναδικό.*
    Πράγματι, αν u, v ήταν μοναδιαία στοιχεία θα είχαμε $u = uv = v$.

Οι προηγούμενες ιδιότητες θα χρησιμοποιούνται παρακάτω χωρίς να γίνεται ιδιαίτερη μνεία.

Στη συνέχεια θα ασχοληθούμε με κάποιες ειδικές αλλά σημαντικές κατηγορίες δακτυλίων.

Ακέραιες περιοχές και σώματα

Υπενθυμίζουμε ότι το γινόμενο δύο μη μηδενικών ακεραίων δεν είναι μηδέν. Στο $\mathbb{Z}_6$, όμως, παρατηρούμε ότι ισχύει $[2][3] = [0]$. Δηλαδή είναι δυνατό σε ένα δακτύλιο R να υπάρχουν μη μηδενικά στοιχεία a και b με την ιδιότητα $ab = 0$.

Στην περίπτωση αυτή, το a ονομάζεται ***αριστερός μηδενοδιαιρέτης*** του R και το b ***δεξιός μηδενοδιαιρέτης*** του R. Αν ο δακτύλιος R είναι μεταθετικός, τότε οι αριστεροί και δεξιοί μηδενοδιαιρέτες ταυτίζονται. Έτσι, όταν ο δακτύλιος είναι μεταθετικός και υπάρχουν μη μηδενικά $a, b \in R$ με $ab = 0$, θα λέμε ότι το a (και το b) είναι ***μηδενοδιαιρέτης*** του R. Για παράδειγμα, το $[2] \in \mathbb{Z}_6$ είναι μηδενοδιαιρέτης του $\mathbb{Z}_6$. Το

$$\begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix} \in M_2(\mathbb{C})$$

είναι αριστερός μηδενοδιαιρέτης του $M_2(\mathbb{C})$, αφού, για παράδειγμα, ισχύει

$$\begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -2 & -2 \end{pmatrix} = 0.$$

2.1.3 Ορισμός. *Ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο $1_R \neq 0_R$ ονομάζεται ακεραία περιοχή αν δεν έχει μηδενοδιαιρέτες.*

Για παράδειγμα, οι δακτύλιοι $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ είναι ακέραιες περιοχές. Επίσης οι $\mathbb{Z}[i]$ και $\mathbb{Q}[\sqrt{2}]$ είναι ακέραιες περιοχές. Ο δακτύλιος $M_n(\mathbb{C})$, $n > 1$, δεν είναι ακεραία περιοχή, γιατί δεν είναι μεταθετικός. Επίσης, ο $2\mathbb{Z}$ δεν είναι ακέραια περιοχή γιατί δεν έχει μοναδιαίο στοιχείο. Ο $\mathbb{Z}_6$, αν και είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο διάφορο του 0, δεν είναι ακεραία περιοχή γιατί έχει έναν τουλάχιστον μηδενοδιαιρέτη. Το ίδιο συμβαίνει για τον $F(\mathbb{R}, \mathbb{R})$ (βλ. Άσκηση 21).

Σημειώσεις

1) Έστω ένας δακτύλιος R με μοναδιαίο στοιχείο 1_R. Η συνθήκη $1_R \neq 0_R$ (που εμφανίζεται στον Ορισμό 2.1.3) ισοδυναμεί με τη συνθήκη $R \neq \{0\}$. Πράγματι, αν $1_R = 0_R$, τότε για το τυχαίο $a \in R$ έχουμε $a = 1_R a = 0_R a = 0_R$, που σημαίνει ότι $R = \{0_R\}$. Αντίστροφα, αν $R = \{0\}$, τότε βέβαια $1_R = 0_R$. Κάθε δακτύλιος R που αποτελείται από ακριβώς ένα στοιχείο (που αναγκαστικά είναι το μηδενικό στοιχείο του R), $R = \{0_R\}$, ονομάζεται ***μηδενικός δακτύλιος***. Η συνθήκη $1_R \neq 0_R$ στον ορισμό 2.1.3 σημαίνει ότι δεχόμαστε ότι ο μηδενικός δακτύλιος δεν είναι ακεραία περιοχή.

2) Έστω R μία ακεραία περιοχή και $a, b, c \in R$ με $ab = ac$. Αν $a \neq 0$, τότε $b = c$. Πράγματι, έχουμε $ab - ac = 0$ δηλαδή $a(b - c) = 0$. Αφού ο R είναι ακεραία περιοχή και $a \neq 0$ παίρνουμε $b - c = 0$.

2.1.4 Πρόταση. *Ο δακτύλιος $\mathbb{Z}_n$ είναι ακεραία περιοχή αν και μόνο αν ο n είναι πρώτος ή μηδέν.*

Απόδειξη. Έστω ότι ο $\mathbb{Z}_n$ είναι ακεραία περιοχή και $n \neq 0$. Τότε θα περιέχει δύο τουλάχιστον στοιχεία και κατά συνέπεια $n > 1$. Αν $n = ab$, όπου a, b είναι θετικοί ακέραιοι, τότε $[0] = [n] = [a][b]$, απ' όπου συμπεραίνουμε ότι $[a] = [0]$ ή

$[b] = [0]$ λόγω της υπόθεσης. Άρα $n|a$ ή $n|b$ και συνεπώς $a = n$ ή $b = n$, δηλαδή ο n είναι πρώτος.

Αντίστροφα, έστω ότι ο n είναι πρώτος. Τότε $n > 1$ και άρα $[1] \neq [0]$. Αν $[a][b] = [0]$, τότε $[ab] = [0]$, δηλαδή $n|ab$. Αφού ο n είναι πρώτος, θα διαιρεί έναν τουλάχιστον από τους a, b (Λήμμα 1.2.5). Επομένως έχουμε $[a] = [0]$ ή $[b] = [0]$. Τέλος, αν $n = 0$, τότε $\mathbb{Z}_n = \mathbb{Z}$. ⊺

Ένα στοιχείο u ενός δακτυλίου R με μοναδιαίο στοιχείο 1_R ονομάζεται ***αντιστρέψιμο*** στο R αν υπάρχει $v \in R$ με την ιδιότητα $uv = vu = 1_R$. Για παράδειγμα, τα αντιστρέψιμα στοιχεία του $\mathbb{Z}$ είναι τα $1, -1$. Στο $\mathbb{Q}$ κάθε μη μηδενικό στοιχείο είναι αντιστρέψιμο. Στην Ενότητα 1 είδαμε ότι τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_n$ είναι τα $[a] \in \mathbb{Z}_n$ για τα οποία ισχύει $\mu\kappa\delta(a, n) = 1$. Υπενθυμίζουμε από τη Γραμμική Άλγεβρα ότι τα αντιστρέψιμα στοιχεία του $M_n(\mathbb{C})$ είναι οι πίνακες που έχουν μη μηδενική ορίζουσα.

Το σύνολο των αντιστρέψιμων στοιχείων ενός δακτυλίου R συμβολίζεται με $U(R)$.

Στην περίπτωση που το στοιχείο $u \in R$ είναι αντιστρέψιμο, εύκολα βλέπουμε ότι υπάρχει μοναδικό $v \in R$ με $uv = vu = 1_R$. (Αν υπήρχε και άλλο, έστω w, τότε $w = w1_R = w(uv) = (wu)v = 1_R v = v$). Το v ονομάζεται το ***αντίστροφο*** του u και συνήθως συμβολίζεται με u^{-1}.

2.1.5 Ορισμός. *Ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο $1_R \neq 0_R$ στο οποίο κάθε μη μηδενικό στοιχείο είναι αντιστρέψιμο ονομάζεται* ***σώμα***.

Για παράδειγμα, σώματα είναι οι δακτύλιοι $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ αλλά όχι ο $\mathbb{Z}$. Ο δακτύλιος $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \in R | a, b \in \mathbb{Q}\}$ είναι σώμα γιατί κάθε μη μηδενικό στοιχείο του, $a + b\sqrt{2}$, είναι αντιστρέψιμο αφού $(a + b\sqrt{2})^{-1} = \dfrac{1}{a + b\sqrt{2}} \dfrac{a - b\sqrt{2}}{a - b\sqrt{2}} = \dfrac{a}{a^2 - 2b^2} + \dfrac{-b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. (Οι παρονομαστές δεν είναι μηδέν γιατί το $\sqrt{2}$ είναι άρρητος όπως είδαμε στην Παράγραφο 1.2). Αντίθετα, ο δακτύλιος $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \in R | a, b \in \mathbb{Z}\}$, όπου οι πράξεις είναι οι συνήθεις πράξεις των πραγματικών αριθμών, δεν είναι σώμα αφού, για παράδειγμα, το $2 \in \mathbb{Z}[\sqrt{2}]$ δεν είναι αντιστρέψιμο: αν $2(a + b\sqrt{2}) = 1$ με $a, b \in \mathbb{Z}$, τότε $b \neq 0$ και επιλύοντας ως προς $\sqrt{2}$ βρίσκουμε $\sqrt{2} \in \mathbb{Q}$, που είναι άτοπο. Οι $\mathbb{Z}_2$ και $\mathbb{Z}_3$ είναι σώματα, αλλά όχι ο $\mathbb{Z}_4$.

Παρατηρούμε ότι κάθε σώμα είναι ακεραία περιοχή, γιατί αν για τα στοιχεία a, b ενός σώματος ισχύει $ab = 0$ με $a \neq 0$, τότε πολλαπλασιάζοντας με a^{-1} παίρνουμε $b = 0$. Το αντίστροφο δεν αληθεύει, αφού, για παράδειγμα, ο $\mathbb{Z}$ δεν είναι σώμα. Όμως ισχύει το εξής αποτέλεσμα.

2.1.6 Πρόταση. *Κάθε πεπερασμένη ακεραία περιοχή είναι σώμα.*

Απόδειξη. Έστω ότι ο R είναι πεπερασμένη ακεραία περιοχή και έστω $R = \{r_1, \ldots, r_n\}$. Σύμφωνα με τους ορισμούς, αρκεί να δείξουμε ότι το τυχαίο μη μηδενικό $r \in R$ είναι αντιστρέψιμο. Θεωρούμε τα στοιχεία του R

$$rr_1, rr_2, \ldots, rr_n$$

Αυτά είναι ανά δύο διάφορα, γιατί αν $rr_i = rr_j$, τότε $r(r_i - r_j) = 0$, από το οποίο συμπεραίνουμε ότι $r_i - r_j = 0$, γιατί $r \neq 0$ και το R είναι ακεραία περιοχή. Συνεπώς το πεπερασμένο σύνολο $\{rr_1, rr_2, \ldots, rr_n\}$ αποτελείται από n στοιχεία και είναι υποσύνολο του R που και αυτό αποτελείται από n στοιχεία. Άρα, $\{rr_1, rr_2, \ldots, rr_n\} = R$. Επειδή $1_R \in R$, έχουμε $1_R = rr_j$ για κάποιο j. Επειδή ο R είναι μεταθετικός, συμπεραίνουμε ότι το r είναι αντιστρέψιμο. ⊺

Από την Πρόταση 2.1.4 και την Πρόταση 2.1.6 συνάγουμε το εξής αποτέλεσμα.

2.1.7 Πόρισμα. *Ο δακτύλιος $\mathbb{Z}_n$ είναι σώμα αν και μόνο αν ο n είναι πρώτος.*

Σημειώνουμε ότι το προηγούμενο Πόρισμα έπεται άμεσα και από την Πρόταση 1.4.5. Η απόδειξη αφήνεται σαν άσκηση.

Υποδακτύλιοι

Η μελέτη των ιδιοτήτων ενός δακτυλίου R συχνά διευκολύνεται αν εστιάσουμε την προσοχή μας σε "κατάλληλα" υποσύνολα του R. Στα Παραδείγματα 2.1.2, είδαμε περιπτώσεις δακτυλίων R που περιέχουν υποσύνολα $S \subseteq R$ που και αυτά είναι δακτύλιοι ως προς τους "περιορισμούς" στο S των πράξεων του R. Για παράδειγμα, έχουμε $2\mathbb{Z} \subseteq \mathbb{Z}$, $\mathbb{Z} \subseteq \mathbb{Q}$, $M_n(\mathbb{Z}) \subseteq M_n(\mathbb{R})$ και $T_n(\mathbb{C}) \subseteq M_n(\mathbb{C})$. Οδηγούμαστε έτσι στην έννοια του υποδακτυλίου. Πριν δώσουμε τον ορισμό, θα πρέπει να καταστήσουμε σαφές τι εννούμε με τον όρο "περιορισμός μιας πράξης".

Έστω $* : R \times R \to R$ μια πράξη στο σύνολο R και έστω S ένα υποσύνολο του R. Λαμβάνοντας τον περιορισμό της πράξης στο $S \times S$ έχουμε μια απεικόνιση $S \times S \to R$ που γενικά δεν ορίζει πράξη στο S. Για παράδειγμα, η πρόσθεση ακεραίων δεν δίνει πράξη στο υποσύνολο των περιττών ακεραίων γιατί το άθροισμα δύο περιττών δεν είναι περιττός. Αν όμως το S είναι τέτοιο ώστε $a * b \in S$ για κάθε $a, b \in S$, τότε ορίζεται μια πράξη στο S που συνήθως συμβολίζουμε πάλι με $* : S \times S \to S$. Στην περίπτωση αυτή λέμε ότι το S είναι ***κλειστό*** ως προς την $* : R \times R \to R$ και ότι η πράξη $* : S \times S \to S$ είναι ο ***περιορισμός*** στο S της πράξης $* : R \times R \to R$. Για παράδειγμα, επειδή το άθροισμα δύο αρτίων ακεραίων είναι άρτιος, το $2\mathbb{Z}$ είναι κλειστό ως προς την πρόσθεση ακεραίων και έτσι λαμβάνουμε τον περιορισμό $+ : 2\mathbb{Z} \times 2\mathbb{Z} \to 2\mathbb{Z}$ της πρόσθεσης του $\mathbb{Z}$ στο $2\mathbb{Z}$.

Επίσης, το υποσύνολο των άνω τριγωνικών πινάκων του $M_n(\mathbb{C})$ είναι κλειστό ως προς την πρόσθεση πινάκων και ως προς τον πολλαπλασιασμό πινάκων.

2.1.8 Ορισμός. *Έστω R ένας δακτύλιος και S ένα μη κενό υποσύνολο του R τέτοιο ώστε οι περιορισμοί των δύο πράξεων του R, $+ : R\times R \to R$, $\cdot : R\times R \to R$, στο $S \times S$ να είναι πράξεις στο S,*

$$+ : S \times S \to S, \quad \cdot : S \times S \to S.$$

Αν το S με τις πράξεις αυτές είναι δακτύλιος, θα λέμε ότι το S είναι **υποδακτύλιος** *του R.*

Για παράδειγμα, το σύνολο των αρτίων ακεραίων, $2\mathbb{Z}$, είναι υποδακτύλιος του $\mathbb{Z}$. Αντίθετα, το σύνολο των περιττών ακεραίων δεν είναι υποδακτύλιος του $\mathbb{Z}$. Επίσης το σύνολο των αρτίων φυσικών αριθμών $2\mathbb{N}$ δεν είναι υποδακτύλιος του $\mathbb{Z}$ αν και είναι κλειστό ως προς την πρόσθεση και τον πολλαπλασιασμό του $\mathbb{Z}$.

Μπορεί να δει κανείς ότι το $M_n(\mathbb{Z})$ είναι ένας υποδακτύλιος του $M_n(\mathbb{C})$ σύμφωνα με τον ορισμό. Υπάρχει όμως ένας πιο "οικονομικός" τρόπος που περιγράφεται από το ακόλουθο κριτήριο.

2.1.9 Πρόταση. *Έστω R ένας δακτύλιος και $S \subseteq R$, $S \neq \emptyset$. Τότε το S είναι υποδακτύλιος του R αν και μόνο αν ισχύουν οι ιδιότητες*

- $a, b \in S \Rightarrow a + b \in S$ *και* $ab \in S$
- $a \in S \Rightarrow -a \in S$.

Απόδειξη. Αν το S είναι υποδακτύλιος του R τότε βέβαια ισχύουν οι ιδιότητες της Πρότασης. Αντίστροφα, έστω ότι ισχύουν οι ιδιότητες της Πρότασης. Σύμφωνα με την πρώτη ιδιότητα, οι περιορισμοί των πράξεων του R στο $S \times S$ είναι πράξεις στο S. Είναι σαφές ότι οι ιδιότητες $1, 4, 5, 6, 7$ στον Ορισμό 2.1.1 είναι τέτοιες που αν ισχύουν σε ένα σύνολο, θα ισχύουν σε κάθε μη κενό υποσύνολό του. Εφόσον ισχύουν στο R, ισχύουν στο S. Για την ιδιότητα 2, έστω $a \in S$. Τότε από την δεύτερη ιδιότητα της Πρότασης έχουμε $-a \in S$, οπότε η πρώτη δίνει $a + (-a) \in S$, δηλαδή $0 \in S$. Τέλος η ιδιότητα 3 ισχύει λόγω της δεύτερης ιδιότητας. ⊺

Έτσι, για να δει κανείς ότι το $M_n(\mathbb{Z})$ είναι ένας υποδακτύλιος του $M_n(\mathbb{C})$ αρκεί να ελέγξει ότι $A + B \in M_n(\mathbb{Z})$, $AB \in M_n(\mathbb{Z})$ και $-A \in M_n(\mathbb{Z})$ για κάθε $A, B \in M_n(\mathbb{Z})$.

Μια ισοδύναμη διατύπωση της προηγούμενης Πρότασης είναι η ακόλουθη. Η απόδειξη αφήνεται σαν άσκηση.

2.1.10 Πρόταση. *Έστω R ένας δακτύλιος και $S \subseteq R$, $S \neq \emptyset$. Τότε το S είναι υποδακτύλιος του R αν και μόνο αν ισχύουν*

$$a, b \in S \Rightarrow a - b \in S \quad \text{και} \quad ab \in S.$$

Σημείωση Έστω S ένας υποδακτύλιος του δακτυλίου R. Τότε $0_S = 0_R$. Στην περίπτωση που οι R, S έχουν μοναδιαία στοιχεία, δεν αληθεύει γενικά ότι $1_S = 1_R$. Πράγματι, αν $R = \mathbb{Z} \times \mathbb{Z}$ και $S = \{(a, 0) \in \mathbb{Z} \times \mathbb{Z}\}$, τότε $1_R = (1, 1)$ και $1_S = (1, 0)$.

Έστω S ένας υποδακτύλιος ενός σώματος R. Αν ο S είναι σώμα, θα λέμε ότι είναι ένα ***υπόσωμα*** του R. Για παράδειγμα το $\mathbb{Q}$ είναι ένα υπόσωμα του $\mathbb{C}$. Αποδεικνύεται ότι κάθε υπόσωμα του $\mathbb{C}$ περιέχει το $\mathbb{Q}$ (βλ. Άσκηση 23).

2.1.11 Παραδείγματα.

1) Το σύνολο $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \in \mathbb{R} | a, b \in \mathbb{Z}\}$ είναι ένας υποδακτύλιος του $\mathbb{R}$ σύμφωνα με την Πρόταση 2.1.9. Πράγματι, αν $a+b\sqrt{2}$, $c+d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, τότε

   - $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{R}[\sqrt{2}]$
   - $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{R}[\sqrt{2}]$
   - $-(a + b\sqrt{2}) = (-a) + (-b)\sqrt{2} \in \mathbb{R}[\sqrt{2}]$

2) Έστω $a \in \mathbb{C}$. Θέτουμε $\mathbb{Z}[a] = \{s_m a^m + \cdots + s_1 a + a s_0 \in \mathbb{C} | s_0, \ldots, s_m \in \mathbb{Z}, m \geq 1\}$. Τότε το $\mathbb{Z}[a]$ είναι ένας υποδακτύλιος του $\mathbb{C}$, σύμφωνα με την Πρόταση 2.1.9. Έστω $a \in \mathbb{C}$ τέτοιο ώστε υπάρχουν ακέραιοι $r_0, \ldots, r_{n-1}$, όπου $n \geq 1$, με την ιδιότητα $a^n + r_{n-1}a^{n-1} + \cdots + r_0 = 0$.[2] Έστω $R = \{s_{n-1}a^{n-1} + \cdots + s_1 a + s_0 \in \mathbb{C} | s_0, \ldots, s_{n-1} \in \mathbb{Z}\}$. Τότε $R = \mathbb{Z}[a]$.

   Πράγματι, είναι φανερό ότι $R \subseteq \mathbb{Z}[a]$. Για να αποδείξουμε ότι $\mathbb{Z}[a] \subseteq R$, αρκεί να δείξουμε ότι $a^{n+m} \in R$ για κάθε $m = 0, 1, \ldots$. Χρησιμοποιούμε επαγωγή στο m. Για $m = 0$, έχουμε $a^{n+m} = a^n = -r_{n-1}a^{n-1} - \cdots - r_1 a - r_0 \in R$. Έστω ότι $m \geq 1$ και $a^{n+m-1} \in R$. Τότε $a^{n+m} = a^{n+m-1}a = (s_{n-1}a^{n-1} + \cdots + s_1 a + s_0)\, a = s_{n-1}a^n + s_{n-2}a^{n-1} + \cdots + s_0 a = s_{n-1}(-r_{n-1}a^{n-1} - \cdots - r_1 a - a_0) + s_{n-2}a^{n-1} + \cdots + s_0 a = (-s_{n-1}r_{n-1} + s_{n-2})a^{n-1} + (-s_{n-1}r_{n-2} + s_{n-3})a^{n-2} + \cdots + (-s_{n-1}a_0) \in R$.

   Οι δακτύλιοι της μορφής $\mathbb{Z}[a]$ παίζουν σημαντικό ρόλο στη Θεωρία Αριθμών.

[2] Στην περίπτωση αυτή, ο a ονομάζεται ***αλγεβρικός ακέραιος***. Για παράδειγμα, κάθε ακέραιος είναι αλγεβρικός ακέραιος. Επίσης, ο $\sqrt{2}$ είναι αλγεβρικός ακέραιος, ενώ οι αριθμοί $\frac{1}{2}, \frac{1}{\sqrt{2}}$ δεν είναι αλγεβρικοί ακέραιοι.

3) Το σύνολο $R = \{a + b\sqrt[3]{2} \in \mathbb{R} | a, b \in \mathbb{Z}\}$ δεν είναι υποδακτύλιος του $\mathbb{R}$, γιατί δεν είναι κλειστό ως προς τον πολλαπλασιασμό. Πράγματι, $\sqrt[3]{2}\sqrt[3]{2} = \sqrt[3]{4} \notin R$ (Αφήνουμε σαν άσκηση την απόδειξη ότι δεν υπάρχουν ακέραιοι a, b με $\sqrt[3]{4} = a + b\sqrt[3]{2}$).

4) Το σύνολο $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} | a, b \in \mathbb{Q}\}$ είναι ένας υποδακτύλιος του $\mathbb{R}$ σύμφωνα με την Πρόταση 2.1.9. Επιπλέον είναι ένα υπόσωμα όπως είδαμε πιο πάνω.

5) Έστω R το υποσύνολο του $M_2(\mathbb{R})$ που αποτελείται από τους πίνακες της μορφής

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

με $a, b \in \mathbb{R}$. Θα δείξουμε ότι το R είναι ένα σώμα με πράξεις την πρόσθεση και τον πολλαπλασιασμό πινάκων. Αρχικά δείχνουμε ότι το R είναι υποδακτύλιος του $M_2(\mathbb{R})$. Για κάθε δύο στοιχεία $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$ του R έχουμε

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \in R$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} \in R$$

$$-\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} -a & -b \\ -(-b) & -a \end{pmatrix} \in R.$$

Από την Πρόταση 2.1.9, το R είναι υποδακτύλιος του $M_2(\mathbb{R})$. Είναι δε μεταθετικός γιατί

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

και επιπλέον έχει μοναδιαίο στοιχείο το

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in R$$

που φυσικά είναι διάφορο του μηδενικού πίνακα. Μένει να δείξουμε ότι κάθε μη μηδενικό στοιχείο του R είναι αντιστρέψιμο. Έστω $a, b \in \mathbb{R}$ όχι

και τα δύο μηδέν και

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \quad B = \frac{1}{a^2+b^2}\begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Τότε $B \in R$ και $AB = BA = I$, δηλαδή το A είναι αντιστρέψιμο.

6) Το σύνολο $R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$ είναι ένας υποδακτύλιος του $T_2(\mathbb{R})$ και το $T_2(\mathbb{R})$ είναι ένας υποδακτύλιος του $M_2(\mathbb{R})$.

Ολοκληρώνουμε την Παράγραφο αυτή με μερικές παρατηρήσεις και παραδείγματα.

Πίνακες πράξεων

Για κάθε μια από τις δύο πράξεις ενός δακτυλίου μπορούμε να κατασκευάσουμε έναν πίνακα που δίνει τα αποτελέσματα της αντίστοιχης πράξης. Για παράδειγμα, οι δύο πράξεις του $\mathbb{Z}_4$ περιγράφονται από τους παρακάτω πίνακες. Το αποτέλεσμα της πράξης $[a]+[b]$ (αντίστοιχα, $[a][b]$) βρίσκεται στην τομή της γραμμής του $[a]$ με τη στήλη του $[b]$ στον αριστερό (αντίστοιχα, δεξιό) πίνακα

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[1]$	$[2]$	$[1]$

Πίνακες πράξεων στο $\mathbb{Z}_4$

Για παράδειγμα, βλέπουμε στον αριστερό πίνακα ότι $[2]+[3]=[1]$ και στον δεξιό $[2][3]=[2]$. Μια ενδιαφέρουσα εφαρμογή των πινάκων των πράξεων θα δούμε στην Παράγραφο 2.7. (Στο εξώφυλλο του παρόντος βιβλίου τα δύο τετράγωνα παριστάνουν τους πίνακες της πρόσθεσης του $\mathbb{Z}_4$ και του $\mathbb{Z}_2 \times \mathbb{Z}_2$).

"Πολλαπλασιασμός" στοιχείων δακτυλίου με ακεραίους

Σε κάθε δακτύλιο R έχουμε $(a+b)+c = a+(b+c)$ για κάθε $a, b, c \in R$. Το στοιχείο αυτό συμβολίζεται με $a+b+c$. Επίσης, όλες οι παραστάσεις $((a+b)+c)+d$, $(a+b)+(c+d)$, $a+((b+c)+d)$, $((a+(b+c))+d$, $a+(b+(c+d))$, ταυτίζονται. Συνηθίζεται δε να παραλείπονται οι παρενθέσεις και να χρησιμοποιείται ο απλούστερος συμβολισμός $a+b+c+d$. Ανάλογο αποτέλεσμα ισχύει στην περίπτωση που έχουμε οποιοδήποτε πεπερασμένο πλήθος προσθετέων και θα χρησιμοποιούμε τον συμβολισμό $a_1+a_2+\cdots+a_n$. Αν

και η απόδειξη του αποτελέσματος αυτού δεν είναι δύσκολη, θα την αφήσουμε για το Παράρτημα 6.2 γιατί απαιτεί δυσανάλογη έκταση στη διατύπωσή της. Επειδή ισχύει η προσεταιριστική ιδότητα του πολλαπλασιασμού, μπορούμε να χρησιμοποιούμε αντίστοιχο συμβολισμό $a_1a_2\dots a_n$ για γινόμενα.

Έστω R ένας δακτύλιος, $a \in R$ και $m \in \mathbb{Z}$. Ορίζουμε

$$ma = \begin{cases} a+\cdots+a, & m>0 \\ 0, & m=0 \\ (-a)+(-a)+\cdots+(-a), & m<0 \end{cases} \qquad \text{και}$$

$$a^m = a\dots a,\ m>0,$$

όπου το a και το $-a$ επαναλαμβάνεται $|m|$ φορές. Στην περίπτωση που ο R περιέχει μοναδιαίο στοιχείο, θέτουμε $a^0 = 1_R$ για κάθε $a \in R$.

Σημειώνουμε ότι είναι δυνατό να ισχύει $ma = 0$ όπου $m \in \mathbb{Z}$ και $a \in R$, ακόμα και αν $m \neq 0$ και $a \neq 0_R$. Για παράδειγμα, στο $\mathbb{Z}_n$ έχουμε $n1_{\mathbb{Z}_n} = n[1] = [n] = [0]$.

Μπορεί να διαπιστώσει κανείς ότι ισχύουν ιδιότητες όπως

$$\begin{aligned} (m+n)a &= ma+na, \\ m(a+b) &= ma+mb, \\ (ma)(nb) &= (mn)(ab), \\ m(ab) &= (ma)b = a(mb), \\ (-m)a &= m(-a) = -(ma) \end{aligned}$$

για κάθε $m,n \in \mathbb{Z}$ και $a,b \in R$, όπως επίσης και

$$\begin{aligned} (a^m)^n &= a^{mn}, \\ a^m a^n &= a^{m+n} \end{aligned}$$

για κάθε $m,n>0$ και $a \in R$. Οι αποδείξεις είναι εύκολες και παραλείπονται.

2.1.12 Παραδείγματα.

1) Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο και έστω $a,b \in R$ τέτοια ώστε $ab = ba$. Για κάθε $n \in \mathbb{N}$ ισχύει $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i}b^i$.
Για την απόδειξη χρησιμοποιούμε επαγωγή στο n. Για $n=0$ η αποδεικτέα ισότητα γράφεται $1=1$. Για το επαγωγικό βήμα έχουμε

$$(a+b)^{n+1} = (a+b)^n(a+b) = (a+b)^n a + (a+b)^n b.$$

Επειδή $ab = ba$ ο συντελεστής του $a^{n+1-i}b^i$, για $i = 1, \ldots, n$, στο δεξιό μέλος είναι $\binom{n}{i} + \binom{n}{i-1}$. Από την Πρόταση 1.1.6 1) έχουμε $\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}$, όταν $i = 1, \ldots, n$. Για $i = 0$, ο συντελεστής στο δεξιό μέλος είναι $1 = \binom{n+1}{0}$ και για $i = n+1$, είναι $1 = \binom{n+1}{n+1}$. Συνεπώς σε κάθε περίπτωση ο συντελεστής του $a^{n+1-i}b^i$ στο δεξιό μέλος είναι $\binom{n+1}{i}$. Άρα

$$(a+b)^{n+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} a^{n+1-i}b^i.$$

2) Έστω p ένας πρώτος αριθμός και R ένας μεταθετικός δακτύλιος για τον οποίο ισχύει $pa = 0$ για κάθε $a \in R$. (Ένας τέτοιος δακτύλιος είναι ο $\mathbb{Z}_p$). Τότε για κάθε $a, b \in R$ έχουμε

i) $(a+b)^p = a^p + b^p$, και

ii) $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ για κάθε θετικό ακέραιο n.

Πράγματι, από το προηγούμενο Παράδειγμα έχουμε

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i}b^i.$$

Αλλά γνωρίζουμε ότι $p \Big| \binom{p}{i}$, $i = 1, \ldots, p-1$,(απόδειξη του Θεωρήματος 1.4.7) και κατά συνέπεια $\binom{p}{i} a^{p-i}b^i = 0$, $i = 1, \ldots, p-1$. Συνεπώς $(a+b)^p = a^p + b^p$. Για να αποδείξουμε τη δεύτερη σχέση, χρησιμοποιούμε επαγωγή στο n. Για $n = 1$, η σχέση έχει ήδη αποδειχτεί. Για το επαγωγικό βήμα έχουμε

$$(a+b)^{p^n} = ((a+b)^p)^{p^{n-1}}$$
$$(a^p + b^p)^{p^{n-1}} = a^{p^n} + b^{p^n}.$$

3) *Έστω $m > 0$. Τότε κάθε $[a] \in \mathbb{Z}_m - \{[0]\}$ είναι αντιστρέψιμο ή μηδενοδιαιρέτης.*

Έστω $[a]$ μη μηδενικό στοιχείο του $\mathbb{Z}_m$ που δεν είναι αντιστρέψιμο. Τότε από την Πρόταση 1.4.5 έχουμε $\mu\kappa\delta(a, m) \neq 1$. Έστω $d = \mu\kappa\delta(a, m)$.

Τότε $d|a$ και $d|m$. Ισχύει $m|\frac{a}{d}m$, δηλαδή $m|a\frac{m}{d}$. Άρα στο $\mathbb{Z}_m$ έχουμε $[a][\frac{m}{d}] = [0]$. Είναι $[a] \neq [0]$ και επίσης $[\frac{m}{d}] \neq 0$ γιατί $d \neq 1$. Άρα το $[a]$ είναι μηδενοδιαιρέτης.

4) **(Quaternions[1] επί του $\mathbb{C}$)**. Δίνουμε εδώ ένα σημαντικό παράδειγμα μη μεταθετικού δακτυλίου $\mathbb{H}$, όπου κάθε μη μηδενικό στοιχείο είναι αντιστρέψιμο. Ο $\mathbb{H}$ είναι ένας διανυσματικός χώρος επί του $\mathbb{R}$ που έχει διάσταση 4. Έστω $\{1, i, j, k\}$ μία βάση του $\mathbb{H}$. Για να ορίσουμε το γινόμενο δύο στοιχείων του, πρώτα θα ορίσουμε το γινόμενο δύο στοιχείων της βάσης. Θέτουμε

$$1x = x1 = x \quad \text{για κάθε} \quad x \in \{1, i, j, k\}$$
$$i^2 = j^2 = k^2 = -1$$
$$ij = k, jk = i, ki = j$$
$$ji = -k, kj = -i, ik = -j.$$

Για να πολλαπλασιάσουμε δύο στοιχεία του $\mathbb{H}$, χρησιμοποιούμε τους επιμεριστικούς νόμους και τις παραπάνω ισότητες, απαιτώντας το 1 να είναι το μοναδιαίο στοιχείο και τα στοιχεία του $\mathbb{R}$ να μετατίθενται με τα i, j, k. Για παράδειγμα, έχουμε $(2+3i-5k)(1+7j) = 2+14j+3i+21ij-5k-35kj = 2 + 14j + 3i + 21k - 5k - 35(-i) = 2 + 32i + 14j + 16k$. Με τις πράξεις της πρόσθεσης του διανυσματικού χώρου $\mathbb{H}$ και του πολλαπλασιασμού που μόλις ορίσαμε μπορεί να αποδειχθεί εύκολα ότι το $\mathbb{H}$ είναι δακτύλιος με μοναδιαίο στοιχείο. (Το μόνο αξίωμα που δεν είναι προφανές είναι η προσεταιριστικότητα του πολλαπλασιασμού που χρειάζεται υπολογισμούς).

Θα δείξουμε τώρα ότι κάθε μη μηδενικό στοιχείο του $\mathbb{H}$ είναι αντιστρέψιμο. Υπολογίζοντας παρατηρούμε ότι

$$(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2.$$

Αν θέσουμε $\beta = a^2 + b^2 + c^2 + d^2$ και υποθέσουμε ότι $a + bi + cj + dk \neq 0$ τότε $\beta \neq 0$, γιατί τα a, b, c, d είναι πραγματικοί αριθμοί. Επομένως, έχουμε

$$(a+bi+cj+dk)\frac{a - bi - cj - dk}{\beta} = \frac{a - bi - cj - dk}{\beta}(a+bi+cj+dk) = 1.$$

[1] Οι quaternions επινοήθηκαν από τον Hamilton το 1843 (ο οποίος νωρίτερα είχε δώσει την πρώτη περιγραφή του $\mathbb{C}$ χρησιμοποιώντας ζεύγη πραγματικών αριθμών) ως ένα αλγεβρικό σύστημα που περιέχει το $\mathbb{C}$, κατά τρόπο ανάλογο που το $\mathbb{C}$ περιέχει το $\mathbb{R}$. Το ότι ο πολλαπλασιασμός στο $\mathbb{H}$ δεν είναι μεταθετικός και ότι η διάσταση του $\mathbb{H}$ επί του $\mathbb{R}$ είναι 4 και όχι 3 ήταν την εποχή αυτή σημαντικά βήματα. Το $\mathbb{H}$ χρησιμοποιείται στην περιγραφή περιστροφών σε τριδιάστατους και τετραδιάστατους χώρους και έχει πολλές εφαρμογές στη Φυσική.

Το στοιχείο $a - bi - cj - dk$ ονομάζεται συζυγές του $a + bi + cj + dk$ κατά αναλογία με τους μιγαδικούς αριθμούς.

Παρατηρούμε ότι το σύνολο των μιγαδικών $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$ είναι ένας υποδακτύλιος του $\mathbb{H}$.

Σημείωση

Ο $\mathbb{H}$ στο προηγούμενο παράδειγμα είναι ένας δακτύλιος με μοναδιαίο στοιχείο όπου κάθε μη μηδενικό στοιχείο είναι αντιστρέψιμο. Τέτοιοι δακτύλιοι ονομάζονται ***δακτύλιοι με διαίρεση*** (ή ***μη μεταθετικά σώματα***). Είναι προφανές ότι ένας δακτύλιος με διαίρεση δεν είναι κατ΄ ανάγκη σώμα γιατί δεν απαιτείται να είναι μεταθετικός ο πολλαπλασιασμός. Ένα Θεώρημα του Wedderburn λέει ότι κάθε πεπερασμένος δακτύλιος διαίρεσης είναι σώμα. Για μια απόδειξη του θεωρήματος αυτού παραπέμπουμε στο βιβλίο του I. Herstein [14].

Ασκήσεις 2.1

1. Εξετάστε ποιες από τις παρακάτω αντιστοιχίες ορίζουν πράξεις στο A.

   i) $A = \mathbb{Z}$, $a * b = c$, όπου $c = \max\{a, b\}$

   ii) $A = \mathbb{Z}_m$, $[a] * [b] = [c]$, όπου $c = \max\{a, b\}$

   iii) $A = \{f : \mathbb{R} \to \mathbb{R} | f \text{ επί}\}$, $f * g = f \circ g$ (σύνθεση συναρτήσεων)

2. Αποδείξτε ότι οι παρακάτω πράξεις στο A δεν ικανοποιούν την πρώτη ιδιότητα του ορισμού του δακτυλίου.

   i) $A = \mathbb{Z}$, $a \bullet b = a - b$

   ii) $A = \{f : \mathbb{R} \to \mathbb{R}\}$, $f \bullet g = f \circ g - g \circ f$

   iii) $A = M_n(\mathbb{R})$, $B \bullet C = BC - CB$.

3. Εξετάστε αν το S είναι υποδακτύλιος του R. Στις περιπτώσεις που ο S είναι υποδακτύλιος του R εξετάστε αν είναι μεταθετικός, αν έχει μοναδιαίο στοιχείο, αν είναι ακεραία περιοχή, και αν είναι σώμα.

   i) $R = M_2(\mathbb{R})$, $S = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} \in M_2(\mathbb{R}) \right\}$.

   ii) $R = M_2(\mathbb{R})$, $S = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \in M_2(\mathbb{R}) \right\}$.

   iii) $R = \mathbb{Z}[\sqrt{2}]$, $S = \{a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] | b \text{ άρτιος}\}$.

   iv) $R = \mathbb{Z}[\sqrt{2}]$, $S = \{a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] | a, b \text{ άρτιοι}\}$.

v) $R = \mathbb{Z}[i]$, $S = \{a + bi \in \mathbb{Z}[i] | a \equiv b \equiv 0 \mod 10\}$.

vi) $R = \mathbb{H}$, $S = \{a + bi + cj + dk \in \mathbb{H} | a, b, c, d \in \mathbb{Q}\}$.

vii) $R = \mathbb{H}$, $S = \{a + bi + cj + dk \in \mathbb{H} | a, b, c, d \in \mathbb{Z},\ a \text{ άρτιος}\}$.

viii) $R = F(\mathbb{R}, \mathbb{R})$, $S = \{f : \mathbb{R} \to \mathbb{R} | f(1) = 0\}$.

ix) $R = F(\mathbb{R}, \mathbb{R})$, $S = \{f : \mathbb{R} \to \mathbb{R} | f(1) = 1\}$.

x) $R = \mathbb{Z}_{12}$, $S = \{[0], [4], [8]\}$.

xi) $R = \mathbb{Z}_{mn}$, $S = \{[kn] | k \in \mathbb{Z}\}$.

4. i) Έστω R_i, $i \in I$, υποδακτύλιοι του δακτυλίου R. Αποδείξτε ότι η τομή $\bigcap_{i \in I} R_i$ είναι ένας υποδακτύλιος του R.

   ii) Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Αποδείξτε ότι η τομή όλων των υποδακτυλίων του R που περιέχουν το 1_R είναι ο υποδακτύλιος $\{n1_R | n \in \mathbb{Z}\}$. Για τον λόγο αυτό, ο δακτύλιος αυτός είναι ο μικρότερος υποδακτύλιος του R που περιέχει το 1_R.

   iii) Αποδείξτε ότι η ένωση $2\mathbb{Z} \cup 3\mathbb{Z}$ δεν είναι υποδακτύλιος του $\mathbb{Z}$.

5. Αποδείξτε ότι κάθε υποδακτύλιος του $\mathbb{Z}$ είναι της μορφής $m\mathbb{Z}$, $m \in \mathbb{Z}$.

6. Βρείτε ένα m τέτοιο ώστε $m\mathbb{Z} = 12\mathbb{Z} \cap 18\mathbb{Z}$. Αποδείξτε ότι $a\mathbb{Z} \cap b\mathbb{Z} = e\mathbb{Z}$, όπου οι a, b είναι θετικοί ακέραιοι και $e = \varepsilon\kappa\pi(a, b)$.

7. Έστω R ένας δακτύλιος. Το ***κέντρο*** του R είναι το σύνολο $C(R) = \{a \in R | ar = ra \text{ για κάθε } r \in R\}$.

   i) Αποδείξτε ότι $C(R) = R$ αν και μόνο αν ο R είναι μεταθετικός.

   ii) Αποδείξτε ότι το $C(R)$ είναι υποδακτύλιος του R.

   iii) Αποδείξτε ότι $C(M_2(\mathbb{R})) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in M_2(\mathbb{R}) \right\}$.

   iv) Ποιο είναι το κέντρο του $M_n(\mathbb{R})$;

8. Ποιο είναι το κέντρο των quaternions;

9. Έστω R ένας δακτύλιος τέτοιος ώστε για κάθε $r \in R$, ισχύει $r^2 + r \in C(R)$ (βλ. Άσκηση 7). Αποδείξτε ότι ο R είναι μεταθετικός.
   Υπόδειξη: Θεωρώντας το στοιχείο $(r + s)^2 + (r + s)$, αποδείξτε πρώτα ότι $rs + sr \in C(R)$ για κάθε $r, s \in R$.

10. Έστω R, S δύο δακτύλιοι.

i) Αποδείξτε ότι ο $R \times S$ είναι μεταθετικός αν και μόνο αν οι R, S είναι μεταθετικοί.

ii) Αποδείξτε ότι ο $R \times S$ έχει μοναδιαίο στοιχείο αν και μόνο αν οι R, S έχουν μοναδιαία στοιχεία.

iii) Αληθεύει ότι το καρτεσιανό γινόμενο δύο ακεραίων περιοχών (αντίστοιχα, σωμάτων) είναι ακεραία περιοχή (αντίστοιχα, σώμα);

11. Έστω R ένας δακτύλιος. Αποδείξτε ότι οι ακόλουθες συνθήκες είναι ισοδύναμες.

i) ο R είναι μεταθετικός

ii) $(a+b)^2 = a^2 + 2ab + b^2$ για κάθε $a, b \in R$

iii) $(a-b)^2 = a^2 - 2ab + b^2$ για κάθε $a, b \in R$

iv) $a^2 - b^2 = (a+b)(a-b)$ για κάθε $a, b \in R$.

12. Έστω R ένας δακτύλιος τέτοιος ώστε $a^2 = a$ για κάθε $a \in R$. Αποδείξτε ότι για κάθε $a \in R$ ισχύει $2a = 0$ και ότι ο R είναι μεταθετικός. (Παραδείγματα τέτοιων δακτυλίων είναι ο $\mathbb{Z}_2 \times \mathbb{Z}_2$ και ο δακτύλιος του Boole).

13. Έστω R, S δύο δακτύλιοι με μοναδιαία στοιχεία. Αποδείξτε ότι $U(R \times S) = U(R) \times U(S)$. Πόσα αντιστρέψιμα στοιχεία περιέχει ο δακτύλιος $\mathbb{Z}_{60} \times \mathbb{Z}_{10}$;

14. Έστω $R = \left\{ \begin{pmatrix} [a] & [b] \\ [0] & [c] \end{pmatrix} \in M_2(\mathbb{Z}_m) \right\}$.

i) Αποδείξτε ότι το R είναι υποδακτύλιος του $M_2(\mathbb{Z}_m)$.

ii) Είναι ο R μεταθετικός;

iii) Αποδείξτε ότι $\begin{pmatrix} [a] & [b] \\ [0] & [c] \end{pmatrix} \in U(R) \Leftrightarrow [a], [c] \in U(\mathbb{Z}_m)$.

iv) Αποδείξτε ότι ο πληθάριθμος του $U(R)$ είναι $m\varphi(m)^2$.

15. i) Ποιά είναι τα αντιστρέψιμα στοιχεία του δακτυλίου
$$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{Z}) \right\} ;$$

ii) Για ποιά $m \in \mathbb{Z}$ το $\begin{pmatrix} 2 & m \\ 3 & m \end{pmatrix}$ είναι αντιστρέψιμο στο $M_2(\mathbb{Z})$; Στο $M_2(\mathbb{R})$;

iii) Αληθεύει ότι $U(M_2(\mathbb{Z})) = U(M_2(\mathbb{R}))$;

16. Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και $a, b \in R$ με a αντιστρέψιμο και $b^2 = 0$. Αποδείξτε ότι το $a + b$ είναι αντιστρέψιμο.

17. Έστω $F = \{0, e, a, b\}$ με πράξεις που ορίζονται από τους πίνακες

$+$	0	e	a	b
0	0	e	a	b
e	e	0	b	a
a	a	b	0	e
b	b	a	e	0

$\cdot$	0	e	a	b
0	0	0	0	0
e	0	e	a	b
a	0	a	b	e
b	0	b	e	a

Υποθέτοντας ότι ο F είναι δακτύλιος, αποδείξτε ότι είναι σώμα.

18. Αν ο $R = \{r, s, t\}$ είναι δακτύλιος και γνωρίζουμε τα παρακάτω τμήματα των πινάκων των πράξεων, συμπληρώστε τους πίνακες αυτούς.

$+$	r	s	t
r	r	s	
s	s	t	
t	t	r	s

$\cdot$	r	s	t
r	r	r	
s	r	s	t
t	r		

19. Έστω S ένας υποδακτύλιος του δακτυλίου R.

    i) Δώστε ένα παράδειγμα που ο R έχει μοναδιαίο στοιχείο ενώ ο S δεν έχει.

    ii) Δώστε ένα παράδειγμα που οι R, S έχουν διαφορετικά μοναδιαία στοιχεία.

    iii) Αποδειξτε ότι $1_R = 1_S$, αν οι R, S είναι ακέραιες περιοχές.

20. Έστω $d \in \mathbb{N}$. Αποδείξτε ότι το σύνολο $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \in \mathbb{C} | a, b \in \mathbb{Q}\}$ με τις συνήθεις πράξεις μιγαδικών αριθμών είναι ένα σώμα.

21. Εξηγήστε γιατί ο δακτύλιος των συνεχών συναρτήσεων $f : \mathbb{R} \to \mathbb{R}$ με πράξεις $(f+g)(x) = f(x)+g(x)$ και $(fg)(x) = f(x)g(x)$ δεν είναι ακεραία περιοχή.

22. Αποδείξτε ότι στο δακτύλιο των quaternions $\mathbb{H}$ η εξίσωση $x^2 = -1$ έχει άπειρες λύσεις. Πόσες λύσεις έχει στο $\mathbb{H}$ η εξίσωση $x^2 = x$;

23. i) Αποδείξτε ότι κάθε υπόσωμα του $\mathbb{C}$ περιέχει το $\mathbb{Q}$.

    ii) Ποιά είναι η τομή των υποσωμάτων $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \in \mathbb{R} | a, b \in \mathbb{Q}\}$ και $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} \in \mathbb{R} | a, b \in \mathbb{Q}\}$;

24. Έστω $R = \left\{ \dfrac{m}{2^a 3^b} \middle| m \in \mathbb{Z}, a, b \in \mathbb{N} \right\}$.

    i) Αποδείξτε ότι το R είναι ένας υποδακτύλιος του $\mathbb{Q}$.

    ii) Είναι ο R ακεραία περιοχή;

    iii) Αποδείξτε ότι ο R περιέχεται σε κάθε υποδακτύλιο του $\mathbb{Q}$ που περιέχει τα στοιχεία $\dfrac{1}{2}$ και $\dfrac{1}{3}$.

    iv) Αποδείξτε ότι $\dfrac{1}{5} \notin R$.

    v) Αληθεύει ότι ο R είναι σώμα;

    vi) Αληθεύει ότι $\mathbb{Z} \subseteq R$;

25. Έστω R ένας υποδακτύλιος ενός σώματος και $m, n \in \mathbb{N}$ με $\mu\kappa\delta(m, n) = 1$. Αν $a, b \in R$ είναι τέτοια ώστε $a^m = b^m$ και $a^n = b^n$, αποδείξτε ότι $a = b$. Που χρησιμοποιήσατε την υπόθεση ότι ο R περιέχεται σε σώμα ;

26. Ένα στοιχείο r ενός δακτυλίου R ονομάζεται μηδενοδύναμο αν $r^n = 0$ για κάποιο θετικό ακέραιο n.

    i) Αποδείξτε ότι αν ο R περιέχει μοναδιαίο στοιχείο και το r είναι μηδενοδύναμο, τότε το $1 - r$ είναι αντιστρέψιμο.
    Υπόδειξη: Θεωρήστε τη γεωμετρική σειρά.

    ii) Αποδείξτε ότι αν ο R είναι μεταθετικός, τότε το άθροισμα δύο μηδενοδύναμων στοιχείων είναι μηδενοδύναμο.
    Υπόδειξη: Αν $r^n = s^m = 0$, αποδείξτε ότι $(r+s)^{m+n-1}$ με τη βοήθεια του διωνυμικού αναπτύγματος, Παράδειγμα 2.1.12.

27. Αποδείξτε ότι κάθε πεπερασμένος μεταθετικός δακτύλιος που δεν έχει μηδενοδιαιρέτες περιέχει μοναδιαίο στοιχείο και είναι σώμα.

28. Αποδείξτε ότι το πλήθος των αντιστρέψιμων στοιχείων του δακτυλίου $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} | a, b \in \mathbb{Z}\}$ είναι άπειρο.
    Υπόδειξη: Τα στοιχεία $(3 + 2\sqrt{2})^n$, $n \in \mathbb{N}$, είναι αντιστρέψιμα.

29. Αποδείξτε ότι αν στο δακτύλιο R το $1 - ab$ είναι αντιστρέψιμο, τότε και το $1 - ba$ είναι αντιστρέψιμο.
    Υπόδειξη: Και εδώ η θεώρηση της γεωμετρικής σειράς βοηθάει.

30. Έστω R ένας δακτύλιος τέτοιος ώστε $x^3 = x$ για κάθε $x \in R$. Αποδείξτε ότι ο R είναι μεταθετικός.

2.2 Πολυώνυμα και Πολυωνυμικές Συναρτήσεις

Στις επόμενες τρεις Παραγράφους θα μελετήσουμε το δακτύλιο $R[x]$ των πολυωνύμων μιας μεταβλητής των οποίων οι συντελεστές ανήκουν σε τυχαίο δακτύλιο R. Θα διαπιστώσουμε ότι πολλές ιδιότητες του $R[x]$ καθορίζονται από τον R. Στην ειδική περίπτωση που ο R είναι σώμα, για παράδειγμα το $\mathbb{Q},$, $\mathbb{R}$, $\mathbb{C}$ ή το $\mathbb{Z}_p$, όπου το p είναι πρώτος, θα δούμε ότι ο δακτύλιος $R[x]$ έχει αλγεβρικές ιδιότητες παρόμοιες με αυτές του $\mathbb{Z}$ που μελετήσαμε στην Ενότητα 1, όπως είναι ο αλγόριθμος διαίρεσης και η μονοσήμαντη ανάλυση σε γινόμενο πρώτων.

Πολυώνυμα

Από τα μαθητικά μας χρόνια είμαστε εξοικειωμένοι με πολυώνυμα που έχουν πραγματικούς συντελεστές. Γνωρίζουμε πως να προσθέτουμε και να πολλαπλασιάζουμε τέτοια πολυώνυμα. Για παράδειγμα αν $f(x) = 2x^2 - x + 5$ και $g(x) = x - 1$, τότε $f(x) + g(x) = 2x^2 + 4$ και $f(x)g(x) = 2x^3 - 2x^2 - x^2 + x + 5x - 5 = 2x^3 - 3x^2 + 6x - 5$.

Ξεκινώντας τώρα από τυχαίο δακτύλιο R που έχει μοναδιαίο στοιχείο θα κατασκευάσουμε το σύνολο των πολυωνύμων που έχουν συντελεστές από το R, το οποίο συμβολίζουμε με $R[x]$. Θα ορίσουμε σε αυτό δύο πράξεις χρησιμοποιώντας τις αντίστοιχες πράξεις του R, έτσι ώστε το $R[x]$ να γίνεται δακτύλιος με μοναδιαίο στοιχείο και να περιέχει το R ως υποδακτύλιο.

2.2.1 Θεώρημα. *Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο 1_R. Τότε υπάρχει δακτύλιος $\mathcal{R}$ με μοναδιαίο στοιχείο το 1_R που περιέχει το R ως υποδακτύλιο και έχει τις εξής ιδιότητες:*

- *Υπάρχει στοιχείο $x \in \mathcal{R}$ τέτοιο ώστε $rx = xr$ για κάθε $r \in R$.*
- *Κάθε στοιχείο του $\mathcal{R}$ έχει μια παράσταση της μορφής*

$$r_0 + r_1x + r_2x^2 + \cdots + r_nx^n,$$

όπου $n \in \mathbb{N}$ και $r_i \in R$ για κάθε i.

- *Αν*

$$r_0 + r_1x + r_2x^2 + \cdots + r_nx^n = s_0 + s_1x + s_2x^2 + \cdots + s_mx^m$$

με $n, m \in \mathbb{N}$, $n \leq m$ και $r_i, s_j \in R$ για κάθε i και j, τότε $r_i = s_i$ για κάθε $i \leq n$ και $s_j = 0_R$ για κάθε $j > n$.

Θα συμβολίζουμε τον δακτύλιο $\mathcal{R}$ με $R[x]$.

Θα δώσουμε την απόδειξη του Θεωρήματος στο Παράρτημα 6.3, γιατί αυτή δε βοηθά άμεσα το σκοπό μας που είναι η μελέτη των ιδιοτήτων πολυωνύμων.

Το ειδικό στοιχείο $x \in R$ ονομάζεται ***μεταβλητή*** και τα στοιχεία του $R[x]$ ονομάζονται ***πολυώνυμα*** της μεταβλητής x με συντελεστές από τον R. Τα στοιχεία του $R[x]$ συμβολίζονται με $f(x), g(x) \ldots$. Τα πολυώνυμα της μορφής rx^i ονομάζονται ***μονώνυμα***. Ο $R[x]$ ονομάζεται ο ***δακτύλιος των πολυωνύμων*** της μεταβλητής x με συντελεστές από το R.

Τονίζουμε εδώ ότι το x είναι ένα *συγκεκριμένο στοιχείο* του δακτυλίου $R[x]$. Η χρήση του όρου "μεταβλητή" για αυτό είναι διαφορετική με την έννοια της μεταβλητής που υπάρχει στις απεικονίσεις. Θα επανέλθουμε στο σημείο αυτό λίγο παρακάτω όταν μελετήσουμε πολυωνυμικές συναρτήσεις.

Επειδή ο R είναι υποδακτύλιος του $R[x]$, έχουμε $0_{R[x]} = 0_R$. Το στοιχείο αυτό θα το συμβολίζουμε συχνά με 0. Επειδή ο $R[x]$ είναι δακτύλιος, ισχύει $0_R x^i = 0_R$. Συνεπώς μπορούμε να παραλείπουμε ή να παρεμβάλλουμε όρους της μορφής $0_R x^i$ στην παράσταση κάθε πολυωνύμου ως άθροισμα μονωνύμων. Επομένως αν $f(x)$, $g(x)$ είναι τυχαία στοιχεία του $R[x]$, μπορούμε να γράψουμε $f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n$ και $g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_n x^n$ αν αυτό κρίνεται σκόπιμο.

Στο $R[x]$ έχουμε

$$(f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n) + (g_0 + g_1 x + g_2 x^2 + \cdots + g_n x^n) = (f_0 + g_0) + (f_1 + g_1)x + (f_2 + g_2)x^2 + \cdots + (f_n + g_n)$$

και

$$(f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n)(g_0 + g_1 x + g_2 x^2 + \cdots + g_m x^m) = (f_0 g_0) + (f_0 g_1 + f_1 g_0)x + \cdots + c_i x^i + \cdots + (f_n g_m)x^{n+m}, \qquad (1)$$

όπου για κάθε i έχουμε $c_i = f_0 g_i + f_1 g_{i-1} + f_2 g_{i-2} + \cdots + f_{i-1} g_1 + f_i g_0$.

2.2.2 Παρατήρηση. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Είναι φανερό ότι αν ο R είναι μεταθετικός, τότε και ο $R[x]$ είναι μεταθετικός.

Αν $f(x) \in R[x]$ και $f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n$ με $f_n \neq 0_R$, τότε λέμε ότι ο ***βαθμός*** του $f(x)$ είναι n. Επομένως τα πολυώνυμα βαθμού 0 στο $R[x]$ έχουν τη μορφή $f(x) = c$, όπου $c \in R$ και $c \neq 0_R$. Τα πολυώνυμα βαθμού 0 μαζί με το μηδενικό πολυώνυμο ονομάζονται ***σταθερά*** πολυώνυμα.

Δεχόμαστε εξ ορισμού ότι ο βαθμός του μηδενικού πολυωνύμου $f(x) = 0_R$ είναι $-\infty$. Επίσης δεχόμαστε ότι $-\infty < n$ για κάθε φυσικό αριθμό n. Αυτό μας επιτρέπει κάποια οικονομία στις διατυπώσεις προτάσεων. Για παράδειγμα, όταν

λέμε "έστω πολυώνυμο $f(x)$ βαθμού μικρότερου ή ίσου του 1", εννούμε ότι το $f(x)$ έχει βαθμό 1 ή 0, ή ότι είναι το μηδενικό πολυώνυμο.

Αν $f(x) \in R[x]$, $f(x) = f_0+f_1x+f_2x^2+\cdots+f_nx^n$ και $f_n \neq 0_R$, ονομάζουμε ***μεγιστοβάθμιο συντελεστή*** του $f(x)$ τον f_n. Το f_0 ονομάζεται ***σταθερός όρος*** του $f(x)$.

2.2.3 Παρατήρηση. *Από τον ορισμό της πρόσθεσης πολυωνύμων προκύπτει ότι*

$$\deg(f(x)+g(x)) \leq \max\{\deg f(x), \deg g(x)\}.$$

Αναφέραμε στην εισαγωγή της Παραγράφου αυτής ότι πολλές αλγεβρικές ιδιότητες του $R[x]$ καθορίζονται από το R. Σχετική είναι η παρακάτω Πρόταση.

2.2.4 Πρόταση. *Έστω R μια ακεραία περιοχή. Τότε*

1) Ο $R[x]$ είναι ακεραία περιοχή.

2) Αν $f(x), g(x) \in R[x]$ είναι μη μηδενικά πολυώνυμα, τότε

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$$

3) Τα αντιστρέψιμα στοιχεία του $R[x]$ είναι τα αντιστρέψιμα στοιχεία του R, δηλαδή $U(R[x]) = U(R)$. Ιδιαίτερα, τα αντιστρέψιμα στοιχεία του $F[x]$, όπου το F είναι ένα σώμα, είναι ακριβώς τα μη μηδενικά στοιχεία του F.

Απόδειξη.

1. Επειδή ο R είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, έχουμε ότι ο $R[x]$ είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Επίσης $1_{R[x]} = 1_R \neq 0_R = 0_{R[x]}$. Έστω $f(x), g(x) \in R[x]$ μη μηδενικά πολυώνυμα. Τότε $f(x) = r_0+r_1x+r_2x^2+\cdots+r_nx^n$ και $g(x) = s_0+s_1x+s_2x^2+\cdots+s_mx^m$ με $r_n \neq 0$ και $s_m \neq 0$. Έχουμε $f(x)g(x) = (r_0s_0) + (r_0s_1 + r_1s_0)x + \cdots + (r_ns_m)x^{n+m}$. Επειδή ο R δεν έχει μηδενοδιαιρέτες ισχύει $r_ns_m \neq 0$ και συνεπώς $f(x)g(x) \neq 0$. Επομένως ο $R[x]$ δεν έχει μηδενοδιαιρέτες.

2. Από τα παραπάνω έχουμε $\deg(f(x)g(x)) = m + n =$ $deg f(x) + \deg g(x)$.

3. Αν το $f(x)$ είναι αντιστρέψιμο στοιχείο του $R[x]$, τότε $f(x)g(x) = 1_R$ για κάποιο $g(x) \in R[x]$. Τα $f(x)$ και $g(x)$ είναι μη μηδενικά (γιατί $1_R \neq 0_R$). Από το 2) της Πρότασης έχουμε $0 = \deg((f(x)g(x)) = \deg f(x) + \deg g(x)$ και άρα $\deg f(x) = \deg g(x) = 0$. Συνεπώς τα $f(x)$ και $g(x)$ είναι αντιστρέψιμα στοιχεία του R. ⊤

2.2.5 Σημειώσεις. 1) Για τυχαίο δακτύλιο R με μοναδιαίο στοιχείο είναι φανερό ότι ισχύει

$$\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x) \quad \text{για κάθε} \quad f(x), g(x) \in R[x].$$

Αν ο R έχει μηδενοδιαιρέτες, είναι δυνατόν να ισχύει $\deg(f(x)g(x)) < \deg f(x) + \deg g(x)$. Για παράδειγμα, έστω $f(x) = 2x+1 \in \mathbb{Z}_6[x]$ και $g(x) = 3x+1 \in \mathbb{Z}_6[x]$. Τότε το γινόμενο $f(x)g(x) = 6x^2 + 5x + 1 = 5x + 1$ έχει βαθμό 1.
2) Επίσης, αν ο R έχει μηδενοδιαιρέτες, είναι δυνατόν να έχουμε $U(R[x]) \neq U(R)$. Για παράδειγμα, στο $\mathbb{Z}_4[x]$ έχουμε $(2x+1)^2 = 1$. Άρα $2x+1 \in U(\mathbb{Z}_4[x])$. Γενικά ισχύει $U(R) \subseteq U(R[x])$.

Πολυωνυμικές συναρτήσεις

Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Αν $f(x) \in R[x]$, όπου $f(x) = f_0 + f_1x + \cdots + f_nx^n$, και $r \in R$ θέτουμε $f(r) = f_0 + f_1r + \cdots + f_nr^n$. Ορίζεται έτσι μια συνάρτηση που συμβολίζουμε με $\bar{f}$,

$$\bar{f} : R \to R, \quad r \mapsto f(r),$$

η οποία ονομάζεται η ***πολυωνυμική συνάρτηση*** που επάγεται από το $f(x)$ στο R.

2.2.6 Παρατήρηση. Εύκολα διαπιστώνουμε ότι για κάθε $f(x), g(x) \in R[x]$ και κάθε $r \in R$ ισχύουν

- $(f + g)(r) = f(r) + g(r)$, και
- $(fg)(r) = f(r)g(r)$.

Οι παραπάνω δύο ιδιότητες μας επιτρέπουν να "αντικαταστήσουμε το x με το r" σε ισότητες πολυωνύμων. Για παράδειγμα, αν στο $R[x]$ ισχύει $f(x) = q(x)g(x) + h(x)$, τότε για κάθε $r \in R$ έχουμε $f(r) = q(r)g(r) + h(r)$.

Σημείωση Είναι πολύ πιθανό να είχαμε συνηθίσει στα μαθητικά μας χρόνια να ταυτίζουμε ένα πολυώνυμο $f(x) \in \mathbb{R}[x]$ με την αντίστοιχη πολυωνυμική συνάρτηση $\bar{f} : \mathbb{R} \to \mathbb{R}$. Το παρακάτω παράδειγμα δείχνει ότι αυτό δεν είναι πάντα επιτρεπτό για τυχαίο R στη θέση του $\mathbb{R}$. Είναι προφανές ότι ίσα πολυώνυμα στο $R[x]$ επάγουν την ίδια πολυωνυμική συνάρτηση στο R. Όμως, είναι δυνατόν *διαφορετικά* πολυώνυμα να επάγουν την ίδια πολυωνυμική συνάρτηση.

2.2.7 Παράδειγμα. Έστω $R = \mathbb{Z}_3$ και $f(x), g(x) \in \mathbb{Z}_3[x]$ όπου $f(x) = x^3 + x$ και $g(x) = 2x$. Μετά από υπολογισμούς στο $\mathbb{Z}_3$ βλέπουμε ότι[1] $f(0) = 0 = g(0)$,

[1] Από εδώ και στο εξής, το στοιχείο $[a] \in \mathbb{Z}_n$ θα συμβολίζεται απλούστερα $a \in \mathbb{Z}_n$, αν δεν υπάρχει πρόβλημα σύγχυσης.

$f(1) = 2 = g(1)$ και $f(2) = 1 = g(2)$, δηλαδή $f(s) = g(s)$ για κάθε $s \in \mathbb{Z}_3$. Άρα, οι πολυωνυμικές συναρτήσεις $\bar{f} : \mathbb{Z}_3 \to \mathbb{Z}_3$, $\bar{g} : \mathbb{Z}_3 \to \mathbb{Z}_3$ είναι ίσες, αν και τα πολυώνυμα $f(x)$, $g(x)$ δεν είναι ίσα. (Ένα κριτήριο που μας πληροφορεί πότε δύο πολυωνυμικές συναρτήσεις $F \to F$ είναι ίσες, όπου το F είναι ένα σώμα, εξετάζεται στην επόμενη Παράγραφο).

Μια ευθεία καθορίζεται από δύο διακεκριμένα σημεία της. Σύμφωνα με το επόμενο αποτέλεσμα, ένα πολυώνυμο $f(x)$ βαθμού n με συντελεστές από ένα σώμα καθορίζεται από $n+1$ τιμές του $f(a_1), \ldots, f(a_{n+1})$ όπου τα a_i είναι διακεκριμένα.

2.2.8 Θεώρημα (*Παρεμβολή του* Lagrange). *Έστω F ένα σώμα και $a_1, a_2, \ldots, a_n$ διακεκριμένα στοιχεία του F, όπου n είναι ένας θετικός ακέραιος. Έστω $b_1, b_2, \ldots, b_n$ στοιχεία του F. Τότε υπάρχει ένα πολυώνυμο $f(x) \in F[x]$ βαθμού το πολύ $n-1$ τέτοιο ώστε $f(a_i) = b_i$ για κάθε i. Το $f(x)$ είναι μοναδικό ως προς τις ιδιότητες αυτές.*

Απόδειξη. Θεωρούμε το $n \times n$ γραμμικό σύστημα

$$\begin{aligned} x_{n-1}a_1^{n-1} + \cdots + x_1 a_1^1 + x_0 a_1^0 &= b_1 \\ &\cdots \\ x_{n-1}a_n^{n-1} + \cdots + x_1 a_n^1 + x_0 a_n^0 &= b_n, \end{aligned}$$

με αγνώστους τους x_i. Οι συντελεστές ανήκουν στο F. Η ορίζουσα των συντελεστών είναι η

$$\begin{vmatrix} a_1^{n-1} & \cdots & a_1^1 & a_1^0 \\ & \cdots & & \\ a_n^{n-1} & \cdots & a_n^1 & a_n^0 \end{vmatrix}.$$

Από τη Γραμμική Άλγεβρα υπενθυμίζουμε ότι η ορίζουσα αυτή (που είναι γνωστή ως ορίζουσα του Vandermonde) ισούται με το γινόμενο $\prod_{i<j}(a_i - a_j)$. (Βλ. και την Παράγραφο 3.4). Από την υπόθεση έπεται ότι $\prod_{i<j}(a_i - a_j) \neq 0$ και κατά συνέπεια το σύστημα έχει (μοναδική) λύση, έστω την $(x_{n-1}, \ldots, x_1, x_0) = (f_{n-1}, \ldots, f_1, f_0)$. Θέτουμε $f(x) = f_{n-1}x^{n-1} + \cdots + f_1 x + f_0 \in F[x]$. Τότε έχουμε $f(a_i) = b_i$ για κάθε i.

Έστω ότι υπάρχει και άλλο $g(x) \in F[x]$ με $\deg g(x) \leq n-1$ και $g(a_i) = b_i$ για κάθε i. Αν $g(x) = g_{n-1}x^{n-1} + \cdots + g_1 x + g_0$, τότε μία λύση του συστήματος είναι η $(g_{n-1}, \ldots, g_1, g_0)$. Επειδή η λύση του συστήματος είναι μοναδική συμπεραίνουμε ότι $f(x) = g(x)$. ⊤

2.2.9 Πόρισμα. *Έστω F ένα πεπερασμένο σώμα και $g : F \to F$ μια απεικόνιση. Τότε υπάρχει πολυώνυμο $f(x) \in F[x]$ τέτοιο ώστε $\bar{f} = g$.*

Απόδειξη. Έστω $F = \{a_1, \ldots, a_n\}$ και $b_i = g(a_i)$, $i = 1, \ldots n$. Τότε από το προηγούμενο Θεώρημα, υπάρχει $f(x) \in F[x]$ τέτοιο ώστε $f(a_i) = b_i = g(a_i)$, $i = 1, \ldots, n$. ⊺

Σύμφωνα με το προηγούμενο Πόρισμα, κάθε απεικόνιση από ένα πεπερασμένο σώμα F στον εαυτό του είναι πολυωνυμική. Για άπειρα σώματα το συμπέρασμα αυτό δεν αληθεύει. Για παράδειγμα, η εκθετική απεικόνιση $\mathbb{R} \to \mathbb{R}$, $x \mapsto e^x$, δεν είναι πολυωνυμική (γιατί;).

Χρησιμοποιώντας το συμβολισμό του Θεωρήματος 2.2.8, αποδεικνύεται ότι το μοναδικό $f(x)$ με $\deg f(x) \leq n-1$ που έχει την ιδιότητα $f(a_i) = b_i$, $i = 1, \ldots, n$ είναι το

$$f(x) = \sum_{i=1}^{n} b_i \frac{(x-a_1)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_n)}{(a_i-a_1)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_n)}.$$

Πράγματι, το πολυώνυμο του δεξιού μέλους έχει βαθμό το πολύ $n-1$ και παίρνει τις τιμές b_i όταν το x αντικατασταθεί με το a_i, $i = 1, \ldots, n$. Από τη μοναδικότητα, το πολυώνυμο αυτό ταυτίζεται με το $f(x)$. (Επισημαίνουμε ότι η παραπάνω παράσταση του πολυωνύμου αυτού προκύπτει από τον κανόνα του Cramer στην επίλυση γραμμικών συστημάτων)

Πολυώνυμα πολλών μεταβλητών

Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο και $S = R[x]$. Εφαρμόζοντας το Θεώρημα 2.2.1 για το S στη θέση του R λαμβάνουμε το δακτύλιο του οποίου τα στοιχεία είναι της μορφής $f_n(x)y^n + \cdots + f_1(x)y + f_0(x)$, όπου $f_i(x) \in R[x]$. Αντικαθιστώντας τα $f_i(x)$ βλέπουμε ότι το τυχαίο στοιχείο του $S[y]$ είναι της μορφής

$$\sum_{i=0,j=0}^{m,n} r_{ij}x^iy^j = r_{00} + \cdots + r_{ij}x^iy^j + \cdots + r_{mn}x^my^n,$$

όπου $r_{ij} \in R$. Ο δακτύλιος $S[y]$ συμβολίζεται με $R[x,y]$ και ονομάζεται δακτύλιος των πολυωνύμων στις μεταβλητές x, y με συντελεστές από το R. Ο συνήθης συμβολισμός για τα στοιχεία του είναι $f(x,y) = \sum_{i=0,j=0}^{m,n} r_{ij}x^iy^i$. Ο δακτύλιος $R[x] = S$ είναι προφανώς υποδακτύλιος του $S[y] = R[x,y]$.

Με ανάλογο τρόπο κατασκευάζεται ο δακτύλιος $R[x_1, \ldots, x_n]$ των πολυωνύμων στις μεταβλητές $x_1, \ldots, x_n$ με συντελεστές από το R. Η θεωρία των πολυωνυμικών δακτυλίων πολλών μεταβλητών $R[x_1, \ldots, x_n]$ αποτελεί μια ευρεία περιοχή της Άλγεβρας και είναι το κεντρικό θέμα της Αλγεβρικής Γεωμετρίας

και της Μεταθετικής Άλγεβρας. Έχει δε και αξιοσημείωτες εφαρμογές σε άλλους τομείς των Μαθηματικών όπως είναι τα Υπολογιστικά Μαθηματικά και η Θεωρία Κωδίκων.

Ασκήσεις 2.2

Στις παρακάτω ασκήσεις υποθέτουμε ότι όλοι οι δακτύλιοι περιέχουν μοναδιαίο στοιχείο.

1. Δείξτε με παράδειγμα ότι είναι δυνατο να ισχύει $\deg(f(x)+g(x)) < \max\{\deg f(x), \deg g(x)\}$.

2. Βρείτε ένα $f(x) \in \mathbb{Z}_{10}[x]$ τέτοιο ώστε $\deg((2x+1)f(x)) = \deg f(x)$.

3. Αν ο R είναι μία ακεραία περιοχή γνωρίζουμε ότι $U(R[x]) = U(R)$. Δώστε ένα παράδειγμα ενός δακτυλίου R τέτοιο ώστε $U(R[x]) \neq U(R)$.

4. Έστω R ένας δακτύλιος και S ένας υποδακτύλιος του R. Αποδείξτε ότι ο $S[x]$ είναι ένας υποδακτύλιος του $R[x]$.

5. Ποια από τα παρακάτω σύνολα είναι υποδακτύλιοι του $\mathbb{Z}[x]$;

   i) $\{f(x) \in \mathbb{Z}[x] | f(1) = 0\}$
   ii) $\{f(x) \in \mathbb{Z}[x] | f(1) = 2\}$
   iii) $\{f(x) \in \mathbb{Z}[x] | f(1)$ άρτιος$\}$
   iv) $\{f(x) \in \mathbb{Z}[x] | \deg f(x) \leq 10\}$

6. Πόσα πολυώνυμα στο $\mathbb{Z}_2[x]$ έχουν βαθμό 2; Πόσα πολυώνυμα στο $\mathbb{Z}_2[x]$ έχουν βαθμό μικρότερο ή ίσο του 100;

7. Αποδείξτε ότι κάθε υποδακτύλιος του $F[x]$, όπου F είναι σώμα, είναι άπειρο σύνολο, αν αυτός περιέχει τουλάχιστον ένα πολυώνυμο θετικού βαθμού.

8. Αν το πολυώνυμο $a_n x^n + \cdots + a_1 x + a_0 \in R[x]$, όπου $a_n \neq 0$, είναι μηδενοδιαιρέτης, τότε το $a_n \in R$ είναι μηδενοδιαιρέτης.

9. Αποδείξτε ότι στο $\mathbb{Z}_4[x]$ υπάρχουν αντιστρέψιμα πολυώνυμα θετικού βαθμού. Βρείτε απείρου πλήθους τέτοια πολυώνυμα.
   Υπόδειξη: $(2x+1)^2 = (4x^2+4x+1) = 1$.

10. Έστω R ένας μεταθετικός δακτύλιος. Αποδείξτε ότι το $ax+b \in R[x]$ είναι αντιστρέψιμο αν και μόνο αν το b είναι αντιστρέψιμο στο R και το a είναι μηδενοδύναμο στο R (βλ. Άσκηση 2.1.26).

11. Αποδείξτε ότι αν ο p είναι πρώτος, τότε $(f(x))^p = f(x^p)$ για κάθε $f(x) \in \mathbb{Z}_p[x]$.
Υπόδειξη: Βλ. Παράδειγμα 2.1.12 2).

12. Είναι δυνατόν ο δακτύλιος $R[x]$ να είναι σώμα;

13. i) Αποδείξτε ότι το $x^3 - x \in \mathbb{Z}_6[x]$ επάγει τη μηδενική συνάρτηση $\mathbb{Z}_6 \to \mathbb{Z}_6$.

    ii) Για κάθε πρώτο αριθμό p, αποδείξτε ότι το πολυώνυμο $x^p - x \in \mathbb{Z}_p[x]$ επάγει τη μηδενική συνάρτηση $\mathbb{Z}_p \to \mathbb{Z}_p$. Ποιά συνάρτηση επάγει το $x^{p-1} - 1 \in \mathbb{Z}_p$;
    Υπόδειξη: Μικρό Θεώρημα του Fermat.

14. i) Έστω $f(x, y) \in \mathbb{Q}[x, y]$ του οποίου ο σταθερός όρος ισούται με 0. Αποδείξτε ότι υπάρχουν $g(x, y), h(x, y) \in \mathbb{Q}[x, y]$ τέτοια ώστε $f(x, y) = xg(x, y) + yh(x, y)$.

    ii) Έστω $f(x, y) \in \mathbb{Q}[x, y]$ τέτοιο ώστε $f(x, 0) = f(0, y) = 0$. Αληθεύει ότι $f(x, y) = 0$;

2.3 Διαιρετότητα Πολυωνύμων

Στην Παράγραφο αυτή θα μελετήσουμε την έννοια της διαιρετότητας στον πολυωνυμικό δακτύλιο $R[x]$. Στην ειδική περίπτωση που ο R είναι σώμα, έστω F, θα διαπιστώσουμε ότι οι δακτύλιοι $\mathbb{Z}$ και $F[x]$ έχουν πολλές κοινές ιδιότητες. Στην Ενότητα 1 είδαμε ότι πολλές αριθμητικές ιδιότητές του $\mathbb{Z}$ ήταν συνέπειες του αλγορίθμου διαίρεσης. Εδώ θα αναπτύξουμε έναν αλγόριθμο διαίρεσης για πολυώνυμα και θα λάβουμε ανάλογα αριθμητικά αποτελέσματα για τον $F[x]$.

Διαιρετότητα και ανάγωγα πολυώνυμα

Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και $f(x), g(x) \in R[x]$. Λέμε ότι το $g(x)$ διαιρεί το $f(x)$ στο $R[x]$ (ή ότι το $f(x)$ είναι *πολλαπλάσιο* του $g(x)$ στο $R[x]$ ή ότι το $g(x)$ είναι *διαιρέτης* του $f(x)$ στο $R[x]$) και γράφουμε $g(x)|f(x)$ αν υπάρχει $h(x) \in R[x]$ με $f(x) = h(x)g(x)$. Για παράδειγμα, το $x-3$ διαιρεί το x^2-5x+6 στο $\mathbb{Q}[x]$ γιατί $x^2-5x+6 = (x-2)(x-3)$. Αλλά και κάθε $c(x-3)$ διαιρεί το x^2-5x+6 στο $\mathbb{Q}[x]$, όπου $c \in \mathbb{Q} - \{0\}$, αφού $x^2-5x+6 = (c(x-2))(c^{-1}(x-3))$.

Παρατηρούμε ότι ισχύουν οι παρακάτω ιδιότητες.

2.3.1 Πρόταση. *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και $f(x), g(x), h(x) \in R[x]$. Τότε ισχύουν τα εξής:*

1) *Αν $g(x)|f(x)$ και $g(x)|h(x)$, τότε $g(x)|a(x)f(x)+b(x)g(x)$ για κάθε $a(x)$, $b(x) \in R[x]$,*

2) *Αν $g(x)|f(x)$ και $h(x)|g(x)$, τότε $h(x)|f(x)$,*

3) *Για κάθε αντιστρέψιμο $c \in R$ έχουμε $c|f(x)$,*

4) *Αν $g(x)|f(x)$ όπου $f(x) \neq 0$ και ο R είναι ακεραία περιοχή, τότε $\deg g(x) \leq \deg f(x)$,*

5) *Αν $g(x)|f(x)$ και $f(x)|g(x)$ και ο R είναι ακεραία περιοχή, τότε υπάρχει αντιστρέψιμο $c \in R$, με $f(x) = cg(x)$.*

Απόδειξη. Οι αποδείξεις των 1), 2) και 3) είναι άμεσες και αφήνονται σαν ασκήσεις.

Η ιδιότητα 4) προκύπτει άμεσα από την Πρόταση 2.2.4 2).

Για την απόδειξη της 5) έχουμε: Αν $f(x) = 0$, τότε $g(x) = 0$ και είναι προφανές ότι ισχύει το ζητούμενο. Έστω $f(x) \neq 0$. Επειδή $f(x) = g(x)a(x)$ και $g(x) = f(x)b(x)$ για κάποια $a(x), b(x) \in R[x]$ παίρνουμε $f(x) = f(x)b(x)a(x)$. Επειδή ο R είναι ακεραία περιοχή, ο $R[x]$ είναι ακεραία περιοχή, και επομένως,

$1 = b(x)a(x)$. Άρα το $a(x)$ είναι αντιστρέψιμο στο $R[x]$. Από την Πρόταση 2.2.4 3) παίρνουμε ότι το $a(x)$ είναι αντιστρέψιμο στοιχείο του R. ⊺

Υπενθυμίζουμε ότι ένας ακέραιος $p > 1$ είναι πρώτος αν δεν υπάρχουν ακέραιοι $a > 1$, $b > 1$ με $p = ab$. Η αντίστοιχη έννοια για πολυώνυμα δίνεται στον επόμενο ορισμό.

2.3.2 Ορισμός. *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Ένα πολυώνυμο $p(x) \in R[x]$ θετικού βαθμού ονομάζεται* ***ανάγωγο*** *στο $R[x]$ (ή ανάγωγο επί του R) αν δεν υπάρχουν πολυώνυμα $f(x)$, $g(x) \in R[x]$ θετικού βαθμού με $p(x) = f(x)g(x)$.*

Για παράδειγμα, αν ο R είναι ακεραία περιοχή, κάθε πολυώνυμο $f(x) \in R[x]$ βαθμού 1 είναι ανάγωγο στο $R[x]$ (Πρόταση 2.2.4 2). Το $5x + 1 \in \mathbb{Z}_6[x]$ αν και είναι βαθμού 1 δεν είναι ανάγωγο στο $\mathbb{Z}_6[x]$ γιατί ισχύει $5x+1 = (2x+1)(3x+1)$. Το $x^2 + 1 \in \mathbb{R}[x]$ είναι ανάγωγο επί του $\mathbb{R}$ αλλά όχι επί του $\mathbb{C}$ γιατί στο $\mathbb{C}[x]$ ισχύει $x^2 + 1 = (x + i)(x - i)$. Στη συνέχεια θα εστιάσουμε το ενδιαφέρον μας στην περίπτωση που ο R είναι ακεραία περιοχή και μάλιστα σώμα.

Επισημαίνουμε ότι το ερώτημα αν ένα δεδομένο πολυώνυμο $f(x) \in R[x]$ είναι ανάγωγο στο $R[x]$ είναι στη γενικότητά του δύσκολο και παραμένει πρακτικά άλυτο ακόμα και όταν $R = \mathbb{Q}$. (Θα δούμε παρακάτω ότι οι απαντήσεις για $R = \mathbb{R}$ και $R = \mathbb{C}$ είναι γνωστές).

Θα διαπιστώσουμε στη συνέχεια ότι αν F είναι ένα σώμα, τότε τα ανάγωγα πολυώνυμα στο $F[x]$ εχουν ιδιότητες ανάλογες με εκείνες των πρώτων αριθμών στο $\mathbb{Z}$. Ιδιαίτερα, θα αποδείξουμε ότι κάθε πολυώνυμο στο $F[x]$ θετικού βαθμού γράφεται κατά τρόπο ουσιαστικά μοναδικό ως γινόμενο αναγώγων πολυωνύμων. Λαμβάνουμε έτσι ένα αποτέλεσμα ανάλογο με το Θεμελιώδες Θεώρημα της Αριθμητικής.

Αλγόριθμος Διαίρεσης στο $F[x]$

Έστω F ένα σώμα. Το παρακάτω αποτέλεσμα είναι ιδιαίτερα σημαντικό για το σκοπό μας, που είναι η μελέτη της αριθμητικής στο $F[x]$, δηλαδή των ιδιοτήτων των δύο πράξεων του $F[x]$.

2.3.3 Θεώρημα (*Αλγόριθμος Διαίρεσης στο $F[x]$*). *Έστω F ένα σώμα και $f(x)$, $g(x) \in F[x]$ με $g(x) \neq 0$. Τότε υπάρχουν μοναδικά $q(x)$, $r(x) \in F[x]$ με*

$$f(x) = q(x)g(x) + r(x) \quad \text{και} \quad \deg r(x) < \deg g(x).$$

Απόδειξη. 1) Ύπαρξη: Έστω $f(x) = f_0 + f_1x + f_2x^2 + \cdots + f_nx^n$ και $g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_mx^m$ με $g_m \neq 0$. Αν $\deg f(x) < \deg g(x)$, έχουμε $f(x) = 0g(x) + f(x)$, οπότε $q(x) = 0$ και $r(x) = f(x)$.

Έστω ότι $\deg f(x) \geq \deg g(x)$. Θα εφαρμόσουμε επαγωγή στο $\deg f(x)$. Αν $\deg f(x) = 0$, τότε $\deg g(x) = 0$ και άρα $f(x) = f_0$ και $g(x) = g_0$. Το g_0 είναι μη μηδενικό στοιχείο σώματος και άρα αντιστρέψιμο. Συνεπώς $f_0 = (f_0 g_0^{-1})g_0 + 0$, οπότε $q(x) = f_0 g_0^{-1}$ και $r(x) = 0$.

Για το επαγωγικό βήμα, θα υποθέσουμε ότι υπάρχουν $q(x)$, $r(x)$ με $f(x) = q(x)g(x)+r(x)$ και $\deg r(x) < \deg g(x)$ για κάθε πολυώνυμο $f(x)$ με $\deg f(x) < n$. Θεωρούμε το πολυώνυμο

$$h(x) = f(x) - f_n g_m^{-1} x^{n-m} g(x) \in F[x].$$

Ο συντελεστής του x^n στο $h(x)$ είναι $f_n - f_n g_m^{-1} g_m = 0$. Άρα $\deg h(x) < n = \deg f(x)$. Από την υπόθεση της επαγωγής υπάρχουν $q(x)$, $r(x) \in F[x]$ με

$$f(x) - f_n g_m^{-1} x^{n-m} g(x) = q(x)g(x) + r(x) \quad \text{και} \quad \deg r(x) < \deg g(x).$$

Επομένως

$$f(x) = (f_n g_m^{-1} x^{n-m} + q(x))g(x) + r(x) \quad \text{και} \quad \deg r(x) < \deg g(x).$$

2) Μοναδικότητα: Έστω ότι υπάρχουν $q(x), r(x), q'(x), r'(x) \in F[x]$ με

$$\begin{aligned} f(x) &= q(x)g(x) + r(x) \quad \text{και} \quad \deg r(x) < \deg g(x), \quad \text{και} \\ f(x) &= q'(x)g(x) + r'(x) \quad \text{και} \quad \deg r'(x) < \deg g(x). \end{aligned}$$

Αφαιρώντας κατά μέλη λαμβάνουμε

$$(q(x) - q'(x))g(x) = r'(x) - r(x).$$

Αν $q(x) - q'(x) \neq 0$, τότε από την Πρόταση 2.2.4 2) προκύπτει ότι $\deg(r'(x) - r(x)) \geq \deg g(x)$. Αυτό είναι άτοπο γιατί $\deg r(x) < \deg g(x)$ και $\deg r'(x) < \deg g(x)$. Άρα $q(x) = q'(x)$ και έτσι $r(x) = r'(x)$. ⊺

Το $r(x)$ (αντίστοιχα, $q(x)$) στο προηγούμενο Θεώρημα ονομάζεται το ***υπόλοιπο*** (αντίστοιχα, το ***πηλίκο***) της διαίρεσης του $f(x)$ με το $g(x)$.

2.3.4 Παράδειγμα. Η απόδειξη του Αλγορίθμου Διαίρεσης μας παρέχει έναν πρακτικό τρόπο υπολογισμού των $q(x)$ και $r(x)$. Όταν το σώμα F είναι το $\mathbb{Q}$ ή το $\mathbb{R}$, ο τρόπος αυτός διαίρεσης πολυωνύμων είναι ακριβώς αυτός που γνωρίζουμε από τα μαθητικά μας χρόνια. Θα δούμε εδώ ένα παράδειγμα για διαφορετικό σώμα.

Έστω $F = \mathbb{Z}_5$ και $f(x) = x^4 + 4x^2 + x + 1 \in \mathbb{Z}_5[x]$, $g(x) = 2x^2 + 1 \in \mathbb{Z}_5[x]$. Ο μεγιστοβάθμιος συντελεστής του $g(x)$ είναι το $2 \in \mathbb{Z}_5$ ($g_m = 2$, με τον συμβολισμό της απόδειξης) και το αντίστροφό του είναι το $3 \in \mathbb{Z}_5$. Σύμφωνα

με την απόδειξη του Αλγορίθμου Διαίρεσης (και συγκεκριμένα στο σημείο όπου θεωρήσαμε το $h(x)$) από το $f(x)$ αφαιρούμε το $3x^{4-2}g(x)$. Έχουμε

$$f(x) - 3x^2 g(x) = x^2 + x + 1.$$

Επαναλαμβάνουμε τώρα την ίδια διαδικασία για το x^2+x+1 στη θέση του $f(x)$. Έχουμε

$$x^2 + x + 1 - 3g(x) = x - 2.$$

Εδώ τερματίζεται η διαδικασία των αφαιρέσεων γιατί ο βαθμός του $x-2$ είναι μικρότερος του βαθμού του $g(x)$. Από τις παραπάνω δύο ταυτότητες παίρνουμε

$$f(x) = 3x^2 g(x) + x^2 + x + 1 = 3x^2 g(x) + 3g(x) + x - 2 = (3x^2+3)g(x) + x - 2.$$

Άρα $q(x) = 3x^2 + 3$ και $r(x) = x - 2$.

Το μοναδικό σημείο στην απόδειξη του Αλγορίθμου Διαίρεσης όπου χρησιμοποιήσαμε ότι τα μη μηδενικά στοιχεία του F είναι αντιστρέψιμα ήταν για να αντιστρέψουμε τον μεγιστοβάθμιο συντελεστή του $g(x)$. Συνεπώς, με παρόμοιο τρόπο μπορεί να αποδειχτεί το ακόλουθο αποτέλεσμα. Η απόδειξη αφήνεται σαν άσκηση.

2.3.5 Θεώρημα (*Αλγόριθμος Διαίρεσης στο $R[x]$*). *Έστω R μια ακεραία περιοχή και $f(x), g(x) \in R[x]$ έτσι ώστε ο μεγιστοβάθμιος συντελεστής του $g(x)$ είναι αντιστρέψιμο στοιχείο του R. Τότε υπάρχουν μοναδικά $q(x), r(x) \in R[x]$ με*

$$f(x) = q(x)g(x) + r(x) \quad \textit{και} \quad \deg r(x) < \deg g(x).$$

Παράδειγμα Στον δακτύλιο $\mathbb{Q}[x,y]$ θεωρούμε τα πολυώνυμα $f(x,y) = xy^2 - 1$ και $g(x,y) = y - x$. Θεωρούμε τα στοιχεία του $\mathbb{Q}[x,y]$ ως πολυώνυμα στη μεταβλητή y με συντελεστές από το δακτύλιο $\mathbb{Q}[x]$, δηλαδή $\mathbb{Q}[x,y] = (\mathbb{Q}[x])[y]$. Εφαρμόζοντας τον Αλγόριθμο Διαίρεσης βρίσκουμε $xy^2 - 1 = (xy + x^2)(y - x) + x^3 - 1$.

Μέγιστος κοινός διαιρέτης

Ένα πολυώνυμο $f(x) \in R[x]$ ονομάζεται ***μονικό*** αν ο μεγιστοβάθμιος συντελεστής του είναι το 1. Παρατηρούμε ότι όταν το F είναι σώμα και $f(x) \in F[x]$ είναι μη μηδενικό με μεγιστοβάθμιο συντελεστή $c \in F$, τότε το $c^{-1}f(x)$ είναι μονικό.

Κατ' αναλογία με τον δακτύλιο $\mathbb{Z}$ μπορούμε να ορίσουμε την έννοια του μέγιστου κοινού διαιρέτη πολυωνύμων στο $F[x]$.

2.3.6 Ορισμός. *Έστω F ένα σώμα και $f(x), g(x) \in F[x]$ από τα οποία τουλάχιστον ένα είναι μη μηδενικό. Ένα μονικό πολυώνυμο $d(x) \in F[x]$ ονομάζεται* ***μέγιστος κοινός διαιρέτης*** *των $f(x)$ και $g(x)$ αν ικανοποιεί τις ιδιότητες*

1) $d(x)|f(x)$ και $d(x)|g(x)$ στο $F[x]$, και

2) αν $c(x) \in F[x]$, $c(x)|f(x)$ και $c(x)|g(x)$ τότε $c(x)|d(x)$.

Σημειώνουμε ότι αν το $d(x)$ είναι ένας μέγιστος κοινός διαιρέτης των $f(x)$, $g(x)$, τότε από την ιδιότητα 2) κάθε άλλος κοινός διαιρέτης των $f(x)$, $g(x)$ έχει βαθμό που είναι μικρότερος ή ίσος του $\deg d(x)$. Έτσι δικαιολογείται η ονομασία *μέγιστος* κοινός διαιρέτης.

Θα δούμε στο επόμενο θεώρημα ότι ο μέγιστος κοινός διαιρέτης των $f(x)$, $g(x) \in F[x]$ (από τα οποία τουλάχιστον ένα είναι μη μηδενικό) υπάρχει και είναι μοναδικός. Συμβολίζεται δε με $\mu\kappa\delta(f(x), g(x))$.

Για παράδειγμα, αν $f(x) = 2x + 2 \in \mathbb{R}[x]$ και $g(x) = x^2 - 1 \in \mathbb{R}[x]$, τότε $\mu\kappa\delta(f(x), g(x)) = x + 1$. Η υπόθεση ότι ο $\mu\kappa\delta$ είναι μονικό πολυώνυμο χρειάζεται για να είναι αυτός μοναδικός. Στο παράδειγμά μας, κάθε πολυώνυμο της μορφής $c(x+1)$, $c \in \mathbb{R} - \{0\}$ ικανοποιεί τις ιδιότητες 1) και 2) στον ορισμό του $\mu\kappa\delta$.

2.3.7 Θεώρημα. *Έστω F ένα σώμα και $f(x), g(x) \in F[x]$ από τα οποία τουλάχιστον ένα δεν είναι μηδέν. Τότε υπάρχει μοναδικός μέγιστος κοινός διαιρέτης $\mu\kappa\delta(f(x), g(x))$ των $f(x)$ και $g(x)$ στο $F[x]$. Επιπλέον, υπάρχουν $a(x)$, $b(x) \in F[x]$ τέτοια ώστε*

$$\mu\kappa\delta(f(x), g(x)) = a(x)f(x) + b(x)g(x).$$

Η απόδειξη που ακολουθεί είναι παρόμοια με την απόδειξη του αντίστοιχου Θεωρήματος για τον δακτύλιο $\mathbb{Z}$.

Απόδειξη. Ύπαρξη: Θεωρούμε το σύνολο

$$I = \{a(x)f(x) + b(x)g(x) \in F[x] | a(x), b(x) \in F[x]\}.$$

Επειδή ένα τουλάχιστον από τα $f(x)$ και $g(x)$ δεν είναι μηδέν, το I περιέχει μη μηδενικά πολυώνυμα. Έστω $d(x) \in I$ ένα μη μηδενικό πολυώνυμο ελάχιστου βαθμού. Τότε έχουμε

$$d(x) = a(x)f(x) + b(x)g(x) \tag{1}$$

για κάποια $a(x), b(x) \in F[x]$.

Θα δείξουμε ότι το $d(x)$ ικανοποιεί τις ιδιότητες 1) και 2) στον ορισμό του *μκδ*. Από τον Αλγόριθμο Διαίρεσης, υπάρχουν $q(x), r(x) \in F[x]$ με τις ιδιότητες $f(x) = q(x)d(x) + r(x)$, $\deg r(x) < \deg d(x)$. Αντικαθιστώντας έχουμε

$$\begin{aligned} r(x) &= f(x) - q(x)d(x) \\ &= f(x) - q(x)(a(x)f(x) + b(x)g(x)) \\ &= (1 - q(x)a(x))f(x) + (-q(x)b(x))g(x) \end{aligned}$$

και άρα

$$r(x) \in I.$$

Από τη σχέση $\deg r(x) < \deg d(x)$ και του ορισμού του $d(x)$ συνάγουμε ότι $r(x) = 0$. Επομένως $d(x)|f(x)$. Με παρόμοιο τρόπο αποδεικνύεται ότι $d(x)|g(x)$.

Για να δείξουμε την ιδιότητα 2) στον ορισμό του μκδ, έστω $c(x) \in F[x]$ με $c(x)|f(x)$ και $c(x)|g(x)$. Από τη σχέση (;;) συμπεραίνουμε ότι $c(x)|d(x)$.

Έχουμε αποδείξει ότι υπάρχει $d(x) \in F[x]$ που ικανοποιεί τις ιδιότητες 1) και 2) στον ορισμό του *μκδ*. Ενδέχεται το $d(x)$ να μην είναι μονικό. Έστω d_n ο μεγιστοβάθμιος συντελεστής του $d(x)$. Είναι $d_n \neq 0$, αφού $d(x) \neq 0$ και επειδή το F είναι σώμα το d_n είναι αντιστρέψιμο. Αφού το $d(x)$ ικανοποιεί τις ιδιότητες 1) και 2), εύκολα διαπιστώνουμε ότι και το μονικό πολυώνυμο $d_n^{-1}d(x)$ τις ικανοποιεί. Τέλος, έχουμε

$$d_n^{-1}d(x) = (d_n^{-1}a(x))f(x) + (d_n^{-1}b(x))g(x).$$

Μοναδικότητα: Έστω $c(x)$, $d(x) \in F[x]$ δύο μέγιστοι κοινοί διαιρέτες των $f(x)$ και $g(x)$. Επειδή $c(x)|f(x)$, $c(x)|g(x)$ και το $d(x)$ είναι μέγιστος κοινός διαιρέτης των $f(x)$ και $g(x)$ παίρνουμε από την ιδιότητα 2) του ορισμού ότι $c(x)|d(x)$. Όμοια παίρνουμε $d(x)|c(x)$. Από την Πρόταση 2.3.1 5) έχουμε $c(x) = rd(x)$ για κάποιο μη μηδενικό $r \in F$. Επειδή τα $c(x)$ και $d(x)$ είναι μονικά, παίρνουμε $r = 1$. ⊤

Δύο πολυώνυμα θα λέγονται σχετικά πρώτα αν ο *μκδ* τους είναι το 1.

Όπως στην περίπτωση του δακτυλίου $\mathbb{Z}$ των ακεραίων, υπάρχει και εδώ ένας πρακτικός τρόπος που υπολογίζει τον *μκδ* και πολυωνυμα $a(x)$, $b(x)$ που έχουν την ιδιότητα $\mu\kappa\delta(f(x), g(x)) = a(x)f(x)+b(x)g(x)$. Πριν ασχοληθούμε με αυτό, ας αποδείξουμε ένα αποτέλεσμα που είναι ανάλογο με το Θεμελιώδες Θεώρημα της Αριθμητικής. Για το σκοπό αυτό χρειαζόμαστε το ακόλουθο Λήμμα (βλ. και το Λήμμα 1.2.5).

2.3.8 Λήμμα. *Έστω F ένα σώμα και $f(x), g(x), p(x) \in F[x]$, όπου το $p(x)$ είναι ανάγωγο. Αν $p(x)|f(x)g(x)$, τότε το $p(x)$ διαιρεί ένα τουλάχιστον από τα $f(x)$, $g(x)$.*

Απόδειξη. Έστω ότι το $p(x)$ δεν διαιρεί το $f(x)$. Επειδή το $p(x)$ είναι ανάγωγο έχουμε $\mu\kappa\delta(f(x), p(x)) = 1$. Από το Θεώρημα 2.3.7 υπάρχουν $a(x), b(x) \in F[x]$ με $1 = a(x)f(x) + b(x)p(x)$, οπότε παίρνουμε $g(x) = a(x)f(x)g(x) + b(x)p(x)g(x)$. Επειδή το $p(x)$ διαιρεί το $a(x)f(x)g(x)$ και το $b(x)p(x)g(x)$, θα διαιρεί και το $g(x)$. ⊤

2.3.9 Πόρισμα. *Έστω F ένα σώμα και $a_1(x), \ldots, a_n(x)$, $p(x) \in F[x]$, όπου το $p(x)$ είναι ανάγωγο. Αν $p(x)|a_1(x)\ldots a_n(x)$, τότε το $p(x)$ θα διαιρεί ένα τουλάχιστον από τα $a_i(x)$.*

Απόδειξη. Η απόδειξη αφήνεται σαν άσκηση. ⊤

2.3.10 Θεώρημα. *Έστω F ένα σώμα. Τότε κάθε πολυώνυμο $f(x) \in F[x]$ θετικού βαθμού γράφεται ως γινόμενο αναγώγων πολυωνύμων στο $F[x]$,*

$$f(x) = p_1(x)\ldots p_m(x),$$

$p_i(x) \in F[x]$, $p_i(x)$ ανάγωγο. Η παράσταση αυτή είναι μοναδική με την εξής έννοια. Αν

$$f(x) = p_1(x)\ldots p_m(x) = q_1(x)\ldots q_n(x),$$

όπου κάθε $p_i(x)$ και $q_j(x)$ είναι ανάγωγο στο $F[x]$, τότε $n = m$ και μετά ενδεχομένως από κάποια αναδιάταξη έχουμε $p_1(x) = c_1q_1(x), \ldots, p_m(x) = c_mq_m(x)$, όπου $c_i \in F$ για κάθε i.

Απόδειξη. Ύπαρξη (Σύγκρινε με την απόδειξη της Πρότασης 1.2.1): Έστω M το σύνολο των $f(x) \in F[x]$ που δεν γράφονται ως γινόμενα αναγώγων και έστω ότι $M \neq \emptyset$. Επιλέγουμε ένα $g(x) \in M$ ελάχιστου βαθμού. Αφού $g(x) \in M$, το $g(x)$ δεν είναι ανάγωγο (κάθε ανάγωγο πολυώνυμο είναι κατά τετριμμένο τρόπο γινόμενο αναγώγων). Άρα $g(x) = a(x)b(x)$ για κάποια $a(x), b(x) \in F[x]$ με $\deg a(x) < \deg g(x)$ και $\deg b(x) < \deg g(x)$. Από το ελάχιστο του βαθμού του $g(x)$ προκύπτει ότι $a(x) \notin M$ και $b(x) \notin M$ και κατά συνέπεια τα $a(x)$ και $b(x)$ γράφονται ως γινόμενα αναγώγων. Το ίδιο συμβαίνει τότε και για το γινόμενό τους $a(x)b(x) = g(x)$, που είναι άτοπο.
Μοναδικότητα (Σύγκρινε με την απόδειξη του Θεωρήματος 1.2.7): Μπορούμε να υποθέσουμε ότι $m \leq n$. Χρησιμοποιούμε επαγωγή στο m. Για $m = 1$ έχουμε $p_1(x) = q_1(x)\ldots q_n(x)$. Από το Πόρισμα 2.3.9 έχουμε (ενδεχομένως μετά από κάποια αναδιάταξη) ότι $p_1(x)|q_1(x)$. Επειδή το $q_1(x)$ είναι ανάγωγο, το $p_1(x)$ θα είναι της μορφής c_1 ή $c_1q_1(x)$, όπου $c_1 \in F - \{0\}$. Όμως το $p_1(x)$ δεν είναι μια σταθερά αφού είναι ανάγωγο. Άρα $p_1(x) = c_1q_1(x)$ και $c_1q_1(x) = q_1(x)\ldots q_n(x)$. Έστω $n > 1$. Τότε, αφού το $F[x]$ είναι ακεραία περιοχή και

$q_1(x) \neq 0$ παίρνουμε $c_1 = q_2(x) \dots q_n(x)$. Αυτό είναι άτοπο (Πρόταση 2.2.4) και άρα $n = 1$.

Έστω τώρα $m > 1$. Από την ισότητα $p_1(x) \dots p_m(x) = q_1(x) \dots q_n(x)$ και το Πόρισμα 2.3.9 παίρνουμε όπως πριν ότι $p_1(x) = c_1 q_1(x)$, για κάποιο $c_1 \in F - \{0\}$, και $p_2(x) \dots p_m(x) = c_1 q_2(x) \dots q_n(x)$. Από την επαγωγική υπόθεση προκύπτει ότι $m-1 = n-1$ και ότι, μετά από αναδιάταξη, για κάθε $i = 2, \dots, m$ υπάρχουν $c_i \in F - \{0\}$ με $p_i(x) = c_i q_i(x)$. ⊤

Είναι φανερό ότι αν το $p(x) \in F[x]$ είναι ανάγωγο και έχει μεγιστοβάθμιο συντελεστή s, τότε το $s^{-1}p(x)$ είναι ανάγωγο και μονικό. Σύμφωνα με το προηγούμενο θεώρημα κάθε $f(x) \in F[x]$ θετικού βαθμού γράφεται κατά μοναδικό τρόπο ως

$$f(x) = c p_1(x)^{r_1} \dots p_m(x)^{r_m},$$

όπου $c \in F - \{0\}$, τα $p_i(x) \in F[x]$ είναι διακεκριμένα μονικά ανάγωγα πολυώνυμα και οι r_i είναι θετικοί ακέραιοι. Η παραγοντοποίηση αυτή ονομάζεται η ***ανάλυση του $f(x)$ σε γινόμενο μονικών αναγώγων πολυωνύμων*** Για παράδειγμα, η ανάλυση του $x^5 - x^4 + 2x^3 - 2x^2 + x - 1 \in \mathbb{R}[x]$ σε γινόμενο μονικών αναγώγων πολυωνύμων είναι $x^5 - x^4 + 2x^3 - 2x^2 + x - 1 = (x^2+1)^2(x-1)$. Η αντίστοιχη ανάλυση του ιδίου πολυωνύμου αν θεωρηθεί ως στοιχείο του $\mathbb{C}[x]$ είναι $(x-i)^2(x+i)^2(x-1)$.

Ο Ευκλείδειος Αλγόριθμος στο $F[x]$

Έστω F ένα σώμα. Ο Ευκλείδειος Αλγόριθμος στο $F[x]$ χρησιμοποιείται για τον υπολογισμό του $\mu\kappa\delta$ δύο πολυωνύμων $f(x), g(x) \in F[x]$ και την εύρεση πολυωνύμων $a(x)$ και $b(x)$ που έχουν την ιδιότητα $\mu\kappa\delta(f(x), g(x)) = a(x)f(x) + b(x)g(x)$. Κατα αναλογία με την περίπτωση του $\mathbb{Z}$, ο αλγόριθμος αυτός συνίσταται σε διαδοχικές εφαρμογές του Αλγορίθμου Διαίρεσης στο $F[x]$ και της ακόλουθης παρατήρησης: αν στο $F[x]$ ισχύει $f(x) = q(x)g(x) + r(x)$, τότε $\mu\kappa\delta(f(x), g(x)) = \mu\kappa\delta(g(x), r(x))$ (γιατί;).

Έστω $f(x), g(x) \in F[x]$ με $g(x) \neq 0$. Από τον αλγόριθμο διαίρεσης έχουμε διαδοχικά

$$\begin{aligned}
f(x) &= q_0(x)g(x) + r_0(x), && \deg r_0(x) < \deg g(x) && (0)\\
g(x) &= q_1(x)r_0(x) + r_1(x), && \deg r_1(x) < \deg r_0(x) && (1)\\
r_0(x) &= q_2(x)r_1(x) + r_2(x), && \deg r_2(x) < \deg r_1(x) && (2)\\
r_1(x) &= q_3(x)r_2(x) + r_3(x), && \deg r_3(x) < \deg r_2(x) && (3)\\
&\cdots\cdots\cdots\\
r_{n-2}(x) &= q_n(x)r_{n-1}(x) + r_n(x), && \deg r_n(x) < \deg r_{n-1}(x) && (n)\\
r_{n-1}(x) &= q_{n+1}(x)r_n(x) + 0,
\end{aligned}$$

Μετά από πεπερασμένο πλήθος βημάτων θα βρούμε ένα υπόλοιπο που είναι ίσο με μηδέν, $r_{n+1}(x) = 0$, γιατί η ακολουθία των φυσικών αριθμών

$$\deg g(x) > \deg r_0(x) > \deg r_1(x) > \deg r_2(x) > \dots$$

είναι γνήσια φθίνουσα. Υποθέτουμε ότι το $r_{n+1}(x)$ είναι το πρώτο υπόλοιπο που είναι ίσο με μηδέν. Εφαρμόζοντας διαδοχικά την παρατήρηση που επισημάναμε πριν παίρνουμε

$$\mu\kappa\delta(f(x), g(x)) = \mu\kappa\delta(g(x), r_0(x)) = \mu\kappa\delta(r_0(x), r_1(x)) = \dots = \mu\kappa\delta(r_n(x), 0).$$

Αν s είναι ο μεγιστοβάθμιος όρος του (μη μηδενικού πολυωνύμου) $r_n(x)$, τότε είναι φανερό ότι

$$\mu\kappa\delta(f(x), g(x)) = \mu\kappa\delta(r_n(x), 0) = s^{-1} r_n(x).$$

Τα $a(x), b(x)$ προσδιορίζονται με διαδοχικές αντικαταστάσεις ξεκινώντας από την προτελευταία ισότητα, την (n), και εφαρμόζοντας την παρακάτω διαδικασία. Γράφουμε τις ισότητες $(0) - (n)$ ως εξής

$$r_0(x) = f(x) - q_0(x) g(x) \qquad (0')$$

$$r_1(x) = g(x) - q_1(x) r_0(x) \qquad (1')$$

$$r_2(x) = r_0(x) - q_2(x) r_1(x) \qquad (2')$$

$$\dots\dots\dots$$

$$r_{n-1}(x) = r_{n-3}(x) - q_{n-1}(x) r_{n-2}(x) \qquad (n-1')$$

$$r_n(x) = r_{n-2}(x) - q_n(x) r_{n-1}(x). \qquad (n')$$

Αντικαθιστούμε τώρα το $r_{n-1}(x)$ από την $(n-1)'$ στην $(n)'$. Λαμβάνουμε έτσι μια παράσταση της μορφής

$$r_n(x) = a_{n-3}(x) r_{n-3}(x) + b_{n-2}(x) r_{n-2}(x).$$

Στην ισότητα αυτή αντικαθιστούμε το $r_{n-3}(x)$ από την ισότητα $(n-2)'$, και ούτω κάθε εξής. Στο τέλος θα προκύψει μια παράσταση της μορφής

$$r_n(x) = A(x) f(x) + B(x) g(x).$$

Αν s είναι ο μεγιστοβάθμιος συντελεστής του $r_n(x)$ έχουμε

$$s^{-1} r_n(x) = s^{-1} A(x) f(x) + s^{-1} B(x) g(x)$$

οπότε μπορούμε να θέσουμε

$$a(x) = s^{-1} A(x) \quad \text{και} \quad b(x) = s^{-1} B(x).$$

Ένα παράδειγμα όπου εφαρμόζεται ο παραπάνω αλγόριθμος υπάρχει αμέσως παρακάτω.

2.3.11 Παραδείγματα.

1) Έστω $f(x), g(x) \in \mathbb{Z}_7[x]$ όπου

$$f(x) = 4x^4 + 2x^3 + 6x^2 + 4x + 5 \text{ και } g(x) = 3x^3 + 5x^2 + 6x.$$

Θα υπολογίσουμε τον $\mu\kappa\delta(f(x), g(x))$, χρησιμοποιώντας τον Ευκλείδειο Αλγόριθμο, και θα προσδιορίσουμε πολυώνυμα $a(x)$ και $b(x)$ τέτοια ώστε $\mu\kappa\delta(f(x), g(x)) = a(x)f(x) + b(x)g(x)$. Για τον Αλγόριθμο Διαίρεσης εφαρμόζουμε τη μέθοδο που περιγράψαμε στο Παράδειγμα 2.3.4. Βρίσκουμε τα εξής

$$\begin{aligned} f(x) &= (6x)g(x) + 5x^2 + 4x + 5 \\ g(x) &= (2x + 5)(5x^2 + 4x + 5) + 4x + 3 \\ 5x^2 + 4x + 5 &= (3x + 4)(4x + 3) + 0. \end{aligned}$$

Το τελευταίο μη μηδενικό υπόλοιπο είναι το $4x + 3$. Το αντίστροφο του 4 στο $\mathbb{Z}_7$ είναι το 2. Άρα

$$\mu\kappa\delta(f(x), g(x)) = 2(4x + 3) = x + 6.$$

Για να προσδιορίσουμε πολυώνυμα $a(x)$ και $b(x)$, ώστε $\mu\kappa\delta(f(x), g(x)) = a(x)f(x) + b(x)g(x)$, γράφουμε την προτελευταία ισότητα ως

$$4x + 3 = g(x) - (2x + 5)(5x^2 + 4x + 5)$$

και αντικαθιστούμε το $5x^2 + 4x + 5$ από την πρώτη,

$$4x + 3 = g(x) - (2x + 5)(f(x) - (6x)g(x)).$$

Μετά από πράξεις βρίσκουμε

$$4x + 3 = (5x + 2)f(x) + (5x^2 + 2x + 1)g(x).$$

Πολλαπλασιάζοντας με το αντίστροφο του 4 στο $\mathbb{Z}_7$, δηλαδή το 2, έχουμε

$$x + 6 = (3x + 4)f(x) + (3x^2 + 4x + 2)g(x),$$

οπότε μπορούμε να θέσουμε $a(x) = 3x + 4$ και $b(x) = 3x^2 + 4x + 2$.

2) Έστω $f(x) = x^4 + 2x^3 + 4x^2 + 8x + 9 \in \mathbb{Z}_p[x]$ και $g(x) = x^2 + 2x + 3 \in \mathbb{Z}_p[x]$, όπου p είναι ένας πρώτος αριθμός. Για ποιούς p ο $\mu\kappa\delta(f(x), g(x))$ έχει βαθμό 2;

Επειδή $\mu\kappa\delta(f(x), g(x))|g(x)$ και το $g(x)$ είναι δευτέρου βαθμού και μονικό, βλέπουμε από την Πρόταση 2.2.4 2) ότι

$$\deg \mu\kappa\delta(f(x), g(x)) = 2 \Leftrightarrow g(x) = \mu\kappa\delta(f(x), g(x)).$$

Από τον ορισμό του $\mu\kappa\delta$ και επειδή το $g(x)$ είναι μονικό είναι φανερό ότι

$$g(x) = \mu\kappa\delta(f(x), g(x)) \Leftrightarrow g(x)|f(x).$$

Από τον Αλγόριθμο Διαίρεσης στο $\mathbb{Z}_p[x]$ βρίσκουμε

$$f(x) = (x^2 + 1)g(x) + 6x + 6.$$

Το υπόλοιπο $6x + 6$ είναι 0 αν και μόνο αν $p = 2$ ή 3.

3) Έστω F ένα σώμα και $p(x), q(x) \in F[x]$ διακεκριμένα μονικά ανάγωγα πολυώνυμα. Αν $p(x)|f(x)$ και $q(x)|f(x)$, όπου $f(x) \in F[x]$, τότε $p(x)q(x)|f(x)$.
Ας το αποδείξουμε αυτό με δύο τρόπους.

1. Από την υπόθεση ισχύει $\mu\kappa\delta(p(x), q(x)) = 1$. Από το Θεώρημα 2.3.7 έχουμε $1 = a(x)p(x) + b(x)q(x)$, όπου $a(x), b(x) \in F[x]$, οπότε

$$f(x) = a(x)p(x)f(x) + b(x)q(x)f(x).$$

Ισχύει $p(x)q(x)|p(x)f(x)$. Συνεπώς $p(x)q(x)|a(x)p(x)f(x)$ και $p(x)q(x)|b(x)q(x)f(x)$. Επομένως $p(x)q(x)|a(x)p(x)f(x)+b(x)q(x)f(x)$, δηλαδή $p(x)q(x)|f(x)$.

2. Από την υπόθεση και το Θεώρημα 2.3.10 έπεται ότι η ανάλυση του $f(x)$ σε γινόμενο μονικών αναγώγων πολυωνύμων είναι της μορφής

$$f(x) = cp(x)^{n_1}q(x)^{n_2}p_3(x)^{n_3}\dots p_m(x)^{n_m},$$

όπου οι n_i είναι θετικοί ακέραιοι και τα $p(x), q(x), p_3(x), \dots, p_m(x) \in F[x]$ είναι διακεκριμένα μονικά ανάγωγα πολυώνυμα. Άρα $p(x)q(x)|f(x)$.

4) Έστω $f(x), g(x), h(x) \in F[x]$, όπου το F είναι ένα σώμα, με $f(x)|g(x)h(x)$ και $\mu\kappa\delta(f(x), g(x)) = 1$. Τότε $f(x)|h(x)$.
Η απόδειξη είναι παρόμοια με την απόδειξη του Παραδείγματος 1.2.8 1).

5) **Θεώρημα του Fermat για πολυώνυμα.**
Θα αποδείξουμε εδώ ότι αν $n > 2$, τότε δεν υπάρχουν πολυώνυμα

$f(x), g(x), h(x) \in \mathbb{C}[x]$ θετικού βαθμού με $\mu\kappa\delta(f(x), g(x)) = 1$ τέτοια ώστε

$$(f(x))^n + (g(x))^n = (h(x))^n.$$

Για την απόδειξη θα χρειαστούμε στοιχειώδεις ιδιότητες της παραγώγου πολυωνύμου με συντελεστές από το $\mathbb{C}$ τις οποίες θα θεωρήσουμε γνωστές.

Έστω ότι υπάρχουν $f(x), g(x), h(x) \in \mathbb{C}[x]$ θετικού βαθμού τέτοια ώστε

$$\mu\kappa\delta(f(x), g(x)) = 1$$

και

$$(f(x))^n + (g(x))^n = (h(x))^n.$$

Κάθε ανάγωγος κοινός παράγοντας των $f(x)$, $h(x)$ διαιρεί το $g(x)$ σύμφωνα με το Πόρισμα 2.3.9 και κατά συνέπεια διαιρεί τον $\mu\kappa\delta(f(x), g(x))$ που είναι 1. Άρα έχουμε $\mu\kappa\delta(f(x), h(x)) = 1$.

Έστω ότι οι βαθμοί των $f(x)$, $g(x)$, $h(x)$ είναι αντίστοιχα a, b, c. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $a \geq b$ και $a \geq c$. Παραγωγίζοντας την αρχική σχέση και διαιρώντας με το n λαμβάνουμε

$$(f(x))^{n-1} f(x)' + (g(x))^{n-1} g(x)' = (h(x))^{n-1} h(x)'.$$

Από αυτή και την αρχική σχέση παίρνουμε

$$(f(x))^{n-1}(f(x)g(x)' - f(x)'g(x)) =$$

$$(h(x))^{n-1}(h(x)g(x)' - h(x)'g(x)).$$

Επειδή $\mu\kappa\delta(f(x), h(x)) = 1$ έχουμε ότι $\mu\kappa\delta((f(x))^{n-1}, (h(x))^{n-1}) = 1$. Άρα το $(f(x))^{n-1}$ διαιρεί το $h(x)g(x)' - h(x)'g(x)$ σύμφωνα με την προηγούμενη Εφαρμογή. Θεωρώντας βαθμούς έχουμε

$$b + c - 1 \geq \deg(h(x)g(x)' - h(x)'g(x)) \geq \deg(f(x))^{n-1} = (n-1)a.$$

Επειδή ισχύει $a \geq b$ και $a \geq c$ παίρνουμε $2a - 1 \geq (n-1)a$ οπότε $n \leq 2$, που είναι άτοπο.

Σημείωση Το Θεώρημα του Fermat για πολυώνυμα δεν αληθεύει για τυχαίο σώμα F στη θέση του $\mathbb{C}$. Για παράδειγμα, στο $\mathbb{Z}_3[x]$ έχουμε

$$x^3 + (x+1)^3 = (2x+1)^3.$$

Αν και οι δακτύλιοι $\mathbb{Z}$ και $F[x]$ παρουσιάζουν πολλές σημαντικές ομοιότητες, η απόδειξη του Θεωρήματος του Fermat για το $\mathbb{Z}$ είναι εξαιρετικά δύσκολη και θεωρείται ένα από τα σημαντικά επιτεύγματα των σύγχρονων Μαθηματικών, όπως έχουμε ήδη επισημάνει στην Εφαρμογή 1.3.8 7.

Ασκήσεις 2.3

1. Να υπολογιστεί ο μκδ των παρακάτω πολυωνύμων στο $F[x]$. Στη συνέχεια να βρεθούν $a(x), b(x) \in F[x]$ ώστε $\mu\kappa\delta(f(x), g(x)) = a(x)f(x) + b(x)g(x)$.[2]

   i. $f(x) = x^5 + 1$, $g(x) = x^3 + 1$, $F = \mathbb{Q}$
   ii. $f(x) = x^3 - x^2 - x + 1$ $g(x) = x^3 + 4x^2 + x - 6$, $F = \mathbb{Q}$
   iii. $f(x) = x^3 - x^2 - x + 1$, $g(x) = x^3 + 4x^2 + x - 6$, $F = \mathbb{Z}_5$
   iv. $f(x) = 2x^3 + 6x^2 + 4x + 5$, $g(x) = 3x^2 + 2$, $F = \mathbb{Q}$
   v. $f(x) = 2x^3 + 6x^2 + 4x + 5$, $g(x) = 3x^2 + 2$, $F = \mathbb{Z}_7$
   vi. $f(x) = x^3 - ix^2 + 4x - 4i$, $g(x) = x^2 + 1$, $F = \mathbb{C}$.

2. Έστω $f(x), g(x) \in \mathbb{R}[x]$. Αν στο $\mathbb{C}[x]$ ισχύει $f(x)|g(x)$ τότε και στο $\mathbb{R}[x]$ ισχύει $f(x)|g(x)$.

3. Έστω F ένα υπόσωμα του σώματος E και $f(x), g(x) \in F[x]$ δύο πολυώνυμα με $g(x) \neq 0$. Από τις δύο ταυτότητες διαίρεσης στο $F[x]$ και $E[x]$ έχουμε ότι $f(x) = q(x)g(x) + r(x)$ για δύο πολυώνυμα $q(x), r(x) \in F[x]$ με $\deg r(x) < \deg g(x)$ και $f(x) = q'(x)g(x) + r'(x)$ για δύο πολυώνυμα $q'(x), r'(x) \in E[x]$ με $\deg r'(x) < \deg g(x)$. Αποδείξτε ότι $q(x) = q'(x)$ και $r(x) = r'(x)$. Συμπεράνετε ότι ο $\mu\kappa\delta$ των $f(x), g(x)$ στο $F[x]$ ισούται με τον $\mu\kappa\delta$ των $f(x), g(x)$ στο $E[x]$.

4. Στο $\mathbb{Z}[x]$ θεωρούμε τα $f(x) = x^5+3x^4+x^3+4x^2-3x-1$, $g(x) = x^2+x+1$. Χρησιμοποιώντας τον αλγόριθμο διαίρεσης δείξτε ότι το $f(x)$ δεν διαιρείται με το $g(x)$. Αν όμως θεωρήσουμε τα πολυώνυμα αυτά στο $\mathbb{Z}_5[x]$, αποδείξτε ότι το $f(x)$ διαιρείται με το $g(x)$.

5. Προσδιορίστε τον $\mu\kappa\delta(x^8 - 1, x^6 - 1)$ στο $F[x]$, όπου το F είναι ένα σώμα.

6. Αποδείξτε ότι στο $F[x]$, όπου το F είναι ένα σώμα, ισχύει $\mu\kappa\delta(x^m - 1, x^n - 1) = x^d - 1$, όπου $d = \mu\kappa\delta(m, n)$.

7. Έστω $f(x), g(x) \in F[x]$, όπου το F είναι ένα σώμα και $\deg g(x) \geq 1$. Τότε υπάρχουν μοναδικά $f_0(x), \ldots, f_n(x) \in F[x]$ με

   $$f(x) = f_n(x)g(x)^n + \cdots + f_1(x)g(x) + f_0(x), \quad \deg f_i(x) < \deg g(x)$$

   όπου $f_n(x) \neq 0$.
   Υπόδειξη: Βλ. Παράδειγμα 1.2.8 9).

[2] Εδώ, αξίζει να παρατηρήσει κανείς ότι (όπως και στην περίπτωση του $\mu\kappa\delta$ ακεραίων αριθμών) τα πολυώνυμα $a(x), b(x)$ με τις παραπάνω ιδιότητες δεν είναι μοναδικά.

8. Στο $\mathbb{Z}_p[x]$, όπου p είναι ένας πρώτος, έστω $f(x) = 2x^3 - 3x^2 + x + 6$, $g(x) = x^2 - 2x$. Για ποιούς πρώτους p το υπόλοιπο της διαίρεσης του $f(x)$ με το $g(x)$

   i. είναι μη μηδενικό;

   ii. έχει μη μηδενικό σταθερό όρο;

9. Στο $\mathbb{Z}_p[x]$, όπου p είναι ένας πρώτος, έστω $f(x) = x^3 - 4x^2 + 3x$, $g(x) = x^2 - 3x + 2$. Για ποιούς πρώτους p ο βαθμός του $\mu\kappa\delta(f(x), g(x))$ είναι

   i. 2;

   ii. 1;

   iii. 0;

10. Να προσδιοριστεί ένα μη μηδενικό $f(x) \in \mathbb{Q}[x]$ βαθμού το πολύ 3 τέτοιο ώστε $\mu\kappa\delta(f(x), x^2 + 1) \neq 1$ και $\mu\kappa\delta(f(x), x^2 - 3x + 2) \neq 1$.

11. Έστω $f(x), g(x) \in F[x]$, σχετικά πρώτα πολυώνυμα θετικού βαθμού, όπου το F είναι ένα σώμα. Αν υπάρχει $h(x) \in F[x]$ με $f(x)g(x) = h(x)^n$, τότε υπάρχουν $a(x), b(x) \in F[x]$ με $f(x) = c_1 a(x)^n$, $g(x) = c_2 b(x)^n$, $c_i \in F$.

12. Αποδείξτε ότι δεν υπάρχει $f(x) \in \mathbb{R}[x]$ τέτοιο ώστε $(x-1)^{143} + (x+1)^{2002} = f(x)^{13}$.

13. Εφαρμόστε τον Αλγόριθμο Διαίρεσης στα πολυώνυμα $f(x, y) = x^2y^2 - xy + 1$, $g(x, y) = x^2 - y$ θεωρώντας αυτά ως στοιχεία του

   i. $(\mathbb{Q}[x])[y]$

   ii. $(\mathbb{Q}[y])[x]$.

14. Έστω F ένα σώμα.

   i. Αποδείξτε ότι υπάρχουν άπειρα το πλήθος ανάγωγα πολυώνυμα στο $F[x]$.

   ii. Έστω ότι το F είναι πεπερασμένο. Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ υπάρχει ανάγωγο πολυώνυμο στο $F[x]$ βαθμού $\geq n$.

2.4 Ρίζες Πολυωνύμων

Στην προηγούμενη Παράγραφο μελετήσαμε ιδιότητες του πολυωνυμικού δακτυλίου $F[x]$, όπου το F είναι ένα σώμα, που ήταν ανάλογες με ιδιότητες του $\mathbb{Z}$. Στην Παράγραφο αυτή θα εξετάσουμε άλλες σημαντικές ιδιότητες του $F[x]$ για τις οποίες δεν υπάρχουν αντίστοιχες ιδιότητες του $\mathbb{Z}$. Αυτές αναφέρονται σε ρίζες πολυωνύμων.

Ρίζες πολυωνύμων

Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και $f(x) \in R[x]$. Ένα στοιχείο $a \in R$ ονομάζεται **ρίζα** του $f(x)$ αν $f(a) = 0$. Για παράδειγμα, οι ρίζες του $x^2 - 5x + 6 \in \mathbb{R}[x]$ είναι οι 2 και 3, ενώ το $x^2 + 1 \in \mathbb{R}[x]$ δεν έχει ρίζες στο $\mathbb{R}$. Αν όμως θεωρήσουμε ότι $x^2 + 1 \in \mathbb{C}[x]$, τότε οι ρίζες του είναι το i και το $-i$.

Στην περίπτωση που ο δακτύλιος R είναι σώμα, έστω F, μπορούμε να συνάγουμε από τον Αλγόριθμο Διαίρεσης στο $F[x]$ σημαντικά συμπεράσματα που αφορούν ρίζες ενός $f(x) \in F[x]$.

2.4.1 Θεώρημα. *Έστω F ένα σώμα, $f(x) \in F[x]$ και $a \in F$. Τότε:*

1) *Το υπόλοιπο της διαίρεσης του $f(x)$ με το $x - a$ είναι το $f(a)$.*

2) *Το a είναι ρίζα του $f(x)$ αν και μόνο αν $x - a | f(x)$.*

Απόδειξη. 1. Από τον Αλγόριθμο Διαίρεσης στο $F[x]$ υπάρχουν $q(x), r(x) \in F[x]$ τέτοια ώστε

$$f(x) = q(x)(x - a) + r(x), \quad \deg r(x) < 1.$$

Επειδή $\deg r(x) < 1$ το $r(x)$ είναι ένα σταθερό πολυώνυμο, έστω $r(x) = c \in F$. Άρα $c = f(x) - q(x)(x - a)$ και κατά συνέπεια $c = f(a) - q(a)(a - a) = f(a)$. 2. Το a είναι ρίζα του $f(x)$ αν και μόνο αν το υπόλοιπο της διαίρεσης του $f(x)$ με το $x - a$ είναι 0, δηλαδή αν και μόνο αν $x - a | f(x)$. ⊤

2.4.2 Πόρισμα. *Έστω F ένα σώμα και $f(x) \in F[x]$ ένα μη μηδενικό πολυώνυμο. Τότε το $f(x)$ έχει το πολύ $\deg f(x)$ ρίζες στο F.*

Απόδειξη. Θα χρησιμοποιήσουμε επαγωγή στο $n = \deg f(x)$. Για $n = 0$, το $f(x)$ είναι μια μη μηδενική σταθερά και κατά συνέπεια δεν έχει ρίζες. Έστω τώρα ότι αληθεύει το Θεώρημα για κάθε πολυώνυμο βαθμού $n - 1$. Αν το $f(x)$ δεν έχει ρίζες στο F τότε το Θεώρημα αληθεύει. Έστω $a \in F$ μια ρίζα του $f(x)$. Τότε από το προηγούμενο Θεώρημα έχουμε

$$f(x) = (x - a)g(x), \quad g(x) \in F[x].$$

Από την Πρόταση 2.2.4 2) παίρνουμε $\deg g(x) = n-1$. Από την επαγωγική υπόθεση, το $g(x)$ έχει το πολύ $n-1$ ρίζες στο F. Άρα το πλήθος των ριζών του $f(x)$ είναι το πολύ $1+(n-1)=n$. ⊤

2.4.3 Σημειώσεις.

1) Το Θεώρημα 2.4.1 και το Πόρισμα 2.4.2 ισχύουν και όταν στη θέση του σώματος F υπάρχει μια ακεραία περιοχή R. Πράγματι, επειδή το $x-a$ που εμφανίζεται στην απόδειξη του Θεωρήματος 2.4.1 είναι μονικό, μπορούμε να εφαρμόσουμε τον Αλγόριθμο Διαίρεσης στο $R[x]$, Θεώρημα 2.3.5, στη θέση του Αλγορίθμου Διαίρεσης στο $F[x]$. Από εκεί και πέρα οι αποδείξεις δεν διαφοροποιούνται.

2) Το Πόρισμα 2.4.2 δεν αληθεύει όταν ο R δεν είναι ακεραία περιοχή. Για παράδειγμα, έστω $f(x) = x^3 - x \in \mathbb{Z}_6[x]$. Τότε εύκολα επαληθεύουμε με πράξεις στο $\mathbb{Z}_6$ ότι $f(a) = 0$ για κάθε $a \in \mathbb{Z}_6$. Το $f(x)$ έχει 6 ρίζες στο $\mathbb{Z}_6$, παρόλο που ο βαθμός του είναι 3.

2.4.4 Εφαρμογή.

Εύκολα βλέπουμε ότι στο $\mathbb{Z}_3$ η εξίσωση $x^2 = 2$ δεν έχει λύση. Δηλαδή, το στοιχείο $2 \in \mathbb{Z}_3$ δεν έχει τετραγωνική ρίζα στο $\mathbb{Z}_3$. Το επόμενο ***κριτήριο του Euler*** περιγράφει τα στοιχεία του $\mathbb{Z}_p$ που έχουν τετραγωνική ρίζα στο $\mathbb{Z}_p$: Έστω p ένας περιττός πρώτος αριθμός και $a \in \mathbb{Z}_p$ με $a \neq 0$. Τότε το a έχει τετραγωνική ρίζα στο $\mathbb{Z}_p$ αν και μόνο αν $a^{\frac{p-1}{2}} = 1$.

Πράγματι, έστω $r = \dfrac{p-1}{2}$, που είναι ένας ακέραιος αριθμός λόγω της υπόθεσης. Θα δείξουμε ότι: υπάρχει $x \in \mathbb{Z}_p$ με $a = x^2$ αν και μόνο αν $a^r = 1$. Για το σκοπό αυτό έστω

$$S = \{b \in \mathbb{Z}_p - \{0\} | b = x^2 \text{ για κάποιο } x \in \mathbb{Z}_p\}, \text{ και}$$
$$T = \{b \in \mathbb{Z}_p | b^r = 1\}.$$

Αρκεί να δείξουμε ότι $S = T$. Παρατηρούμε τα εξής:

1. Ισχύει $S \subseteq T$. Πράγματι, αν $s \in S$, τότε $s = x^2$ για κάποιο μη μηδενικό $x \in \mathbb{Z}_p$, οπότε από το Μικρό Θεώρημα του Fermat παίρνουμε $s^r = x^{2r} = x^{p-1} = 1$.

2. Τα στοιχεία $1^2, 2^2, \ldots, r^2$ του S είναι διακεκριμένα.
Πράγματι, αν $i^2 = j^2$ τότε $(i-j)(i+j) = 0$ και επειδή ο $\mathbb{Z}_p$ είναι ακεραία περιοχή παίρνουμε $i = j$ ή $i + j = 0$. Όμως δεν είναι δυνατό να ισχύει η τελευταία ισότητα, αφού το $i+j$ ανήκει στο σύνολο $\{2, 3, \ldots, 2r = p-1\}$ που δεν περιέχει το 0.

3. Το σύνολο T περιέχει το πολύ r στοιχεία.
   Πράγματι, αυτό έπεται από το Πόρισμα 2.4.2 γιατί κάθε στοιχείο του T είναι ρίζα του πολυωνύμου $x^r - 1 \in \mathbb{Z}_p[x]$.

Από τα 1,2,3 συμπεραίνουμε ότι $S = T$.

Ρίζες και ανάγωγα πολυώνυμα

Έστω $f(x) \in F[x]$ με $\deg f(x) > 1$. Από το Θεώρημα 2.4.1 2) είναι φανερό ότι αν το $f(x)$ είναι ανάγωγο, τότε δεν έχει ρίζα στο F. Το αντίστροφο γενικά δεν ισχύει. Για παράδειγμα το $(x^2+1)^2 \in \mathbb{R}[x]$ δεν έχει ρίζα στο $\mathbb{R}$ και δεν είναι ανάγωγο στο $\mathbb{R}[x]$. Όταν όμως ο βαθμός του $f(x)$ είναι 2 ή 3 έχουμε το ακόλουθο αποτέλεσμα.

2.4.5 Πρόταση. *Έστω F ένα σώμα και $f(x) \in F[x]$ με $\deg f(x) = 2$ ή 3. Αν το $f(x)$ δεν έχει ρίζα στο F τότε το $f(x)$ είναι ανάγωγο στο $F[x]$.*

Απόδειξη. Έστω ότι $\deg f(x) = 2$ ή 3 και ότι το $f(x)$ δεν είναι ανάγωγο στο $F[x]$. Θα δείξουμε ότι το $f(x)$ έχει μια τουλάχιστον ρίζα στο F. Επειδή το $f(x)$ δεν είναι ανάγωγο, υπάρχουν μη σταθερά $g(x), h(x) \in F[x]$ τέτοια ώστε

$$f(x) = g(x)h(x),$$

όπου $\deg g(x) < \deg f(x)$ και $\deg h(x) < \deg f(x)$. Άρα

$$\deg f(x) = \deg h(x) + \deg g(x).$$

Επειδή $\deg f(x) = 2$ ή 3 συμπεραίνουμε ότι ένα τουλάχιστον από τα $h(x)$ και $g(x)$ έχει βαθμό 1. Αλλά κάθε πολυώνυμο στο $F[x]$ βαθμού 1 είναι της μορφής $ax + b$, όπου $a, b \in F$, $a \neq 0$, και συνεπώς έχει ρίζα (την $-a^{-1}b$) στο F. ⊤

2.4.6 Εφαρμογές.

1) Θα προσδιορίσουμε την ανάλυση του $f(x) = x^4+2x^3+x^2+2x+2 \in \mathbb{Z}_3[x]$ σε γινόμενο αναγώγων.
   Πρώτα ελέγχουμε αν το $f(x)$ έχει ρίζες στο $\mathbb{Z}_3$. Υπολογίζουμε τα $f(0)$, $f(1)$ και $f(2)$ και διαπιστώνουμε ότι $f(2) = 0$. Από το Θεώρημα 2.4.1 2) συμπεραίνουμε ότι $x - 2 | f(x)$. Εφαρμόζοντας τον Αλγόριθμο Διαίρεσης στο $\mathbb{Z}_3[x]$ βρίσκουμε ότι $f(x) = (x-2)(x^3+x^2+2)$. Εξετάζουμε τώρα αν το x^3+x^2+2 είναι ανάγωγο. Με πράξεις διαπιστώνουμε ότι το x^3+x^2+2 δεν έχει ρίζα στο $\mathbb{Z}_3$. Επειδή το πολυώνυμο αυτό έχει βαθμό 3, από την Πρόταση 2.4.5 έχουμε ότι αυτό είναι ανάγωγο στο $\mathbb{Z}_3[x]$. Άρα η ζητούμενη ανάλυση του $f(x)$ είναι $f(x) = (x-2)(x^3+x^2+2)$.

2) Έστω p ένας πρώτος αριθμός. Στο $\mathbb{Z}_p[x]$ ισχύει

$$x^p - x = x(x-1)(x-2)\dots(x-(p-1)). \tag{1}$$

Πράγματι, έστω $f(x) = x^p - x$ και $g(x) = x(x-1)(x-2)\dots(x-(p-1))$. Από το Μικρό Θεώρημα του Fermat, κάθε $a \in \mathbb{Z}_p$ είναι ρίζα του $f(x)$. Συνεπώς από το Θεώρημα 2.4.1 2) συμπεραίνουμε ότι $x-a|f(x)$ για κάθε $a \in \mathbb{Z}_p$. Επειδή τα πολυώνυμα $x-a$, $a = 0, 1, \dots, p-1 \in \mathbb{Z}_p$, είναι μονικά ανάγωγα και ανά δύο διάφορα, παίρνουμε από το Παράδειγμα 2.3.11 2) ότι το γινόμενό τους διαιρεί το $f(x)$. Δηλαδή έχουμε $g(x)|f(x)$. Επειδή όμως $\deg g(x) = \deg f(x)$, από τη σχέση $g(x)|f(x)$ συμπεραίνουμε ότι $f(x) = cg(x)$ για κάποιο $c \in \mathbb{Z}_p$. Παρατηρούμε ότι τα $f(x)$ και $g(x)$ είναι μονικά. Άρα $c = 1$ και $f(x) = g(x)$.

3) **(Θεώρημα του Wilson)** Για κάθε πρώτο αριθμό p ισχύει $(p-1)! \equiv -1 \mod p$.

Είναι φανερό ότι το ζητούμενο ισχύει για $p = 2$, αφού $1 \equiv -1 \mod 2$. Έστω τώρα ότι $p > 2$. Ο συντελεστής του x του αριστερού μέλους της ισότητας (;;) στο προηγούμενο παράδειγμα είναι - $1 \in \mathbb{Z}_p$ ενώ ο συντελεστής του x στο δεξιό μέλος της (;;) είναι
$(-1)(-2)\dots(-(p-1)) = (-1)^{p-1} \cdot 1 \cdot 2 \cdot \dots \cdot (p-1) \in \mathbb{Z}_p$. Άρα στο $\mathbb{Z}_p$ έχουμε

$$-1 = (-1)^{p-1} \cdot 1 \cdot 2 \cdot \dots \cdot (p-1).$$

Επειδή ο p είναι περιττός έχουμε $(-1)^{p-1} = 1$ και άρα $-1 = 1 \cdot 2 \cdot \dots \cdot (p-1)$ στο $\mathbb{Z}_p$. Τελικά στο $\mathbb{Z}$ έχουμε $-1 \equiv (p-1)! \mod p$.

4) Έστω F ένα άπειρο σώμα και $f(x), g(x) \in F[x]$. Τότε

$$f(a) = g(a) \text{ για κάθε } a \in F \Leftrightarrow f(x) = g(x).$$

Έστω $f(a) = g(a)$ για κάθε $a \in F$. Τότε το πολυώνυμο $g(x) - f(x)$ έχει άπειρες ρίζες. Από το Πόρισμα 2.4.2 έχουμε ότι $f(x) - g(x) = 0$. Αντίστροφα, αν $f(x) = g(x)$, τότε είναι προφανές ότι $f(a) = g(a)$ για κάθε $a \in F$.

5) Έστω p ένας πρώτος αριθμός και $f(x), g(x) \in \mathbb{Z}_p[x]$. Τότε

$$f(a) = g(a) \text{ για κάθε } a \in \mathbb{Z}_p \Leftrightarrow x^p - x | f(x) - g(x).$$

Πράγματι, έστω $f(a) = g(a)$ για κάθε $a \in \mathbb{Z}_p$. Τότε κάθε $a \in \mathbb{Z}_p$ είναι ρίζα του $f(x) - g(x)$. Όπως ακριβώς στην απόδειξη της Εφαρμογής 2)

παίρνουμε ότι $x(x-1)\dots(x-(p-1))|f(x)-g(x)$. Αλλά $x(x-1)\dots(x-(p-1))=x^p-x$. Αντίστροφα, έστω ότι $x^p-x|f(x)-g(x)$ οπότε υπάρχει $h(x)\in F[x]$ τέτοιο ώστε $f(x)-g(x)=(x^p-x)h(x)$. Τότε έχουμε $f(a)-g(a)=(a^p-a)h(a)=0$ για κάθε $a\in\mathbb{Z}_p$, αφού $a^p-a=0$ για κάθε $a\in\mathbb{Z}_p$ από το Μικρό Θεώρημα του Fermat.

2.4.7 Σημείωση. Έστω F ένα σώμα και $f(x),g(x)\in F[x]$. Είναι προφανές ότι αν $f(x)=g(x)$ τότε οι αντίστοιχες πολυωνυμικές συναρτήσεις $\bar{f},\bar{g}:F\to F$ (βλ. Παράγραφο 2.2) είναι ίσες. Γνωρίζουμε ότι το αντίστροφο γενικά δεν ισχύει (βλ. Παράδειγμα 2.2.7). Η Εφαρμογή 2.4.6 4) μας πληροφορεί ότι αν το F είναι άπειρο ισχύει το αντίστροφο,

$$\bar{f}=\bar{g}\Rightarrow f(x)=g(x).$$

Η εφαρμογή 2.4.6 5) μας πληροφορεί ότι αν $F=\mathbb{Z}_p$, p πρώτος, τότε

$$\bar{f}=\bar{g}\Rightarrow x^p-x|f(x)-g(x).$$

Θεμελιώδες Θεώρημα της Άλγεβρας

Θα ασχοληθούμε τώρα με πολυώνυμα των οποίων οι συντελεστές ανήκουν στο $\mathbb{R}$ ή το $\mathbb{C}$. Το παρακάτω Θεώρημα αποδείχτηκε από τον Gauss στη διδακτορική διατριβή του το 1799 και είναι τόσο σημαντικό για την Άλγεβρα με αποτέλεσμα να ονομάζεται το Θεμελιώδες Θεώρημα της Άλγεβρας. Θα παραλείψουμε την απόδειξη γιατί όλες οι γνωστές αποδείξεις χρησιμοποιούν μέσα που υπερβαίνουν το σκοπό του βιβλίου αυτού.

2.4.8 Θεμελιώδες Θεώρημα της Άλγεβρας. *Κάθε πολυώνυμο $f(x)\in\mathbb{C}[x]$ θετικού βαθμού έχει μία τουλάχιστον ρίζα στο $\mathbb{C}$.*

Γνωρίζουμε ότι κάθε πολυώνυμο $f(x)\in F[x]$, F σώμα, γράφεται ως γινόμενο αναγώγων πολυωνύμων (Θεώρημα 2.3.10). Το Θεμελιώδες Θεώρημα της Άλγεβρας μας πληροφορεί ότι τα ανάγωγα πολυώνυμα του $\mathbb{C}[x]$ είναι τα πολυώνυμα που έχουν βαθμό 1. Επομένως ισχύει το εξής.

2.4.9 Πόρισμα. *Κάθε $f(x)\in\mathbb{C}[x]$ βαθμού $n\geq 1$ έχει μια παραγοντοποίηση της μορφής*

$$f(x)=c(x-a_1)(x-a_2)\dots(x-a_n),$$

με $c\in\mathbb{C}\setminus\{0\}$ και $a_1,\dots,a_n\in\mathbb{C}$ (όχι αναγκαστικά διακεκριμένα).

Είδαμε στο Πόρισμα 2.4.2 ότι κάθε μη μηδενικό $f(x)\in F[x]$, όπου το F είναι σώμα, έχει το πολύ $n=\deg f(x)$ ρίζες στο F . Το Πόρισμα 2.4.9 μας

πληροφορεί ότι κάθε μη μηδενικό $f(x) \in \mathbb{C}[x]$ βαθμού n έχει ακριβώς n ρίζες (όχι αναγκαστικά διακεκριμένες) στο $\mathbb{C}$.

Χρησιμοποιώντας τα προηγούμενα, θα προσδιορίσουμε τώρα όλα τα ανάγωγα πολυώνυμα του $\mathbb{R}[x]$. Υπενθυμίζουμε ότι αν $z \in \mathbb{C}$, $z = a + bi (a, b \in \mathbb{R})$ τότε ο συζυγής του z είναι $\bar{z} = a - bi$. Έχουμε $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$, $\overline{z_1} \cdot \overline{z_2} = \overline{z_1 \cdot z_2}$ για κάθε $z_1, z_2 \in \mathbb{C}$.

2.4.10 Θεώρημα. *Έστω $f(x) \in \mathbb{R}[x]$.*

1. *Αν ο μιγαδικός αριθμός z είναι ρίζα του $f(x)$, τότε και ο συζυγής του, $\bar{z}$, είναι ρίζα του $f(x)$.*

2. *Το $f(x)$ είναι ανάγωγο στο $\mathbb{R}[x]$ αν και μόνο αν*

   - $f(x) = ax + b$, $a \neq 0$, *ή*
   - $f(x) = ax^2 + bx + c$ *και* $b^2 - 4ac < 0$.

Απόδειξη. 1. Έστω $z \in \mathbb{C}$ μία ρίζα του $f(x) \in \mathbb{R}[x]$, $f(x) = f_n x^n + \cdots + f_1 x + f_0$. Τότε παίρνουμε:

$$\begin{aligned} 0 = f(z) \Rightarrow 0 = \overline{f(z)} &= \overline{f_n z^n + \cdots + f_1 z + f_0} = \overline{f_n z^n} + \cdots + \overline{f_1 z} + \overline{f_0} \\ &= \overline{f_n}\overline{z^n} + \cdots + \overline{f_1}\bar{z} + \overline{f_0} = f_n \overline{z^n} + \cdots + f_1 \bar{z} + f_0 = f(\bar{z}). \end{aligned}$$

2. Έστω $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$. Από την Πρόταση 2.4.5, το $f(x)$ είναι ανάγωγο στο $\mathbb{R}[x]$ αν και μόνο αν δεν έχει καμιά πραγματική ρίζα, δηλαδή αν και μόνο αν $b^2 - 4ac < 0$.

Έστω τώρα $f(x) \in \mathbb{R}[x]$ ένα πολυώνυμο βαθμού ≥ 3. Θα δείξουμε ότι το $f(x)$ δεν είναι ανάγωγο. Από το Θεμελιώδες Θεώρημα της Άλγεβρας, το $f(x)$ έχει μια ρίζα $z \in \mathbb{C}$. Αν $z \in \mathbb{R}$, τότε το $f(x)$ δεν είναι ανάγωγο. Έστω $z \in \mathbb{C} - \mathbb{R}$. Από το 1. του Θεωρήματος το $\bar{z}$ είναι επίσης ρίζα. Θεωρώντας ότι $f(x) \in \mathbb{C}[x]$, η Πρόταση 2.4.1 2) δίνει ότι

$$x - z | f(x) \quad \text{και} \quad x - \bar{z} | f(x) \quad \text{στο} \quad \mathbb{C}[x].$$

Επειδή ισχύει $z \neq \bar{z}$ από το Παράδειγμα 2.3.11 3) έχουμε ότι $(x - z)(x - \bar{z}) | f(x)$ στο $\mathbb{C}[x]$. Αλλά παρατηρούμε ότι το $(x - z)(x - \bar{z})$ έχει πραγματικούς συντελεστές, αφού $(x - z)(x - \bar{z}) = x^2 - (z + \bar{z})x + z\bar{z}$ και $z + \bar{z}, z\bar{z} \in \mathbb{R}$. Τότε σύμφωνα με την Άσκηση 2.3.2 έχουμε ότι $(x - z)(x - \bar{z}) | f(x)$ στο $\mathbb{R}[x]$. Επειδή $\deg f(x) > 2$ αυτό σημαίνει ότι το $f(x)$ δεν είναι ανάγωγο στο $\mathbb{R}[x]$. ⊤

Ένα αποτέλεσμα που μας βοηθά να προσδιορίζουμε πιθανές ρητές ρίζες ενός πολυωνύμου που έχει ακεραίους συντελεστές είναι το επόμενο.

2.4.11 Πρόταση. *Έστω* $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. *Αν το* $\frac{r}{s} \in \mathbb{Q}$ *είναι μία ρίζα του* $f(x)$, *όπου* $r, s \in \mathbb{Z}$, $\mu\kappa\delta(r,s) = 1$, *τότε* $r|a_0$ *και* $s|a_n$.

Απόδειξη. Από τη σχέση $f\left(\frac{r}{s}\right) = 0$ παίρνουμε

$$a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n = 0.$$

Επομένως ο ακέραιος r διαιρεί τον $a_0 s^n$. Επειδή $\mu\kappa\delta(r,s) = 1$, έχουμε $r|a_0$. Με όμοιο τρόπο αποδεικνύεται ότι $s|a_n$. ⊺

Παράδειγμα. Για να βρούμε την ανάλυση του $f(x) = x^3 - 3x^2 + 2x - 6 \in \mathbb{Q}[x]$ σε γινόμενο αναγώγων, εξετάζουμε πρώτα αν το $f(x)$ έχει ρίζα στο $\mathbb{Q}$. Σύμφωνα με την προηγούμενη Πρόταση οι υποψήφιες ρητές ρίζες του $f(x)$ είναι $\pm 1, \pm 2, \pm 3, \pm 6$. Παρατηρούμε ότι $f(3) = 0$. Άρα $x - 3 | f(x)$. Από τον Αλγόριθμο Διαίρεσης έχουμε $f(x) = (x-3)(x^2+2)$. Είναι φανερό ότι το $x^2 + 2$ είναι ανάγωγο στο $\mathbb{Q}[x]$.

Ασκήσεις 2.4

1. Να βρεθεί το a ώστε το υπόλοιπο της διαίρεσης του $x^3 + 2x^2 - 3ax + 1 \in \mathbb{Q}[x]$ με το $x - 2$ να είναι 1.

2. Ποια από τα παρακάτω πολυώνυμα είναι ανάγωγα επί του F;

   a. $x^2 - 7$, $F = \mathbb{R}$
   b. $x^2 - 7$, $F = \mathbb{Q}$
   c. $x^2 - 7$, $F = \mathbb{C}$
   d. $x^3 - 9$, $F = \mathbb{Z}_{11}$
   e. $2x^3 + x^2 + 2x + 2$, $F = \mathbb{Z}_5$.

3. Να βρεθεί ένα πολυώνυμο $f(x) \in \mathbb{R}[x]$ βαθμού 4 που αφήνει υπόλοιπα 3 και 4 όταν διαιρεθεί με τα $x - 1$ και $x - 2$ αντίστοιχα.

4. Αποδείξτε ότι κάθε $f(x) \in \mathbb{R}[x]$ περιττού βαθμού έχει μία τουλάχιστον πραγματική ρίζα. Δώστε ένα παράδειγμα πολυωνύμου στο $\mathbb{R}[x]$ βαθμού 2004 που δεν έχει πραγματικές ρίζες.

5. Για ποιους πρώτους p το $x^3 + 3x^2 - 6x + 1 \in \mathbb{Z}_p[x]$ διαιρείται με το $x - 1$;

6. Πόσες ρίζες έχει το $x^2 - x$ στο $\mathbb{Z}_{10}$; Στο $\mathbb{Z}_{11}$; Γιατί οι απαντήσεις είναι διαφορετικές;

7. Ποια είναι η παραγοντοποίηση του $x^3+2x^2+x+1 \in \mathbb{Z}_3[x]$ σε γινόμενο αναγώγων;

8. Ποια είναι η παραγοντοποίηση των x^4+2, $x^5+3x^4+2x+1 \in \mathbb{Z}_5[x]$ σε γινόμενο αναγώγων;

9. Να βρεθεί ένα πολυώνυμο στο $\mathbb{Z}_5[x]$ βαθμού το πολύ 4 που επάγει την ίδια απεικόνιση $\mathbb{Z}_5 \to \mathbb{Z}_5$ με αυτήν που επάγει το πολυώνυμο $x^9+2x^7+3x^3+1$.

10. Γιατί η απεικόνιση $\mathbb{R} \ni x \mapsto \eta\mu x \in \mathbb{R}$ δεν είναι πολυωνυμική;

11. Να βρεθεί η παραγοντοποίηση του x^4-1 σε γινόμενο αναγώγων πολυωνύμων επί των σωμάτων $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$ και $\mathbb{Z}_3$.

12. Αποδείξτε ότι το σύνολο $S = \{f(x) \in \mathbb{R}[x] | f(1) = 0\}$ είναι ένας υποδακτύλιος του $\mathbb{R}[x]$. Αληθεύει ότι το S είναι σώμα; Ακεραία περιοχή; Αποδείξτε ότι $S = \{(x-1)g(x) | g(x) \in \mathbb{R}[x]\}$.

13. Έστω F ένα σώμα και $a_1, \ldots, a_n$ διακεκριμένα στοιχεία του. Αποδείξτε ότι το σύνολο $S = \{f(x) \in F[x] | f(a_1) = \cdots = f(a_n) = 0\}$ είναι υποδακτύλιος του $F[x]$ και ότι $S = \{(x-a_1)\cdots(x-a_n)g(x) | g(x) \in F[x]\}$.

14. Να βρεθούν οι ρίζες του πολυωνύμου x^3-4x^2+6x-4 στο $\mathbb{C}$ αν είναι γνωστό ότι μία ρίζα του είναι η $1-i$.

15. Να βρεθούν οι ρίζες του πολυωνύμου x^4+x^2+1 στο $\mathbb{C}$ αν είναι γνωστό ότι μία ρίζα του είναι η $\dfrac{-1+i\sqrt{3}}{2}$.

16. Αληθεύει ότι το στοιχείο $3 \in \mathbb{Z}_{11}$ έχει τετραγωνική ρίζα; Υπάρχει ακέραιος b τέτοιος ώστε $7 \equiv b^2 \mod 31$;

17. Έστω $\zeta = \sigma\upsilon\nu\dfrac{2\pi}{n} + i\eta\mu\dfrac{2\pi}{n} \in \mathbb{C}$ όπου n είναι ένας θετικός ακέραιος. Δείξτε ότι $x^n-1 = (x-1)(x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{n-1})$. Συμπεράνετε ότι αν $n \geq 3$ τότε $\displaystyle\sum_{0 \leq k < l \leq n-1} \sigma\upsilon\nu\frac{(k+l)2\pi}{n} = 0$, όπου $k, l \in \mathbb{N}$.

18. Αποδείξτε ότι

    i. $\displaystyle\sum_{0<i<j<p} ij \equiv 0 \mod p$ για κάθε πρώτο αριθμό $p > 3$, και

    ii. $\displaystyle\sum_{0<i<j<k<p} ijk \equiv 0 \mod p$ για κάθε πρώτο αριθμό $p \geq 5$.

Υπόδειξη: Χρησιμοποιήστε τη σχέση $x^p - x = \prod_{i=0}^{p-1}(x-i) \in \mathbb{Z}_p[x]$.

19. Να βρεθεί το υπόλοιπο της διαίρεσης του $98!$ με το 101 και να δειχθεί ότι $(50!)^2 \equiv -1 \mod 101$.

20. Έστω p ένας πρώτος αριθμός τέτοιος ώστε $p \equiv 3 \mod 4$. Αποδείξτε ότι

    i. $1^2 2^2 3^2 \ldots \left(\frac{p-1}{2}\right)^2 \equiv 1 \mod p$.

    ii. $1^2 3^2 5^2 \ldots (p-2)^2 \equiv 1 \mod p$.

    iii. $\left(\frac{p-1}{2}\right)! \equiv \pm 1 \mod p$.

21. Αποδείξτε ότι το $x^2 + 1 \in \mathbb{Z}_p[x]$, p πρώτος, είναι ανάγωγο αν και μόνο αν δεν υπάρχουν $a, b \in \mathbb{Z}$ με $p = a + b$ και $ab \equiv 1 \mod p$.

22. Η άσκηση αυτή αφορά πολυώνυμα υπεράνω του $\mathbb{Z}_2$ και σκιαγραφεί ένα αλγόριθμο που προσδιορίζει τα ανάγωγα πολυώνυμα.

    i. Δείξτε ότι το $x-1$ διαιρεί το $f(x)$ στο $\mathbb{Z}_2[x]$ αν και μόνον αν το $f(x)$ έχει άρτιο πλήθος μη μηδενικών συντελεστών.

    ii. Δείξτε ότι αν $\deg f(x) > 1$ και το $f(x)$ είναι ανάγωγο στο $\mathbb{Z}_2[x]$ τότε το $f(x)$ έχει σταθερό όρο το 1 και ένα περιττό πλήθος μη-μηδενικών συντελεστών.

    iii. Καθορίστε όλα τα ανάγωγα πολυώνυμα βαθμού ≤ 4 στο $\mathbb{Z}_2[x]$.

    iv. Συνεχίζοντας την προηγούμενη εργασία, μπορείτε να βρείτε όλα τα ανάγωγα πολυώνυμα βαθμού ≤ 5 στο $\mathbb{Z}_2$; Είναι πρακτικός κατά τη γνώμη σας αυτός ο αλγόριθμος;

23. Να βρεθεί η ανάλυση του $f(x) = x^4 - 2x^3 - 2x + 4$ σε γινόμενο αναγώγων πολυωνύμων επί των σωμάτων $\mathbb{Q}$, $\mathbb{R}$ και $\mathbb{C}$.

24. Αποδείξτε ότι το $x^2 + x + 1$ διαιρεί το $(x+1)^n + x^n + 1$ στο $\mathbb{C}[x]$ αν και μόνο αν $n \equiv 2, 4 \mod 6$.

2.5 Ομομορφισμοί και Ιδεώδη

Ομομορφισμοί δακτυλίων

Ένα από τα πιο βασικά ερωτήματα που συναντάμε στη μελέτη αλγεβρικών συστημάτων (δηλαδή, συνόλων που είναι εφοδιασμένα με μία ή περισσότερες πράξεις, όπως είναι για παράδειγμα οι δακτύλιοι) είναι να αποφανθούμε αν δύο από αυτά είναι "ίδια". Ας δούμε ένα πολύ απλό παράδειγμα. Έστω το σύνολο $R = \{a, b\}$ με πράξεις που ορίζονται από τους πίνακες

$+$	a	b
a	a	b
b	b	a

$\cdot$	a	b
a	a	a
b	a	b

Εύκολα ελέγχουμε ότι το R είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο (το b). Θεωρούμε τώρα το δακτύλιο $\mathbb{Z}_2$ και τους αντίστοιχους πίνακες:

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

Παρατηρούμε ότι αν στους πρώτους πίνακες "μετονομάσουμε" τα στοιχεία a και b σε $[0]$, $[1]$ αντίστοιχα, τότε προκύπτουν οι πίνακες για τον $\mathbb{Z}_2$. Αυτό σημαίνει ότι οι πράξεις στο R είναι ουσιαστικά ίδιες με τις αντίστοιχες πράξεις στο $\mathbb{Z}_2$ και το μόνο που αλλάζει είναι ο συμβολισμός των στοιχείων. Συνεπώς οι R και $\mathbb{Z}_2$ έχουν τις ίδιες ιδιότητες ως δακτύλιοι και επομένως δεν υπάρχει λόγος διάκρισής τους. Οι δακτύλιοι αυτοί είναι, όπως λέμε, *ισόμορφοι*. (Ακριβής ορισμός δίνεται παρακάτω).

Ας δούμε τώρα ένα άλλο παράδειγμα. Το σύνολο των μιγαδικών αριθμών $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$ με τις συνήθεις πράξεις είναι ένας δακτύλιος. Θεωρούμε το υποσύνολο R του $M_2(\mathbb{R})$ που αποτελείται από τους πίνακες της μορφής $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $a, b \in \mathbb{R}$. Εύκολα αποδεικνύεται ότι το R ως προς τη πρόσθεση και τον πολλαπλασιασμό πινάκων είναι δακτύλιος (βλ. Παράδειγμα 2.1.11 5). Μεταξύ του R και $\mathbb{C}$ υπάρχει η $1-1$ και επί απεικόνιση

$$\phi : R \ni \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + bi \in \mathbb{C}.$$

Ας υπολογίσουμε τις εικόνες του αθροίσματος και του γινομένου δύο πινάκων.

Έχουμε

$$\begin{aligned}\phi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) &= \phi\begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \\ &= (a+c)+(b+d)i \\ &= (a+bi)+(a+d)i \\ &= \phi\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \phi\begin{pmatrix} c & d \\ -c & d \end{pmatrix},\end{aligned}$$

και

$$\begin{aligned}\phi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) &= \phi\begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} \\ &= (ac-bd)+(ad+bd)i \\ &= (a+bi)(c+di) \\ &= \phi\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\phi\begin{pmatrix} c & d \\ -c & d \end{pmatrix}.\end{aligned}$$

Δηλαδή έχουμε

$$\begin{aligned}\phi(A+B) &= \phi(A)+\phi(B), \\ \phi(AB) &= \phi(A)\phi(B)\end{aligned}$$

για κάθε $A, B \in R$. Επειδή η ϕ είναι $1-1$ και επί, συμπεραίνουμε ότι *οι πράξεις στο R (αντίστοιχα, $\mathbb{C}$) καθορίζονται πλήρως από τις πράξεις στο $\mathbb{C}$ (αντίστοιχα, R)*. Μιλώντας με κάποιο βαθμό ελευθερίας, αν ταυτίσουμε τον πίνακα $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ με τον μιγαδικό αριθμό $\phi(A) = a+bi$, τότε οι πράξεις των R και $\mathbb{C}$ είναι ουσιαστικά οι ίδιες και το μόνο που αλλάζει είναι ο συμβολισμός των στοιχείων. Από τη σκοπιά της Άλγεβρας, δηλαδή από τη σκοπιά της μελέτης των ιδιοτήτων των πράξεων των R και $\mathbb{C}$, δεν υπάρχει λόγος διάκρισης των R και $\mathbb{C}$. Οι δακτύλιοι αυτοί είναι, όπως λέμε, ισόμορφοι.

2.5.1 Ορισμός. *Έστω $(R, +, \cdot)$ και $(S, \oplus, *)$ δύο δακτύλιοι. Μια απεικόνιση $\phi : R \to S$ ονομάζεται* **ομομορφισμός δακτυλίων** *αν για κάθε $a, b \in R$ ισχύουν*

$$\phi(a+b) = \phi(a) \oplus \phi(b) \quad \text{και} \quad \phi(a \cdot b) = \phi(a) * \phi(b)$$

Αν επιπλέον η ϕ είναι επί (αντίστοιχα, 1-1) θα ονομάζεται **επιμορφισμός** *(αντίστοιχα,* **μονομορφισμός***). Ένας ομομορφισμός δακτυλίων ονομάζεται* **ισομορφισμός** *αν είναι 1-1 και επί απεικόνιση.*

Σχόλιο

Βλέπουμε ότι οι ομομορφισμοί δακτυλίων "διατηρούν τις πράξεις". Υπενθυμίζουμε ότι μια ανάλογη περίπτωση έχουμε συναντήσει στη Γραμμική Άλγεβρα με τις γραμμικές απεικονίσεις διανυσματικών χώρων. Επειδή κάθε αλγεβρικό σύστημα είναι ένα σύνολο εφοδιασμένο με μία ή περισσότερες πράξεις, οι απεικονίσεις που μελετάμε στην Άλγεβρα είναι συνήθως τέτοιες που διατηρούν τις πράξεις των αλγεβρικών συστημάτων. Θα δούμε παρακάτω ότι οι ομομορφισμοί δακτυλίων είναι ένα μέσο με το οποίο μπορούμε να "συγκρίνουμε" δύο δακτυλίους και ειδικά οι ισομορφισμοί είναι ένα μέσο με το οποίο μπορούμε να "ταυτίζουμε" δύο δακτυλίους.

2.5.2 Παραδείγματα.

1) Έστω $R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_2(\mathbb{R}) \right\}$ ο δακτύλιος του Παραδείγματος 2.1.11 5). Η απεικόνιση

$$\varphi : R \to \mathbb{C}, \quad \phi \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a + bi \in \mathbb{C}$$

είναι ένας ισομορφισμός όπως είδαμε πιο πάνω.

2) Έστω $R = \{a, b\}$ ο δακτύλιος που είδαμε στην αρχή αυτής της Παραγράφου. Η απεικόνιση, $\varphi : R \to \mathbb{Z}_2$, $\varphi(a) = [0]$ και $\varphi(b) = [1]$, είναι ένας ισομορφισμός δακτυλίων.

3) Για κάθε δακτύλιο R, η ταυτοτική απεικόνιση $R \to R$, $r \mapsto r$, είναι ένας ισομορφισμός δακτυλίων. Για κάθε δύο δακτυλίους R, S η απεικόνιση $R \to S$, $r \mapsto 0_S$, είναι ένας ομομορφισμός δακτυλίων που ονομάζεται ο *τετριμμένος ομομορφισμός* (ή μηδενικός ομομορφισμός).

4) Η απεικόνιση $\varphi : \mathbb{C} \to \mathbb{C}$, $\varphi(a + bi) = a - bi$, είναι ένας ομομορφισμός δακτυλίων γιατί

$$\begin{aligned} \varphi((a + bi) + (c + di)) &= \varphi((a + c) + (b + d)i) \\ &= (a + c) - (b + d)i = (a - bi) + (c - di) \\ &= \varphi(a + bi) + \varphi(c + di) \end{aligned}$$

και

$$\begin{aligned} \varphi((a + bi)(c + di)) &= \varphi((ac - bd) + (ad + bc)i) \\ &= (ac - bd) - (ad + bc)i = (a - bi)(c - di) \\ &= \varphi(a + bi)\varphi(c + di). \end{aligned}$$

Επιπλέον είναι φανερό ότι η φ είναι 1-1 και επί. Άρα αυτή είναι ισομορφισμός.

5) Έστω ο δακτύλιος $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} | a, b \in \mathbb{Z}\}$. Η απεικόνιση $\varphi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$, $\varphi(a+b\sqrt{2}) = a-b\sqrt{2}$, είναι ένας ομομορφισμός δακτυλίων. Πράγματι, όπως στο προηγούμενο παράδειγμα, έχουμε

$$\begin{aligned}\varphi(a+b\sqrt{2}+c+d\sqrt{2}) &= \varphi(a+c+(b+d)\sqrt{2}) \\ &= a+c-(b+d)\sqrt{2} \\ &= \varphi(a+b\sqrt{2})+\varphi(c+d\sqrt{2}),\end{aligned}$$

και

$$\begin{aligned}\varphi\big((a+b\sqrt{2})(c+d\sqrt{2})\big) &= \varphi(ac+2bd+(ad+bc)\sqrt{2}) \\ &= ac+2bd-(ad+bc)\sqrt{2} \\ &= (a-b\sqrt{2})(c-d\sqrt{2}) \\ &= \varphi(a-b\sqrt{2})\varphi(c-d\sqrt{2}),\end{aligned}$$

Επιπλέον ο φ είναι $1-1$. Για να το δούμε αυτό, πρώτα παρατηρούμε ότι αν $a, b \in \mathbb{Z}$, τότε

$$a+b\sqrt{2} = 0 \Leftrightarrow a = b = 0.$$

Πράγματι, έστω $a+b\sqrt{2} = 0$. Αν $b = 0$, τότε $a = 0$. Αν $b \neq 0$, τότε $\sqrt{2} = -a/b \in \mathbb{Q}$, που είναι άτοπο (βλ.Παράγραφο 1.2). Επομένως

$$\begin{aligned}&\varphi(a+b\sqrt{2}) = \varphi(c+d\sqrt{2}) \Rightarrow a-b\sqrt{2} = c-d\sqrt{2} \\ &\Rightarrow a-c+(d-b)\sqrt{2} = 0 \Rightarrow a-c = d-b = 0 \\ &\Rightarrow a = c \ \text{ και } \ b = d \Rightarrow a+b\sqrt{2} = c+d\sqrt{2}.\end{aligned}$$

Τέλος είναι φανερό ότι η φ είναι επί και κατά συνέπεια είναι ισομορφισμός.

6) Η απεικόνιση $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(a) = [a]$ είναι ένας επιμορφισμός δακτυλίων, αφού είναι επί και για κάθε $a, b \in \mathbb{Z}$ έχουμε

$$\begin{aligned}&\varphi(a+b) = [a+b] = [a]+[b] = \varphi(a)+\varphi(b), \\ &\varphi(ab) = [ab] = [a][b] = \varphi(a)\varphi(b).\end{aligned}$$

Παρατηρούμε ότι ο φ δεν είναι μονομορφισμός όταν $n \neq 0$.

7) Η απεικονίσεις $\mathbb{Z} \to \mathbb{Q}$, $a \mapsto a$, και $M_n(\mathbb{Z}) \to M_n(\mathbb{Q})$, $A \mapsto A$, είναι μονομορφισμοί δακτυλίων αλλά όχι επιμορφισμοί.

8) Έστω $R = F(\mathbb{R}, \mathbb{R})$ ο δακτύλιος των συναρτήσεων $\mathbb{R} \to \mathbb{R}$. Έστω $c \in \mathbb{R}$. Τότε η απεικόνιση $\varphi : R \to \mathbb{R}$, $\varphi(f) = f(c)$, είναι ένας επιμορφισμός δακτυλίων, αφού είναι επί (γιατί;) και για κάθε $f, g \in R$ έχουμε

$$\varphi(f+g) = (f+g)(c) = f(c) + g(c) = \varphi(f) + \varphi(g) \quad \text{και}$$
$$\varphi(fg) = (fg)(c) = f(c)g(c) = \varphi(f)\varphi(g).$$

9) **Ομομορφισμός εκτίμησης**. Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Για κάθε $r \in R$, ορίζουμε την απεικόνιση $\epsilon_r : R[x] \to R$, $f(x) \mapsto f(r)$. Εύκολα επαληθεύεται ότι η ϵ_r είναι ένας επιμομορφισμός δακτυλίων (βλ. Παρατήρηση 2.2.6). Η απεικόνιση ϵ_r ονομάζεται η ***εκτίμηση*** στο r.

10) Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Θεωρούμε το δακτύλιο $F(R, R)$ των απεικονίσεων $R \to R$. Από την Παρατήρηση 2.2.6 έπεται ότι η απεικόνιση

$$\psi : R[x] \ni f(x) \mapsto \bar{f} \in F(R, R)$$

είναι ένας ομομορφισμός δακτυλίων. Ας εξετάσουμε αν η ψ είναι $1-1$ ή επί σε ορισμένες περιπτώσεις.

Έστω $R = \mathbb{R}$. Τότε η ψ δεν είναι επί, αφού, για παράδειγμα, η εκθετική απεικόνιση $\mathbb{R} \ni a \to e^a \in \mathbb{R}$ δεν είναι πολυωνυμική. Ο ψ είναι $1-1$. (Βλ. Εφαρμογή 2.4.6 4)).

Έστω τώρα $R = \mathbb{Z}_p$, p πρώτος. Τότε η ψ είναι επί. Αυτό προκύπτει από το Πόρισμα 2.2.9. Όμως η ψ δεν είναι $1-1$, γιατί αν $f(x) \in \mathbb{Z}_p[x]$, τότε $\psi(f(x)) = \psi(f(x) + x^p - x)$. Πράγματι, από το Μικρό Θεώρημα του Fermat έχουμε $\psi(x^p - x) = 0$, οπότε $\psi(f(x) + x^p - x) = \psi(f(x)) + \psi(x^p - x) = \psi(f(x))$.

11) Θεωρούμε τους υποδακτυλίους του $M_2(\mathbb{Z})$, $R = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in M_2(\mathbb{Z}) \right\}$ και
$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) \right\}$. Η απεικόνιση $R \to M_2(\mathbb{Z})$, $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, είναι ένας μονομορφισμός δακτυλίων που δεν είναι επιμορφισμός.
Η απεικόνιση $R \to S$, $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, είναι ένας ισομορφισμός

δακτυλίων. Επίσης οι απεικονίσεις $R \to \mathbb{Z}$, $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mapsto a$, και $S \to \mathbb{Z}$, $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mapsto a$ είναι ισομορφισμοί δακτυλίων.

12) Έστω $R = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in M_2(\mathbb{Z}) \right\}$. Εύκολα αποδείκνύεται ότι ο R είναι ένας υποδακτύλιος του $M_2(\mathbb{Z})$ και ότι η απεικόνιση $R \to \mathbb{Z} \times \mathbb{Z}$, $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mapsto (a, b)$ είναι ένας ισομορφισμός δακτυλίων.

13) Έστω V ένας πεπερασμένης διάστασης πραγματικός διανυσματικός χώρος και έστω n η διάστασή του. Τότε υπάρχει ένας ισομορφισμός δακτυλίων $L(V, V) \to M_n(\mathbb{R})$.

Πράγματι, έστω B μία διατεταγμένη βάση του V. Υπενθυμίζουμε από τη Γραμμική Άλγεβρα ότι σε κάθε $f \in L(V, V)$ αντιστοιχεί ένας $n \times n$ πραγματικός πίνακας, που συμβολίζουμε με $[f]_B$, και ισχύουν οι ιδιότητες

$$[f + g]_B = [f]_B + [g]_B$$
$$[f \circ g]_B = [f]_B [g]_B$$

για κάθε $f, g \in L(V, V)$. (Βλ. [4]). Συνεπώς η απεικόνιση $L(V, V) \to \mathcal{M}_n(\mathbb{R})$, $f \mapsto [f]_B$, είναι ένας ομομορφισμός δακτυλίων. Η απεικόνιση αυτή είναι $1 - 1$ και επί, οπότε είναι ένας ισομορφισμός.

Ας δούμε τώρα μερικές απλές ιδιότητες των ομομορφισμών. Έστω $\varphi : R \to S$ ένας ομομορφισμός δακτυλίων. Τότε ισχύουν τα παρακάτω:

- $\varphi(0_R) = 0_S$
- $\varphi(-a) = -\varphi(a)$ για κάθε $a \in R$
- $\varphi(a_1 + \cdots + a_n) = \varphi(a_1) + \cdots + \varphi(a_n)$, για κάθε $a_1, \ldots, a_n \in R$, $n \geq 1$
- $\varphi(a_1 \ldots a_n) = \varphi(a_1) \ldots \varphi(a_n)$, για κάθε $a_1, \ldots, a_n \in R$, $n \geq 1$
- $\varphi(ma) = m\varphi(a)$, για κάθε $m \in \mathbb{Z}$ και $a \in R$
- $\varphi(a^n) = \varphi(a)^n$, για κάθε θετικό ακέραιο n και $a \in R$.

Πράγματι, για την πρώτη σχέση παρατηρούμε ότι $0_R + 0_R = 0_R$ και άρα $\varphi(0_R + 0_R) = \varphi(0_R)$, δηλαδή $\varphi(0_R) + \varphi(0_R) = \varphi(0_R)$ και επομένως $\varphi(0_R) = 0_S$ λόγω του νόμου της διαγραφής. Για τη δεύτερη σχέση έχουμε $0_S = \varphi(0_R) =$

$\varphi(a+(-a))=\varphi(a)+\varphi(-a)$, οπότε $\varphi(-a)=-\varphi(a)$ πάλι λόγω του νόμου της διαγραφής. Οι επόμενες δύο σχέσεις αποδεικνύονται εύκολα με επαγωγή στο n. Οι τελευταίες δύο σχέσεις προκύπτουν άμεσα από τις προηγούμενες.

Αν οι R και S περιέχουν μοναδιαία στοιχεία, δεν είναι απαραίτητο να ισχύει $\varphi(1_R)=1_S$, όπως φαίνεται στο παράδειγμα $\mathbb{Z}\to\mathbb{Z}\times\mathbb{Z}$, $n\mapsto(n,0)$. Αν όμως ο φ είναι επιμορφισμός και ο R περιέχει μοναδιαίο στοιχείο, τότε και ο S περιέχει μοναδιαίο στοιχείο και επιπλέον έχουμε $\varphi(1_R)=1_S$. Πράγματι, αν $r\in R$ τότε $\varphi(r)=\varphi(r1_R)=\varphi(r)\varphi(1_R)$ και όμοια $\varphi(r)=\varphi(1_R)\varphi(r)$. Επειδή η φ είναι επί, συμπεραίνουμε ότι το $\varphi(1_R)$ είναι το μοναδιαίο στοιχείο του S.

Εφαρμογή

Έστω m,n δύο θετικοί ακέραιοι. Τότε υπάρχει ένας ισομορφισμός δακτυλίων $\mathbb{Z}_{mn}\to\mathbb{Z}_m\times\mathbb{Z}_n$ αν και μόνο αν $\mu\kappa\delta(m,n)=1$.

Πράγματι, έστω ότι $\mu\kappa\delta(m,n)=1$. Θεωρούμε την αντιστοιχία

$$\psi:\mathbb{Z}_{mn}\to\mathbb{Z}_m\times\mathbb{Z}_n,\quad [a]_{mn}\mapsto([a]_m,[a]_n).$$

Εύκολα αποδεικνύεται ότι αυτή είναι μια απεικόνιση. Η ψ είναι ένας ομομορφισμός αφού $\psi([a]_{mn}+[b]_{mn})=\psi([a+b]_{mn})=([a+b]_m,[a+b]_n)=([a]_m,[a]_n)+([b]_m,[b]_n)=\psi([a]_{mn})+\psi([b]_{mn})$, και όμοια $\psi([a]_{mn}[b]_{mn})=\psi([a]_{mn})\psi([b]_{mn})$. Θα δείξουμε τώρα ότι η ψ είναι $1-1$. Έστω $([a]_m,[a]_n)=([b]_m,[b]_n)$. Τότε $m|a-b$ και $n|a-b$. Επειδή $\mu\kappa\delta(m,n)=1$, έχουμε $mn|a-b$. Άρα $[a]_{mn}=[b]_{mn}$ και η ϕ είναι $1-1$. Επειδή τα σύνολα $\mathbb{Z}_{mn}$ και $\mathbb{Z}_m\times\mathbb{Z}_n$ έχουν το ίδιο πεπερασμένο πλήθος στοιχείων και η $\psi:\mathbb{Z}_{mn}\to\mathbb{Z}_m\times\mathbb{Z}_n$ είναι $1-1$, συμπεραίνουμε ότι η ψ είναι και επί. Τελικά η ψ είναι ένας ισομορφισμός δακτυλίων.

Έστω τώρα ότι $d=\mu\kappa\delta(m,n)>1$ και $\psi:\mathbb{Z}_{mn}\to\mathbb{Z}_m\times\mathbb{Z}_n$ ένας ισομορφισμός δακτυλίων. Θα φθάσουμε σε άτοπο. Χρειαζόμαστε μία παρατήρηση: Αν $k\in\mathbb{Z}$ είναι ένα κοινό πολλαπλάσιο των m,n τότε για κάθε στοιχείο $x\in\mathbb{Z}_m\times\mathbb{Z}_n$ έχουμε $kx=0_{\mathbb{Z}_m\times\mathbb{Z}_n}$. Πράγματι, αν $x=([a]_m,[b]_n)$, τότε $kx=([ka]_m,[kb]_n)=([0]_m,[0]_n)$. Έστω τώρα $e=\epsilon\kappa\pi(m,n)$. Επειδή $d>1$, έχουμε $e<mn$ (αφού $mn=de$ όπως είδαμε στην Παράγραφο 1.2.) και άρα $[e]_{mn}\neq[0]_{mn}$. Όμως $\psi([e]_{mn})=\psi([0]_{mn})$. Πράγματι, $\psi([e]_{mn})=\psi(e[1]_{mn})=e\psi([1_{mn}])=0_{\mathbb{Z}_m\times\mathbb{Z}_n}=\psi([0]_{mn})$. Αυτό είναι άτοπο, αφού η ψ είναι $1-1$ και $[e]_{mn}\neq[0]_{mn}$.

Παρατηρήσεις

1) Η απεικόνιση $\psi:\mathbb{Z}_{mn}\to\mathbb{Z}_m\times\mathbb{Z}_n$ στην προηγούμενη Εφαρμογή είναι ένας ομομορφισμός δακτυλίων για κάθε θετικούς ακεραίους m,n. Η υπόθεση $\mu\kappa\delta(m,n)=1$ χρησιμοποιήθηκε για να αποδείξουμε ότι η ψ είναι $1-1$.

2) Υπενθυμίζουμε ότι στην απόδειξη της Πρότασης 1.6.1 είχαμε θεωρήσει μια απεικόνιση $U(\mathbb{Z}_{mn})\to U(\mathbb{Z}_m)\times U(\mathbb{Z}_n)$. Επισημαίνουμε ότι αυτή είναι περιορι-

σμός της ψ στο $U(\mathbb{Z}_{mn})$.

Αν υπάρχει ισομορφισμός δακτυλίων $\varphi : R \to S$, θα λέμε ότι ο R είναι ***ισόμορφος*** με το S και θα γράφουμε $R \cong S$.

Έστω $n > 1$ ένας θετικός ακέραιος και $n = p_1^{n_1} \dots p_r^{n_r}$ η ανάλυσή του σε γινόμενο διακεκριμένων πρώτων. Χρησιμοποιώντας την προηγούμενη Εφαρμογή και επαγωγή στο r μπορεί να αποδειχτεί ότι οι δακτύλιοι

$$\mathbb{Z}_n \text{ και } \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_r^{n_r}}$$

είναι ισόμορφοι. Αφήνουμε την απόδειξη σαν άσκηση.

2.5.3 Πρόταση.

1) Έστω ότι υπάρχει ένας ισομορφισμός δακτυλίων $R \cong S$. Τότε υπάρχει ένας ισομορφισμός δακτυλίων $S \cong R$.

2) Έστω ότι υπάρχουν ισομορφισμοί δακτυλίων $R \cong S$ και $S \cong T$. Τότε υπάρχει ένας ισομορφισμός δακτυλίων $R \cong T$.

Απόδειξη. 1) Έστω $\varphi : R \to S$ ένας ισομορφισμός δακτυλίων. Η απεικόνιση φ είναι 1-1 και επί, οπότε ορίζεται η αντίστροφη απεικόνιση

$$\varphi^{-1} : S \to R,$$

και έχουμε $\varphi^{-1}(s) = r$ αν και μόνο αν $s = \varphi(r)$. Εύκολα διαπιστώνουμε ότι και η φ^{-1} είναι ισομορφισμός δακτυλίων: Πράγματι η φ^{-1} είναι 1-1 και επί. Αρκεί να δείξουμε ότι αυτή είναι ομομορφισμός. Έστω s_1, $s_2 \in S$. Τότε υπάρχουν $r_1, r_2 \in R$ με $s_i = \varphi(r_i)$, $i = 1, 2$. Επομένως

$$\begin{aligned}\varphi^{-1}(s_1 + s_2) &= \varphi^{-1}(\varphi(r_1) + \varphi(r_2)) = \varphi^{-1}(\varphi(r_1 + r_2)) = r_1 + r_2 \\ &= \varphi^{-1}(s_1) + \varphi^{-1}(s_2), \quad \text{και}\end{aligned}$$

$$\varphi^{-1}(s_1 s_2) = \varphi^{-1}(\varphi(r_1)\varphi(r_2)) = \varphi^{-1}(\varphi(r_1 r_2)) = r_1 r_2 = \varphi^{-1}(s_1)\varphi^{-1}(s_2).$$

2) Αφήνουμε σαν άσκηση την απόδειξη ότι η σύνθεση δύο ισομορφισμών είναι ισομορφισμός. ⊤

Σχόλιο

Τονίσαμε προηγουμένως ότι στην Άλγεβρα ισόμορφοι δακτύλιοι θεωρούνται "ίδιοι". Συνεπώς είναι εύλογο το ερώτημα με ποιο τρόπο μπορούμε να αποφανθούμε αν δύο δακτύλιοι R, S είναι ή δεν είναι ισόμορφοι. Ισόμορφοι δακτύλιοι έχουν το ίδιο πλήθος στοιχείων, αλλά και πολλές άλλες

κοινές ιδιότητες. Για παράδειγμα, αν ένας από δύο ισόμορφους δακτυλίους είναι μεταθετικός (σώμα, ακεραία περιοχή) τότε και ο άλλος είναι μεταθετικός (αντίστοιχα, σώμα, ακεραία περιοχή). Άλλες ιδιότητες που διατηρούνται από ισομορφισμούς υπάρχουν στην Άσκηση 1. Συνεπώς αν από δύο δακτυλίους μόνο ο ένας έχει κάποια από τις προηγούμενες ιδιότητες συμπεραίνουμε ότι αυτοί δεν είναι ισόμορφοι.

Για παράδειγμα, οι $\mathbb{Z}$ και $\mathbb{Q}$ δεν είναι ισόμορφοι (αν και έχουν το ίδιο πλήθος στοιχείων ως άπειρα αριθμήσιμα σύνολα) αφού ο $\mathbb{Z}$ δεν είναι σώμα. Όμως, δεν είναι πάντα προφανές ποια ιδιότητα πρέπει να εξετάσουμε στην προσπάθεια απόδειξης ότι δύο δακτύλιοι δεν είναι ισόμορφοι. Ας δούμε μερικά απλά παραδείγματα.

Παραδείγματα

1. Οι $\mathbb{R}$, $\mathbb{C}$ δεν είναι ισόμορφοι γιατί αν $\varphi : \mathbb{C} \to \mathbb{R}$ είναι ένας ισομορφισμός έχουμε $-1 = -\varphi(1) = \varphi(-1) = \varphi(i^2) = (\varphi(i))^2$ που είναι άτοπο, αφού $\varphi(i) \in \mathbb{R}$.

2. Επίσης οι $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} | a, b \in \mathbb{Z}\}$, $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \in \mathbb{R} | a, b \in \mathbb{Z}\}$ δεν είναι ισόμορφοι, γιατί αν $\varphi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{3}]$ είναι ένας ισομορφισμός, τότε έχουμε $(\varphi(\sqrt{2}))^2 = \varphi((\sqrt{2})^2) = \varphi(2) = \varphi(1+1) = 2\varphi(1) = 2$. Συνεπώς, $\varphi(\sqrt{2}) = \pm\sqrt{2}$. Αλλά το $\pm\sqrt{2}$ δεν ανήκει στο $\mathbb{Z}[\sqrt{3}]$ (γιατί;).

   Στο πρώτο παράδειγμα χρησιμοποιήσαμε το γεγονός ότι η εξίσωση $x^2 = -1$ δεν έχει λύση στο $\mathbb{R}$ και στο δεύτερο ότι η εξίσωση $x^2 = 2$ δεν έχει λύση στο $\mathbb{Z}[\sqrt{3}]$.

3. Ο δακτύλιος $\mathbb{Z}[\sqrt{2}]$ είναι ισόμορφος με τον

$$\left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} | a, b \in \mathbb{Z} \right\}.$$

   Πράγματι, εύκολα αποδεικνύεται ότι η απεικόνιση $a + b\sqrt{2} \mapsto \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ είναι ένας ισομορφισμός. Όμως ο δακτύλιος $\mathbb{Z}[\sqrt{2}]$ δεν είναι ισόμορφος με τον

$$R = \left\{ \begin{pmatrix} a & 2b \\ 2b & a \end{pmatrix} | a, b \in \mathbb{Z} \right\}.$$

   Πράγματι, ο $\mathbb{Z}[\sqrt{2}]$ δεν έχει μηδενοδιαιρέτες αφού είναι υποδακτύλιος ενός σώματος, ενώ ο R έχει αφού, για παράδειγμα,

$$\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Αν R, S είναι δακτύλιοι θα λέμε ότι ο S είναι ***ομομορφική εικόνα*** του R αν υπάρχει ένας επιμορφισμός δακτυλίων $\varphi : R \to S$. Για παράδειγμα ο $\mathbb{Z}_m$ είναι ομομορφική εικόνα του $\mathbb{Z}$ και ο $\mathbb{R}$ είναι ομομορφική εικόνα του $\mathbb{R}[x]$ (βλ αντίστοιχα τα Παραδείγματα 2.5.2 6) και 9).

Εφαρμογή (Ένα κριτήριο για ανάγωγα πολυώνυμα)

1. Έστω $\varphi : R \to S$ ένας ομομορφισμός μεταθετικών δακτυλίων που έχουν μοναδιαία στοιχεία, τέτοιος ώστε $\varphi(1_R) = 1_S$. Τότε η απεικόνιση

$$\tilde{\varphi} : R[x] \to S[x], \quad \tilde{\varphi}(r_m x^m + \cdots + r_0) = \varphi(r_m)x^m + \cdots + \varphi(r_0)$$

είναι ένας ομομορφισμός δακτυλίων τέτοιος ώστε $\tilde{\varphi}(1_R) = 1_S$.
Πράγματι, με εύκολους υπολογισμούς επαληθεύεται ότι

$$\tilde{\varphi}(f(x) + g(x)) = \tilde{\varphi}(f(x)) + \tilde{\varphi}(g(x)) \quad \text{και}$$
$$\tilde{\varphi}(f(x)g(x)) = \tilde{\varphi}(f(x))\tilde{\varphi}(g(x))$$

για κάθε $f(x), g(x) \in R[x]$. Η $\tilde{\varphi}$ ονομάζεται η επέκταση της φ στο $R[x]$

2. Έστω $f(x) \in \mathbb{Z}[x]$ ένα μονικό πολυώνυμο. Τότε το $f(x)$ είναι ανάγωγο στο $\mathbb{Z}[x]$ αν υπάρχει $m > 0$ τέτοιο ώστε το $\tilde{\varphi}(f(x))$ είναι ανάγωγο στο $\mathbb{Z}_m[x]$, όπου $\tilde{\varphi} : \mathbb{Z}[x] \to \mathbb{Z}_m[x]$ είναι η επέκταση του φυσικού επιμορφισμού $\varphi : \mathbb{Z} \to \mathbb{Z}_m$ στο $\mathbb{Z}[x]$.
Πράγματι, έστω ότι υπάρχουν θετικού βαθμού πολυώνυμα $g(x), h(x) \in \mathbb{Z}[x]$ με $f(x) = g(x)h(x)$. Μπορούμε να υποθέσουμε ότι τα $g(x), h(x)$ είναι μονικά. Τότε τα $\tilde{\varphi}(g(x)), \tilde{\varphi}(h(x))$ είναι μονικά και

$$\deg \tilde{\varphi}(g(x)) = \deg g(x), \quad \deg \tilde{\varphi}(h(x)) = \deg h(x).$$

Από το 1 έχουμε επίσης ότι $\tilde{\varphi}(f(x)) = \tilde{\varphi}(g(x))\tilde{\varphi}(h(x))$. Επειδή το $\tilde{\varphi}(f(x))$ είναι ανάγωγο καταλήγουμε σε άτοπο.

3. Το $f(x) = x^3 + 10x^2 + 30x - 1027 \in \mathbb{Z}[x]$ είναι ανάγωγο.
Πράγματι, έστω $m = 3$. Τότε $\tilde{\varphi}(f(x)) = x^3 + x^2 - 1$. Παρατηρούμε ότι στο $\mathbb{Z}_3$, το $x^3 + x^2 - 1$ δεν έχει ρίζα και επειδή ο βαθμός του είναι 3 συμπεραίνουμε ότι αυτό είναι ανάγωγο στο $\mathbb{Z}_3[x]$. Από το 2 έπεται ότι το $f(x)$ είναι ανάγωγο στο $\mathbb{Z}[x]$.
Σημείωση Αν επιλέγαμε $m = 5$, τότε το $\tilde{\varphi}(f(x)) = x^3 - 2$ δεν είναι ανάγωγο στο $\mathbb{Z}_5[x]$ αφού έχει μια ρίζα στο $\mathbb{Z}_5$, την 3. Συνεπώς για αυτόν τον m το κριτήριο δεν μπορεί να εφαρμοστεί.

Σχόλιο

Έστω ότι ο δακτύλιος S είναι ομομορφική εικόνα του δακτυλίου R. Τότε οι R, S έχουν κάποιες κοινές ιδιότητες. Για παράδειγμα, αν ο R είναι μεταθετικός, τότε και ο S είναι μεταθετικός. Συνεπώς αν μία ομομορφική εικόνα του R δεν είναι μεταθετικός δακτύλιος, τότε και ο R δεν είναι μεταθετικός. Άλλες τέτοιες ιδιότητες υπάρχουν στην Άσκηση 2. Όμως είναι δυνατόν οι R, S να διαφέρουν ουσιαστικά. Για παράδειγμα, ο $\mathbb{Z}$ δεν είναι σώμα αλλά η ομομορφική του εικόνα $\mathbb{Z}_p$ (p πρώτος) είναι. Επίσης, ο δακτύλιος $\mathbb{Z} \times M_2(\mathbb{Z})$ δεν είναι μεταθετικός, αλλά μία ομομορφική εικόνα του, ο $\mathbb{Z}$, είναι.

Σε κάθε ομομορφισμό δακτυλίων θα αντιστοιχίσουμε τώρα δύο άλλους δακτυλίους. Έστω $\varphi : R \to S$ ένας ομομορφισμός δακτυλίων. Ορίζουμε το υποσύνολο του R

$$\ker \varphi = \{r \in R | \varphi(r) = 0_S\},$$

και το υποσύνολο του S

$$\mathrm{Im}\varphi = \{\varphi(r) | r \in R\}.$$

Παρατηρούμε ότι αυτά είναι μη κενά. Πράγματι, από τη σχέση $\varphi(0_R) = 0_S$ έπεται ότι $0_R \in \ker \varphi$ και $0_S \in \mathrm{Im}\varphi$. Το $\ker \varphi$ ονομάζεται ο ***πυρήνας*** της φ και το $\mathrm{Im}\varphi$ η ***εικόνα*** της φ. Για παράδειγμα, ο πυρήνας του ομομορφισμού $\mathbb{Z} \to \mathbb{Z}_m$, $a \mapsto [a]$, είναι το $m\mathbb{Z}$. Ο πυρήνας του ομομορφισμού $\mathbb{Z}[x] \to \mathbb{Z}$, $f(x) \mapsto f(0)$, είναι το σύνολο των πολυωνύμων που έχουν σταθερό όρο ίσο με μηδέν, ενώ η εικόνα είναι το $\mathbb{Z}$.

Ο $\ker \varphi$ είναι ένας υποδακτύλιος του R και η $\mathrm{Im}\varphi$ ένας υποδακτύλιος του S. Πράγματι, έστω $a, b \in \ker \varphi$. Έχουμε $\varphi(a-b) = \varphi(a) - \varphi(b) = 0_S - 0_S = 0_S$, οπότε $a - b \in \ker \varphi$. Επίσης, $\varphi(ab) = \varphi(a)\varphi(b) = 0_S 0_S = 0_S$, οπότε $ab \in \ker \varphi$. Από την Πρόταση 2.1.10 έπεται ότι ο $\ker \varphi$ είναι υποδακτύλιος του R. Η απόδειξη για την $\mathrm{Im}\varphi$ είναι παρόμοια.

Παραδείγματα

1. Η απεικόνιση $\varphi : M_2(\mathbb{Z}) \to M_2(\mathbb{Z}_m)$, $m \in \mathbb{N}$, όπου

$$\varphi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} [a] & [b] \\ [c] & [d] \end{pmatrix}$$

είναι ένας επιμορφισμός δακτυλίων.

Έχουμε $\ker \varphi = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) | \begin{pmatrix} [a] & [b] \\ [c] & [d] \end{pmatrix} = \begin{pmatrix} [0] & [0] \\ [0] & [0] \end{pmatrix} \right\} = \left\{ \begin{pmatrix} ma' & mb' \\ mc' & md' \end{pmatrix} | a', b', c', d' \in \mathbb{Z} \right\} = M_2(m\mathbb{Z})$. Πιο γενικά, έστω ψ :

$R \to S$ ένας ομομορφισμός δακτυλίων. Τότε η απεκόνιση

$$\varphi : M_n(R) \to M_n(S), \quad (a_{ij}) \mapsto (\psi(a_{ij}))$$

είναι ένας ομομορφισμός δακτυλίων με $\ker\varphi = \{(a_{ij}) \in M_n(R) | a_{ij} \in \ker\psi\} = M_n(\ker\psi)$.

2. Έστω $\tilde{\varphi} : \mathbb{Z}[x] \to \mathbb{Z}_m[x]$, $m \in \mathbb{N}$, η επέκταση του φυσικού επιμορφισμού $\varphi : \mathbb{Z} \to \mathbb{Z}_m$, $a \mapsto [a]$. Τότε $\ker\tilde{\varphi} = \{a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] | m | a_i$ για κάθε $i\}$. Πιο γενικά, αν $\varphi : R \to S$ είναι ένας ομομορφισμός μεταξύ δύο δακτυλίων που έχουν μοναδιαία στοιχεία τέτοιος ώστε $\varphi(1_R) = 1_S$, τότε για τον πυρήνα της επέκτασης $\tilde{\varphi} : R[x] \to S[x]$ έχουμε $\ker\tilde{\varphi} = \{a_n x^n + \cdots + a_1 x + a_0 \in R[x] | a_i \in \ker\varphi$ για κάθε $i\}$.

3. Έστω R μία ακεραία περιοχή και $a \in R$. Ο πυρήνας του ομομορφισμού εκτίμησης (βλ. Παράδειγμα 2.5.2 9))

$$\epsilon_a : R[x] \to R, \quad f(x) \mapsto f(a)$$

είναι το σύνολο $I = \{(x-a)g(x) | g(x) \in R[x]\}$. Πράγματι, η σχέση $I \subseteq \ker\epsilon_a$ είναι προφανής. Έστω $f(x) \in \ker\epsilon_a$. Τότε $f(a) = 0$ και επομένως $x - a | f(x)$ (Σημείωση 2.4.3 1)). Άρα $f(x) \in I$ και $\ker\epsilon_a \subseteq I$. Συνεπώς $\ker\epsilon_a = I$.

4. Ο πυρήνας του ομομορφισμού $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}_m$, $(a, b) \mapsto (0, [b])$ είναι το σύνολο $\mathbb{Z} \times m\mathbb{Z} = \{(a, mb) \in \mathbb{Z} \times \mathbb{Z} | a, b \in \mathbb{Z}\}$. Η εικόνα του ομομορφισμού αυτού είναι το σύνολο $\{(0, [b]) \in \mathbb{Z} \times \mathbb{Z}_m\}$.

5. Έστω $\varphi : R \to S$ και $\psi : S \to T$ δύο ομομορφισμοί δακτυλίων. Τότε η σύνθεση $\psi \circ \varphi : R \to T$ είναι ένας ομομορφισμός δακτυλίων. Έχουμε τα εξής

   - Ο ομομορφισμός $\psi \circ \varphi$ είναι τετριμμένος αν και μόνο αν $\mathrm{Im}\varphi \subseteq \ker\psi$
   - $\ker\varphi \subseteq \ker(\psi \circ \varphi)$
   - $\mathrm{Im}(\psi \circ \varphi) \subseteq \mathrm{Im}\psi$.

   Πράγματι, έχουμε $\psi(\varphi(r)) = 0$ για κάθε $r \in R$ αν και μόνο αν $\varphi(r) \in \ker\psi$ για κάθε $r \in R$, δηλαδή αν και μόνο αν $\mathrm{Im}\varphi \subseteq \ker\psi$.
   Αν $\varphi(r) = 0_S$, τότε $\psi(\varphi(r)) = \psi(0_S) = 0_T$ και άρα $r \in \ker(\psi \circ \varphi)$.
   Καθώς $(\psi \circ \varphi)(r) = \psi(\varphi(r)) \in \mathrm{Im}\psi$, για κάθε $r \in R$, έχουμε $\mathrm{Im}(\psi \circ \varphi) \subseteq \mathrm{Im}\psi$.

6. Η απεικόνιση

$$\varphi : \mathbb{Q}[x] \to \mathbb{Q} \times \mathbb{Q}, \quad f(x) \mapsto (f(0), f(1))$$

είναι ένας ομομορφισμός. Ισχύει $\mathrm{Im}\varphi = \mathbb{Q}\times\mathbb{Q}$, γιατί δοθέντος του $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ έχουμε $\varphi((b-a)x+a) = (a, b)$. Για τον πυρήνα έχουμε

$$\begin{aligned}\ker\varphi &= \{f(x) \in \mathbb{Q}[x] | f(0) = f(1) = 0\} \\ &= \{f(x) \in \mathbb{Q}[x] | x|f(x) \ \text{ και } \ x-1|f(x)\} \ \text{ (Θεώρημα 2.4.1)} \\ &= \{f(x) \in \mathbb{Q}[x] | x(x-1)|f(x)\} \ \text{ (Παράδειγμα 2.3.11 2))} \\ &= \{x(x-1)g(x) | g(x) \in \mathbb{Q}[x]\}.\end{aligned}$$

Θα δούμε στη συνέχεια ότι ο πυρήνας έχει ενδιαφέρουσες ιδιότητες. Σύμφωνα με την επόμενη πρόταση ο $\ker\varphi$ καθορίζει το αν ο φ είναι μονομορφισμός.

2.5.4 Πρόταση. *Έστω $\varphi : R \to S$ ένας ομομορφισμός δακτυλίων. Τότε ο φ είναι μονομορφισμός αν και μόνο αν $\ker\varphi = \{0_R\}$.*

Απόδειξη. Έστω ότι ο φ είναι μονομορφισμός και $r \in \ker\varphi$. Τότε $\varphi(r) = 0_S = \varphi(0_R)$ και, επειδή η απεικόνιση φ είναι 1-1, παίρνουμε $r = 0_R$. Συνεπώς $\ker\varphi = \{0_R\}$. Αντίστροφα, έστω $\ker\varphi = \{0_R\}$ και $\varphi(r) = \varphi(r')$. Από την τελευταία σχέση έχουμε $\varphi(r) - \varphi(r') = 0_S$, δηλαδή $\varphi(r - r') = 0_S$. Συνεπώς $r - r' \in \ker\varphi = \{0_R\}$, οπότε $r = r'$. ⊺

Παράδειγμα Οι απεικονίσεις $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, $(a, b) \mapsto (b, a)$, $\psi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, $(a, b) \mapsto (a, 0)$, είναι ομομορφισμοί δακτυλίων. Έχουμε $\ker\varphi = \{(0, 0)\}$ και συνεπώς ο φ είναι μονομορφισμός. Μάλιστα ο φ είναι ισομορφισμός. Για τον ψ έχουμε $\ker\psi = \{(0, b) \in \mathbb{Z}\times\mathbb{Z}\} = \{0\}\times\mathbb{Z}$. Ο ψ δεν είναι μονομορφισμός.

Ιδεώδη

Μια από τις ιδιότητες του πυρήνα ενός ομομορφισμού δακτυλίων $\varphi : R \to S$ είναι ότι αυτός είναι ένας υποδακτύλιος του R, όπως είδαμε πριν.

Μια άλλη ιδιότητα του $\ker\varphi$ είναι ότι

$$r \in R \ \text{ και } \ a \in \ker\varphi \Rightarrow ra \in \ker\varphi \ \text{ και } \ ar \in \ker\varphi.$$

Πράγματι, $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0_S = 0_S$, οπότε $ra \in \ker\varphi$. Όμοια έχουμε $ar \in \ker\varphi$.

Οι υποδακτύλιοι του R που έχουν την προηγούμενη ιδιότητα παίζουν σημαντικό ρόλο στη μελέτη του R, όπως θα διαπιστώσουμε στην επόμενη Παράγραφο. Για τον λόγο αυτό δίνουμε τον εξής ορισμό.

2.5.5 Ορισμός. *Έστω R ένας δακτύλιος. Ένα μη κενό υποσύνολο I του R ονομάζεται* ***ιδεώδες*** *του R αν ισχύουν οι ιδιότητες*

- $a, b \in I \Rightarrow a - b \in I$,
- $r \in R$, $a \in I \Rightarrow ra \in I$ *και* $ar \in I$.

Παρατήρηση Συγκρίνοντας τον προηγούμενο Ορισμό με την Πρόταση 2.1.10, συμπεραίνουμε ότι κάθε ιδεώδες του R είναι υποδακτύλιος του R. Δεν ισχύει το αντίστροφο. Για παράδειγμα, ο υποδακτύλιος $\mathbb{Z}$ του $\mathbb{Q}$ δεν είναι ιδεώδες του $\mathbb{Q}$, γιατί διαφορετικά θα είχαμε $1/2 = (1/2)1 \in \mathbb{Z}$.

2.5.6 Παραδείγματα.

1. Είδαμε πριν ότι ο πυρήνας κάθε ομομορφισμού δακτυλίων $\varphi : R \to S$ είναι ένα ιδεώδες του R.
2. Ιδεώδη του δακτυλίου R είναι το ίδιο το R και το σύνολο $\{0_R\}$ που ονομάζεται ***μηδενικό ιδεώδες***.
3. Το $n\mathbb{Z}$ είναι ένα ιδεώδες του $\mathbb{Z}$. Μάλιστα, κάθε ιδεώδες του $\mathbb{Z}$ είναι της μορφής $n\mathbb{Z}$ (βλ. Άσκηση 2.1.5).
4. Γενικεύοντας λίγο το προηγούμενο παράδειγμα, έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και $a \in R$. Τότε το σύνολο
$$\{ra \in R | r \in R\}$$
είναι ένα ιδεώδες του R που περιέχει το a. Πράγματι, αν ra, $sa \in I$ και $t \in R$, τότε $ra - sa = (r - s)a \in I$ και $t(ra) = (tr)a \in I$. Επίσης $a = 1$ $a \in I$. Το $\{ra \in R | r \in R\}$ ονομάζεται το ***κύριο ιδεώδες*** που παράγεται από το a και συμβολίζεται συχνά με $< a >$. Για $R = \mathbb{Z}$ και $a = n$, έχουμε $< n >= n\mathbb{Z}$. Το ιδεώδες I του $\mathbb{C}[x, y]$ που αποτελείται από τα πολυώνυμα που έχουν μηδενικό σταθερό όρο δεν είναι κύριο. Πράγματι, έστω $I =< f(x, y) >$. Επειδή $x \in I$ έχουμε $x = g(x, y)f(x, y)$ για κάποιο $g(x, y) \in \mathbb{C}[x, y]$. Άρα $f(x, y) = cx$ ή $f(x, y) = c$, $c \in \mathbb{C} - \{0\}$. Αυτό είναι άτοπο αφού $y \in I$.
5. Το $I = \{[0], [2], [4], [6], [8]\}$ στο $\mathbb{Z}_{10}$ είναι ένα ιδεώδες. Μάλιστα, I είναι το κύριο ιδεώδες που παράγεται από το $[2]$, δηλαδή $I =< [2] >$. Παρατηρούμε ότι στο παράδειγμα αυτό έχουμε $I =< [2] >=< [4] >=< [6] >=< [8] >$.
6. Έστω $R = F(\mathbb{R}, \mathbb{R})$ και $c \in R$. Το σύνολο $I = \{f \in R | f(c) = 0\}$ είναι ένα ιδεώδες του R. Πράγματι, το I είναι ο πυρήνας του ομομορφισμού του Παραδείγματος 2.5.2 8).

7. **Πυρήνας ομομορφισμού εκτίμησης**
Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και $r \in R$. Τότε το σύνολο $I = \{f(x) \in R[x] | f(r) = 0\}$ είναι ένα ιδεώδες του $R[x]$. Ισχύει $I = \ker \epsilon_r$, όπου $\epsilon_r : R[x] \to R$, $f(x) \mapsto f(r)$, είναι ο ομομορφισμος εκτίμησης του Παραδείγματος 2.5.2 9). Στην ειδική περίπτωση που ο R είναι ακεραία περιοχή, έχουμε $I = \ker \epsilon_r =< x - r >$, το κύριο ιδεώδες που παράγεται από το $x - r$. Αυτό έπεται από τη Σημείωση 2.4.3 1).

8. Στο δακτύλιο $R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} | a, b \in \mathbb{R} \right\}$ θεωρούμε το υποσύνολο $I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} | b \in \mathbb{R} \right\}$. Το I είναι ιδεώδες γιατί για κάθε $b, b', r, s \in \mathbb{R}$ έχουμε

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b - b' \\ 0 & 0 \end{pmatrix} \in I,$$
$$\begin{pmatrix} r & s \\ 0 & r \end{pmatrix} \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & rb \\ 0 & 0 \end{pmatrix} \in I \quad \text{και}$$
$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} r & s \\ 0 & r \end{pmatrix} = \begin{pmatrix} 0 & br \\ 0 & 0 \end{pmatrix} \in I.$$

2.5.7 Παρατηρήσεις.

1. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο και έστω I ένα ιδεώδες του R. Παρατηρούμε ότι αν το I περιέχει ένα αντιστρέψιμο στοιχείο u τότε $I = R$. Πράγματι, αν $u\nu = \nu u = 1$ με $\nu \in R$, τότε $1 = u\nu \in I$. Άρα για το τυχαίο $r \in R$ έχουμε $r = 1r \in I$. Συνεπώς, $R \subseteq I$, οπότε $R = I$.

2. Από το 1 βλέπουμε ότι τα μόνα ιδεώδη ενός σώματος F είναι το ίδιο το F και το μηδενικό ιδεώδες. Την ιδιότητα αυτή μπορεί να έχει ένας δακτύλιος που δεν είναι σώμα, όπως για παράδειγμα ο δακτύλιος των quaternions $\mathbb{H}$ (γιατί;). Άλλο παράδειγμα δίνεται αμέσως παρακάτω.

3. Από το 2 και την Πρόταση 2.5.4 συμπεραίνουμε ότι κάθε ομομορφισμός δακτυλίων $F \to S$, όπου το F είναι σώμα, είναι μηδενικός ή μονομορφισμός.

Παράδειγμα Έστω F ένα σώμα και $R = M_2(F)$. Θα δείξουμε ότι δεν υπάρχουν άλλα ιδεώδη του R εκτός από το μηδενικό και το R.

Έστω I ένα μη μηδενικό ιδεώδες του R. Τότε υπάρχει μη μηδενικός πίνακας $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in I$. Έστω ότι $a \neq 0$. Επειδή το I είναι ιδεώδες έχουμε

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I,$$

δηλαδή

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in I.$$

Επομένως

$$\begin{pmatrix} xa^{-1} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in I, \quad \text{για κάθε} \quad x \in F$$

δηλαδή

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \in I, \quad \text{για κάθε} \quad x \in F.$$

Από τη σχέση αυτή και το γεγονός ότι το I είναι ιδεώδες συμπεραίνουμε ότι

$$\begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} y & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in I, \quad \text{για κάθε} \quad y \in F$$

$$\begin{pmatrix} 0 & 0 \\ z & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} z & 0 \\ 0 & 0 \end{pmatrix} \in I, \quad \text{για κάθε} \quad z \in F$$

$$\begin{pmatrix} 0 & 0 \\ 0 & w \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} w & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in I, \quad \text{για κάθε} \quad w \in F$$

Επειδή κάθε στοιχείο του $M_2(F)$ είναι της μορφής

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ z & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & w \end{pmatrix},$$

έχουμε $M_2(F) \subseteq I$. Άρα $M_2(F) = I$.

Αποδείξαμε τον ισχυρισμό μας στην περίπτωση που $a \neq 0$. Η γενική περίπτωση ανάγεται σε αυτή, γιατί αν ένα από τα a, b, c, d είναι μη μηδενικό, τότε υπάρχουν πίνακες $A, B \in M_2(F)$, τέτοιοι ώστε το στοιχείο αυτό να βρίσκεται στη θέση $(1,1)$ του πίνακα $A \begin{pmatrix} a & b \\ c & d \end{pmatrix} B \in I$.

Σημείωση Ένας δακτύλιος που δεν έχει άλλα ιδεώδη εκτός από τον εαυτό του και το μηδενικό λέγεται **απλός**. Οι απλοί δακτύλιοι είναι σημαντικοί στη θεωρία δακτυλίων και έχουν σπουδαίες εφαρμογές στη θεωρία των πεπερασμένων ομάδων.

Κατασκευή ιδεωδών
Θα δούμε εδώ ότι από δεδομένα ιδεώδη ενός δακτυλίου μπορούμε να κατασκευάσουμε άλλα ιδεώδη. Έστω I και J υποσύνολα ενός δακτυλίου R. Ορίζουμε τα υποσύνολα του R

$$I + J = \{a + b \in R | a \in I, b \in J\}$$
$$IJ = \{a_1b_1 + \cdots + a_nb_n \in R | a_i \in I, \quad b_i \in J, \quad n \geq 1\}.$$

2.5.8 Πρόταση. *Έστω R ένας δακτύλιος και I, J ιδεώδη του R. Τότε τα παρακάτω σύνολα είναι ιδεώδη του R*

- $I \cap J$
- $I + J$
- IJ.

Επιπλέον έχουμε $I \subseteq I + J$, $J \subseteq I + J$ και $IJ \subseteq I \cap J$.

Απόδειξη. Θα αποδείξουμε ότι το $I + J$ είναι ιδεώδες του R. Οι αποδείξεις για τα άλλα σύνολα είναι ανάλογες και αφήνονται σαν ασκήσεις.

Το σύνολο $I + J$ είναι μη κενό αφού $0_R = 0_R + 0_R \in I + J$. Έστω $r \in R$, $a + b \in I + J$, $c + d \in I + J$, όπου $a, c \in I$ και $b, d \in J$. Τότε έχουμε $(a + b) - (c + d) = (a - c) + (b - d) \in I + J$, αφού $a - c \in I$ και $b - d \in J$. Επίσης $r(a + b) = ra + rb \in I + J$, αφού $ra \in I$ και $rb \in J$. Όμοια έχουμε $(a + b)r = ar + br \in I + J$. Συνεπώς το $I + J$ είναι ιδεώδες του R.

Έστω $a \in I$. Τότε $a = a + 0_R \in I + J$. Άρα $I \subseteq I + J$. Όμοια, $J \subseteq I + J$. Για κάθε $a \in I$ και $b \in J$ έχουμε $ab \in I$ και $ab \in J$ γιατί τα I και J είναι ιδεώδη. Συμπεραίνουμε ότι $a_1b_1 + \cdots + a_nb_n \in I \cap J$ για κάθε $a_i \in I$ και $b_j \in J$. Άρα $IJ \subseteq I \cap J$. ⊤

Παρατηρήσεις

1. Είναι δυνατό η ένωση ιδεωδών να μην είναι ιδεώδες. Για παράδειγμα, το $2\mathbb{Z} \cup 3\mathbb{Z}$ δεν είναι ιδεώδες του $\mathbb{Z}$ (Άσκηση 7).

2. Έστω I, J ιδεώδη ενός δακτυλίου R. Τότε το σύνολο $\{ab \in R | a \in I, b \in J\}$ δεν είναι γενικά ίσο με το IJ. Για παράδειγμα, έστω $R = \mathbb{Q}[x_1, x_2, x_3, x_4]$, $I =< x_1 > + < x_2 >$, $J =< x_3 > + < x_4 >$. Τότε $x_1x_3 + x_2x_4 \in IJ$ αλλά $x_1x_3 + x_2x_4 \notin \{ab \in R | a \in I, b \in J\}$ (γιατί;). Ισχύει ότι $\{ab \in R | a \in I, b \in J\} \subseteq IJ$. Το παράδειγμα αυτό δείχνει ότι γενικά το σύνολο $\{ab \in R | a \in I, b \in J\}$ δεν είναι ιδεώδες.

3. Εύκολα αποδεικνύεται ότι η τομή οποιουδήποτε πλήθους ιδεωδών ενός δακτυλίου R είναι ένα ιδεώδες του R.

Έστω R ένας δακτύλιος και έστω X ένα μη κενό υποσύνολο του R. Η τομή όλων των ιδεωδών του R που περιέχουν το X είναι ένα ιδεώδες του R, σύμφωνα με την προηγούμενη Παρατήρηση, που περιέχει το X. Το ιδεώδες αυτό συμβολίζεται με $< X >$. Στην περίπτωση που το X είναι πεπερασμένο, έστω $X = \{a_1, \ldots, a_n\}$, θα χρησιμοποιούμε το συμβολισμό $< X >=< a_1, \ldots, a_n >$. Η παρακάτω Πρόταση δίνει μία χρήσιμη περιγραφή του $< X >$ όταν ο R είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο.

Επισημαίνουμε ότι αν το a είναι ένα στοιχείο ενός μεταθετικού δακτυλίου που έχει μοναδιαίο στοιχείο,τότε έχουμε παραστήσει με $< a >$ δύο ενδεχομένως διαφορετικά πράγματα, το κύριο ιδεώδες που παράγεται από το a και την τομή όλων των ιδεωδών που περιέχουν το a. Σύμφωνα με την επόμενη Πρόταση, αυτά συμπίπτουν.

2.5.9 Πρόταση. *Έστω X ένα μη κενό υποσύνολο ενός μεταθετικού δακτυλίου R που έχει μοναδιαίο στοιχείο. Τότε*

$$< X >= \{r_1a_1 + \cdots + r_ma_m | r_i \in R, a_i \in X, m \geq 1\}$$

Απόδειξη. Έστω $J = \{r_1a_1 + \cdots + r_ma_m | r_i \in R, a_i \in X, m \geq 1\}$. Έχουμε $< X >= \bigcap_{I \supseteq X} I$, όπου το I διατρέχει τα ιδεώδη του R που περιέχουν το X. Είναι φανερό ότι το J περιέχεται σε κάθε τέτοιο I. Άρα $J \subseteq < X >$. Χρησιμοποιώντας τη μεταθετικότητα του R, εύκολα αποδεικνύεται ότι το J είναι ένα ιδεώδες του R που περιέχει το X. Συνεπώς το J είναι ένα από τα I. Άρα $< X > \subseteq J$. ⊤

Για παράδειγμα, αν $R = \mathbb{Z}[x]$ και $X = \{x, 2\}$ τότε το $< x, 2 >$ είναι το σύνολο των πολυωνύμων στο $\mathbb{Z}[x]$ που έχουν άρτιο σταθερό όρο (γιατί;).

Στην περίπτωση που για ένα ιδεώδες I έχουμε $I =< X >$, θα λέμε ότι το I ***παράγεται*** από το X, ή ότι το X είναι ένα σύνολο ***γεννητόρων*** του I.

Παράδειγμα. Στο δακτύλιο $\mathbb{Q}[x, y]$ θεωρούμε τα ιδεώδη

$$I =< x^2y - 1, xy^2 - 1 >$$
$$J =< x - y, x^3 - 1 > .$$

Θα δείξουμε ότι $I = J$.

Πράγματι, από τις σχέσεις

$$x - y = y(x^2y - 1) - x(xy^2 - 1) \tag{1}$$

$$x^3 - 1 = (x^2y + 1)(x^2y - 1) - x^3(xy^2 - 1) \tag{2}$$

συμπεραίνουμε ότι $\{x - y, x^3 - 1\} \subseteq I$ και άρα $J \subseteq I$. Από τις σχέσεις

$$x^2y - 1 = -x^2(x - y) + x^3 - 1 \tag{3}$$

$$xy^2 - 1 = (-xy - x^2)(x - y) + x^3 - 1 \tag{4}$$

συμπεραίνουμε ότι $\{x^2y - 1, xy^2 - 1\} \subseteq J$ και άρα $I \subseteq J$. Συνεπώς $I = J$.

Επισημαίνουμε ότι οι ισότητες (3) και (4) προκύπτουν από τον Αλγόριθμο Διαίρεσης στο $\mathbb{Q}[x, y] = (\mathbb{Q}[x])[y]$. Δηλαδή, διαιρούμε τα $x^2y - 1, xy^2 - 1$ με το $y - x$ στο $(\mathbb{Q}[x])[y]$. Για τις ισότητες (1) και (2) δεν είναι δυνατό να δοθεί ικανοποιητική εξήγηση μέσα σε λίγες γραμμές. Γενικά, η εύρεση μιας παράστασης ενός στοιχείου ιδεώδους πολυωνυμικού δακτυλίου συναρτήσει δεδομένων γεννητόρων είναι ένα ενδιαφέρον πρόβλημα της Υπολογιστικής Άλγεβρας. Βλ. [6].

Σημείωση Πολλοί μεταθετικοί δακτύλιοι R που εμφανίζονται στην Άλγεβρα έχουν την ιδιότητα ότι για κάθε ιδεώδες I του R υπάρχει πεπερασμένο υποσύνολο X του I τέτοιο ώστε $< X >= I$. Οι δακτύλιοι αυτοί ονομάζονται δακτύλιοι της Noether[1]. Δακτύλιοι της Noether είναι, για παράδειγμα, οι $\mathbb{Z}$ και $F[x]$ όπου το F είναι σώμα. Πράγματι, κάθε ιδεώδες αυτών είναι κύριο (βλ. Άσκηση 11), δηλαδή είναι της μορφής $< X >$, όπου το X έχει ένα στοιχείο. Πληροφοριακά αναφέρουμε ένα σημαντικό θεώρημα του Hilbert σύμφωνα με το οποίο αν ο R είναι δακτύλιος της Noether, τότε και ο $R[x]$ είναι δακτύλιος της Noether (βλ. [21]).

Ασκήσεις 2.5

1. Μια ιδιότητα ενός δακτυλίου R ονομάζεται "αλγεβρική" αν κάθε δακτύλιος ισόμορφος με τον R έχει την ιδιότητα αυτή. Αποδείξτε ότι οι παρακάτω ιδιότητες είναι αλγεβρικές.

   i) R είναι μεταθετικός.

[1] Η Emmy Noether (1882-1935) εργάστηκε κυρίως στη Μαθηματική Φυσική και στην Άλγεβρα με ιδιαίτερη έμφαση στη θεωρία δακτυλίων. Σύμφωνα με τον Alexandroff "Η Emmy Noether μας δίδαξε να σκεπτόμαστε με πιο απλό και γενικό τρόπο: με ομομορφισμούς και ιδεώδη - και όχι με πολύπλοκους αλγεβρικούς υπολογισμούς".

ii) R έχει μοναδιαίο στοιχείο.

iii) R έχει μηδενοδιαιρέτες.

iv) R είναι πεπερασμένο σύνολο.

v) R είναι άπειρο σύνολο.

vi) R είναι αριθμήσιμο σύνολο.

vii) R είναι ακεραία περιοχή.

viii) R είναι σώμα.

ix) κάθε ιδεώδες του R είναι κύριο.

x) $U(R)$ είναι πεπερασμένο σύνολο.

xi) $mr = 0$ για κάθε $r \in R$, όπου $m \in \mathbb{Z}_{>0}$.

Η ιδιότητα: "το R είναι υποσύνολο του $\mathbb{C}$" δεν είναι αλγεβρική.

2. Έστω S ένας δακτύλιος που είναι ομομορφική εικόνα του δακτυλίου R. Αποδείξτε ότι:

i) R μεταθετικός $\Rightarrow$ S μεταθετικός

ii) R έχει μοναδιαίο στοιχείο $\Rightarrow$ S έχει μοναδιαίο στοιχείο

iii) κάθε μη σταθερό $f(x) \in R[x]$ έχει ρίζα στο $R \Rightarrow$ κάθε μη σταθερό $g(x) \in S[x]$ έχει ρίζα στο S.

Η συνεπαγωγή "R ακεραία περιοχή $\Rightarrow$ S ακεραία περιοχή" δεν αληθεύει Δώστε ένα συγκεκριμένο αντιπαράδειγμα.

3. Για καθένα από τα παρακάτω ζεύγη εξετάστε αν οι δακτύλιοι είναι ισόμορφοι

i) $\mathbb{Z}, \mathbb{R}$

ii) $2\mathbb{Z}, \mathbb{Z}$

iii) $2\mathbb{Z}$, $3\mathbb{Z}$

iv) $\mathbb{Z}[x]$, $\mathbb{Q}[x]$

v) $\mathbb{Z}$, $M_2(\mathbb{Z})$

vi) $\mathbb{Q}$, $M_2(\mathbb{Z})$

vii) $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{5}]$

viii) $\mathbb{Z}[i]$, $\mathbb{Q}[i]$

ix) $\mathbb{Z}$, $\left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) \right\}$

x) $\mathbb{Z}$, $\left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) \right\}$

xi) $\mathbb{Z}_m$, $\mathbb{Z}_n$

xii) $\mathbb{Z}[i]$, $\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_2(\mathbb{Z}) \right\}$

xiii) $\mathbb{Z}[\sqrt{3}]$, $\left\{ \begin{pmatrix} a & 3b \\ 3b & a \end{pmatrix} | a, b \in \mathbb{Z} \right\}$

xiv) $\mathbb{R} \times \mathbb{R}$, $\mathbb{C}$

4. Εξετάστε ποιες από τις παρακάτω απεικονίσεις είναι ομομορφισμοί δακτυλίων. Στις περιπτώσεις που ο φ είναι ομομορφισμός, να υπολογιστεί ο πυρήνας του.

   i) $\phi : \mathbb{Z} \to \mathbb{Z}_m$, $\phi(a) = [a]$.

   ii) $\phi : \mathbb{Z} \to \mathbb{Z}_m$, $\phi(a) = [a+1]$.

   iii) $\phi : \mathbb{Z} \to \mathbb{Z}$, $\phi(a) = -a$.

   iv) $\phi : \mathbb{Q}[x] \to \mathbb{Q}$, $\phi(f(x)) = 1$.

   v) $\phi : \mathbb{Q}[x] \to \mathbb{Q}$, $\phi(f(x)) = f(1)$.

   vi) $\phi : \mathbb{Z} \to M_2(\mathbb{Z}_m)$, $\phi(a) = \begin{pmatrix} [1] & [0] \\ [0] & [a] \end{pmatrix}$.

5. Εξετάστε αν τα παρακάτω σύνολα είναι ιδεώδη του

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{Z}) \right\}.$$

   i) $\left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in R \right\}$ iii) $\left\{ \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} \in R \right\}$

   ii) $\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in R \right\}$ iv) $\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in R | b \in 2\mathbb{Z} \right\}$

6. Εξετάστε αν τα παρακάτω σύνολα είναι ιδεώδη του $\mathbb{Q}[x]$.

   i) $\{f(x) \in \mathbb{Q}[x] | f(0) = 0\}$ iv) $\{f(x) \in \mathbb{Q}[x] | f(1/2) \in 2\mathbb{Z}\}$

   ii) $\{f(x) \in \mathbb{Q}[x] | f(0) = 1\}$ v) $\{f(x) \in \mathbb{Q}[x] | f(1) = f(2) = 0\}$

   iii) $\{f(x) \in \mathbb{Q}[x] | f(1/2) = 0\}$ vi) $\{f(x) \in \mathbb{Q}[x] | x^2 - 2x + 1 | f(x)\}$

7. i) Αποδείξτε πλήρως την Πρόταση 2.5.8.

   ii) Αποδείξτε ότι η ένωση $2\mathbb{Z} \cup 3\mathbb{Z}$ δεν είναι ιδεώδες του $\mathbb{Z}$.

8. i) Αποδείξτε ότι στο $\mathbb{Z}$ ισχύει $< m > \subseteq < n > \Leftrightarrow n | m$.

   ii) Έστω a, b στοιχεία μιας ακεραίας περιοχής R. Αποδείξτε ότι $< a > = < b >$ αν και μόνο αν $a = ub$ για κάποιο αντιστρέψιμο $u \in R$.

9. Έστω I, J δύο ιδεώδη ενός δακτυλίου R. Αποδείξτε ότι $I + J = I$ αν και μόνο αν $J \subseteq I$.

10. Έστω m, n, δύο θετικοί ακέραιοι $d = \mu\kappa\delta(m, n)$ και $e = \epsilon\kappa\pi(m, n)$. Αποδείξτε τις παρακάτω ισότητες ιδεωδών στο $\mathbb{Z}$.

i) $< m > + < n >=< d >$

ii) $< m > \cap < n >=< e >$

iii) $< m >< n >=< mn >$

11. i) Αποδείξτε ότι κάθε ιδεώδες του $\mathbb{Z}$ και κάθε ιδεώδες του $F[x]$ (F σώμα) είναι κύριο.
Υπόδειξη: Αλγόριθμος διαίρεσης.
ii) Να βρεθεί το πλήθος των ιδεωδών I του $\mathbb{Z}$ που έχουν την ιδιότητα $20\mathbb{Z} \subseteq I \subseteq 2\mathbb{Z}$.

12. Έστω $I = \{f(x) \in \mathbb{R}[x] | f(2-3i) = 0\}$ και J το κύριο ιδεώδες του $\mathbb{R}[x]$ που παράγεται από το $x^2 - 4x + 13$. Αποδείξτε ότι $I = J$.

13. Έστω R, S δακτύλιοι. Αποδείξτε ότι οι απεικονίσεις

$$R \times S \to R, \quad (r,s) \mapsto r$$
$$R \times S \to S, \quad (r,s) \mapsto s$$

είναι επιμορφισμοί δακτυλίων με αντίστοιχους πυρήνες $\{(0,s) \in R \times S\}$, $\{(r,0) \in R \times S\}$, και οι απεικονίσεις

$$R \to R \times S, \quad r \mapsto (r,0)$$
$$S \to R \times S, \quad s \mapsto (0,s)$$

είναι μονομορφισμοί δακτυλίων.

14. i) Η απεικόνιση $\varphi : \mathbb{Q}[x] \to \mathbb{Q}[x]$, $f(x) \mapsto f(2x+3)$, είναι ένας ισομορφισμός δακτυλίων.

ii) Η απεικόνιση $\psi : \mathbb{Z}_4[x] \to \mathbb{Z}_4[x]$, $f(x) \mapsto f(2x+3)$, είναι ένας ομομορφισμός δακτυλίων που δεν είναι ισομορφισμός.

15. i) Στο δακτύλιο $\mathbb{Q}[x,y]$ έχουμε $< x+y, x-y >=< x, y >$.

ii) Στο δακτύλιο $\mathbb{Z}[x,y]$ έχουμε $< x+y, x-y > \subsetneq < x, y >$.

16. Αποδείξτε ότι στο $\mathbb{Q}[x,y]$ έχουμε

i) $< x^2 - y^2, x+y >=< x+y >$

ii) $< x^2 - y^2 + 1, x+y >= \mathbb{Q}[x,y]$.

iii) $< x^2 + y^2 + 2xy > \subsetneq < x^2 + y^2, xy >$.

17. Αποδείξτε ότι τα ιδεώδη του $R \times S$ είναι τα $I \times J$ όπου το I (αντίστοιχα, J) διατρέχει τα ιδεώδη του R (αντίστοιχα, S).

18. Έστω I, J δύο ιδεώδη ενός δακτυλίου R.

    i) Γνωρίζουμε ότι $IJ \subseteq I \cap J$. Αληθεύει ότι $IJ = I \cap J$;
    Υπόδειξη: Άσκηση 10.

    ii) Έστω ότι ο R είναι μεταθετικός και $I + J = R$. Αποδείξτε ότι $IJ = I \cap J$.

19. Εξετάστε ποιες από τις παρακάτω προτάσεις είναι αληθείς.

    i) Έστω $m, n \in \mathbb{N}$. Τότε $m\mathbb{Z} \cong n\mathbb{Z}$ αν και μόνο αν $m = n$.

    ii) Στο $\mathbb{Z}$ ισχύει $< 6 >=< 24 > + < m >$ αν και μόνο αν $\mu\kappa\delta(6, m) \neq 1$.

    iii) Κάθε ιδεώδες του $\mathbb{Z} \times \mathbb{Z}$ είναι της μορφής $< m > \times < n >$, $m, n \in \mathbb{Z}$.

    iv) Κάθε ιδεώδες του $\mathbb{Z} \times \mathbb{Z}$ είναι κύριο.

20. Έστω R ένας μεταθετικός δακτύλιος και I ένα ιδεώδες του R. Το ριζικό του I είναι το σύνολο $\sqrt{I} = \{r \in R | r^n \in I \text{ για κάποιο } n \geq 1\}$.

    i) Αποδείξτε ότι το $\sqrt{I}$ είναι ένα ιδεώδες του R που περιέχει το I.

    ii) Έστω $R = \mathbb{Z}$. Να προσδιορίσετε τα $\sqrt{< 3 >}$, $\sqrt{< 12 >}$.

    iii) Έστω $R = \mathbb{Z}_4$. Ποιό είναι το $\sqrt{< 0 >}$;

    iv) Έστω $R = \mathbb{Z}_6$. Ποιό είναι το $\sqrt{< 0 >}$;

    v) Έστω $R = \mathbb{Z}_n$. Αποδείξτε ότι $\sqrt{< 0 >} =< [p_1 \dots p_r]_n >$, όπου $n = p_1^{n_1} \dots p_r^{n_r}$ είναι η ανάλυση του n σε γινόμενο διακεκριμένων πρώτων.

21. Χρησιμοποιώντας τον φυσικό επιμορφισμό $\mathbb{Z} \to \mathbb{Z}_8$, αποδείξτε ότι κανένας από τους ακεραίους $2, 10, 18, 26, \dots$ δεν είναι τρίτη δύναμη ακεραίου.

22. Έστω I το ιδεώδες του $\mathbb{C}[x, y]$ που αποτελείται από τα πολυώνυμα που έχουν μηδενικό σταθερό όρο. Αποδείξτε ότι $I =< x > + < y >= < x, y >$.

23. Αποδείξτε ότι τα μόνα ιδεώδη του $M_n(F)$, όπου το F είναι ένα σώμα, είναι τα $< 0 >$, $M_n(F)$.

24. Έστω $\phi : R \to S$ ένας ομομορφισμός δακτυλίων. Αληθεύει ότι η εικόνα $\text{Im}\phi$ είναι ιδεώδες του S;

25. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο και $e \in R$ που έχει τις ιδιότητες: $e^2 = e$, $er = re$ για κάθε $r \in R$. Αποδείξτε ότι τα $< e >= \{re | r \in R\}$ και $< 1-e >= \{r(1-e) | r \in R\}$ είναι ιδεώδη του R, $(1-e)^2 = 1-e$, και η απεικόνιση $\varphi : R \to < e > \times < 1-e >$, $\varphi(r) =< re, r(1-e) >$ είναι ένας ισομορφισμός δακτυλίων.

26. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο και ιδεώδη I, J του R που έχουν τις ιδιότητες $I + J = R$, $I \cap J =< 0 >$. Αποδείξτε ότι υπάρχει ισομορφισμός δακτυλίων $R \cong I \times J$.

27. Έστω m, n θετικοί ακέραιοι με $\mu\kappa\delta(m, n) = 1$. Είδαμε ότι υπάρχει ένας ισομορφισμός δακτυλίων $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. Δώστε μία άλλη απόδειξη χρησιμοποιώντας την προηγούμενη άσκηση.

28. Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Αποδείξτε ότι το σύνολο $N(R)$ των μηδενοδυνάμων στοιχείων του R (βλ Άσκηση 2.1.26) αποτελεί ιδεώδες του R.

29. Αποδείξτε ότι υπάρχει μόνο ένας ισομορφισμός δακτυλίων $R \to R$, στις παρακάτω περιπτώσεις.

    i) $R = \mathbb{Z}$
    Υπόδειξη: $f(n) = nf(1)$.

    ii) $R = \mathbb{Q}$
    Υπόδειξη: $f(\frac{m}{n}) = mf\left(\frac{1}{n}\right)$ και $f(1) = nf\left(\frac{1}{n}\right)$.

    iii) $R = \mathbb{R}$
    Υπόδειξη: Κάθε $r \in \mathbb{R}$ είναι όριο ακολουθίας ρητών αριθμών.

30. Έστω $\varphi : R \to S$ ένας ομομορφισμός δακτυλίων.

    i) Αποδείξτε ότι: J ιδεώδες του $S \Rightarrow \varphi^{-1}(J)$ ιδεώδες του R.

    ii) Δείξτε με συγκεκριμένο παράδειγμα ότι η συνεπαγωγή "I ιδεώδες του $R \Rightarrow \varphi(I)$ ιδεώδες του S" δεν αληθεύει.

    iii) Αποδείξτε ότι η συνεπαγωγή του ii) είναι αληθής αν υποθέσουμε ότι η φ είναι επί.

31. Έστω $\varphi : R \to S$ ένας ισομορφισμός δακτυλίων που έχουν μοναδιαία στοιχεία. Αποδείξτε τις εξής προτάσεις:

    i) Έστω $u \in R$. Τότε $u \in U(R)$ αν και μόνο αν $\varphi(u) \in U(S)$.

    ii) Η απεικόνιση $U(R) \ni u \mapsto \varphi(u) \in U(S)$ είναι $1-1$ και επί.

32. i) Έστω $\varphi : R \to S$ ένας επιμορφισμός μεταθετικών δακτυλίων που έχουν μοναδιαία στοιχεία. Αν κάθε ιδεώδες του R είναι κύριο, αποδείξτε ότι κάθε ιδεώδες του S είναι κύριο. Άρα κάθε ιδεώδες του $\mathbb{Z}_m$ είναι κύριο.

    ii) Να βρεθούν όλα τα ιδεώδη του $\mathbb{Z}_6$ και $\mathbb{Z}_{12}$.

33. Να βρεθούν όλοι οι ομομορφισμοί δακτυλίων

    i) $\mathbb{Z}_m \to \mathbb{Z}$

    ii) $\mathbb{Z} \to \mathbb{Z}_m$

    iii) $\mathbb{Z}_6 \to \mathbb{Z}_2$

    iv) $\mathbb{Z}_2 \to \mathbb{Z}_6$

34. Αποδείξτε ότι η αντιστοιχία $\varphi : \mathbb{Z}_{12} \to \mathbb{Z}_4$, $\varphi([a]_{12}) = [a]_4$ είναι μία απεικόνιση και μάλιστα ένας επιμορφισμός δακτυλίων. Να βρεθεί ο $\ker\varphi$.

35. Αληθεύει ότι υπάρχει δακτύλιος S και ομομορφισμός δακτυλίων $\varphi : \mathbb{R} \to S$ με $\ker\varphi = \mathbb{Z}$;

2.6 Δακτύλιος Πηλίκο

Ο σκοπός της Παραγράφου αυτής είναι να εξηγήσουμε πώς από ένα δακτύλιο R και ένα ιδεώδες I του R κατασκευάζεται ένας νέος δακτύλιος R/I, που ονομάζεται δακτύλιος πηλίκο του R modulo I. Η μέθοδος που θα δούμε εδώ αποτελεί γενίκευση της κατασκευής του $\mathbb{Z}_n$ που μελετήσαμε στην Παράγραφο 1.4.

Έστω R ένας δακτύλιος και I ένα ιδεώδες του R. Ορίζουμε μια σχέση στο R, ως εξής:

$$a \equiv b \mod I \Leftrightarrow a - b \in I.$$

Όταν το I είναι δεδομένο συχνά θα χρησιμοποιούμε τον συμβολισμό $a \equiv b$ στη θέση του $a \equiv b \mod I$. Αυτή η σχέση είναι μια σχέση ισοδυναμίας. Πράγματι, παρατηρούμε ότι: 1) $a - a = 0 \in I$ για κάθε $a \in R$. 2) Αν έχουμε $a \equiv b$, τότε $a - b \in I$ και άρα $-(a - b) \in I$. Συνεπώς $b - a \in I$ δηλαδή $b \equiv a$. 3) Αν έχουμε $a \equiv b$ και $b \equiv c$, τότε $a - b \in I$, $b - c \in I$ και άρα $(a - b) + (b - c) \in I$. Συνεπώς $a - c \in I$, δηλαδή $a \equiv c$.

Η κλάση ισοδυναμίας του a συμβολίζεται με $a + I$. Παρατηρούμε ότι

$$\begin{aligned} a + I &= \{x \in R | x \equiv a\} = \{x \in R | x - a \in I\} \\ &= \{x \in R | x - a = y \in I\} = \{a + y | y \in I\}. \end{aligned}$$

Η κλάση ισοδυναμίας $a + I$ ονομάζεται η ***κλάση του a modulo I***. Το σύνολο αυτών των κλάσεων ισοδυναμίας συμβολίζεται με R/I,

$$R/I = \{a + I | a \in R\}.$$

Για παράδειγμα, αν $R = \mathbb{Z}$ και $I = 2\mathbb{Z}$, τότε $\mathbb{Z}/2\mathbb{Z} = \{2\mathbb{Z}, 1 + 2\mathbb{Z}\}$. Η κλάση $1 + 2\mathbb{Z}$ είναι το σύνολο των περιττών ακεραίων. Με τον συμβολισμό της Παραγράφου 1.4 έχουμε $1 + 2\mathbb{Z} = [1]$.

Υπενθυμίζουμε (βλ. Παράγραφο 1.4) ότι δύο κλάσεις ισοδυναμίας είτε ταυτίζονται (αν οι αντιπρόσωποί τους είναι ισοδύναμοι) είτε είναι ξένα σύνολα. Επομένως

$$a + I = b + I \Leftrightarrow a \equiv b \mod I \Leftrightarrow a - b \in I. \tag{1}$$

Επισημαίνουμε ότι μέχρι εδώ δεν έχει χρησιμοποιηθεί η δεύτερη ιδιότητα στον ορισμό του ιδεώδους (Ορισμός 2.5.5). Συνεπώς το σύνολο R/I έχει νόημα όταν το I είναι, για παράδειγμα, υποδακτύλιος του R.

Χρησιμοποιώντας τις πράξεις του R, θα ορίσουμε τώρα δύο πράξεις στο R/I ως προς τις οποίες το R/I είναι δακτύλιος. Εδώ θα χρησιμοποιηθεί και η δεύτερη ιδιότητα στον ορισμό του ιδεώδους.

Η πρόσθεση και ο πολλαπλασιασμός ορίζονται από τις αντιστοιχίες

$$R/I \times R/I \to R/I,\ (a+I, b+I) \mapsto (a+b)+I$$

$$R/I \times R/I \to R/I,\ (a+I, b+I) \mapsto ab+I$$

Πρώτα από όλα πρέπει να δείξουμε ότι οι αντιστοιχίες αυτές είναι απεικονίσεις. Έστω λοιπόν $a+I = c+I$ και $b+I = d+I$, δηλαδή $a-c \in I$ και $b-d \in I$. Τότε για την πρόσθεση έχουμε

$$(a+b)-(c+d) = (a-c)+(b-d) \in I \Rightarrow (a+b)+I = (c+d)+I.$$

Για τον πολλαπλασιασμό έχουμε

$$ab-cd = ab-cb+cb-cd = (a-c)b+c(b-d) \in I$$

γιατί το I είναι ιδεώδες. Άρα $ab+I = cd+I$.

Η επαλήθευση τώρα των ιδιοτήτων στον ορισμό του δακτυλίου είναι υπόθεση ρουτίνας. Για παράδειγμα, για την προσεταιριστική ιδιότητα της πρόσθεσης έχουμε: $((a+I)+(b+I))+(c+I) = ((a+b)+I)+(c+I) = ((a+b)+c)+I = (a+(b+c))+I = (a+I)+((b+c)+I) = (a+I)+((b+I)+(c+I))$. Παρατηρούμε ότι στην απόδειξη κάθε μιας από αυτές τις ιδιότητες για το R/I, χρησιμοποιούμε την αντίστοιχη ιδιότητα του R. Το μηδενικό στοιχείο είναι το

$$0+I = I,$$

ενώ το αντίθετο του $a+I$ είναι το $(-a)+I$, δηλαδή

$$-(a+I) = (-a)+I.$$

Αν ο R έχει μοναδιαίο στοιχείο το 1, τότε ο R/I έχει μοναδιαίο στοιχείο το

$$1+I$$

γιατί $(1+I)(a+I) = 1a+I = a+I$ και όμοια $(a+I)(1+I) = a+I$ για κάθε $a \in R$. Επιπλέον, αν ο R είναι μεταθετικός τότε και ο R/I είναι μεταθετικός, γιατί $(a+I)(b+I) = ab+I = ba+I = (b+I)(a+I)$.

Ο δακτύλιος R/I ονομάζεται ο ***δακτύλιος πηλίκο του R modulo I***.

Συνοψίζοντας τα παραπάνω, έχουμε το εξής αποτέλεσμα:

2.6.1 Πρόταση. *Έστω I ένα ιδεώδες του δακτυλίου R. Τότε*

1. *Το R/I είναι δακτύλιος ως προς τις πράξεις*

$$R/I \times R/I \to R/I,\ (a+I, b+I) \mapsto (a+b)+I$$

$$R/I \times R/I \to R/I,\ (a+I, b+I) \mapsto ab+I$$

2. *Αν ο R έχει μοναδιαίο στοιχείο, τότε και ο R/I έχει μοναδιαίο στοιχείο.*

3. *Αν ο R είναι μεταθετικός, τότε και ο R/I είναι μεταθετικός.*

Παρατηρούμε ότι η απεικόνιση $\pi : R \to R/I$, $r \mapsto r + I$, είναι ένας επιμορφισμός δακτυλίων. Πράγματι, είναι προφανές ότι η π είναι επί. Επίσης έχουμε $\pi(a+b) = (a+b)+I = (a+I)+(b+I) = \pi(a)+\pi(b)$. Όμοια αποδεικνύεται ότι $\pi(ab) = \pi(a)\pi(b)$. Η απεικόνιση αυτή ονομάζεται ***φυσικός επιμορφισμός***.

2.6.2 Παραδείγματα.

1) Για $R = \mathbb{Z}$ και $I = n\mathbb{Z}$ έχουμε $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

2) Για $R = 2\mathbb{Z}$ και $I = 4\mathbb{Z}$ έχουμε $2\mathbb{Z}/4\mathbb{Z} = \{4\mathbb{Z}, 2 + 4\mathbb{Z}\}$. Σημειώνουμε ότι ο δακτύλιος $2\mathbb{Z}/4\mathbb{Z}$ δεν είναι ισόμορφος με τον $\mathbb{Z}_2$ (γιατί;).

3) Στο $\mathbb{Q}[x]$ θεωρούμε το κύριο δεώδες $I =< x - 1 >= \{f(x)(x-1) | f(x) \in \mathbb{Q}[x]\}$. Θα σχολιάσουμε την αριθμητική στο πηλίκο $\mathbb{Q}[x]/I$.

   Το $\mathbb{Q}[x]/I$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο σύμφωνα με την παραπάνω Πρόταση. Κάθε στοιχείο του $\mathbb{Q}[x]/I$ έχει τη μορφή $f(x) + I$, όπου $f(x) \in \mathbb{Q}[x]$ και ισχύει

$$\begin{aligned} f(x) + I = g(x) + I \Leftrightarrow \\ f(x) - g(x) \in I \Leftrightarrow \\ x - 1 | f(x) - g(x). \end{aligned}$$

   Δηλαδή έχουμε $f(x) + I = g(x) + I$ αν και μόνο αν, τα πολυώνυμα

   $f(x)$ και $g(x)$ αφήνουν το ίδιο υπόλοιπο όταν διαιρεθούν με το $x - 1$. (2)

   Επομένως, αν $r(x)$ είναι το υπόλοιπο της διαίρεσης του $f(x)$ με το $x - 1$, τότε

$$f(x) + I = r(x) + I.$$

   Αλλά το υπόλοιπο της διαίρεσης του $f(x)$ με το $x-1$ είναι το $f(1)$ σύμφωνα με το Θεώρημα 2.4.1. Άρα $f(x) + I = f(1) + I$. Για παράδειγμα, έχουμε $(x^2 - 2x + 4) + I = 3 + I$.

   Έχοντας υπόψη τα προηγούμενα, είναι φυσικό να θεωρήσουμε την αντιστοιχία

$$\varphi : \mathbb{Q}[x]/I \to \mathbb{Q},\ f(x) + I \mapsto f(1),$$

που είναι απεικόνιση (και μάλιστα 1-1) λόγω του (2). Είναι δε και επί γιατί δοθέντος του $c \in \mathbb{Q}$, έχουμε $\varphi(c+I) = c$. Η φ είναι και ομομορφισμός δακτυλίων αφού

$$\begin{aligned}\varphi((f(x)+I)+(g(x)+I)) &= \varphi((f(x)+g(x))+I)\\ &= f(1)+g(1) = \varphi(f(x)+I)+\varphi(f(x)+I), \quad \text{και}\\ \varphi((f(x)+I)(g(x)+I)) &= \varphi((f(x)g(x)+I)) = f(1)g(1)\\ &= \varphi(f(x)+I)\varphi(f(x)+I).\end{aligned}$$

Συνεπώς ο δακτύλιος $\mathbb{Q}[x]/I$ είναι ισόμορφος με το $\mathbb{Q}$, και άρα είναι σώμα. Το αντίστροφο του μη μηδενικού $f(x)+I$ είναι το $f(1)^{-1}+1$. (Εφόσον το $f(x)+I$ είναι μη μηδενικό στοιχείο του πηλίκου έχουμε $f(x)+I \neq I$, δηλαδή το $x-1$ δεν διαιρεί το $f(x)$ και άρα $f(1) \neq 0$.) Βλέπουμε, λοιπόν, ότι η αριθμητική των κλάσεων $f(x)+I$ ανάγεται στην αριθμητική του $\mathbb{Q}$ κάτω από την αντιστοιχία $f(x)+I \mapsto f(1)$.

Θα διαπιστώσουμε παρακάτω ότι ο ισομορφισμός αυτού του παραδείγματος εντάσσεται σε ένα γενικότερο πλαίσιο, βλ. Πρώτο Θεώρημα Ισομορφισμών.

4) Θεωρούμε το κύριο ιδεώδες $I =< x^2+x+1 >$ του $\mathbb{Z}_2[x]$. Θα δείξουμε ότι το πηλίκο $\mathbb{Z}_2[x]/I$ είναι ένα σώμα που αποτελείται από 4 στοιχεία. Σύμφωνα με την Πρόταση 2.6.1 το $\mathbb{Z}_2[x]/I$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Έχουμε

$$\begin{aligned} f(x)+I = g(x)+I &\Leftrightarrow\\ f(x)-g(x) \in I &\Leftrightarrow\\ x^2+x+1 | f(x)-g(x).&\end{aligned}$$

Δηλαδή έχουμε $f(x)+I = g(x)+I$, αν και μόνο αν, τα πολυώνυμα

$f(x)$ και $g(x)$ αφήνουν το ίδιο υπόλοιπο όταν διαιρεθούν με το x^2+x+1.

Βλέπουμε, έτσι, ότι κάθε $f(x)+I$ έχει μία παράσταση της μορφής

$$f(x)+I = r(x)+I,$$

όπου $r(x)$ είναι το υπόλοιπο της διαίρεσης του $f(x)$ με το x^2+x+1. Επειδή $\deg r(x) < 2$ έχουμε

$$f(x)+I = (ax+b)+I.$$

Η παράσταση αυτή του $f(x)+I$ με αντιπρόσωπο πολυώνυμο βαθμού ≤ 1 είναι βέβαια μοναδική, γιατί

$$\begin{gathered}(ax+b)+I=(cx+d)+I \Rightarrow \\ x^2+x+1|(ax+b)-(cx+d) \Rightarrow \\ (ax+b)-(cx+d)=0.\end{gathered}$$

Επειδή έχουμε ότι $a,b\in\mathbb{Z}_2$, συμπεραίνουμε ότι το πηλίκο $\mathbb{Z}_2[x]/I$ αποτελείται απο $2\cdot 2=4$ στοιχεία,

$$\mathbb{Z}_2[x]/I=\{I,1+I,x+I,(x+1)+I\}.$$

Έχουμε $(x+I)((x+1)+I)=(x^2+x)+I=1+I$, γιατί το υπόλοιπο της διαίρεσης του x^2+x με το x^2+x+1 στο $\mathbb{Z}_2[x]$ είναι το 1. Άρα τα $x+I$ και $(x+1)+I$ είναι αντιστρέψιμα και συνεπώς το $\mathbb{Z}_2[x]/I$ είναι σώμα.

Θέτοντας για συντομία $0=I$, $1=1+I$, $\alpha=x+I$, βλέπουμε μετά από μερικούς υπολογισμούς ότι οι πίνακες των πράξεων είναι:

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Μια εφαρμογή των πινάκων αυτών σε ένα ενδιαφέρον συνδυαστικό πρόβλημα θα δούμε στην Παράγραφο 2.7.

5) Θεωρούμε το κύριο ιδεώδες $I=<x^2+1>$ του $\mathbb{Z}_2[x]$. Τότε το πηλίκο $\mathbb{Z}_2[x]/I$ δεν είναι ακεραία περιοχή.

Πράγματι, στο $\mathbb{Z}_2[x]$ έχουμε $x^2+1=(x+1)^2$. Επίσης το $(x+1)+I$ είναι μη μηδενικό στοιχείο του πηλίκου, δηλαδή $(x+1)+I\neq I$, αφού το x^2+1 δεν διαιρεί το $x+1$ στο $\mathbb{Z}_2[x]$. Ένας μηδενοδιαρέτης του πηλίκου $\mathbb{Z}_2[x]/I$ είναι το $(x+1)+I$, γιατί

$$((x+1)+I)((x+1)+I)=(x+1)^2+I=(x^2+1)+I=I.$$

6) Έστω $R = M_2(\mathbb{Z})$ και $I = M_2(2\mathbb{Z})$. Εύκολα αποδεικνύεται ότι το I είναι ένα ιδεώδες του R. Θα δούμε εδώ ότι το πλήθος των στοιχείων του R/I είναι ίσο με 16. Πράγματι, έστω $\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in R$. Έστω r_i το υπόλοιπο της διαίρεσης του a_i με το 2. Τότε

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} - \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} \in I,$$

και κατά συνέπεια στο R/I έχουμε

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} + I = \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} + I$$

Επειδή $r_i \in \{0, 1\}$, συμπεραίνουμε ότι ο R/I έχει το πολύ 16 στοιχεία. Είναι φανερό ότι αν $\begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} \neq \begin{pmatrix} r'_1 & r'_2 \\ r'_3 & r'_4 \end{pmatrix}$ με $r_i, r'_i \in \{0, 1\}$, τότε $\begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} + I \neq \begin{pmatrix} r'_1 & r'_2 \\ r'_3 & r'_4 \end{pmatrix} + I$. Άρα ο R/I αποτελείται από 16 στοιχεία. Μπορεί να αποδειχτεί ότι $R/I \cong M_2(\mathbb{Z}_2)$: Πράγματι, η απεικόνιση $R/I \to M_2(\mathbb{Z}_2)$, $\begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} + I \mapsto \begin{pmatrix} [r_1] & [r_2] \\ [r_3] & [r_4] \end{pmatrix} \in M_2(\mathbb{Z}_2)$ είναι ένας ισομορφισμός δακτυλίων. (Βλ. Άσκηση 26).

Από τα παραδείγματα που μόλις είδαμε, τα 3, 4 και 5 αφορούσαν πηλίκα της μορφής $F[x]/I$, όπου F είναι ένα σώμα και I ένα ιδεώδες της μορφής $< p(x) >$. Στα παραδείγματα 3 και 4 το $p(x)$ ήταν ανάγωγο και τα αντίστοιχα πηλίκα ήταν σώματα. Στο παράδειγμα 5 το $p(x)$ δεν ήταν ανάγωγο και το αντίστοιχο πηλίκο δεν ήταν σώμα. Σχετικά ισχύει το ακόλουθο αποτέλεσμα.

2.6.3 Θεώρημα. *Έστω F ένα σώμα, $p(x) \in F[x]$ και $I =< p(x) >$. Τότε ο δακτύλιος πηλίκο $F[x]/I$ είναι σώμα αν και μόνο αν το $p(x)$ είναι ανάγωγο στο $F[x]$.*

Απόδειξη. Έστω ότι ο $F[x]/I$ είναι σώμα και $p(x) = a(x)b(x)$ με $a(x), b(x) \in F[x]$ και $\deg a(x) < \deg p(x)$ και $\deg b(x) < \deg p(x)$. Τότε στο $F[x]/I$ ισχύει

$$I = p(x) + I = a(x)b(x) + I = (a(x) + I)(b(x) + I).$$

Επειδή το $F[x]/I$ δεν έχει μηδενοδιαιρέτες έχουμε $a(x) + I = I$ ή $b(x) + I = I$, δηλαδή $a(x) \in I$ ή $b(x) \in I$. Επειδή $I =< p(x) >$ παίρνουμε $p(x)|a(x)$ ή $p(x)|b(x)$ που σημαίνει ότι $\deg a(x) \geq \deg p(x)$ ή $\deg b(x) \geq \deg p(x)$. Αυτό είναι άτοπο.

Αντίστροφα, έστω ότι το $p(x)$ είναι ανάγωγο στο $F[x]$. Από την Πρόταση 2.6.1 αρκεί να δείξουμε ότι κάθε μη μηδενικό στοιχείο του $F[x]/I$ είναι αντιστρέψιμο. Έστω $f(x)+I \in F[x]/I$ με $f(x)+I \neq I$. Τότε το $f(x)$ δεν ανήκει στο I και κατά συνέπεια το $p(x)$ δεν διαιρεί το $f(x)$. Επειδή το $p(x)$ είναι ανάγωγο έχουμε $\mu\kappa\delta(f(x),p(x))=1$. Από το Θεώρημα 2.3.7 υπάρχουν $a(x),b(x)\in F[x]$ τέτοια ώστε

$$1 = a(x)f(x)+b(x)p(x).$$

Επειδή $b(x)p(x)\in I$ έχουμε $b(x)p(x)+I=I$ και επομένως

$$\begin{aligned} 1+I &= (a(x)f(x)+I)+(b(x)p(x)+I) \\ &= a(x)f(x)+I = (a(x)+I)(f(x)+I). \end{aligned}$$

Άρα το $f(x)+I$ είναι αντιστρέψιμο. ⊤

Σημείωση Καλό είναι να συγκριθεί η παραπάνω απόδειξη με αυτή της Πρότασης 1.4.5 και να σημειωθεί η αναλογία μεταξύ αναγώγων πολυωνύμων και πρώτων αριθμών. Η απόδειξη μας παρέχει έναν τρόπο προσδιορισμού του αντίστροφου ενός μη μηδενικού στοιχείου του $F[x]/<p(x)>$. Ας δούμε ένα παράδειγμα.

2.6.4 Παράδειγμα. Έστω $p(x)=x^2+x+1\in\mathbb{Z}_5[x]$. Επειδή $\deg p(x)=2$ και το $p(x)$ δεν έχει ρίζα στο $\mathbb{Z}_5$, από την Πρόταση 2.4.5 έχουμε ότι το $p(x)$ είναι ανάγωγο στο $\mathbb{Z}_5[x]$. Άρα το πηλίκο $\mathbb{Z}_5[x]/I$, όπου $I=<p(x)>$, είναι σώμα λόγω του Θεωρήματος 2.6.3. Θα προσδιορίσουμε το αντίστροφο του $f(x)+I$, όπου $f(x)=x^3+x+1$. Εφαρμόζοντας τον Ευκλείδειο Αλγόριθμο (Παράγραφος 2.3) βρίσκουμε $\mu\kappa\delta(f(x),p(x))=1$ και

$$1=(3x+2)f(x)+(2x^2-4x+4)p(x).$$

Άρα το αντίστροφο του $f(x)+I$ είναι το $(3x+2)+I$.

Στη συνέχεια θα εξετάσουμε τη σχέση μεταξύ ιδεωδών, ομομορφισμών δακτυλίων και δακτυλίων πηλίκο. Είδαμε πριν ότι ο πυρήνας κάθε ομομορφισμού δακτυλίων είναι ένα ιδεώδες. Θα δούμε τώρα ότι κάθε ιδεώδες I είναι πυρήνας κάποιου ομομορφισμού δακτυλίων.

2.6.5 Πρόταση. *Έστω I ένα ιδεώδες του δακτυλίου R. Τότε η απεικόνιση*

$$\pi : R\to R/I,\ \pi(r)=r+I$$

είναι ένας επιμορφισμός δακτυλίων και ισχύει $\ker\pi = I$.

Απόδειξη. Είδαμε μετά την Πρόταση 2.6.1 ότι η απεικόνιση π είναι ένας επιμορφισμός δακτυλίων. Ο πυρήνας του είναι $\ker\pi = \{r \in R | \pi(r) = 0_{R/I}\} = \{r \in R | r + I = I\} = \{r \in R | r \in I\} = I$. ⊤

Επειδή ο πυρήνας $\ker\varphi$ ενός ομομορφισμού δακτυλίων $\varphi : R \to S$ είναι ένα ιδεώδες του R, το σύνολο $R/\ker\varphi$ είναι ένας δακτύλιος ως προς τις πράξεις της Πρότασης 2.6.1. Σύμφωνα με το επόμενο αποτέλεσμα οι δακτύλιοι $R/\ker\varphi$ και $\mathrm{Im}\varphi$ είναι ισόμορφοι.

2.6.6 Πρώτο Θεώρημα Ισομορφισμών Δακτυλίων. *Έστω $\varphi : R \to S$ ένας ομομορφισμός δακτυλίων. Τότε η απεικόνιση*

$$R/\ker\phi \cong Im\phi,\ r + \ker\phi \mapsto \phi(r)$$

είναι ένας ισομορφισμός δακτυλίων.

Απόδειξη. Πρώτα θα δείξουμε ότι η αντιστοιχία

$$\psi : R/\ker\varphi \to \mathrm{Im}\varphi,\ \psi(r + \ker\varphi) = \varphi(r)$$

είναι μία απεικόνιση. Για συντομία έστω $I = \ker\varphi$. Έστω $r + I = s + I$, όπου $r, s \in R$. Τότε

$$\begin{aligned} r + I = s + I \Rightarrow r - s \in I \Rightarrow \phi(r - s) = 0 \\ \Rightarrow \phi(r) = \phi(s) \Rightarrow \psi(r + I) = \psi(s + I). \end{aligned}$$

Η ψ είναι ένας ομομορφισμός δακτυλίων επειδή για κάθε $r, s \in R$, έχουμε

$$\begin{aligned} \psi((r + I) + (s + I)) = \psi((r + s) + I) = \phi(r + s) = \phi(r) + \phi(s) \\ = \psi(r + I) + \psi(s + I) \end{aligned}$$

και

$$\psi((r + I)(s + I)) = \psi(rs + I) = \phi(rs) = \phi(r)\phi(s) = \psi(r + I)\psi(s + I).$$

Είναι προφανές ότι η απεικόνιση ψ είναι επί. Τέλος, για να διαπιστώσουμε ότι ο ψ είναι μονομορφισμός, αρκεί να δείξουμε ότι $\ker\psi = \{0_{R/I}\}$. Έχουμε

$$\begin{aligned} r + I \in \ker\psi \Rightarrow \psi(r + I) = 0_S \Rightarrow \phi(r) = 0_S \\ \Rightarrow r \in \ker\phi = I \Rightarrow r + I = I = 0_{R/I}. \end{aligned}$$ ⊤

Το προηγούμενο θεώρημα μας επιτρέπει πολλές φορές να "αναγνωρίσουμε" σαν κάτι πιο οικείο ένα δακτύλιο πηλίκο, όπως φαίνεται στα παρακάτω παραδείγματα.

2.6.7 Παραδείγματα.

1) Για κάθε $m, n \in \mathbb{Z}$ υπάρχει ένας ισομορφισμός δακτυλίων $\frac{\mathbb{Z}_{mn}}{< n >} \cong \mathbb{Z}_n$. Πράγματι, εύκολα διαπιστώνουμε ότι η αντιστοιχία $\mathbb{Z}_{mn} \to \mathbb{Z}_n$, $[a]_{mn} \mapsto [a]_n$ είναι μία απεικόνιση αφού αν $[a]_{mn} = [b]_{mn}$ τότε $n|a-b$ και άρα $[a]_n = [b]_n$. Η απεικόνιση αυτή είναι ένας επιμορφισμός δακτυλίων. Ο πυρήνας της είναι το ιδεώδες $< n >$ του $\mathbb{Z}_{mn}$. Άρα από το πρώτο Θεώρημα Ισομορφισμών υπάρχει ένας ισομορφισμός $\frac{\mathbb{Z}_{mn}}{< n >} \cong \mathbb{Z}_n$.

2) Η απεικόνιση $\epsilon_0 : \mathbb{Z}[x] \to \mathbb{Z}$, $f(x) \mapsto f(0)$, είναι ένας επιμορφισμός δακτυλίων. Ισχύει $\ker \epsilon_0 =< x >$. (Βλ. Παράδειγμα 2.5.6 7)). Από το Θεώρημα 2.6.6, έχουμε $\mathbb{Z}[x]/ < x > \cong \mathbb{Z}$.

3) Έστω F ένα σώμα και $I =< x-1 >= \{f(x)(x-1) \in F[x] | f(x) \in F[x]\}$ το κύριο ιδεώδες του $F[x]$ που παράγεται από το $x-1$. Ισχυριζόμαστε ότι $F[x]/I \cong F$. Πράγματι, θεωρούμε τον επιμορφισμό δακτυλίων $\epsilon_1 : F[x] \to F$, $\epsilon_1(f(x)) = f(1)$. Έχουμε $\ker \epsilon_1 =< x-1 >$ σύμφωνα με το Παράδειγμα 2.5.6 7). Το Θεώρημα 2.6.6 δίνει το ζητούμενο.

Με παρόμοιο τρόπο μπορεί να αποδειχτεί ότι $F[x]/I \cong F$, όπου $I = < ax-b >$, $a, b \in F$, $a \neq 0$.

4) Τα σώματα $\mathbb{R}[x]/ < x^2+1 >$ και $\mathbb{C}$ είναι ισόμορφα.
Πράγματι, η απεικόνιση $\varphi : \mathbb{R}[x] \to \mathbb{C}$, $f(x) \mapsto f(i)$ είναι ένας επιμορφισμός δακτυλίων. Αν $f(x) \in \ker \varphi$, τότε $x-i|f(x)$ στο $\mathbb{C}[x]$ σύμφωνα με το Θεώρημα 2.4.1. Από το Θεώρημα 2.4.10 συμπεραίνουμε ότι $x+i|f(x)$. Άρα $x^2+1|f(x)$ στο $\mathbb{C}[x]$, αφού τα $x-i, x+i$ είναι σχετικά πρώτα πολυώνυμα. Από την Άσκηση 2.3.2 έχουμε ότι $x^2+1|f(x)$ στο $\mathbb{R}[x]$. Άρα $\ker \varphi \subseteq < x^2+1 >$. Προφανώς έχουμε $< x^2+1 > \subseteq \ker \varphi$, οπότε $< x^2+1 >= \ker \varphi$. Από το 1^o Θεώρημα Ισομορφισμών έχουμε ότι $\mathbb{R}[x]/ < x^2+1 > \cong \mathbb{C}$.

5) Θεωρούμε το δακτύλιο R και το ιδεώδες I του παραδείγματος 2.5.6 8). Ισχυριζόμαστε ότι $R/I \cong \mathbb{R}$. Πράγματι, έστω η απεικόνιση

$$\phi : R \to \mathbb{R},\ \phi \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = a.$$

Η φ είναι επιμορφισμός δακτυλίων επειδή

$$\phi\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + \begin{pmatrix} c & d \\ 0 & c \end{pmatrix}\right) = \phi\begin{pmatrix} a+c & b+d \\ 0 & a+c \end{pmatrix}$$
$$= a + c = \phi\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + \phi\begin{pmatrix} c & d \\ 0 & c \end{pmatrix}$$

και

$$\phi\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0 & c \end{pmatrix}\right) = \phi\begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix}$$
$$= ac = \phi\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \cdot \phi\begin{pmatrix} c & d \\ 0 & c \end{pmatrix}$$

για κάθε $a, b, c, d \in \mathbb{R}$. Επιπλέον, ο πυρήνας είναι

$$\ker\varphi = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| a = 0 \right\} = I.$$

Άρα $R/I \cong \mathbb{R}$.

6) Έστω $R = \{m/n \in \mathbb{Q} | m, n \in \mathbb{Z},\ \mu\kappa\delta(m,n) = 1,\ n \text{ περιττός}\}$ και $I = \{m/n \in \mathbb{Q} | m, n \in \mathbb{Z},\ \mu\kappa\delta(m,n) = 1,\ n \text{ περιττός},\ m \text{ άρτιος }\}$. Τότε το R είναι ένας δακτύλιος και το I ένα ιδεώδες του R (άσκηση). Ισχυριζόμαστε ότι $R/I \cong \mathbb{Z}_2$. Πράγματι, ορίζουμε την απεικόνιση $\varphi : R \to \mathbb{Z}_2$, όπου $\varphi(m/n) = [0]$, αν το m είναι άρτιος, και $\varphi(m/n) = [1]$, αν το m είναι περιττός (εννοείται ότι $\mu\kappa\delta(m,n) = 1$). Τότε η φ είναι ένας επιμορφισμός δακτυλίων με πυρήνα το I (άσκηση), οπότε το ζητούμενο προκύπτει από το Θεώρημα 2.6.6.

7) Οι δακτύλιοι $\mathbb{R}[x]/ < x^2 >$ και $S = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in M_2(\mathbb{R}) \right\}$ είναι ισόμορφοι.
Πράγματι, εύκολα επαληθεύεται ότι η απεικόνιση

$$\varphi : \mathbb{R}[x] \to S,\ f_n x^n + \cdots + f_1 x + f_0 \mapsto \begin{pmatrix} f_0 & f_1 \\ 0 & f_0 \end{pmatrix} \in S$$

είναι ένας επιμορφισμός δακτυλίων. Έχουμε $\ker\varphi = \{f_n x^n + \cdots + f_1 x + f_0 \in \mathbb{R}[x] | f_0 = f_1 = 0\} = \{f_n x^n + \cdots + f_2 x^2 \in \mathbb{R}[x]\} =< x^2 >$. Από το 1^o Θεώρημα Ισομορφισμών συνάγουμε ότι $\mathbb{R}[x]/ < x^2 > \cong S$.

2.6.8 Δεύτερο Θεώρημα Ισομορφισμών. *Έστω I, J ιδεώδη ενός δακτυλίου R. Τότε υπάρχει ένας ισομορφισμός δακτυλίων* $\dfrac{I}{I \cap J} \cong \dfrac{I+J}{J}$.

Απόδειξη. Η απεικόνιση $\varphi : I \to \dfrac{I+J}{J}$, $a \mapsto a+J$, είναι ένας ομομορφισμός. Είναι δε και επί, αφού αν $a \in I$ και $b \in J$, τότε $a+b+J = a+J = \varphi(a)$. Έχουμε $\ker\varphi = I \cap J$. Το ζητούμενο προκύπτει από το $1^{ο}$ Θεώρημα Ισομορφισμών. ⊤

2.6.9 Τρίτο Θεώρημα Ισομορφισμών. *Έστω I, J ιδεώδη ενός δακτυλίου R με $I \subseteq J$. Τότε το $\dfrac{J}{I}$ είναι ένα ιδεώδες του $\dfrac{R}{I}$ και υπάρχει ένας ισομορφισμός δακτυλίων*

$$\frac{R/I}{J/I} \cong \frac{R}{J}$$

Απόδειξη. Η αντιστοιχία $\dfrac{R}{I} \to \dfrac{R}{J}$, $r+I \mapsto r+J$, είναι απεικόνιση αφού $I \subseteq J$. Είναι φανερό ότι αυτή είναι ένας επιμορφισμός. Ο πυρήνας της είναι το σύνολο $\{a+I | a \in J\}$ δηλαδή το $\dfrac{J}{I}$. Συνεπώς το $\dfrac{J}{I}$ είναι ένα ιδεώδες του $\dfrac{R}{I}$. Από το $1^{ο}$ Θεώρημα Ισομορφισμών προκύπτει ότι $\dfrac{R/I}{J/I} \cong \dfrac{R}{J}$. ⊤

Παράδειγμα

Έστω m, n θετικοί ακέραιοι και $d = μκδ(m,n)$, $e = εκπ(m,n)$. Γνωρίζουμε ότι $m\mathbb{Z} \cap n\mathbb{Z} = e\mathbb{Z}$ και $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ (βλ. Άσκηση 2.5.10). Έτσι, ο ισομορφισμός $\dfrac{m\mathbb{Z}}{m\mathbb{Z} \cap n\mathbb{Z}} \cong \dfrac{m\mathbb{Z}+n\mathbb{Z}}{n\mathbb{Z}}$ του $2^{ου}$ Θεωρήματος Ισομορφισμών ανάγεται σε έναν ισομορφισμό δακτυλίων $\dfrac{m\mathbb{Z}}{e\mathbb{Z}} \cong \dfrac{d\mathbb{Z}}{n\mathbb{Z}}$.

2.6.10 Θεώρημα Αντιστοιχίας Ιδεωδών. *Έστω $\varphi : R \to S$ ένας επιμορφισμός δακτυλίων και $I = \ker\varphi$. Έστω X το σύνολο των υποδακτυλίων του R που περιέχουν το I και Y το σύνολο των υποδακτυλίων του S. Τότε η απεικόνιση*

$$\Phi : X \to Y, \quad A \mapsto \varphi(A)$$

είναι $1-1$ και επί. Επίσης η απεικόνιση

$$\Phi' : X' \to Y', \quad J \mapsto \varphi(J)$$

είναι $1-1$ και επί, όπου X' είναι το σύνολο των ιδεωδών του R που περιέχουν το I και Y' το σύνολο των ιδεωδών του S.

Απόδειξη. Ας αποδείξουμε ότι η Φ' είναι $1-1$ και επί. Η απόδειξη για τη Φ είναι παρόμοια. Έστω $J \in X'$. Αφού η φ είναι επιμορφισμός, το $\varphi(J)$ είναι ένα ιδεώδες του S (γιατί;) και επομένως $\varphi(J) \in Y'$. Έστω $J_1, J_2 \in X'$ με $\varphi(J_1) = \varphi(J_2)$. Αν $a \in J_1$, τότε $\varphi(a) = \varphi(b)$ για κάποιο $b \in J_2$ και άρα

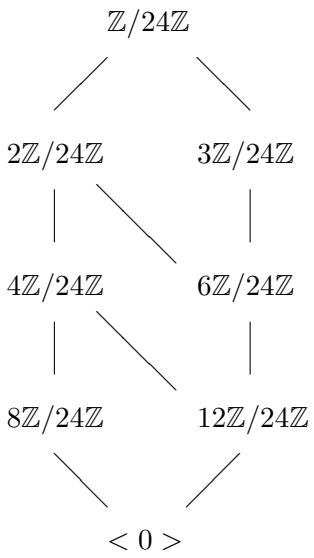
$a - b \in \ker \varphi = I$. Επειδή $I \subseteq J_2$ συμπεραίνουμε ότι $a \in J_2$. Συνεπώς $J_1 \subseteq J_2$. Όμοια αποδεικνύεται ότι $J_2 \subseteq J_1$. Άρα $J_1 = J_2$ και η Φ' είναι $1-1$. Έστω τώρα K ένα ιδεώδες του S. Τότε το $\varphi^{-1}(K)$ είναι ένα ιδεώδες του R που περιέχει το I (γιατί;). Ισχύει $\varphi(\varphi^{-1}(K)) = K$ και άρα η Φ' είναι επί. ⊤

2.6.11 Πόρισμα. *Έστω I ένα ιδεώδες του δακτυλίου R. Τότε κάθε ιδεώδες K του R/I είναι της μορφής $K = J/I$ για κάποιο ιδεώδες J του R που περιέχει το I. Επιπλέον, για κάθε K υπάρχει μοναδικό τέτοιο J.*

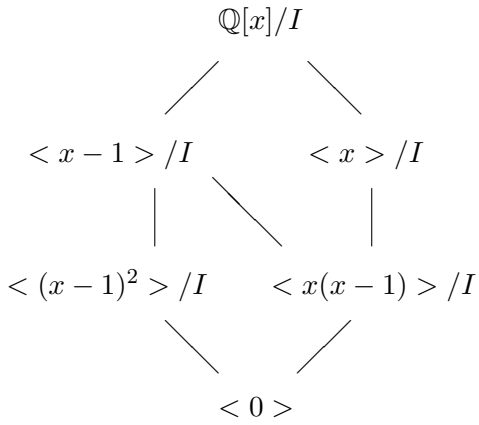
Απόδειξη. Η απόδειξη έπεται άμεσα αν εφαρμόσουμε το προηγούμενο Θεώρημα για τον φυσικό επιμορφισμό $R \to R/I$. ⊤

Παραδείγματα

1. Από το προηγούμενο Πόρισμα και την Άσκηση 2.5.11 συμπεραίνουμε ότι κάθε ιδεώδες του $\mathbb{Z}/m\mathbb{Z}$, $m \in \mathbb{N}$, είναι της μορφής $d\mathbb{Z}/m\mathbb{Z}$ για μοναδικό $d \in \mathbb{N}$ που είναι διαιρέτης του m. Έστω, για παράδειγμα, $m = 24$. Τότε τα ιδεώδη του $\mathbb{Z}/24\mathbb{Z}$ είναι τα εξής: $\mathbb{Z}/24\mathbb{Z}$, $2\mathbb{Z}/24\mathbb{Z}$, $3\mathbb{Z}/24\mathbb{Z}$, $4\mathbb{Z}/24\mathbb{Z}$, $6\mathbb{Z}/24\mathbb{Z}$, $8\mathbb{Z}/24\mathbb{Z}$, $12\mathbb{Z}/24\mathbb{Z}$, $24\mathbb{Z}/24\mathbb{Z} =< 0 >$. Μπορούμε να κατασκευάσουμε το "γράφημα των ιδεωδών"του δακτυλίου $R = \mathbb{Z}/24\mathbb{Z}$: Οι κορυφές του γραφήματος αντιστοιχούν στα ιδεώδη του R. Δύο ιδεώδη I, J του R συνδέονται με μία ακμή αν ισχύει $I \subseteq J$ ή $J \subseteq I$ και δεν υπάρχει ιδεώδες K με $I \subsetneqq K \subsetneqq J$ ή $J \subsetneqq K \subsetneqq I$. Στην περίπτωση αυτή, το ιδεώδες που αντιστοιχεί στο "άνω άκρο"της ακμής περιέχει το ιδεώδες που αντιστοιχεί στο "κάτω άκρο". Για τον δακτύλιο $R = \mathbb{Z}/24\mathbb{Z}$ το εν λόγω διάγραμμα είναι το εξής.



2. Έστω $R = \mathbb{Q}[x]/ < x^3 - 2x^2 + x >$. Θα ταξινομήσουμε τα ιδεώδη του R. Για συντομία, έστω $f(x) = x^3 - 2x^2 + x \in \mathbb{Q}[x]$. Όπως και στο προηγούμενο παράδειγμα, συμπεραίνουμε ότι κάθε ιδεώδες του R είναι της μορφής $< g(x) > / < f(x) >$, όπου $g(x) \in \mathbb{Q}[x]$ και $g(x)|f(x)$. Έχουμε $f(x) = x(x-1)^2$. Επομένως το διάγραμμα των ιδεωδών του R είναι το ακόλουθο, όπου με I συμβολίζουμε το ιδεώδες $< f(x) >$ του $\mathbb{Q}[x]$.



3. Έστω F ένα σώμα και $R = F[x]/ < x^2 >$. Από το Πόρισμα 2.6.11 και την Άσκηση 2.5.11 είναι φανερό ότι ο R περιέχει ένα μοναδικό ιδεώδες I με $I \neq < 0 >$ και $I \neq R$. Έχουμε $I = < x > / < x^2 >$. Από το 3^o Θεώρημα

Ισομορφισμών έχουμε $R/I \cong F[x]/ < x >$. Επειδή $F[x]/ < x > \cong F$ παίρνουμε ότι ο R/I είναι ισόμορφος με το F. Άρα ο R/I είναι ένα σώμα.

Ασκήσεις 2.6

1. Υπολογίστε τους πίνακες των πράξεων του δακτυλίου $3\mathbb{Z}/6\mathbb{Z}$. Παρατηρήστε ότι ο $3\mathbb{Z}/6\mathbb{Z}$ έχει μοναδιαίο στοιχείο αν και ο $3\mathbb{Z}$ δεν έχει.

2. Θεωρούμε το ιδεώδες $I = \{[0], [3]\}$ του $\mathbb{Z}_6$. Υπολογίστε τους πίνακες των πράξεων των $\mathbb{Z}_6/I$ και διαπιστώστε ότι $\mathbb{Z}_6/I \cong \mathbb{Z}_3$.

3. Έστω R, S δυο δακτύλιοι και $I = \{(r, 0)|r \in R\} \subseteq R \times S$. Αποδείξτε ότι το I είναι ένα ιδεώδες του $R \times S$ και ότι $(R \times S)/I \cong S$.

4. Αποδείξτε ότι $(\mathbb{Z} \times \mathbb{Z})/(m\mathbb{Z} \times n\mathbb{Z}) \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

5. Αποδείξτε ότι $\mathbb{Z}[x]/ < x^2 + 1 > \cong \mathbb{Z}[i]$.

6. Θεωρούμε τον δακτύλιο $R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{R}) \right\}$ και το ιδεώδες $I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R}) \right\}$. Αποδείξτε ότι $R/I \cong \mathbb{R} \times \mathbb{R}$.

7. Έστω p ένας πρώτος αριθμός,

$$R_p = \left\{ \frac{m}{n} \in \mathbb{Q} | m, n \in \mathbb{Z}, p \nmid n, \mu\kappa\delta(m, n) = 1 \right\},$$
$$I_p = \left\{ \frac{m}{n} \in \mathbb{Q} | m, n \in \mathbb{Z}, p \nmid n, \mu\kappa\delta(m, n) = 1, p|m \right\}.$$

   Αποδείξτε ότι το I_p είναι ένα ιδεώδες του R_p και $R_p/I_p \cong \mathbb{Z}_p$.

9. Έστω I ένα ιδεώδες του δακτυλίου R. Αποδείξτε ότι ο R/I είναι μεταθετικός αν και μόνο αν $ab - ba \in I$ για κάθε $a, b \in R$.

10. Έστω $R = \mathbb{Z} \times \mathbb{Z}$, $I = \{(3m, n) \in \mathbb{Z} \times \mathbb{Z} | m, n \in \mathbb{Z}\}$ και $J = \{(3m, 0) \in \mathbb{Z} \times \mathbb{Z} | m \in \mathbb{Z}\}$. Αποδείξτε ότι

    i) Ο R/I είναι ένα σώμα.

    ii) Ο R/J δεν είναι σώμα.

11. Αφού αποδείξετε ότι ο δακτύλιος $\mathbb{Z}_5[x]/ < p(x) >$ είναι σώμα, όπου $p(x) = x^2 + x + 2$, βρείτε το αντίστροφο του $2x + 3 + < p(x) >$.

12. Έστω $R = \mathbb{R}[x]$, $I =< x^2+1 >$, $J =< x^2+2 >$. Αποδείξτε ότι $R/I \cong R/J$ και $I \neq J$.

13. Εξετάστε αν οι παρακάτω δακτύλιοι είναι σώματα

    i) $\mathbb{Z}_5[x]/ < x^2+3, \ \ 3 >$

    ii) $\mathbb{Z}_5[x]/ < x^2+3, \ \ 5 >$

14. Εξετάστε αν οι παρακάτω δακτύλιοι είναι ακέραιες περιοχές

    i) $\mathbb{Z}[x,y]/ < x >$

    ii) $\mathbb{Z}[x,y]/ < xy >$

    iii) $\mathbb{Z}[x,y]/ < x,y >$

15. Έστω $f(x) = x^2+x+1 \in \mathbb{Z}_2[x]$. Στο Παράδειγμα 2.6.2 4) είδαμε ότι το πηλίκο $\mathbb{Z}_2[x]/ < f(x) >$ είναι σώμα που έχει 4 στοιχεία, $\mathbb{Z}_2[x]/ < f(x) >= \{I, 1+I, x+I, (x+1)+I\}$, όπου $I =< f(x) >$. Να υπολογιστεί το $(x+I)^{-1}((x+1)+I)^{64}$.

16. Ποια από τα παρακάτω πηλίκα είναι σώματα ή/και ακέραιες περιοχές;

    i) $\mathbb{Z}[x]/ < x >$

    ii) $\mathbb{Q}[x]/ < x^2-9 >$

    iii) $\mathbb{Q}[x]/ < x^3-2 >$

    iv) $\mathbb{Z}_3[x]/ < x^2+x+1 >$

17. Έστω $f(x) = x^2+1 \in \mathbb{Z}_3[x]$. Αποδείξτε ότι το $\mathbb{Z}_3[x]/ < f(x) >$ είναι ένα σώμα που έχει 9 στοιχεία. Ποιο είναι το αντίστροφο (αν υπάρχει) του $x^4+x+1+ < f(x) >$ στο $\mathbb{Z}_3[x]/ < f(x) >$.

18. Κατασκευάστε ένα σώμα που έχει 25 στοιχεία.

19. i) Έστω F ένα σώμα και $a,b,c,d \in F$ με $a \neq 0$, $c \neq 0$. Αποδείξτε ότι $F[x]/ < ax-b > \cong F[x]/ < cx-d >$.

    ii) Αποδείξτε ότι

$$\mathbb{Q}[x]/ < x^2-2 > \cong \mathbb{Q}[\sqrt{2}],$$

$$\mathbb{Q}[x]/ < x^2-3 > \cong \mathbb{Q}[\sqrt{3}]$$

    και

$$\mathbb{Q}[x]/ < x^2-2 > \ncong \mathbb{Q}[x]/ < x^2-3 > .$$

20. **Κινεζικό θεώρημα υπολοίπων**. Έστω R ένας δακτύλιος και I, J ιδεώδη του R.

    i) Αποδείξτε ότι υπάρχει ένας μονομορφισμός δακτυλίων $R/I \cap J \to R/I \times R/J$, $r + I \cap J \mapsto (r + I, r + J)$.

    ii) Αν τα ιδεώδη I, J είναι τέτοια ώστε $I + J = R$, αποδείξτε ότι υπάρχει ένας ισομορφισμός δακτυλίων $R/I \cap J \to R/I \times R/J$.

    iii) Για $R = \mathbb{Z}$, $I =< m >$, $J =< n >$, όπου $\mu\kappa\delta(m, n) = 1$, προκύπτει ότι $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

21. Έστω $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{R}[x]$. Αποδειξτε ότι

$$\mathbb{R}[x]/ < f(x) > \cong \begin{cases} \mathbb{C} \Leftrightarrow \deg f(x) = 2 \quad \text{και} \quad a_1^2 - 4a_0 < 0 \\ \mathbb{R} \Leftrightarrow \deg f(x) = 1 \end{cases}$$

22. Εξετάστε αν υπάρχει ισομορφισμός $\mathbb{Q}[x]/ < x^2 - 2 > \cong \mathbb{Q}[x]/ < x^2 + 2 >$.

23. Έστω R μια ακεραία περιοχή. Αποδείξτε ότι κάθε ισομορφισμός δακτυλίων $\varphi : R[x] \to R[x]$ με $\varphi(r) = r$ για κάθε $r \in R$ είναι της μορφής $\varphi(f(x)) = f(ax + b)$, όπου $a \in U(R)$, $b \in R$.

24. Αποδείξτε ότι $\mathbb{R}[x]/ < x^3 > \cong \left\{ \begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} \in M_3(\mathbb{R}) \right\}$ (βλ. Παράδειγμα 2.6.7 7). Βρείτε και αποδείξτε μία γενίκευση.

25. Αποδείξτε ότι $\mathbb{Q}[x]/ < x^2 - 1 > \cong \mathbb{Q} \times \mathbb{Q}$.
    Υπόδειξη: Άσκηση 20.

26. Έστω I ένα ιδεώδες του δακτυλίου R. Αποδείξτε ότι το $M_n(I)$ είναι ιδεώδες του $M_n(R)$ και $M_n(R)/M_n(I) \cong M_n(R/I)$.

27. Έστω $F = \{a_1, \ldots, a_n\}$ ένα πεπερασμένο σώμα. Έστω $p(x) = (x - a_1)(x - a_2) \cdots (x - a_n) \in F[x]$. Αποδείξτε ότι υπάρχει ένας ισομορφισμός δακτυλίων $F[x]/ < p(x) > \cong R$, όπου R είναι ο δακτύλιος των απεικονίσεων $F \to F$ (βλ. Παράδειγμα 2.1.2 4)).

28. Ποιό είναι το διάγραμμα των ιδεωδών του δακτυλίου

$$\left\{ \begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} \in M_3(\mathbb{R}) \right\}.$$

    Υπόδειξη: Άσκηση 24 και Θεώρημα 2.6.10.

29. Έστω R ένας δακτύλιος και I ένας υποδακτύλιος του R. Αποδείξτε ότι οι αντιστοιχίες

$$R/I \times R/I \to R/I,\ (a+I, b+I) \mapsto (a+b)+I$$

$$R/I \times R/I \to R/I,\ (a+I, b+I) \mapsto ab+I$$

είναι απεικονίσεις αν και μόνο αν το I είναι ιδεώδες.

2.7 Σώμα Πηλίκων, Χαρακτηριστική Δακτυλίου

Σώμα πηλίκων ακεραίας περιοχής

Το σώμα $\mathbb{Q}$ των ρητών αριθμών περιέχει την ακεραία περιοχή $\mathbb{Z}$ των ακεραίων αριθμών και κάθε στοιχείο του $\mathbb{Q}$ είναι "πηλίκο" δύο στοιχείων του $\mathbb{Z}$. Ξεκινώντας από μια ακεραία περιοχή R θα κατασκευάσουμε ένα σώμα F που "περιέχει" το R και που αποτελείται από "πηλίκα" στοιχείων του R.

Πριν προχωρήσουμε στην κατασκευή του F δίνουμε εδώ τη βασική ιδέα της. Στο $\mathbb{Q}$ ισχύει $3/5 = -3/-5 = 6/10 = 9/15 = \ldots$ πράγμα που σημαίνει ότι ο ρητός αριθμός $3/5$ δεν αντιπροσωπεύει μόνο το διατεταγμένο ζεύγος $(3,5)$ αλλά ένα σύνολο διατεταγμένων ζευγών που περιλαμβάνει τα

$$(3,5), (-3,-5), (6,10), (9,15), \ldots.$$

Ο ρητός αριθμός α/β αντιπροσωπεύει το σύνολο αυτό, όπου $(\alpha,\beta) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$, αν και μόνο αν $\alpha/\beta = 3/5$, δηλαδή $5\alpha = 3\beta$. Η κύρια ιδέα εδώ είναι ότι στο σύνολο $\mathbb{Z} \times (\mathbb{Z} - \{0\})$, η σχέση που ορίζεται από "$(\alpha,\beta) \equiv (\gamma,\delta)$ αν και μόνο αν $\alpha\delta = \beta\gamma$" είναι μια σχέση ισοδυναμίας. Ο ρητός αριθμός $3/5$ είναι η κλάση ισοδυναμίας που περιέχει το στοιχείο $(3,5)$.

Έστω R μια ακεραία περιοχή. Στο σύνολο $R \times (R - \{0\})$ ορίζουμε μια σχέση

$$(\alpha,\beta) \equiv (\gamma,\delta) \Leftrightarrow \alpha\delta = \beta\gamma.$$

Η σχέση αυτή είναι σχέση ισοδυναμίας γιατί,

1) $(\alpha,\beta) \equiv (\alpha,\beta)$ για κάθε $(\alpha,\beta) \in R \times (R - \{0\})$, αφού $\alpha\beta = \beta\alpha$,

2) αν $(\alpha,\beta) \equiv (\gamma,\delta)$, όπου $(\alpha,\beta), (\gamma,\delta) \in R \times (R - \{0\})$, τότε $\alpha\delta = \beta\gamma$ και άρα $(\gamma,\delta) \equiv (\alpha,\beta)$,

3) αν $(\alpha,\beta) \equiv (\gamma,\delta)$ και $(\gamma,\delta) \equiv (\epsilon,\zeta)$, όπου $(\alpha,\beta), (\gamma,\delta), (\epsilon,\zeta) \in R \times (R - \{0\})$, τότε $\alpha\delta = \beta\gamma$ και $\gamma\zeta = \delta\epsilon$ οπότε $\alpha\delta\zeta = (\beta\gamma)\zeta = \beta(\gamma\zeta) = \beta\delta\epsilon$, δηλαδή $\alpha\zeta\delta = \beta\epsilon\delta$. Επειδή $\delta \neq 0$ και ο R είναι ακεραία περιοχή, από την τελευταία ισότητα έπεται ότι $\alpha\zeta = \beta\epsilon$, δηλαδή $(\alpha,\beta) \equiv (\epsilon,\zeta)$.

Με α/β συμβολίζουμε την κλάση ισοδυναμίας του (α,β)

$$\alpha/\beta = \{(x,y) \in R \times (R - \{0\}) | (x,y) \equiv (\alpha,\beta)\}.$$

Με F συμβολίζουμε το σύνολο των παραπάνω κλάσεων ισοδυναμίας

$$F = \{\alpha/\beta | (\alpha,\beta) \in R \times (R - \{0\})\}.$$

Στη συνέχεια θα οριστούν στο F δύο πράξεις ως προς τις οποίες το F είναι ένα σώμα τέτοιο ώστε να περιέχει δακτύλιο ισόμορφο με το R. Έστω $(\alpha,\beta), (\gamma,\delta) \in$

$R \times (R - \{0\})$. Τότε $\beta\delta \neq 0$, γιατί ο R είναι ακεραία περιοχή. Ορίζουμε δύο αντιστοιχίες $+ : F \times F \to F$ και $\cdot : F \times F \to F$ θέτοντας

$$\alpha/\beta + \gamma/\delta = (\alpha\delta + \beta\gamma)/\beta\delta \quad \text{και} \quad (\alpha/\beta)(\gamma/\delta) = \alpha\gamma/\beta\delta.$$

Πρώτα από όλα πρέπει να δείξουμε ότι οι αντιστοιχίες αυτές είναι απεικονίσεις. Για το σκοπό αυτό, έστω $\alpha/\beta = \alpha'/\beta'$ και $\gamma/\delta = \gamma'/\delta'$, δηλαδή $\alpha\beta' = \beta\alpha'$ και $\gamma\delta' = \delta\gamma'$. Τότε έχουμε

$$\begin{aligned}(\alpha\delta + \beta\gamma)\beta'\delta' &= \alpha\delta\beta'\delta' + \beta\gamma\beta'\delta' = (\alpha\beta')\delta\delta' + (\gamma\delta')\beta\beta' \\ &= (\alpha'\beta)\delta\delta' + (\delta\gamma')\beta\beta' = (\alpha'\delta' + \beta'\gamma')\beta\delta.\end{aligned}$$

Συνεπώς, $(\alpha\delta+\beta\gamma)/\beta\delta = (\alpha'\delta'+\beta'\gamma')/\beta'\delta'$, δηλάδή $\alpha/\beta+\gamma/\delta = \alpha'/\beta'+\gamma'/\delta'$, που σημαίνει ότι η $+ : F \times F \to F$ είναι απεικόνιση. Με παρόμοιο τρόπο δείχνει κανείς ότι και η $\cdot : F \times F \to F$ είναι απεικόνιση. Η επαλήθευση των ιδιοτήτων στον ορισμό του σώματος είναι θέμα ρουτίνας. Ενδεικτικά, ας δούμε τον επιμεριστικό νόμο. Έστω $\alpha/\beta, \gamma/\delta, \epsilon/\zeta \in F$. Τότε αφενός

$$\alpha/\beta(\gamma/\delta + \epsilon/\zeta) = (\alpha(\gamma\zeta + \delta\epsilon))/\beta\delta\zeta = (\alpha\gamma\zeta + \alpha\delta\epsilon)/\beta\delta\zeta$$

και αφετέρου

$$(\alpha/\beta)(\gamma/\delta) + (\alpha/\beta)(\epsilon/\zeta) = (\alpha\gamma)/(\beta\delta) + (\alpha\epsilon)/(\beta\zeta) = (\alpha\gamma\beta\zeta + \beta\delta\alpha\epsilon)/(\beta^2\delta\zeta).$$

Τα δεξιά μέλη είναι ίσα γιατί $(\alpha\gamma\zeta + \alpha\delta\epsilon)(\beta^2\delta\zeta) = \beta\delta\zeta(\alpha\gamma\beta\zeta + \beta\delta\alpha\epsilon)$.

Το μηδενικό στοιχείο του F είναι το $0_R/1_R$. Το αντίθετο του α/β είναι το $(-\alpha)/\beta$. Το μοναδιαίο στοιχείο του F είναι το $1_R/1_R$ και αν το α/β είναι μη μηδενικό, τότε το αντίστροφό του είναι το β/α.

Θα αποδείξουμε τώρα ότι το σώμα F περιέχει έναν δακτύλιο ισόμορφο με τον R. Η απεικόνιση $i : R \to F$, $\alpha \mapsto \alpha/1_R$, είναι ένας ομομορφισμός δακτυλίων γιατί στο F ισχύει $(\alpha + \beta)/1_F = \alpha/1_F + \beta/1_F$ και $(\alpha\beta)/1_F = (\alpha/1_F)(\beta/1_F)$. Ο πυρήνας της i είναι τετριμμένος, γιατί αν $\alpha/1_F = 0_R/1_R$, τότε $\alpha = 0_R$. Άρα έχουμε $R \cong \mathrm{Im}i$.

Το σώμα F που κατασκευάσαμε από την ακεραία περιοχή R ονομάζεται το σώμα πηλίκων της R και ο μονομορφισμός δακτυλίων $i : R \to F$, $\alpha \mapsto \alpha/1_R$, ονομάζεται η φυσική εμφύτευση του R στο F.

Παραδείγματα

1. Το σώμα πηλίκων των ακεραίων του Gauss $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} | a, b \in \mathbb{Z}\}$ είναι ισόμορφο με το $\mathbb{Q}[i] = \{a + bi \in \mathbb{C} | a, b \in \mathbb{Q}\}$. Πράγματι, έστω F το σώμα πηλίκων του $\mathbb{Z}[i]$. Τότε εύκολα αποδεικνύεται ότι η απεικόνιση $F \to \mathbb{Q}[i]$, $\alpha/\beta \to \alpha\beta^{-1}$, είναι ένας ισομορφισμός δακτυλίων.

2. Το σώμα πηλίκων της ακεραίας περιοχής
$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} | a, b \in \mathbb{Z}\}$ είναι ισόμορφο με το
$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} | a, b \in \mathbb{Q}\}$

3. Έστω F ένα σώμα. Τότε το σώμα πηλίκων του πολυωνυμικού δακτυλίου $F[x]$ είναι το $\{f(x)/g(x) | f(x), g(x) \in F[x], g(x) \neq 0\}$. Το σώμα πηλίκων του $F[x]$ συνήθως συμβολίζεται με $F(x)$.

Είναι φανερό ότι κάθε υπόσωμα του $\mathbb{C}$ περιέχει το $\mathbb{Z}$ και άρα περιέχει το $\mathbb{Q}$. Η επόμενη Πρόταση μας πληροφορεί ότι αν ένα σώμα περιέχει έναν υποδακτύλιο R που είναι ακεραία περιοχή, τότε θα "περιέχει" και το σώμα πηλίκων της R.

2.7.1 Πρόταση. *Έστω $\varphi : R \to E$ ένας μονομορφισμός δακτυλίων, όπου ο R είναι ακεραία περιοχή και ο E είναι σώμα. Τότε υπάρχει ένας μονομορφισμός $\psi : F \to E$, όπου F είναι το σώμα πηλίκων της R, για τον οποίο ισχύει $\psi \circ i = \varphi$, όπου $i : R \to F$ είναι η φυσική εμφύτευση.*

Απόδειξη. Ορίζουμε $\psi(\alpha/\beta) = \varphi(\alpha)\varphi(\beta)^{-1}$. Η επαλήθευση ότι ο ψ είναι ένας μονομορφισμός δακτυλίων είναι θέμα ρουτίνας που αφήνεται σαν άσκηση. Για κάθε $\alpha \in R$ έχουμε $(\psi \circ i)(\alpha) = \psi(\alpha/1_R) = \varphi(\alpha)\varphi(1_R)^{-1}$. Έχουμε $\varphi(1_R) = 1_S$ και άρα $(\psi \circ i)(\alpha) = \varphi(\alpha)$. ⊤

Χαρακτηριστική δακτυλίου

Σε ένα δακτύλιο R είναι δυνατόν να ισχύει $mr = 0$, όπου m είναι ένας μη μηδενικός ακέραιος και r ένα μη μηδενικό στοιχείο του R. Ακόμα περισσότερο, έχουμε δει ότι είναι δυνατόν να υπάρχει μη μηδενικός ακέραιος m τέτοιος ώστε για κάθε $r \in R$ να ισχύει $mr = 0$.

2.7.2 Ορισμός. *Έστω R ένας δακτύλιος.*

- *Αν δεν υπάρχει θετικός ακέραιος m τέτοιος ώστε $mr = 0$ για κάθε $r \in R$, θα λέμε ότι η χαρακτηριστική του R είναι μηδέν.*
- *Αν υπάρχει θετικός ακέραιος m τέτοιος ώστε $mr = 0$ για κάθε $r \in R$, θα λέμε ότι η χαρακτηριστική του R είναι ο ελάχιστος τέτοιος m.*

Για παράδειγμα, οι δακτύλιοι $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ έχουν χαρακτηριστική μηδέν. Ο $\mathbb{Z}_m$, $m > 0$, έχει χαρακτηριστική m. Ο $\mathbb{Z}_m \times \mathbb{Z}_n$, όπου $m, n > 0$, έχει χαρακτηριστική το $\epsilon\kappa\pi(m, n)$. Η χαρακτηριστική του δακτυλίου R συμβολίζεται με $\chi\alpha\rho R$.

2.7.3 Παρατήρηση. Αν ο δακτύλιος R έχει μοναδιαίο στοιχείο, τότε στον ορισμό της χαρακτηριστικής αρκεί να εξετάσει κανείς πότε ισχύει $m1_R = 0$. Ακριβέστερα: Αν δεν υπάρχει θετικός ακέραιος m με την ιδιότητα $m1_R = 0$,

τότε $\chi\alpha\rho R = 0$, ενώ αν υπάρχει θετικός ακέραιος m με την ιδιότητα $m1_R = 0$, τότε η $\chi\alpha\rho R$ ισούται με τον ελάχιστο τέτοιο m. Πράγματι, στην πρώτη περίπτωση προκύπτει άμεσα από τον ορισμό ότι $\chi\alpha\rho R = 0$. Για την άλλη περίπτωση, έστω ότι υπάρχει θετικός ακέραιος m με την ιδιότητα $m1_R = 0$. Θεωρούμε τον ελάχιστο τέτοιο m. Τότε για κάθε $r \in R$, έχουμε $mr = m(1_R r) = (m1_R)r = 0r = 0$ και κατά συνέπεια $\chi\alpha\rho R \leq m$. Επειδή όμως ισχύει $(\chi\alpha\rho R)1_R = 0$, το ελάχιστο του m δίνει $m \leq \chi\alpha\rho R$. Άρα $m = \chi\alpha\rho R$.

Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Τότε το σύνολο

$$S_R = \{n1_R \in R | n \in \mathbb{Z}\}$$

είναι ένας υποδακτύλιος του R και μάλιστα είναι ο μικρότερος υποδακτύλιος που περιέχει το 1_R (Άσκηση 2.1.4). Η επόμενη πρόταση μας πληροφορεί ότι η χαρακτηριστική του R "προσδιορίζει" το S_R.

2.7.4 Πρόταση. *Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο και $< m >$ ο πυρήνας του ομομορφισμού δακτυλίων*

$$\varphi : \mathbb{Z} \to R,\ \varphi(n) = n1_R.$$

Τότε υπάρχει ένας ισομορφισμός δακτυλίων $S_R \cong \mathbb{Z}_m$. Επιπλέον έχουμε $\chi\alpha\rho R = m$.

Απόδειξη. Επειδή ο $\ker\varphi$ είναι ένα ιδεώδες του $\mathbb{Z}$, αυτός θα είναι της μορφής $< m >$ για κάποιο $m \in \mathbb{N}$. Είναι φανερό ότι $\mathrm{Im}\varphi = S_R$, οπότε από το Θεώρημα 2.6.6 έχουμε $\mathbb{Z}/ < m > \cong S_R$. Συνεπώς $\mathbb{Z}_m \cong \mathbb{Z}/ < m > \cong S_R$. Θα δείξουμε τώρα ότι $\chi\alpha\rho R = m$. Πρώτα παρατηρούμε ότι από τη σχέση $m1_R = 0$ έπεται ότι $\chi\alpha\rho R \leq m$ σύμφωνα με την Παρατήρηση 2.7.3. Επίσης έχουμε $\chi\alpha\rho R \in \ker\varphi$ από τον ορισμό της χαρακτηριστικής, δηλαδή $\chi\alpha\rho R \in < m >$ και άρα $\chi\alpha\rho R \geq m$. Συνεπώς $\chi\alpha\rho R = m$. ⊤

2.7.5 Πόρισμα. *Η χαρακτηριστική μιας ακεραίας περιοχής είναι 0 ή ένας πρώτος αριθμός.*

Απόδειξη. Έστω R μια ακεραία περιοχή χαρακτηριστικής m. Από την προηγούμενη Πρόταση, βλέπουμε ότι ο R περιέχει έναν υποδακτύλιο ισόμορφο με το $\mathbb{Z}_m$. Επειδή ο R δεν έχει μηδενοδιαιρέτες, ο $\mathbb{Z}_m$ δεν έχει μηδενοδιαιρέτες. Από την Πρόταση 2.1.4 συμπεραίνουμε ότι ο m είναι 0 ή πρώτος. ⊤

2.7.6 Πόρισμα. *Έστω R μια ακεραία περιοχή. Τότε ο μικρότερος υποδακτύλιος του R που περιέχει το 1_R είναι ισόμορφος είτε με το $\mathbb{Z}$ (αν $\chi\alpha\rho R = 0$) είτε με το σώμα $\mathbb{Z}_p$ (αν $\chi\alpha\rho R = p > 0$).*

Απόδειξη. Το Πόρισμα έπεται άμεσα από την Πρόταση 2.7.4 και το Πόρισμα 2.7.5. ⊺

Ας θεωρήσουμε τώρα την περίπτωση που ο δακτύλιος R είναι σώμα, έστω F. Από το προηγούμενο Πόρισμα, έχουμε ότι $\chi\alpha\rho F = 0$ ή p (p πρώτος).

Έστω ότι $\chi\alpha\rho F = 0$. Τότε το F περιέχει έναν υποδακτύλιο ισόμορφο με τον $\mathbb{Z}$. Από την Πρόταση 2.7.1 έπεται ότι το F περιέχει ένα υπόσωμα ισόμορφο με το $\mathbb{Q}$. Έστω ότι $\chi\alpha\rho F = p$ (p πρώτος). Τότε το F περιέχει ένα υπόσωμα ισόμορφο με το $\mathbb{Z}_p$.

Η τομή όλων των υποσωμάτων του F είναι ένα υπόσωμα του F. Το υπόσωμα αυτό ονομάζεται το πρώτο υπόσωμα του F. Υπενθυμίζουμε ότι το $\mathbb{Q}$ δεν περιέχει γνήσιο υπόσωμα. Άρα το πρώτο υπόσωμα του $\mathbb{Q}$ είναι το $\mathbb{Q}$. Όμοια, το πρώτο υπόσωμα του $\mathbb{Z}_p$ είναι το $\mathbb{Z}_p$.

2.7.7 Πρόταση. *Έστω F ένα σώμα και F' το πρώτο υπόσωμα του F. Αν $\chi\alpha\rho F = 0$, τότε $F' \cong \mathbb{Q}$, ενώ αν $\chi\alpha\rho F = p$ (p πρώτος), τότε $F' \cong \mathbb{Z}_p$.*

Απόδειξη. Έστω ότι $\chi\alpha\rho F = 0$. Τότε το F περιέχει ένα υπόσωμα ισόμορφο με το $\mathbb{Q}$ και το F' είναι ισόμορφο με υπόσωμα του $\mathbb{Q}$. Επειδή το $\mathbb{Q}$ δεν περιέχει γνήσιο υπόσωμα, έχουμε $F' \cong \mathbb{Q}$. Η απόδειξη στην περίπτωση που $\chi\alpha\rho F = p$ (p πρώτος) είναι παρόμοια. ⊺

Ασκήσεις 2.7

1. Αποδείξτε ότι το σώμα πηλίκων ενός σώματος F είναι ισόμορφο με το F.

2. Αποδείξτε ότι το σώμα πηλίκων του $\mathbb{Z}[\sqrt{3}]$ είναι ισόμορφο με το $\mathbb{Q}[\sqrt{3}]$.

3. Αποδείξτε ότι ισόμορφοι δακτύλιοι έχουν ίσες χαρακτηριστικές. Αποδείξτε ότι ισόμορφες ακέραιες περιοχές έχουν ισόμορφα σώματα πηλίκων. Δώστε ένα παράδειγμα μη ισόμορφων ακεραίων περιοχών που έχουν ισόμορφα σώματα πηλίκων.

4. Έστω R ένας μεταθετικός δακτύλιος με $\chi\alpha\rho R = 4$. Αποδείξτε ότι για κάθε $a, b \in R$ έχουμε $(a+b)^4 = (a^2+b^2)^2$ και γενικά $(a+b)^{2^{n+1}} = (a^{2^n}+b^{2^n})^2$ για κάθε $n \in \mathbb{N}$.

5. Έστω a, b στοιχεία μιας ακεραίας περιοχής R. Αν $a^n = b^n$ και $a^m = b^m$ για κάποια $m, n \in \mathbb{Z}$ με $\mu\kappa\delta(m, n) = 1$, τότε δείξτε ότι $a = b$.

6. Ποια είναι η χαρακτηριστική των δακτυλίων $M_2(\mathbb{Z}_m)$, $M_2(\mathbb{Z})$ και $\mathbb{Z}_3 \times \mathbb{Q}[x]$;

7. Έστω $F \to E$ ένας μονομορφισμός σωμάτων. Αποδείξτε ότι χαρF =χαρE.

8. Αποδείξτε ότι χαρR =χαρF, όπου F είναι το σώμα πηλίκων της ακεραίας περιοχής R.

9. Έστω S ένας μη τετριμμένος υποδακτύλιος του δακτυλίου R.

   a. Αληθεύει ότι χαρS =χαρR;

   b. Αν ο S είναι ακεραία περιοχή, αληθεύει ότι χαρS =χαρR;

   c. Έστω ότι ο R είναι μια ακεραία περιοχή. Αποδείξτε ότι χαρS =χαρR.

10. Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο τέτοιος ώστε χαρ$R = mn$, $\mu\kappa\delta(m, n) = 1$. Αποδείξτε ότι υπάρχουν υποδακτύλιοι R_1, R_2 του R τέτοιοι ώστε $R \cong R_1 \times R_2$, χαρ$R_1 = m$, χαρ$R_2 = n$.
Υπόδειξη: Εφαρμόστε την Άσκηση 2.6.20 για κατάλληλα ιδεώδη του R.

11. Δώστε ένα παράδειγμα

    a. άπειρου σώματος που έχει θετική χαρακτηριστική

    b. δακτυλίου που έχει χαρακτηριστική πρώτο αριθμό και δεν είναι ακεραία περιοχή.

12. Ποιές είναι οι χαρακτηριστικές των παρακάτω δακτυλίων;

    i) $\mathbb{Z}[i]/ < 3 >$

    ii) $\mathbb{Z}[i]/ < 2 + i >$

    iii) $\mathbb{Z}_6[x]/ < 2 >$.

2.8 Πεπερασμένα Σώματα

Σε παραδείγματα της Παραγράφου 2.6 είδαμε ότι πηλίκα του πολυωνυμικού δακτυλίου $\mathbb{Z}_p[x]$ με ιδεώδη της μορφής $< f(x) >$, όπου το $f(x)$ είναι ανάγωγο, είναι σώματα και μάλιστα πεπερασμένα. Για κάθε πρώτο p και κάθε θετικό ακέραιο k θα αποδείξουμε την ύπαρξη ενός σώματος που έχει p^k στοιχεία. Στη συνέχεια θα ταξινομήσουμε τα υποσώματα των πεπερασμένων σωμάτων. Τέλος θα μελετήσουμε μια εφαρμογή στη συνδυαστική.

Πεπερασμένα σώματα

Έστω F ένα πεπερασμένο σώμα. Η απεικόνιση

$$\varphi : \mathbb{Z} \ni m \mapsto m1_F \in F$$

είναι ένας μη τετριμμένος ομομορφισμός δακτυλίων. Έστω $I = \ker \varphi$. Επειδή το F είναι πεπερασμένο, το I είναι μη μηδενικό. Από το 1^o Θεώρημα Ισομορφισμών λαμβάνουμε έναν μονομορφισμό $\mathbb{Z}/I \to F$. Άρα ο δακτύλιος $\mathbb{Z}/I$ είναι μια ακεραία περιοχή. Ως ιδεώδες του $\mathbb{Z}$, το I είναι της μορφής $I =< p >$ για κάποιο $p \in \mathbb{N}$. Αφού το I είναι μη μηδενικό, έχουμε $p \neq 0$, και επειδή ο $\mathbb{Z}/I$ είναι ακεραία περιοχή έχουμε ότι ο p είναι πρώτος. Επομένως έχουμε έναν μονομορφισμό σωμάτων

$$\psi : \mathbb{Z}_p \to F.$$

Από την Παρατήρηση 2.7.3 έπεται ότι η χαρακτηριστική του F είναι p. Θεωρούμε το F ως έναν $\mathbb{Z}_p$ - διανυσματικό χώρο: η πρόσθεση των στοιχείων του F είναι η πρόσθεση του σώματος F και ο πολλαπλασιασμός στοιχείων του F με στοιχεία του $\mathbb{Z}_p$ δίδεται από την απεικόνιση $\mathbb{Z}_p \times F \to F$ που στέλνει το (α, x) στο $\psi(\alpha)x$, όπου $\alpha \in \mathbb{Z}_p$, $x \in F$. Η επαλήθευση των ιδιοτήτων του ορισμού του διανυσματικού χώρου είναι πολύ εύκολη και παραλείπεται.

Στη συνέχεια θα ταυτίζουμε το σώμα $\mathbb{Z}_p$ με την εικόνα του, $\psi(\mathbb{Z}_p)$. Συνεπώς θα γράφουμε αx στη θέση του $\psi(\alpha)x$. Η διάσταση του F ως $\mathbb{Z}_p$ - διανυσματικός χώρος είναι πεπερασμένη, γιατί το F είναι ένα πεπερασμένο σύνολο. Έστω $\{x_1, \ldots, x_k\}$ μια βάση του. Κάθε στοιχείο του F γράφεται κατά μοναδικό τρόπο στη μορφή $\alpha_1 x_1 + \cdots + \alpha_k x_k$, όπου $\alpha_i \in \mathbb{Z}_p$. Επειδή το $\mathbb{Z}_p$ έχει p στοιχεία βλέπουμε ότι το πλήθος των στοιχείων της μορφής $\alpha_1 x_1 + \cdots + \alpha_k x_k$ είναι p^k. Επομένως έχουμε το εξής αποτέλεσμα:

2.8.1 Θεώρημα. *Έστω F ένα πεπερασμένο σώμα. Τότε για κάποιο θετικό ακέραιο k έχουμε $|F| = p^k$, όπου ο πρώτος p είναι η χαρακτηριστική του F.*

Στη συνέχεια θα αποδείξουμε ότι για κάθε πρώτο p και κάθε θετικό ακέραιο k υπάρχει σώμα που έχει p^k στοιχεία. Τα βασικά βήματα της απόδειξης που θα δώσουμε είναι τα εξής.

1) Υπάρχει ένα σώμα E που περιέχει το $\mathbb{Z}_p$ και είναι τέτοιο ώστε το πολυώνυμο $x^{p^k} - x \in E[x]$ να έχει p^k ρίζες στο E.

2) Οι ρίζες του $x^{p^k} - x$ στο E είναι διακεκριμένες.

3) Το σύνολο των ριζών του $x^{p^k} - x$ στο E είναι ένα σώμα.

Για το 1) θα αποδείξουμε κάτι γενικότερο (που ισχύει για τυχαίο σώμα - όχι αναγκαστικά πεπερασμένο - και τυχαίο πολυώνυμο θετικού βαθμού).

Αν υπάρχει μονομορφισμός σωμάτων $\varphi : F \to E$, θα λέμε ότι το E είναι μια ***επέκταση*** του F. Στην περίπτωση αυτή, είναι φανερό ότι το E περιέχει υπόσωμα, το $\varphi(F)$, που είναι ισόμορφο με το F. Συχνά θα ταυτίζουμε τα $\varphi(F)$, F. Για παράδειγμα, το $\mathbb{C}$ είναι μια επέκταση του $\mathbb{R}$, το $\mathbb{C}$ είναι επέκταση του $\mathbb{Q}[x]/ < x^2 + 1 >$, και το $\mathbb{Q}[x]/ < x^2 + 1 >$ είναι επέκταση του $\mathbb{Q}$. Κάθε πεπερασμένο σώμα που αποτελείται από p^k στοιχεία είναι επέκταση του $\mathbb{Z}_p$, όπως είδαμε πριν.

Αν $\varphi : F \to E$ είναι ένας ομομορφισμός σωμάτων, μπορούμε να ορίσουμε έναν ομομορφισμό δακτυλίων

$$\tilde{\varphi} : F[x] \to E[x],\ a_n x^n + \cdots + a_0 \mapsto \varphi(a_n)x^n + \cdots + \varphi(a_0),$$

για τον οποίο ισχύει $\tilde{\varphi}(a) = \varphi(a)$ για κάθε $a \in F$. (Βλ. την Εφαρμογή μετά την Πρόταση 2.5.3). Στην περίπτωση που ο φ είναι μονομορφισμός, θα ταυτίζουμε συχνά ένα $f(x) \in F[x]$ με την εικόνα του στο $E[x]$. Μπορούμε τότε να θεωρήσουμε ότι $F[x] \subseteq E[x]$.

2.8.2 Θεώρημα. *Έστω F ένα σώμα (όχι αναγκαστικά πεπερασμένο) και $f(x) \in F[x]$ με $\deg f(x) \geq 1$. Τότε υπάρχει επέκταση E του F τέτοια ώστε το $f(x)$ έχει τουλάχιστον μία ρίζα στο E.*

Απόδειξη. Έστω $p(x)$ ένας ανάγωγος παράγοντας του $f(x)$. Από το Θεώρημα 2.6.3, το πηλίκο $E = F[x]/ < p(x) >$ είναι ένα σώμα. Θα δείξουμε ότι το E είναι μια επέκταση του F που περιέχει τουλάχιστον μία ρίζα του $f(x)$. Εύκολα επαληθεύεται ότι η απεικόνιση

$$\psi : F \ni a \mapsto a + < p(x) > \in E$$

είναι ένας μονομορφισμός σωμάτων. Μία ρίζα του πολυωνύμου $\tilde{\psi}(f(x))$ είναι το $x + < p(x) >$. Πράγματι, συμβολίζοντας για συντομία το ιδεώδες $< p(x) >$ του $F[x]$ με I, έχουμε: Αν $f(x) = a_n x^n + \cdots + a_0$, τότε

$$\tilde{\psi}(f(x)) = (a_n + I)x^n + \cdots + (a_1 + I)x + (a_0 + I)$$

και χρησιμοποιώντας πράξεις στο πηλίκο $F[x]/I$ έχουμε

$$\begin{aligned}
&(a_n + I)(x + I)^n + \cdots + (a_1 + I)(x + I) + (a_0 + I) = \\
&(a_n + I)(x^n + I) + \cdots + (a_1 + I)(x + I) + (a_0 + I) = \\
&(a_n x^n + I) + \cdots + (a_1 x + I) + (a_0 + I) = \\
&f(x) + I = I = 0_E.
\end{aligned}$$

Η προτελευταία ισότητα ισχύει γιατί το $p(x)$ διαιρεί το $f(x)$. ⊤

2.8.3 Παραδείγματα.

1. Έστω $F = \mathbb{R}$ και $f(x) = x^2 + 1$. Το $f(x)$ είναι ανάγωγο επί του $\mathbb{R}$. Μια επέκταση του $\mathbb{R}$ όπου το $f(x)$ έχει ρίζα, είναι, σύμφωνα με το προηγούμενο Θεώρημα, το σώμα $\mathbb{R}[x]/ < x^2 + 1 >$. Πράγματι, αν συμβολίσουμε με ρ την εικόνα του x στο $\mathbb{R}[x]/ < x^2 + 1 >$ κάτω από τον φυσικό επιμορφισμό $\mathbb{R}[x] \ni g(x) \mapsto g(x) + < x^2 + 1 > \in \mathbb{R}[x]/ < x^2 + 1 >$, έχουμε $\rho^2 + 1 = 0$.

2. Έστω $F = \mathbb{Z}_2$ και $f(x) = x^2 + x + 1$. Το $f(x)$ είναι ανάγωγο επί του $\mathbb{Z}_2$. Μία επέκταση του $\mathbb{Z}_2$ όπου το $f(x)$ έχει ρίζα είναι η $E = \mathbb{Z}_2[x]/ < x^2 + x + 1 >$. Αν ρ είναι η εικόνα του x στο $\mathbb{Z}_2[x]/ < x^2 + x + 1 >$, έχουμε $\rho^2 + \rho + 1 = 0$.

3. Έστω $F = \mathbb{Z}_2$ και $f(x) = (x^2 + x + 1)g(x)$, $g(x) \in F[x]$. Μία επέκταση του $\mathbb{Z}_2$ όπου το $f(x)$ έχει ρίζα είναι η $E = \mathbb{Z}_2[x]/ < x^2 + x + 1 >$.

2.8.4 Σημείωση. Έστω E μια επέκταση του $\mathbb{Z}_p$. Επισημαίνουμε ότι $pa = 0$ για κάθε $a \in E$. Πράγματι, $pa = (p1_E)a = (p1_{\mathbb{Z}_p})a = 0a = 0$.

Είδαμε ότι δεδομένου ενός $f(x) \in F[x]$ υπάρχει επέκταση E όπου το $f(x)$ έχει τουλάχιστον μια ρίζα. Συνεπώς στο $E[x]$ έχουμε μια παραγοντοποίηση της μορφής $f(x) = (x - \rho)g(x)$, όπου $\rho \in F$, $g(x) \in E[x]$ (Θεώρημα 2.4.1).

Θα λέμε ότι ένα πολυώνυμο $f(x) \in E[x]$ **διασπάται** στο E αν υπάρχει μια παραγοντοποίηση της μορφής $f(x) = c(x-\rho_1)(x-\rho_2)\dots(x-\rho_n)$, $c, \rho_1, \dots, \rho_n \in E$. Για παράδειγμα, το $x^2 - 2$ δεν διασπάται στο $\mathbb{Q}$, αλλά διασπάται στο $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$. Από το Θεμελιώδες Θεώρημα της Άλγεβρας κάθε $f(x) \in \mathbb{C}[x]$ διασπάται στο $\mathbb{C}$.

2.8.5 Πόρισμα. *Έστω $f(x) \in F[x]$, όπου το F είναι ένα σώμα (όχι απαραίτητα πεπερασμένο) και* $\deg f(x) \geq 1$. *Τότε υπάρχει μία επέκταση E του F όπου το $f(x)$ διασπάται.*

Απόδειξη. Χρησιμοποιούμε επαγωγή στο $n = \deg f(x)$. Αν $n = 1$, τότε $f(x) = a_1x + a_0$, $a_1 \neq 0$, και το $f(x)$ έχει μία ρίζα στο F, δηλαδή αυτό διασπάται στο F. Έστω τώρα $n > 1$. Σύμφωνα με το προηγούμενο Θεώρημα υπάρχει μια επέκταση E_1 όπου το $f(x)$ έχει τουλάχιστον μία ρίζα. Συνεπώς $f(x) = (x - \rho)g(x)$, όπου $\rho \in E_1$, $g(x) \in E_1[x]$. Έχουμε $\deg g(x) = n - 1$ και από την υπόθεση της επαγωγής υπάρχει επέκταση E του E_1 όπου το $g(x)$ διασπάται. Αφού το E περιέχει και το ρ, το $f(x)$ διασπάται στο E. ⊤

Σχόλιο

Όταν το $f(x)$ διασπάται στο E, λέμε συχνά - και μάλλον καταχρηστικά - ότι το E "περιέχει όλες τις ρίζες" του $f(x)$. Οι ρίζες ενός $f(x)$ δεν είναι μονοσήμαντα ορισμένες αλλά εξαρτώνται από την επέκταση που τις περιέχει. Για παράδειγμα, το $x^2 + 1$ έχει δύο ριζες στο $\mathbb{C}$ και δύο άλλες ρίζες στο $\mathbb{R}[x]/ < x^2 + 1 >$. Ένα πολυώνυμο $f(x) \in F[x]$ μπορεί να έχει ρίζες σε διαφορετικές επεκτάσεις του F. Αν ένα $f(x)$ διασπάται στο E, τότε στο E περιέχονται $\deg f(x)$ ρίζες του $f(x)$. Το πλήθος αυτό είναι το μέγιστο πλήθος ριζών του $f(x)$ που είναι δυνατόν να περιέχει ένα σώμα (Πόρισμα 2.4.2). Έτσι δικαιολογείται η χρήση της παραπάνω έκφρασης.

Επιστρέφουμε τώρα στην συγκεκριμένη περίπτωση που μας ενδιαφέρει. Από το προηγούμενο Πόρισμα γνωρίζουμε ότι υπάρχει επέκταση E του $\mathbb{Z}_p$ όπου το πολυώνυμο $x^{p^k} - x$ διασπάται. Θα δείξουμε τώρα ότι οι ρίζες αυτού του πολυωνύμου στο E είναι διακεκριμένες. Για τον σκοπό αυτό, θα χρειαστούμε την έννοια της παραγώγου πολυωνύμου. Επειδή δεν έχουμε (τουλάχιστον κατά προφανή τρόπο) την έννοια του ορίου σε τυχαίο σώμα θα δώσουμε ένα αλγεβρικό ορισμό.

Έστω F ένα σώμα. Η ***παράγωγός*** του

$$f(x) = a_nx^n + \cdots + a_1x + a_0 \in F[x]$$

είναι το

$$f(x)' = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 \in F[x].$$

Η επαλήθευση των γνώριμων κανόνων παραγώγισης,

$$(af(x) + bg(x))' = af(x)' + bg(x)',$$
$$(f(x)g(x))' = f(x)'g(x) + f(x)g(x)',$$

για κάθε $a, b \in F$, $f(x), g(x) \in F[x]$, αφήνεται σαν άσκηση.

Μια ρίζα $\rho \in F$ ενός $f(x) \in F[x]$ ονομάζεται ***επαναλαμβανόμενη*** (ή ***πολλαπλή***) αν $(x - \rho)^2 | f(x)$. Μια ρίζα του $f(x)$ που δεν είναι επαναλαμβανόμενη λέγεται ***απλή***. Έχουμε το ακόλουθο απλό, αλλά χρήσιμο κριτήριο.

2.8.6 Λήμμα. *Έστω F ένα σώμα και $f(x) \in F[x]$. Τότε μια ρίζα ρ του $f(x)$ στο F είναι απλή αν και μόνο αν $f(\rho)' \neq 0$.*

Απόδειξη. Έχουμε

$$f(x) = (x-\rho)g(x),\ g(x) \in F[x], \quad \text{και} \quad f(x)' = g(x) + (x-\rho)g(x)'.$$

Αν η ρ είναι απλή, τότε από την πρώτη ισότητα παίρνουμε ότι το $x-\rho$ δεν διαιρεί το $g(x)$, δηλαδή $g(\rho) \neq 0$. Από την δεύτερη ισότητα έχουμε $f(\rho)' = g(\rho) \neq 0$.

Αντίστροφα, αν $f(\rho)' \neq 0$, τότε $g(\rho) \neq 0$ και άρα το $x-\rho$ δεν διαιρεί το $g(x)$, οπότε το $(x-\rho)^2$ δεν διαιρεί το $f(x)$. ⊤

2.8.7 Πόρισμα. *Έστω E μια επέκταση του $\mathbb{Z}_p$. Έστω ότι το πολυώνυμο $x^{p^k} - x$ διασπάται στο E, όπου $k > 0$. Τότε οι p^k ρίζες του $x^{p^k} - x$ στο E είναι διακεκριμένες.*

Απόδειξη. Έχουμε $(x^{p^k} - x)' = p^k x^{p^k - 1} - 1 = -1$. Το ζητούμενο προκύπτει άμεσα από το προηγούμενο Λήμμα. ⊤

2.8.8 Θεώρημα (Ύπαρξη πεπερασμένων σωμάτων). *Για κάθε πρώτο p και κάθε θετικό ακέραιο k υπάρχει σώμα F τέτοιο ώστε $|F| = p^k$.*

Απόδειξη. Έστω E μια επέκταση του $\mathbb{Z}_p$, όπου το $x^{p^k} - x$ διασπάται (Πόρισμα 2.8.5). Έστω F το υποσύνολο του E που αποτελείται από τις ρίζες του $x^{p^k} - x$. Από το Πόρισμα 2.8.7, έχουμε ότι $|F| = p^k$. Θα δείξουμε ότι το F είναι ένα σώμα. Για τον σκοπό αυτό αρκεί να αποδείξουμε ότι το F είναι υποδακτύλιος του E και κάθε μη μηδενικό στοιχείο του είναι αντιστρέψιμο, δηλαδή, ότι για κάθε $\alpha, \beta \in F$ έχουμε $\alpha - \beta \in F$, $\alpha\beta \in F$, και αν $\alpha \neq 0$, τότε $\alpha^{-1} \in F$.

Έστω $\alpha, \beta \in F$, οπότε $\alpha^{p^k} = \alpha$, $\beta^{p^k} = \beta$. Από τη Σημείωση 2.8.4, έχουμε $pa = 0$ για κάθε $a \in E$, οπότε από το Παράδειγμα 2.1.12 2) παίρνουμε

$$(\alpha - \beta)^{p^k} = \alpha^{p^k} - \beta^{p^k} = \alpha - \beta$$

Επίσης έχουμε

$$(\alpha\beta)^{p^k} = \alpha^{p^k}\beta^{p^k} = \alpha\beta, \quad \text{και}$$
$$(\alpha^{-1})^{p^k} = (\alpha^{p^k})^{-1} = a^{-1}. \quad ⊤$$

Στην πράξη, για να κατασκευάσουμε ένα σώμα που έχει p^k στοιχεία, συνήθως βρίσκουμε ένα ανάγωγο πολυώνυμο $f(x) \in \mathbb{Z}_p[x]$ βαθμού k (αυτό δεν

είναι πάντα εύκολο) και σχηματίζουμε το πηλίκο $\mathbb{Z}_p[x]/ < f(x) >$. Παραδείγματα της κατασκευής αυτής είδαμε στην Παράγραφο 2.6. Επομένως ένα σώμα που έχει 8 στοιχεία είναι το $\mathbb{Z}_2[x]/ < x^3 + x + 1 >$ και ένα άλλο είναι το $\mathbb{Z}_2[x]/ < x^3 + x^2 + 1 >$. Ποιά είναι η σχέση αυτών των δύο σωμάτων; Υπάρχει ένα Θεώρημα σύμφωνα με το οποίο κάθε δύο πεπερασμένα σώματα με το ίδιο πλήθος στοιχείων είναι ισόμορφα. Η απόδειξη, ενώ δεν είναι δύσκολη, είναι κάπως μακροσκελής γιατί απαιτούνται μερικά στοιχεία από τη Θεωρία Σωμάτων στα οποία δεν έχουμε αναφερθεί. Επειδή το Θεώρημα αυτό δεν θα χρησιμοποιηθεί παρακάτω θα παραλείψουμε την απόδειξη.

Στην απόδειξη του Θεωρήματος 2.8.8 κατασκευάσαμε ένα σώμα που έχει p^k στοιχεία ως ένα σύνολο ριζών του $x^{p^k} - x \in \mathbb{Z}_p[x]$. Μπορούμε να δείξουμε ότι τα στοιχεία κάθε σώματος F με $|F| = p^k$ είναι ρίζες του $x^{p^k} - x$. Η τεχνική της απόδειξης είναι παρόμοια με αυτή που είδαμε στο Θεώρημα του Euler στην Ενότητα 1 (Βλ. Θεώρημα 1.6.2): Έστω

$$F^* = \{a_1, \ldots, a_n\}$$

το σύνολο των μη μηδενικών στοιχείων πεπερασμένου σώματος F, όπου $|F| = p^k$ και $n = p^k - 1$. Αν $a \in \{a_1, \ldots, a_n\}$, τότε από το νόμο της διαγραφής του πολλαπλασιασμού συμπεραίνουμε ότι

$$\{a_1, \ldots, a_n\} = \{aa_1, \ldots, aa_n\}.$$

Πολλαπλασιάζοντας παίρνουμε

$$a_1 \ldots a_n = a^n a_1 \ldots a_n$$

οπότε πάλι από το νόμο της διαγραφής έχουμε

$$a^n = 1. \tag{1}$$

Αυτό σημαίνει ότι κάθε μη μηδενικό στοιχείο είναι ρίζα του $x^{p^k-1} - 1$. Επομένως έχουμε αποδείξει το εξής αποτέλεσμα.

2.8.9 Πρόταση. *Έστω F ένα πεπερασμένο σώμα με $|F| = p^k$. Τότε κάθε στοιχείο του F είναι ρίζα του $x^{p^k} - x$.*

Σημείωση Παρατηρούμε ότι στην απόδειξη της παραπάνω Πρότασης χρησιμοποιήσαμε μόνο ιδιότητες του πολλαπλασιασμού του σώματος. Οι "ομάδες" είναι θεμελιώδη αλγεβρικά συστήματα που έχουν μία μόνο πράξη. Αυτές μελετώνται στην Ενότητα 4. Η ισότητα (1) που μόλις αποδείξαμε, έπεται και από το "Θεώρημα του Lagrange" στις ομάδες.

Υποσώματα πεπερασμένων σωμάτων
Έστω E ένα πεπερασμένο σώμα με $|E| = p^k$. Θα ταξινομήσουμε τα υποσώματα του E. Σύμφωνα με το επόμενο αποτέλεσμα, για κάθε θετικό διαιρέτη r του k υπάρχει μοναδικό υπόσωμα του E που έχει p^r στοιχεία. Πέρα από αυτά δεν υπάρχουν άλλα υποσώματα του E.

2.8.10 Θεώρημα. *Έστω E ένα πεπερασμένο σώμα με $|E| = p^k$. Τότε*

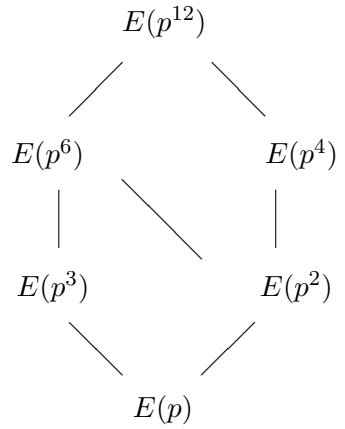
1. *Κάθε υπόσωμα του E έχει p^r στοιχεία, όπου $r|k$.*
2. *Για κάθε θετικό διαιρέτη r του k υπάρχει μοναδικό υπόσωμα του E που έχει p^r στοιχεία.*

Απόδειξη. 1. Έστω F ένα υπόσωμα του E που αποτελείται από m στοιχεία. Μπορούμε να θεωρήσουμε το E ως έναν διανυσματικό χώρο υπεράνω του F. Αν $n = \dim_F E$, τότε με έναν συλλογισμό παρόμοιο με αυτόν που είδαμε πριν από το Θεώρημα 2.8.1 συμπεραίνουμε ότι $p^k = m^n$. Από τη μοναδικότητα της παραγοντοποίησης ακεραίων παίρνουμε $m = p^r$, για κάποιο r, και κατά συνέπεια $p^k = p^{rn}$, δηλαδή $r|k$. Συνεπώς το πλήθος των στοιχείων του F είναι p^r, όπου $r|k$.
2. Έστω r ένας διαιρέτης του k. Τότε ο $p^r - 1$ διαιρεί τον $p^k - 1$ επειδή, αν $k = rs$, έχουμε

$$p^k - 1 = (p^r - 1)((p^r)^{s-1} + \cdots + p^r + 1).$$

Επομένως το πολυώνυμο $x^{p^r-1} - 1$ διαιρεί το $x^{p^k-1} - 1$ στο $\mathbb{Z}_p[x]$ και άρα το $x^{p^r} - x$ διαιρεί το $x^{p^k} - x$. Από την Πρόταση 2.8.9, τα στοιχεία του E είναι ρίζες του $x^{p^k} - x$. Έστω F το υποσύνολο του E που αποτελείται από τις ρίζες του $x^{p^r} - x$. Τότε το F είναι ένα σώμα και $|F| = p^r$ (σύμφωνα με την απόδειξη του Θεωρήματος 2.8.8). Έχουμε αποδείξει ότι κάθε υπόσωμα του E έχει p^r στοιχεία, όπου το r διαιρεί το k. Από την Πρόταση 2.8.9 και το Πόρισμα 2.4.2 προκύπτει ότι δεν είναι δυνατό να υπάρχουν δύο διαφορετικά υποσώματα του E που έχουν p^r στοιχεία. ⊺

2.8.11 Παράδειγμα. Έστω E ένα σώμα με p^{12} στοιχεία, p πρώτος. Μπορούμε να παραστήσουμε τα υποσώματα του E με το παρακάτω διάγραμμα. Με $E(p^r)$, όπου $r|12$, συμβολίζουμε το μοναδικό υπόσωμα του E που έχει p^r στοιχεία.



Εφαρμογή: Λατινικά τετράγωνα
Θα εξετάσουμε εδώ μια εφαρμογή των πεπερασμένων σωμάτων στον σχεδιασμό πειραμάτων.

Πρόβλημα. Ένας γεωπόνος θέλει να μελετήσει την επίδραση τριών διαφορετικών ειδών λιπάσματος σε τρεις διαφορετικές ποικιλίες σιταριού. Επιθυμεί δε να εντοπίσει το συνδυασμό λιπάσματος - σιταριού που έχει τη μέγιστη απόδοση. Με ποιό τρόπο μπορεί να σχεδιάσει ένα πείραμα που θα πραγματοποιηθεί σε ένα χωράφι και θα δίνει απάντηση στο ερώτημα αυτό;

Είναι σαφές ότι θα πρέπει να χωριστεί το χωράφι σε $3 \times 3 = 9$ τμήματα ώστε κάθε μια από τις ποικιλίες σιταριού να καλλιεργηθεί με τη βοήθεια καθενός από τα είδη λιπάσματος. Όμως για να είναι το πείραμα όσο γίνεται αξιόπιστο, θα πρέπει να ελαχιστοποιηθεί η επίδραση που μπορεί να έχει το γεγονός ότι κάποια σημεία του χωραφιού είναι πιο γόνιμα από τα υπόλοιπα. Για το λόγο αυτό, ο γεωπόνος αποφασίζει να χωρίσει το χωράφι σε τρεις γραμμές και τρεις στήλες ώστε κάθε είδος σιταριού να καλλιεργηθεί ακριβώς μια φορά σε κάθε γραμμή και στήλη και όμοια κάθε είδος λιπάσματος να χρησιμοποιηθεί ακριβώς μία φορά σε κάθε γραμμή και στήλη. Είναι αυτό δυνατό; Όπως θα δούμε στη συνέχεια, η λύση του προβλήματος αυτού ισοδυναμεί με την ύπαρξη δύο 3×3 "ορθογωνίων Λατινικών τετραγώνων".

Ορισμός *Ένα $n \times n$* ***Λατινικό τετράγωνο*** *είναι ενας $n \times n$ πίνακας με στοιχεία από ένα σύνολο $\{a_1, \ldots, a_n\}$ που έχει την ιδιότητα ότι σε κάθε γραμμή και κάθε στήλη το a_i εμφανίζεται ακριβώς μία φορά, $i = 1, \ldots, n$.*

Συνήθως χρησιμοποιούμε το σύνολο $\{1, 2, \ldots, n\}$ στη θέση του $\{a_1, \ldots, a_n\}$.

Για παράδειγμα, τα

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$$

είναι Λατινικά τετράγωνα, ενώ το

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

δεν είναι. Από τον νόμο της διαγραφής, έπεται ότι ο πίνακας της πρόσθεσης κάθε πεπερασμένου δακτυλίου είναι ένα Λατινικό τετράγωνο, όπως και ο πίνακας πολλαπλασιασμού των μη μηδενικών στοιχείων κάθε πεπερασμένου σώματος.

Ορισμός *Δύο $n \times n$ Λατινικά τετράγωνα $A = (a_{ij})$, $B = (b_{ij})$ ονομάζονται* ***ορθογώνια*** *αν τα διατεταγμένα ζεύγη (a_{ij}, b_{ij}), $i, j = 1, \ldots, n$, είναι διακεκριμένα, ή ισοδύναμα αν $\{(a_{ij}, b_{ij}) | i, j = 1, \ldots, n\} = \{1, \ldots, n\} \times \{1, \ldots, n\}$. Ένα σύνολο $\{A_1, \ldots, A_m\}$ $n \times n$ Λατινικών τετραγώνων ονομάζεται* ***ορθογώνιο*** *αν τα A_i, A_j είναι ορθογώνια για κάθε $i \neq j$.*

Για παράδειγμα, τα A, B που είδαμε πριν είναι ορθογώνια. Τα

$$\begin{pmatrix} 3 & 2 & 1 \\ 2 & 1 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix}$$

δεν είναι ορθογώνια αφού $(a_{12}, b_{12}) = (a_{21}, b_{21}) = (2, 3)$.

Τα ορθογώνια Λατινικά τετράγωνα A, B που είδαμε πριν λύνουν το πρόβλημά μας. Σχηματίζουμε τον πίνακα

$$C = \begin{pmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{pmatrix}$$

όπου στην i γραμμή και j στήλη του πίνακα C υπάρχει το διατεταγμένο ζεύγος (a_{ij}, b_{ij}). Τα ζεύγη αυτά περιγράφουν τον τρόπο που μπορεί να πραγματοποιηθεί το πείραμα: αν η πρώτη συντεταγμένη παριστάνει την ποικιλία σιταριού και η δεύτερη το είδος λιπάσματος, τότε γνωρίζουμε σε ποιο σημείο του χωραφιού θα καλλιεργηθεί κάθε ποικιλία και ποιο λίπασμα θα χρησιμοποιήσουμε.

Σημειώσεις

1) Η λύση του προβλήματος για $n = 3$, δηλαδή η εύρεση δύο 3×3 ορθογωνίων

Λατινικών τετραγώνων, ήταν εύκολη. Μετά από κάποιες δοκιμές με 3×3 πίνακες, δεν υπάρχει αμφιβολία ότι θα βρίσκαμε τα συγκεκριμένα A, B. Όμως η συνδυαστική πολυπλοκότητα του προβλήματος αυξάνει ραγδαία με το n.
2) Ο Euler μελέτησε το 1782 ένα πρόβλημα ισοδύναμο με την εύρεση δύο 6×6 ορθογωνίων Λατινικών τετραγώνων, που όμως δεν μπόρεσε να λύσει. Πολύ αργότερα (το 1901) αποδείχτηκε ότι δεν υπάρχουν δύο 6×6 ορθογώνια Λατινικά τετράγωνα. Σήμερα είναι γνωστό ότι για κάθε $n \geq 3$, εκτός από $n = 6$, υπάρχουν τουλάχιστον δύο $n \times n$ ορθογώνια Λατινικά τετράγωνα (βλ. [22]).

Μπορεί να αποδειχτεί σχετικά εύκολα ότι ο πληθάριθμος κάθε ορθογωνίου συνόλου $n \times n$ Λατινικών τετραγώνων είναι το πολύ $n - 1$ (Άσκηση 7). Το επόμενο αποτέλεσμα παρέχει για κάθε n της μορφής $n = p^r$, p πρώτος, ένα ορθογώνιο σύνολο $n \times n$ Λατινικών τετραγώνων που έχει $n - 1$ στοιχεία.

Ένα ανοικτό ερώτημα είναι η εύρεση όλων των n τέτοιων ώστε υπάρχει ένα ορθογώνιο σύνολο $n \times n$ Λατινικών τετραγώνων που έχει $n - 1$ στοιχεία. Ακόμα και πιο ειδικά ερωτήματα είναι δύσκολα. Για παράδειγμα, παραμένει ανοικτό το ερώτημα της εύρεσης του μέγιστου πλήθους 10×10 ορθογωνίων Λατινικών τετραγώνων. Ένα ζεύγος 10×10 ορθογωνίων Λατινικών τετραγώνων κατασκευάστηκε για πρώτη φορά μόλις το 1958.

2.8.12 Θεώρημα. *Για κάθε n της μορφής $n = p^k$, p πρώτος, υπάρχει ορθογώνιο σύνολο $n \times n$ Λατινικών τετραγώνων που έχει $n - 1$ στοιχεία.*

Απόδειξη. Έστω $n = p^k$, p πρώτος. Έστω F ένα σώμα με $|F| = n$ (γνωρίζουμε ότι υπάρχει τέτοιο σώμα από το Θεώρημα 2.8.8),

$$F = \{a_1 = 1, a_2, \ldots, a_{n-1}, a_n = 0\}$$

Για κάθε $r = 1, 2, \ldots, n-1$ ορίζουμε τον πίνακα $A_r \in M_n(F)$,

$$A_r = (a_{ij}^{(r)}), \quad \text{όπου} \quad a_{ij}^{(r)} = a_r a_i + a_j.$$

Παρατηρούμε ότι

$$a_{ij}^{(r)} = a_{il}^{(r)} \Rightarrow a_r a_i + a_j = a_r a_i + a_l \Rightarrow a_j = a_l$$

και κατά συνέπεια κάθε γραμμή περιέχει κάθε στοιχείο του F ακριβώς μία φορά. Για τις στήλες έχουμε

$$a_{ij}^{(r)} = a_{lj}^{(r)} \Rightarrow a_r a_i + a_j = a_r a_l + a_j \Rightarrow a_r a_i = a_r a_l \Rightarrow a_i = a_l,$$

αφού $a_r \neq 0$ $(r \neq n)$. Συνεπώς κάθε A_r είναι Λατινικό τετράγωνο. Για να δείξουμε ότι αυτά είναι ανά δύο ορθογώνια έστω ότι $(a_{ij}^{(r)}, a_{ij}^{(s)}) = (a_{uv}^{(r)}, a_{uv}^{(s)})$ με

$r \neq s$. Τότε

$$a_r a_i + a_j = a_r a_u + a_\nu$$
$$a_s a_i + a_j = a_s a_u + a_\nu.$$

Αφαιρώντας παίρνουμε $(a_r - a_s)a_i = (a_r - a_s)a_u$ και επειδή $a_r - a_s \neq 0$ έχουμε $a_i = a_u$, δηλαδή $i = u$. Αντικαθιστώντας στην πρώτη εξίσωση βλέπουμε ότι $a_j = a_\nu$, δηλαδή $j = \nu$. ⊤

Παράδειγμα
Θα κατασκευάσουμε εδώ τρία 4×4 ορθογώνια Λατινικά τετράγωνα. Για το σκοπό αυτό θα χρησιμοποιήσουμε το σώμα F των 4 στοιχείων που κατασκευάσαμε στο Παράδειγμα 2.6.2 4). Υπενθυμίζουμε ότι $F = \{a_1 = 1, a_2 = a, a_3 = a + 1, a_4 = 0\}$. Σύμφωνα με την απόδειξη του Θεωρήματος 2.7.12 το πρώτο Λατινικό τετράγωνο έχει στη θέση (i, j) το στοιχείο $a_i + a_j$. Με τη βοήθεια των πινάκων των πράξεων του Παραδείγματος 2.6.2 4), βρίσκουμε

$$A_1 = \begin{pmatrix} a_4 & a_3 & a_2 & a_1 \\ a_3 & a_4 & a_1 & a_2 \\ a_2 & a_1 & a_4 & a_3 \\ a_1 & a_2 & a_3 & a_4 \end{pmatrix}$$

Συνεχίζοντας λαμβάνουμε

$$A_2 = \begin{pmatrix} a_3 & a_4 & a_1 & a_2 \\ a_2 & a_1 & a_4 & a_3 \\ a_4 & a_3 & a_2 & a_1 \\ a_1 & a_2 & a_3 & a_4 \end{pmatrix}.$$

$$A_3 = \begin{pmatrix} a_2 & a_1 & a_4 & a_3 \\ a_4 & a_3 & a_2 & a_1 \\ a_3 & a_4 & a_1 & a_2 \\ a_1 & a_2 & a_3 & a_4 \end{pmatrix}.$$

Αναφέρουμε πληροφοριακά, ότι το πρόβλημα του προσδιορισμού των $n \geq 3$ για τους οποίους υπάρχει ένα ορθογώνιο σύνολο $n \times n$ Λατινικών τετραγώνων που έχει $n-1$ στοιχεία είναι ισοδύναμο με ένα πρόβλημα της Προβολικής Γεωμετρίας, αυτό της ύπαρξης "προβολικού επιπέδου τάξης n" (βλ. [26]). Τα προβλήματα αυτά παραμένουν μέχρι σήμερα ανοικτά.

Ασκήσεις 2.8

1. Έστω F ένα πεπερασμένο σώμα. Αποδείξτε ότι δεν είναι δυνατό να υπάρχουν δύο υποσώματα F_1, F_2 του F τέτοια ώστε $F_1 \cong \mathbb{Z}_5$, $F_2 \cong \mathbb{Z}_7$.

2. Θεωρούμε το σώμα $F = \mathbb{Z}_2[x]/ < x^3 + x + 1 >$. Συμβολίζουμε με α την εικόνα του x στο F. Αποδείξτε ότι κάθε υπόσωμα του F που περιέχει το α^2 ταυτίζεται με το F.

3. Κατασκευάστε ένα σώμα που έχει 25 στοιχεία και ένα άλλο που έχει 27 στοιχεία.

4. Έστω ρ μια ρίζα του x^2+1 στο σώμα $\mathbb{Z}_3[x]/ < x^2+1 >$. Κατασκευάστε ένα πολυώνυμο στο $\mathbb{Z}_3[x]$ δευτέρου βαθμού που έχει ρίζες τις $2\rho + 1$ και $\rho + 1$.

5. Ποιο είναι το διάγραμμα υποσωμάτων ενός σώματος που έχει p^{36} στοιχεία (p πρώτος);

6. Έστω F ένα πεπερασμένο σώμα χαρακτηριστικής p. Αποδείξτε ότι η απεικόνιση
$$\varphi : F \to F,\ a \mapsto a^p$$
είναι ένας ισομορφισμός και ότι $\varphi(a) = a$ για κάθε $a \in \mathbb{Z}_p$.

7. Κάθε ορθογώνιο σύνολο $n \times n$ Λατινικών τετραγώνων περιέχει το πολύ $n-1$ στοιχεία.
Υπόδειξη: Αλλάζουμε τη θέση των στηλών κάθε Λατινικού τετραγώνου του συνόλου ώστε η πρώτη γραμμή να είναι η $123\ldots n$. Το νέο σύνολο παραμένει ορθογώνιο. Μετρήστε τώρα τις δυνατότητες για το στοιχείο στη θέση $(2,1)$.

8. Κατασκευάστε ένα ζεύγος ορθογωνίων 7×7 Λατινικών τετραγώνων.

9. Κατασκευάστε ένα ζεύγος ορθογωνίων 8×8 Λατινικών τετραγώνων.

2.9 Επεκτάσεις Σωμάτων και Γεωμετρικές Κατασκευές

Στην Παράγραφο αυτή θα δούμε πώς μπορούμε να χρησιμοποιήσουμε μερικά βασικά αποτελέσματα από τη θεωρία των σωμάτων για να δείξουμε ότι ορισμένα κλασικά προβλήματα της Ευκλείδειας Γεωμετρίας δεν έχουν λύση. Πιο συγκεκριμένα, θεωρούμε τα παρακάτω προβλήματα:

1. Να κατασκευαστεί με κανόνα και διαβήτη η ακμή ενός κύβου με όγκο διπλάσιο του όγκου ενός δοθέντος κύβου (***διπλασιασμός του κύβου***).

2. Να τριχοτομηθεί με κανόνα και διαβήτη μια δεδομένη γωνία (***τριχοτόμηση γωνίας***).

3. Να κατασκευαστεί με κανόνα και διαβήτη ένα κανονικό πολύγωνο με n πλευρές (***κατασκευή κανονικού n-γώνου***).

4. Να κατασκευαστεί με κανόνα και διαβήτη η πλευρά ενός τετραγώνου με εμβαδόν ίσο με αυτό ενός δεδομένου κύκλου (***τετραγωνισμός του κύκλου***).

Τα παραπάνω προβλήματα απασχόλησαν τους μαθηματικούς επί αιώνες, από την εποχή του Ευκλείδη μέχρι το 19ο αιώνα, οπότε αποδείχτηκε ότι αυτά είναι άλυτα. Για να δείξουμε το άλυτο των προβλημάτων αυτών, θα ορίσουμε αυστηρά τι σημαίνει ***κατασκευή με κανόνα και διαβήτη*** και θα περιγράψουμε αλγεβρικά το σύνολο των σημείων που κατασκευάζονται με τον τρόπο αυτό. Τότε, θα δούμε ότι τα ζητούμενα συμπεράσματα προκύπτουν από ορισμένες βασικές ιδιότητες των επεκτάσεων σωμάτων.

Επεκτάσεις σωμάτων και αλγεβρικοί αριθμοί.

Έστω F ένα σώμα και $E \subseteq F$ ένα υπόσωμά του. Χρησιμοποιώντας τον πολλαπλασιασμό του σώματος F, μπορούμε να ορίσουμε σ΄ αυτό τη δομή ενός E-διανυσματικού χώρου. Η διάσταση $\dim_E F$ του διανυσματικού αυτού χώρου ονομάζεται ***βαθμός της επέκτασης*** $E \subseteq F$ και συμβολίζεται με $[F : E]$. Η επέκταση $E \subseteq F$ λέγεται πεπερασμένης διαστάσεως αν ο βαθμός $[F : E]$ είναι πεπερασμένος.

2.9.1 Παραδείγματα.

1) Για την επέκταση $\mathbb{R} \subseteq \mathbb{C}$ έχουμε $[\mathbb{C} : \mathbb{R}] = \dim_{\mathbb{R}} \mathbb{C} = 2$. Χρησιμοποιώντας την αριθμησιμότητα του σώματος $\mathbb{Q}$ των ρητών αριθμών, έπεται εύκολα ότι κάθε $\mathbb{Q}$-διανυσματικός χώρος πεπερασμένης διαστάσεως είναι αριθμήσιμο σύνολο. Καθώς το σώμα $\mathbb{R}$ είναι υπεραριθμήσιμο, βλέπουμε ότι ο βαθμός $[\mathbb{R} : \mathbb{Q}]$ είναι άπειρος.

2) Έστω E ένα πεπερασμένο σώμα με p^n στοιχεία, για κάποιον πρώτο αριθμό

p και κάποιο θετικό ακέραιο n. Τότε, όπως έχουμε δει στην προηγούμενη Παράγραφο, το E είναι μια επέκταση του $\mathbb{Z}_p$ βαθμού n.

Η επόμενη απλή ιδιότητα του βαθμού μιας επέκτασης θα αποδειχτεί πολύ χρήσιμη στη συνέχεια.

2.9.2 Πρόταση. *Θεωρούμε δύο διαδοχικές επεκτάσεις σωμάτων $E \subseteq F \subseteq K$. Τότε, ο βαθμός $[K : E]$ είναι πεπερασμένος αν και μόνο αν και οι δύο βαθμοί $[K : F]$ και $[F : E]$ είναι πεπερασμένοι. Μάλιστα, στην περίπτωση αυτή, έχουμε $[K : E] = [K : F] \cdot [F : E]$.*

Απόδειξη. Ας υποθέσουμε ότι $[K : E] < \infty$, δηλαδή ότι ο K είναι πεπερασμένης διαστάσεως E-διανυσματικός χώρος. Τότε, υπάρχουν πεπερασμένα το πλήθος στοιχεία $v_1, \ldots, v_n$ του K, που είναι τέτοια ώστε κάθε $v \in K$ γράφεται ως γραμμικός συνδυασμός των v_i με συντελεστές από το E. Καθώς $E \subseteq F$, έπεται ότι τα στοιχεία $v_1, \ldots, v_n$ παράγουν τον F-διανυσματικό χώρο K και άρα $[K : F] = \dim_F K \leq n < \infty$. Είναι γνωστό από τη Γραμμική Άλγεβρα ότι κάθε υπόχωρος του E-διανυσματικού χώρου K είναι επίσης πεπερασμένης διαστάσεως. Ειδικότερα, για τον υπόχωρο F του K ισχύει $[F : E] = \dim_E F < \infty$.

Αντίστροφα, ας υποθέσουμε ότι οι βαθμοί $[F : E] = a$ και $[K : F] = b$ είναι πεπερασμένοι. Θεωρούμε μια βάση $w_1, \ldots, w_a$ (αντιστ. $u_1, \ldots, u_b$) του E-διανυσματικού χώρου F (αντιστ. του F-διανυσματικού χώρου K). Θα δείξουμε ότι το σύνολο

$$B = \{w_i u_j : 1 \leq i \leq a, \ \ 1 \leq j \leq b\},$$

το οποίο έχει ab το πλήθος στοιχεία, αποτελεί μια βάση του E-διανυσματικού χώρου K. Κατ' αρχήν, παρατηρούμε ότι κάθε στοιχείο $v \in K$ είναι της μορφής $\sum_{j=1}^{b} \lambda_j u_j$ για κατάλληλα $\lambda_j \in F$. Γράφοντας $\lambda_j = \sum_{i=1}^{a} \mu_{ij} w_i$ για κατάλληλα $\mu_{ij} \in E$, έπεται ότι $v = \sum_{i,j} \mu_{ij} w_i u_j$ και άρα το B παράγει τον E-διανυσματικό χώρο K. Για να δείξουμε τη γραμμική ανεξαρτησία του B πάνω από το E, ας υποθέσουμε ότι $\sum_{i,j} \nu_{ij} w_i u_j = 0 \in K$ για κάποια $\nu_{ij} \in E$. Τότε, χρησιμοποιώντας τη γραμμική ανεξαρτησία των u_j πάνω από το F, έπεται ότι $\sum_i \nu_{ij} w_i = 0 \in F$ για κάθε $j = 1, \ldots, b$. Χρησιμοποιώντας τέλος τη γραμμική ανεξαρτησία των w_i πάνω από το E, έπεται ότι $\nu_{ij} = 0 \in E$ για κάθε i, j. ⊤

Θα εστιάσουμε την προσοχή μας σε σώματα E, τα οποία είναι υποσώματα του σώματος $\mathbb{C}$ των μιγαδικών αριθμών. Γνωρίζουμε ότι κάθε τέτοιο σώμα E είναι μια επέκταση του σώματος $\mathbb{Q}$ των ρητών αριθμών (βλέπε την παράγραφο πριν απο την Πρόταση 2.7.1).

Έπεται άμεσα από τους ορισμούς ότι η τομή κάθε συλλογής υποδακτυλίων (αντιστ. υποσωμάτων) του σώματος $\mathbb{C}$ είναι ένας υποδακτύλιος (αντιστ. υπόσωμα) του $\mathbb{C}$. Ειδικότερα, αν E είναι ένα υπόσωμα του $\mathbb{C}$ και S ένα σύνολο

μιγαδικών αριθμών, μπορούμε να θεωρήσουμε τον ελάχιστο υποδακτύλιο $E[S]$ που περιέχει το σύνολο $E \cup S$, δηλαδή την τομή όλων των υποδακτυλίων του $\mathbb{C}$ που περιέχουν το $E \cup S$, καθώς και το ελάχιστο υπόσωμα $E(S)$ που περιέχει το σύνολο $E \cup S$, δηλαδή την τομή όλων των υποσωμάτων του $\mathbb{C}$ που περιέχουν το $E \cup S$. Θα λέμε ότι ο δακτύλιος $E[S]$ (αντιστ. το σώμα $E(S)$) παράγεται από το E και το S (αντιστ. είναι η επέκταση του E που παράγεται από το S). Είναι φανερό ότι αν $S = \emptyset$, τότε $E[S] = E(S) = E$.

2.9.3 Πρόταση. *Θεωρούμε ένα υπόσωμα E του σώματος $\mathbb{C}$ και ένα μη-κενό σύνολο μιγαδικών αριθμών S.*

(i) Ο δακτύλιος $E[S]$ που παράγεται από το E και το S αποτελείται από τα στοιχεία $f(z_1, \ldots, z_n) \in \mathbb{C}$, όπου $n \geq 1$, $f(x_1, \ldots, x_n) \in E[x_1, \ldots, x_n]$ είναι ένα πολυώνυμο n μεταβλητών με συντελεστές από το E (βλέπε τον ορισμό στο τέλος της Παραγράφου 2.2) και $z_1, \ldots, z_n \in S$.

(ii) Η επέκταση $E(S)$ του E που παράγεται από το S είναι το σώμα των πηλίκων της ακεραίας περιοχής $E[S] \subseteq \mathbb{C}$.

Απόδειξη. (i) Είναι φανερό ότι το σύνολο R που αποτελείται από τα αναφερόμενα στοιχεία είναι ένας υποδακτύλιος του σώματος των μιγαδικών αριθμών, ο οποίος περιέχει το E και το S. Ας θεωρήσουμε έναν άλλο υποδακτύλιο R' του $\mathbb{C}$ που περιέχει το E και το S. Τότε, $f(z_1, \ldots, z_n) \in R'$ για κάθε πολυώνυμο $f(x_1, \ldots, x_n) \in E[x_1, \ldots, x_n]$ και κάθε επιλογή $z_1, \ldots, z_n \in S$. Συνεπώς, θα έχουμε $R \subseteq R'$ και άρα ο R είναι πράγματι ο ελάχιστος υποδακτύλιος του $\mathbb{C}$ που περιέχει το E και το S. Με άλλα λόγια, αυτό σημαίνει ότι $R = E[S]$.

(ii) Το σώμα των πηλίκων K της ακεραίας περιοχής $E[S]$ είναι μια επέκταση του E που περιέχει το S. Αν F είναι ένα άλλο υπόσωμα του $\mathbb{C}$ που περιέχει το E και το S, τότε το F (ως ένας υποδακτύλιος του $\mathbb{C}$ που περιέχει το E και το S) περιέχει την ακεραία περιοχή $E[S]$. Τότε όμως το F (ως σώμα) περιέχει όλα τα στοιχεία της μορφής a/b, με $a, b \in E[S]$ και $b \neq 0$, και άρα $K \subseteq F$. Συμπεραίνουμε λοιπόν ότι το K είναι το ελάχιστο υπόσωμα του $\mathbb{C}$ που περιέχει το E και το S, δηλαδή $K = E(S)$. ⊺

Αν E είναι ένα υπόσωμα του $\mathbb{C}$ και $S = \{z_1, \ldots, z_n\}$, τότε θα γράφουμε $E[S] = E[z_1, \ldots, z_n]$ και $E(S) = E(z_1, \ldots, z_n)$. Είναι φανερό ότι ο δακτύλιος $E[z_1, \ldots, z_n]$ είναι η εικόνα του ομομορφισμού

$$\phi : E[x_1, \ldots, x_n] \longrightarrow \mathbb{C},$$

ο οποίος αντιστοιχεί σε κάθε πολυώνυμο $f(x_1, \ldots, x_n) \in E[x_1, \ldots, x_n]$ την τιμή του $f(z_1, \ldots, z_n) \in \mathbb{C}$.

2.9.4 Ορισμός. *Έστω E ένα υπόσωμα του $\mathbb{C}$ και z ένας μιγαδικός αριθμός. Ο z λέγεται* **αλγεβρικός** *υπεράνω του E αν υπάρχει μη-μηδενικό πολυώνυμο $f(x) \in E[x]$, τέτοιο ώστε $f(z) = 0$. Αν δεν υπάρχει τέτοιο μη-μηδενικό πολυώνυμο, τότε ο z λέγεται* **υπερβατικός** *υπεράνω του E.*

Στην ειδική περίπτωση όπου $E = \mathbb{Q}$, μιλάμε απλά για αλγεβρικούς και υπερβατικούς αριθμούς.

2.9.5 Παραδείγματα.

1) Το $i \in \mathbb{C}$ είναι αλγεβρικό (υπεράνω του $\mathbb{Q}$), αφού είναι ρίζα του πολυωνύμου $x^2 + 1 \in \mathbb{Q}[x]$.

2) Ο αριθμός $\pi = 3.14159\ldots$ είναι υπερβατικός. Η απόδειξη του αποτελέσματος αυτού, το οποίο δείχτηκε πρώτα από τον F. Lindemann το 1882, δεν είναι απλή και ξεφεύγει από τους σκοπούς του παρόντος βιβλίου. Για μια απόδειξη, παραπέμπουμε στον I. Stewart [28].

Ας θεωρήσουμε ένα υπόσωμα E του $\mathbb{C}$ και ένα μιγαδικό αριθμό z, ο οποίος είναι υπερβατικός υπεράνω του E. Τότε, τα στοιχεία $1, z, z^2, \ldots$ του E-διανυσματικού χώρου $\mathbb{C}$ είναι γραμμικά ανεξάρτητα. Θεωρούμε τον ομομορφισμό δακτυλίων

$$\phi : E[x] \longrightarrow \mathbb{C},$$

με $\phi(f(x)) = f(z)$ για κάθε πολυώνυμο $f(x) \in E[x]$, ο οποίος είναι 1-1 και έχει εικόνα το δακτύλιο $E[z]$ που παράγεται από το E και το z. Από την Πρόταση 2.7.1, έπεται ότι ο ϕ επεκτείνεται σε ένα μονομορφισμό

$$\psi : E(x) \longrightarrow \mathbb{C},$$

όπου $E(x)$ είναι το σώμα των πηλίκων του πολυωνυμικού δακτυλίου $E[x]$ (βλέπε το Παράδειγμα 3, πριν από την Πρόταση 2.7.1). Από την Πρόταση 2.9.3 (ii) έπεται ότι η εικόνα $Im\,\psi$ του ψ είναι ακριβώς η επέκταση $E(z)$ του E που παράγεται από το z. Καθώς τα στοιχεία $1, z, z^2, \ldots$ του E-διανυσματικού χώρου $E(z)$ είναι γραμμικά ανεξάρτητα, έπεται ότι ο βαθμός $[E(z) : E]$ είναι άπειρος.

Ας υποθέσουμε τώρα ότι ο μιγαδικός αριθμός z είναι αλγεβρικός υπεράνω του E. Τότε, ο ομομορφισμός ϕ που ορίστηκε παραπάνω δεν είναι 1-1. Πράγματι, από τον ορισμό, υπάρχει ένα μη-μηδενικό πολυώνυμο που ανήκει στον πυρήνα $ker\,\phi$ του ϕ. Καθώς κάθε ιδεώδες του δακτυλίου πολυωνύμων $E[x]$ είναι κύριο (Άσκηση 2.5.11 (i)), υπάρχει ένα μοναδικό μονικό πολυώνυμο $f(x) \in E[x]$, τέτοιο ώστε $ker\,\phi =< f(x) >$. Το πολυώνυμο $f(x) \in E[x]$ είναι το μονικό

πολυώνυμο με τον ελάχιστο βαθμό που έχει ρίζα το z και καλείται το ***ελάχιστο πολυώνυμο*** του z υπεράνω του σώματος E. Επιπλέον, κάθε άλλο πολυώνυμο $g(x) \in E[x]$ που έχει ρίζα το z είναι πολλαπλάσιο του $f(x)$.

Η εικόνα του ομομορφισμού ϕ ισούται, και στην περίπτωση αυτή, με το δακτύλιο $E[z]$ που παράγεται από το E και το z. Συνεπώς, σύμφωνα με το πρώτο θεώρημα των ισομορφισμών δακτυλίων (Θεώρημα 2.6.6), ο δακτύλιος πηλίκο $E[x]/<f(x)>$ είναι ισόμορφος με την ακεραία περιοχή $E[z] \subseteq \mathbb{C}$. Από το Θεώρημα 2.6.3 έπεται ότι το πολυώνυμο $f(x) \in E[x]$ είναι ανάγωγο. Τότε όμως, το ίδιο θεώρημα μας λέει ότι ο δακτύλιος πηλίκο $E[x]/<f(x)>$ είναι σώμα. Συνεπώς, η ακεραία περιοχή $E[z]$ είναι επίσης σώμα και άρα ισούται με το σώμα $E(z)$ των πηλίκων της, δηλαδή $E[z] = E(z)$.

Θεωρώντας τα σώματα $E[x]$ και $\mathbb{C}$ ως διανυσματικούς χώρους υπεράνω του E, η απεικόνιση ϕ είναι προφανώς γραμμική. Έτσι, ο ισομορφισμός των δακτυλίων $E[x]/<f(x)> \simeq E[z]$, ο οποίος κατασκευάστηκε στην απόδειξη του Θεωρήματος 2.6.6, είναι επιπλέον ένας ισομορφισμός E-διανυσματικών χώρων. Καθώς η διάσταση του E-διανυσματικού χώρου $E[x]/<f(x)>$ είναι ίση με το βαθμό του πολυωνύμου $f(x)$ (γιατί;), συμπεραίνουμε ότι για το βαθμό της επέκτασης $E(z) = E[z]$ του E ισχύει $[E(z) : E] = \deg f(x)$.

Διατυπώνουμε τα παραπάνω συμπεράσματα με τη μορφή ενός θεωρήματος:

2.9.6 Θεώρημα. *Έστω E ένα υπόσωμα του $\mathbb{C}$ και z ένας μιγαδικός αριθμός. Τότε, ο z είναι αλγεβρικός υπεράνω του E αν και μόνο αν η επέκταση $E \subseteq E(z)$ είναι πεπερασμένης διαστάσεως. Στην περίπτωση αυτή, έχουμε $E(z) = E[z]$, ενώ ο βαθμός $[E(z) : E]$ είναι ίσος με το βαθμό του ελάχιστου πολυωνύμου του z υπεράνω του E.*

2.9.7 Παραδείγματα.

1) Έστω E ένα υπόσωμα του $\mathbb{C}$ και $a \in E$ ένα στοιχείο του, τέτοιο ώστε οι τετραγωνικές ρίζες $\pm\sqrt{a} \in \mathbb{C}$ δεν ανήκουν στο E. Τότε, το στοιχείο $\sqrt{a}$ είναι αλγεβρικό υπεράνω του E με ελάχιστο πολυώνυμο $x^2 - a \in E[x]$. Συνεπώς, η επέκταση $E \subseteq E[\sqrt{a}] = E(\sqrt{a})$ είναι βαθμού 2.

2) Έστω $a = \sqrt{2}+i$. Θα δείξουμε ότι ο μιγαδικός αριθμός a είναι αλγεβρικός και θα προσδιορίσουμε το ελάχιστο πολυώνυμό του.
Πράγματι, έχουμε $a^2 = 1 + 2\sqrt{2}i$ και άρα $(a^2 - 1)^2 = -8$. Συνεπώς, $a^4 - 2a^2 + 9 = 0$ και άρα το a είναι αλγεβρικό με ελάχιστο πολυώνυμο ένα διαιρέτη του $f(x) = x^4 - 2x^2 + 9 \in \mathbb{Q}[x]$. Θα δείξουμε ότι το $f(x)$ είναι ανάγωγο και άρα ισούται με το ελάχιστο πολυώνυμο του a. Για το σκοπό αυτό, αρκεί να δείξουμε ότι $[\mathbb{Q}(a) : \mathbb{Q}] = 4$. Καθώς $a^3 = -\sqrt{2}+5i$, έχουμε $i = \frac{1}{6}(a + a^3)$ και $\sqrt{2} = \frac{1}{6}(5a - a^3)$. Έτσι, $\mathbb{Q}[a] = \mathbb{Q}[i, \sqrt{2}]$ και

άρα η ζητούμενη σχέση έπεται άμεσα, εφαρμόζοντας την Πρόταση 2.9.2 για τις διαδοχικές επεκτάσεις

$$\mathbb{Q} \subseteq \mathbb{Q}[i] \subseteq (\mathbb{Q}[i])[\sqrt{2}] = \mathbb{Q}[i, \sqrt{2}],$$

με βάση το 1) παραπάνω.

3) Για κάθε μιγαδικό αριθμό z ο βαθμός της επέκτασης $\mathbb{Q}(\sqrt{z}) \subseteq \mathbb{Q}(z)$ είναι 1 ή 2 (βλέπε 1) παραπάνω). Συνεπώς, εφαρμόζοντας την Πρόταση 2.9.2 για τις διαδοχικές επεκτάσεις

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{z}) \subseteq \mathbb{Q}(z),$$

έπεται ότι $[\mathbb{Q}(z) : \mathbb{Q}] \leq 2 \cdot [\mathbb{Q}(\sqrt{z}) : \mathbb{Q}]$. Έτσι, χρησιμοποιώντας το Θεώρημα 2.9.6, βλέπουμε ότι αν ο αριθμός z είναι υπερβατικός, τότε και ο $\sqrt{z}$ είναι υπερβατικός. Ειδικότερα, ο αριθμός $\sqrt{\pi}$ είναι υπερβατικός (βλέπε Παράδειγμα 2.9.5 2)).

4) Ο αριθμός $\sqrt[3]{2}$ είναι αλγεβρικός και μηδενίζει το ανάγωγο μονικό πολυώνυμο $x^3 - 2 \in \mathbb{Q}[x]$. Συνεπώς, το $x^3 - 2$ είναι το ελάχιστο πολυώνυμο του $\sqrt[3]{2}$ και άρα η επέκταση $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ είναι βαθμού 3.

5) Έστω $a = \cos\frac{\pi}{9} \in \mathbb{R}$. Τότε, ο αριθμός a είναι αλγεβρικός και μάλιστα ισχύει $[\mathbb{Q}(a) : \mathbb{Q}] = 3$.
Πράγματι, η τριγωνομετρική ταυτότητα $\cos 3t = 4\cos^3 t - 3\cos t$, για $t = \frac{\pi}{9}$, δείχνει ότι $\frac{1}{2} = 4a^3 - 3a$ και άρα ο αριθμός a είναι ρίζα του μονικού πολυωνύμου $f(x) = x^3 - \frac{3}{4}x - \frac{1}{8} \in \mathbb{Q}[x]$. Καθώς είναι εύκολο να δειχτεί ότι το $f(x)$ είναι ανάγωγο (βλέπε Άσκηση 2.9.4), έπεται ότι αυτό είναι ακριβώς το ελάχιστο πολυώνυμο του a.

6) Έστω $b = \cos\frac{2\pi}{7} \in \mathbb{R}$. Θα δείξουμε ότι ο αριθμός b είναι αλγεβρικός και μάλιστα ισχύει $[\mathbb{Q}(b) : \mathbb{Q}] = 3$.
Για το σκοπό αυτό, θεωρούμε την πρωταρχική έβδομη ρίζα της μονάδας $\zeta = e^{2\pi i/7}$ και παρατηρούμε ότι

$$1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 = 0. \tag{2}$$

Καθώς $\zeta + \zeta^6 = \zeta + \zeta^{-1} = 2b$, έχουμε $\zeta^2 + 2 + \zeta^{-2} = 4b^2$ και άρα $\zeta^2 + \zeta^5 = \zeta^2 + \zeta^{-2} = 4b^2 - 2$. Επίσης, $\zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} = 8b^3$ και άρα $\zeta^3 + \zeta^4 = \zeta^3 + \zeta^{-3} = 8b^3 - 6b$. Συνεπώς, η ισότητα (2) γράφεται ισοδύναμα $1 + 2b + (4b^2 - 2) + (8b^3 - 6b) = 0$ και άρα ο αριθμός b είναι ρίζα του πολυωνύμου $8x^3 + 4x^2 - 4x - 1 \in \mathbb{Q}[x]$. Καθώς είναι εύκολο να δειχτεί ότι το πολυώνυμο αυτό είναι ανάγωγο (βλέπε Άσκηση 2.9.4), έπεται ότι το ελάχιστο πολυώνυμο $f(x)$ του b είναι τρίτου βαθμού (και μάλιστα $f(x) = x^3 + \frac{1}{2}x^2 - \frac{1}{2}x - \frac{1}{8}$).

Κατασκευές με κανόνα και διαβήτη.

Για να διατυπώσουμε αυστηρά το πρόβλημα των Ευκλείδειων κατασκευών (των κατασκευών δηλαδή με κανόνα και διαβήτη), θεωρούμε το επίπεδο Π και ένα σύνολο σημείων $\Sigma \subseteq \Pi$. Ορίζουμε δε τα σύνολα $L(\Sigma)$ και $C(\Sigma)$, ως εξής:

- Το σύνολο $L(\Sigma)$ είναι το σύνολο των ευθειών του επιπέδου, οι οποίες διέρχονται από δύο (διαφορετικά μεταξύ τους) σημεία του Σ.
- Το σύνολο $C(\Sigma)$ είναι το σύνολο των κύκλων του επιπέδου, οι οποίοι έχουν κέντρο κάποιο σημείο του Σ και ακτίνα ίση με την απόσταση μεταξύ δύο σημείων του Σ.

Θα συμβολίζουμε με Σ' το σύνολο των σημείων του επιπέδου Π, που αποτελείται από τα σημεία του Σ καθώς και τα σημεία τομής δύο διακεκριμένων ευθειών $L_1, L_2 \in L(\Sigma)$ ή μιας ευθείας $L \in L(\Sigma)$ και ενός κύκλου $C \in C(\Sigma)$ ή δύο διακεκριμένων κύκλων $C_1, C_2 \in C(\Sigma)$.

2.9.8 Πρόταση. *Έστω Σ ένα υποσύνολο του επιπέδου $\Pi = \mathbb{R}^2$, E το υπόσωμα του $\mathbb{R}$ που παράγεται από τις συντεταγμένες των σημείων του Σ και $P = (\kappa, \lambda)$ ένα σημείο με $P \in \Sigma'$. Τότε, ο βαθμός της επέκτασης $E \subseteq E(\kappa, \lambda)$ είναι 1 ή 2.*

Απόδειξη. Θα πρέπει να διακρίνουμε τρεις περιπτώσεις:

(i) Υπάρχουν δύο διακεκριμένες τεμνόμενες ευθείες $L_1, L_2 \in L(\Sigma)$, έτσι ώστε $P \in L_1 \cap L_2$. Θεωρούμε τις εξισώσεις $a_1x + b_1y + c_1 = 0$ και $a_2x + b_2y + c_2 = 0$ των ευθειών L_1 και L_2 αντίστοιχα. Είναι φανερό ότι οι συντελεστές $a_1, b_1, c_1, a_2, b_2, c_2$ μπορεί να επιλεγούν από το σώμα E. Χρησιμοποιώντας τον κανόνα του Cramer, βλέπουμε ότι οι συντεταγμένες κ και λ του σημείου τομής P των ευθειών αυτών ανήκουν στο E και άρα $E(\kappa, \lambda) = E$.

(ii) Υπάρχει μια ευθεία $L \in L(\Sigma)$ και ένας κύκλος $C \in C(\Sigma)$, έτσι ώστε $P \in L \cap C$. Θεωρούμε την εξίσωση $ax + by + c = 0$ της ευθείας L και την εξίσωση $x^2 + y^2 + dx + ey + f = 0$ του κύκλου C με τους συντελεστές a, b, c, d, e, f να ανήκουν στο E. Λύνοντας την εξίσωση της ευθείας ως προς μία μεταβλητή, ας πούμε την y, και αντικαθιστώντας στην εξίσωση του κύκλου, βλέπουμε ότι οι τετμημένες x_1, x_2 των σημείων τομής της ευθείας και του κύκλου δίνονται από τις ρίζες μιας δευτεροβάθμιας εξίσωσης της μορφής $x^2 + sx + t = 0$ με $s, t \in E$. Επιπλέον, για τις τεταγμένες y_1, y_2 των σημείων τομής θα είναι $E(x_1, y_1) = E(x_1)$ και $E(x_2, y_2) = E(x_2)$. Χρησιμοποιώντας το γνωστό τύπο για τις ρίζες μιας δευτεροβάθμιας εξίσωσης, βλέπουμε ότι ο βαθμός της επέκτασης $E \subseteq E(\kappa) = E(\kappa, \lambda)$ είναι 1 αν ο μιγαδικός αριθμός $\sqrt{s^2 - 4t}$ ανήκει στο E και 2 αν όχι (βλέπε Παράδειγμα 2.9.7 1)).

(iii) Υπάρχουν δύο διακεκριμένοι τεμνόμενοι κύκλοι $C_1, C_2 \in C(\Sigma)$, έτσι ώστε $P \in C_1 \cap C_2$. Έστω ότι οι εξισώσεις των κύκλων είναι $x^2 + y^2 + d_1x +$

$e_1y + f_1 = 0$ και $x^2 + y^2 + d_2x + e_2y + f_2 = 0$ αντίστοιχα, για κατάλληλους συντελεστές $d_1, e_1, f_1, d_2, e_2, f_2 \in E$. Θεωρούμε επίσης την ευθεία L με εξίσωση $(d_1-d_2)x+(e_1-e_2)y+(f_1-f_2) = 0$. Καθώς είναι προφανές ότι $C_1 \cap C_2 = C_1 \cap L$, αναγόμαστε στην περίπτωση (ii) παραπάνω. ⊺

Έστω Σ ένα σύνολο σημείων του επιπέδου Π. Θεωρούμε το σύνολο $\Gamma(\Sigma)$, το οποίο αποτελείται από όλα τα σημεία P του επιπέδου που έχουν την εξής ιδιότητα: Υπάρχει $n \geq 1$ και μια ακολουθία σημείων του επιπέδου $P_1, \ldots, P_n$ με $P_n = P$, τέτοια ώστε

$$P_i \in (\Sigma \cup \{P_1, \ldots, P_{i-1}\})'$$

για κάθε $i = 1, \ldots, n$. Έτσι, το σύνολο $\Gamma(\Sigma)$ αποτελείται από τα σημεία του επιπέδου Π τα οποία μπορούν να κατασκευαστούν σε ένα πεπερασμένο αριθμό βημάτων με τη χρήση του κανόνα και του διαβήτη από τα σημεία του Σ. Θα λέμε ότι το $\Gamma(\Sigma)$ είναι το σύνολο των ***κατασκευάσιμων από το*** Σ ***σημείων του επιπέδου***.

Παρατηρούμε ότι αν το σύνολο Σ περιέχει μόνο ένα ή κανένα σημείο, τότε $\Gamma(\Sigma) = \Sigma$. Συνεπώς, η ενδιαφέρουσα περίπτωση είναι αυτή όπου το Σ περιέχει τουλάχιστον δύο σημεία P_1, P_2. Επιλέγοντας κατάλληλα το Καρτεσιανό σύστημα συντεταγμένων, μπορούμε να υποθέσουμε ότι $P_1 = (0, 0)$ και $P_2 = (1, 0)$.

Με τον παραπάνω συμβολισμό, τα τέσσερα γεωμετρικά προβλήματα που αναφέραμε στην αρχή της Παραγράφου αυτής μπορούν να διατυπωθούν ως εξής:

1. (διπλασιασμός του κύβου) Θεωρούμε τα σημεία $P_1 = (0, 0)$ και $P_2 = (1, 0)$, τα οποία ορίζουν την ακμή του μοναδιαίου κύβου, και το σύνολο $\Sigma = \{P_1, P_2\}$. Ανήκει το σημείο $P = (\sqrt[3]{2}, 0)$ (το οποίο ορίζει μαζί με το P_1 τον κύβο με όγκο 2 κυβικές μονάδες) στο σύνολο $\Gamma(\Sigma)$ των κατασκευάσιμων από το Σ σημείων του επιπέδου;

2. (τριχοτόμηση γωνίας) Θεωρούμε τα σημεία $P_1 = (0, 0)$, $P_2 = (1, 0)$ και $P_3 = (\cos\theta, \sin\theta)$, τα οποία ορίζουν τις πλευρές της γωνίας θ, και το σύνολο $\Sigma = \{P_1, P_2, P_3\}$. Ανήκει το σημείο $P = (\cos\frac{\theta}{3}, \sin\frac{\theta}{3})$, το οποίο ορίζει μαζί με τα P_1 και P_2 τις πλευρές της γωνίας $\frac{\theta}{3}$, στο $\Gamma(\Sigma)$;

3. (κατασκευή κανονικού n-γώνου) Θεωρούμε τα σημεία $P_1 = (0, 0)$ και $P_2 = (1, 0)$, τα οποία ορίζουν την ακτίνα του μοναδιαίου κύκλου, και το σύνολο $\Sigma = \{P_1, P_2\}$. Ανήκει το σημείο $P = (\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n})$, το οποίο ορίζει μαζί με τα P_1 και P_2 τις κορυφές του κανονικού n-γώνου, στο $\Gamma(\Sigma)$;

4. (τετραγωνισμός του κύκλου) Θεωρούμε τα σημεία $P_1 = (0, 0)$ και $P_2 = (1, 0)$, τα οποία ορίζουν την ακτίνα του μοναδιαίου κύκλου, και το σύνολο $\Sigma = \{P_1, P_2\}$. Ανήκει το σημείο $P = (\sqrt{\pi}, 0)$, το οποίο μαζί με το P_1 ορίζει την πλευρά ενός τετραγώνου με εμβαδόν ίσο με αυτό του κύκλου, στο $\Gamma(\Sigma)$;

Το κριτήριο που αποδεικνύεται στο επόμενο αποτέλεσμα θα μας επιτρέψει να δείξουμε το αδύνατο των παραπάνω γεωμετρικών προβλημάτων.

2.9.9 Θεώρημα. *Έστω Σ ένα υποσύνολο του επιπέδου $\Pi = \mathbb{R}^2$ και E το υπόσωμα του $\mathbb{R}$ που παράγεται από τις συντεταγμένες των σημείων του Σ. Τότε, για κάθε σημείο $P = (a, b)$ που ανήκει στο $\Gamma(\Sigma)$ οι επεκτάσεις $E \subseteq E(a)$ και $E \subseteq E(b)$ έχουν βαθμό δυνάμεις του 2, δηλαδή $[E(a) : E] = 2^u$ και $[E(b) : E] = 2^v$ για κατάλληλους φυσικούς αριθμούς u, v.*

Απόδειξη. Καθώς $P \in \Gamma(\Sigma)$, υπάρχει ένας φυσικός αριθμός $n \geq 1$ και μια ακολουθία σημείων $P_1, \ldots, P_n$ με $P_n = P$, τέτοια ώστε $P_i \in (\Sigma \cup \{P_1, \ldots, P_{i-1}\})'$ για κάθε $i = 1, \ldots, n$. Έστω ότι $P_i = (a_i, b_i)$ για κάθε i. Ειδικότερα, έχουμε $a_n = a$ και $b_n = b$. Θεωρούμε τις διαδοχικές επεκτάσεις

$$E = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n,$$

όπου $E_i = E(a_1, b_1, a_2, b_2, \ldots, a_i, b_i)$ για κάθε i. Καθώς $E_i = E_{i-1}(a_i, b_i)$, μπορούμε να χρησιμοποιήσουμε την Πρόταση 2.9.8 και να συμπεράνουμε ότι ο βαθμός της επέκτασης $E_{i-1} \subseteq E_i$ είναι 1 ή 2 για κάθε $i = 1, \ldots, n$. Συνεπώς, από την Πρόταση 2.9.2 έπεται ότι ο βαθμός της επέκτασης $E \subseteq E_n$ είναι μια δύναμη του 2. Καθώς $a, b \in E_n$, οι επεκτάσεις $E \subseteq E(a)$ και $E \subseteq E(b)$ είναι υποεπεκτάσεις της επέκτασης $E \subseteq E_n$. Συνεπώς, το ζητούμενο έπεται από την Πρόταση 2.9.2. ⊺

Είμαστε τώρα σε θέση να δικαιολογήσουμε το αδύνατο της λύσης των τεσσάρων γεωμετρικών προβλημάτων:

1. (διπλασιασμός του κύβου) Εδώ έχουμε $\Sigma = \{(0, 0), (1, 0)\}$ και άρα $E = \mathbb{Q}$. Ο αριθμός $\sqrt[3]{2}$ είναι αλγεβρικός και η επέκταση $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ είναι βαθμού 3 (βλέπε Παράδειγμα 2.9.7 4)). Συνεπώς, με βάση το Θεώρημα 2.9.9, βλέπουμε ότι $(\sqrt[3]{2}, 0) \notin \Gamma(\Sigma)$ και άρα δεν είναι δυνατό να διπλασιαστεί ο κύβος με κανόνα και διαβήτη.

2. (τριχοτόμηση γωνίας) Υπάρχουν γωνίες θ οι οποίες μπορεί να τριχοτομηθούν με κανόνα και διαβήτη. Για παράδειγμα, αυτό συμβαίνει αν $\theta = \frac{\pi}{2}$, αφού είναι γνωστό ότι μπορεί να κατασκευαστεί με κανόνα και διαβήτη γωνία 30^o. Υπάρχουν όμως και γωνίες θ οι οποίες δε μπορεί να τριχοτομηθούν με κανόνα και διαβήτη. Θα δείξουμε ότι αυτό το τελευταίο συμβαίνει αν $\theta = \frac{\pi}{3}$. Στην περίπτωσή μας, καθώς $(\cos\frac{\pi}{3}, \sin\frac{\pi}{3}) = (\frac{1}{2}, \frac{\sqrt{3}}{2})$, έχουμε $\Sigma = \{(0, 0), (1, 0), (\frac{1}{2}, \frac{\sqrt{3}}{2})\}$ και άρα $E = \mathbb{Q}(\sqrt{3})$. Με σκοπό να οδηγηθούμε σε άτοπο, ας υποθέσουμε ότι $(\cos\frac{\pi}{9}, \sin\frac{\pi}{9}) \in \Gamma(\Sigma)$. Τότε, για τον πραγματικό αριθμό $a = \cos\frac{\pi}{9}$, ο βαθμός της επέκτασης $E \subseteq E(a)$ είναι μια δύναμη του 2 (βλέπε Θεώρημα 2.9.9). Καθώς το

E είναι μια γνήσια τετραγωνική επέκταση του $\mathbb{Q}$ (βλέπε Παράδειγμα 2.9.7 1)), έχουμε $[E:\mathbb{Q}]=2$ και άρα ο βαθμός της επέκτασης $\mathbb{Q}\subseteq E(a)$ είναι επίσης μια δύναμη του 2 (βλέπε Πρόταση 2.9.2). Όμως $[E(a):\mathbb{Q}]=[E(a):\mathbb{Q}(a)]\cdot[\mathbb{Q}(a):\mathbb{Q}]$ και άρα $[\mathbb{Q}(a):\mathbb{Q}]\mid[E(a):\mathbb{Q}]$. Συνεπώς, ο βαθμός της επέκτασης $\mathbb{Q}\subseteq\mathbb{Q}(a)$ θα πρέπει να είναι επίσης μια δύναμη του 2. Αυτό το τελευταίο όμως δε συμβαίνει, αφού $[\mathbb{Q}(a):\mathbb{Q}]=3$, όπως δείχτηκε στο Παράδειγμα 2.9.7 5).

3. (κατασκευή κανονικού n-γώνου) Εδώ έχουμε $\Sigma=\{(0,0),(1,0)\}$ και άρα $E=\mathbb{Q}$. Υπάρχουν τιμές του φυσικού αριθμού n για τις οποίες η κατασκευή ενός κανονικού n-γώνου είναι δυνατή. Για παράδειγμα, αυτό συμβαίνει αν $n=4$. Αυτό όμως δε συμβαίνει για όλες τις τιμές του n. Θα δείξουμε ότι το κανονικό επτάγωνο δε μπορεί να κατασκευαστεί με κανόνα και διαβήτη, δείχνοντας ότι $(\cos\frac{2\pi}{7},\sin\frac{2\pi}{7})\notin\Gamma(\Sigma)$.[2] Χρησιμοποιώντας το Θεώρημα 2.9.9, αρκεί να δειχτεί ότι για τον πραγματικό αριθμό $b=\cos\frac{2\pi}{7}$ ο βαθμός της επέκτασης $\mathbb{Q}\subseteq\mathbb{Q}(b)$ δεν είναι μια δύναμη του 2. Αυτό όμως έπεται από το Παράδειγμα 2.9.7 6), όπου δείξαμε ότι $[\mathbb{Q}(b):\mathbb{Q}]=3$.

4. (τετραγωνισμός του κύκλου) Και εδώ έχουμε $\Sigma=\{(0,0),(1,0)\}$ και άρα $E=\mathbb{Q}$. Καθώς ο αριθμός $\sqrt{\pi}$ είναι υπερβατικός (βλέπε Παράδειγμα 2.9.7 3)), το κριτήριο του Θεωρήματος 2.9.9 μας δείχνει ότι $(\sqrt{\pi},0)\notin\Gamma(\Sigma)$. Συνεπώς, δεν είναι δυνατό να τετραγωνιστεί ο κύκλος με κανόνα και διαβήτη.

Ασκήσεις 2.9

1. Να δειχτεί ότι $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$ και να βρεθεί το ελάχιστο πολυώνυμο του $\sqrt{2}+\sqrt{3}$ υπεράνω του $\mathbb{Q}$.

2. Έστω $a,b\in\mathbb{C}$ δύο αλγεβρικοί αριθμοί. Να δειχτεί ότι ο $a+b$ είναι επίσης αλγεβρικός.
   Υπόδειξη: Θεωρήστε τις διαδοχικές επεκτάσεις $\mathbb{Q}\subseteq\mathbb{Q}(a)\subseteq\mathbb{Q}(a,b)$.

3. Έστω E ένα υπόσωμα του $\mathbb{C}$ και z ένας μιγαδικός αριθμός που είναι αλγεβρικός υπεράνω του E, με ελάχιστο πολυώνυμο (υπεράνω του E) περιττού βαθμού. Να δειχτεί ότι $E(z)=E(z^2)$.

[2] Έστω p ένας πρώτος αριθμός. Ο Gauss έδειξε ότι το κανονικό πολύγωνο με p πλευρές μπορεί να κατασκευαστεί με κανόνα και διαβήτη αν και μόνο αν $p=2^{2^n}+1$ για κάποιο φυσικό αριθμό n. Οι πρώτοι αριθμοί της μορφής αυτής ονομάζονται πρώτοι αριθμοί του Fermat. Για $n=0,1,2,3$ και 4, παίρνουμε τους πρώτους $3,5,17,257$ και 65537 αντίστοιχα. (Δεν είναι γνωστό αν υπάρχουν άλλοι πρώτοι αριθμοί του Fermat, εκτός από τους προηγούμενους. Για $n=5$, ο αριθμός $2^{2^5}+1=641\cdot6700417$ δεν είναι πρώτος.) Πιο γενικά, ας θεωρήσουμε έναν ακέραιο $n\geq1$. Ο Gauss έδειξε ότι το κανονικό πολύγωνο με n πλευρές είναι κατασκευάσιμο με κανόνα και διαβήτη αν και μόνο αν ο n είναι της μορφής $2^m p_1\cdots p_s$, όπου $m\geq0$ και οι $p_1,\ldots,p_s$ είναι διακεκριμένοι πρώτοι αριθμοί του Fermat.

4. Να δειχτεί ότι τα πολυώνυμα $a(x), b(x) \in \mathbb{Q}[x]$, όπου $a(x) = 8x^3 - 6x - 1$ και $b(x) = 8x^3 + 4x^2 - 4x - 1$, είναι ανάγωγα.

5. Έστω Σ ένα σύνολο σημείων του επιπέδου και $\Gamma(\Sigma)$ το σύνολο των σημείων που μπορούν να κατασκευαστούν με κανόνα και διαβήτη από το Σ. Να δειχτεί ότι $\Gamma(\Sigma) = \Gamma(\Gamma(\Sigma))$.

6. Να δειχτεί ότι το κανονικό 9-γωνο δε μπορεί να κατασκευαστεί με κανόνα και διαβήτη.
   Υπόδειξη: Αν μπορούσαμε να κατασκευάσουμε μια γωνία 40^o, θα μπορούσαμε να κατασκευάσουμε και μια γωνία 20^o.

2.10 Πρώτα και Μεγιστικά Ιδεώδη

Στην Παράγραφο 2.1 είδαμε ότι το πηλίκο $\mathbb{Z}/ < p >$ είναι ένα σώμα αν και μόνο αν ο p είναι πρώτος αριθμός και στην Παράγραφο 2.6 είδαμε ότι το πηλίκο $F[x]/ < p(x) >$, όπου το F είναι ένα σώμα και $p(x) \in F[x]$, είναι σώμα αν και μόνο αν το $p(x)$ είναι ανάγωγο. Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και I ένα ιδεώδες του R. Στην παρούσα Παράγραφο θα εξετάσουμε γενικότερα πότε ο δακτύλιος πηλίκο R/I είναι σώμα ή ακεραία περιοχή.

Αν ο p είναι ένας πρώτος αριθμός και $a, b \in \mathbb{Z}$, τότε έχουμε (βλ. Λήμμα 1.2.5)

$$p|ab \Rightarrow p|a \ \ \text{ή} \ \ p|b. \tag{1}$$

Χρησιμοποιώντας ιδεώδη στο $\mathbb{Z}$, βλέπουμε ότι η ιδιότητα (;;) είναι ισοδύναμη με την

$$ab \in < p > \Rightarrow a \in < p > \ \ \text{ή} \ \ b \in < p > .$$

2.10.1 Ορισμός. *Έστω R ένας μεταθετικός δακτύλιος και $P \neq R$ ένα ιδεώδες του R. Το P ονομάζεται* **πρώτο** *ιδεώδες αν*

$$a, b \in R, \ ab \in P \Rightarrow a \in P \ \ \text{ή} \ \ b \in P.$$

2.10.2 Παραδείγματα.

1) Για κάθε πρώτο αριθμό p το ιδεώδες $< p >$ του $\mathbb{Z}$ είναι πρώτο.

2) Το ιδεώδες $< 6 >$ του $\mathbb{Z}$ δεν είναι πρώτο γιατί $2 \cdot 3 \in < 6 >$, αλλά $2 \notin < 6 >$ και $3 \notin < 6 >$.

3) Για κάθε ανάγωγο πολυώνυμο $p(x) \in F[x]$, όπου F είναι ένα σώμα, το ιδεώδες $< p(x) >$ του $F[x]$ είναι πρώτο λόγω του Λήμματος 2.3.8.

4) Το ιδεώδες $< f(x) >$ του $\mathbb{Q}[x]$, όπου $f(x) = (x-1)(x-2)$, δεν είναι πρώτο γιατί $(x-1)(x-2) \in < f(x) >$, αλλά $x - 1 \notin < f(x) >$ και $x - 2 \notin < f(x) >$.

5) Σε κάθε ακεραία περιοχή το μηδενικό ιδεώδες είναι πρώτο.

6) Το ιδεώδες $< x >$ του $\mathbb{Z}[x]$ είναι πρώτο.

Στα παραδείγματα 1 και 3 γνωρίζουμε ότι οι αντίστοιχοι δακτύλιοι πηλίκα είναι σώματα. Στο παράδειγμα 6 παρατηρούμε ότι ο δακτύλιος πηλίκο $\mathbb{Z}[x]/ < x >$ είναι ισόμορφος με το $\mathbb{Z}$ (Παράδειγμα 2.6.7 2)) και άρα δεν είναι σώμα, αλλά μόνο ακεραία περιοχή. Σχετικά έχουμε το ακόλουθο αποτέλεσμα.

2.10.3 Θεώρημα. *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Τότε ένα ιδεώδες P του R είναι πρώτο αν και μόνο αν ο δακτύλιος πηλίκο R/P είναι ακεραία περιοχή.*

Απόδειξη. Έστω ότι το P είναι πρώτο ιδεώδες. Γνωρίζουμε από την Πρόταση 2.6.1 ότι ο δακτύλιος πηλίκο R/P είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Από τον ορισμό του πρώτου ιδεώδους έχουμε $P \neq R$ και άρα $1 \notin P$. Συνεπώς στο R/P ισχύει $0_{R/P} = P \neq 1 + P = 1_{R/P}$. Για να δείξουμε ότι ο R/P είναι ακεραία περιοχή, αρκεί να δείξουμε ότι ο δακτύλιος αυτός δεν περιέχει μηδενοδιαιρέτες. Έστω, λοιπόν, $(a + P)(b + P) = P$. Τότε

$$ab + P = P \Rightarrow ab \in P$$
$$\Rightarrow a \in P \ \text{ ή } \ b \in P \ \text{ (γιατί το } P \text{ είναι πρώτο)}$$
$$\Rightarrow a + P = P = 0_{R/P} \ \text{ ή } \ b + P = P = 0_{R/P}.$$

Αντίστροφα, έστω ότι ο R/P είναι ακεραία περιοχή. Τότε $0_{R/P} \neq 1_{R/P}$, δηλαδή $P \neq 1 + P$ και κατά συνέπεια $1 \notin P$. Άρα $P \neq R$. Έστω $ab \in P$, όπου $a, b \in R$. Στο R/P έχουμε

$$ab + P = P \Rightarrow (a + P)(b + P) = P = 0_{R/P}$$
$$\Rightarrow a + P = P \ \text{ ή } \ b + P = P \ (\text{γιατί ο } R/P \text{ είναι ακεραία περιοχή})$$
$$\Rightarrow a \in P \ \text{ ή } \ b \in P.$$

Άρα το ιδεώδες P είναι πρώτο. ⊤

Είδαμε πριν ότι για να είναι ο δακτύλιος R/I σώμα δεν αρκεί το I να είναι πρώτο ιδεώδες. Ας υποθέσουμε ότι ο R/I είναι σώμα. Γνωρίζουμε ότι δεν υπάρχουν μη τετριμμένα γνήσια ιδεώδη ενός σώματος. Επίσης γνωρίζουμε ότι κάθε ιδεώδες του R/I είναι της μορφής J/I, όπου το J είναι ένα ιδεώδες τέτοιο ώστε $I \subseteq J \subseteq R$ (Πόρισμα 2.6.11). Επομένως αν το J είναι ένα ιδεώδες του R και $I \subseteq J \subseteq R$, τότε $J = I$ ή $J = R$. Οδηγούμαστε έτσι στον επόμενο ορισμό.

2.10.4 Ορισμός. *Έστω R ένας δακτύλιος και $M \neq R$ ένα ιδεώδες του R. Το M ονομάζεται* ***μεγιστικό*** *αν για κάθε ιδεώδες I του R με $M \subseteq I$ είναι $I = M$ ή $I = R$.*

2.10.5 Παράδειγμα. Έστω p ένας πρώτος αριθμός. Τότε το ιδεώδες $< p >$ του $\mathbb{Z}$ είναι μεγιστικό. Πράγματι, έστω I ένα ιδεώδες του $\mathbb{Z}$ που περιέχει το $< p >$ και έστω ότι $< p > \neq I$. Τότε υπάρχει ένα $a \in I$ που δεν είναι πολλαπλάσιο του p. Ισχύει $\mu\kappa\delta(p, a) = 1$ και από το Θεώρημα 1.2.4 υπάρχουν $b, c \in \mathbb{Z}$ με $1 = bp + ac$. Επειδή $a \in I$ και $p \in < p > \subseteq I$ παίρνουμε $bp + ac \in I$ γιατί το I είναι ιδεώδες. Άρα $1 \in I$ που σημαίνει ότι $I = \mathbb{Z}$. Συνεπώς το $< p >$ είναι μεγιστικό.

2.10.6 Θεώρημα. *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Τότε ένα ιδεώδες M του R είναι μεγιστικό αν και μόνο αν ο δακτύλιος πηλίκο R/M είναι σώμα.*

Απόδειξη. Έστω ότι το M είναι μεγιστικό ιδεώδες. Γνωρίζουμε από την Πρόταση 2.6.1 ότι ο δακτύλιος πηλίκο R/M είναι μεταθετικός με μοναδιαίο στοιχείο. Από τον ορισμό του μεγιστικού ιδεώδους έχουμε $M \neq R$ και άρα $1 \notin M$. Συνεπώς στο R/M ισχύει $0_{R/M} = M \neq 1 + M = 1_{R/M}$. Για να δείξουμε ότι ο R/M είναι σώμα, αρκεί να δείξουμε ότι κάθε μη μηδενικό στοιχείο του είναι αντιστρέψιμο. Έστω $a + M \in R/M$, $a + M \neq M$. Τότε $a \notin M$. Το σύνολο

$$I = M + < a >= \{m + ra \in R | m \in M,\ r \in R\}$$

είναι ένα ιδεώδες του R που περιέχει το M (βλ. Πρόταση 2.5.8). Ισχύει $M \neq I$, γιατί $a \notin M$ και $a \in I$. Επειδή το M είναι μεγιστικό παίρνουμε $I = R$. Συνεπώς έχουμε $1 \in R = I$ και άρα

$$1 = m + ra$$

για κάποια $m \in M$, $r \in R$. Αφού $1 - ra = m \in M$ έχουμε στο R/M τη σχέση $1 + M = ra + M$. Επομένως

$$1 + M = ra + M = (r + M)(a + M),$$

που σημαίνει ότι το $a + M$ είναι αντιστρέψιμο στο R/M.

Αντίστροφα, έστω ότι ο R/M είναι ένα σώμα. Έστω I ένα ιδεώδες του R με $M \subseteq I \subseteq R$ και $M \neq I$. Τότε το I/M είναι ένα μη τετριμμένο ιδεώδες του R/M. Επειδή ο R/M είναι σώμα συμπεραίνουμε ότι $I/M = R/M$. Από το Πόρισμα 2.6.11 (ή και από τους ορισμούς) συμπεραίνουμε ότι $I = R$. ⊺

2.10.7 Πόρισμα. *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Τότε κάθε μεγιστικό ιδεώδες του R είναι πρώτο.*

Απόδειξη. Το Πόρισμα έπεται από το Θεώρημα 2.10.6 και το Θεώρημα 2.10.3. ⊺

2.10.8 Παραδείγματα.

1. Τα μεγιστικά ιδεώδη του $\mathbb{Z}$ είναι τα $< p >$, όπου p είναι πρώτος αριθμός. Τα ιδεώδη αυτά μαζί με το $< 0 >$ είναι τα πρώτα ιδεώδη του $\mathbb{Z}$.

2. Αν το F είναι ένα σώμα και το $p(x) \in F[x]$ είναι ανάγωγο, τότε το ιδεώδες $< p(x) >$ είναι μεγιστικό. Αυτό έπεται άμεσα από το Θεώρημα 2.10.6 και το Θεώρημα 2.6.3.

3. Το ιδεώδες $< x >$ στο $\mathbb{Z}[x]$ είναι πρώτο, αλλά όχι μεγιστικό αφού $\mathbb{Z}[x]/ < x > \cong \mathbb{Z}$ που είναι ακεραία περιοχή αλλά όχι σώμα. Όμοια, τα ιδεώδη $< x >, < y >, < x, y >$ του $\mathbb{Z}[x, y]$ είναι πρώτα, αλλά όχι μεγιστικά.

4. Στο $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} | a, b \in \mathbb{Z}\}$ θεωρούμε το ιδεώδες $M = \{a + bi \in \mathbb{Z}[i] | a, b \in 3\mathbb{Z}\}$. Θα δείξουμε ότι το M είναι ένα μεγιστικό ιδεώδες.
Έστω I ένα ιδεώδες του R με $M \subseteq I \subseteq R$ και $I \neq M$. Τότε υπάρχει $a+bi \in I$, όπου ένα τουλάχιστον από τα a, b δεν είναι ακέραιο πολλαπλάσιο του 3. Χρησιμοποιώντας ισοτιμίες $\mod 3$ βλέπουμε ότι το $a^2 + b^2$ δεν είναι πολλαπλάσιο του 3 (άσκηση). Συνεπώς $\mu\kappa\delta(a^2 + b^2, 3) = 1$ και άρα υπάρχουν ακέραιοι x, y με

$$1 = (a^2 + b^2)x + 3y.$$

Ισχύει

$$a^2 + b^2 \in I,$$

γιατί $a^2+b^2 = (a+bi)(a-bi)$ και το I είναι ιδεώδες που περιέχει το $a+bi$. Επειδή ισχύει και η σχέση

$$3 \in M \subseteq I$$

παίρνουμε $1 \in I$. Άρα $I = R$ και κατά συνέπεια το M είναι μεγιστικό.

5. Στο $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} | a, b \in \mathbb{Z}\}$ θεωρούμε το ιδεώδες $M = \{a + bi \in \mathbb{Z}[i] | a, b \in 5\mathbb{Z}\}$. Θα δείξουμε ότι το M δεν είναι μεγιστικό ιδεώδες.
Θεωρούμε το ιδεώδες $I =< 2+i >$. Έχουμε $5 = 4+1 = (2+i)(2-i) \in I$. Άρα $M \subseteq I$. Ισχύει $M \neq I$ γιατί $2+i \notin M$. Μένει να δείξουμε ότι $I \neq R$. Έστω $I = R$. Τότε $1 \in I$ και επομένως

$$1 = (2 + i)(x + yi)$$

για κάποιους ακεραίους x, y. Λύνοντας το σύστημα $1 = 2x - y$ και $0 = 2y + x$, βρίσκουμε $x = 5/2$ που είναι άτοπο.

Σημείωση Ο προσδιορισμός των μεγιστικών (και των πρώτων) ιδεωδών του $\mathbb{Z}[i]$ επιτυχγάνεται στην Παράγραφο 3.3. Εκεί δίνεται και μια ενδιαφέρουσα αριθμοθεωρητική εφαρμογή του αποτελέσματος αυτού.

6. Έστω X το σύνολο των μεγιστικών ιδεωδών του $\mathbb{C}[x]$. Θα αποδείξουμε ότι υπάρχει μια 1-1 και επί αντιστοιχία

$$J : \mathbb{C} \to X, a \mapsto < x - a > .$$

Για κάθε $a \in \mathbb{C}$ το ιδεώδες $< x-a >$ του $\mathbb{C}[x]$ είναι μεγιστικό. Πράγματι, θεωρώντας τον επιμορφισμό $\epsilon_a : \mathbb{C}[x] \to \mathbb{C}$, $f(x) \mapsto f(a)$, συμπεραίνουμε

από το 1^o Θεώρημα Ισομορφισμών (βλ 2.6.6) ότι $\mathbb{C}[x]/ < x-a > \cong \mathbb{C}$. Σύμφωνα με το Θεώρημα 2.10.6, το ιδεώδες $< x-a >$ είναι μεγιστικό.

Έστω $< x-a >=< x-b >$. Τότε $x-a \in < x-b >$ και άρα υπάρχει $f(x) \in \mathbb{C}[x]$ με $x-a = f(x)(x-b)$. Συνεπώς $f(x)=1$ και $a=b$. Άρα η απεικόνιση J είναι 1-1.

Έστω M ένα μεγιστικό ιδεώδες του $\mathbb{C}[x]$. Από την Άσκηση 2.5.11 έχουμε $M =< f(x) >$, για κάποιο $f(x) \in \mathbb{C}[x]$. Επειδή το $\mathbb{C}$ είναι σώμα, μπορούμε να υποθέσουμε ότι το $f(x)$ είναι μονικό. Από το Θεώρημα 2.10.6 έχουμε ότι το $\mathbb{C}[x]/M$ είναι σώμα. Σύμφωνα με το Θεώρημα 2.6.3 το $f(x)$ είναι ανάγωγο. Από το Θεμελιώδες Θεώρημα της Αλγεβρας συμπεραίνουμε ότι ο βαθμός του $f(x)$ είναι 1 (βλ. Πόρισμα 2.4.9). Συνεπώς το $f(x)$ είναι της μορφής $x-a$, για κάποιο $a \in \mathbb{C}$. Άρα η απεικόνιση J είναι επί.

Σημείωση Το προηγούμενο αποτέλεσμα μπορεί να γενικευθεί ως εξής.
Θεώρημα Ριζών του Hilbert (Nullstellensatz[1]). *Το σύνολο των μεγιστικών ιδεωδών του* $\mathbb{C}[x_1, \ldots, x_n]$ *είναι το*

$$\{< x_1 - a_1, \ldots, x_n - a_n > | a_1, \ldots, a_n \in \mathbb{C}\}.$$

Το αποτέλεσμα αυτό είναι ένα από τα θεμελιώδη θεωρήματα της Αλγεβρικής Γεωμετρίας. Για μια απόδειξή του παραπέμπουμε στο M. Reid [20] όπου μπορεί να βρεί ο αναγνώστης και μια προσιτή εξήγηση της σημασίας του αποτελέσματος αυτού. (βλ. επίσης Μ. Μαλιάκας [17]).

Ασκήσεις 2.10

1. Δώστε ένα παράδειγμα πρώτου ιδεώδους του $\mathbb{Q}[x]$ που δεν είναι μεγιστικό.
2. Ποια από τα παρακάτω ιδεώδη είναι πρώτα ή και μεγιστικά;
   i) $< x-1 >$ στο $\mathbb{Q}[x]$
   ii) $< x^2-1 >$ στο $\mathbb{Q}[x]$
   iii) $< x^2+1 >$ στο $\mathbb{Q}[x]$
   iv) $< 0 >$ στο $\mathbb{Z}_6$.
   v) $< 0 >$ στο $\mathbb{Z}_7$.
   vi) $\{[0],[2],[4]\}$ στο $\mathbb{Z}_6$
   vii) $\{[0],[6]\}$ στο $\mathbb{Z}_{12}$

[1] Το Θεώρημα αυτό αποδείχθηκε από τον D. Hilbert το 1893. Ο όρος Nullstellensatz σημαίνει στα Γερμανικά "Θεώρημα ριζών"

viii) $< 1 + i >$ στο $\mathbb{Z}[i]$

ix) $< 2 >$ στο $\mathbb{Z}[i]$.

3. Ποια από τα παρακάτω πηλίκα είναι σώματα;

   i) $\mathbb{Z}[x]/ < x^2 + 1 >$

   ii) $\mathbb{Q}[x]/ < x^3 + 2 >$

   iii) $\mathbb{R}[x]/ < x^3 + 2 >$

   iv) $\mathbb{Z}[i]/ < 4 >$

   v) $\mathbb{Z}[i]/ < 7 >$

   vi) $\mathbb{Z}[i]/ < 1 + i >$

4. Δώστε ένα παράδειγμα που δείχνει ότι η τομή δύο πρώτων ιδεωδών δεν είναι γενικά πρώτο ιδεώδες.

5. Να βρεθούν όλα τα μεγιστικά ιδεώδη των δακτυλίων $\mathbb{Z}_4$, $\mathbb{Z}_6$ και $\mathbb{Z}_{12}$ και να προσδιορισθούν τα αντίστοιχα πηλίκα.

6. Έστω R πεπερασμένος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Αποδείξτε ότι τα πρώτα και τα μεγιστικά ιδεώδη του R ταυτίζονται.
   Υπόδειξη: Βλ. Πρόταση 2.1.6.

7. Το ιδεώδες $I = \{f(x) \in \mathbb{Z}[x] | f(0) \in 2\mathbb{Z}\}$ του $\mathbb{Z}[x]$ είναι μεγιστικό.

8. Το ιδεώδες $< p > \times \mathbb{Z}$ του $\mathbb{Z} \times \mathbb{Z}$ είναι μεγιστικό αν και μόνο ο p είναι πρώτος αριθμός.

9. Αληθεύει ότι το ιδεώδες $< p > \times < p >$ του $\mathbb{Z} \times \mathbb{Z}$ είναι μεγιστικό αν το p είναι πρώτος;

10. Έστω $\varphi : R \to F$ ένας μη τετριμμένος ομομορφισμός δακτυλίων, όπου ο R είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και το F είναι ένα σώμα. Αποδείξτε ότι το ιδεώδες $\ker \varphi$ είναι πρώτο.

11. Έστω $\varphi : R \to S$ ένας επιμορφισμός μεταθετικών δακτυλίων που έχουν μοναδιαία στοιχεία.

    i) Αποδείξτε ότι το $\varphi^{-1}(J)$ είναι ένα πρώτο ιδεώδες του R για κάθε πρώτο ιδεώδες J του S.

    ii) Έστω I ένα ιδεώδες του R. Αποδείξτε ότι κάθε πρώτο ιδεώδες του R/I είναι της μορφής J/I, όπου J είναι ένα πρώτο ιδεώδες του R που περιέχει το I.

iii) Αληθεύει ότι για κάθε πρώτο ιδεώδες I του R το $\varphi(I)$ είναι πρώτο ιδεώδες του S;
Υπόδειξη: $\mathbb{Z} \to \mathbb{Z}_2$, $I =< 3 >$.

12. Το ιδεώδες $< 5 >= \{5a+5b\sqrt{2}|a,b \in \mathbb{Z}\}$ του $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2}|a,b \in \mathbb{Z}\}$ είναι μεγιστικό. Αληθεύει ότι το $< 3 >$ είναι μεγιστικό;

13. Στο Παράδειγμα 2.10.8 3) είδαμε ότι το ιδεώδες $< x, y >$ του $\mathbb{Z}[x,y]$ είναι πρώτο αλλά όχι μεγιστικό. Να βρεθεί ένα ιδεώδες I του $\mathbb{Z}[x,y]$ τέτοιο ώστε $< x, y > \subsetneq I$, $I \neq \mathbb{Z}[x,y]$.

14. Να βρεθεί ένα παράδειγμα δακτυλίου που δεν έχει κανένα μη-μηδενικό μεγιστικό ιδεώδες. Μπορείτε να βρείτε ένα παράδειγμα ενός τέτοιου δακτυλίου, ο οποίος να μην είναι μεταθετικός;

15. Η άσκηση αυτή σχετίζεται με το Θεώρημα Ριζών του Hilbert. Έστω F ένα σώμα και $a_1, \ldots, a_n \in F$. Η απεικόνιση

$$\varphi : F[x_1, \ldots, x_n] \to F, \quad f(x_1, \ldots, x_n) \mapsto f(a_1, \ldots, a_n)$$

είναι ένας ομομορφισμός δακτυλίων. Θεωρούμε το ιδεώδες $I =< x_1 - a_1, \ldots, x_n - a_n >$ του $F[x_1, \ldots, x_n]$. Αποδείξτε τα εξής.

i) $I \subseteq \ker \varphi$.

ii) Έστω $f(x_1, \ldots, x_n) \in \ker \varphi$. Τότε υπάρχουν πολυώνυμα $g_i(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$, $i = 1, \ldots, n$, τέτοια ώστε

$$f(x_1, \ldots, x_n) = \sum\nolimits_{i-1}^{n} g_i(x_1, \ldots, x_n)(x_i - a_i).$$

Υπόδειξη: Χρησιμοποιήστε επαγωγή στο n και το Θεώρημα 2.3.5.

iii) $I = \ker \varphi$.

iv) Το ιδεώδες I είναι μεγιστικό.

16. Έστω M και N δύο διακεκριμένα μεγιστικά ιδεώδη ενός μεταθετικού δακτυλίου R με μοναδιαίο στοιχείο, τέτοια ώστε $M \cap N =< 0 >$. Αποδείξτε ότι οι δακτύλιοι M και N είναι σώματα και ότι $R \cong R/M \times R/N \cong M \times N$.

3 Δακτύλιοι και Παραγοντοποίηση

Στην Ενότητα 1 μελετήσαμε την έννοια της διαιρετότητας στο $\mathbb{Z}$ και ως εφαρμογή της μοναδικότητας της παραγοντοποίησης σε γινόμενο πρώτων αριθμών λύσαμε τη Διοφαντική εξίσωση $x^2 + y^2 = z^2$. Με τη βοήθεια αυτής δείξαμε ότι η Διοφαντική εξίσωση $x^4 + y^4 = z^4$ δεν έχει μη τετριμμένες λύσεις. Το 1874 ο Lame ανακοίνωσε στην Ακαδημία των Παρισίων την "απόδειξή" του ότι η εξίσωση του Fermat, $x^n + y^n = z^n$, $n > 2$, δεν έχει μη τετριμμένες ακέραιες λύσεις. Η βασική ιδέα του συλλογισμού του Lame ήταν η εξής. Έστω ότι υπάρχουν $x, y, z \in \mathbb{Z} - \{0\}$ με $x^n + y^n = z^n$. Θέτοντας $\zeta = \sigma\upsilon\nu(2\pi/n) + i\eta\mu(2\pi/n) \in \mathbb{C}$, θεώρησε στο δακτύλιο

$$\mathbb{Z}[\zeta] = \{a_{n-1}\zeta^{n-1} + \cdots + a_1\zeta + a_0 \in \mathbb{C} | a_i \in \mathbb{Z}\}$$

την παραγοντοποίηση

$$x^n = z^n - y^n = (z - y)(z - \zeta y)(z - \zeta^2 y) \cdots (z - \zeta^{n-1} y).$$

Υποθέτοντας ότι στο $\mathbb{Z}$ οι x, y, z είναι σχετικά πρώτοι, απέδειξε ότι οι παράγοντες στο δεξιό μέλος είναι "σχετικά πρώτοι" στο $\mathbb{Z}[\zeta]$. Στη συνέχεια επιχειρηματολόγησε ότι *αφού το γινόμενο των παραγόντων αυτών είναι μια n-στή δύναμη, τότε κάθε ένας από αυτούς είναι μια n-στη δύναμη στο* $\mathbb{Z}[\zeta]$. Από εκεί συνέχισε για να φτάσει σε άτοπο. Στο βήμα αυτό υπάρχει λάθος γιατί η συγκεκριμένη ιδιότητα της παραγοντοποίησης που χρησιμοποίησε ο Lame *δεν ισχύει* γενικά στο $\mathbb{Z}[\zeta]$. Η ιδιότητα αυτή προϋποθέτει την *μοναδικότητα* της "παραγοντοποίησης σε γινόμενο αναγώγων", την κεντρική έννοια αυτής της Ενότητας.

Στις επόμενες Παραγράφους θα μελετήσουμε την έννοια της διαιρετότητας σε τυχαίες ακέραιες περιοχές. Θα ορίσουμε μια οικογένεια δακτυλίων (τις περιοχές μοναδικής παραγοντοποίησης) όπου η διαιρετότητα έχει ιδιότητες παρόμοιες με αυτές που εξετάσαμε στους ακεραίους και τα πολυώνυμα. Στη συνέχεια θα

ασχοληθούμε με την εύρεση περιοχών που ανήκουν στην οικογένεια αυτή και θα δούμε διάφορες εφαρμογές.

3.1 Περιοχές Μοναδικής Παραγοντοποίησης

Έστω R μια ακεραία περιοχή. Για να ορίσουμε τα στοιχεία του R που θα έχουν ιδιότητες παρόμοιες με αυτές των πρώτων αριθμών και των αναγώγων πολυωνύμων πάνω από σώμα, χρειαζόμαστε την έννοια της διαιρετότητας. Έστω $a, b \in R$. Θα λέμε ότι το a διαιρεί το b στο R (ή ότι το b είναι πολλαπλάσιο του a στο R ή ότι το a είναι διαιρέτης του b στο R) αν υπάρχει $c \in R$ με $b = ac$. Στην περίπτωση αυτή γράφουμε "$a|b$ στο R" ή απλά $a|b$ αν είναι σαφές ποιόν R εννούμε. Για παράδειγμα, έχουμε $2|3$ στο $\mathbb{Q}$, αλλά όχι στο $\mathbb{Z}$. Παρατηρούμε ότι οι διαιρέτες του μοναδιαίου στοιχείου $1 \in R$ είναι ακριβώς τα αντιστρέψιμα στοιχεία του R. Ισχύουν εδώ μερικές απλές ιδιότητες:

- αν $a|b$ και $a|c$ τότε $a|rb + sc$ για κάθε $r, s \in R$.
- αν $a|b$ και $b|c$ τότε $a|c$.
- $a = ub$ για κάποιο αντιστρέψιμο $u \in R$, αν και μόνο αν $a|b$ και $b|a$.

Ας αποδείξουμε την τρίτη ιδιότητα. Αν $a = 0$, τότε $b = 0$ και η ιδιότητα ισχύει. Υποθέτουμε ότι $a \neq 0$. Έστω ότι $a = ub$, οπότε $b|a$. Επειδή το u είναι αντιστρέψιμο υπάρχει $\nu \in R$ με $\nu u = 1$. Τότε από τη σχέση $a = ub$ παίρνουμε $\nu a = \nu ub = b$ και άρα $a|b$. Αντίστροφα, έστω $a|b$ και $b|a$. Τότε υπάρχουν $u, \nu \in R$ με $b = ua$ και $a = \nu b$, οπότε $a = \nu ua$. Επειδή ο R είναι ακεραία περιοχή λαμβάνουμε $1 = \nu u$, δηλαδή το u είναι αντιστρέψιμο.

Αν a, b είναι δύο στοιχεία μιας ακεραίας περιοχής R τέτοια ώστε $a = ub$ για κάποιο αντιστρέψιμο $u \in R$, θα λέμε ότι το a είναι ***συντροφικό*** του b στο R, ή ότι τα a, b είναι συντροφικά στο R. Εύκολα επαληθεύεται ότι η σχέση που ορίζεται R με "$a \sim b$ αν και μόνο αν $a = ub$ για κάποιο αντιστρέψιμο $u \in R$" είναι μια σχέση ισοδυναμίας.

Για παράδειγμα, τα συντροφικά στοιχεία του m στο $\mathbb{Z}$ είναι το m και το $-m$. Τα συντροφικά ενός πολυωνύμου $f(x) \in F[x]$, F σώμα, είναι τα $uf(x)$, όπου $u \in F - \{0\}$. Στο $\mathbb{Z}[i]$ τα στοιχεία $3 + 2i$ και $-2 + 3i$ είναι συντροφικά αφού $3 + 2i = -i(-2 + 3i)$ και το $-i$ είναι αντιστρέψιμο. Σε ένα σώμα κάθε δύο μη μηδενικά στοιχεία είναι συντροφικά.

Κάθε $a \in R$ έχει μερικούς προφανείς διαιρέτες, τα συντροφικά του και τα αντιστρέψιμα στοιχεία του R. Ιδιαίτερο ενδιαφέρον παρουσιάζει η περίπτωση που το a δεν έχει άλλους διαιρέτες. Σχετικά δίνουμε τον εξής ορισμό.

3.1.1 Ορισμός. *Έστω R μια ακεραία περιοχή και $p \in R$ ένα μη μηδενικό μη αντιστρέψιμο στοιχείο. Το p ονομάζεται* ***ανάγωγο*** *στο R αν οι μόνοι διαιρέτες του στο R είναι τα συντροφικά του και τα αντιστρέψιμα στοιχεία του R.*

Για παράδειγμα, τα ανάγωγα στοιχεία του $\mathbb{Z}$ είναι τα p και $-p$, όπου p είναι πρώτος. Επειδή κάθε μη μηδενικό στοιχείο σώματος είναι αντιστρέψιμο, βλέπουμε ότι δεν υπάρχουν ανάγωγα στοιχεία σε ένα σώμα. Τα ανάγωγα στοιχεία του πολυωνυμικού δακτυλίου $F[x]$, F σώμα, είναι αυτά που ονομάσαμε ανάγωγα πολυώνυμα στον Ορισμό 2.3.2. Στην περίπτωση όμως που το F δεν είναι σώμα χρειάζεται λίγη προσοχή στην ορολογία: Στο $\mathbb{Z}[x]$ το πολυώνυμο $2x+2$ είναι ανάγωγο σύμφωνα με τον Ορισμό 2.3.2, αλλά δεν είναι ανάγωγο στοιχείο του $\mathbb{Z}[x]$ σύμφωνα με τον Ορισμό 3.1.1, γιατί ο διαιρέτης 2 δεν είναι ούτε αντιστρέψιμο στοιχείο του $\mathbb{Z}[x]$ ούτε συντροφικό του $2x+2$.

Στην πράξη, για να δείξουμε ότι ένα μη μηδενικό μη αντιστρέψιμο στοιχείο $p \in R$ είναι ανάγωγο, συνήθως υποθέτουμε ότι $p = ab$, όπου $a, b \in R$, και δείχνουμε ότι ένα από τα a, b είναι αντιστρέψιμο. Αυτό αρκεί, γιατί αν ένα από τα a, b είναι αντιστρέψιμο, τότε το άλλο θα είναι συντροφικό του p.

Μπορούμε τώρα να ορίσουμε την κύρια έννοια αυτής της Παραγράφου.

3.1.2 Ορισμός. *Μια ακεραία περιοχή R ονομάζεται* ***περιοχή μοναδικής παραγοντοποίησης*** *αν ισχύουν οι παρακάτω ιδιότητες.*

1. *Κάθε στοιχείο του R που δεν είναι μηδέν ή αντιστρέψιμο γράφεται ως γινόμενο αναγώγων στοιχείων του R.*
2. *Αν $a = p_1 \dots p_r$ και $a = q_1 \dots q_s$, όπου τα p_i και q_j είναι ανάγωγα στοιχεία του R, τότε $r = s$ και (μετά ενδεχομένως από κάποια αναδιάταξη) για κάθε i το p_i είναι συντροφικό του q_i.*

Για παράδειγμα, η ακεραία περιοχή $\mathbb{Z}$ είναι περιοχή μοναδικής παραγοντοποίησης σύμφωνα με το Θεμελιώδες Θεώρημα της Αριθμητικής (Θεώρημα 1.2.7). Ο πολυωνυμικός δακτύλιος $F[x]$, όπου F σώμα, είναι περιοχή μοναδικής παραγοντοποίησης λόγω του Θεωρήματος 2.3.10. Επίσης κάθε σώμα είναι περιοχή μοναδικής παραγοντοποίησης κατά τετριμμένο τρόπο, αφού κάθε στοιχείο του είναι 0 ή αντιστρέψιμο. Στην επόμενη Παράγραφο θα αποδείξουμε αποτελέσματα από τα οποία προκύπτουν πολλά άλλα παραδείγματα περιοχών μοναδικής παραγοντοποίησης, όπως είναι ο $\mathbb{Z}[i]$, ο $\mathbb{Z}[x]$ και ο πολυωνυμικός δακτύλιος $R[x_1, \dots, x_n]$, όπου R είναι περιοχή μοναδικής παραγοντοποίησης. Στο παράδειγμα που ακολουθεί δείχνουμε ότι η περιοχή $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \in \mathbb{C} | a, b \in \mathbb{Z}\}$ δεν είναι περιοχή μοναδικής παραγοντοποίησης.

3.1.3 Παράδειγμα. Θα δείξουμε ότι η ακεραία περιοχή $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} \in \mathbb{C} | a, b \in \mathbb{Z}\}$ δεν ικανοποιεί την ιδιότητα 2 του Ορισμού 3.1.2. Πράγματι, παρατηρούμε ότι

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \tag{1}$$

Θα δείξουμε ότι τα στοιχεία $2, 3, 1 + \sqrt{-5}$, $1 - \sqrt{-5}$

1. δεν είναι αντιστρέψιμα

2. είναι ανάγωγα

3. ανά δύο είναι μη συντροφικά.

Από τις ιδιότητες αυτές είναι φανερό ότι η (;;) παρέχει δύο διαφορετικές παραγοντοποιήσεις του 6 σε γινόμενο αναγώγων στοιχείων του $\mathbb{Z}[\sqrt{-5}]$.
1. Ορίζουμε την απεικόνιση

$$N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}, \quad N(a+b\sqrt{-5}) = a^2+5b^2$$

και παρατηρούμε ότι $N(xy) = N(x)N(y)$ για κάθε $x, y \in \mathbb{Z}[\sqrt{-5}]$, γιατί ο a^2+5b^2 είναι το τετράγωνο του μέτρου του μιγαδικού αριθμού $a+b\sqrt{-5}$. Με τη βοήθεια της N βρίσκουμε τα αντιστρέψιμα στοιχεία του $\mathbb{Z}[\sqrt{-5}]$. Αν το $u \in \mathbb{Z}[\sqrt{-5}]$ είναι αντιστρέψιμο, τότε από τη σχέση $u\nu = 1$ παίρνουμε $N(u\nu) = N(1)$, δηλαδή $N(u)N(\nu) = 1$, οπότε $N(u) = 1$. Αν $u = u_0 + u_1\sqrt{-5}$, όπου $u_0, u_1 \in \mathbb{Z}$, τότε $u_0^2 + 5u_1^2 = 1$ και επομένως $u_0 = \pm 1$ και $u_1 = 0$. Άρα τα αντιστρέψιμα στοιχεία του $\mathbb{Z}[\sqrt{-5}]$ είναι τα ± 1.
2. Δείχνουμε ότι το 2 είναι ανάγωγο στο $\mathbb{Z}[\sqrt{-5}]$. Οι αποδείξεις για τα υπόλοιπα στοιχεία είναι παρόμοιες. Έστω $2 = cd$, όπου $c, d \in \mathbb{Z}[\sqrt{-5}]$. Τότε $N(2) = N(cd)$, δηλαδή $4 = N(c)N(d)$ και κατά συνέπεια $N(c) = 1$, ή 2, ή 4. Αν $N(c) = 1$, τότε $c = \pm 1$ (όπως είδαμε πριν) και το c είναι αντιστρέψιμο. Αν $N(c) = 4$, τότε $N(d) = 1$ οπότε το d είναι αντιστρέψιμο. Έστω $N(c) = 2$, και $c = c_0 + c_1\sqrt{-5}$. Τότε έχουμε $c_0^2 + 5c_1^2 = 2$. Είναι φανερό ότι αυτή η Διοφαντική εξίσωση δεν έχει λύσεις.
3. Επειδή τα αντιστρέψιμα στοιχεία του $\mathbb{Z}[\sqrt{-5}]$ είναι τα ± 1, είναι προφανές ότι τα στοιχεία $2, 3, 1+\sqrt{-5}$, $1-\sqrt{-5}$, είναι ανά δύο μη συντροφικά.

Στο παράδειγμα αυτό, ας δούμε το λάθος του Lame που αναφέραμε στην εισαγωγή της Παραγράφου αυτής. Στην ακεραία περιοχή $\mathbb{Z}[\sqrt{-5}]$ έχουμε την παραγοντοποίηση

$$6^2 = 2 \cdot 3 \cdot (1+\sqrt{-5}) \cdot (1-\sqrt{-5}).$$

Όμως κανένα από τα (ανά δύο μη συντροφικά στοιχεία) $2, 3, (1+\sqrt{-5})$, $(1-\sqrt{-5})$ δεν είναι τετράγωνο στο $\mathbb{Z}[\sqrt{-5}]$, γιατί τα στοιχεία αυτά είναι ανάγωγα!

3.1.4 Παρατηρήσεις. Έστω R μια περιοχή μοναδικής παραγοντοποίησης.

1) Αν $a, b \in R$ είναι μη μηδενικά στοιχεία, τότε έχουμε $a = up_1^{a_1} \dots p_n^{a_n}$ και $b = \nu p_1^{b_1} \dots p_n^{b_n}$, όπου a_i, $b_i \in \mathbb{N}$, τα u, ν είναι αντιστρέψιμα στοιχεια του

R και τα p_i είναι ανάγωγα στοιχεία του R ανά δύο μη συντροφικά. Στην περίπτωση αυτή ισχύει

$$a|b \Leftrightarrow a_i \leq b_i \ \text{ για κάθε } \ i.$$

Πράγματι, η συνεπαγωγή "$\Leftarrow$" είναι προφανής. Έστω $a|b$. Από τη σχέση $b = ac$ έχουμε $up_1^{b_1} \dots p_n^{b_n} = \nu p_1^{a_1} \dots p_n^{a_n} c$. Τώρα αν $a_1 > b_1$ παίρνουμε

$$up_2^{b_2} \dots p_n^{b_n} = \nu p_1^{a_1 - b_1} \dots p_n^{a_n} c$$

γιατί ο R είναι ακεραία περιοχή. Από την ισότητα αυτή και την ιδιότητα 2 στον Ορισμό 3.1.2 συμπεραίνουμε ότι το p_1 είναι συντροφικό με κάποιο p_j, $j \neq 1$. Αυτό είναι άτοπο.

2) Αν $a \in R$ είναι μη μηδενικό στοιχείο του R, τότε δεν υπάρχει άπειρη ακολουθία στοιχείων του R της μορφής

$$r_1 = a, \ r_2, r_3, \dots$$

όπου για κάθε i το r_{i+1} διαιρεί το r_i και δεν είναι συντροφικό του. Πράγματι, αν έχουμε $a = up_1^{a_1} \dots p_n^{a_n}$, όπου το u είναι αντιστρέψιμο και τα p_i είναι ανάγωγα και ανά δύο μη συντροφικά, τότε από την προηγούμενη παρατήρηση συμπεραίνουμε οτι κάθε r_i θα έχει μια παράσταση της μορφής $r_i = \nu_i p_1^{b_{i_1}} \dots p_n^{b_{in}}$, όπου για κάθε i το ν_i είναι αντιστρέψιμο στοιχείο και $b_{i_j} \leq a_j$ για κάθε j. Θέτουμε $\partial(r_i) = b_{i_1} + \dots + b_{i_n}$ και παρατηρούμε ότι $\partial(r_{i+1}) < \partial(r_i)$ εφόσον το r_{i+1} διαιρεί το r_i και το r_{i+1} δεν είναι συντροφικό του r_i. Συνεπώς παίρνουμε μια γνήσια φθίνουσα ακολουθία φυσικών αριθμών

$$\partial(r_1) > \partial(r_2) > \partial(r_3) > \dots$$

η οποία βέβαια δεν μπορεί να είναι άπειρη.

Μιλώντας με κάποιο βαθμό ελευθερίας, βλέπουμε ότι αν εξαιρέσουμε αντιστρέψιμα στοιχεία και αν ταυτίσουμε συντροφικούς διαιρέτες, τότε το πλήθος των διαιρετών του a είναι πεπερασμένο.

3) Αν διατυπώσουμε την προηγούμενη παρατήρηση με ιδεώδη έχουμε: δεν υπάρχει γνήσια αύξουσα αλυσίδα κυρίων ιδεωδών του R της μορφής

$$< r_1 > \subsetneq < r_2 > \subsetneq < r_3 > \subsetneq \dots,$$

ή, ισοδύναμα, κάθε αύξουσα αλυσίδα κυρίων ιδεωδών του R της μορφής

$$< r_1 > \subseteq < r_2 > \subseteq < r_3 > \subseteq \dots$$

είναι τελικά σταθερή (δηλαδή υπάρχει $N \in \mathbb{N}$ τέτοιο ώστε $< r_N >=< r_{N+1} >=< r_{N+2} >= \ldots$). Πράγματι, παρατηρούμε ότι

$$r_{i+1}|r_i \Leftrightarrow < r_i > \subseteq < r_{i+1} >,$$

ενώ

$$r_{i+1}|r_i \text{ και } r_{i+1} \text{ μη συντροφικό του } r_i \Leftrightarrow < r_i > \subsetneq < r_{i+1} > .$$

Για την απόδειξη της πρώτης ισοδυναμίας έχουμε

$$r_{i+1}|r_i \Leftrightarrow r_i = cr_{i+1},\ c \in R \Leftrightarrow r_i \in < r_{i+1} > \Leftrightarrow < r_i > \subseteq < r_{i+1} > .$$

Η δέυτερη ισοδυναμία αίναι άμεση συνέπεια της πρώτης, από την οποία έπεται ότι τα r_i και r_{i+1} είναι συντροφικά αν και μόνο αν $< r_i >=< r_{i+1} >$.

4) Γνωρίζουμε ότι αν ο πρώτος p διαιρεί το γινόμενο ab δύο ακεραίων a, b, τότε θα διαιρεί έναν τουλάχιστον από τους a και b (Λήμμα 1.2.5). Αντίστοιχο αποτέλεσμα είδαμε και στα πολυώνυμα (Λήμμα 2.3.8). Γενικά σε κάθε περιοχή μοναδικής παραγοντοποίησης R ισχύει το ακόλουθο. Αν το p είναι ανάγωγο και $p|ab$, όπου $a, b \in R$, τότε το p διαιρεί έναν τουλάχιστον από τα a και b. Η απόδειξη προκύπτει άμεσα από την Παρατήρηση 1).

Οι ιδιότητες που αναφέρονται στις Παρατηρήσεις 3) και 4) παρουσιάζουν ιδιαίτερο ενδιαφέρον γιατί *χαρακτηρίζουν* τις περιοχές μοναδικής παραγοντοποίησης. Ακριβέστερα, έχουμε το ακόλουθο κριτήριο που μας πληροφορεί πότε μια ακεραία περιοχή είναι περιοχή μοναδικής παραγοντοποίησης.

3.1.5 Θεώρημα. *Μια ακεραία περιοχή R είναι περιοχή μοναδικής παραγοντοποίησης αν και μόνο αν ισχύουν οι παρακάτω δύο ιδιότητες.*

1. *Κάθε αύξουσα ακολουθία κυρίων ιδεωδών του R είναι τελικά σταθερή, και*
2. *Αν το $p \in R$ είναι ανάγωγο και $p|ab$, όπου $a, b \in R$, τότε $p|a$ ή $p|b$.*

Απόδειξη. Η μια συνεπαγωγή έχει αποδειχτεί στις προηγούμενες Παρατηρήσεις.

Αντίστροφα, έστω ότι ισχύουν οι ιδιότητες 1 και 2 του Θεωρήματος. Έστω $a \in R$ που δεν είναι μηδέν ή αντιστρέψιμο και έστω ότι το a δεν γράφεται ως γινόμενο αναγώγων στοιχείων του R. Τότε το a δεν είναι ανάγωγο και έτσι έχουμε $a = a_1 b_1$, όπου $a_1, b_1 \in R$ είναι μη αντιστρέψιμα στοιχεία. Αν τα a_1 και b_1 είναι γινόμενα αναγώγων, τότε το ίδιο συμβαίνει και για το $a = a_1 b_1$, που είναι άτοπο. Έστω ότι το a_1 δεν είναι γινόμενο αναγώγων. Ισχύει βέβαια

$$< a > \subseteq < a_1 >,$$

και επιπλέον

$$< a > \neq < a_1 > .$$

Πράγματι, αν $< a >=< a_1 >$ τότε τα a, a_1 είναι συντροφικά (βλ. τη σχέση (;;)) και κατά συνέπεια το b_1 είναι αντιστρέψιμο, που είναι άτοπο.

Τώρα επαναλαμβάνουμε την προηγούμενη διαδικασία για το a_1 στη θέση του a. Έτσι λαμβάνουμε ένα μη αντιστρέψιμο a_2 που δεν είναι γινόμενο αναγώγων και

$$< a_1 > \subsetneq < a_2 > .$$

Συνεχίζοντας λαμβάνουμε μία γνήσια αύξουσα αλυσίδα κυρίων ιδεωδών,

$$< a > \subsetneq < a_1 > \subsetneq < a_2 > \subsetneq \ldots .$$

Από την ιδιότητα 1 αυτό είναι άτοπο.

Η απόδειξη της ιδιότητας 2 στον Ορισμό 3.1.2 είναι παρόμοια με την απόδειξη του Θεωρήματος 2.3.10 (Μοναδικότητα): Στη θέση του Λήμματος 2.3.8 έχουμε την ιδιότητα 2 του Θεωρήματος, στη θέση των c_i έχουμε αντιστρέψιμα στοιχεία του R και στη θέση της Πρότασης 2.2.4 2) μπορούμε να χρησιμοποιήσουμε τον ορισμό του αναγώγου στοιχείου. Οι λεπτομέρειες αφήνονται σαν άσκηση. ⊺

3.1.6 Σημείωση. Η ιδιότητα 2 στο προηγούμενο Θεώρημα είναι ισοδύναμη με την εξής ιδιότητα: αν το $p \in R$ είναι ανάγωγο τότε το ιδεώδες $< p >$ είναι πρώτο. Βλέπουμε έτσι ότι οι δύο ιδιότητες του Θεωρήματος αυτού αναφέρονται σε κύρια ιδεώδη.

Στην επόμενη Παράγραφο θα εφαρμόσουμε το προηγούμενο κριτήριο για να αποδείξουμε ότι οι "ακέραιες περιοχές κυρίων ιδεωδών" είναι περιοχές μοναδικής παραγοντοποίησης.

Θα χρειαστούμε στη συνέχεια την έννοια του μέγιστου κοινού διαιρέτη σε τυχαία περιοχή μοναδικής παραγοντοποίησης. Έστω R μια περιοχή μοναδικής παραγοντοποίησης, $a, b \in R$ μη μηδενικά στοιχεία και $a = up_1^{a_1} \ldots p_n^{a_n}$, $b = \nu p_1^{b_1} \ldots p_n^{b_n}$, όπου $a_i, b_i \in \mathbb{N}$, τα u, ν είναι αντιστρέψιμα στοιχεια του R και τα p_i είναι ανάγωγα στοιχεία του R ανά δύο μη συντροφικά. Θέτοντας $c_i = \min\{a_i, b_i\}$, παρατηρούμε ότι το στοιχείο $c = p_1^{n_1} \ldots p_n^{c_n}$ διαιρεί τα a και b και επιπλέον διαιρείται από κάθε κοινό διαιρέτη των a, b σύμφωνα με την Παρατήρηση 3.1.4 1). Τις ιδιότητες αυτές έχει κάθε στοιχείο της μορφής uc, όπου $u \in R$ είναι αντιστρέψιμο. Κάθε στοιχείο της μορφής uc ονομάζεται ένας μέγιστος κοινός διαιρέτης των a, b. Τονίζουμε ότι ο μέγιστος κοινός διαιρέτης των a, b δεν ορίζεται εδώ μονοσήμαντα, σε αντίθεση με τις ειδικές περιπτώσεις $R = \mathbb{Z}$, $F[x]$, όπου F σώμα. Όμως το κύριο ιδεώδες $< c >$ ορίζεται μονοσήμαντα (γιατί;). Τα στοιχεία a, b λέγονται σχετικά πρώτα αν το 1 είναι ένας μέγιστος

κοινός διαιρέτης των a, b, δηλαδή αν δεν υπάρχει ανάγωγο στοιχείο του R που διαιρεί τα a, b.

Ασκήσεις 3.1

Στις παρακάτω ασκήσεις υποθέτουμε ότι όλοι οι δακτύλιοι είναι *ακέραιες περιοχές*.

1. Έστω $a, b \in R$ με $a \neq 0$. Αν το b δεν είναι αντιστρέψιμο, τότε θα είναι $< ab > \subsetneq < a >$.

2. Αν κάθε δύο μη μηδενικά στοιχεία του R είναι συντροφικά, τότε το R είναι σώμα.

3. Αποδείξτε τα εξής:

   a. Αν το μη μηδενικό ιδεώδες $< p >$ του R είναι πρώτο τότε το $p \in R$ είναι ανάγωγο.

   b. Στο Παράδειγμα 2.10.3, το 2 είναι είναι ανάγωγο στοιχείο, αλλά το ιδεώδες $< 2 >$ δεν είναι πρώτο.

4. Τα αντιστρέψιμα στοιχεία του $\mathbb{Z}[i]$ είναι τα ± 1, $\pm i$. Στο $\mathbb{Z}[i]$ το 3 είναι ανάγωγο, αλλά το 5 δεν είναι.

5. Αληθεύει ότι κάθε ομομορφική εικόνα περιοχής μοναδικής παραγοντοποίησης είναι περιοχή μοναδικής παραγοντοποίησης;

6. Κάθε συντροφικό στοιχείο ενός αναγώγου στοιχείου είναι ανάγωγο.

7. Έστω S μία περιοχή που περιέχεται σε περιοχή μοναδικής παραγοντοποίησης. Αληθεύει ότι η S είναι περιοχή μοναδικής παραγοντοποίησης;

8. Έστω $\varphi : R \to S$ ένας ισομορφισμός δακτυλίων. Τότε το $p \in R$ είναι ανάγωγο αν και μόνο αν το $\varphi(p) \in S$ είναι ανάγωγο.

9. Ο δακτύλιος $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \in \mathbb{C} | a, b \in \mathbb{Z}\}$ δεν είναι περιοχή μοναδικής παραγοντοποίησης.
   Υπόδειξη: $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$.

10. Ο δακτύλιος $\mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} \in \mathbb{C} | a, b \in \mathbb{Z}\}$ δεν είναι περιοχή μοναδικής παραγοντοποίησης.

11. Έστω $n \neq 0, 1$ ένας ακέραιος που δεν διαιρείται με το τετράγωνο ακεραίου μεγαλυτέρου του 1. Αποδείξτε ότι αν ο δακτύλιος $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \in \mathbb{C} | a, b \in \mathbb{Z}\}$ είναι περιοχή μοναδικής παραγοντοποίησης, τότε το 2 δεν είναι ανάγωγο σε αυτόν.
Υπόδειξη: $2|n(n-1) = (n + \sqrt{n})(n - \sqrt{n})$.

3.2 Περιοχές Κυρίων Ιδεωδών, Ευκλείδειες Περιοχές

Περιοχές κυρίων ιδεωδών

Είδαμε στην προηγούμενη Παράγραφο ότι σε μια περιοχή μοναδικής παραγοντοποίησης

1) κάθε αύξουσα ακολουθία κυρίων ιδεωδών είναι τελικά σταθερή, και

2) κάθε κύριο ιδεώδες που παράγεται από ανάγωγο στοιχείο είναι πρώτο.

Συνεπώς βλέπουμε ότι στις περιοχές μοναδικής παραγοντοποίησης τα κύρια ιδεώδη παίζουν σημαντικό ρόλο.

3.2.1 Ορισμός. *Μια ακεραία περιοχή R ονομάζεται* ***περιοχή κυρίων ιδεωδών*** *αν κάθε ιδεώδες της R είναι κύριο.*

Για παράδειγμα, ο $\mathbb{Z}$ και ο $F[x]$, όπου F σώμα, είναι περιοχές κυρίων ιδεωδών. Κάθε σώμα είναι περιοχή κυρίων ιδεωδών γιατί τα μόνα ιδεώδη σώματος είναι το $<0>$ και το $<1>$ που είναι κύρια. Ένα παράδειγμα ακεραίας περιοχής που δεν είναι περιοχή κυρίων ιδεωδών είναι ο δακτύλιος $\mathbb{Z}[x]$. Πράγματι, θεωρούμε το ιδεώδες $<2,x>=\{2f(x)+xg(x)|f(x),g(x)\in\mathbb{Z}[x]\}$. Έστω ότι $<2,x>=<h(x)>$ για κάποιο $h(x)\in F[x]$. Επειδή $x\in(2,x)$ το $h(x)$ διαιρεί το x και άρα $h(x)=\pm1$ ή $h(x)=\pm x$. Στην πρώτη περίπτωση έχουμε $\pm1=2f(x)+xg(x)$, για κάποια $f(x)$, $g(x)\in\mathbb{Z}[x]$, που βλέπουμε ότι είναι άτοπο αν θεωρήσουμε τους σταθερούς όρους. Στη δεύτερη περίπτωση, έχουμε $2\in<2,x>=<x>$, οπότε $2=xg(x)$ για κάποιο $g(x)\in\mathbb{Z}[x]$, άτοπο. Επίσης, και η ακεραία περιοχή $\mathbb{C}[x,y]$ δεν είναι περιοχή κυρίων ιδεωδών (βλ. Παράδειγμα 2.5.6 4)).

Στη συνέχεια θα αποδείξουμε ότι κάθε περιοχή κυρίων ιδεωδών είναι περιοχή μοναδικής παραγοντοποίησης, που είναι το κύριο αποτέλεσμα αυτής της Παραγράφου. Για τον σκοπό αυτό θα εφαρμόσουμε το Θεώρημα 3.1.5. Η πρώτη ιδιότητα του Θεωρήματος αυτού ισχύει για τις περιοχές κυρίων ιδεωδών:

3.2.2 Λήμμα. *Έστω R μια περιοχή κυρίων ιδεωδών. Τότε κάθε αύξουσα ακολουθία ιδεωδών του R είναι τελικά σταθερή.*

Απόδειξη. Έστω $I_1\subseteq I_2\subseteq I_3\subseteq\ldots$ μια ακολουθία ιδεωδών του R. Θεωρούμε το σύνολο $I=\bigcup_{k=1}^{\infty}I_k$. Το I είναι ένα ιδεώδες του R. Πράγματι, αν $a,b\in I$ και $r\in R$ τότε $a\in I_{k_1}$ και $b\in I_{k_2}$ για κάποια k_1 και k_2. Μπορούμε να υποθέσουμε χωρίς περιορισμό της γενικότητας ότι $k_1\leq k_2$, οπότε $I_{k_1}\subseteq I_{k_2}$ και κατά συνέπεια $a,b\in I_{k_2}$. Επειδή το I_{k_2} είναι ιδεώδες έχουμε $a-b\in I_{k_2}\subseteq I$ και επειδή το I_{k_1} είναι ιδεώδες έχουμε $ra\in I_{k_1}\subseteq I$.

Από την υπόθεση έχουμε $I =< a >$ για κάποιο $a \in R$. Άρα $a \in I_N$ για κάποιο N. Ισχυριζόμαστε ότι $I_N = I_{N+1} = I_{N+2} = \ldots$. Πράγματι, έχουμε $< a > \subseteq I_N$ και άρα $I \subseteq I_N$. Επειδή ισχύει και $I_N \subseteq I$ έχουμε $I_N = I$. Για κάθε $k \in \mathbb{N}$ ισχύει $I_N \subseteq I_{N+k} \subseteq I$ και επομένως $I_N = I_{N+k}$. ⊤

Σύμφωνα με το επόμενο Λήμμα, ισχύει και η δεύτερη ιδιότητα του Θεωρήματος 3.1.5 για τις περιοχές κυρίων ιδεωδών.

3.2.3 Λήμμα. *Έστω R μια περιοχή κυρίων ιδεωδών. Αν $p \in R$ είναι ένα ανάγωγο στοιχείο τότε το ιδεώδες $< p >$ είναι μεγιστικό.*

Απόδειξη. Έστω I ένα γνήσιο ιδεώδες του R που περιέχει το $< p >$. Θα δείξουμε ότι $I =< p >$. Από την υπόθεση στο R έχουμε $I =< a >$ για κάποιο $a \in R$. Αφού $p \in < a >$ έχουμε $a|p$ και επειδή το p είναι ανάγωγο το a θα είναι αντιστρέψιμο στοιχείο ή συντροφικό του p. Η πρώτη περίπτωση αποκλείεται γιατί $I \neq R$, ενώ στη δεύτερη περίπτωση ισχύει $< a >=< p >$ (από τη σχέση (;;) της Παραγράφου 3.1). ⊤

Από τα δύο προηγούμενα Λήμματα, το Θεώρημα 3.1.5 και τη Σημείωση 3.1.6 συμπεραίνουμε το εξής.

3.2.4 Θεώρημα. *Κάθε περιοχή κυρίων ιδεωδών είναι περιοχή μοναδικής παραγοντοποίησης.*

Σημειώνουμε ότι το αντίστροφο του προηγούμενου Θεωρήματος δεν ισχύει. Είδαμε ήδη ότι ο δακτύλιος $\mathbb{Z}[x]$ δεν είναι περιοχή κυρίων ιδεωδών. Θα αποδείξουμε στην Παράγραφο 3.4 ότι ο $\mathbb{Z}[x]$ είναι περιοχή μοναδικής παραγοντοποίησης.

Σημείωση Η ιδιότητα "κάθε αύξουσα ακολουθία ιδεωδών του R είναι τελικά σταθερή" χαρακτηρίζει μια ευρεία οικογένεια δακτυλίων. Οι δακτύλιοι αυτοί ονομάζονται δακτύλιοι της Noether προς τιμή της Emmy Noether (1882-1935) που τους μελέτησε συστηματικά. Οι δακτύλιοι της Noether είναι εξαιρετικά σημαντικοί για τη Μεταθετική Άλγεβρα, την Αλγεβρική Γεωμετρία και την Αλγεβρική Θεωρία Αριθμών. (Βλ. και την Σημείωση στο τέλος της Παραγράφου 2.5).

Ευκλείδειες περιοχές

Στις Παραγράφους 1.2 και 2.3 είδαμε ότι στο $\mathbb{Z}$ και $F[x]$, όπου F είναι ένα σώμα, υπάρχουν Αλγόριθμοι Διαίρεσης από τους οποίους έπονται θεμελιώδεις ιδιότητες των $\mathbb{Z}$ και $F[x]$. Μία από αυτές είναι η μοναδική παραγοντοποίηση σε γινόμενα αναγώγων στοιχείων. Άρα είναι φυσιολογικό, στην προσπάθειά μας να

προσδιορίσουμε και άλλες περιοχές μοναδικής παραγοντοποίησης, να θεωρήσουμε δακτυλίους που είναι εφοδιασμένοι με έναν "αλγόριθμο διαίρεσης".

3.2.5 Ορισμός. *Μια* ***Ευκλείδεια περιοχή*** *είναι μια ακεραία περιοχή R εφοδιασμένη με μία απεικόνιση $\delta : R - \{0\} \to \mathbb{Z}_{>0}$ που έχει τις ιδιότητες*

- $a|b \Rightarrow \delta(a) \leq \delta(b)$
- *Για κάθε $a, b \in R$, $a \neq 0$, υπάρχουν $q, r \in R$ με $b = qa + r$, όπου $r = 0$ ή $\delta(r) < \delta(a)$.*

Η απεικόνιση δ ονομάζεται Ευκλείδεια συνάρτηση της R.

Για παράδειγμα, η περιοχή $\mathbb{Z}$ είναι Ευκλείδεια περιοχή ως προς την απεικόνιση $\delta(m) = |m|$ (απόλυτη τιμή). Το $F[x]$, όπου F είναι ένα σώμα, είναι Ευκλείδεια περιοχή ως προς την απεικόνιση $\delta(f(x)) = \deg f(x)$ (βαθμός πολυωνύμου).

Σημειώνουμε ότι μπορεί μια περιοχή να είναι Ευκλείδεια ως προς διαφορετικές απεικονίσεις (βλ. Άσκηση 4).

Έχοντας υπόψη τα προηγούμενα παραδείγματα, το επόμενο αποτέλεσμα είναι χωρίς αμφιβολία αναμενόμενο.

3.2.6 Θεώρημα. *Κάθε Ευκλείδεια περιοχή είναι περιοχή κυρίων ιδεωδών.*

Απόδειξη. Έστω R μια Ευκλείδεια περιοχή με Ευκλείδεια απεικόνιση δ και I ένα μη μηδενικό ιδεώδες του R. Έστω $a \in I \setminus \{0\}$ με την ιδιότητα ο θετικός ακέραιος $\delta(a)$ να είναι ελάχιστος. Ισχύει $I =< a >$. Πράγματι, αν $b \in I$, τότε υπάρχουν $q, r \in R$ με $b = qa + r$, όπου $r = 0$ ή $\delta(r) < \delta(a)$. Επειδή $r = b - qa \in I$, συνάγουμε από τον ορισμό του $\delta(a)$ ότι $r = 0$. Άρα $b = qa \in < a >$ και κατά συνέπεια $I =< a >$. Συνεπώς το R είναι περιοχή κυρίων ιδεωδών. ⊤

Επομένως κάθε Ευκλείδεια περιοχή είναι περιοχή μοναδικής παραγοντοποίησης.

Στην απόδειξη του προηγούμενου Θεωρήματος δεν χρησιμοποιήσαμε την πρώτη ιδιότητα του ορισμού της Ευκλείδειας περιοχής. Αυτή χρησιμοποιείται συχνά για τον προσδιορισμό των αντιστρέψιμων στοιχείων.

3.2.7 Πρόταση. *Έστω R μια Ευκλείδεια περιοχή με Ευκλείδεια απεικόνιση δ. Τότε το $u \in R$ είναι αντιστρέψιμο αν και μόνο αν $\delta(u) = \delta(1)$.*

Απόδειξη. Αν το u είναι αντιστρέψιμο, τότε από $u|1$ παίρνουμε $\delta(u) \leq \delta(1)$. Αλλά ισχύει βέβαια $1|u$ και $\delta(1) \leq \delta(u)$. Άρα $\delta(u) = \delta(1)$. Αντίστροφα, έστω $\delta(u) = \delta(1)$. Έχουμε $1 = qu + r$ με $r = 0$ ή $\delta(r) < \delta(u)$. Αν $r \neq 0$ έχουμε $1|r$ και άρα $\delta(1) \leq \delta(r)$, δηλαδή $\delta(u) \leq (r)$, άτοπο. Έτσι $r = 0$ και επομένως το u είναι αντιστρέψιμο. ⊤

Συγκεκριμένες εφαρμογές της προηγούμενης Πρότασης θα δούμε παρακάτω.

Έχοντας υπόψη το Θεώρημα 3.2.6 είναι εύλογο να αναρωτηθούμε αν υπάρχει μια περιοχή κυρίων ιδεωδών που δεν είναι Ευκλείδεια. Το πρώτο τέτοιο παράδειγμα βρέθηκε το 1949 από τον Motzkin. Μια πιο κατατοπιστική ανάλυση αυτού του παραδείγματος υπάρχει στο άρθρο [5]. Η εν λόγω περιοχή είναι το σύνολο των μιγαδικών αριθμών της μορφής $a+bw$, όπου $a, b \in \mathbb{Z}$ και $w = \dfrac{-1+\sqrt{-19}}{2}$.

Ακέραιοι του Gauss

Θα δούμε εδώ ότι ο δακτύλιος των ακεραίων του Gauss

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} | a, b \in \mathbb{Z}\}$$

είναι Ευκλείδεια περιοχή (και άρα περιοχή κυρίων ιδεωδών και περιοχή μοναδικής παραγοντοποίησης). Ως εφαρμογή της μοναδικής παραγοντοποίησης στο $\mathbb{Z}[i]$ θα λύσουμε μια Διοφαντική εξίσωση που οφείλεται στο Fermat. Στην επόμενη Παράγραφο θα ασχοληθούμε πιο συστηματικά με το $\mathbb{Z}[i]$: θα περιγράψουμε τα ανάγωγα στοιχεία του και θα δούμε ως εφαρμογή μερικά κλασσικά αποτελέσματα που αφορούν αθροίσματα τετραγώνων ακεραίων.

Αν $z = a + bi \in \mathbb{C}$, όπου $a, b \in \mathbb{R}$, θέτουμε $\delta(z) = (a+bi)(a-bi) = a^2 + b^2$ και υπενθυμίζουμε ότι $\delta(zz') = \delta(z)\delta(z')$ για κάθε $z, z' \in \mathbb{C}$. Επομένως ο περιορισμός της απεικόνισης δ στο $\mathbb{Z}[i] - \{0\}$, που συμβολίζουμε πάλι με δ, ικανοποιεί την πρώτη ιδιότητα του Ορισμού 3.2.5. Για τη δεύτερη ιδιότητα, έστω $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$. Ο μιγαδικός αριθμός $a + bi$ $(a, b \in \mathbb{R})$ παριστάνεται στο πραγματικό επίπεδο από το σημείο (a, b). Αν $a + bi \in \mathbb{Z}[i]$, τότε το σημείο (a, b) έχει ακέραιες συντεταγμένες και τα σημεία αυτά αποτελούν κορυφές τετραγώνων με μήκος πλευράς 1. Θεωρούμε το $\alpha/\beta \in \mathbb{C}$. Επειδή το μήκος κάθε διαγωνίου τετραγώνου με πλευρά μηκους 1 είναι $\sqrt{2}$, υπάρχει κορυφή τετραγώνου από την οποία το σημείο α/β απέχει απόσταση μικρότερη ή ίση του $\sqrt{2}/2$. Έστω q μια τέτοια κορυφή. Έχουμε

$$|\alpha/\beta - q| \leq \sqrt{2}/2 < 1.$$

Θέτοντας $r = \alpha - \beta q$ έχουμε

$$\alpha = \beta q + r \quad \text{και} \quad |r| = |\alpha - \beta q| = |\beta||\alpha/\beta - q| < |\beta|.$$

Επομένως ισχύει $\delta(r) = |r|^2 < |\beta|^2 = \delta(\beta)$ και ο $\mathbb{Z}[i]$ είναι Ευκλείδεια περιοχή ως προς τη συνάρτηση δ. Αν $u = u_0 + u_1 i$ είναι ένα αντιστρέψιμο στοιχείο του $\mathbb{Z}[i]$, τότε από την Πρόταση 3.2.7 έχουμε

$$\delta(u) = \delta(1) = 1 \Rightarrow u_0^2 + u_1^2 = 1 \Rightarrow u = \pm 1, \pm i$$

γιατί $u_0, u_1 \in \mathbb{Z}$. Συνοψίζοντας τα παραπάνω έχουμε αποδείξει το εξής.

3.2.8 Θεώρημα. *Ο δακτύλιος των ακεραίων του Gauss* $\mathbb{Z}[i] = \{a+bi \in \mathbb{C} | a, b \in \mathbb{Z}\}$ *είναι μία Ευκλείδεια περιοχή ως προς την απεικόνιση που ορίζεται από τη σχέση* $\delta(a+bi) = a^2 + b^2$. *Το σύνολο των αντιστρέψιμων στοιχείων του* $\mathbb{Z}[i]$ *είναι το* $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

3.2.9 Παρατηρήσεις.

1) Η ακόλουθη απλή παρατήρηση είναι συχνά χρήσιμη όταν αναζητούμε ανάγωγα στοιχεία του $\mathbb{Z}[i]$. Αν $\alpha \in \mathbb{Z}[i]$ είναι τέτοιο ώστε $\delta(\alpha) = p$, όπου p είναι ένας πρώτος αριθμός, τότε το α είναι ανάγωγο. Πράγματι, αν $\alpha = \beta\gamma$ τότε $p = \delta(\alpha) = \delta(\beta)\delta(\gamma)$ και άρα $\delta(\beta) = 1$ ή $\delta(\gamma) = 1$, δηλαδή το β ή το γ είναι αντιστρέψιμο. Για παράδειγμα, το $2 + i$ είναι ανάγωγο αφού $\delta(2 + i) = 5$. Η συνθήκη αυτή, όμως, δεν είναι αναγκαία αφού, για παράδειγμα, το 3 είναι ανάγωγο στο $\mathbb{Z}[i]$ (άσκηση) αλλά $\delta(3) = 9$ που δεν είναι πρώτος. Επίσης δεν αληθεύει ότι κάθε πρώτος αριθμός p είναι ανάγωγο στοιχείο του $\mathbb{Z}[i]$. Για παράδειγμα, $5 = (2 + i)(2 - i)$, και τα $2 + i, 2 - i$, είναι ανάγωγα αφού $\delta(2+i) = \delta(2-i) = 5$ που είναι πρώτος. Περισσότερα επί αυτού θα δούμε στην επόμενη Παράγραφο (Θεώρημα 3.3.3).

2) Ας βρούμε την παραγοντοποίηση του $1+3i$ σε γινόμενο αναγώγων. Επειδή $\delta(1 + 3i) = 10$ και η συνάρτηση δ ικανοποιεί τη σχέση $\delta(xy) = \delta(x)\delta(y)$ εξετάζουμε αν υπάρχουν $a+bi$ με $\delta(a+bi) = 2$ ή 5. Έχουμε $\delta(1+i) = 2$. Διαιρούμε το $1+3i$ με το $1+i$ στο $\mathbb{C}$ και παρατηρούμε ότι το πηλίκο $2+i$ είναι στοιχείο του $\mathbb{Z}[i]$ (αν δεν ήταν θα απορρίπταμε το $1 + i$ ως διαιρέτη). Στη συνέχεια επαναλαμβάνεται η διαδικασία για το πηλίκο και ούτω κάθ΄ εξής. Στο συγκεκριμένο παράδειγμα, όμως, το $\delta(2 + i) = 5$ είναι πρώτος. Από την προηγούμενη παρατήρηση το $2 + i$ είναι ανάγωγο. Με παρόμοιο τρόπο διαπιστώνουμε ότι είναι ανάγωγο και το $1 + i$. Τελικά, η ζητούμενη παραγοντοποίηση είναι $1 + 3i = (1 + i)(2 + i)$.

3) Για κάθε μη μηδενικό $\alpha \in \mathbb{Z}[i]$, ο δακτύλιος πηλίκο $\mathbb{Z}[i]/ < \alpha >$ είναι πεπερασμένος. Πράγματι, κάθε κλάση modulo(α) είναι της μορφής $\beta + < \alpha >$, όπου $\beta \in \mathbb{Z}[i]$. Υπάρχουν $q, r \in \mathbb{Z}[i]$ τέτοια ώστε $\beta = q\alpha + r$ και $r = 0$ ή $\delta(r) < \delta(\alpha)$. Τότε $\beta + < \alpha >= r + < \alpha >$. Αλλά υπάρχουν πεπερασμένα το πλήθος r με $\delta(r) < \delta(\alpha)$, αφού η Διοφαντική εξίσωση $x^2 + y^2 = z$, όπου $z < \delta(\alpha)$, έχει προφανώς πεπερασμένο πλήθος λύσεων .

4) Ο δακτύλιος $\mathbb{Z}[i]$ είναι ένας από μια οικογένεια δακτυλίων της μορφής $\mathbb{Z}[\sqrt{d}] = \{a+b\sqrt{d} \in \mathbb{C} | a, b \in \mathbb{Z}\}$, όπου ο $d \in \mathbb{Z}$ δεν διαιρείται με το τετράγωνο ακεραίου μεγαλύτερου του 1. Για $d = -5$, είδαμε στο Παράδειγμα 3.1.3 ότι ο δακτύλιος $\mathbb{Z}[\sqrt{d}]$ δεν είναι περιοχή μοναδικής παραγοντοποίησης και άρα δεν είναι Ευκλείδεια περιοχή. Σημειώνουμε ότι για $d < 0$ ο

$\mathbb{Z}[\sqrt{d}]$ είναι περιοχή μοναδικής παραγοντοποίησης αν και μόνο αν $d = -1$ ή -2 (Άσκηση 22). Για θετικά d το ερώτημα ποιοι από τους $\mathbb{Z}[\sqrt{d}]$ είναι περιοχές μοναδικής παραγοντοποίησης παραμένει μέχρι σήμερα ανοικτό.

Εφαρμογή σε Διοφαντικές εξισώσεις

Γνωρίζουμε από την προηγούμενη Παράγραφο ότι υπάρχουν δακτύλιοι που, αν και περιέχουν το $\mathbb{Z}$, δεν είναι περιοχές μοναδικής παραγοντοποίησης. Η περίπτωση όμως που ένας δακτύλιος περιέχει το $\mathbb{Z}$ και έχει την ιδιότητα της μοναδικής παραγοντοποίησης είναι συχνά χρήσιμη στην επίλυση Διοφαντικών εξισώσεων, γιατί μπορούμε τότε να εργαστούμε στον ευρύτερο δακτύλιο και να χρησιμοποιήσουμε ιδιότητές του.

Για την εφαρμογή της μοναδικής παραγοντοποίησης του $\mathbb{Z}[i]$ που ακολουθεί, χρειαζόμαστε πρώτα ένα Λήμμα. Υπενθυμίζουμε ότι δύο μη μηδενικά στοιχεία a, b μιας περιοχής μοναδικής παραγοντοποίησης R λέγονται σχετικά πρώτα αν δεν υπάρχει ανάγωγο $p \in R$ τέτοιο ώστε $p|a$ και $p|b$. Γνωρίζουμε από την Ενότητα 1 ότι αν το γινόμενο ab δύο σχετικά πρώτων θετικών ακεραίων είναι n-στή δύναμη ακεραίου, τότε οι a, b είναι n-στές δυνάμεις. Θα χρειαστούμε μια γενίκευση αυτού.

3.2.10 Λήμμα. *Έστω R μια περιοχή μοναδικής παραγοντοποίησης και $a, b, c \in R$ με $ab = c^n$, $n > 0$. Αν τα a, b είναι σχετικά πρώτα, τότε υπάρχουν $d, e \in R$ και αντιστρέψιμα $u, v \in R$ τέτοια ώστε $a = ud^n$ και $b = ve^n$.*

Απόδειξη. Έστω

$$c = wp_1^{c_1} \dots p_r^{c_k},$$

όπου το w είναι αντιστρέψιμο, τα p_i είναι ανά δύο μη συντροφικά ανάγωγα στοιχεία και οι c_i είναι θετικοί ακέραιοι. Επειδή έχουμε $ab = c^n$, από τη μοναδικότητα της παραγοντοποίησης στο R συμπεραίνουμε ότι

$$a = up_1^{a_1} \dots p_r^{a_k}, \quad b = \nu p_1^{b_1} \dots p_r^{b_k},$$

όπου $u\nu = w^n$ και $a_i, b_i \in \mathbb{N}$ με $a_i + b_i = nc_i$. Επειδή τα a, b είναι σχετικά πρώτα στοιχεία, βλέπουμε ότι για κάθε i ακριβώς ένα από τα a_i, b_i είναι 0. Συνεπώς

$$a = up_{i_1}^{nc_{i_1}} \dots p_{i_s}^{nc_{i_s}}, \quad b = \nu p_{j_1}^{nc_{j_1}} \dots p_{j_t}^{nc_{j_t}},$$

και $\{i_1, \dots, i_s, j_1, \dots, j_t\} = \{1, 2, \dots, r\}$. Θέτουμε $d = p_{i_1}^{c_{i_1}} \dots p_{i_s}^{c_{i_s}}$ και $e = p_{j_1}^{c_{j_1}} \dots p_{j_t}^{c_{j_t}}$. ∎

3.2.11 Εφαρμογή (Fermat). Θα αποδείξουμε ότι οι λύσεις της Διοφαντικής εξίσωσης

$$2x^3 = y^2 + 1$$

είναι οι $(x, y) = (1, 1), (1, -1)$.

Έστω $x, y \in \mathbb{Z}$ τέτοιοι ώστε $2x^3 = y^2 + 1$. Παρατηρούμε ότι ο y είναι περιττός. Στο $\mathbb{Z}[i]$ θεωρούμε την παραγοντοποίηση

$$(y + i)(y - i) = 2x^3. \tag{1}$$

Κάθε κοινός διαιρέτης των $y + i$ και $y - i$ διαιρεί το $(y + i) - (y - i) = 2i = (1 + i)^2$. Το $1 + i$ είναι ανάγωγο από την Παρατήρηση 3.2.9 1) και επομένως από τη μοναδικότητα της παραγοντοποίησης στο $\mathbb{Z}[i]$ παίρνουμε ότι κάθε κοινός διαιρέτης των $y+i$ και $y-i$ είναι συντροφικός με έναν από τους $1, 1+i, (1+i)^2$. Επειδή ο y είναι περιττός έχουμε $y + i = 2k + 1 + i$, για κάποιο $k \in \mathbb{Z}$, και άρα το $y+i$ διαιρείται με το $1+i$ αλλά όχι με το $(1+i)^2$. Επίσης το $1+i$ διαιρεί το $y - i = 2k + 1 - i$. Συνεπώς ένας *μκδ* των $y + i$ και $y - i$ είναι το $1 + i$, οπότε έχουμε

$$y + i = (1 + i)(a + bi) \quad \text{και} \quad y - i = (1 + i)(c + di),$$

όπου τα $a+bi, c+di \in \mathbb{Z}[i]$ είναι σχετικά πρώτα στοιχεία. Χρησιμοποιώντας την (;;) λαμβάνουμε

$$(ix)^3 = (a + bi)(c + di).$$

Από το Λήμμα 3.2.10 έπεται ότι υπάρχει αντιστρέψιμο $u \in \mathbb{Z}[i]$ και $\gamma + \delta i \in \mathbb{Z}[i]$ με $a + bi = u(\gamma + \delta i)^3$. Επειδή κάθε αντιστρέψιμο στοιχείο του $\mathbb{Z}[i]$ είναι τρίτη δύναμη στο $\mathbb{Z}[i]$, μπορούμε να υποθέσουμε ότι $u = 1$ (γιατί αν $u = \nu^3$, τότε $u(\gamma + \delta i)^3 = \nu^3(\gamma + \delta i)^3 = (\nu\gamma + \nu\delta i)^3$). Έχουμε

$$\begin{aligned} y + i &= (1 + i)(a + bi) = (1 + i)(\gamma + \delta i)^3 = \\ &= (\gamma^3 - 3\gamma^2\delta - 3\gamma\delta^2 + \delta^3) + (\gamma^3 + 3\gamma^2\delta - 3\gamma\delta^2 - \delta^3)i, \end{aligned}$$

και κατά συνέπεια λαμβάνουμε το σύστημα

$$\begin{aligned} y &= \gamma^3 - 3\gamma^2\delta - 3\gamma\delta^2 + \delta^3 = (\gamma + \delta)(\gamma^2 - 4\gamma\delta + \delta^2) \\ 1 &= \gamma^3 + 3\gamma^2\delta - 3\gamma\delta^2 - \delta^3 = (\gamma - \delta)(\gamma^2 + 4\gamma\delta + \delta^2). \end{aligned}$$

Επειδή $\gamma, \delta \in \mathbb{Z}$, εύκολα διαπιστώνουμε από την δεύτερη εξίσωση του συστήματος ότι $(\gamma, \delta) = (1, 0), (0, -1)$. Αντικαθιστώντας στην πρώτη βρίσκουμε ότι $y = \pm 1$, οπότε $x = 1$.

Με παρόμοιο τρόπο μπορεί να αποδειχτεί ότι οι λύσεις της Διοφαντικής εξίσωσης,

$$x^3 = y^2 + 4,$$

που επίσης μελετήθηκε από τον Fermat, είναι οι $(x, y) = (2, \pm 2), (5, \pm 11)$. Πράγματι, αν ο x είναι άρτιος τότε και ο y είναι άρτιος, οπότε γράφοντας $x = 2X$

και $y = 2Y$ παίρνουμε την εξίσωση $2X^3 = Y^2 + 1$ που λύσαμε προηγουμένως. Άρα μπορούμε να υποθέσουμε ότι ο x είναι περιττός. Με την υπόθεση αυτή μπορούμε να αποδείξουμε ότι τα στοιχεία $2 + yi, 2 - yi$ είναι σχετικά πρώτα στο $\mathbb{Z}[i]$. Επομένως εφαρμόζουμε το Λήμμα 3.2.10 στη σχέση $(2+yi)(2-yi) = x^3$. Το σύστημα που προκύπτει εδώ είναι το

$$2 = \gamma(\gamma^2 - 3\delta^2),$$
$$y = \delta(3\gamma^2 - \delta^2)$$

που εύκολα επιλύεται αφού $\gamma, \delta \in \mathbb{Z}$. Οι λεπτομέρειες αφήνονται σαν άσκηση.

Ασκήσεις 3.2

Στις παρακάτω ασκήσεις υποθέτουμε ότι όλοι οι δακτύλιοι είναι ακέραιες περιοχές.

1. Να βρεθεί ένα $d \in \mathbb{Z}[i]$ τέτοιο ώστε $< 2 > + < 3 + 3i > = < d >$.

2. Έστω R μια περιοχή κυρίων ιδεωδών και $a, b \in R$. Τότε $< a > + < b > = < d >$ αν και μόνο αν το d είναι ένας *μκδ* των a, b.

3. Στον ορισμό της Ευκλείδειας περιοχής, τα q, r δεν είναι αναγκαστικά μοναδικά.
   Υπόδειξη: Στο $\mathbb{Z}[i]$, έστω $a = 5 + 3i, b = -4 + i$. Ένα q είναι το $-1 + i$ και ένα άλλο είναι το -1.

4. Η περιοχή $\mathbb{Z}$ είναι Ευκλείδεια περιοχή ως προς την απεικόνιση δ_k που ορίζεται από $\delta_k(m) = |m| + k$, όπου $k \in \mathbb{N}$.

5. Έστω R μια περιοχή κυρίων ιδεωδών και $a \in R$, $a \neq 0$. Αποδείξτε ότι το πλήθος των ιδεωδών του R που περιέχουν το $< a >$ είναι πεπερασμένο.

6. Έστω R μια περιοχή κυρίων ιδεωδών και $p \in R$, $p \neq 0$. Αποδείξτε ότι το ιδεώδες $< p >$ είναι μεγιστικό αν και μόνο αν το p είναι ανάγωγο.

7. Κάθε γνήσιο ιδεώδες μιας περιοχής κυρίων ιδεωδών περιέχεται σε μεγιστικό ιδεώδες.

8. Έστω $R = \{\frac{m}{n} | m, n \in \mathbb{Z}, n \text{ περιττός}\}$. Αποδείξτε ότι:

   a. Ο R είναι μια ακεραια περιοχή που περιέχει το $\mathbb{Z}$.

b. Τα στοιχεία της μορφής $\frac{m}{n}$ με m, n περιττούς είναι αντιστρέψιμα.

c. Κάθε μη μηδενικό ιδεώδες του R περιέχει στοιχείο της μορφής 2^t για κάποιο $t > 0$.

d. Η περιοχή R είναι περιοχή κυρίων ιδεωδών.
Υπόδειξη: Αν I είναι μη μηδενικό ιδεώδες του R, αποδείξτε ότι $I =< 2^k >$, όπου k είναι ελάχιστο με την ιδιότητα $2^k \in I$.

9. Εξετάστε αν αληθεύουν οι παρακάτω προτάσεις.

a. R Ευκλείδεια περιοχή $\Rightarrow R[x]$ Ευκλείδεια περιοχή.

b. R περιοχή κυρίων ιδεωδών $\Rightarrow R[x]$ περιοχή κυρίων ιδεωδών.

10. Έστω R μία περιοχή κυρίων ιδεωδών και $p \in R - \{0\}$. Τα ακολουθα είναι ισοδύναμα

a. p είναι ανάγωγο

b. $R/ < p >$ είναι σώμα

c. $R/ < p >$ είναι ακεραία περιοχή.

11. Κάθε μη μηδενικό πρώτο ιδεώδες περιοχής κυρίων ιδεωδών είναι μεγιστικό.

12. Αποδείξτε ότι αν ο $R[x]$ είναι περιοχή κυρίων ιδεωδών, τότε ο R σώμα.
Υπόδειξη: Θεωρήστε τον επιμορφισμό $R[x] \ni f(x) \mapsto f(0) \in R$. Ο πυρήνας είναι το $< x >$. Εφαρμόστε το Λήμμα 3.2.3.

13. Έστω R μια περιοχή με την ιδιότητα: κάθε γνήσια φθίνουσα ακολουθία ιδεωδών $I_1 \supsetneq I_2 \supsetneq \ldots$ είναι πεπερασμένη. Αποδείξτε ότι ο R είναι σώμα.
Υπόδειξη: Για να δείξετε ότι το $a \neq 0$ είναι αντιστρέψιμο, θεωρήστε την ακολουθία $< a > \supseteq < a^2 > \supseteq \ldots$

14. Έστω $\varphi : R \to S$ ένας επιμορφισμός δακτυλίων, όπου ο R είναι περιοχή κυρίων ιδεωδών. Τότε κάθε ιδεώδες του S είναι κύριο.

15. Έστω $\varphi : R \to S$ ένας επιμορφισμός δακτυλίων, όπου ο R είναι περιοχή κυρίων ιδεωδών και ο S ακεραία περιοχή. Αποδείξτε ότι αν ο φ δεν είναι ισομορφισμός, τότε το S είναι σώμα.
Υπόδειξη: Ο πυρήνας είναι μη μηδενικό πρώτο ιδεώδες. Εφαρμόστε την Άσκηση 11.

16. Έστω R ένας δακτύλιος με $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$. Αποδείξτε ότι το R είναι περιοχή κυρίων ιδεωδών.
Υπόδειξη: Αν I είναι ένα ιδεώδες του R θεωρήστε το σύνολο $Z \cap I$.

17. Αποδείξτε ότι $\mathbb{Z}[i]/ < 1+i > \cong \mathbb{Z}_2$.

18. Να προσδιοριστεί ένα m τέτοιο ώστε $\mathbb{Z}[i]/ < 1+3i > \cong \mathbb{Z}_m$.
Υπόδειξη: Αναλύστε το $1+3i$ σε γινόμενο αναγώγων και εφαρμόστε το Κινεζικό Θεώρημα Υπολοίπων (Άσκηση 2.6.19).

19. Στο $\mathbb{Z}[i]$, που είναι περιοχή μοναδικής παραγοντοποίησης, έχουμε $10 = 2 \cdot 5 = (1+3i)(1-3i)$. Εξηγήστε.

20. Αποδείξτε ότι ο $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \in \mathbb{C} | a, b \in \mathbb{Z}\}$ είναι Ευκλείδεια περιοχή ως προς την απεικόνιση $\delta(a + b\sqrt{-2}) = a^2 + 2b^2$.

21. Συμπληρώστε την απόδειξη ότι οι λύσεις της Διοφαντικής εξίσωσης $x^3 = y^2 + 4$ είναι οι $(x, y) = (2, \pm 2), (5, \pm 11)$. (Βλ. την Εφαρμογή 3.2.11).

22. Έστω n ένας αρνητικός ακέραιος που δεν διαιρείται με το τετράγωνο ακεραίου μεγαλύτερου του 1. Αποδείξτε ότι:

    a. Αν $n \leq -2$, τότε τα μοναδικά αντιστρέψιμα στοιχεία του δακτυλίου $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \in \mathbb{C} | a, b \in \mathbb{Z}\}$ είναι τα ± 1.

    b. Ο δακτύλιος $\mathbb{Z}[\sqrt{n}]$ είναι περιοχή μοναδικής παραγοντοποίησης αν και μόνο αν $n = -1, -2$.
    Υπόδειξη: Υποθέτοντας ότι $n < -2$ και ότι ο δακτύλιος είναι περιοχή μοναδικής παραγοντοποίησης αποδείξτε με τη βοήθεια της συνάρτησης $\delta(a+b\sqrt{n}) = a^2 - nb^2$, ότι το 2 είναι ανάγωγο. Αυτό είναι άτοπο λόγω της Άσκησης 3.1.11. Για το αντίστροφο, δες την Άσκηση 20.

3.3 Εφαρμογές: Αθροίσματα Τετραγώνων

Χρησιμοποιώντας τη μοναδικότητα της παραγοντοποίησης στο $\mathbb{Z}[i]$ θα αποδείξουμε εδώ ένα θεώρημα του Fermat που περιγράφει τους φυσικούς αριθμούς που μπορούν να παρασταθούν ως άθροισμα δύο τετραγώνων φυσικών αριθμών. Στη συνέχεια θα αποδείξουμε ένα Θεώρημα του Lagrange που λέει ότι κάθε φυσικός αριθμός είναι άθροισμα τεσσάρων τετραγώνων.

Οι πρώτοι p της μορφής $p = x^2 + y^2$

Εστιάζοντας αρχικά την προσοχή μας στους πρώτους αριθμούς, παρατηρούμε ότι $2 = 1^2 + 1^2$, $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, $29 = 2^2 + 5^2$, ενώ οι $3, 7, 11, 19, 23$ δεν μπορούν να παρασταθούν ως άθροισμα δύο τετραγώνων. Το επόμενο αποτέλεσμα μας λέει ότι ο πρώτος $p \neq 2$ είναι άθροισμα δύο τετραγώνων αν και μόνο αν $p \equiv 1 \mod 4$.

3.3.1 Θεώρημα. *Έστω $p > 2$ ένας πρώτος αριθμός. Τα ακόλουθα είναι ισοδύναμα*

1. $p \equiv 1 \mod 4$
2. *το p δεν είναι ανάγωγο στοιχείο του $\mathbb{Z}[i]$*
3. *υπάρχουν ακέραιοι a, b τέτοιοι ώστε $p = a^2 + b^2$.*

Απόδειξη. $1 \Rightarrow 2$. Έστω $p \equiv 1 \mod 4$. Τότε $(-1)^{\frac{p-1}{2}} = 1$. Επομένως από το κριτήριο του Euler (Εφαρμογή 2.4.4) έπεται ότι υπάρχει $q \in \mathbb{Z}$ τέτοιος ώστε

$$q^2 \equiv -1 \mod p.$$

Το p διαιρεί το $q^2 + 1$ στο $\mathbb{Z}$ και κατά συνέπεια διαιρεί το $(q+i)(q-i)$ στο $\mathbb{Z}[i]$. Για να δείξουμε ότι το p δεν είναι ανάγωγο στοιχείο στο $\mathbb{Z}[i]$, θα δείξουμε ότι το p δεν διαιρεί κανένα από τα $q+i, q-i$ στο $\mathbb{Z}[i]$. Αυτό αρκεί γιατί ο $\mathbb{Z}[i]$ είναι περιοχή μοναδικής παραγοντοποίησης. Έστω $p|q+i$. Τότε $q + i = p(a + bi)$, για κάποια $a, b \in \mathbb{Z}$, και επομένως $1 = pb$, που είναι άτοπο. Με παρόμοιο τρόπο αποδεικνύεται ότι το p δεν διαιρεί το $q - i$.
$2 \Rightarrow 3$. Προφανώς το p δεν είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}[i]$. Αφού το p δεν είναι ανάγωγο στο $\mathbb{Z}[i]$ έχουμε $p = (a + bi)(c + di)$ για κάποια μη αντιστρέψιμα στοιχεία $a + bi, c + di \in \mathbb{Z}[i]$. Επομένως $\delta(p) = \delta(a + bi)\delta(c + di)$, όπου δ είναι η συνάρτηση που είδαμε στο Θεώρημα 3.2.8. Άρα $p^2 = (a^2 + b^2)(c^2 + d^2)$. Επειδή $a^2 + b^2, c^2 + d^2 > 1$, από τη μοναδικότητα της παραγοντοποίησης στο $\mathbb{Z}$ παίρνουμε $p = a^2 + b^2 (= c^2 + d^2)$.
$3 \Rightarrow 1$. Έστω $p = a^2 + b^2$, όπου $a, b \in \mathbb{Z}$. Επειδή το τετράγωνο κάθε ακεραίου

είναι ισότιμο με $0, 1 \mod 4$ παίρνουμε $p \equiv 0, 1, 2 \mod 4$. Αλλά ο p είναι περιττός ακέραιος διάφορος του 2. Άρα $p \equiv 1 \mod 4$. ⊤

Σημειώσεις
1) Στην εκφώνηση του προηγούμενου Θεωρήματος δεν συμπεριλάβαμε τον πρώτο 2. Στον δακτύλιο $\mathbb{Z}[i]$ το στοιχείο 2 δεν είναι ανάγωγο, αφού $2 = -i(1+i)^2$ και το $1+i$ είναι ανάγωγο (γιατί $\delta(1+i) = 2$ που είναι πρώτος αριθμός, βλ Παρατήρηση 3.2.9 1)).
2) Επισημαίνουμε ότι αν ο πρώτος p γράφεται ως άθροισμα δύο τετραγώνων μη αρνητικών ακεραίων, $p = a^2 + b^2$, τότε οι a, b είναι "ουσιαστικά" μοναδικοί. Βλ. Άσκηση 5.

Οι φυσικοί αριθμοί n της μορφής $n = x^2 + y^2$

Έχουμε προσδιορίσει τους πρώτους αριθμούς που παρίστανται ως άθροισμα δύο τετραγώνων ακεραίων. Θα χαρακτηρίσουμε τώρα τους φυσικούς αριθμούς που παρίστανται ως άθροισμα δύο τετραγώνων. Από τη στοιχειώδη ταυτότητα

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \tag{1}$$

συμπεραίνουμε ότι το γινόμενο δύο ακεραίων που γράφονται ως αθροίσματα δύο τετραγώνων είναι άθροισμα δύο τετραγώνων. Συνεπώς, από το Θεώρημα 3.3.1 έχουμε ότι κάθε δύναμη p^m, όπου $p \equiv 1 \mod 4$, είναι άθροισμα δύο τετραγώνων. Το ίδιο συμβαίνει για τις δυνάμεις 2^m. Έστω

$$n = 2^{n_0} p_1^{n_1} \dots p_r^{n_r} p_{r+1}^{n_{r+1}} \dots p_s^{n_s}$$

η παραγοντοποίηση του n σε γινόμενο πρώτων, όπου

$$p_1, \dots, p_r \equiv 1 \mod 4 \text{ και } p_{r+1}, \dots, p_s \equiv 3 \mod 4.$$

Καθένας από τους παράγοντες $2^{n_0}, p_1^{n_1}, \dots, p_r^{n_r}$ είναι άθροισμα δύο τετραγώνων και συνεπώς το γινόμενό τους είναι άθροισμα δύο τετραγώνων. Αν υποθέσουμε ότι οι εκθέτες $n_{r+1}, \dots, n_s$ είναι άρτιοι, τότε βέβαια καθένας από τους $p_{r+1}^{n_{r+1}}, \dots, p_s^{n_s}$ είναι άθροισμα δύο τετραγώνων (κατά τετριμμένο τρόπο), οπότε από την (;;) συμπεραίνουμε ότι το n είναι άθροισμα δύο τετραγώνων. Θα αποδείξουμε στη συνέχεια ότι ισχύει και το αντίστροφο:

3.3.2 Θεώρημα. *Ένας φυσικός αριθμός n γράφεται ως άθροισμα δύο τετραγώνων φυσικών αριθμών αν και μόνο αν στην ανάλυση του n σε γινόμενο πρώτων ο εκθέτης κάθε πρώτου p με $p \equiv 3 \mod 4$ είναι άρτιος.*

Για παράδειγμα, ο $2002 = 2 \cdot 7 \cdot 11 \cdot 13$ δεν γράφεται ως άθροισμα δύο τετραγώνων, ενώ ο $154154 = 2 \cdot 7^2 \cdot 11^2 \cdot 13$ γράφεται.

Για την απόδειξη του προηγουμένου Θεωρήματος θα χρειαστούμε τα ανάγωγα στοιχεία του $\mathbb{Z}[i]$.

3.3.3 Θεώρημα. *Τα ανάγωγα στοιχεία του $\mathbb{Z}[i]$ είναι τα ακόλουθα:*

1) $\pm p$, $\pm ip$, *όπου* $p \in \mathbb{N}$ *είναι πρώτος με* $p \equiv 3 \mod 4$

2) $a + bi \in \mathbb{Z}[i]$, *όπου* $a^2 + b^2$ *είναι πρώτος.*

Απόδειξη. Από το Θεώρημα 3.3.1 και το γεγονός ότι τα ± 1, $\pm i$ είναι αντιστρέψιμα στο $\mathbb{Z}[i]$, προκύπτει αμέσως ότι τα στοιχεία του 1) είναι ανάγωγα. Στην Παρατήρηση 3.2.9 1) είδαμε ότι τα στοιχεία στην περίπτωση 2) του θεωρήματος είναι επίσης ανάγωγα.

Αντίστροφα, έστω $a + bi \in \mathbb{Z}[i]$ ένα ανάγωγο στοιχείο.

Αν $b = 0$, τότε επειδή το $a \in \mathbb{Z}$ είναι ανάγωγο, ο $|a|$ ειναι πρώτος. Από το Θεώρημα 3.2.1, έπεται ότι $a \equiv 3 \mod 4$.

Αν $a = 0$, αποδεικνύεται με παρόμοιο τρόπο ότι $b = \pm p$, όπου p πρώτος με $p \equiv 3 \mod 4$.

Έστω τώρα $a, b \neq 0$. Ως εικόνα αναγώγου στοιχείου κάτω από έναν ισομορφισμό δακτυλίων το $a - bi \in \mathbb{Z}[i]$ είναι ανάγωγο (Άσκηση 3.1.8). Έχουμε

$$a^2 + b^2 = (a + bi)(a - bi).$$

Έστω $a^2+b^2 = cd$, με $c, d \in \mathbb{N}$, $c, d > 1$. Αν τα c, d ήταν ανάγωγα στο $\mathbb{Z}[i]$, τότε από την ισότητα $(a + bi)(a - bi) = cd$ και το γεγονός ότι ο δακτύλιος $\mathbb{Z}[i]$ είναι περιοχή μοναδικής παραγοντοποίησης θα παίρναμε ότι το $a+bi$ είναι συντροφικό με το c ή d, πράγμα άτοπο. Αν ένα από τα c, d δεν ήταν ανάγωγο, τότε η ισότητα $(a + bi)(a - bi) = cd$ οδηγεί πάλι σε άτοπο αφού στο αριστερό μέλος έχουμε γινόμενο δύο αναγώγων στοιχείων και στο δεξιό έχουμε γινόμενο τουλάχιστον τριών. Αποδείξαμε ότι ο $a^2 + b^2$ είναι πρώτος αριθμός. ⊤

Είμαστε τώρα σε θέση να αποδείξουμε το Θεώρημα 3.3.2.

Απόδειξη του Θεωρήματος 3.3.2. Η μία κατεύθυνση έχει ήδη αποδειχτεί στα σχόλια που προηγήθηκαν της εκφώνησης του Θεωρήματος. Έστω τώρα $n = a^2 + b^2$, όπου $a, b \in \mathbb{Z}$. Τότε

$$n = (a + ib)(a - ib).$$

Έστω

$$a + ib = \pi_1 \dots \pi_r (a_1 + ib_1) \dots (a_s + ib_s)$$

η παραγοντοποίηση του $a + ib$ σε γινόμενο αναγώγων, όπου τα π_j είναι της μορφής $\pm p_j$ ή $\pm ip_j$ ($p_j \in \mathbb{Z}$ είναι πρώτος και $p_j \equiv 3 \mod 4$) και για τα $a_j + ib_j \in \mathbb{Z}[i]$ ισχύει ότι οι $a_j^2 + b_j^2$ είναι πρώτοι αριθμοί (Θεώρημα 3.3.3). Θεωρώντας συζυγείς μιγαδικούς παίρνουμε

$$a - ib = \overline{\pi_1} \dots \overline{\pi_r} (a_1 - ib_1) \dots (a_s - ib_s)$$

και κατά συνέπεια

$$n = |\pi_1|^2 \dots |\pi_r|^2 (a_1^2 + b_1^2) \dots (a_s^2 + b_s^2). \tag{2}$$

Για κάθε $j = 1, \dots, r$ ισχύει $|\pi_j|^2 = p_j^2$ και $p_j \equiv 3 \mod 4$. Καθένας από τους $a_j^2 + b_j^2 (j = 1, \dots, s)$ είναι ένας πρώτος αριθμός που δεν είναι ισότιμος με το 3 modulo 4 (Θεώρημα 3.3.1). Συνεπώς ο εκθέτης στο δεξιό μέλος της (;;) κάθε πρώτου που είναι ισότιμος με το 3 modulo 4 είναι άρτιος αριθμός. ⊤

Σχόλια

Εδώ εγείρονται πολλά ενδιαφέροντα ερωτήματα. Για παράδειγμα, υπάρχει k τέτοιος ώστε κάθε φυσικός αριθμός να είναι άθροισμα k τετραγώνων; Αν ναι ποιο είναι ένα k; Επειδή το 7 δεν γράφεται ως άθροισμα 3 τετραγώνων, βλέπουμε ότι αν υπάρχει k, τότε $k \geq 4$. Ο Lagrange απέδειξε ότι το ελάχιστο k είναι 4: *κάθε φυσικός αριθμός αριθμός είναι άθροισμα 4 τετραγώνων.* Αρκετές αποδείξεις αυτού είναι γνωστές σήμερα. Στο βιβλίο των Hardy και Wright [13] υπάρχουν τρεις. Μια άλλη απόδειξη δίνουμε παρακάτω.

Ποιο γενικά, δοθέντος του n υπάρχει $g(n)$ τέτοιος ώστε κάθε φυσικός αριθμός να είναι άθροισμα $g(n)$ το πλήθος n-στών δυνάμεων; Αυτό είναι γνωστό ως το ***πρόβλημα του Waring*** (ο οποίος το μελέτησε το 1770). Η απάντηση είναι θετική όπως έδειξε ο Hilbert το 1909. Ποιος είναι ο ελάχιστος $g(n)$; Το 1964, απεδείχθη ότι για $n = 5$ ο ελάχιστος $g(n)$ είναι 37. Για μεγάλα n, η ελάχιστη τιμή του $g(n)$ παραμένει μέχρι σήμερα άγνωστη.

Ένα άλλο ερώτημα που μπορούμε να θέσουμε εδώ είναι: κατά πόσους διαφορετικούς τρόπους παρίσταται ένας φυσικός αριθμός ως άθροισμα $g(n)$ n-στων δυνάμεων; Για συναφή προβλήματα και αποτελέσματα παραπέμπουμε στο βιβλίο του Grosswald [11]. Γιατί να ενδιαφερθεί κανείς για τέτοια προβλήματα; Ο ίδιος ο Grosswald λέει: "Ενώ οι Μαθηματικοί σπάνια εγείρουν τέτοιους προβληματισμούς, συχνά επισημαίνουν τις εφαρμογές των καθαρών μαθηματικών στη φυσική, μηχανολογία και άλλους επιστημονικούς τομείς. Επίσης, στην παρούσα περίπτωση, μπορεί να υποστηριχθεί η θέση ότι η μελέτη αθροισμάτων τετραγώνων ακεραίων είναι χρήσιμη σε προβλήματα που αφορούν σημεία δικτυωτών (lattices), στην κρυσταλλογραφία, και σε ορισμένα προβλήματα στη μηχανική."

Οι πρώτοι p της μορφής $p = x^2 + 2y^2$

Στο Θεώρημα 3.3.1 χαρακτηρίσαμε τους πρώτους p που γράφονται στη μορφή $p = x^2 + y^2$. Τα κύρια σημεία της απόδειξης ήταν τα εξής.

- Η ισοτιμία $q^2 \equiv -1 \mod p$ έχει λύση όταν $p \equiv 1 \mod 4$

- Ο $\mathbb{Z}[i]$ είναι περιοχή μοναδικής παραγοντοποίησης.

Ας θεωρήσουμε εδώ ένα συναφές ερώτημα: Ποιοι πρώτοι p γράφονται στη μορφή

$$p = x^2 + 2y^2;$$

Καθώς η περίπτωση $p = 2$ είναι τετριμμένη υποθέτουμε $p \neq 2$. Θεωρώντας περιπτώσεις modulo 2 για τα x, y βλέπουμε ότι $x^2 + 2y^2 \equiv 0, 1, 2, 3$, modulo 8 και επειδή ο p είναι περιττός πρώτος βρίσκουμε την αναγκαία συνθήκη

$$p \equiv 1, 3 \mod 8.$$

Αποδεικνύεται ότι η συνθήκη αυτή είναι και ικανή. Δεν θα το αποδείξουμε αυτό, αλλά θα αρκεστούμε στο να περιγράψουμε τα βασικά σημεία της απόδειξης.

Ας υποθέσουμε ότι γνωρίζουμε τα εξής.

i) Η ισοτιμία $q^2 \equiv -2 \mod p$ έχει λύση όταν $p \equiv 1, 3 \mod 8$

ii) Ο $\mathbb{Z}[\sqrt{-2}] = \{a + bi\sqrt{2} \in \mathbb{C} | a, b \in \mathbb{Z}\}$ είναι περιοχή μοναδικής παραγοντοποίησης.

Τότε από το i) υπάρχει $q \in \mathbb{Z}$ με $p | q^2 + 2$, οπότε

$$p | (q + i\sqrt{2})(q - i\sqrt{2}) \text{ στο } \mathbb{Z}[\sqrt{-2}].$$

Το p δεν είναι ανάγωγο στο $\mathbb{Z}[\sqrt{-2}]$, γιατί σε αντίθετη περίπτωση θα έπρεπε, λόγω του ii), να διαιρεί ένα από τα $q + \sqrt{-2}$, $q - \sqrt{-2}$, πράγμα αδύνατο. Τα αντιστρέψιμα στοιχεία του $\mathbb{Z}[\sqrt{-2}]$ είναι τα ± 1 (άσκηση). Επομένως έχουμε $p = (a + b\sqrt{-2})(c + d\sqrt{-2})$, όπου $a + b\sqrt{-2}, c + d\sqrt{-2} \neq \pm 1$. Λαμβάνοντας τα τετράγωνα των μέτρων μιγαδικών αριθμών έχουμε $p^2 = (a^2 + 2b^2)(c^2 + 2d^2)$. Επειδή $a^2 + 2b^2, c^2 + 2d^2 > 1$, η μοναδικότητα της παραγοντοποίησης στο $\mathbb{Z}$ δίνει $p = a^2 + 2b^2$ $(= c^2 + 2d^2)$. Συνεπώς ο p είναι της μορφής $x^2 + 2y^2$.

Ας σχολιάσουμε τώρα τις υποθέσεις i) και ii). Για την ii) μπορεί να αποδειχτεί ότι ο δακτύλιος $\mathbb{Z}[\sqrt{-2}]$ είναι Ευκλείδεια περιοχή ως προς τη συνάρτηση $\delta : \mathbb{Z}[\sqrt{-2}] \to \mathbb{N}$, $\delta(a + bi\sqrt{2}) = a^2 + 2b^2$ (Άσκηση 3.2.20) Επομένως ο δακτύλιος αυτός είναι περιοχή μοναδικής παραγοντοποίησης. Η απόδειξη του i) είναι κάπως τεχνική και για τον λόγο αυτό παραλείπεται. Γενικά το ερώτημα πότε μια ισοτιμία της μορφής $x^2 \equiv a \mod p$ έχει λύση είναι ένα σημαντικό θέμα της Θεωρίας Αριθμών που μελετήθηκε συστηματικά - μεταξύ των άλλων - από τους Euler, Legendre, Jacobi και Gauss. Παραπέμπουμε στο βιβλίο του Rosen [24] και ειδικά στο Κεφάλαιο 9.

Οι φυσικοί αριθμοί της μορφής $n = x^2 + 2y^2$

Για συντομία έστω A το σύνολο των φυσικών αριθμών n της μορφής $n = x^2 + 2y^2$, όπου $x, y \in \mathbb{N}$. Από την ταυτότητα

$$(a^2 + 2b^2)(c^2 + 2d^2) = (ac - 2bd)^2 + 2(ad + bc)^2$$

συμπεραίνουμε ότι

$$m, n \in A \Rightarrow mn \in A.$$

Από αυτό και τον χαρακτηρισμό των πρώτων της μορφής $x^2 + 2y^2$ που είδαμε πιο πάνω συνάγουμε ότι: αν στην παραγοντοποίηση του n σε γινόμενο πρώτων κάθε πρώτος p με $p \equiv 5, 7 \mod 8$ εμφανίζεται με άρτιο εκθέτη, τότε $n \in A$.

Μπορεί να αποδειχτεί το αντίστροφο κατά τρόπο παρόμοιο με την απόδειξη του Θεωρήματος 3.3.2. Για το σκοπό αυτό θα πρέπει να προσδιοριστούν τα ανάγωγα στοιχεία της Ευκλείδειας περιοχής $\mathbb{Z}[\sqrt{-2}]$. Αυτά είναι τα $\pm p$, όπου p είναι πρώτος με $p \equiv 5, 7 \mod 8$, και τα $a + bi\sqrt{2}$, όπου $a^2 + 2b^2$ είναι πρώτος αριθμός. Η απόδειξη είναι παρόμοια με αυτή του Θεωρήματος 3.3.3. Τελικά αποδεικνύεται ότι

ο φυσικός αριθμός n είναι της μορφής $x^2 + 2y^2$, όπου $x, y \in \mathbb{N}$, αν και μόνο αν στην παραγοντοποίηση του n κάθε πρώτος p με $p \equiv 5, 7 \mod 8$ εμφανίζεται με άρτιο εκθέτη.

Σχόλια

Δυστυχώς η μέθοδος που περιγράψαμε προηγούμενα δεν εφαρμόζεται σε πιο γενικές παραστάσεις της μορφής $n = x^2 + dy^2$, όπου το $d \in \mathbb{Z}$ δεν διαιρείται με το τετράγωνο ακεραίου μεγαλυτέρου του 1. Αυτό οφείλεται στο γεγονός ότι για $d > 2$ οι δακτύλιοι $\mathbb{Z}[\sqrt{-d}]$ δεν είναι περιοχές μοναδικής παραγοντοποίησης (βλ. Άσκηση 3.2.22). Όμως, έχουν αναπτυχθεί άλλες μέθοδοι στην Αλγεβρική Θεωρία Αριθμών που υποσκελίζουν την έλλειψη της ιδιότητας της μοναδικότητας στην παραγοντοποίηση στοιχείων σε γινόμενο αναγώγων. Μια από αυτές βασίζεται στη μοναδικότητα της παραγοντοποίησης *ιδεωδών* ορισμένων δακτυλίων, όπως είναι οι $\mathbb{Z}[\sqrt{-d}]$, σε γινόμενο πρώτων ιδεωδών. Η ιδέα αυτή ανήκει στον Kummer και ήταν ο λόγος που εισήγαγε τη νέα για την εποχή αυτή έννοια του ιδεώδους! Για συγκεκριμένα παραδείγματα της μεθόδου αυτής παραπέμπουμε στην Παράγραφο 11.12 του Artin, *Algebra*, [2].

Θεώρημα των τεσσάρων τετραγώνων

Θα αποδείξουμε στη συνέχεια ότι κάθε φυσικός αριθμός είναι άθροισμα 4 τετραγώνων φυσικών αριθμών. Η απόδειξη που θα δώσουμε χρησιμοποιεί 2×2

πίνακες με στοιχεία από το $\mathbb{Z}[i]$ και οφείλεται στον C. Small [27]. Αν και η απόδειξη αυτή δεν χρησιμοποιεί τη μοναδικότητα της παραγοντοποίησης στο $\mathbb{Z}[i]$, την αναπτύσσουμε εδώ λόγω της κομψότητας που παρουσιάζει. Στην παρακάτω απόδειξη θα θεωρήσουμε γνωστές βασικές ιδιότητες από τη Θεωρία Ομάδων, οι οποίες μελετώνται στην Ενότητα 4. Συγκεκριμένα θα χρησιμοποιήσουμε το Θεώρημα του Lagrange και το γεγονός ότι η πολλαπλασιαστική ομάδα των μη μηδενικών στοιχείων κάθε πεπερασμένου σώματος είναι κυκλική.

3.3.4 Λήμμα. *Κάθε στοιχείο ενός πεπερασμένου σώματος F είναι άθροισμα δύο τετραγώνων στοιχείων του F. Επιπλέον, αν η χαρακτηριστική του F είναι 2, τότε κάθε στοιχείο του F είναι τετράγωνο στοιχείου του F. Αν η χαρακτηριστική του F δεν είναι 2, τότε ακριβώς τα μισά από τα μη μηδενικά στοιχεία του F είναι τετράγωνα.*

Απόδειξη. Αν η χαρακτηριστική του F είναι 2, τότε η απεικόνιση $F \ni a \mapsto a^2 \in F$ είναι $1-1$. Επειδή το F είναι πεπερασμένο, η απεικόνιση αυτή είναι επί. Άρα κάθε στοιχείο του F είναι τετράγωνο στοιχείου του F.

Έστω τώρα ότι η χαρακτηριστική του F είναι διάφορη του 2. Γνωρίζουμε ότι η πολλαπλασιαστική ομάδα F^* των μη μηδενικών στοιχείων του F είναι κυκλική, και από το Θεώρημα 2.7.1 η ομάδα αυτή έχει άρτια τάξη. Άρα $F^* = \{g, g^2, \ldots, g^{2m} = 1\}$ $g \in F$. Τα στοιχεία $g^2, g^4, \ldots, g^{2m}$ είναι βέβαια τετράγωνα. Κάθε στοιχείο της μορφής g^{2k+1} δεν είναι τετράγωνο γιατί αν υπάρχει $h \in F^*$ με $g^{2k+1} = h^2$, τότε από το Θεώρημα του Lagrange στις ομάδες παίρνουμε $g^{(2k+1)m} = h^{2m} = 1$ οπότε $2m|(2k+1)m$, δηλαδή $2|2k+1$, που είναι άτοπο. Αποδείξαμε ότι ακριβώς τα μισά από τα στοιχεία του F^* είναι τετράγωνα. Θα αποδείξουμε τώρα ότι κάθε στοιχείο του F είναι άθροισμα δύο τετραγώνων. Έστω $z \in F^*$, όπου το z δεν είναι τετράγωνο. Θεωρούμε τα υποσύνολα του F^*

$$T = \{x^2 \in F^* | x \in F^*\} \quad \text{και} \quad S = \{z - y^2 \in F^* | y \in F^*\}.$$

Τα T και S έχουν τον ίδιο πληθάριθμο γιατί η αντιστοιχία $T \ni x^2 \mapsto z - x^2 \in S$ είναι $1-1$ και επί. Άρα $\frac{1}{2}|F^*| = |T| = |S|$. Επειδή $z \notin T$, $z \notin S$, συμπεραίνουμε ότι $S \cap T \neq \emptyset$. Άρα υπάρχουν $x, y \in F$ με $x^2 = z - y^2$, δηλαδή $z = x^2 + y^2$. ⊤

3.3.5 Πόρισμα. *Αν ο θετικός ακέραιος n είναι πρώτος ή το γινόμενο διακεκριμένων πρώτων, τότε κάθε στοιχείο του $\mathbb{Z}_n$ είναι άθροισμα δύο τετραγώνων.*

Απόδειξη. Αν $n = p$ είναι πρώτος, ο $\mathbb{Z}_p$ είναι σώμα και το αποτέλεσμα προκύπτει άμεσα από το προηγούμενο Λήμμα. Έστω $n = p_1 \ldots p_r$, όπου τα p_i είναι διακεκριμένοι πρώτοι. Υπενθυμίζουμε από την Άσκηση 2.6.20 ότι υπάρχει ένας ισομορφισμός δακτυλίων

$$\varphi : \mathbb{Z}_n \ni a \mapsto (a_1, \ldots, a_r) \in \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r},$$

όπου a_i είναι η κλάση υπολοίπων modulo p_i ενός (οποιουδήποτε) αντιπροσώπου της κλάσης a. Σύμφωνα με το Λήμμα 3.3.4, κάθε $a_i \in \mathbb{Z}_{p_i}$ γράφεται ως άθροισμα δύο τετραγώνων, $a_i = b_i^2 + c_i^2$, όπου $b_i, c_i \in \mathbb{Z}_{p_i}$. Συνεπώς η εικόνα του a είναι

$$\begin{aligned}\varphi(a) &= (a_1, \ldots, a_r) = \\ &= (b_1^2 + c_1^2, \ldots, b_r^2 + c_r^2) = \\ &= (b_1^2, \ldots, b_r^2) + (c_1^2, \ldots, c_r^2) = \\ &= (b_1, \ldots, b_r)^2 + (c_1, \ldots, c_r)^2.\end{aligned}$$

Επειδή ο φ είναι ισομορφισμός δακτυλίων, συμπεραίνουμε ότι το $a \in \mathbb{Z}_n$ γράφεται ως άθροισμα δύο τετραγώνων στο $\mathbb{Z}_n$. ⊺

Ερχόμαστε τώρα στο κεντρικό σημείο της απόδειξης. Θα εργαστούμε με το δακτύλιο $M_2(\mathbb{Z}[i])$ των 2×2 πινάκων με στοιχεία από το $\mathbb{Z}[i]$. Για λόγους συντομίας έστω $M = M_2(\mathbb{Z}[i])$. Αν $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M$, θέτουμε $A^* = \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} \in M$, τον συζυγή ανάστροφο του A.

3.3.6 Λήμμα. *Έστω $m, n, c, d \in \mathbb{Z}$ και*

$$A = \begin{pmatrix} n & c + di \\ c - di & m \end{pmatrix} \in M.$$

Αν $\det A = 1$, τότε υπάρχει $B \in M$ τέτοιο ώστε $A = BB^*$.

Απόδειξη. Εφαρμόζουμε επαγωγή στο c^2+d^2. Αν $c^2+d^2 = 0$, τότε $c = d = 0$ και επομένως $A = I$. Στην περίπτωση αυτή θέτουμε $B = I$.
Έστω τώρα $c^2 + d^2 > 0$. Διακρίνουμε δύο περιπτώσεις.
$1^η$ *Περίπτωση* $0 < n \leq m$.
Θέτουμε

$$C = \begin{pmatrix} 1 & 0 \\ x - yi & 1 \end{pmatrix} \in M \quad \text{και} \quad D = CAC^*.$$

Πολλαπλασιάζοντας παρατηρούμε ότι

$$D = \begin{pmatrix} n & r + si \\ r - si & * \end{pmatrix} \in M, \quad \text{όπου} \quad r = c + nx, \quad s = d + ny$$

και $*$ είναι κάποιος ακέραιος. Επίσης $\det D = (\det C)(\det A)(\det C^*) = 1$.
Ισχυριζόμαστε ότι υπάρχουν $x, y \in \mathbb{Z}$ τέτοια ώστε $r^2 + s^2 < c^2 + d^2$. Αν αληθεύει ο ισχυρισμός, τότε από την επαγωγική υπόθεση υπάρχει $E \in M$ τέτοιο

ώστε $D = EE^*$. Θέτοντας $B = C^{-1}E$ εύκολα επαληθεύουμε ότι $BB^* = A$, που είναι το ζητούμενο.

Τώρα αποδεικνύουμε τον παραπάνω ισχυρισμό. Διακρίνουμε περιπτώσεις.
Αν $c > n/2$, επιλέγουμε $x = -1$ και $y = 0$, οπότε $r^2+s^2 = (c-n)^2+d^2 < c^2+d^2$.
Αν $c < -n/2$, επιλέγουμε $x = 1$ και $y = 0$.
Αν $d > -n/2$, επιλέγουμε $x = 0$ και $y = -1$.
Αν $d < -n/2$, επιλέγουμε $x = 0$ και $y = 1$.
Μένει να εξετάσουμε την περίπτωση που $|c| \leq n/2$ και $|d| \leq n/2$. Θα δείξουμε ότι στην περίπτωση αυτή δεν εμπίπτει κανένα n. Αρχικά παρατηρούμε ότι $n \neq 1$, αφού οι ακέραιοι c, d είναι μη μηδενικοί. Έστω τώρα $n > 1$. Από την υπόθεση έχουμε $0 < n \leq m$, και επομένως

$$n^2 \leq nm = c^2 + d^2 + 1 \leq (n/2)^2 + (n/2)^2 + 1 = n^2/2 + 1 < n^2,$$

που είναι άτοπο.
2^{η} *Περίπτωση* $0 < m \leq n$.
Η περίπτωση αυτή είναι παρόμοια με την προηγούμενη: Θέτουμε

$$C = \begin{pmatrix} 1 & x+yi \\ 0 & 1 \end{pmatrix} \in M$$

και ακολουθούμε ανάλογα βήματα. ⊺

Είμαστε τώρα σε θέση να αποδείξουμε το Θεώρημα των τεσσάρων τετραγώνων.

3.3.7 Θεώρημα των τεσσάρων τετραγώνων. [1] *Για κάθε φυσικό αριθμό n υπάρχουν φυσικοί αριθμοί w, x, y, z τέτοιοι ώστε $n = w^2 + x^2 + y^2 + z^2$.*

Απόδειξη. Μπορούμε να υποθέσουμε ότι ο n δεν διαιρείται με το τετράγωνο κανενός ακεραίου μεγαλυτέρου του 1, γιατί αν $n = a^2q$ και το q είναι άθροισμα τεσσάρων τετραγώνων, $q = w^2 + x^2 + y^2 + z^2$, τότε και το n είναι άθροισμα τεσσάρων τετραγώνων, $n = (aw)^2 + (ax)^2 + (ay)^2 + (az)^2$. Από το Πόρισμα 3.3.5 υπάρχουν ακέραιοι c, d τέτοιοι ώστε $-1 \equiv c^2 + d^2 \mod n$, δηλαδή έχουμε $mn - c^2 - d^2 = 1$, $m \in \mathbb{Z}$. Θεωρούμε τον πίνακα

$$A = \begin{pmatrix} n & c+di \\ c-di & m \end{pmatrix}$$

[1] Το Θεώρημα αυτό αποδείχτηκε από τον J. Lagrange το 1770. Ο Lagrange εργάσθηκε σε πολλούς τομείς των Μαθηματικών και της Φυσικής, όπως είναι η Θεωρία Αριθμών, η Θεωρία των Εξισώσεων, οι Διαφορικές Εξισώσεις, ο Λογισμός των Μεταβολών, η Ουράνια Μηχανική και η Υδροδυναμική.

και παρατηρούμε ότι $\det A = 1$. Εφαρμόζοντας το Λήμμα 3.3.6 παίρνουμε $A = BB^*$ για κάποιο $B \in M$. Από τη σχέση

$$\begin{pmatrix} n & c+di \\ c-di & m \end{pmatrix} = \begin{pmatrix} w+xi & y+zi \\ * & * \end{pmatrix} \begin{pmatrix} w-xi & * \\ y-zi & * \end{pmatrix}$$

βλέπουμε ότι $n = w^2 + x^2 + y^2 + z^2$. ⊤

Ασκήσεις 3.3

1. Ποια είναι η παραγοντοποίηση σε γινόμενο αναγώγων των 2002 και 2004 στο $\mathbb{Z}[i]$; Στο $\mathbb{Z}[\sqrt{-2}]$;

2. Για ποιά p η ισοτιμία $(x+1)^2 \equiv -1 \mod p$ έχει λύση;

3. Έστω p ένας πρώτος αριθμός. Εστω R το υποσύνολο του $M_2(\mathbb{Z}_p)$ που αποτελείται από τους πίνακες της μορφής $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Αποδείξτε ότι το R είναι σώμα αν και μόνο αν $p \equiv 3 \mod 4$.

4. Για ποιούς πρώτους p ο δακτύλιος $\mathbb{Z}_p[x]/ < x^2 + 1 >$ είναι σώμα; Ποια είναι η σχέση του δακτυλίου αυτού με τον R της προηγούμενης άσκησης;

5. Έστω p ένας πρώτος τέτοιος ώστε $p = a^2+b^2 = c^2+d^2$, όπου $a, b, c, d \in \mathbb{N}$. Τότε είτε $a = c$, $b = d$ είτε $a = d$, $b = c$.
Υπόδειξη: $(a+ib)(a-ib) = (c+id)(c-id)$. Χρησιμοποιήστε τη μοναδικότητα της παραγοντοποίησης στο $\mathbb{Z}[i]$ και το Θεώρημα 3.3.3.

6. Έστω a, b δύο σχετικά πρώτοι ακέραιοι. Αποδείξτε ότι κάθε θετικός διαιρέτης του ακεραίου $a^2 + b^2$ είναι της μορφής $c^2 + d^2$ όπου $\mu\kappa\delta(c, d) = 1$.
Υπόδειξη: Θεωρήματα 3.3.2 και 3.3.3.

7. Για κάθε $n \in \mathbb{N}$ υπάρχει ακέραιος $m > n$ που δεν είναι άθροισμα των τετραγώνων 4 *θετικών* ακεραίων.
Υπόδειξη: $m = 2^k$, k περιττός και αρκετά μεγάλος.

8. Να βρεθεί η ανάλυση των 29 και 31 σε γινόμενα αναγώγων στο $\mathbb{Z}[i]$.

3.4 Μοναδική Παραγοντοποίηση και Πολυώνυμα

Έστω R μια περιοχή μοναδικής παραγοντοποίησης. Στην Παράγραφο αυτή θα αποδείξουμε ότι ο πολυωνυμικός δακτύλιος $R[x]$ είναι περιοχή μοναδικής παραγοντοποίησης. Επίσης θα δούμε μερικές εφαρμογές.

3.4.1 Θεώρημα. *Αν ο δακτύλιος R είναι περιοχή μοναδικής παραγοντοποίησης, τότε και ο δακτύλιος $R[x]$ είναι περιοχή μοναδικής παραγοντοποίησης.*

Η βασική ιδέα της απόδειξης του παραπάνω Θεωρήματος είναι απλή. Για να παραγοντοποιήσουμε ένα $f(x) \in R[x]$ σε γινόμενο αναγώγων εφαρμόζουμε επαγωγή στο $\deg f(x)$. Για τη μοναδικότητα της παραγοντοποίησης αυτής, θεωρούμε το $f(x)$ ως στοιχείο του $F[x]$, όπου F είναι το σώμα πηλίκων του R, και χρησιμοποιούμε τη μοναδικότητα της παραγοντοποίησης στο $F[x]$. Υπάρχουν βέβαια κάποιες δυσκολίες καθώς δεν γνωρίζουμε (προς το παρόν) αν ένα ανάγωγο πολυώνυμο του $R[x]$ παραμένει ανάγωγο στο $F[x]$. Επειδή το F είναι το σώμα πηλίκων του R, είναι αναμενόμενο ότι στη μελέτη της συσχέτισης των πολυωύμων του $R[x]$ και $F[x]$ σημαντικό ρόλο θα παίξουν οι συντελεστές. Δίνουμε τους ακόλουθους ορισμούς.

Έστω R μια περιοχή μοναδικής παραγοντοποίησης. Ένα $f(x) = a_n x^n + \cdots + a_0 \in R[x]$ ονομάζεται ***πρωταρχικό*** αν το 1 είναι ένας $\mu\kappa\delta$ των $a_0, \ldots, a_n$. Για παράδειγμα, κάθε μονικό πολυώνυμο του $R[x]$ είναι πρωταρχικό. Το $2x^3 - 6x^2 + 5x - 4 \in \mathbb{Z}[x]$ είναι πρωταρχικό, ενώ το $2x^3 - 6x^2 + 4x - 4 \in \mathbb{Z}[x]$ δεν είναι.

Παρατηρούμε ότι αν $f(x) = a_n x^n + \cdots + a_0 \in R[x]$ είναι μη μηδενικό και c είναι ένας $\mu\kappa\delta$ των συντελεστών $a_0, \ldots, a_n$, τότε έχουμε $f(x) = cg(x)$, για κάποιο $g(x) \in R[x]$ που είναι πρωταρχικό. Κάθε τέτοιο c ονομάζεται ***περιεχόμενο*** του $f(x)$. Παρατηρούμε ότι αυτό δεν ορίζεται μοναδικά. Για παράδειγμα, στο $\mathbb{Z}[x]$ έχουμε

$$6x^2 - 3x + 12 = 3(2x^2 - x + 4) = (-3)(-2x^2 + x - 4),$$

οπότε ένα περιεχόμενο του $6x^2 - 3x + 12 \in \mathbb{Z}[x]$ είναι το 3 και ένα άλλο είναι το -3. Σύμφωνα με το επόμενο Λήμμα, κάθε δύο περιεχόμενα ενός πολυωνύμου είναι συντροφικά στοιχεία.

3.4.2 Λήμμα. *Έστω R μια περιοχή μοναδικής παραγοντοποίησης και $f(x) \in R[x]$, $f(x) \neq 0$. Αν $f(x) = cg(x)$ και $f(x) = c'g'(x)$, όπου τα c, c' είναι περιεχόμενα του $f(x)$, τότε τα $g(x)$, $g'(x)$ είναι πρωταρχικά και υπάρχει αντιστρέψιμο R τέτοιο ώστε $c = uc'$ και $g(x) = u^{-1}g'(x)$.*

Απόδειξη. Είναι προφανές ότι τα $g(x)$, $g'(x)$ είναι πρωταρχικά. Από τον ορισμό του περιεχομένου προκύπτει ότι $c = uc'$ για κάποιο αντιστρέψιμο $u \in R$. Έχουμε $cg(x) = c'g'(x)$ οπότε $g(x) = u^{-1}g'(x)$. ⊤

Ας αποδείξουμε τώρα το "εύκολο μισό" του Θεωρήματος 3.4.1. Υπενθυμίζουμε πρώτα ότι χρησιμοποιούμε την έννοια του αναγώγου στοιχείου σύμφωνα με τον Ορισμό 3.1.1.

3.4.3 Πρόταση. *Έστω R μια περιοχή μοναδικής παραγοντοποίησης και $f(x) \in R[x]$ που δεν είναι αντιστρέψιμο ή το μηδενικό πολυώνυμο. Τότε το $f(x)$ γράφεται ως γινόμενο αναγώγων στοιχείων του $R[x]$.*

Απόδειξη. Έχουμε $f(x) = cg(x)$, όπου $g(x) \in R[x]$ είναι πρωταρχικό. Το c είναι είτε αντιστρέψιμο είτε γινόμενο αναγώγων στοιχείων του R, αφού το R είναι περιοχή μοναδικής παραγοντοποίησης. Επιπλέον, κάθε ανάγωγο στοιχείο του R είναι ανάγωγο στοιχείο του $R[x]$. Άρα αρκεί να αποδείξουμε ότι κάθε πρωταρχικό πολυώνυμο είναι αντιστρέψιμο στο $R[x]$ ή γινόμενο αναγώγων. Χρησιμοποιούμε επαγωγή στο $\deg g(x)$. Αν $\deg g(x) = 0$, τότε το $g(x)$ είναι αντιστρέψιμο, αφού είναι πρωταρχικό. Έστω ότι $\deg g(x) > 0$. Αν το $g(x)$ είναι ανάγωγο, έχουμε το ζητούμενο. Έστω ότι το $g(x)$ δεν είναι ανάγωγο. Επειδή το $g(x)$ είναι πρωταρχικό, υπάρχουν $h_1(x), h_2(x) \in R[x]$ με $g(x) = h_1(x)h_2(x)$, $0 < \deg h_1(x) < \deg g(x)$ και $< \deg h_2(x) < \deg g(x)$. Τα $h_i(x)$ είναι πρωταρχικά, αφού το γινόμενό τους είναι πρωταρχικό. Από την υπόθεση της επαγωγής κάθε $h_i(x)$ είναι αντιστρέψιμο στο $R[x]$ ή γινόμενο αναγώγων. Συνεπώς το ίδιο ισχύει για το $h_1(x)h_2(x)$. ⊤

Η απόδειξη του "άλλου μισού" του Θεωρήματος είναι κάπως πιο απαιτητική καθώς πρέπει να κατανοήσουμε τη σχέση των αναγώγων στοιχείων του $R[x]$ με αυτά του $F[x]$. Για παράδειγμα, αληθεύει ότι ένα ανάγωγο $f(x) \in \mathbb{Z}[x]$ παραμένει ανάγωγο στο $\mathbb{Q}[x]$; Για να απαντήσουμε στο ερώτημα αυτό χρειαζόμαστε το ακόλουθο αποτέλεσμα.

3.4.4 Λήμμα του Gauss. *Έστω R μια περιοχή μοναδικής παραγοντοποίησης. Τότε το γινόμενο δύο πρωταρχικών πολυωνύμων του $R[x]$ είναι πρωταρχικό.*

Απόδειξη. Έστω $f(x), g(x) \in R[x]$ δύο πρωταρχικά πολυώνυμα. Ας υποθέσουμε ότι το γινόμενο $f(x)g(x)$ δεν είναι πρωταρχικό. Τότε υπάρχει ανάγωγο $p \in R$ που διαιρεί όλους τους συντελεστές του $f(x)g(x)$. Η απεικόνιση

$$\varphi : R[x] \to \frac{R}{< p >}[x],\ a_n x^n + \cdots + a_0 \mapsto \overline{a_n}x^n + \cdots + \overline{a_0},$$

όπου $\bar{a} = a + < p > \in \dfrac{R}{< p >}$, είναι ένας ομομορφισμός δακτυλίων. Έχουμε $\varphi(f(x)g(x)) = 0$ και άρα $\varphi(f(x))\varphi(g(x)) = 0$. Το ιδεώδες $< p >$ είναι πρώτο, αφού το p είναι ανάγωγο (Σημείωση 3.1.6), και συνεπώς ο $R/ < p >$ είναι ακεραία περιοχή (Θεώρημα 2.10.3), οπότε και ο δακτύλιος $\dfrac{R}{< p >}[x]$ είναι ακεραία περιοχή (Πρόταση 2.2.4). Άρα $\varphi(f(x)) = 0$ ή $\varphi(g(x)) = 0$, πράγμα που σημαίνει ότι ο p διαιρεί όλους τους συντελεστές του $f(x)$ ή όλους τους συντελεστές του $g(x)$. Αυτό είναι άτοπο γιατί τα $f(x)$, $g(x)$ είναι πρωταρχικά πολυώνυμα. ⊤

3.4.5 Πόρισμα. *Έστω R μια περιοχή μοναδικής παραγοντοποίησης, F το σώμα πηλίκων της R και $f(x) \in R[x]$.*

1. *Αν το $f(x)$ είναι ανάγωγο στο $R[x]$ τότε είναι ανάγωγο και στο $F[x]$.*
2. *Αν το $f(x)$ είναι πρωταρχικό και ανάγωγο στο $F[x]$ τότε είναι ανάγωγο στο $R[x]$.*

Απόδειξη. 1. Έστω ότι το $f(x)$ είναι ανάγωγο στο $R[x]$. Έστω $f(x) = g(x)h(x)$, όπου $g(x), h(x) \in F[x]$. Απαλοίφοντας τους παρονομαστές όλων των συντελεστών (το F είναι το σώμα πηλίκων του R) παίρνουμε

$$df(x) = g_1(x)h_1(x),$$

όπου $d \in R$, $g_1(x), h(x) \in R[x]$, $\deg g_1(x) = \deg g(x)$, $\deg h_1(x) = \deg h(x)$. Έχουμε

$$f(x) = cf_1(x),\ g_1(x) = c_1g_2(x),\ h_1(x) = c_2h_2(x),$$

όπου τα $f_1(x), g_2(x), h_2(x) \in R[x]$ είναι πρωταρχικά, $c, c_1, c_2 \in R$ και $\deg f(x) = \deg f_1(x)$, $\deg g_1(x) = \deg g_2(x)$, $\deg h_1(x) = \deg h_2(x)$. Έχουμε

$$dcf_1(x) = c_1c_2g_2(x)h_2(x)$$

και από το Λήμμα του Gauss έπεται ότι το $g_2(x)h_2(x)$ είναι πρωταρχικό. Από το Λήμμα 3.4.2 έχουμε $c_1c_2 = dcu$ για κάποιο αντιστρέψιμο u, οπότε $dcf_1(x) = dcug_2(x)h_2(x)$ και $f(x) = cf_1(x) = cug_2(x)h_2(x)$. Επειδή το $f(x)$ είναι ανάγωγο στο $R[x]$ παίρνουμε $\deg g_2(x) = 0$ ή $\deg h_2(x) = 0$, δηλαδή $\deg g(x) = 0$ ή $\deg h(x) = 0$. Συνεπώς το $f(x)$ είναι ανάγωγο και στο $F[x]$.
2. Αυτό είναι άμεσο αφού $R[x] \subseteq F[x]$ και το $f(x)$ είναι πρωταρχικό. ⊤

Αποδεικνύουμε τώρα τη *μοναδικότητα* της παραγοντοποίησης στο $R[x]$, όπου R είναι μια περιοχή μοναδικής παραγοντοποίησης.

3.4.6 Πρόταση. *Έστω R μια περιοχή μοναδικής παραγοντοποίησης και*

$$f(x) = c_1 \dots c_s p_1(x) \dots p_m(x) = d_1 \dots d_t q_1(x) \dots q_n(x) \tag{1}$$

δύο παραγοντοποιήσεις του $f(x)$ σε γινόμενα αναγώγων στοιχείων του $R[x]$, όπου $c_i, d_j \in R$ και $\deg p_i(x), \deg q_j(x) > 0$. Τότε $s = t$, $m = n$, και (μετά ενδεχομένως από κάποια αναδιάταξη) τα c_i, d_i είναι συντροφικά στο R και τα $p_i(x), q_i(x)$ είναι συντροφικά στο $R[x]$.

Απόδειξη. Αφού τα $p_i(x), q_j(x)$ είναι θετικού βαθμού και ανάγωγα, είναι πρωταρχικά. Από το Λήμμα του Gauss τα πολυώνυμα $p_1(x) \dots p_m(x)$, $q_1(x) \dots q_n(x)$ είναι πρωταρχικά. Από το Λήμμα 3.4.2 και την ισότητα (;;) παίρνουμε ότι τα $c_1 \dots c_s$, $d_1 \dots d_t$ είναι συντροφικά. Από τη μοναδικότητα της παραγοντοποίησης στο R παίρνουμε $s = t$ και, μετά ενδεχομένως από κάποια αναδιάταξη, τα c_i, d_i είναι συντροφικά. Άρα

$$p_1(x) \dots p_m(x) = u q_1(x) \dots q_n(x)$$

για κάποιο αντιστρέψιμο $u \in R$. Τα $p_i(x), q_j(x)$ είναι ανάγωγα στο $F[x]$ από το Πόρισμα 3.4.5. Από τη μοναδικότητα της παραγοντοποίησης στο $F[x]$ παίρνουμε $m = n$ και, μετά ενδεχομένως από κάποια αναδιάταξη, τα $p_i(x), q_i(x)$ είναι συντροφικά στο $F[x]$. Άρα $p_i(x) = u_i q_i(x)$ για κάποια $u_i \in F$. Γράφοντας $u_i = a_i/b_i$ με $a_i, b_i \in R$ έχουμε $b_i p_i(x) = a_i q_i(x)$, οπότε από το Λήμμα 3.4.2 έχουμε ότι τα $p_i(x), q_i(x)$ είναι συντροφικά στο $R[x]$. ⊺

Από την Πρόταση 3.4.3 και την Πρόταση 3.4.6 προκύπτει το Θεώρημα 3.4.1.

Ένα σημαντικό αποτέλεσμα που αποδεικνύεται εύκολα με επαγωγή είναι το ακόλουθο.

3.4.7 Πόρισμα. *Αν ο δακτύλιος R είναι μια περιοχή μοναδικής παραγοντοποίησης, τότε και ο $R[x_1, \dots, x_n]$ είναι περιοχή μοναδικής παραγοντοποίησης για κάθε θετικό ακέραιο n.*

Για παράδειγμα, οι δακτύλιοι $\mathbb{Z}[x_1, \dots, x_n]$ και $F[x_1, \dots, x_n]$, όπου F είναι ένα σώμα, είναι περιοχές μοναδικής παραγοντοποίησης.

3.4.8 Εφαρμογές.
1) Αλγεβρικές καμπύλες

Έστω F ένα σώμα και $f(x,y) \in F[x,y]$. Το σύνολο των σημείων $(a,b) \in F \times F$ για τα οποία ισχύει $f(a,b) = 0$ ονομάζεται ***επίπεδη αλγεβρική καμπύλη***[1] και συμβολίζεται με C_f. Για παράδειγμα, αν $f(x,y) = x^2 - y$ και $F = \mathbb{R}$, τότε το C_f είναι η γνωστή μας παραβολή. Χρησιμοποιώντας την ιδιότητα της μοναδικής παραγοντοποίησης του $F[x,y]$, θα αποδείξουμε ότι:

> *Αν το $f(x,y)$ είναι ανάγωγο τότε οι καμπύλες C_f, C_g τέμνονται το πολύ σε πεπερασμένο πλήθος σημείων για κάθε $g(x,y) \in F[x,y]$ που δεν είναι πολλαπλάσιο του $f(x,y)$.*

Από αυτό μπορούμε να συμπεράνουμε ότι για τυχαία μη μηδενικά πολυώνυμα $f(x,y), g(x,y) \in \mathbb{C}[x,y]$, οι καμπύλες C_f, C_g τέμνονται το πολύ σε πεπερασμένο πλήθος σημείων (δηλαδή, το σύστημα $f(x,y) = g(x,y) = 0$ έχει πεπερασμένο σύνολο λύσεων) αν και μόνο αν τα $f(x,y)$, $g(x,y)$ είναι σχετικά πρώτα στο $\mathbb{C}[x,y]$ (Άσκηση 9).

Για την απόδειξη του πρώτου ισχυρισμού μας, έστω $f(x,y), g(x,y) \in F[x,y]$, όπου το $f(x,y)$ είναι ανάγωγο και δεν διαιρεί το $g(x,y)$. Μπορούμε χωρίς περιορισμό της γενικότητας να υποθέσουμε ότι ο βαθμός του $f(x,y)$ ως προς x είναι θετικός. Θα θεωρήσουμε τα πολυώνυμα $f(x,y)$, $g(x,y)$ ως στοιχεία του $F(y)[x]$, δηλαδή ως πολυώνυμα στη μεταβλητή x με συντελεστές από το σώμα $F(y)$ που είναι το σώμα πηλίκων του $F[y]$.

Ως στοιχείο του $F(y)[x]$, το $f(x,y)$ παραμένει ανάγωγο σύμφωνα με το Πόρισμα 2.12.5. Επιπλέον το $f(x,y)$ εξακολουθεί να μη διαιρεί το $g(x,y)$ στο $F(y)[x]$, γιατί σε αντίθετη περίπτωση θα είχαμε $g(x,y) = f(x,y)A(x,y)$ για κάποιο $A(x,y) \in F(y)[x]$. Αλλά κάθε στοιχείο του $F(y)[x]$ έχει τη μορφή $B(x,y)/C(y)$, όπου $B(x,y) \in F[x,y]$ και $C(y) \in F[y]$. Συνεπώς παίρνουμε $C(y)g(x,y) = f(x,y)B(x,y)$ και επειδή το $f(x,y)$ είναι ανάγωγο στην περιοχή μοναδικής παραγοντοποίησης $F[x,y]$ και δεν διαιρεί το $g(x,y)$ συμπεραίνουμε ότι το $f(x,y)$ διαιρεί το $C(y)$. Αυτό είναι άτοπο γιατί ο βαθμός του $f(x,y)$ ως προς x είναι θετικός. Από τα προηγούμενα προκύπτει ότι στον δακτύλιο $F(y)[x]$ ισχύει $\mu\kappa\delta(f(x,y), g(x,y)) = 1$ και επομένως (Θεώρημα 2.3.7) υπάρχουν $A(x,y), A'(x,y) \in F(y)[x]$ τέτοια ώστε

$$f(x,y)A(x,y) + g(x,y)A'(x,y) = 1.$$

Με απαλοιφή παρονομαστών παίρνουμε μια σχέση της μορφής

$$f(x,y)B(x,y) + g(x,y)B'(x,y) = C(y),$$

όπου $B(x,y), B'(x,y) \in F[x,y]$ και $C(y) \in F[y]$, $C(y) \neq 0$.

[1] Η λέξη *αλγεβρική* τονίζει ότι η καμπύλη ορίζεται από πολυώνυμο (σε αντίθεση για παράδειγμα με την καμπύλη που ορίζεται από τη σχέση $y = e^x$, $x \in \mathbb{R}$), ενώ η λέξη *επίπεδη* υποδηλώνει ότι η καμπύλη είναι υποσύνολο του δισδιάστατου χώρου $F \times F$.

Έστω $(a,b) \in C_f \cap C_g$, δηλαδή $f(a,b) = g(a,b) = 0$ για κάποιο $(a,b) \in F \times F$. Από την παραπάνω σχέση έχουμε $C(b) = 0$. Επειδή το $C(y)$ είναι μη μηδενικό πολυώνυμο με συντελεστές από σώμα, το πλήθος των ριζών του είναι πεπερασμένο. Ετσι το πλήθος των b είναι πεπερασμένο. Επειδή κάθε a είναι ρίζα του $f(x,b)$ που είναι πολυώνυμο θετικού βαθμού ως προς x, συμπεραίνουμε ότι και το πλήθος των a είναι πεπερασμένο. Η απόδειξη είναι πλήρης.

Ας θεωρήσουμε τώρα την ειδική περίπτωση $F = \mathbb{C}$. Έστω $f(x,y), g(x,y) \in \mathbb{C}[x,y]$ όπου το $f(x,y)$ είναι ανάγωγο. Επειδή κάθε μη σταθερό πολυώνυμο στο $\mathbb{C}[x,y]$ έχει άπειρες ρίζες $(a,b) \in \mathbb{C} \times \mathbb{C}$ (άσκηση), παρατηρούμε ότι αν $C_f \subseteq C_g$ τότε το $f(x,y)$ διαιρεί το $g(x,y)$. Αποδείξαμε έτσι ότι:

αν $f(x,y), g(x,y) \in \mathbb{C}[x,y]$ όπου το $f(x,y)$ είναι ανάγωγο και $C_f \subseteq C_g$, τότε το $g(x,y)$ είναι πολλαπλάσιο του $f(x,y)$.

Η πρόταση αυτή είναι μια ειδική περίπτωση ενός θεμελιώδους θεωρήματος της Αλγεβρικής Γεωμετρίας που λέει ότι αν κάποιο $g(x_1,\ldots,x_n) \in \mathbb{C}[x_1,\ldots,x_n]$ μηδενίζεται στις λύσεις του συστήματος $f_1(x_1,\ldots,x_n) = \cdots = f_m(x_1,\ldots,x_n) = 0$, τότε υπάρχουν $g_1(x_1,\ldots,x_n),\ldots,g_m(x_1,\ldots,x_n) \in \mathbb{C}[x_1,\ldots,x_n]$ και $k \in \mathbb{N}$ τέτοια ώστε

$$(g(x_1,\ldots,x_n))^k = \\ g_1(x_1,\ldots,x_n)f_1(x_1,\ldots,x_n) + \cdots + g_m(x_1,\ldots,x_n)f_m(x_1,\ldots,x_n).$$

Το αποτέλεσμα αυτό είναι μία άλλη μορφή του **" Nullstellensatz '** (βλ. Παράδειγμα 2.9.8 6)).

2) Υπολογισμός οριζουσών

Στη συνέχεια θα εφαρμόσουμε ιδιότητες του $\mathbb{Z}[x_1,\ldots,x_n]$ που σχετίζονται με τη μοναδικότητα της παραγοντοποίησης για να λάβουμε μια χρήσιμη μέθοδο υπολογισμού οριζουσών.

Υπενθυμίζουμε ότι ένα μη μηδενικό πολυώνυμο του $R[x_1,\ldots,x_n]$, R ακεραία περιοχή, ονομάζεται ***ομογενές*** βαθμού r αν είναι της μορφής $f(x_1,\ldots,x_n) = \sum_{i_1+\cdots+i_n=r} a_{i_1\ldots i_n} x_1^{i_1}\ldots x_n^{i_n}$, όπου $a_{i_1\ldots i_n} \in R$. Για παράδειγμα το $3x^2+5y^2-4xy \in \mathbb{Z}[x,y]$ είναι ομογενές βαθμού 2 αλλά το $3x^2+5y^2-4x$ δεν είναι ομογενές.

3.4.9 Παρατήρηση. Εύκολα διαπιστώνουμε ότι το γινόμενο δύο ομογενών πολυωνύμων βαθμών r και s είναι ομογενές βαθμού $r+s$. Επίσης είναι προφανές ότι το γινόμενο ενός μη ομογενούς πολυωνύμου με ένα ομογενές, δεν είναι ομογενές.

Ορίζουσα Vandermonde. Έστω $a_1,\ldots,a_n$ στοιχεία ενός μεταθετικού δα-

κτυλίου R που έχει μοναδιαίο στοιχείο. Θα υπολογίσουμε την ορίζουσα

$$D = \begin{vmatrix} a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \\ a_1^{n-2} & a_2^{n-2} & \cdots & a_n^{n-2} \\ \cdots & \cdots & \cdots & \cdots \\ a_1 & a_2 & \cdots & a_n \\ 1 & 1 & \cdots & 1 \end{vmatrix}.$$

Για το σκοπό αυτό θεωρούμε στο $\mathbb{Z}[x_1, \ldots x_n]$ το πολυώνυμο

$$\Delta = \begin{vmatrix} x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \\ x_1^{n-2} & x_2^{n-2} & \cdots & x_n^{n-2} \\ \cdots & \cdots & \cdots & \cdots \\ x_1 & x_2 & \cdots & x_n \\ 1 & 1 & \cdots & 1 \end{vmatrix}.$$

Θεωρώντας το Δ ως πολυώνυμο στη μεταβλητή x_1 με συντελεστές από το $\mathbb{Z}[x_2, \ldots x_n]$, παρατηρούμε ότι η αντικατάσταση $x_1 \to x_i (i \neq 1)$ το μηδενίζει, αφού μια ορίζουσα με δύο ίσες στήλες είναι μηδέν. Από το Θεώρημα 2.4.1 και τη Σημείωση 2.4.3 1) συμπεραίνουμε ότι το $x_1 - x_i$ διαιρεί το Δ. Με παρόμοιο τρόπο, βλέπουμε ότι το Δ διαιρείται με κάθε $x_i - x_j (i < j)$. Τα πολυώνυμα αυτά είναι ανάγωγα στοιχεία του $\mathbb{Z}[x_1, \ldots, x_n]$, αφού είναι μονικά βαθμού 1, και ανά δύο σχετικά πρώτα. Συνεπώς το γινόμενό τους διαιρεί το Δ, δηλαδή

$$\Delta = f \prod_{1 \leq i < j \leq n} (x_i - x_j),$$

για κάποιο $f \in \mathbb{Z}[x_1, \ldots, x_n]$. Παρατηρούμε ότι το $\prod_{1 \leq i < j \leq n} (x_i - x_j)$ είναι ένα ομογενές πολυώνυμο βαθμού $\frac{(n-1)n}{2}$. Επίσης το Δ είναι ένα ομογενές πολυώνυμο βαθμού $(n-1) + (n-2) + \cdots + 1 = \frac{(n-1)n}{2}$. Από την Παρατήρηση 3.4.9 συμπεραίνουμε ότι το f είναι ομογενές βαθμού 0, δηλαδή $f \in \mathbb{Z}$. Για να προσδιορίσουμε το f συγκρίνουμε τους συντελεστές του $x_1^{n-1} x_2^{n-2} \ldots x_{n-1}$ στα πολυώνυμα Δ και $f \prod_{1 \leq i < j \leq n} (x_i - x_j)$ και βλέπουμε ότι είναι 1 και f αντίστοιχα. Άρα $f = 1$ και

$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Θεωρούμε τώρα τον ομομορφισμό δακτυλίων

$$\Phi : \mathbb{Z}[x_1, \ldots, x_n] \to R, \quad h(x_1, \ldots, x_n) \mapsto h(a_1, \ldots, a_n).$$

Τελικά έχουμε

$$D = \Phi(\Delta) = \prod_{1 \le i < j \le n} (a_i - a_j).$$

Κυκλοειδής ορίζουσα. Ας δούμε ένα άλλο παράδειγμα λίγο πιο πολύπλοκο. Θα υπολογίσουμε την ορίζουσα

$$C = \begin{vmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{vmatrix},$$

όπου $a_i \in \mathbb{C}$. Για το σκοπό αυτό στον πολυωνυμικό δακτύλιο $\mathbb{C}[x_1, \ldots, x_n]$ θεωρούμε το πολυώνυμο

$$\Gamma = \begin{vmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ x_n & x_1 & x_2 & \cdots & x_{n-1} \\ x_{n-1} & x_n & x_1 & \cdots & x_{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ x_2 & x_3 & x_4 & \cdots & x_1 \end{vmatrix},$$

Έστω

$$\zeta_k = \sigma\upsilon\nu\frac{2k\pi}{n} + i\eta\mu\frac{2k\pi}{n} \in \mathbb{C},$$

$k = 0, 1, \ldots, n-1$. Έχουμε ότι $\zeta_k^n = 1$. Στην ορίζουσα εκτελούμε την εξής πράξη στηλών: προσθέτουμε στην πρώτη στήλη το

$$\zeta_k \Gamma_2 + \zeta_k^2 \Gamma_3 + \cdots + \zeta_k^{n-1} \Gamma_n,$$

όπου Γ_i παριστάνει την i στήλη της Γ. Η νέα πρώτη στήλη είναι η

$$\begin{gathered} x_1 + \zeta_k x_2 + \zeta_k^2 x_3 + \cdots + \zeta_k^{n-1} x_n \\ x_n + \zeta_k x_1 + \zeta_k^2 x_2 + \cdots + \zeta_k^{n-1} x_{n-1} \\ x_{n-1} + \zeta_k x_n + \zeta_k^2 x_1 + \cdots + \zeta_k^{n-1} x_{n-2} \\ \cdots \\ x_2 + \zeta_k x_3 + \zeta_k^2 x_4 + \cdots + \zeta_k^{n-1} x_n \end{gathered}$$

Από κάθε στοιχείο της στήλης αυτής βγάζουμε κοινό παράγοντα το

$$x_1 + \zeta_k x_2 + \zeta_k^2 x_3 + \cdots + \zeta_k^{n-1} x_n.$$

Συνεπώς τα πολυώνυμα αυτά (για $k = 0, 1, \ldots, n-1$) διαιρούν το Γ και επειδή είναι ανάγωγα και ανά δύο σχετικά πρώτα, παίρνουμε ότι το

$$\prod_{0\leq k\leq n-1} (x_1 + \zeta_k x_2 + \zeta_k^2 x_3 + \cdots + \zeta_k^{n-1} x_n)$$

διαιρεί το Γ. Συνεπώς $\Gamma = f \prod_{0\leq k\leq n-1} (x_1+\zeta_k x_2+z_k^2 x_3+\cdots+\zeta_k^{n-1} x_n)$ για κάποιο $f \in \mathbb{C}[x_1, \ldots, x_n]$. Όπως και στην περίπτωση της ορίζουσας Vandermonde, παρατηρούμε ότι το f είναι ομογενες βαθμού 0, δηλαδή $f \in \mathbb{C}$. Συγκρίνοντας συντελεστές του x_1^n, συμπεραίνουμε ότι $f = 1$, οπότε

$$\Gamma = \prod_{0\leq k\leq n-1} (x_1 + \zeta_k x_2 + \zeta_k^2 x_3 + \cdots + \zeta_k^{n-1} x_n).$$

Εφαρμόζοντας τον ομομορφισμό δακτυλίων $\mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}$, $h(x_1, \ldots, x_n) \mapsto h(a_1, \ldots, a_n)$, παίρνουμε τελικά

$$C = \prod_{0\leq k\leq n-1} (a_1 + \zeta_k a_2 + \zeta_k^2 a_3 + \cdots + \zeta_k^{n-1} a_n).$$

Ασκήσεις 3.4

Στις ασκήσεις που ακολουθούν, R παριστάνει μια περιοχή μοναδικής παραγοντοποίησης και F το σώμα πηλίκων της, εκτός αν αναφέρεται σαφώς κάτι άλλο.

1. Έστω $f(x) \in R[x]$ ένα πρωταρχικό πολυώνυμο. Αποδείξτε ότι κάθε διαιρέτης του $f(x)$ είναι πρωταρχικό πολυώνυμο.

2. Δώστε ένα παράδειγμα δύο πολυωνύμων του $\mathbb{Z}[x]$ που είναι συντροφικά στο $\mathbb{Q}[x]$, αλλά όχι στο $\mathbb{Z}[x]$.

3. Ποια είναι η παραγοντοποίηση σε γινόμενο αναγώγων στοιχείων του $2x^2 - 2x + 4$ στο $\mathbb{Z}[x]$; Στο $\mathbb{Q}[x]$;

4. Έστω R ένας δακτύλιος τέτοιος ώστε ο $R[x]$ είναι περιοχή μοναδικής παραγοντοποίησης. Αποδείξτε ότι και ο R είναι περιοχή μοναδικής παραγοντοποίησης.

5. i) Αληθεύει ότι κάθε ομομορφική εικόνα περιοχής μοναδικής παραγοντοποίησης είναι περιοχή μοναδικής παραγοντοποίησης;

ii) Έστω S ο υποδακτύλιος του $\mathbb{Q}[x,y]$ που αποτελείται από τα $f(x,y)$ που έχουν την ιδιότητα $f(-x,y)=f(x,-y)=f(x,y)$. Αληθεύει ότι το S είναι περιοχή μοναδικής παραγοντοποίησης;
Up'odeixh: $x^2y^2=(xy)(xy)$.

6. Έστω R ένας δακτύλιος τέτοιος ώστε ο $R[x]$ είναι περιοχή κυρίων ιδεωδών. Αποδείξτε ότι το R είναι σώμα.

7. Ο $\mathbb{Z}[x,y]$ είναι περιοχή μοναδικής παραγοντοποίησης, αλλά όχι Ευκλείδεια περιοχή. Όμοια και ο $R[x,y]$, όπου $R=\mathbb{Z}[i]$. Διατυπώστε και αποδείξτε μια γενίκευση.

8. Για ποια από τα παρακάτω ιδεώδη του $\mathbb{Z}[i]$ ο δακτύλιος $R[x,y]$ είναι περιοχή μοναδικής παραγοντοποίησης, όπου $R=\mathbb{Z}[i]/I$;

   1. $<5>$
   2. $<7>$
   3. $<-2+3i>$

9. Έστω $f(x,y),g(x,y)\in\mathbb{C}[x,y]$ μη μηδενικά πολυώνυμα. Αποδείξτε ότι οι καμπύλες C_f, C_g τέμνονται το πολύ σε πεπερασμένο πλήθος σημείων αν και μόνο αν τα $f(x,y)$, $g(x,y)$ είναι σχετικά πρώτα.

10. Υπολογίστε τις ορίζουσες

    a.
    $$\begin{vmatrix} a_1^n & a_2^n & \cdots & a_n^n \\ a_1^{n-2} & a_2^{n-2} & \cdots & a_n^{n-2} \\ a_1^{n-3} & a_2^{n-3} & \cdots & a_n^{n-3} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & 1 & \cdots & 1 \end{vmatrix}, \quad \text{όπου} \quad a_i \quad \text{είναι στοιχεία}$$
    μεταθετικού δακτυλίου με μοναδιαίο στοιχείο.

    b.
    $$\begin{vmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ -a_n & a_1 & a_2 & \cdots & a_{n-1} \\ -a_{n-1} & -a_n & a_1 & \cdots & a_{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ -a_2 & -a_3 & -a_4 & \cdots & a_1 \end{vmatrix}, \quad \text{όπου} \quad a_i\in\mathbb{C}.$$

11. i) Έστω $f(x)\in\mathbb{Z}[x]$. Αν το $f(x)$ είναι ανάγωγο στοιχείο, τότε το ιδεώδες $<f(x)>$ είναι πρώτο ιδεώδες στον $\mathbb{Z}[x]$.

ii) Έστω p ένας πρώτος αριθμός και $f(x) \in \mathbb{Z}[x]$ τέτοιο ώστε η εικόνα του $\bar{f}(x)$, κάτω από τον ομομορφισμό $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$, που επάγεται από τον φυσικό επιμορφισμό $\mathbb{Z} \to \mathbb{Z}_p$, είναι ένα ανάγωγο στοιχείο. Αποδείξτε ότι το ιδεώδες $< p, f(x) >$ είναι μεγιστικό ιδεώδες του $\mathbb{Z}[x]$.

12. Ας θεωρήσουμε ένα σώμα F.

(i) Έστω $f(x,y) \in k[x,y]$. Αν το $f(x,y)$ είναι ανάγωγο, τότε το ιδεώδες $< f(x,y) >$ είναι ένα πρώτο ιδεώδες του $k[x,y]$.

(ii) Έστω $p(x) \in k[x]$ ένα ανάγωγο πολυώνυμο (οπότε $\deg p(x) \geq 1$) και $f(x,y) \in k[x,y]$ τέτοιο ώστε η εικόνα του, $\bar{f}(x,y)$, κάτω από τον ομομορφισμό $(k[x])[y] \to (k[x]/ < p(x) >)[y]$ που επάγεται από τον φυσικό επιμορφισμό $k[x] \to k[x]/ < p(x) >$, είναι ένα ανάγωγο στοιχείο. Αποδείξτε ότι το ιδεώδες $< p(x), f(x,y) >$ είναι μεγιστικό ιδεώδες του $k[x,y]$.

4 Ομάδες

Σ' αυτή, την τέταρτη, Ενότητα του βιβλίου αναπτύσσεται η στοιχειώδης θεωρία των ομάδων. Στην αρχή μελετώνται συγκεκριμένες ομάδες μέσω των οποίων πηγάζει η θεμελιώδης έννοια της ομάδας. Κατόπιν δίνονται αρκετά παραδείγματα ομάδων και εξετάζονται στοιχειώδεις ιδιότητες αυτών. Στη συνέχεια υπεισέρχεται η έννοια της υποομάδας μιας ομάδας και η έννοια του ομομορφισμού ομάδων. Μέσω αυτών αναπτύσσεται η βασική μελέτη της δομής μιας ομάδας. Τα αποτελέσματα της μελέτης αυτής εφαρμόζονται σε διάφορα θέματα που έχουν σχέση με τη θεωρία αριθμών.

4.1 Ομάδες Συμμετρίας

Ένας από τους λόγους που η έννοια της ομάδας εμφανίζεται και χρησιμοποιείται σχεδόν σε όλες τις επιστήμες είναι ότι σχετίζεται με την ιδέα της συμμετρίας, με την οποία ο άνθρωπος είναι, ίσως, περισσότερο εξοικειωμένος και από αυτή την ιδέα του αριθμού. Εδώ θα εξετάσουμε αυτή τη συσχέτιση με γεωμετρικό τρόπο που είναι ιδιαίτερα διαισθητικός . Για μια φιλοσοφικομαθηματική και πιο λεπτομερή θεώρηση της έννοιας "συμμετρία" παραπέμπουμε τον αναγνώστη στο κλασσικό βιβλίο *"Symmetry"* γραμμένο από το μεγάλο μαθηματικό του περασμένου αιώνα Hermann Weyl [30] .

Γεωμετρικά, ο κοινά αποδεκτός όρος "συμμετρία" ενός γεωμετρικού σχήματος είναι κάθε δυνατός "μετασχηματισμός", ο οποίος "μετακινεί" το σχήμα με τέτοιο τρόπο που η νέα του θέση να μη διακρίνεται από την αρχική του. Δηλαδή μετά την μετακίνησή του να φαίνεται σαν να μην έχει μετακινηθεί. Για παράδειγμα, ας θεωρήσουμε ένα ισοσκελές τρίγωνο, που δεν είναι ισόπλευρο, με κορυφές 1, 2 και 3 και έστω $\mathcal{E}$ η ευθεία γραμμή που διέρχεται από την κορυφή 1 και είναι κάθετη στην πλευρά που συνδέει τις κορυφές 2 και 3, όπως στο σχήμα 4.1.1.

ε

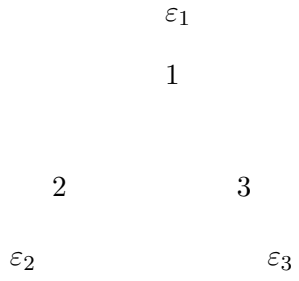
1

2 3

Σχήμα 4.1.1

Είναι φανερό, τουλάχιστον διαισθητικά, ότι η ανάκλαση R ως προς την ευθεία $\mathcal{E}$ είναι η μοναδική συμμετρία του θεωρούμενου τριγώνου. Αν όμως θεωρήσουμε ένα ισόπλευρο τρίγωνο, τότε αυτό έχει πέντε συμμετρίες, που είναι οι τρεις ανακλάσεις $R_1,\ R_2$ και R_3 ως προς τις ευθείες $\mathcal{E}_1,\ \mathcal{E}_2$ και $\mathcal{E}_3$ αντίστοιχα (σχήμα 4.1.2) και οι δύο στροφές S_1 και S_2 γύρω από το κέντρο του τριγώνου κατά γωνία 120^0 και 240^0 αντίστοιχα κατά τη θετική φορά, (που είναι η αντίθετη

προς τη φορά των δεικτών του ωρολογίου).



Σχήμα 4.1.2

Όμοια, το ορθό πρίσμα του σχήματος $4.1.3_\beta$ έχει επτά συμμετρίες. Πράγματι, αν θεωρήσουμε τη διατομή του πρίσματος (σχήμα $4.1.3_\alpha$) αυτή έχει τρεις συμμετρίες που είναι οι στροφές S_1, S_2 και S_3 γύρω από το κέντρο της κατά γωνία 90^0, 180^0 και 270^0 αντίστοιχα.

Σχήμα $4.1.3_\alpha$ Σχήμα $4.1.3_\beta$

Αυτές οι στροφές δεν αλλάζουν τη μορφή και τη θέση του πρίσματος. Επίσης, η ανάκλαση R ως προς το επίπεδο που τέμνει κάθετα το πρίσμα στο μέσον του, ορίζει μία άλλη συμμετρία. Επιπλέον αν εφαρμόσουμε στο πρίσμα την ανάκλαση R και μετά μία από τις στροφές S_1, S_2 και S_3 παίρνουμε τις υπόλοιπες τρεις συμμετρίες του. Οι συμμετρίες αυτές είναι πράγματι οι μόνες συμμετρίες του πρίσματος (γιατί;).

Άλλες ενδιαφέρουσες συμμετρίες συναντάμε σε πολλά διακοσμητικά σχέδια. Για παράδειγμα αν υποθέσουμε ότι ένα άνθος επαναλαμβάνεται με σταθερή α-

πόσταση δ άπειρες φορές κατά μήκος της ευθείας $\mathcal{E}$, όπως φαίνεται στο σχήμα 4.1.4, τότε οι άπειρες επαναλήψεις της ολισθαίνουσας ανάκλασης A ως προς την ευθεία $\mathcal{E}$ κατά διάστημα δ (δηλαδή μετατόπιση κατά μήκος της ευθείας $\mathcal{E}$ και ανάκλαση) είναι όλες οι συμμετρίες του σχήματος.

Σχήμα 4.1.4

Είναι φανερό από τα προηγούμενα παραδείγματα, αλλά όπως θα δούμε και πιο κάτω, ότι το σύνολο των συμμετριών ενός σχήματος καθορίζει ορισμένες από τις ιδιότητες που έχουν η μορφή και η θέση του. Συνεπώς είναι φυσιολογικό να στρέψουμε την προσοχή μας στη λεπτομερή μελέτη των ιδιοτήτων του συνόλου των συμμετριών ενός σχήματος. Για τη μελέτη αυτή είναι χρήσιμο να δώσουμε τώρα έναν ορισμό της συμμετρίας.

Υπενθυμίζουμε ότι στον Ευκλείδειο χώρο $\mathbb{R}^n$ ορίζεται το εσωτερικό γινόμενο $x \cdot y = \sum_{i=1}^{n} x_i y_i$ και η απόσταση $d(x,\, y) = \sqrt{\sum (x_i - y_i)^2}$ δύο (οποιωνδήποτε) σημείων $x = (x_1, \ldots, x_n),\ y = (y_1, \ldots, y_n) \in \mathbb{R}^n$.

4.1.1 Ορισμός. *Μια απεικόνιση $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ που διατηρεί την απόσταση, δηλαδή $d(f(x), f(y)) = d(x, y)$, για κάθε $x, y \in \mathbb{R}^n$, λέγεται* ***ισομετρία****. Μια ισομετρία f θα λέγεται* ***συμμετρία*** *του M αν $f(M) = M$, όπου M είναι ένα μη κενό υποσύνολο του $\mathbb{R}^n$. Το σύνολο των συμμετριών του M το συμβολίζουμε με $S(M)$.*

Κάθε ισομετρία f είναι μία 1 - 1 απεικόνιση, αφού από τον ορισμό αν $x \neq y$, τότε $f(x) \neq f(y)$. Αποδεικνύεται ότι κάθε ισομετρία είναι και επί απεικόνιση. Επιπλέον αν $f(0) = 0$, τότε η f είναι μια γραμμική απεικόνιση που αφήνει το εσωτερικό γινόμενο αναλλοίωτο, δηλαδή $f(x) \cdot f(y) = x \cdot y$. Στην περίπτωση αυτή η f λέγεται ***ορθογώνιος μετασχηματισμός***. Αν μία ισομετρία δεν είναι ορθογώνιος μετασχηματισμός, τότε αυτή είναι η σύνθεση $g \circ \tau_\alpha$ ενός ορθογώνιου μετασχηματισμού g και μίας μετατόπισης τ_α, $\alpha \in \mathbb{R}^n$, όπου $\tau_\alpha(x) = x + \alpha$, για κάθε $x \in \mathbb{R}^n$ (βλέπε Άσκηση 4.1 (4)).

Μια πρώτη γενική ιδιότητα που διακρίνουμε για τις συμμετρίες του M είναι ότι αν εφαρμόσουμε στο M διαδοχικά δύο (ή περισσότερες) συμμετρίες του, τότε θα πάρουμε είτε μία συμμετρία του M ή την απεικόνιση που αφήνει κάθε σημείο του M σταθερό, δηλαδή την ταυτοτική απεικόνιση I. Αυτή η απεικόνιση I, η οποία μολονότι για μη μαθηματικούς ίσως να μην θεωρείται συμμετρία, σύμφωνα με τον Ορισμό 4.1.1 είναι ένα στοιχείο του $S(M)$. Την λέμε δε *ταυτοτική συμμετρία* του M *ή ταυτοτικό στοιχείο* του $S(M)$.

Μια δεύτερη γενική ιδιότητα που προφανώς ισχύει μεταξύ των στοιχείων του συνόλου $S(M)$ είναι: Αν πριν ή μετά την εφαρμογή μιας συμμετρίας f επί του M εφαρμόσουμε την I, τότε το αποτέλεσμα είναι το ίδιο αν εφαρμόζαμε μόνο την f επί του M.

Όπως αναφέρθηκε προηγουμένως κάθε συμμετρία f του M είναι 1 - 1 και επί απεικόνιση (Άσκηση 4.1 (4)). Συνεπώς μπορούμε να δούμε ότι στην f αντιστοιχεί μια άλλη συμμετρία του M (η οποία ενδέχεται να είναι και η ίδια η f), που αν εφαρμοσθεί πριν ή μετά την εφαρμογή της f επί του M το αποτέλεσμα είναι το ίδιο με αυτό της I, δηλαδή αυτή είναι η αντίστροφη απεικόνιση f^{-1} της f. Αυτή είναι η τρίτη γενική ιδιότητα.

Τέλος μια τέταρτη γενική ιδιότητα που διακρίνουμε είναι η εξής. Αν εφαρμόσουμε διαδοχικά μία συμμετρία f_1 και μετά τη συμμετρία που πέρνουμε από τη διαδοχική εφαρμογή δύο συμμετριών f_2 και f_3, το αποτέλεσμα είναι το ίδιο με το αποτέλεσμα που προκύπτει αν εφαρμόσουμε πρώτα τη συμμετρία που προκύπτει από τη διαδοχική εφαρμογή της f_1 και f_2 και μετά εφαρμόσουμε την f_3.

Οι προηγούμενες ιδιότητες ουσιαστικά αναφέρονται στην ιδέα της ***"διαδοχικής εφαρμογής"*** που στη γλώσσα των απεικονίσεων είναι η σύνθεσή τους. Επομένως θα μπορούσαμε να πούμε ακριβέστερα ότι αυτές οι ιδιότητες είναι ιδιότητες του συνόλου $S(M)$ ως προς τη σύνθεση των στοιχείων του.

Εδώ θα θέλαμε να παρατηρήσουμε ότι αυτές οι ιδιότητες, αν και είναι πολύ εύκολο να αποδειχθεί ότι ισχύουν για το $S(M)$, ήταν πολύ δύσκολο για τον άνθρωπο να τις διαγνώσει και να διαβλέψει ότι θα έπαιζαν - όπως γνωρίζουμε σήμερα - θεμελιώδη ρόλο στην ανάπτυξη της σύγχρονης Άλγεβρας και γενικά στα Μαθηματικά.

Είναι σκόπιμο τώρα να διατυπώσουμε τις παραπάνω ιδιότητες χρησιμοποιώντας το σύμβολο "$\circ$" της σύνθεσης απεικονίσεων. Έτσι λέμε ότι το σύνολο $S(M)$ ως προς τη σύνθεση των στοιχείων του ικανοποιεί τις εξής ιδιότητες.

Α. Για οποιαδήποτε δύο στοιχεία $f,\ g$ του $S(M)$ ισχύει
$f \circ g \in S(M)$.

Β. Υπάρχει ένα στοιχείο I του $S(M)$ τέτοιο ώστε $I \circ f = f \circ I = f$, για κάθε στοιχείο f του $S(M)$.

Γ. Για κάθε $f \in S(M)$ υπάρχει ένα στοιχείο $f^{-1} \in S(M)$ - το αντίστροφο της f - τέτοιο ώστε $f \circ f^{-1} = f^{-1} \circ f = I$.

Δ. Για $f, g, h \in S(M)$ ισχύει $f \circ (g \circ h) = (f \circ g) \circ h$.

4.1.2 Ορισμός. *Το σύνολο $S(M)$, εφοδιασμένο με την σύνθεση απεικονίσεων "$\circ$" λέγεται* ***ομάδα συμμετριών*** *του M.*

4.1.3 Παραδείγματα.

1. Έστω M ένα ισοσκελές τρίγωνο που δεν είναι ισόπλευρο. Όπως έχουμε ήδη αναφέρει το M έχει μία μη τετριμμένη συμμετρία R για την οποία ισχύει
   $R \circ R = I$. Η ομάδα συμμετρίας $(S(M), \circ)$ είναι το σύνολο $\{I, R\}$. Εδώ το αντίστροφο στοιχείο του R είναι το R και του I το I.

2. Αν το M είναι το ισόπλευρο τρίγωνο που είχαμε θεωρήσει στην αρχή της παραγράφου,τότε η ομάδα συμμετρίας $(S(M), \circ)$ είναι το σύνολο $\{I, R_1, R_2, R_3, S_1, S_2\}$. Τα αντίστροφα των R_1, R_2, R_3, S_1 και S_2 είναι αντίστοιχα τα στοιχεία R_1, R_2, R_3, S_2 και S_1. Έχουμε δε, για παράδειγμα,
   $R_1 \circ R_1 = R_2 \circ R_2 = R_3 \circ R_3 = I, \quad R_3 \circ R_1 = S_1$ και $S_2 \circ R_3 = R_1$.

3. Διαισθητικά, ο κύκλος είναι ένα από τα γεωμετρικά σχήματα που έχουν τις περισσότερες συμμετρίες. Αυτό διαπιστώνεται βρίσκοντας την ομάδα συμμετρίας του. Έστω M ο μοναδιαίος κύκλος $x_1^2 + x_2^2 = 1$. Μπορούμε να δούμε ότι η ομάδα συμμετρίας $S(M)$ αποτελείται από όλους τους ορθογώνιους μετασχηματισμούς του $\mathbb{R}^2$ (Άσκηση 4.1 (6)). Αυτοί είναι αφενός

όλες οι στροφές, που εκφράζονται, ως προς τη βάση $\{(1,0),\ (0,1)\}$ υπό μορφήν πίνακα ως

$$A(\theta) = \begin{pmatrix} \sigma\upsilon\nu\,\theta & -\eta\mu\,\theta \\ \eta\mu\,\theta & \sigma\upsilon\nu\,\theta \end{pmatrix}$$

(στροφή γύρω από την αρχή των αξόνων κατά γωνία θ) και αφετέρου όλες οι ανακλάσεις ως προς τις ευθείες της μορφής

$$\mathcal{E}_\theta : x_1\,\eta\mu(\theta/2) - x_2\,\sigma\upsilon\nu(\theta/2) = 0$$

που διέρχονται από την αρχή των αξόνων και σχηματίζουν με τον άξονα x γωνία ίση με $\theta/2$. Αυτές εκφράζονται υπό μορφήν πίνακα, ως εξής

$$R(\theta) = \begin{pmatrix} \sigma\upsilon\nu\,\theta & \eta\mu\,\theta \\ \eta\mu\,\theta & -\sigma\upsilon\nu\,\theta \end{pmatrix}$$

Σημειώνουμε ότι ισχύουν οι σχέσεις $R(\theta)\circ R(\theta') = A(\theta-\theta')$ (άρα $R(\theta)\circ R(\theta) = I$), $R(\theta)\circ A(\theta') = R(\theta'-\theta)$, $A(\theta)\circ R(\theta') = R(\theta+\theta')$ και $A(\theta)\circ A(\theta') = A(\theta+\theta')$ (άρα $A(\theta)\circ A(-\theta) = I$). Αυτές οι ισότητες επιβεβαιώνουν τις αναφερθείσες ιδιότητες της $S(M)$. Η ομάδα συμμετρίας $S(M)$ ονομάζεται ***ορθογώνια ομάδα*** και τη συμβολίζουμε $O(\mathbb{R}^2)$. Αν τους ορθογώνιους μετασχηματισμούς τους θεωρήσουμε υπό μορφήν πινάκων, τότε την ορθογώνια ομάδα τη συμβολίζουμε $O_2(\mathbb{R})$.

Παρατήρηση. Από τις προηγούμενες ισότητες βλέπουμε ότι το σύνολο όλων των στροφών $A(\theta)$, σε σχέση με τη σύνθεση, ικανοποιεί και αυτό τις τέσσερεις ιδιότητες που ικανοποιεί η $O_2(\mathbb{R})$. Αυτό το σύνολο εφοδιασμένο με τη σύνθεση απεικονίσεων το ονομάζουμε ***ειδική ορθογώνια ομάδα*** και το συμβολίζουμε $SO_2(\mathbb{R})$. Βλέπουμε δε ότι

$$SO_2(\mathbb{R}) = \{T \in O_2(\mathbb{R}) \mid det\,T = 1\}.$$

Επίσης, για μία σταθερή ανάκλαση $R(\theta) \neq I$, ένα στοιχείο της $O_2(\mathbb{R})$ αν δεν είναι στοιχείο της $SO_2(\mathbb{R})$, θα είναι ένα στοιχείο του συνόλου

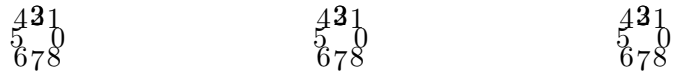
$$R(\theta)\,SO_2(\mathbb{R}) = \{R(\theta)A(\theta') \mid 0 < \theta' \leq 2\pi\},$$

δηλαδή $O_2(\mathbb{R}) = SO_2(\mathbb{R})\dot{\cup}R(\theta)\,SO_2(\mathbb{R})$ (ξένη ένωση). Ας σημειωθεί ότι κάτι ανάλογο δεν ισχύει για το σύνολο των ανακλάσεων, αφού η σύνθεση δύο ανακλάσεων είναι μια στροφή.

4. Μια άλλη ομάδα συμμετρίας, με την οποία θα ασχοληθούμε λεπτομερέστερα αργότερα, είναι αυτή ενός κανονικού πολυγώνου Π_n με n κορυφές, το οποίο είναι εγγεγραμμένο σε κύκλο (έστω τον μοναδιαίο) κέντρου O. Έστω $0, 1, \ldots, n-1$ οι κορυφές του. Κάθε φυσικός αριθμός d πρώτος προς τον n και μικρότερος του $n/2$ ορίζει ένα κανονικό πολύγωνο $\Pi_{n,d}$, του οποίου οι πλευρές είναι αυτές που ενώνουν την κορυφή i με την κορυφή $(i+d) \bmod n$. Υπάρχουν $\frac{1}{2}\phi(n)$ το πλήθος κανονικά πολύγωνα με κορυφές τις $0, 1, \ldots, n-1$ (Άσκηση 4.1 (9)), όπου ϕ είναι η συνάρτηση του Euler (δηλαδή $\phi(n)$ είναι το πλήθος των φυσικών αριθμών μικροτέρων του n και πρώτων προς το n). Για παράδειγμα, αν $n = 5$, τότε υπάρχουν δύο κανονικά πολύγωνα (σχήμα 4.1.5).

Σχήμα 4.1.5

Ενώ για $n = 9$ υπάρχουν τρία κανονικά πολύγωνα (σχήμα 4.1.6).



Σχήμα 4.1.6

Όλα αυτά τα κανονικά πολύγωνα έχουν την ίδια ομάδα συμμετρίας, η οποία μπορεί να μελετηθεί μέσω του (μοναδικού) κυρτού κανονικού πολυγώνου $\Pi_{n,1}$. Κάθε $T \in S(\Pi_{n,1})$ αφήνει το O σταθερό και άρα $S(\Pi_{n,1}) \subseteq O_2(\mathbb{R})$. Η $S(\Pi_{n,1})$ περιέχει τη στροφή ϱ γύρω από το O κατά γωνία $2\pi/n$ που παριστάνεται αλγεβρικά με τον πίνακα $A = A(2\pi/n)$. Επίσης, αυτή περιέχει και όλες τις στροφές

$$A(2\pi\kappa/n) = \underbrace{(A \circ A \circ \cdots \circ A)}_{\kappa}, \quad 1 \leq \kappa \leq n.$$

Το σύνολο αυτών των στροφών ικανοποιεί τις τέσσερεις ιδιότητες που ικανοποιεί και η $S(\Pi_{n,1})$ και είναι υποσύνολο της $SO_2(\mathbb{R})$, δηλαδή

$$\{A(2\pi\kappa/n) \mid 1 \leq \kappa \leq n\} = S(\Pi_{n,1}) \cap SO_2(\mathbb{R}).$$

Το πολύγωνο $\Pi_{n,1}$ (όπως και κάθε $\Pi_{n,d}$) έχει n άξονες συμμετρίας. Αν ο n είναι άρτιος, τότε υπάρχουν δύο τύποι αξόνων: $n/2$ το πλήθος άξονες που διέρχονται από απέναντι κορυφές και $n/2$ άξονες που διέρχονται από τα μέσα απέναντι πλευρών. Αν ο n είναι περιττός, τότε κάθε πλευρα έχει απέναντί της μία κορυφή, ενώ κάθε άξονας συμμετρίας διέρχεται από το μέσον μιας πλευράς και από την απέναντι κορυφή. Έστω σ η ανάκλαση ως προς τον άξονα που διέρχεται από την κορυφή 0 και ας θεωρήσουμε αυτόν τον άξονα σαν τον x-άξονα στο $\mathbb{R}^2$. Στην ανάκλαση σ αντιστοιχεί ο πίνακας $R(0) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, ενώ στις άλλες ανακλάσεις αντιστοιχούν οι πίνακες $R(2\pi j/n)$, $j = 0, 1, \ldots, n-1$ (δες Παράδειγμα 3). Άρα η ομάδα $S(\Pi_{n,1})$ αποτελείται από τις στροφές $A(2\pi j/n)$, $j = 0, 1, \ldots, n-1$ και τις ανακλάσεις $R(2\pi j/n) = R(0) \cdot A(2\pi j/n)$, δηλαδή η $S(\Pi_{n,1})$ έχει $2n$ στοιχεία. Επίσης βλέπουμε ότι ισχύει $R(0) \cdot R(0) = I$, $\underbrace{(A \circ A \circ \cdots \circ A)}_{n} = I$ και $R(0) \cdot A \cdot R(0) = \underbrace{(A \circ A \circ \cdots \circ A)}_{n-1}$.

Η ομάδα $S(\Pi_{n,1})$ ονομάζεται ***διεδρική ομάδα*** και τη συμβολίζουμε με D_n.

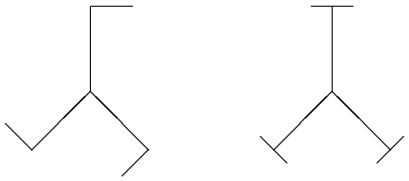
Από τα προηγούμενα παραδείγματα βλέπουμε ότι η ομάδα συμμετρίας ενός υποσυνόλου M του $\mathbb{R}^n$ μας δίνει ένα μέτρο συμμετρίας του M, δηλαδή μας λέει πόσο συμμετρικό είναι το M. Όσο μεγαλύτερη είναι η ομάδα συμμετρίας του M τόσο πιο συμμετρικό είναι το M. Για παράδειγμα ο κύκλος είναι μεταξύ των σχημάτων του επιπέδου, που έχουν τις περισσότερες συμμετρίες, αφού η ομάδα συμμετρίας του αποτελείται από όλους τους ορθογώνιους μετασχηματισμούς του $\mathbb{R}^2$, ενώ η ομάδα συμμετρίας ενός σκαλινού τριγώνου αποτελείται μόνο από την ταυτοτική απεικόνιση.

Για μια λεπτομερή μελέτη κανονικών σχημάτων ο αναγνώστης παραπέμπεται στο βιβλίο του H. S. M. Coxeter, *"Regular Polytopes"* [8].

Ασκήσεις 4.1

1. Ποιες είναι οι δυνατές μεταθέσεις των κορυφών ενός τετραγώνου που δεν αντιστοιχούν σε συμμετρίες του τετραγώνου ;

2. Να βρεθούν οι ομάδες συμμετρίας των σχημάτων



3. Ποιες είναι οι ομάδες συμμετρίας των γραφημάτων των εξισώσεων
   α) $y = x^2$, β) $3x^2 + 4y^2 = 12$, γ) $xy = 1$;

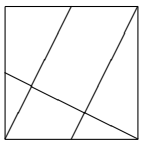
4. Δείξτε ότι κάθε ισομετρία του $\mathbb{R}^n$ μπορεί να γραφτεί μοναδικά ως $g \circ \tau$, όπου g είναι ένας ορθογώνιος μετασχηματισμός και τ είναι μια μετατόπιση. Από αυτό να συμπεράνετε ότι μια ισομετρία είναι $1-1$ και επί απεικόνιση.

5. Ταξινομείστε όλα τα κεφαλαία γράμματα της αλφαβήτου ως προς τις ομάδες συμμετρίας των. (Θεωρήστε το O ως μια έλλειψη).

6. Δείξτε ότι η ομάδα συμμετρίας του μοναδιαίου κύκλου αποτελείται από όλους τους ορθογώνιους μετασχηματισμούς του $\mathbb{R}^2$.

7. Ποια είναι η ομάδα συμμετρίας μιας 4×4 σκακιέρας με εναλλασσόμενα άσπρα-μαύρα τετραγωνίδια; Το ίδιο ερώτημα για μια 3×3 σκακιέρα.

8. Προσθέστε στο επόμενο σχήμα μια ευθεία ούτως ώστε το σχήμα να γίνει όσο το δυνατόν περισσότερο συμμετρικό.



9. Δείξτε ότι υπάρχουν $\frac{1}{2}\,\phi(n)$ το πλήθος κανονικά πολύγωνα με κορυφές τις $0, 1, \ldots, n-1$, όπου ϕ είναι η συνάρτηση του Euler.

10. Σχεδιάστε ένα επίπεδο σχήμα έτσι ώστε

    α) να περιλαμβάνει δύο ορθογώνια παραλληλόγραμμα και η ομάδα συμμετρίας του να είναι η D_4.

    β) να περιλαμβάνει τρία ισόπλευρα τρίγωνα και η ομάδα συμμετρίας του να είναι η D_3.

11. Δείξτε ότι η διεδρική ομάδα D_n έχει ακριβώς $n + \dfrac{1}{2} + \dfrac{(-1)^n}{2}$ στοιχεία x τέτοια ώστε $x \circ x = 1$.

4.2 Μεταθέσεις και Συμμετρικές Ομάδες

Ένα από τα σημαντικότερα παραδείγματα πεπερασμένων ομάδων είναι οι συμμετρικές ομάδες. Ένας από τους λόγους για τους οποίους αυτές παίζουν σημαντικό ρόλο στην όλη θεωρία των ομάδων οφείλεται, όπως θα δούμε στα επόμενα, στο θεώρημα του Cayley. Ουσιαστικά αυτό αναφέρει ότι η μελέτη των πεπερασμένων ομάδων ανάγεται στην μελέτη των ομάδων μεταθέσεων.

Είναι λοιπόν σκόπιμο εδώ να μελετήσουμε αρκετές από τις ιδιότητες των συμμετρικών ομάδων αφού αυτές θα μας βοηθήσουν να κατανοήσουμε τη "δομή" των ομάδων.

Έστω X ένα μη κενό σύνολο. Μία απεικόνιση $\sigma : X \longrightarrow X$ που είναι 1 - 1 και επί λέγεται ***μετάθεση*** του X. Παραδείγματος χάριν, αν X είναι οι πραγματικοί αριθμοί $\mathbb{R}$, η απεικόνιση $\sigma : \mathbb{R} \longrightarrow \mathbb{R}$, $\sigma(x) = e^x$, είναι 1 - 1 αλλά δεν είναι επί, αφού $\sigma(\mathbb{R}) = \mathbb{R}^+$ είναι οι θετικοί πραγματικοί αριθμοί και συνεπώς η σ δεν είναι μετάθεση. Αν X είναι οι ακέραιοι $\mathbb{Z}$ και $\sigma : \mathbb{Z} \longrightarrow \mathbb{Z}$, $\sigma(x) = x+1$, τότε η σ είναι μία μετάθεση του $\mathbb{Z}$. Στα επόμενα θα θεωρούμε το σύνολο X να είναι πεπερασμένο, δηλαδή θα θεωρούμε μεταθέσεις πεπερασμένων συνόλων. Παραδείγματος χάρη, αν $X = \{1, 2, 3, 4\}$, η απεικόνιση $\sigma : X \longrightarrow X$ με $\sigma(1) = 3$, $\sigma(2) = 2$, $\sigma(3) = 4$ και $\sigma(4) = 1$ είναι μία μετάθεση του X, ενώ η απεικόνιση $\sigma : X \longrightarrow X$ με $\sigma(1) = 2$, $\sigma(2) = 1$, $\sigma(3) = 3$ και $\sigma(4) = 3$ δεν είναι. Ένα άλλο παράδειγμα είναι το εξής. Έστω X το σύνολο όλων των κορυφών ενός κανονικού κυρτού πολυγώνου που έχει n κορυφές. Τότε μπορούμε εύκολα να δούμε ότι όλες οι συμμετρίες του ορίζουν μεταθέσεις του X. Θα δούμε αργότερα πως οι μεταθέσεις μπορούν να χρησιμοποιηθούν σαν ένα βασικό εργαλείο για την περιγραφή των συμμετριών ενός γεωμετρικού σχήματος.

Όπως θα διαπιστωθεί πιο κάτω τα στοιχεία του συνόλου X δεν παίζουν κανένα ουσιαστικό ρόλο στη μελέτη των μεταθέσεων και είναι κοινή αποδοχή, για λόγους ευκολίας, να θεωρούμε για ένα σύνολο με n στοιχεία το σύνολο $X = \{1, 2, \ldots, n\}$. Επίσης μία μετάθεση σ του X συνήθως περιγράφεται από ένα πίνακα με 2 γραμμές και n στήλες. Η πρώτη γραμμή αποτελείται από τους αριθμούς $1, 2, \ldots, n$ και η δεύτερη γραμμή από τους αριθμούς $\sigma(1), \sigma(2), \ldots, \sigma(n)$, όπου $\sigma(i)$ είναι η εικόνα του i μέσω της σ, δηλαδή παριστάνουμε τη σ ως

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}.$$

Για παράδειγμα, αν $n = 3$, τότε έχουμε τις εξής έξι μεταθέσεις του

$X = \{1, 2, 3\}$.

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

4.2.1 Πρόταση. *Για το σύνολο $X = \{1, 2, \ldots, n\}$ υπάρχουν $n!$ το πλήθος μεταθέσεις.*

Απόδειξη. Έστω σ μία μετάθεση του X. Θεωρώντας την παράσταση της σ, βλέπουμε ότι υπάρχουν n επιλογές για την εικόνα $\sigma(1)$ του 1. Επιλέγοντας μία εικόνα για το 1, έχουμε $n-1$ επιλογές για την εικόνα του 2 (αφού η σ είναι 1-1). Συνεχίζοντας με τον ίδιο τρόπο, έχοντας επιλέξει τις εικόνες των $1, 2, \ldots, n-1$, έχουμε μόνο μία επιλογή για την εικόνα του n. Άρα ο συνολικός αριθμός των δυνατών επιλογων για τη σ είναι $n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 2 \cdot 1 = n!$. ⊤

Αν σ_1 και σ_2 είναι δύο μεταθέσεις του $X = \{1, 2, \ldots, n\}$ τότε η σύνθεσή τους $\sigma_2 \circ \sigma_1$ είναι μία απεικόνιση $X \to X$. Αυτό όμως που είναι σημαντικό, όπως και στις συμμετρίες γεωμετρικών σχημάτων, είναι ότι η απεικόνιση $\sigma_2 \circ \sigma_1$ είναι και αυτή μία μετάθεση του X, αφου και οι δύο απεικονίσεις είναι 1 - 1 και επί.

Την μετάθεση $\sigma_2 \circ \sigma_1$ θα την ονομάζουμε ***γινόμενο*** των σ_1 και σ_2 και θα γράφουμε απλά $\sigma_2\,\sigma_1$ παραλείποντας το σύμβολο $\circ$ της σύνθεσης απεικονίσεων. Επίσης λέμε ότι το γινόμενο $\sigma_2\,\sigma_1$ είναι το αποτέλεσμα της σ_1 επι την σ_2. Αν θεωρούσαμε το γινόμενο $\sigma_1\,\sigma_2$, θα λέγαμε ότι έχουμε το αποτέλεσμα της σ_2 επί την σ_1.

Η παράσταση του γινομένου $\sigma_2\,\sigma_1$ σε $2 \times n$ πίνακα είναι

$$\begin{pmatrix} 1 & 2 & \cdots & \sigma_1(i) & \cdots & n \\ \sigma_2(1) & \sigma_2(2) & \cdots & \sigma_2\,\sigma_1(i) & \cdots & \sigma_2(n) \end{pmatrix} \circ$$

$$\begin{pmatrix} 1 & 2 & \cdots & i & \cdots & n \\ \sigma_1(1) & \sigma_1(2) & \cdots & \sigma_1(i) & \cdots & \sigma_1(n) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & n \\ (\sigma_2\,\sigma_1)(1) & (\sigma_2\,\sigma_1)(2) & \cdots & (\sigma_2\,\sigma_1)(i) & \cdots & (\sigma_2\,\sigma_1)(n) \end{pmatrix}.$$

Για παράδειγμα έχουμε

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix}$$

αφού $1 \xrightarrow{\sigma_1} 3 \xrightarrow{\sigma_2} 1$ και άρα $1 \xrightarrow{\sigma_2\sigma_1} 1$, $2 \xrightarrow{\sigma_1} 2 \xrightarrow{\sigma_2} 3$
και άρα $2 \xrightarrow{\sigma_2\sigma_1} 3$, $3 \xrightarrow{\sigma_1} 4 \xrightarrow{\sigma_2} 5$ και άρα $3 \xrightarrow{\sigma_2\sigma_1} 5$, $4 \xrightarrow{\sigma_1} 1 \xrightarrow{\sigma_2} 2$ και άρα $4 \xrightarrow{\sigma_2\sigma_1} 2$, και τέλος $5 \xrightarrow{\sigma_1} 5 \xrightarrow{\sigma_2} 4$ και άρα $5 \xrightarrow{\sigma_2\sigma_1} 4$.

Επισημαίνουμε ότι γενικά για το γινόμενο μεταθέσεων, δεν ισχύει $\sigma_1\sigma_2 = \sigma_2\sigma_1$. Πράγματι στο προηγούμενο παράδειγμα, όπως εύκολα διαπιστώνουμε, έχουμε $\sigma_1\sigma_2 \neq \sigma_2\sigma_1$, αφού $(\sigma_1\sigma_2)(1) = 2$
$\neq (\sigma_2\sigma_1)(1) = 1$.

Μεταξύ των μεταθέσεων του $X = \{1, 2, \ldots, n\}$ περιλαμβάνεται και η ταυτοτική μετάθεση του X, την οποία συνήθως την συμβολίζουμε με i_X ή απλά με i, δηλαδή η απεικόνιση του X για την οποία η εικόνα του τυχαίου στοιχείου x του X είναι το x. Είναι φανερό ότι για κάθε μετάθεση σ του X ισχύει $i\sigma = \sigma i = \sigma$. Η παράσταση της ταυτοτικής μετάθεσης σε $2 \times n$ πίνακα είναι προφανώς η

$$i = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & n \\ 1 & 2 & \cdots & i & \cdots & n \end{pmatrix}$$

Επίσης για κάθε μετάθεση σ του X, αφού η σ είναι 1 - 1 και επί, ορίζεται η αντίστροφη απεικόνιση $\sigma^{-1} : X \longrightarrow X$ με $\sigma^{-1}(x) = y$, όπου $\sigma(y) = x$. Η σ^{-1} είναι και αυτή 1 - 1 και επί, δηλαδή μία μετάθεση του X. Για το γινόμενο μεταθέσεων η σ^{-1} ικανοποιεί τη σχέση $\sigma\sigma^{-1} = \sigma^{-1}\sigma = i$. Αν η σ παρασταθεί σε μορφή $2 \times n$ πίνακα, τότε η αντίστροφή της παριστάνεται από τον $2 \times n$ πίνακα που ορίζεται ως εξής. Κατ' αρχήν εναλλάσουμε τις δύο γραμμές του πίνακα της σ και κατόπιν τοποθετούμε τις στήλες έτσι ώστε πάλι η πρώτη γραμμή να είναι η $1, 2, \ldots, n$. Για παράδειγμα έστω $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 6 & 4 & 1 \end{pmatrix}$. Για να καθορίσουμε τη μορφή της σ^{-1} θεωρούμε τον πίνακα $\begin{pmatrix} 3 & 2 & 5 & 6 & 4 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$ που προκύπτει από την εναλλάγη των γραμμών του πίνακα της σ και κατόπιν διατάσουμε τις στήλες έτσι ώστε η πρώτη γραμμή να είναι η $1\,2\,3\,4\,5\,6$, δηλαδή έχουμε

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 1 & 5 & 3 & 4 \end{pmatrix}$$

Για το γινόμενο $\sigma\sigma^{-1}$ αυτού του παραδείγματος βλέπουμε πράγματι ότι

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 6 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 1 & 5 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}.$$

Τέλος η ιδιότητα της προσεταιριστικότητας $\sigma_3\,(\,\sigma_2\,\sigma_1\,) = (\,\sigma_3\,\sigma_2\,)\,\sigma_1$ ισχύει για το γινόμενο μεταθέσεων, αφού ισχύει γενικά για τη σύνθεση οποιωνδήποτε απεικονίσεων του X. Έτσι αντί για $\sigma_3\,(\,\sigma_2\,\sigma_1\,)$ θα γράφουμε απλά $\sigma_3\,\sigma_2\,\sigma_1$.

Από εδώ και στο εξής θα συμβολίζουμε με S_n το σύνολο όλων των μεταθέσεων του $X = \{\,1, 2, \ldots, n\,\}$. Όπως είδαμε προηγουμένως, για το σύνολο S_n η σύνθεση μεταθέσεων, ικανοποιεί τις τέσσερεις ιδιότητες που ικανοποιεί και η σύνθεση των στοιχείων της ομάδας συμμετρίας ενός μη κενού υποσυνόλου του Ευκλειδείου χώρου $\mathbb{R}^n$ (δηλαδή τις ιδιότητες (A), (B), (Γ) και (Δ)).

4.2.2 Ορισμός. *Το σύνολο S_n ονομάζεται* ***συμμετρική ομάδα βαθμού*** *n, όταν μαζί με αυτό θεωρήσουμε και την σύνθεση των στοιχείων του. Ένα μη κενό υποσύνολο G της S_n θα ονομάζεται* ***ομάδα μεταθέσεων βαθμού*** *n αν για κάθε δύο στοιχεία σ_1, σ_2 του G το γινόμενο $\sigma_2\,\sigma_1$ είναι ένα στοιχείο του G, δηλαδή $\sigma_2\,\sigma_1 \in G$.*

4.2.3 Παράδειγμα. Θεωρούμε τη συμμετρική ομάδα S_4 και το υποσύνολό της

$$H = \left\{ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},\ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \right.$$
$$\left. \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \right\}$$

Εύκολοι υπολογισμοί δίνουν ότι $\sigma_1\sigma_2 = \sigma_2\sigma_1 = \sigma_3 \in H$, $\sigma_1\sigma_3 = \sigma_3\sigma_1 = \sigma_2 \in H$, $\sigma_2\sigma_3 = \sigma_3\sigma_2 = \sigma_1 \in H$, αλλά $\sigma_1\sigma_1 = \sigma_2\sigma_2 = \sigma_3\sigma_3 = i \notin H$. Άρα το H δεν είναι ομάδα μεταθέσεων. Αν στο H επισυνάψουμε και την ταυτοτική μετάθεση i, αν δηλαδή θεωρήσουμε το υποσύνολο $G = H \cup \{\,i\,\}$, τότε το G είναι μια ομάδα μεταθέσεων βαθμού 4.

Επίσης το υποσύνολο $\left\{ i,\ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix},\ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \right\}$ της S_4 είναι μια ομάδα μεταθέσεων βαθμού 4. Ας παρατηρήσουμε εδώ ότι οι μεταθέσεις αυτού του συνόλου αφήνουν το 4 σταθερό και συνεπώς θα μπορούσαν να θεωρηθούν μεταθέσεις βαθμού 3. Δηλαδή αν το k, όπου $k \leq n$, είναι ο μεγαλύτερος φυσικός αριθμός που δεν μένει σταθερός κάτω από μια μετάθεση $\sigma \in S_n$, τότε αυτή η μετάθεση μπορεί να θεωρηθεί στοιχείο της S_k. Με άλλα λόγια, μπορούμε να θεωρήσουμε τη συμμετρική ομάδα S_k σαν μια ομάδα μεταθέσεων βαθμού n για κάθε $n \geq k$.

4.2.4 Πρόταση. *Έστω G μία ομάδα μεταθέσεων βαθμού n. Τότε η ταυτοτική μετάθεση i είναι ένα στοιχείο της G. Επίσης η αντίστροφη μετάθεση μιας οποιασδήποτε μετάθεσης που ανήκει στη G είναι στοιχείο της G.*

Απόδειξη. Είδαμε ότι το σύνολο S_n είναι πεπερασμένο σύνολο και συνεπώς το G είναι πεπερασμένο σύνολο. Έστω $G = \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$. Αφού το G είναι μία ομάδα μεταθέσεων, για ένα τυχαίο $\sigma \in G$, τα γινόμενα

$$\sigma\sigma_1, \sigma\sigma_2, \ldots, \sigma\sigma_k$$

είναι στοιχεία της G. Όλα αυτά τα γινόμενα είναι ανά δύο διάφορα μεταξύ τους και συνεπώς αυτά είναι όλα τα k στοιχεία της G. Πράγματι, αν υπήρχαν δείκτες $s,\ r$ με $s \neq r$ έτσι ώστε $\sigma\sigma_s = \sigma\sigma_r$, τότε θα είχαμε και $\sigma_s = (\sigma^{-1}\sigma)\sigma_s = \sigma^{-1}(\sigma\sigma_s) = \sigma^{-1}(\sigma\sigma_r) = (\sigma^{-1}\sigma)\sigma_r) = \sigma_r$, που είναι άτοπο. Άρα για το τυχαίο στοιχείο σ της G θα πρέπει να υπάρχει ένα στοιχείο σ_ℓ της G τέτοιο ώστε $\sigma\sigma_\ell = \sigma$. Αυτό σημαίνει ότι $\sigma_\ell = i$, δηλαδή $i \in G$. Για τον ίδιο λόγο, αφού η i είναι ένα από τα $\sigma_j,\quad j = 1, 2, \ldots, k$, θα πρέπει να υπάρχει $s,\ 1 \leq s \leq k$, τέτοιο ώστε $\sigma\sigma_s = i$ και άρα $\sigma_s = \sigma^{-1} \in G$. ⊤

4.2.5 Παρατήρηση. Από την προηγούμενη πρόταση βλέπουμε ότι αν ένα υποσύνολο G είναι μία ομάδα μεταθέσεων βαθμού n, τότε οι τέσσερεις ιδιότητες που ικανοποιεί η σύνθεση των στοιχείων της S_n ικανοποιούνται όταν περιορισθούμε στη σύνθεση των στοιχείων του συνόλου G. Φυσικά, η προσεταιριστική ιδιότητα του περιορισμού του γινομένου στο G ικανοποιείται αφου ισχύει για όλα τα στοιχεία της S_n.

Στην πρώτη Ενότητα του βιβλίου είδαμε ότι οι πρώτοι αριθμοί παίζουν σημαντικό ρόλο στις ιδιότητες των φυσικών αριθμών. Υπενθυμίζουμε ότι η θεμελιώδης ιδιότητα γι' αυτούς είναι ότι κάθε φυσικός αριθμός, διάφορος των 0 και 1, αναλύεται μοναδικά σε γινόμενο πρώτων αριθμών. Εδώ θα δούμε ότι για τις μεταθέσεις ισχύει κάτι ανάλογο. Για τον ορισμό αυτών των μεταθέσεων κατ' αρχήν χρειάζεται να ορίσουμε τις δυνάμεις μιας μετάθεσης.

Έστω $\sigma \in S_n$ και k ένας μη αρνητικός ακέραιος. Ορίζουμε επαγωγικά το γινόμενο της σ επί τον εαυτό της k φορές που συμβολίζεται σ^k ως εξής.

$$\sigma^0 = i,\ \sigma^1 = \sigma,\ \sigma^2 = \sigma\circ\sigma, \ldots, \sigma^k = (\sigma^{k-1})\circ\sigma$$

Επίσης για $k < 0$ ορίζουμε την μετάθεση σ^k να είναι η αντίστροφη της σ^{-k}. Η μετάθεση σ^k, για $k \in \mathbb{Z}$, ονομάζεται ***k*-δύναμη** της σ.

Η επόμενη πρόταση δίνει τις "συνήθεις" ιδιότητες των δυνάμεων. Η απόδειξή της γίνεται με επαγωγή και αφήνεται ως άσκηση.

4.2.6 Πρόταση. *Έστω $\sigma \in S_n$ και $n,\ m$ ακέραιοι αριθμοί. Τότε*

1. $\sigma^{n+m} = \sigma^n\sigma^m = \sigma^m\sigma^n$.

2. $\sigma^{mn} = (\sigma^m)^n$.

3. $\sigma^{-n} = (\sigma^{-1})^n = (\sigma^n)^{-1}$, *δηλαδή η αντίστροφη της* σ^n *είναι η* σ^{-n}.

4.2.7 Παράδειγμα. Έστω $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 1 & 6 & 5 \end{pmatrix}$. Για τις δυνάμεις της σ έχουμε

$$\sigma^2 = \sigma\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 5 & 6 \end{pmatrix},$$
$$\sigma^3 = \sigma^2\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 2 & 6 & 5 \end{pmatrix},$$
$$\sigma^4 = \sigma^3\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = i.$$

Γενικά, για $k \in \mathbb{N}$, η $k-$δύναμη σ^k, της σ στο παράδειγμα, μπορεί να υπολογισθεί ως εξής. Διαιρούμε το k με το 4, $k = 4\pi + \upsilon,\ 0 \leq \upsilon \leq 3$. Από την προηγούμενη πρόταση έχουμε, $\sigma^k = \sigma^{4\pi+\upsilon} = (\sigma^4)^\pi\sigma^\upsilon = i^\pi\sigma^\upsilon = \sigma^\upsilon$. Δηλαδή η δύναμη σ^k της σ εξαρτάται μόνο από την κλάση υπολοίπων του $k \bmod 4$ και θα ισούται με μία από τις δυνάμεις σ^0, σ^1, σ^2, σ^3. Η αντίστροφη μετάθεση σ^{-1} της σ μπορεί να υπολογιστεί με τον κανόνα που περιγράψαμε προηγουμένως. Επίσης μπορεί ευκολότερα να υπολογισθεί από τη σχέση $\sigma^4 = i$. Πράγματι, αυτή η σχέση είναι ισοδύναμη με τη σχέση $\sigma^3 = \sigma^{-1}$, από την οποία καθορίζονται και όλες οι αρνητικές δυνάμεις της σ.

Είναι ευκαιρία να επισημάνουμε εδώ ότι για κάθε μη ταυτοτική μετάθεση $\sigma \in S_n$, όταν $n \geq 3$, υπάρχει τουλάχιστον μία άλλη μετάθεση σ' για την οποία $\sigma\,\sigma' \neq \sigma'\,\sigma$ (Άσκηση 4.2.18). Όταν για δύο μεταθέσεις σ_1 και σ_2 της S_n ισχύει $\sigma_1\,\sigma_2 = \sigma_2\,\sigma_1$, τότε λέμε ότι αυτές ***μετατίθενται***. Επίσης λέμε ότι αυτές είναι ***ξένες*** μεταξύ τους αν $\{\, i : \sigma_1(i) \neq i \,\} \cap \{\, j : \sigma_2(j) \neq j \,\} = \emptyset$.

4.2.8 Παράδειγμα.

Οι μεταθέσεις $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ και $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$ είναι ξένες μεταξύ τους και μετατίθενται.

Οι μεταθέσεις $\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ και $\tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ μετατίθενται αλλά δεν είναι ξένες μεταξύ τους. Γενικότερα ισχύει το εξής.

4.2.9 Λήμμα. *Αν οι μεταθέσεις* $\sigma_1,\ \sigma_2 \in S_n$ *είναι ξένες μεταξύ τους, τότε μετατίθενται.*

Απόδειξη. Διακρίνουμε δύο περιπτώσεις. Έστω $x \in X$ με $\sigma_1(x) = x$. Θα δείξουμε ότι $(\sigma_1\,\sigma_2)(x) = (\sigma_2\,\sigma_1)(x)$. Πράγματι, αν $\sigma_2(x) = x$, τότε προφανώς

$(\sigma_1\,\sigma_2)(x) = (\sigma_2\,\sigma_1)(x) = x$. Αν $\sigma_2(x) \neq x$, τότε $(\sigma_2\,\sigma_2)(x) \neq \sigma_2(x)$, οπότε επειδή οι σ_1 και σ_2 είναι ξένες μεταξύ τους έχουμε $(\sigma_1\,\sigma_2)(x) = \sigma_2(x)$ και $(\sigma_2\,\sigma_1)(x) = \sigma_2(x)$. Έστω τώρα $x \in X$ με $\sigma_1(x) \neq x$. Τότε $\sigma_2(x) = x$, οπότε εναλλάσοντας τους ρόλους των σ_2 και σ_1 έχουμε την προηγούμενη περίπτωση. Άρα για κάθε $x \in X$ ισχύει $(\sigma_1\,\sigma_2)(x) = (\sigma_2\,\sigma_1)(x)$, δηλαδή οι δύο μεταθέσεις μετατίθενται. ⊺

Κυκλικές Μεταθέσεις

Ορίζουμε τώρα τις κυκλικές μεταθέσεις στις οποίες βασίζεται το θεμελιώδες θεώρημα των μεταθέσεων.

4.2.10 Ορισμός. *Μία μετάθεση $\sigma \in S_n$ ονομάζεται* ***κυκλική ή k - κύκλος*** *αν για ένα υποσύνολο $\{x_1, x_2, \ldots, x_k\}$ του X ισχύει $\sigma(x_i) = x_{i+1}$, για $i = 1, 2, \ldots, k-1$ και $\sigma(x_k) = x_1$, ενώ για κάθε άλλο $x \in X$ με $x \neq x_i$, $i = 1, 2, \ldots, k$ ισχύει $\sigma(x) = x$. Το πλήθος k των στοιχείων του συνόλου $\{x_1, x_2, \ldots, x_k\}$ λέγεται* ***μήκος*** *της σ.*

Για λόγους διευκόλυνσης στους υπολογισμούς και οικονομίας χώρου, συνηθίζεται ο προηγούμενος k - κύκλος να γράφεται στη μορφή

$$\sigma = (x_1\, x_2 \cdots x_k).$$

4.2.11 Παραδείγματα.

1. Όλοι οι 1 - κύκλοι, δηλαδή οι κυκλικές μεταθέσεις μήκους 1, συμπίπτουν με την ταυτοτική μετάθεση (γιατί;).

2. Όλα τα στοιχεία της S_3 είναι κυκλικές μεταθέσεις (γιατί;).

3. Οι κυκλικές μεταθέσεις της S_4 είναι οι εξής.

   2 - κύκλοι
   $(1\,2)$, $(1\,3)$, $(1\,4)$, $(2\,3)$, $(2\,4)$, $(3\,4)$.

   3 - κύκλοι
   $(1\,2\,3)$, $(1\,3\,2)$, $(1\,2\,4)$, $(1\,4\,2)$, $(1\,3\,4)$, $(1\,4\,3)$, $(2\,3\,4)$, $(2\,4\,3)$.

   4 - κύκλοι
   $(1\,2\,3\,4)$, $(1\,4\,3\,2)$, $(1\,3\,2\,4)$, $(1\,4\,2\,3)$, $(1\,2\,4\,3)$, $(1\,3\,4\,2)$.

Δηλαδή η S_4 έχει 21 κυκλικές μεταθέσεις. Οι μη κυκλικές μεταθέσεις είναι οι $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$, $\rho = \sigma\,\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$.

4.2.12 Παρατηρήσεις.

1. Αν $\sigma = (x_1\, x_2 \cdots x_k)$ είναι ένας $k-$κύκλος, τότε $\sigma^s(x_1) = x_{1+s}$ για κάθε $s = 0, 1, \ldots, k-1$ και $\sigma^k(x_1) = x_1$.
   Αντίστροφα, αν σ είναι μια μετάθεση του X για την οποία υπάρχει ένα $x \in X$ τέτοιο ώστε τα μόνα στοιχεία του X που δεν μένουν σταθερά μέσω της σ είναι αυτά που ανήκουν στο σύνολο $\Sigma = \{x, \sigma(x), \sigma^2(x), \sigma^3(x), \ldots\}$, τότε αυτή είναι μία κυκλική μετάθεση. Πράγματι, επειδή το Σ είναι περπερασμένο, μπορούμε να θεωρήσουμε τον μικρότερο θετικό ακέραιο k με την ιδιότητα $\sigma^k(x) = x$. Άρα $\Sigma = \{x, \sigma(x), \sigma^2(x), \ldots, \sigma^{k-1}(x)\}$, όπου $\sigma^k(x) = x$.

2. Ο συμβολισμός $(x_1\, x_2 \cdots x_k)$ ενός $k-$κύκλου δεν μας δηλώνει σε ποια συμμετρική ομάδα S_n ανήκει, ενώ ο συμβολισμός σε $2 \times n$ πίνακα το δηλώνει. Για παράδειγμα, η κυκλική μετάθεση $(1\,2\,3)$ ανήκει στην S_3, αλλά θα μπορούσε να ανήκει και σε οποιαδήποτε άλλη S_n για $n \geq 3$. Στην πράξη αυτό δεν δημιουργεί σύγχυση, καθώς αν m είναι ο μεγαλύτερος φυσικός αριθμός μεταξύ των $x_j,\ j = 1, 2, \ldots, k$, τότε η S_m, όπως έχουμε ήδη παρατηρήσει, μπορεί να ταυτιστεί με την ομάδα μεταθέσεων που αποτελείται απ' όλες τις μεταθέσεις της $S_n,\ n \geq m$, που αφήνουν σταθερά όλα τα στοιχεία που είναι μεγαλύτερα του m.

3. Αν $(x_1\, x_2 \cdots x_k)$ και $(y_1\, y_2 \cdots y_\ell)$ είναι δύο κυκλικές μεταθέσεις με $\{x_1, x_2, \ldots, x_k\} \cap \{y_1, y_2, \ldots, y_\ell\} = \emptyset$, τότε αυτές είναι ξένες μεταξύ τους και συνεπώς μετατίθενται, σύμφωνα με το Λήμμα 4.2.9. Οι μεταθέσεις αυτές λέγονται ***ξένοι κύκλοι***.

4. Η αντίστροφη μετάθεση ενός $k-$κύκλου $(x_1\, x_2 \cdots x_k)$ προφανώς είναι ο $k-$ κύκλος $(x_k, x_{k-1}, \cdots, x_1)$. Φυσικά αυτές οι μεταθέσεις δεν είναι ξένες μεταξύ τους αλλά μετατίθενται.

5. Είναι φανερό ότι ο $k-$κύκλος $(x_1\, x_2 \cdots x_k)$ είναι ο ίδιος με τον $k-$κύκλο $(x_i\, x_{i+1} \cdots x_k\, x_1 \cdots x_{i-1})$ για κάθε $i = 1, 2, \ldots, k$, αφού $\sigma(x_i) = x_{i+1}$ για κάθε $i = 1, \ldots, k-1$ και $\sigma(x_k) = x_1$. Για παράδειγμα, οι 3 - κύκλοι $(3\,5\,7)$, $(5\,7\,3)$ και $(7\,3\,5)$ είναι ίδιοι, αλλά είναι διάφοροι από τον 3 - κύκλο $(5\,3\,7)$ που είναι ίδιος με τους $(3\,7\,5)$ και $(7\,5\,3)$. Επομένως, στο εξής, για να θεωρείται μοναδική η παράσταση ενός $k-$κύκλου $(x_1\, x_2 \cdots x_k)$ θα θεωρούμε πάντα ότι το πρώτο στοιχείο x_1 είναι ο μικρότερος φυσικός αριθμός μεταξύ όλων των $x_i,\ i = 1, \ldots, k$.

4.2.13 Θεώρημα. *Έστω $\sigma \in S_n$ μία μετάθεση διάφορη της ταυτοτικής i. Τότε υπάρχουν μοναδικές κυκλικές μεταθέσεις $\sigma_1, \sigma_2, \ldots, \sigma_s$ ξένες ανά δύο και διάφορες της ταυτοτικής, τέτοιες ώστε*

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_s .$$

Μία τέτοια ανάλυση της σ σε γινόμενο ξένων ανά δύο κύκλων λέγεται ***κυκλική παράσταση*** της σ και οι σ_i ***κυκλικοί παράγοντες*** . Η σειρά με την οποία γράφονται οι κυκλικές μεταθέσεις σ_i δεν λαμβάνεται υπ΄ όψη αφού αυτές είναι ξένες ανά δύο μεταξύ τους και άρα μετατίθενται.

Απόδειξη. Έστω k το πλήθος των στοιχείων του X που δεν μένουν σταθερά από τη σ. Αφού $\sigma \neq i$, έχουμε ότι $k > 1$. Για την απόδειξη εφαρμόζουμε επαγωγή στο k. Αν $k = 2$, έστω x και y τα δύο στοιχεία του X που δεν μένουν σταθερά από τη σ. Τότε αναγκαστικά $\sigma(x) = y$ και $\sigma(y) = x$ ενώ $\sigma(z) = z$, για κάθε $z \in X$ με $z \neq x, y$. Άρα στην περίπτωση αυτή η σ είναι ο $2-$κύκλος $(x\, y)$. Υποθέτουμε ότι το θεώρημα ισχύει αν το πλήθος k των στοιχείων του X που δεν μένουν σταθερά μέσω της σ είναι μικρότερο ή ίσο του $m-1$. Θα δείξουμε ότι αυτό ισχύει και για $k = m$. Έστω x ένα στοιχείο του X που δεν μένει σταθερό μέσω της σ. Θεωρούμε την κυκλική μετάθεση $\tau = (x\, \sigma(x) \cdots \sigma^{\ell-1}(x))$, όπου ℓ είναι ο μικρότερος φυσικός αριθμός για τον οποίο ισχύει $\sigma^\ell(x) = x$. Αν $\ell = m$, τότε η σ είναι η κυκλική μετάθεση τ, αφού η σ έχει m ακριβώς στοιχεία που δεν μένουν σταθερά. Αν $\ell \neq m$, τότε η μετάθεση $\rho = \tau^{-1}\sigma$ αφήνει σταθερά όλα τα στοιχεία του X που μένουν σταθερά μέσω της σ, επιπλέον αυτή αφήνει σταθερά και όλα τα στοιχεία $x, \sigma(x), \ldots, \sigma^{\ell-1}(x)$. Συνεπώς η ρ πρέπει να γράφεται ως γινόμενο κυκλικών μεταθέσεων ανά δύο ξένων μεταξύ τους, έστω $\rho = \sigma_1 \sigma_2 \cdots \sigma_s$. Επειδή οι $\sigma_j, \quad j = 1, \ldots, s$ είναι ανά δύο ξένες μεταξύ τους, τα στοιχεία που δεν μένουν σταθερά από κάθε $\sigma_j, \quad j = 1, \ldots, s$, δεν μένουν σταθερά και από την ρ. Άρα όλες οι κυκλικές μεταθέσεις $\sigma_j,\ j = 1, \ldots, s$, είναι ξένες προς την τ, αφου αυτή είναι ξένη προς τη ρ. Επομένως από τη σχέση $\rho = \tau^{-1}\sigma$, έχουμε $\sigma = \tau\, \sigma_1 \sigma_2 \cdots \sigma_s$, δηλαδή η σ έχει γραφεί ως γινόμενο ανά δύο ξένων κυκλικών μεταθέσεων.

Υποθέτουμε τώρα ότι η σ γράφεται ως γινόμενο ξένων ανά δύο κυκλικών μεταθέσεων με δύο διαφορετικούς τρόπους, δηλαδή

$$\sigma = \sigma_1 \cdot \sigma_2 \cdot \cdots \cdot \sigma_m = \tau_1 \cdot \tau_2 \cdot \cdots \cdot \tau_s ,$$

όπου $\sigma_1, \sigma_2, \ldots, \sigma_m$ και $\tau_1, \tau_2, \ldots, \tau_s$ είναι κύκλοι μήκους ≥ 2. Δείχνουμε ότι $m = s$ και για μια κατάλληλη αρίθμηση $\sigma_j = \tau_j,\ j = 1, \ldots, m$. Έστω ένα $x \in X$ που δεν μένει σταθερό από τη σ, (η σ δεν είναι η ταυτοτική μετάθεση). Καθώς οι κύκλοι σ_i είναι ανά δύο ξένοι και οι τ_j ανά δύο ξένοι, υπάρχει ένας (μοναδικός) κύκλος από τους σ_i και ένας μοναδικός κύκλος από τους τ_j που

μεταθέτει το x, ενώ το x περαμένει σταθερό από όλους τους άλλους κύκλους. Αφου ξένοι κύκλοι μετατίθενται, χωρίς να βλάπτεται η γενικότητα, μπορούμε να υποθέσουμε ότι ο σ_m και ο τ_s μεταθέτουν το x. Επομένως έχουμε $\sigma_m(x) = \sigma(x) = \tau_s(x)$. Από τη σχέση αυτή έπεται ότι $\sigma\,(\,\sigma_m(x)) = \sigma^2(x) = \sigma_m^2(x)$, όμοια $\sigma\,(\,\tau_s(x)) = \sigma^2(x) = \tau_s^2(x)$ και επαγωγικά για κάθε ακέραιο k έχουμε $\sigma_m^k(x) = \tau_s^k(x)$. Άρα οι κύκλοι σ_m και τ_s είναι ίδιοι. Οπότε έχουμε

$$\sigma_1\,\sigma_2\,\cdots\,\sigma_{m-1} = \sigma\,\sigma_m^{-1} = \tau_1\,\tau_2\,\cdots\,\tau_{s-1}\,.$$

Από την υπόθεση της επαγωγής έχουμε $m-1 = s-1$ και άρα $m = s$ και για μια κατάλληλη αρίθμηση, $\sigma_j = \tau_j,\ \ j = 1, \ldots, m.$ ⊺

4.2.14 Παρατήρηση. Η απόδειξη του προηγουμένου θεωρήματος μας δίνει τη μέθοδο με την οποία μπορούμε να βρούμε την κυκλική παράσταση μιας δεδομένης σ. Για παράδειγμα, έστω

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 8 & 2 & 1 & 9 & 7 & 5 & 6 \end{pmatrix}.$$

Θεωρούμε ένα στοιχείο $x \in \{\,1, 2, \ldots, 9\,\}$ τέτοιο ώστε $\sigma(x) \neq x$, παραδείγματος χάρη $x = 1$, και παίρνουμε την κυκλική μετάθεση $(\,1\,\sigma(1)\,\sigma^2(1)\cdots) = (\,1\,3\,8\,5\,)$. Κατόπιν θεωρούμε ένα $x \in \{\,1, 2, \ldots, 9\,\}$ διάφορο από τα στοιχεία που εμφανίζονται στον κύκλο $(\,1\,3\,8\,5\,)$, έστω το 9 και παίρνουμε την κυκλική μετάθεση $(\,9\,\sigma(9)\,\sigma^2(9)\cdots) = (\,9\,6\,) = (\,6\,9\,)$. Όμοια για $x = 2$ παίρνουμε την $(\,2\,4\,)$ και για $x = 7$ παίρνουμε τον 1 - κύκλο τον οποίο μπορούμε να παραλείψουμε στην κυκλική παράσταση της σ, αφού αυτός παριστά την ταυτοτική μετάθεση. Έτσι έχουμε $\sigma = (\,1\,3\,8\,5\,)\cdot(\,6\,9\,)\cdot(\,2\,4\,)$. Η σειρά με την οποία γράφουμε τους κύκλους στην παράσταση της σ δεν λαμβάνεται υπ΄ όψη, αφού αυτοί είναι ανά δύο ξένοι μεταξύ τους και άρα μετατίθενται.

Τύπος Μετάθεσης

Μερικές φορές μας διευκολύνει να συμπεριλαμβάνουμε στην κυκλική παράσταση μιας μετάθεσης $\sigma \in S_n$ και τα στοιχεία του X που μένουν σταθερά μέσω της σ. Δηλαδή στην κυκλική παράσταση της σ θεωρούμε σαν παράγοντες και τους 1 - κύκλους, αν υπάρχουν, αφού ο καθένας απ΄ αυτούς παριστά την ταυτοτική μετάθεση. Αυτό είναι απαραίτητο όταν πρέπει να δηλώνεται ο βαθμός της σ. Για παράδειγμα στην κυκλική παράσταση $(\,1\,3\,5\,2\,)(\,4\,8\,)$ της
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 5 & 8 & 2 & 6 & 7 & 4 \end{pmatrix}$, αν τη θεωρήσουμε στοιχείο της S_8 (δηλαδή βαθμού 8), προσθέτουμε και τους 1 - κύκλους $(\,6\,)$ και $(\,7\,)$ γράφοντας $\sigma =$

$(6)(7)(48)(1352)$. Αν όμως τη θεωρούσαμε βαθμού 9 θα γράφαμε $\sigma = (6)(7)(9)(48)(1352)$.

Παριστάνοντας μ΄ αυτόν τον τρόπο μια μετάθεση σ του X παίρνουμε μια διαμέριση του X σε ξένα ανά δύο υποσύνολά του, όπου καθένα απ΄ αυτά περιέχει ακριβώς τα στοιχεία του X που δεν μένουν σταθερά από έναν (μοναδικό) κυκλικό παράγοντα της σ. Αντίστροφα, από μία διαμέριση του X παίρνουμε ένα, ή περισσότερα γινόμενα, ξένων ανά δύο κυκλικών μεταθέσεων. Για παράδειγμα, η προηγούμενη μετάθεση ορίζει τη διαμέριση $\{6\} \cup \{7\} \cup \{4, 8\} \cup \{1, 2, 3, 5\}$ του $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Αλλά αυτή η διαμέριση ορίζει έξι γινόμενα
$(6)(7)(48)(1235)$, $(6)(7)(48)(1253)$, $(6)(7)(48)(1325)$,
$(6)(7)(48)(1352)$, $(6)(7)(48)(1523)$ και $(6)(7)(48)(1532)$.

Τώρα μία διαμέριση ενός θετικού ακεραίου n είναι μία ακολουθία θετικών ακεραίων $\lambda_1, \lambda_2, \ldots \lambda_s$ με $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_s$ και $\lambda_1 + \lambda_2 + \cdots + \lambda_s = n$. Άρα μία διαμέριση του $X = X_1 \cup X_2 \cup \cdots \cup X_s, X_i \neq \emptyset,\ X_i \cap X_j = \emptyset,\ i \neq j$, ορίζει τη διαμέριση

$$(|X_1|,\ |X_2|,\ \ldots,\ |X_s|)$$

του n, όπου έχουμε θεωρήσει ότι $|X_i| \leq |X_{i+1}|$. Χρησιμοποιώντας τις διαμερίσεις του n, μπορούμε να ταξινομήσουμε όλες τις μεταθέσεις της S_n, θεωρώντας τις κυκλικές παραστάσεις τους (με την προσθήκη σ΄ αυτές των 1-κύκλων), ως εξής: Έστω $\sigma = \sigma_1 \sigma_2 \cdots \sigma_s$ η κυκλική παράσταση μιας μετάθεσης $\sigma \in S_n$. Αν λ_i είναι το μήκος κάθε $\sigma_i,\ i = 1, \ldots, s$, μπορούμε να υποθέσουμε ότι η σειρά των κυκλικών παραγόντων της σ είναι τέτοια ώστε $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_s$. Προφανώς έχουμε $\lambda_1 + \lambda_2 + \cdots + \lambda_s = n$, δηλαδή η ακολουθία $\lambda_1, \lambda_2, \ldots, \lambda_s$ είναι μια διαμέριση του n. Αυτή η διαμέριση ονομάζεται ***τύπος*** της σ. Για παράδειγμα, στη συμμετρική ομάδα S_5 οι μεταθέσεις που έχουν τύπο $(1, 2, 2)$ είναι οι εξής:
$(12)(34)$, $(12)(35)$, $(12)(45)$, $(13)(24)$,
$(13)(25)$, $(13)(45)$, $(14)(23)$, $(14)(25)$,
$(14)(35)$, $(15)(23)$, $(15)(24)$, $(15)(34)$,
$(23)(45)$, $(24)(35)$, $(25)(34)$.
Αυτές οι 15 μεταθέσεις εκτός του ότι έχουν τον ίδιο τύπο έχουν και ένα άλλο κοινό χαρακτηριστικό που θα δούμε αμέσως τώρα.

4.2.15 Θεώρημα. *Δύο μεταθέσεις $\sigma,\ \tau \in S_n$ έχουν τον ίδιο τύπο αν και μόνο αν υπάρχει μία μετάθεση $\rho \in S_n$ έτσι ώστε $\tau = \rho\,\sigma\,\rho^{-1}$.*

Απόδειξη. Κατ΄ αρχήν αποδεικνύουμε το θεώρημα στην περίπτωση που οι μεταθέσεις είναι κυκλικές. Έστω δύο κύκλοι

$$\sigma = (a_1\, a_2 \cdots a_k) \quad \text{και} \quad \tau = (b_1\, b_2 \cdots b_k)$$

του ιδίου μήκους k. Τότε, με απευθείας υπολογισμό, βλέπουμε ότι για κάθε μετάθεση $\rho \in S_n$ με $\rho(a_i) = b_i$ για κάθε $i = 1, \ldots, k$ ισχύει $\rho \circ \sigma \circ \rho^{-1} = \tau$.

Αντίστροφα, έστω $\sigma = (a_1\, a_2 \cdots a_k)$ ένας κύκλος μήκους k και ρ μια μετάθεση. Τότε, έχουμε $\rho\,\sigma\,\rho^{-1} = (\,\rho(a_1)\;\rho(a_2)\;\cdots\;\rho(a_k)\,)$. Πράγματι, για κάθε $i = 1, \ldots, k-1$ είναι $\rho\,\sigma\,\rho^{-1}\,(\,\rho(a_i)\,) = \rho\,\sigma\,(\,a_i\,) = \rho\,(\,a_{i+1}\,)$, ενώ $\rho\sigma\rho^{-1}(\rho(a_k)) = \rho(a_1)$. Επίσης, για κάθε $x \in \{1, \ldots, n\} \setminus \{a_1, \ldots, a_k\}$ έχουμε $\sigma(x) = x$ και άρα $\rho\,\sigma\,\rho^{-1}\,(\,\rho(x)\,) = \rho(x)$.

Έστω τώρα $\sigma = \sigma_1 \cdots \sigma_k$ η κυκλική παράσταση μιας μετάθεσης $\sigma \in S_n$. Τότε οι σ και $\rho\,\sigma\,\rho^{-1}$, για κάθε $\rho \in S_n$, είναι του ιδίου τύπου. Πράγματι, έχουμε $\rho\,\sigma\,\rho^{-1} = \rho\,\sigma_1\,\rho^{-1}\,\rho\,\sigma_2\,\rho^{-1} \cdots \rho\,\sigma_k\,\rho^{-1}$. Αλλά η σ_i και η $\rho\,\sigma_i\,\rho^{-1}$ είναι κυκλικές μεταθέσεις του ιδίου μήκους. Επίσης η $\rho\,\sigma_i\,\rho^{-1}$ είναι ξένη με την $\rho\,\sigma_j\,\rho^{-1}$, για κάθε $i \neq j$ (γιατί;). Οπότε προφανώς οι σ και $\rho\,\sigma\,\rho^{-1}$ είναι του ιδίου τύπου.

Αντίστροφα, έστω σ και τ δύο μεταθέσεις του ιδίου τύπου. Αν σ_i είναι ένας κυκλικός παράγοντας στην κυκλική παράσταση της σ μήκους k_i, τότε υπάρχει ένας κυκλικός παράγοντας τ_i στην κυκλική παράσταση της τ μήκους k_i και αντιστρόφως. Συνεπώς, υπάρχει μετάθεση $\rho \in S_n$, τέτοια ώστε $\rho\,\sigma_i\,\rho^{-1} = \tau_i$ για κάθε δείκτη i. Είναι φανερό ότι τότε ισχύει $\rho\,\sigma\,\rho^{-1} = \tau$. ⊺

Δύο μεταθέσεις σ και τ που έχουν τον ίδιο τύπο ή ισοδύναμα για τις οποίες υπάρχει μία μετάθεση ρ έτσι ώστε $\rho\,\sigma\,\rho^{-1} = \tau$ λέγονται ***συζυγείς*** ή ***όμοιες*** μεταθέσεις. Η σχέση $\rho\,\sigma\,\rho^{-1} = \tau$ ορίζει μία σχέση ισοδυναμίας στο σύνολο S_n όλων των μεταθέσεων (γιατί;) και άρα έχουμε μία 1 - 1 και επί αντιστοιχία μεταξύ των κλάσεων ισοδυναμίας και των διαμερίσεων του n. Κάθε κλάση ισοδυναμίας είναι ένα υποσύνολο της μορφής $\{\,\rho\,\sigma\,\rho^{-1} \mid \rho \in S_n\,\}$, το οποίο ονομάζεται κλάση ***συζυγίας***.

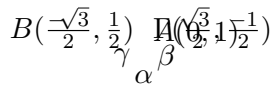
4.2.16 Παράδειγμα.

Οι μεταθέσεις της S_4 ταξινομούνται σε πέντε κλάσεις συζυγίας, οι οποίες αντιστοιχούν στις διαμερίσεις του 4: $(1, 1, 1, 1)$, $(1, 1, 2)$, $(1, 3)$, $(2, 2)$ και (4) αντίστοιχα.

Σημειώνουμε ότι το πλήθος των μεταθέσεων του ιδίου τύπου θα υπολογισθεί στην Παράγραφο 5.2. Προς το παρόν θα δώσουμε μία ερμηνεία της έννοιας της συζυγίας μεταθέσεων μέσω της ομάδας συμμετρίας ενός ισοπλεύρου τριγώνου.

Έστω $A\,B\,\Gamma$ ένα ισόπλευρο τρίγωνο και α, β και γ οι διάμεσοί του. Θεω-

ρούμε το τρίγωνο εγγεγραμμένο στον μοναδιαίο κύκλο όπως στο σχήμα 4.2.1.



Σχήμα 4.2.1

Η ομάδα συμμετρίας του τριγώνου, όπως είδαμε στο Παράδειγμα 4.1.3 (2) , αποτελείται αφενός από τις ανακλάσεις

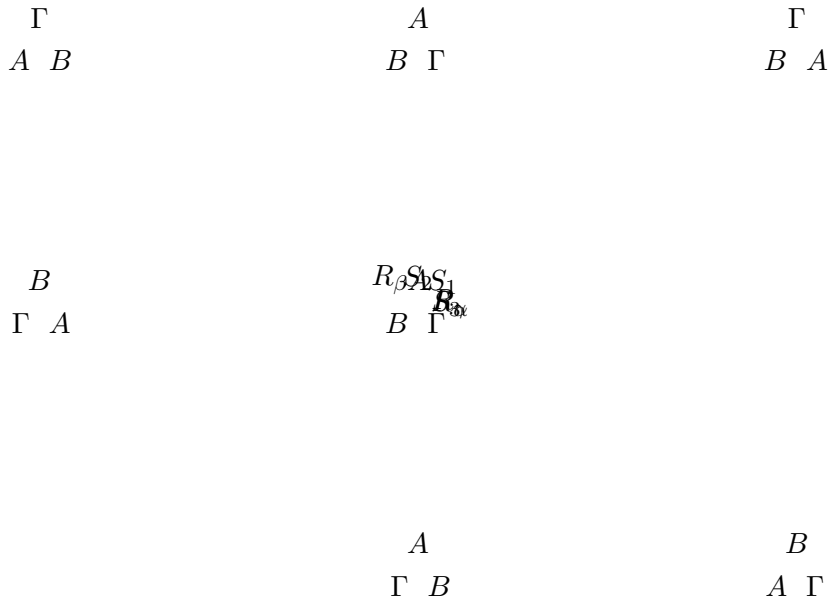
$R_\alpha = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, $R_\beta = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix}$ και $R_\gamma = \frac{1}{2}\begin{pmatrix} 1 & -\sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix}$

ως προς τους άξονες $\alpha,\ \beta$ και γ αντίστοιχα και αφετέρου από τις στροφές

$S_1 = \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix}$, $S_2 = \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix}$ και $S_3 = I_2$

γύρω απ΄ το κέντρο O του κύκλου κατά γωνία 120°, 240° και 360° αντίστοιχα,

όπως στο σχήμα 4.2.2.



Σχήμα 4.2.2

(Εδώ έχουμε θεωρήσει τις συμμετρίες υπό μορφή πινάκων ως προς τη βάση $e_1 = (1, 0), \quad e_2 = (0, 1)$ του $\mathbb{R}^2$).

Αν θεωρήσουμε το σύνολο $\{A, B, \Gamma\}$ των κορυφών του τριγώνου, η συμμετρική του ομάδα, που είναι η S_3, αποτελείται από τις μεταθέσεις $(A, B), (A, \Gamma), (B, \Gamma), (A, B, \Gamma), (A, \Gamma, B)$ και την ταυτοτική μετάθεση i. Οι κλάσεις συζυγίας είναι $\{i\}$, $\{(A, B), (A, \Gamma), (B, \Gamma)\}$ και $\{(A, B, \Gamma), (A, \Gamma, B)\}$ (βλ. Θεώρημα 4.2.15). Παρατηρούμε τώρα ότι οι μεταθέσεις των κορυφών του τριγώνου μας δίνουν τις έξι "θέσεις" του τριγώνου που μας δίνουν οι συμμετρίες του. Συγκεκριμένα έχουμε την αντιστοιχία
$R_\alpha \longleftrightarrow (B, \Gamma), \quad R_\beta \longleftrightarrow (A, \Gamma), \quad R_\gamma \longleftrightarrow (A, B),$
$S_1 \longleftrightarrow (A, B, \Gamma), \quad S_2 \longleftrightarrow (A, \Gamma, B)$ και $S_3 \longleftrightarrow i$

Αν θεωρήσουμε τον πολλαπλασιασμό των 2×2 πινάκων τότε βλέπουμε εύκολα ότι από την προηγούμενη αντιστοιχία μεταθέσεων - συμμετριών, η σχέση συζυγίας μεταξύ μεταθέσεων αντιστοιχεί στη γνωστή σχέση ομοιότητας μεταξύ πινάκων. Πράγματι, παραδείγματος χάρη έχουμε· $R_\beta\, R_\alpha\, R_\beta^{-1} = R_\gamma = R_\alpha\, R_\beta\, R_\alpha^{-1}$ και $R_\alpha\, S_1\, R_\alpha = S_2$.

Το ίδιο προκύπτει αν θεωρήσουμε το σχήμα 4.2.3 που σχηματίζεται από τις τρεις διαμέσους του τριγώνου

Σχήμα 4.2.3

Η ομάδα συμμετρίας αυτού του γεωμετρικού σχήματος είναι η ίδια μ΄ αυτή του ισοπλεύρου τριγώνου $A\,B\,\Gamma$ (γιατί;). Εδώ η συμμετρική ομάδα S_3 θεωρείται επί του συνόλου $\{\,\alpha,\,\beta,\,\gamma\,\}$.

Ασκήσεις 4.2

1. Δείξτε ότι το γινόμενο $(1\ 4\ 5\ 6)(2\ 1\ 5)$ είναι το ίδιο με το γινόμενο $(1\ 6)(2\ 4\ 5)(3)$.

2. Να βρεθούν μεταθέσεις x και y τέτοιες ώστε $x\alpha = \beta = \alpha y$, όπου

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 3 & 4 & 7 & 6 & 1 \end{pmatrix} \quad \text{και} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 7 & 6 & 3 & 5 \end{pmatrix}.$$

3. Οι επόμενες μεταθέσεις να γραφούν ως γινόμενα ξένων ανά δύο κύκλων

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix},$$
$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}.$$

4. Έστω $\sigma = (2\ 5\ 3)$, $\tau = (\ 2\ 4) \in S_5$. Να βρεθούν οι μεταθέσεις

   α) $\sigma\tau$, β) $\tau\sigma$, γ) $\sigma\tau\sigma^{-1}$, δ) $\tau\sigma\tau^{-1}$.

5. Θεωρούμε τις μεταθέσεις $\sigma = (\ 2\ 3)$, $\tau = (2\ 3\ 4\ 5\ 6)$ και $\rho = (1\ 4\ 6\ 3)$ της S_6. Υπολογίστε τις μεταθέσεις σ^{-1}, $\sigma\tau\rho$, $\sigma\tau\rho^2$, $\rho^{-1}\tau$ και $(\sigma\rho\tau)^{-1}$.

6. Έστω $\sigma \in S_n$. Δείξτε ότι αν $\sigma(i) \neq i$ τότε $\sigma^2(i) \neq \sigma(i)$.

7. Έστω $\sigma = (1\ 2\ 3)(2\ 3\ 4)(3\ 4\ 5)(5\ 6\ 7)(6\ 7\ 8)(7\ 8\ 9)$ στην S_9.

   α) Γράψτε την σ ως γινόμενο κύκλων ξένων ανά δύο.

   β) Ποια σύμβολα μένουν σταθερά από την σ;

   γ) Γράψτε την σ^{-1} σε γινόμενο κύκλων ξένων ανά δύο.

8. Έστω $n > 2$, $n \in \mathbb{N}$. Θεωρούμε το σύνολο $\mathbb{Z}_n$ των ακεραίων modulo n και έναν ακέραιο α, έτσι ώστε μ.κ.δ.$(\alpha,\, n) = 1$.

   α) Δείξτε ότι ο πολλαπλασιασμός επί $\alpha \mod n$ ορίζει μια μετάθεση P_α του $\mathbb{Z}_n$. Για $\alpha = 2$ και $n = 9$ γράψτε την αντίστοιχη μετάθεση ως γινόμενο ξένων ανά δύο κύκλων. Μπορείτε από αυτή την έκφραση να βρείτε το μικρότερο θετικό ακέραιο m τέτοιον ώστε $\alpha^m \equiv 1 \mod m$;

   β) Γράφοντας την P_α ως γινόμενο κύκλων ξένων ανά δύο, δείξτε ότι αυτοί οι κύκλοι κατατάσσονται σε δύο κατηγορίες. Η μια περιλαμβάνει κύκλους των οποίων τα σημεία είναι αντιστρέψιμα $\mod n$ και η άλλη κατηγορία περιλαμβάνει κύκλους των οποίων τα σημεία δεν είναι αντιστρέψιμα $\mod n$.

9. Δείξτε ότι τα στοιχεία $(1\ 3\ 4\ 5)$ και $(3\ 4\ 2\ 6)$ της S_7 είναι συζυγή. Να βρεθεί $\sigma \in S_7$ τέτοια ώστε $\sigma^{-1}(1\ 3\ 4\ 5)\sigma = (3\ 4\ 2\ 6)$.

10. Πόσα στοιχεία έχει η κλάση συζυγίας στην S_7 που περιέχει την μετάθεση $\pi = (1\,2)(3\,4\,5)$;

11. Με ποιες από τις μεταθέσεις $(1\ 2\ 3)(4\ 5\ 6)(7\ 8)$, $(6\ 7\ 8)(8\ 9)(1\ 2\ 3\ 4)$, $(1\ 2\ 3\ 4)(5\ 6)(7\ 8\ 9)$ της S_9 είναι συζυγής η μετάθεση $(1\ 4\ 5)(2\ 3)(6\ 7\ 8\ 9)$;

12. Όταν γράφουμε μια μετάθεση $\sigma \in S_n$ ως γινόμενο ξένων ανά δύο κύκλων ποια είναι η ικανή και αναγκαία συνθήκη έτσι ώστε $\sigma = \sigma^{-1}$;

13. α) Αν $\sigma \in S_n$ είναι ένας k - κύκλος δείξτε ότι $\sigma^k = i$.

    β) Αν $\tau \in S_n$ και $N =$ ε.κ.π.$(2,\, 3,\, 4,\, \ldots,\, n-1,\, n)$, δείξτε (γράφοντας την τ ως γινόμενο ξένων κύκλων) ότι $\tau^N = i$.

γ) Αν $N = \text{ε.κ.π.}(2, 3, 4, \ldots, n-1, n)$ και $M < N$, δείξτε ότι υπάρχει μια μετάθεση τ της S_n για την οποία ισχύει $\tau^M \neq i$.

14. Έστω m, n θετικοί ακέραιοι. Υποθέτουμε ότι ο m διαιρεί τον n. Αν σ είναι ένας n-κύκλος της S_n, τότε δείξτε ότι η σ^m είναι το γινόμενο m ξένων ανά δύο κύκλων μήκους $\dfrac{n}{m}$.

15. Έστω G ομάδα μεταθέσεων βαθμού n και $G_1 = \{\, \sigma \in G \mid \sigma(1) = 1 \,\}$. Δείξτε ότι η G_1 είναι επίσης μια ομάδα μεταθέσεων.

16. Δείξτε ότι τα μόνα στοιχεία της S_n που μετατίθενται με τη μετάθεση $\sigma = (\,1\,2\,\ldots\,n\,) \in S_n$ είναι οι δυνάμεις της σ.

17. Δείξτε ότι αν $n \geq 3$ τότε το σύνολο όλων των μεταθέσεων $\sigma \in S_n$, που έχουν την ιδιότητα $\sigma\,\sigma' = \sigma'\,\sigma$ για κάθε μετάθεση $\sigma' \in S_n$, αποτελείται μόνο από την ταυτοτική μετάθεση i.

4.3 Ορισμός και Βασικές Ιδιότητες Ομάδων

Η μελέτη των ομάδων συμμετρίας και ομάδων μεταθέσεων που προηγήθηκε βασίστηκε στο γεγονός ότι για κάθε δύο στοιχεία (απεικονίσεις) σ και τ αυτών υπάρχει ένας τρόπος συνδυασμού των (η σύνθεση απεικονίσεων) $\sigma\,\tau$. Αυτός ο τρόπος συνδυασμού ικανοποιεί τις τέσσερεις θεμελειώδεις ιδιότητες (Α), (Β), (Γ) και (Δ). Εκτός από τις ομάδες συμμετρίας και μεταθέσεων υπάρχουν και άλλα σημαντικά σύνολα που τα στοιχεία τους συνδυάζονται με τέτοιο τρόπο που να ικανοποιουνται αυτές οι τέσσερεις βασικές ιδιότητες. Μερικά από αυτά είναι τα εξής:

Το σύνολο $\mathbb{Z}$ των ακεραίων αριθμών. Εδώ ο τρόπος συνδυασμού $x\,y$ δύο ακεραίων x και y είναι η γνωστή πρόσθεση $x+y$. (Όταν μελετάμε το σύνολο $\mathbb{Z}$ ως προς την πρόσθεση, τότε το ονομάζουμε ***προσθετική ομάδα των ακεραίων***). Το ίδιο ισχύει, ως προς την πρόσθεση, για τα σύνολα $\mathbb{Q}$, $\mathbb{R}$, και $\mathbb{C}$ των ρητών, πραγματικών και μιγαδικών αριθμών αντίστοιχα. Επίσης στα προηγούμενα κεφάλαια η πρόσθεση που ορίσθηκε στο σύνολο $\mathbb{Z}_n$, των κλάσεων υπολοίπων $\bmod n$, ικανοποιεί τις τέσσερεις βασικές ιδιότητες (Α), (Β), (Γ) και (Δ).

Ένα άλλο σημαντικό παράδειγμα, που θα μας απασχολήσει και στα επόμενα, είναι το εξής. Αν θεωρήσουμε τους $n \times n$ αντιστρέψιμους πίνακες με στοιχεία από ένα σώμα K, τότε το σύνολο αυτό με πράξη τον πολλαπλασιασμό πινάκων ικανοποιεί τις ιδιότητες (Α), (Β), (Γ) και (Δ). Το σύνολο αυτό ονομάζεται ***Γενική Γραμμική Ομάδα*** βαθμού n επί του σώματος K και συμβολίζεται με $GL_n(K)$.

Με την εξέλιξη των Μαθηματικών, μετά τον 19^0 αιώνα, έγινε αντιληπτό ότι για όλα τα μαθηματικά συστήματα, που είναι όμοια με τα προηγούμενα, η μελέτη τους θα μπορούσε (κατ΄ αρχήν) να αντιμετωπιστεί ενιαία δίνοντας έμφαση μόνο στις τέσσερεις ιδιότητες (Α), (Β), (Γ) και (Δ) και αδιαφορώντας αφενός για το είδος των στοιχείων του συνόλου (δηλαδή αν αποτελείται από απεικονίσεις, αριθμούς, πίνακες κ.λ.π.) και αφετέρου για το είδος του τρόπου συνδυασμού των στοιχείων (δηλαδή αν είναι η σύνθεση απεικονίσεων ή η πρόσθεση αριθμών ή ο πολλαπλασιασμός πινάκων κ.λ.π.). Έτσι προέκυψε ο συγχρονος ορισμός της έννοιας της ομάδας που οφείλεται στον μαθηματικό Arthur Cayley. Ας σημειωθεί ότι ο πρώτος που καθιέρωσε τον όρο ομάδα ήταν ο E. Galois το 1827 όταν ανακάλυψε τις ομάδες μεταθέσεων μέσω των οποίων απέδειξε την μη επιλυσιμότητα με ριζικά των αλγεβρικών εξισώσεων βαθμού μεγαλυτέρου ή ίσου του 5. (βλέπε Παράγραφο 4.10). [2]

Στα προηγούμενα παραδείγματα παρατηρούμε ότι ο τρόπος που συνδυάζονται

[2] Μια πολύ σοβαρή έρευνα σχετικά με την προέλευση της έννοιας της ομάδας δίνεται στο βιβλίο του Hans Wussing [32] .

τα στοιχεία του εν λόγω συνόλου G καθορίζεται από μια απεικόνιση από το $G \times G$ στο G. Κάθε τέτοια απεικόνιση $f : G \times G \longrightarrow G$, όπως αναφέρουμε και στο Παράρτημα 6.2, ονομάζεται πράξη επί του G.

4.3.1 Ορισμός. *Ένα σύνολο G λέμε ότι έχει τη δομή μιας* ***ομάδας*** *ή απλά ότι είναι μια ομάδα ως προς μια πράξη $f : G \times G \longrightarrow G$, για την οποία γράφουμε $f(x, y) = x \circ y$, για κάθε $x, y \in G$, αν ικανοποιούνται οι εξής ιδιότητες.*

1. *Υπάρχει ένα στοιχείο $e \in G$ τέτοιο ώστε για κάθε $x \in G$ να ισχύει $x \circ e = e \circ x = x$.*
2. *Για κάθε $x \in G$, υπάρχει ένα $y \in G$ τέτοιο ώστε $x \circ y = y \circ x = e$, όπου e είναι ένα στοιχείο που ικανοποιεί την ιδιότητα 1.*
3. *Για κάθε $x, y, z \in G$ ισχύει $x \circ (y \circ z) = (x \circ y) \circ z$, δηλαδή ισχύει η προσεταιριστική ιδιότητα.*

Συνηθίζεται για την πράξη να χρησιμοποιούμε τον όρο "πολλαπλασιασμός" και για το αποτέλεσμα $x \circ y$, το οποίο θα συμβολίζουμε xy (παραλείποντας το σύμβολο $\circ$), τον όρο "γινόμενο". Μερικές φορές, όταν αναφερόμαστε σε συγκεκριμένες ομάδες, είναι δυνατόν για την πράξη να χρησιμοποιείται άλλος όρος και άλλος συμβολισμός. Έτσι για την προσθετική ομάδα των ακεραίων το όνομα της πράξης είναι "πρόσθεση" και ο συμβολισμός $x + y$. Επίσης, πολλές φορές, όταν δεν υπάρχει κίνδυνος σύγχυσης, αντί να λέμε ότι ένα σύνολο G είναι ομάδα ως προς μια πράξη, θα λέμε ότι το G είναι ομάδα.

Εδώ θα θέλαμε να επισημάνουμε ότι σε μία ομάδα γενικά ισχύει $x \circ y \neq y \circ x$. Για παράδειγμα, αν A, B είναι δύο αντιστρέψιμοι πίνακες τότε γενικά έχουμε $AB \neq BA$. Αν σε μία ομάδα G ισχύει $xy = yx$ για κάθε $x, y \in G$, τότε η ομάδα θα λέγεται ***μεταθετική*** *ή* ***Αβελιανή***.

Σε όλα τα προηγούμενα παραδείγματα ομάδων είδαμε ότι όχι μόνο υπάρχει ένα στοιχείο e που ικανοποιεί την πρώτη ιδιότητα του ορισμού 4.3.1 , αλλά ότι αυτό είναι και μοναδικό. Το ίδιο είδαμε ότι ισχύει και για τα στοιχεία που αναφέρονται στη δεύτερη ιδιότητα, δηλαδή αν x είναι ένα οποιοδήποτε στοιχείο μιας ομάδας, απ΄ αυτές των παραδειγμάτων, τότε υπάρχει μοναδικό y τέτοιο ώστε $xy = yx = e$. Συνεπώς εγείρεται το ερώτημα: Μπορούν οι δύο πρώτες ιδιότητες του προηγούμενου ορισμού να απλουστευθούν; δηλαδή να αντικατασταθούν από άλλες ασθενέστερες; Η απάντηση είναι θετική και δίνεται στο επόμενο θεώρημα.

4.3.2 Θεώρημα. *Έστω G ένα σύνολο του οποίου τα στοιχεία συνδυάζονται με μία πράξη $f : G \times G \longrightarrow G$, $f(x, y) = xy$, η οποία ικανοποιεί την*

προσεταιριστική ιδιότητα. Το σύνολο G είναι ομάδα αν και μόνο αν ικανοποιείται η εξής ιδιότητα.

4. Για κάθε δύο στοιχεία $x, y \in G$ υπάρχουν μοναδικά στοιχεία $z, w \in G$ τέτοια ώστε

$$4_\alpha \qquad x\,z = y \quad \textit{και} \quad 4_\beta \qquad w\,x = y.$$

Απόδειξη. Υποθέτουμε ότι ισχύει η 4. Τότε για $y = x$, λόγω της 4_α, υπάρχει ένα μοναδικό στοιχείο e_1 τέτοιο ώστε $x\,e_1 = x$. Για το στοιχείο αυτό ισχύει $z\,e_1 = z$, για κάθε $z \in G$. Πράγματι, αν $z \in G$, από την 4_β έχουμε ότι για το x και z υπάρχει μοναδικό $w \in G$ έτσι ώστε $w\,x = z$. Συνεπώς από την προσεταιριστικότητα έχουμε $z\,e_1 = (w\,x)\,e_1 = w\,(x\,e_1) = w\,x = z$. Με τον ίδιο τρόπο αποδεικνύεται η ύπαρξη και η μοναδικότητα ενός στοιχείου e_2 της G τέτοιου ώστε $e_2\,z = z$, για κάθε $z \in G$. Οπότε από τη σχέση $z\,e_1 = z$ για $z = e_2$ έχουμε $e_2\,e_1 = e_2$ και από τη σχέση $e_2\,z = z$ για $z = e_1$ έχουμε $e_2\,e_1 = e_1$. Άρα $e_1 = e_2$. Δηλαδή υπάρχει ένα μοναδικό $e \in G$ που ικανοποιεί την πρώτη ιδιότητα του ορισμού. Τώρα γι΄ αυτό το στοιχείο e, για κάθε $x \in G$, λόγω της 4, υπάρχουν μοναδικά στοιχεία z και w τέτοια ώστε $x\,z = e$ και $w\,x = e$. Οπότε έχουμε ότι $z = w$, αφού $w\,(x\,z) = w\,e = w$ και $(w\,x)\,z = e\,z = z$. Συνεπώς, για κάθε $x \in G$, υπάρχει μοναδικό $z \in G$ που ικανοποιεί τη δεύτερη ιδιότητα του ορισμού, δηλαδή $x\,z = z\,x = e$. Άρα το σύνολο G είναι ομάδα.

Αντίστροφα, υποθέτουμε ότι ισχύουν οι ιδιότητες 1 και 2 του ορισμού. Έστω ένα στοιχείο $e \in G$ για το οποίο ισχύει $e\,x = x\,e = x$, για κάθε $x \in G$. Έστω $x \in G$. Τότε λόγω της 2, υπάρχει $z' \in G$ τέτοιο ώστε $x\,z' = e = z'\,x$, οπότε, για κάθε $y \in G$, έχουμε $x\,(z'\,y) = (x\,z')\,y = e\,y = y$. Επομένως για $x, y \in G$ υπάρχει ένα z, το $z = z'\,y$, έτσι ώστε $x\,z = y$. Μάλιστα αυτό είναι μοναδικό, αφού αν υπήρχε και ένα άλλο $s \in G$ τέτοιο ώστε $x\,z = x\,s$, τότε θα είχαμε $z = e\,z = (z'\,x)\,z = z'\,(x\,z) = z'\,(x\,s) = (z'\,x)\,s = e\,s = s$. Άρα ισχύει η ιδιότητα 4_α. Η ιδιότητα 4_β αποδεικύεται με τον ίδιο τρόπο. ⊺

Το μοναδικό στοιχείο $e \in G$ με την ιδιότητα $e\,x = x\,e = x$, για κάθε $x \in G$ ονομάζεται ***ουδέτερο*** ή ***ταυτοτικό*** ή ***μοναδιαίο*** στοιχείο της ομάδας και στο εξής γενικά θα το συμβολίζουμε με 1 εκτός εαν, σε ειδικές περιπτώσεις, επιλέξουμε διαφορετικό συμβολισμό. Επίσης αν $x \in G$, το μοναδικό $y \in G$ για το οποίο ισχύει $x\,y = y\,x = e$ ονομάζεται ***αντίστροφο*** του x και συμβολίζεται με x^{-1}. Συνεπώς το αντίστροφο του x^{-1} είναι το x, δηλαδή $(x^{-1})^{-1} = x$. Επίσης παρατηρούμε ότι το αντίστροφο στοιχείο του γινομένου $x\,y$ δύο στοιχείων της G είναι το $y^{-1}\,x^{-1}$, διότι $(x\,y)\,(y^{-1}\,x^{-1}) = x\,(y\,(y^{-1}\,x^{-1})) = x\,(y\,y^{-1}\,x^{-1}) = x(e\,x^{-1}) = x\,x^{-1} = e$. Δηλαδή $(x\,y)^{-1} = y^{-1}\,x^{-1}$.

Οι ιδιότητες 1 και 2 του ορισμού της ομάδας μπορούν να απλουστευθούν ακόμη περισσότερο.

4.3.3 Θεώρημα. *Έστω G ένα σύνολο του οποίου τα στοιχεία συνδυάζονται μέσω μιας πράξης $f : G \times G \longrightarrow G, \quad f((x, y)) = xy$, η οποία ικανοποιεί την προσεταιριστική ιδιότητα. Το σύνολο είναι ομάδα αν και μόνο αν ισχύουν οι ιδιότητες.*

1′) Υπάρχει ένα στοιχείο $e \in G$ τέτοιο ώστε $ex = x$, για κάθε $x \in G$.

2′) Για κάθε $x \in G$ υπάρχει ένα $y \in G$ τέτοιο ώστε $yx = e$, όπου e είναι ένα στοιχείο που ικανοποιεί την 1′).

Απόδειξη Η απόδειξη είναι τεχνική, παρόμοια με την προηγούμενη, και αφήνεται ως άσκηση. ⊤

4.3.4 Παρατήρηση. Το προηγούμενο Θεώρημα μας λέει ότι αν θέλουμε να ελέγξουμε αν ένα σύνολο G, του οποίου τα στοιχεία συνδυάζονται με μία προσεταιριστική πράξη, είναι όμάδα, αρκεί να δείξουμε την ύπαρξη αφενός ενός "αριστερού" ουδετέρου στοιχείου $e \in G$ (δηλαδή $ex = x$ για κάθε $x \in G$) και αφετέρου την ύπαρξη ενός "αριστερού" αντιστρόφου x^{-1} για κάθε $x \in G$ (δηλαδή $x^{-1}x = e$). Με άλλα λόγια στον Ορισμό 4.3.1 υπάρχουν περισσότερες πληροφορίες για τον τρόπο με τον οποίο συνδυάζονται τα στοιχεία της G απ΄ ότι χρειάζεται. Εντελώς ανάλογα συνηθίζουμε να λέμε ότι το τετράγωνο είναι ένας ρόμβος που έχει και τις τέσσερεις γωνίες του ορθές, ενώ θα αρκούσε να απαιτήσουμε να έχει μόνο μία ορθή γωνία.

Το πλήθος των στοιχείων μιας ομάδας G το συμβολίζουμε με $|G|$ και το ονομάζουμε ***τάξη*** της G. Όταν η τάξη της G είναι πεπερασμένη λέμε ότι η G είναι ***πεπερασμένη*** ομάδα. Σε διαφορετική περίπτωση λέμε ότι η G είναι ***άπειρη***. Για παράδειγμα, οι ομάδες $\mathbb{Z}_n$ και S_n είναι πεπερασμένες με τάξεις n και $n!$ αντίστοιχα. Το ίδιο είναι και η διεδρική ομάδα D_n με τάξη $2n$, ενώ οι προσθετικές ομάδες των ακεραίων, των ρητών, των πραγματικών και των μιγαδικών είναι άπειρες ομάδες.

Στα επόμενα παραδείγματα παραθέτουμε διάφορες συγκεκριμένες ομάδες. Επιλέξαμε αυτές τις ομάδες πρώτον διότι η κάθε μία από αυτές παρουσιάζει ενδιαφέρουσες ξεχωριστές ιδιότητες και δεύτερον διότι αυτές συγκαταλέγονται μεταξύ των ομάδων οι οποίες εμφανίζονται σε διάφορα προβλήματα των Μαθηματικών, της Φυσικής, της Χημείας και άλλων επιστημών.

4.3.5 Παραδείγματα.

1. Το σύνολο των φυσικών αριθμών $\mathbb{N}$ με πράξη την συνήθη πρόσθεση αριθμών δεν αποτελεί ομάδα αφού δεν υπάρχουν αντιστρέψιμα στοιχεία, για κάθε φυσικό αριθμό . Το ίδιο ισχύει για το σύνολο των ακεραίων αριθμών $\mathbb{Z}$ με πράξη τον πολλαπλασιασμό. Τα σύνολα $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ και $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ αποτελούν άπειρες ομάδες με πράξη τον

πολλαπλασιασμό. Αλλά και τα σύνολα $\mathbb{Q}^{\times}_{>0}$ και $\mathbb{R}^{\times}_{>0}$ των θετικών ρητών και πραγματικών αντίστοιχα αποτελούν άπειρες ομάδες με πράξη τον πολλαπλασιασμό. Αν R είναι ένας δακτύλιος, τότε ο R ως προς την πρόσθεση είναι Αβελιανή ομάδα. Αν ο R είναι δακτύλιος με μονάδα, τότε το σύνολο $U(R)$ των αντιστρεψίμων στοιχείων (ως προς τον πολλαπλασιασμό του δακτυλίου) αποτελεί ομάδα με πράξη τον πολλαπλασιασμό του δακτυλίου και ονομάζεται ***πολλαπλασιαστική ομάδα*** του δακτυλίου. Παραδείγματος χάρη, αν έχουμε τον δακτύλιο $\mathbb{Z}$ των ακεραίων, τότε $U(\mathbb{Z}) = \{\,1, -1\,\}$, ενώ αν ο R είναι ένα σώμα, τότε $U(R) = R \setminus \{\,0\,\} = R^{\times}$. Αν R είναι ένας δακτύλιος με μονάδα, τότε μπορούμε να θεωρήσουμε τον δακτύλιο $M_n(R)$ των $n \times n$ πινάκων με στοιχεία από τον R. Η ομάδα $U(\,M_n(R))$ είναι η γενική γραμμική ομάδα $GL_n(R)$. Αν επιπλέον ο R είναι μεταθετικός, ένας πίνακας A ανήκει στην $GL_n(R)$ αν και μόνο αν η ορίζουσα $\mid A \mid$ του A ανήκει στην ομάδα $U(R)$. (Αυτό προκύπτει από τη γνωστή σχέση $A\,(adj\,A) = (adj\,A)\,A = \mid A \mid I_n$, όπου $adj\,A$ είναι ο προσαρτημένος πίνακας του A). Για παράδειγμα, για το δακτύλιο των ακεραίων έχουμε $GL_n(\mathbb{Z}) = \{\,A \in M_n(\mathbb{Z})\,\mu\epsilon \mid A \mid = \pm 1\,\}$ και για τον δακτύλιο $\mathbb{Z}_m$ των ακεραίων $\bmod m$ έχουμε $GL_n(\mathbb{Z}_m) = \{\,A \in M_n(\mathbb{Z}_m) \mid A \mid \in U(\mathbb{Z}_m)\,\}$. Προφανώς η τάξη της $GL_n(\mathbb{Z})$ είναι άπειρη (γιατί;), ενώ η τάξη της $GL_n(\mathbb{Z}_m)$ είναι πεπερασμένη (γιατί;).
Τέλος ας σημειωθεί ότι, αν R είναι ενας δακτύλιος με μονάδα, τότε εκτός από την πολλαπλασιαστική ομάδα $U(R)$, είναι δυνατόν να υπάρχουν και άλλα υποσύνολα του συνόλου $R \setminus \{\,0\,\}$ που να αποτελούν ομάδες ως προς τον πολλαπλασιασμό του R. Για παράδειγμα, αν $R = \mathbb{Z}_m$ και H είναι ένα τέτοιο υποσύνολο, τότε $H \cap U(\,\mathbb{Z}_m\,) = \emptyset$ ή $H \subseteq U(\,\mathbb{Z}_m\,)$. Πράγματι, αν $a \in H \cap U(\,\mathbb{Z}_m\,)$, τότε για κάποιο θετικό ακέραιο n έχουμε $a^n = 1$ στην $U(\,\mathbb{Z}_m\,)$, καθώς $a^n \in H$, το μοναδιαίο στοιχείο 1 της $U(\,\mathbb{Z}_m\,)$ ανήκει στην H. Τώρα, επειδή η H είναι ομάδα, η εξίσωση $b\,x = 1$ έχει λύση, για κάθε $b \in H$. Αλλά τότε $b \in U(\,\mathbb{Z}_m\,)$, αφού το b είναι αντιστρέψιμο και συνεπώς $H \subseteq U(\,\mathbb{Z}_m\,)$. Για παράδειγμα, έστω $m = 26$. Τότε το υποσύνολο $H = \{\,2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24\,\}$ είναι μια τέτοια ομάδα με ουδέτερο στοιχείο το 14. Αν $m = 24$, τότε το $H = \{\,3, 9, 15, 21\,\}$ είναι μια πολλαπλασιαστική ομάδα με ουδέτερο στοιχείο το 9.

2. Το σύνολο όλων των 2×2 πινάκων της μορφής $\begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix}, \quad \alpha,\ \beta \in \mathbb{R}$ με πράξη τον πολλαπλασιασμό πινάκων δεν είναι ομάδα. Διότι για έναν πίνακα $\begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix}$ υπάρχουν περισσότερα από ένα αριστερά ουδέτερα, αφού

για κάθε $x \in \mathbb{R}$, έχουμε $\begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix}$. Επιπλέον παρατηρούμε ότι
$\begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \alpha & \alpha\, x \\ 0 & 0 \end{pmatrix}$. (Υπάρχουν δεξιά ουδέτερα;)

3. Έστω $\prod$ το σύνολο των σημείων ενός επιπέδου και O ένα σταθερό σημείο του. Για κάθε δύο σημεία A, $B \in \prod$ θεωρούμε το σημείο $A * B = \Gamma$, έτσι ώστε το $O\,A\,\Gamma\,B$ να είναι ένα παραλληλόγραμμο (δηλαδή να ισχύει $\overrightarrow{O\Gamma} = \overrightarrow{OA} + \overrightarrow{OB}$. Το σύνολο $\prod$ με πράξη την $*$ είναι ομάδα. Το $\prod$ με την πράξη $*$ ουσιαστικά είναι ο διανυσματικός χώρος $\mathbb{R}^2$ και η πράξη $*$ είναι η πρόσθεση διανυσμάτων. (Γενικά κάθε διανυσματικός χώρος V επί ενός σώματος με πράξη την πρόσθεση είναι μία Αβελιανή ομάδα). Αν αντί της πράξης $*$ θεωρήσουμε την πράξη $\bigodot$, όπου το σημείο $A \bigodot B = \Gamma$ ορίζεται να είναι το σημείο του $\prod$ έτσι ώστε το $O\,A\,B\,\Gamma$ να είναι παραλληλόγραμμο, τότε το $\prod$ δεν είναι ομάδα, αφου εύκολα διαπιστώνουμε ότι η πράξη $\bigodot$ δεν είναι προσεταιριστική. Επίσης εδώ παρατηρούμε ότι υπάρχει μοναδικό αριστερό ουδέτερο στοιχείο (το σημείο O), αλλά δεν υπάρχει δεξιό ουδέτερο στοιχείο.

4. Έστω $\mathcal{P}(X)$ το σύνολο όλων των υποσυνόλων ενός συνόλου X (δηλαδή το δυναμοσύνολο του X). Για κάθε A, $B \in \mathcal{P}(X)$ θεωρούμε την πράξη $A\triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$ (τη λεγόμενη ***συμμετρική διαφορά*** του A και B). Εύκολα μπορούμε να διαπιστώσουμε, από τα διαγράμματα του Venn, ότι ισχύει η προσεταιριστική ιδιότητα $A\triangle(B\triangle\Gamma) = (A\triangle B)\triangle\Gamma$.

Το κενό σύνολο $\emptyset$ είναι το ταυτοτικό στοιχείο ως προς αυτή την πράξη. Το αντίστροφο ενός υποσυνόλου A του X είναι το ίδιο το A, αφού $A\triangle A = \emptyset$.

Συνεπώς το $\mathcal{P}(X)$ είναι ομάδα ως προς αυτή την πράξη.
Ας θεωρήσουμε τώρα αντί του συνόλου $\mathcal{P}(X)$ το σύνολο $\mathcal{X}(X)$ των χαρακτηριστικών συναρτήσεων των υποσυνόλων του X. Η ***χαρακτηριστική*** συνάρτηση ενός υποσυνόλου A του X ορίζεται να είναι η συνάρτηση $\mathcal{X}_A : X \longrightarrow \mathbb{Z}_2$ με $\mathcal{X}_A(x) = 0 \bmod 2$ αν $x \notin A$ και $\mathcal{X}_A(x) = 1 \bmod 2$ αν $x \in A$. Παρατηρούμε ότι αν $A, B \in \mathcal{P}(X)$, τότε $\mathcal{X}_A(x) + \mathcal{X}_B(x) = 1 \bmod 2$ αν $x \in A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$. Επίσης $\mathcal{X}_A(x) + \mathcal{X}_B(x) = 0 \bmod 2$ αν $x \notin A$ και $x \notin B$ ή $x \in A$ και $x \in B$. Συνεπώς $\mathcal{X}_A(x) + \mathcal{X}_B(x) = 0$ αν $x \notin A \triangle B$. Δηλαδή έχουμε $\mathcal{X}_{A \triangle B}(x) = \mathcal{X}_A(x) + \mathcal{X}_B(x)$. Αυτό δείχνει ότι αν στο σύνολο των χαρακτηριστικών συναρτήσεων ορίσουμε μία πρόσθεση $\mathcal{X}_A \oplus \mathcal{X}_B = \mathcal{X}_{A \triangle B}$, τότε το σύνολο αυτό είναι μία ομάδα. Εύκολα βλέπουμε ότι το ουδέτερο στοιχείο είναι η χαρακτηριστική συνάρτηση του κενού συνόλου $\mathcal{X}_\emptyset$, ενώ το αντίστροφό της $\mathcal{X}_A$ είναι η ίδια η $\mathcal{X}_A$, αφού $\mathcal{X}_A + \mathcal{X}_A = \mathcal{X}_\emptyset$.
Αν το σύνολο X είναι πεπερασμένο, τότε η τάξη της ομάδας $\mathcal{X}(X)$ είναι $2^{|X|} = |\mathcal{P}(X)|$ (γιατί;).

5. Έχουμε ήδη δει ότι μια ομάδα μεταθέσεων G βαθμού n, ως προς τη σύνθεση απεικονίσεων είναι ομάδα (Παρατήρηση 4.2.5). Έτσι βλέπουμε ότι για να είναι ένα μη κενό υποσύνολο G της S_n ομάδα ως προς τη σύνθεση μεταθέσεων, αρκεί το γινόμενο $\sigma_1 \sigma_2 \in G$, για κάθε $\sigma_1,\ \sigma_2 \in G$. Αν όμως θεωρήσουμε τη γενική γραμμική ομάδα $GL_n(K)$ επί ενός σώματος K, ένα υποσύνολό της H το οποίο είναι ***κλειστό*** ως προς τον πολλαπλασιασμό, δηλαδή ισχύει $A\,B \in H$ για κάθε $A,\ B \in H$ δεν είναι κατ' ανάγκη ομάδα ως προς τον πολλαπλασιασμό πινάκων. Παραδειγματος χάρη το υποσύνολο της $GL_n(\mathbb{Q})$ που αποτελείται από όλους τους πίνακες με στοιχεία ακεραίους αριθμούς δεν είναι ομάδα. Αν όμως πάρουμε το υποσύνολο που αποτελείται από τους πίνακες με στοιχεία ακεραίους αριθμούς και ορίζουσα ίση με ± 1, τότε, όπως είδαμε στο Παράδειγμα 1, αυτό είναι η ομάδα $GL_n(\mathbb{Z})$.
Γενικά, αν ένα υποσύνολο H της $GL_n(K)$ είναι ομάδα, ως προς τον πολλαπλασιασμό πινάκων, θα το ονομάζουμε ***γραμμική ομάδα*** επί του σώματος K. Ένα σημαντικό παράδειγμα μιας τέτοιας ομάδας είναι η λεγόμενη ***ειδική γραμμική ομάδα*** βαθμού n επί του σώματος K, την οποία συμβολίζουμε με $SL_n(K)$, που αποτελείται απ' όλους τους $n \times n$ πίνακες με στοιχεία από το K που έχουν ορίζουσα ίση με 1.
Ένα άλλο παράδειγμα γραμμικής ομάδας είναι η λεγόμενη ***ορθογώνια*** ομάδα, που συμβολίζεται με $O_n(K)$ και αποτελείται απ' όλους τους $n \times n$ πίνακες A με στοιχεία από το K που ικανοποιούν τη σχέση $A^{-1} = A^T$. (Σημειώνουμε ότι την ομάδα $O_2(\mathbb{R})$ την έχουμε ήδη συναντήσει στην 1^η

παράγραφο).

6. Έστω H το σύνολο των πινάκων της μορφής $\mathbf{h} = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$, $a, b \in \mathbb{C}$. Αν θεωρήσουμε ως πράξη την πρόσθεση πινάκων, τότε το H είναι μια Αβελιανή ομάδα. Παρατηρούμε ότι, επειδή η ορίζουσα του παραπάνω πίνακα είναι ίση με $\mid a \mid^2 + \mid b \mid^2$, ο μόνος μη αντιστρέψιμος πίνακας αυτής της μορφής είναι ο μηδενικός πίνακας. Επίσης αν $\mathbf{h}_1 = \begin{pmatrix} a_1 & b_1 \\ -\bar{b_1} & \bar{a_1} \end{pmatrix}$ και $\mathbf{h}_2 = \begin{pmatrix} a_2 & b_2 \\ -\bar{b_2} & \bar{a_2} \end{pmatrix}$, τότε $\mathbf{h}_1 \mathbf{h}_2 = \begin{pmatrix} a_1a_2 - b_1\bar{b_2} & a_1b_2 + b_1\bar{a_2} \\ -\overline{a_1b_2 + b_1\bar{a_2}} & \overline{a_1a_2 - b_1\bar{b_2}} \end{pmatrix} \in H$. Επιπλέον, αν $\mathbf{h} \neq 0$, τότε $\mathbf{h}^{-1} = \frac{1}{|\mathbf{h}|}\begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix} \in H$. Συνεπώς το σύνολο $H \setminus \{0\}$ με πράξη των πολλαπλασιασμό πινάκων είναι ομάδα που δεν είναι Αβελιανή. Δηλαδή το H έχει όλες τις ιδιότητες ενός σώματος εκτός την ιδιότητα της αντιμεταθετικότητας ως προς τον πολλαπλασιασμό, είναι όπως λέμε ένας ***δακτύλιος με διαίρεση*** ή ένα ***μη μεταθετικό*** σώμα.

   Ο δακτύλιος H μπορεί να θεωρηθεί ως ένας διανυσματικός χώρος επί του σώματος των πραγματικών αριθμών. Αν $a = a_1 + a_2 i$ και $b = b_1 + b_2 i$, τότε

   $\mathbf{h} = a_1\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + a_2\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + b_1\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + b_2\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ και άρα το σύνολο $\{I, A, B, \Gamma\}$, όπου

   $$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ \Gamma = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

   είναι μια βάση του H ως προς το σώμα των πραγματικών αριθμών. Επιπλέον, το σύνολο $Q_8 = \{\pm I, \pm A, \pm B, \pm\Gamma\}$ ως προς τον πολλαπλασιασμό πινάκων είναι ομάδα, η λεγόμενη ***ομάδα των quaternions***. Παρατηρούμε ότι: $A^2 = B^2 = \Gamma^2 = -I$, $AB = \Gamma$, $B\Gamma = A$, $\Gamma A = B$ και $BA = -\Gamma$, $\Gamma B = -A$, $A\Gamma = -B$.

7. Θεωρούμε το σύνολο των 2×2 πινάκων της μορφής $L(v) = \frac{1}{\sqrt{1-\frac{u^2}{c^2}}}\begin{pmatrix} 1 & -v \\ -\frac{v}{c^2} & 1 \end{pmatrix}$, $\mid v \mid < c$, $v \in \mathbb{R}$, όπου c είναι μία θετική σταθερά. Παρατηρούμε ότι $L(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ και $L(v)^{-1} = \frac{1}{\sqrt{1-\frac{u^2}{c^2}}}\begin{pmatrix} 1 & v \\ \frac{v}{c^2} & 1 \end{pmatrix}$. Επιπλέον ισχύει $L(u)\,L(v) = L(w)$ όπου $w = \frac{u+v}{1+\frac{uv}{c^2}}$.

Συνεπώς το σύνολο αυτό με πράξη τον πολλαπλασιασμό των πινάκων είναι μια άπειρη Αβελιανή ομάδα. Η ομάδα αυτή λέγεται ***ομάδα του Lorenz*** και παιζει σημαντικό ρόλο στην Ειδική Θεωρία της Σχετικότητας. Ο τύπος $w = \frac{u+v}{1+\frac{uv}{c^2}}$ είναι ***"ο νόμος πρόσθεσης των ταχύτήτων"*** του Einstein και η φυσική σημασία του είναι η εξής: Θεωρούμε τον άξονα των x με αρχή O σαν σταθερό σύστημα αναφοράς κι έναν άλλο άξονα x' με αρχή O' να ολισθαίνει επί του πρώτου με σταθερά ταχύτητα u. Ένα κινητό M έχει ταχύτητα v ως προς το κινούμενο σύστημα αναφοράς $(O'X')$. Στην Ειδική Θεωρία της Σχετικότητας η ταχύτητα του κινητού ως προς το ακίνητο σύστημα (OX) είναι η $w = \frac{u+v}{1+\frac{uv}{c^2}}$. Η ομάδα του Lorenz είναι η "ομάδα συμμετριών" του κόσμου της Ειδικής Θεωρίας της Σχετικότητας, δηλαδή η ομάδα των μετασχηματισμών που διατηρούν τους νόμους της όταν μεταβαίνουμε από ένα σύστημα συντεταγμένων σε ένα άλλο. (Βλέπε σχετικά το βιβλίο *Classical Mechanics* του H. Goldstein [10]).

8. Θεωρούμε το σύνολο $\mathcal{E}_\nu$ των $\nu-$οστών ριζών της μονάδας, δηλαδή τις μιγαδικές ρίζες του πολυωνύμου $x^\nu - 1$. Είναι γνωστό ότι αυτές είναι της μορφής $e^{\frac{2\pi k}{\nu}i}$, $k = 0, \ldots, \nu-1$. Είναι εύκολο να δούμε ότι το σύνολο $\mathcal{E}_\nu$ είναι μια ομάδα τάξης ν ως προς τον πολλαπλασιασμό μιγαδικών αριθμών, αφού $e^{\frac{2\pi k_1}{\nu}i} \cdot e^{\frac{2\pi k_2}{\nu}i} = e^{\frac{2\pi k_3}{\nu}i}$, όπου $k_3 \equiv (k_1 + k_2) \pmod{\nu}$, καθώς επίσης $e^0 = 1 \in \mathcal{E}_\nu$ και $e^{-\frac{2\pi k}{\nu}i} \in \mathcal{E}_\nu$. Παρατηρούμε ότι αν ο k είναι πρώτος προς τον ν, τότε κάθε στοιχείο της $\mathcal{E}_\nu$ είναι της μορφής $(e^{\frac{2\pi k}{\nu}i})^s$, για κάποιο $s = 0, \ldots, \nu-1$ (γιατί ;). Ένα τέτοιο στοιχείο της $\mathcal{E}_\nu$ λέγεται ***πρωταρχική*** $\nu-$οστη ρίζα της μονάδας. Συνεπώς υπάρχουν $\phi(\nu)$ πρωταρχικές ρίζες της μονάδας (όπου φ είναι η συνάρτηση του Euler). Αυτά τα υποσύνολα $\mathcal{E}_\nu$, $\nu \in \mathbb{N}$ εξαντλούν όλα τα πεπερασμένα υποσύνολα της πολλαπλασιαστικής ομάδας $\mathbb{C}^\times$ που είναι πολλαπλασιαστικά κλειστά. Πράγματι, αν S είναι ένα τέτοιο σύνολο και z ένα στοιχείο του, τότε εύκολα βλέπουμε ότι υπάρχει $k \in \mathbb{Z}$ με $z^k = 1$. Δηλαδή το S αποτελείται από ν διακεκριμένες ρίζες της μονάδας. Έστω $e^{\frac{2\pi k_1}{m_1}i}$, $e^{\frac{2\pi k_2}{m_2}i}$, $\ldots$, $e^{\frac{2\pi k_\nu}{m_\nu}i}$ τα στοιχεία του S. Λαμβάνοντας το $m = \text{ε.κ.π.}(m_1, \ldots, m_\nu)$ τα στοιχεία του S έχουν τη μορφή $z_1 = e^{\frac{2\pi n_1}{m}i}$, $z_2 = e^{\frac{2\pi n_2}{m}i}$, $\ldots$, $z_\nu = e^{\frac{2\pi n_\nu}{m}i}$. Επειδή το γινόμενο δύο στοιχείων του S είναι και αυτό στοιχείο του S, εύκολα βλέπουμε ότι το μικρότερο από τα n_i, έστω το n_1, διαιρεί τα υπόλοιπα n_i. Άρα έχουμε ότι τα ν στοιχεία του S είναι τα $z_1, z_1^2, \ldots, z_1^\nu = 1$, δηλαδή είναι οι ρίζες του $x^\nu - 1$. Γεωμετρικά μπορούμε να παραστήσουμε τις $\nu-$ οστές ρίζες της μονάδας με τα σημεία z_i, $i = 1, \ldots, \nu$ πάνω σε ένα κύκλο ακτίνας 1 έτσι ώστε δύο διαδοχικά σημεία να βρίσκονται σε απόσταση κατά γωνία

$\theta = \frac{2\pi k}{\nu}$ (βλέπε το επόμενο σχήμα), όπως προκύπτει από την γεωμετρική παράσταση των μιγαδικών αριθμών.

Επίσης, η ένωση $\bigcup_{\nu=1}^{\infty} \mathcal{E}_\nu$, καθώς και το σύνολο $\{\, z \in \mathbb{C} \mid \mid z \mid = 1 \,\}$ είναι ομάδες.

9. Έστω p ένας πρώτος αριθμός. Τα σύνολα $\mathbb{Q}_p = \{\, \frac{\alpha}{\beta} \in \mathbb{Q} \mid \ p \nmid \beta \,\}$ και $\mathbb{Q}^p = \{\, \frac{\alpha}{\beta} \in \mathbb{Q} \mid \ \beta = p^i, \ i \geq 0 \,\}$ με πράξη την πρόσθεση ρητών αριθμών είναι Αβελιανές ομάδες.

10. Έστω $G_1, G_2, \ldots, G_n$ ομάδες με αντίστοιχες πράξεις $*_1, *_2, \ldots, *_n$. Θεωρούμε το καρτεσιανό γινόμενο $G = G_1 \times G_2 \times \cdots \times G_n$, το οποίο με πράξη $(\, g_1, g_2, \ldots, g_n \,) * (\, r_1, r_2, \ldots, r_n \,) = (\, g_1 *_1 r_1, g_2 *_2 r_2, \ldots, g_n *_n r_n \,)$ είναι, προφανώς, μια ομάδα και ονομάζεται ***ευθύ γινόμενο*** των $G_1, G_2, \ldots, G_n$.

Στα προηγούμενα παραδείγματα ομάδων είδαμε ότι ικανοποιούνται ιδιότητες ανάλογες με βασικές ιδιότητες των ακεραίων αριθμών. Θα δούμε ότι αυτές ισχύουν γενικά σε κάθε ομάδα. Μια πρώτη ιδιότητα είναι αυτή της ***διαγραφής***.

4.3.6 Θεώρημα. *Έστω G μία ομάδα. Αν $a, b, c \in G$, τότε*

1. $a\,c = b\,c \iff a = b$ *και*
2. $c\,a = c\,b \iff a = b$.

Απόδειξη. Πολλαπλασιάζοντας την $a\,c = b\,c$ από τα δεξιά με c^{-1} (αντίστοιχα την $c\,a = c\,b$ από τα αριστερά), λόγω της προσεταιριστικής ιδιότητας, προκύπτει $a = b$. Το αντίστροφο είναι προφανές. ⊺

Το αντίστροφο του προηγούμενου Θεωρήματος δεν ισχύει γενικά. Δηλαδή αν σε ένα σύνολο G, του οποίου τα στοιχεία συνδυάζονται με μία προσεταιριστική πράξη, ισχύουν οι (1) και (2), τότε το G με την πράξη αυτή δεν είναι αναγκαστικά ομάδα. Για παράδειγμα, στο σύνολο των φυσικών αριθμών $\mathbb{N}$ με πράξη την πρόσθεση που είναι προσεταιριστική, ισχύουν οι (1) και (2), αλλά το $\mathbb{N}$ δεν είναι ομάδα. Επίσης αν θεωρήσουμε το σύνολο των $n\times n$ πινάκων με ορίζουσα διάφορη του μηδενός και στοιχεία ακεραίους αριθμούς και πράξη τον πολλαπλασιασμό πινάκων, τότε η προσεταιριστικότητα ισχύει, όπως επίσης και οι ιδιότητες (1) και (2). Αλλά το σύνολο αυτό δεν είναι ομάδα, αφού ο αντίστροφος ενός τέτοιου πίνακα είναι ένας πίνακας που τα στοιχεία του δεν είναι, κατ' ανάγκη ακέραιοι αριθμοί. Για να ήταν ομάδα, όπως έχουμε δει στο Παράδειγμα 4.3.5 (1), θα έπρεπε να περιοριστούμε στους πίνακες με οριζουσα ± 1.

Τα δύο προηγούμενα παραδείγματα για τα οποία δεν ισχύει το αντίστροφο του Θεωρήματος αναφέρονται σε άπειρα σύνολα. Για πεπερασμένα σύνολα τέτοια παραδείγματα δεν είναι δυνατόν να υπάρχουν, αφού ισχύει η εξής

4.3.7 Πρόταση. *Έστω G ένα πεπερασμένο σύνολο. Τότε το G μαζί με μία προσεταιριστική πράξη επί των στοιχείων του είναι ομάδα αν και μόνο αν ισχύουν οι ιδιότητες (1) και (2) του Θεωρήματος 4.3.6.*

Απόδειξη. Έστω $G = \{\, g_1, g_2, \ldots, g_n \,\}$. Υποθέτουμε ότι ισχύουν οι (1) και (2). Αν g είναι ένα τυχαίο στοιχείο του G, τότε τα στοιχεία $g\,g_1$, $g\,g_2$, $\ldots$, $g\,g_n$ είναι όλα τα στοιχεία του G. Πράγματι, αν $g\,g_i = g\,g_j$ τότε, λόγω της (2), $g_i = g_j$. Συνεπώς κάθε $h \in G$ μπορεί να γραφεί στη μορφή $h = g\,g_i$ για κάποιο $i = 1, 2, \ldots, n$. Αυτό σημαίνει ότι η εξίσωση $g\,x = h$ έχει μοναδική λύση για κάθε $g, h \in G$. Όμοια η εξίσωση $x\,g = h$ έχει μοναδική λύση στο G. Άρα, σύμφωνα με το Θεώρημα 4.3.2 , το G με την εν λόγω πράξη είναι ομάδα. ⊺

Δυνάμεις

Έστω τώρα G μια ομάδα. Για τρία στοιχεία a, b, $c \in G$ έχουμε συμβολίσει το γινόμενο $a(bc)$ με abc που λόγω της προσεταιριστικότητας ισούται με $(ab)c$. Τώρα για τέσσερα στοιχεία a, b, c, $d \in G$ έχουμε $a((bc)d) = a(b(cd)) = (ab)(cd) = a(bc)d = ((ab)c)d$. Δηλαδή όπου και να βάλουμε τις παρενθέσεις στο γινόμενο τεσσάρων στοιχείων παίρνουμε το ίδιο στοιχείο. Συνεπώς έχει νόημα να συμβολίσουμε το $a((bc)d)$ με $abcd$. Γενικότερα, για n στοιχεία $a_1, a_2, \ldots, a_n \in G$ ορίζουμε το γινόμενο $a_1\,a_2\,\cdots\,a_n$ με τον εξής επαγωγικό τρόπο: για $n = 0$ αυτό

είναι το ουδέτερο στοιχείο e και θεωρώντας ότι έχουμε ορίσει για κάθε $m < n$ το γινόμενο $a_1\, a_2 \cdots a_m$, ορίζουμε το $a_1\, a_2 \cdots a_n = (a_1\, a_2 \cdots a_{n-1})a_n$. Μπορεί να δειχθεί ότι το γινόμενο αυτό είναι ίδιο με με το γινόμενο $b_1\, b_2 \cdots b_k$, όπου $b_1 = a_1 \cdots a_{s_1-1}$, $b_2 = a_{s_1} \cdots a_{s_2-1}$, $\ldots$, $b_k = a_{s_k} \cdots a_n$, όπου $1 \leq s_1 \leq s_2 \leq \cdots \leq s_k \leq n$ (βλέπε Παράρτημα 6.2). Αν η G είναι Αβελιανή ομάδα τότε προφανώς ισχύει $a_1\, a_2 \cdots a_n = a_{\sigma(1)}\, a_{\sigma(2)} \cdots a_{\sigma(n)}$ για κάθε μετάθεση σ των $1, 2, \ldots, n$.

Έχοντας ορίσει επαγωγικά το γινόμενο $a_1\, a_2 \cdots a_n$, στην περίπτωση που όλα τα a_i είναι ίσα προς ένα στοιχείο $a \in G$, τότε το γινόμενο αυτό συμβολίζεται με a^n και λέγεται ***n*-οστή δύναμη** του a (αν η πράξη είναι η πρόσθεση, τότε αυτό το στοιχείο συμβολίζεται με $n\, a$ και λέγεται ***n*-οστό πολλαπλάσιο** του a). Έτσι έχουμε

$$a^0 = e,\ a^1 = a,\ a^{m+n} = a^m\, a^n,\ a^{m\, n} = (a^m)^n$$

για κάθε $m, n \in \mathbb{N}$. (Χρησιμοποιώντας τον προσθετικό συμβολισμό, οι προηγούμενες σχέσεις γράφονται ως εξής, $0\, a = 0$, $1\, a = a$, $(m+n)\, a = m\, a + n\, a$, $(m\, n)\, a = n\, (m\, a)$.) Αν n είναι ένας αρνητικός ακέραιος, ορίζουμε a^n να είναι το αντίστροφο στοιχείο του a^{-n}. Οι παραπάνω ιδιότητες των δυνάμεων ισχύουν και για αρνητικούς εκθέτες:

4.3.8 Πρόταση. *Έστω a ένα στοιχείο μιας ομάδας και $m, n \in \mathbb{Z}$. Τότε ισχύουν τα εξής:*

1. $a^m\, a^n = a^{m+n} = a^n\, a^m$.
2. $(a^m)^n = a^{m\, n}$.
3. $a^{-n} = (a^{-1})^n = (a^n)^{-1}$, *(συνεπώς ο αντίστροφος του a^n είναι ο a^{-n}).*

Απόδειξη. Η απόδειξη αφήνεται σαν άσκηση. ⊺

Ας θεωρήσουμε τώρα την περίπτωση που για ένα στοιχείο a μιας ομάδας G η $n-$οστή δύναμη του a είναι το ταυτοτικό στοιχείο e (δηλαδή $a^n = e$) για κάποιον $n \in \mathbb{Z} \setminus \{0\}$. Αν $n < 0$, τότε και $a^{-n} = e$, αφού $e = a^0 = a^{n-n} = a^n\, a^{-n} = e\, a^{-n} = a^{-n}$. Συνεπώς, μπορούμε να υποθέσουμε ότι ο n είναι φυσικός αριθμός. Με βάση το Αξίωμα του Ελαχίστου, μπορούμε επίσης να θεωρήσουμε ότι ο n είναι ο μικρότερος θετικός ακέραιος έτσι ώστε $a^n = e$. Από το προηγούμενο θεώρημα έχουμε $a^{k\, n} = a^{n\, k} = (a^n)^k = e$ για κάθε $k \in \mathbb{Z}$, δηλαδή η δύναμη του a σε κάθε ακέραιο πολλαπλάσιο του n ισούται με e. Αυτές οι δυνάμεις του a είναι οι μόνες που ισούνται με e. Πράγματι, αν $a^m = e$, τότε διαιρώντας τον m με τον n εχουμε $m = n\, k + u$, $0 \leq u < n$, οπότε

$e = a^m = a^{nk+u} = a^{nk}\,a^u = a^u$, συνεπώς $u = 0$ αφού ο n είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα $a^n = e$. Ο ίδιος ισχυρισμός δείχνει ότι οι δυνάμεις $a^0 = e$, $a^1 = a$, a^2, $\ldots$, a^{n-1} είναι όλες ανά δύο διαφορετικές και αν $a^m = e$, για κάποιον $m \in \mathbb{Z}$, τότε $m \equiv i \mod n$, όπου $i \in \{0, 1, \ldots, n-1\}$. Με άλλα λόγια οι δυνάμεις του a παρουσιάζουν μια περιοδικότητα με περίοδο n. Παρατηρούμε δε ότι το στοιχείο a^{-1} του a είναι το a^{n-1} του οποίου οι δυνάμεις έχουν την ίδια περιοδικότητα με αυτή του a.

Έχουμε ήδη δει ότι αν η ομάδα G είναι η συμμετρική ομάδα S_n ή η προσθετική ομάδα $\mathbb{Z}_n$ ή η πολλαπλασιαστική ομάδα $U(\mathbb{Z}_n)$ του δακτυλίου $\mathbb{Z}_n$, τότε όλα τα στοιχεία τους παρουσιάζουν περιοδικότητα, δηλαδή ότι ικανοποιούν την ιδιότητα $a^m = e$, για κάποιο m θετικό ακέραιο (που εξαρτάται από το a). Αυτό ισχύει για κάθε πεπερασμένη ομάδα G, αφού οι δυνάμεις a^k, $k = 1, 2, \ldots$, ενός στοιχείου a της G δεν μπορεί να είναι όλες ανά δύο διαφορετικές, διότι τότε η G θα περιείχε άπειρα στοιχεία. Συνεπώς για κάποιο s και κάποιο r θα πρέπει $a^s = a^r$, δηλαδή $a^{s-r} = e$ με $s - r \neq 0$. Αν η ομάδα G ήταν η προσθετική ομάδα $\mathbb{Z}$ των ακεραίων που είναι άπειρη, τότε για κανένα στοιχείο $z \neq 0$ δεν υπάρχει θετικός ακέραιος n τέτοιος ώστε $n\,z = 0$. Από την άλλη πλευρά, η ομάδα $\bigcup_{\nu=1}^{\infty} \mathcal{E}_\nu$ του Παραδείγματος 4.3.5 (8) είναι άπειρη, αλλά για κάθε στοιχείο της a υπάρχει $n > 0$ τέτοιο ώστε $a^n = 1$. Επίσης στην άπειρη ομάδα $GL_2(\mathbb{Q})$ για τον πίνακα $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ έχουμε $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, ενώ για τον πίνακα $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ έχουμε $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

4.3.9 Ορισμός. *Έστω a ένα στοιχείο μιας ομάδας G. Αν υπάρχει θετικός ακέραιος m για τον οποίο $a^m = e$, τότε ο μικρότερος φυσικός n για τον οποίο ισχύει $a^n = e$ ονομάζεται* **τάξη** *του a. Αν δεν υπάρχει θετικός ακέραιος m έτσι ώστε $a^m = e$, τότε λέμε ότι το στοιχείο έχει* **άπειρη τάξη**.

4.3.10 Παρατηρήσεις.

1. Το μόνο στοιχείο μιας ομάδας που έχει τάξη 1 είναι το ουδέτερο στοιχείο της. Όπως είδαμε η τάξη του αντιστρόφου ενός στοιχείου μιας ομάδας είναι ίση με την τάξη του στοιχείου.

2. Αν a και b είναι δύο στοιχεία μιας ομάδας τότε η τάξη του aba^{-1} είναι ίση με την τάξη του b. Αυτό προκύπτει από την ισότητα $(aba^{-1})^m = (aba^{-1}) \cdot (aba^{-1}) \cdots (aba^{-1}) = ab^m a^{-1}$ για κάθε $m > 0$.

3. Αν a και b είναι δύο στοιχεία μιας ομάδας τότε τα στοιχεία ab και ba έχουν την ίδια τάξη. Πράγματι, αφού $ab = a(ba)a^{-1}$, αυτό προκύπτει από την προηγούμενη παρατήρηση.

4. Μπορούμε να έχουμε δύο στοιχεία πεπερασμένης τάξης μέσα σε μία άπειρη ομάδα και το γινόμενό τους να έχει άπειρη τάξη. Έτσι, τα στοιχεία $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ και $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ της $GL_2(\mathbb{Z})$ έχουν και τα δύο τάξη 2, αλλά το γινόμενό τους έχει άπειρη τάξη. Επίσης το στοιχείο $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ έχει τάξη 4 και το στοιχείο $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ έχει τάξη 3, αλλά το γινόμενό τους έχει άπειρη τάξη. Επίσης μπορεί να ισχύει και το αντίστροφο, δηλαδή να έχουμε δύο στοιχεία άπειρης τάξης, αλλά το γινόμενό τους να έχει πεπερασμένη τάξη. Παραδείγματος χάρη, οι πίνακες $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ και $\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$ έχουν αυτή την ιδιότητα (γιατί;).

5. Το πλήθος των στοιχείων a μιας πεπερασμένης ομάδας G που έχουν τάξη $k \neq 1, 2$ είναι άρτιος αριθμός. Πράγματι, αν το a έχει τάξη k, τότε $a = a^{-1}$ αν και μόνο αν $k = 1, 2$. Συνεπώς αν $k \neq 1, 2$, τότε τα a και a^{-1} έχουν τάξη k και $a \neq a^{-1}$.

Περισσότερες ιδιότητες για τις τάξεις των στοιχείων μιας ομάδας θα αναφερθούν στην παράγραφο 4.6. Εδώ θα δείξουμε μόνο την εξής.

4.3.11 Πρόταση. *Έστω g ένα στοιχείο μιας ομάδας, του οποίου η τάξη είναι n. Τότε ισχύουν τα εξής.*

1. *$g^k = 1$ αν και μόνο αν $n \mid k$.*

2. *Η τάξη μιας δύναμης g^m του G είναι ίση με $\frac{n}{d}$, όπου $d = \mu.\kappa.\delta.(n, m)$.*

Απόδειξη. 1. Προφανώς αν $k = \lambda n$, τότε $g^k = g^{\lambda n} = (g^n)^\lambda = 1$.

Αντίστροφα, έστω $g^k = 1$. Από τη διαίρεση του k με το n έχουμε $k = nt+u$ με $0 \leq u < n$, οπότε $1 = g^k = g^{nt} g^u = g^u$ και επομένως $u = 0$, από τον ορισμό του n.

2. Η τάξη του g^m, έστω s, είναι πεπερασμένη (γιατί ;), δηλαδή $(g^m)^s = 1$ με s να είναι ο μικρότερος θετικός ακέραιος με αυτή την ιδιότητα. Αλλά $g^{ms} = 1$ ισχύει αν και μόνο αν $n \mid ms$. Αρα το πρόβλημα ανάγεται στην εύρεση του

μικροτέρου θετικού ακεραίου s για τον οποίο ισχύει $n \mid ms$. Με άλλα λόγια αναζητούμε τον μικρότερο θετικό ακέραιο s για τον οποίο ο ρητός αριθμός $\frac{ms}{n}$ να είναι ακέραιος. Αλλά, αν $d = \mu.\kappa.\delta.(n, m)$, τότε $\frac{ms}{n} = \frac{\frac{m}{d}s}{\frac{n}{d}}$. Επειδή οι ακέραιοι $\frac{m}{d}$ και $\frac{n}{d}$ είναι πρώτοι μεταξύ τους, για να είναι το κλάσμα αυτό ακέραιος πρέπει ο $\frac{n}{d}$ να διαιρεί τον s. Ο μικρότερος θετικός s που διαιρείται με τον $\frac{n}{d}$ είναι ο ίδιος ο $\frac{n}{d}$. T

4.3.12 Πόρισμα. *Έστω g ένα στοιχείο μιας ομάδας του οποίου η τάξη είναι n. Τότε μία δύναμη g^m του g έχει τάξη n αν και μόνο αν $\mu.\kappa.\delta.(n, m) = 1$.*

Από το προηγούμενο Πόρισμα έπεται ότι στην $\mathbb{Z}_m$ υπάρχουν $\varphi(m)$ το πλήθος στοιχεία με τάξη m, όπου, ως γνωστόν, $\varphi(m)$ είναι η συνάρτηση του Euler.

Ασκήσεις 4.3

1. Έστω G το σύνολο των διατεταγμένων τριάδων της μορφής $(k_1, k_2, 1)$ ή $(k_1, k_2, -1)$, όπου $k_1, k_2 \in \mathbb{Z}$. Στο G ορίζουμε μια πράξη θέτοντας $(k_1, k_2, \varepsilon) * (m_1, m_2, \varepsilon') = (k_1 + m_1, k_2 + m_2, \varepsilon\varepsilon')$. Δείξτε ότι το σύνολο G με την πράξη $*$ είναι ομάδα.

2. Έστω X το σύνολο όλων των πραγματικών αριθμών, εκτός του 0 και του 1, και G το σύνολο των εξής απεικονίσεων του X: $\vartheta_1(x) = x$, $\vartheta_2(x) = \frac{1}{x}$, $\vartheta_3(x) = 1 - x$, $\vartheta_4(x) = \frac{x}{x-1}$, $\vartheta_5(x) = \frac{x-1}{x}$, $\vartheta_6(x) = \frac{1}{1-x}$. Δείξτε ότι το σύνολο G είναι ομάδα, ως προς τη σύνθεση απεικονίσεων.

3. Στο σύνολο των ακεραίων ορίζουμε μια πράξη ως εξής $n * m = n + m$, αν ο n είναι άρτιος και $n * m = n - m$, αν ο n είναι περιττός. Δείξτε ότι το σύνολο των ακεραίων με την πράξη αυτή είναι ομάδα.

4. Έστω $G = \{(a, b) \in \mathbb{R}^2, \text{ όπου } a \neq 0\}$. Στο G ορίζουμε μία πράξη ως εξής: $(a_1, b_1) \circ (a_2, b_2) = (a_1a_2, a_1b_2 + b_1)$. Δείξτε ότι σύνολο G με την πράξη $\circ$ είναι ομάδα.

5. Ορίζουμε μια πράξη στο $G = \mathbb{Z}^3$, ως εξής: $(x_1, x_2, x_3) \circ (y_1, y_2, y_3) = (x_1 + y_1, x_2 + y_2, x_3 + y_3 + x_2y_1)$. Δείξτε ότι το σύνολο G με την πράξη $\circ$ είναι ομάδα.

6. Δίνεται το σύνολο $G = \left\{ \begin{pmatrix} \bar{1} & \bar{a} \\ \bar{0} & \bar{b} \end{pmatrix} \mid \bar{0}, \bar{1}, \bar{a}, \bar{b} \in Z_m,\ (b, m) = 1 \right\}$. Δείξτε ότι το σύνολο G είναι ομάδα με πράξη τον πολλαπλασιασμό πινάκων. Επίσης δείξτε ότι $|\, G \,| = m \cdot \varphi(m)$, όπου φ είναι η συνάρτηση του Euler.

7. Έστω G το σύνολο των $n \times n$ πινάκων με στοιχεία πραγματικούς αριθμούς, οι οποίοι είναι ταυτόχρονα συμμετρικοί και ορθογώνιοι. Αποδείξτε ότι το σύνολο G είναι μια άπειρη ομάδα με πράξη τον πολλαπλασιασμό πινάκων.

8. Έστω X ένα σύνολο με μια πράξη $*$ ως προς την οποία ισχύει η σχέση $x * (y * z) = (x * z) * y$, γαι όλα τα στοιχεία $x, y, z \in X$. Δείξτε ότι η πράξη αυτή είναι μεταθετική και προσεταιριστική. Είναι το σύνολο X αναγκαστικά ομάδα ως προς αυτή την πράξη ;

9. Έστω X ένα σύνολο με μία πράξη $*$, η οποία είναι προσεταιριστική και επιπλέον για κάθε $a \in X$ υπάρχει μοναδικό $\bar{a} \in X$ έτσι ώστε $a * \bar{a} * a = a$. Δείξτε ότι το σύνολο X είναι ομάδα ως προς αυτή την πράξη.

10. Έστω G Αβελιανή ομάδα και $x, y \in G$ τέτοια ώστε $x^n = y^n$, όπου n θετικός ακέραιος. Δείξτε ότι $y = x \cdot w$, όπου $w \in G$ έχει τάξη που διαιρεί το n.

11. Υποθέτουμε ότι για τα στοιχεία x, u, v μιας ομάδας G ισχύουν οι σχέσεις: $x = u \cdot v = v \cdot u$ και $u^p = 1$, $v^q = 1$, όπου p, q είναι θετικοί ακέραιοι σχετικά πρώτοι. Δείξτε ότι υπάρχουν σχετικά πρώτοι ακέραιοι αριθμοί n, m έτσι ώστε $u = x^n$ και $v = x^m$.

12. Έστω ότι το στοιχείο x μιας ομάδας G έχει τάξη $n\,m$, όπου οι n και m είναι σχετικά πρώτοι. Δείξτε ότι υπάρχουν u και v στοιχεία της G με $x = u\,v = v\,u$ και $u^n = v^m = 1$. Μπορείτε να γενικεύσετε, αν η τάξη του στοιχείου x είναι $n = p_1^{\lambda_1}\, p_2^{\lambda_2} \cdots p_k^{\lambda_k}$, όπου $p_1, \ldots, p_k$ είναι διακεκριμένοι πρώτοι ;

13. Υποθέτουμε ότι τα τέσσερα στοιχεία a_1, a_2, b_1, b_2 μιας ομάδας G ικανοποιούν τις σχέσεις $a_1\,b_1 = b_1\,a_1 = a_2\,b_2 = b_2\,a_2$ και $a_1^n = a_2^n = b_1^m = b_2^m = 1$, όπου n, m είναι σχετικά πρώτοι ακέραιοι. Δείξτε ότι $a_1 = a_2$ και $b_1 = b_2$.

14. Δείξτε ότι η πολλαπλασιαστική ομάδα $U(\mathbb{Z}_m)$ των ακεραίων modulo m για $m = 2^k$, $k \geq 2$ έχει περιττό πλήθος στοιχεία τάξης 2.
Γενικότερα, αποδείξτε ότι κάθε Αβελιανή ομάδα τάξης 2^m, $m \geq 1$ έχει περιττό πλήθος στοιχεία τάξης 2.

15. Έστω G μια ομάδα και g ένα στοιχείο της με τάξη $m \geq 3$. Δείξτε ότι υπάρχουν τουλάχιστον $\varphi(m)$ το πλήθος στοιχεία της G με τάξη m, όπου φ είναι η συνάρτηση του Euler.

16. α) Έστω p πρώτος αριθμός. Δείξτε ότι η τάξη κάθε στοιχείου της πολλαπλασιαστικής ομάδας $U(\mathbb{Z}_{p^2})$ διαιρεί το $p(p-1)$.
Υπόδειξη: Εφαρμόστε το Θεώρημα του Euler.
Για $p=5$ βρείτε ένα στοιχείο τάξης 4 της $U(\mathbb{Z}_{p^2})$.

β) Δείξτε ότι για κάθε ακέραιο αριθμό n και κάθε p πρώτο ισχύει $n^{p(p-1)+2}-n^2 \equiv 0 \bmod p^2$. Δείξτε ότι $2^{4k+1}-2^{2k} \equiv 1 \bmod 9$, για κάθε ακέραιο k.

17. Πόσα στοιχεία τάξης 2 και πόσα τάξης 3 έχει η ομάδα S_4;

18. Έστω G πεπερασμένη ομάδα τάξης n και $a_1, a_2, \ldots, a_n$ στοιχεία της G (όχι κατ' ανάγκη διακεκριμένα). Δείξτε ότι υπάρχουν $1 \le i \le j \le n$ έτσι ώστε $a_i\, a_{i+1} \cdots a_j = 1$.
Υπόδειξη: Έστω $b_1 = a_1$, $b_2 = a_1\, a_2, \ldots, b_n = a_1 \cdots a_n$. Είναι τα b_i, $i = 1, 2, \ldots, n$ διακεκριμένα ;

19. Δίνεται μια πεπερασμένη ομάδα G και $m, r, s, t, u, v, k \in \mathbb{Z}$.
Αν $a, b \in G$ δείξτε τα εξής.

α) Αν $ba = a^m b^m$, τότε οι τάξεις των στοιχείων $a^m b^{m-2}$, $a^{m-2}b^m$, ab^{-1} είναι ίσες.

β) Αν $b^{-1}ab = a^k$, τότε $b^{-r}a^s b^r = a^{s\cdot k^r}$.

γ) Αν $b^{-1}ab = a^k$, τότε $a^u b^v = b^v a^{u\cdot k^v}$ και $(b^v a^u)^t = b^{tv} a^w$, όπου $w = \frac{k^{tv}-1}{k^v-1}$.

20. Δείξτε ότι κάθε μία από τις παρακάτω συνθήκες συνεπάγεται ότι η ομάδα G είναι Αβελιανή.

α) $(ab)^2 = a^2b^2$, για όλα τα $a, b \in G$.

β) $(ab)^k = a^k b^k$, για $k = j, j+1, j+2$, $j \in \mathbb{Z}$ και για κάθε $a, b \in G$.

γ) $a^2 = 1$, για κάθε $a \in G$.

21. Έστω G μια πεπερασμένη ομάδα με την ιδιότητα: το 3 δεν διαιρεί την τάξη της ομάδας και $(ab)^3 = a^3b^3$, για όλα τα $a, b \in G$. Δείξτε ότι η G είναι Αβελιανή.

22. Έστω A ένα υποσύνολο μιας πεπερασμένης ομάδας G, το οποίο περιέχει περισσότερα από τα μισά στοιχεία της ομαδας. Δείξτε ότι για κάθε $g \in G$ υπάρχουν $a, b \in A$ με $g = a\, b$.

4.4 Υποομάδες και το Θεώρημα του Lagrange

Αυτό που παίζει τον πρωτεύοντα ρόλο στη θεωρία των ομάδων είναι η αλγεβρική δομή τους. Συνεπώς τα υποσύνολα μιας ομάδας που παρουσιάζουν ενδιαφέρον είναι αυτά που χαρακτηρίζονται από αλγεβρικές ιδιότητες οι οποίες απορρέουν από τη δομή της ομάδας. Στην παράγραφο αυτή θα ασχοληθούμε με τα υποσύνολα μιας ομάδας G που έχουν τη δομή ομάδας η οποία ορίζεται από την πράξη της G.

4.4.1 Ορισμός.

Ένα υποσύνολο H μιας ομάδας G θα λέγεται ***υποομάδα*** *της G αν το H είναι ομάδα ως προς την πράξη που ορίζεται στη G. Σ' αυτή την περίπτωση γράφουμε $H \leq G$.*

Έχουμε συναντήσει αρκετά παραδείγματα ομάδων που είναι υποομάδες μιας άλλης ομάδας. Έτσι, όλες οι γραμμικές ομάδες βαθμού n πάνω από ένα σώμα K είναι υποομάδες της γενικής γραμμικής ομάδας $GL_n(K)$. Επίσης κάθε ομάδα μεταθέσεων βαθμού n είναι υποομάδα της συμμετρικής ομάδας S_n. Οι προσθετικές ομάδες των ακεραίων $\mathbb{Z}$, των ρητών $\mathbb{Q}$ και των πραγματικών $\mathbb{R}$ είναι υποομάδες της προσθετικής ομάδας $\mathbb{C}$ των μιγαδικών αριθμών. Ενώ οι πολλαπλασιαστικές ομάδες $\mathbb{Q}^*$, $\mathbb{R}^*$ και $\mathbb{C}^*$ αν και είναι υποσύνολα της προσθετικής ομάδας $\mathbb{C}$ δεν είναι υποομάδες της $\mathbb{C}$. Όπως επίσης η ομάδα $\{1, -1\}$ με πράξη τον πολλαπλασιασμό δεν είναι υποομάδα της προσθετικής ομάδας $\mathbb{Z}$. Γενικά το υποσύνολο $U(R)$ των αντιστρέψιμων στοιχείων ενός δακτυλίου με μονάδα, το οποίο έχει τη δομή ομάδας, δεν είναι υποομάδα της προσθετικής ομάδας του R. Δηλαδή μπορεί ένα υποσύνολο μιας ομάδας G να είναι ομάδα αλλά όχι υποομάδα της G.

4.4.2 Παρατηρήσεις.

1. Το ουδέτερο στοιχείο 1 μιας ομάδας G είναι το ουδέτερο στοιχείο κάθε υποομάδας. Το κενό υποσύνολο $\emptyset$ δεν είναι υποομάδα και το μόνο μονοσύνολο που είναι υποομάδα της G είναι το μονοσύνολο $\{1\}$. Συνεπώς η τομή όλων των υποομάδων της G είναι αυτό το μονοσύνολο, δηλαδή το $\{1\}$. Αυτή την υποομάδα την λέμε "τετριμμένη υποομάδα" της G.

2. Κάθε ομάδα G έχει τουλάχιστον δύο υποομάδες, την τετριμμένη και την ίδια τη G. Κάθε άλλη υποομάδα H της G λέγεται ***γνήσια υποομάδα*** και γράφουμε σ' αυτή την περίπτωση $1 < H < G$. Υπάρχουν ομάδες που δεν έχουν γνήσιες υποομάδες. Αυτές οι ομάδες θα καθοριστούν πλήρως στην παράγραφο 4.6.

3. Η σχέση $\leq$ μεταξύ των υποομάδων μιας ομάδας είναι μεταβατική. Δηλαδή αν $H_1 \leq H_2$ και $H_2 \leq H_3$ τότε $H_1 \leq H_3$.

4. Για να δείξουμε ότι ένα υποσύνολο H μιας ομάδας G είναι υποομάδα δε χρειάζεται να εξετάζουμε αν ισχύει η προσεταιριστική ιδιότητα για την H, αφού αυτή ισχύει για όλη την G.

Σύμφωνα με τον ορισμό της υποομάδας, όταν θέλουμε να εξετάσουμε αν ένα υποσύνολο μιας ομάδας είναι υποομάδα θα πρέπει να ελέγχουμε αν ισχύουν οι ιδιότητες της ομάδας ως προς τον περιορισμό της πράξης στο υποσύνολο. Υπάρχει όμως συντομότερος τρόπος να εξετάσουμε ταυτόχρονα την κλειστότητα της πράξης, την ύπαρξη ουδέτερου και την ύπαρξη αντίστροφου στοιχείου για κάθε στοιχείο του υποσυνόλου.

4.4.3 Λήμμα. *Έστω H ένα μη κενό υποσύνολο μιας ομάδας G. Τότε τα εξής είναι ισοδύναμα*

1. *Το υποσύνολο H είναι υποομάδα.*

2. *Για κάθε δύο στοιχεία h_1 και h_2 της G που ανήκουν στο H το στοιχείο $h_1 h_2^{-1}$ ανήκει στην H.*

3. *(α) Αν δύο στοιχεία h_1 και h_2 της G ανήκουν στο H τότε $h_1 h_2 \in H$. (Συνήθως αυτό εκφράζεται λέγοντας ότι το H είναι κλειστό ως προς την πράξη της G.)*

   (β) Αν το στοιχείο h της G ανήκει στο H τότε και το αντίστροφο αυτού h^{-1} είναι στοιχείο του H.

Απόδειξη. Προφανώς από το 1 προκύπτουν τα 2 και 3. Υποθέτουμε ότι ισχύει το 2. Αφού το H είναι μη κενό, υπάρχει ένα στοιχείο h της G που ανήκει στο H. Συνεπώς, σύμφωνα με την υπόθεση, το ουδέτερο στοιχείο $1 = hh^{-1}$ ανήκει στην H. Άρα για κάθε στοιχείο $h \in H$, το στοιχείο $h^{-1} = 1\,h^{-1} \in H$. Από αυτό προκύπτει ότι για κάθε δύο στοιχεία $h_1, h_2 \in H$ το $h_1 h_2 = h_1 (h_2^{-1})^{-1}$ ανήκει στην H. Δηλαδή το H είναι υποομάδα.

Υποθέτουμε ότι ισχύει το 3. Τότε, επιλέγοντας ένα $h \in H$, έχουμε $h^{-1} \in H$ και άρα $1 = hh^{-1} \in H$. Έτσι, το H είναι υποομάδα. ⊺

Αν I είναι ένα σύνολο δεικτών και H_i, $i \in I$, είναι υποομάδες μιας ομάδας G τότε η τομή

$$H = \bigcap_{i \in I} H_i = \{\, h \in G \mid h \in H_i, \text{ για κάθε } i \in I \,\}$$

είναι υποομάδα της G. Πράγματι, καθώς το $1 \in H_i$, για κάθε $i \in I$, η τομή H είναι διάφορη του κενού. Αν $h_1, h_2 \in H$ τότε το στοιχείο $h_1 h_2^{-1} \in H_i$, για κάθε $i \in I$, αφού τα h_1 και h_2 είναι στοιχεία όλων των υποομάδων H_i, $i \in I$. Συνεπώς και το $h_1 h_2^{-1} \in H$, που σημαίνει, λόγω του 4.4.3, ότι το H είναι υποομάδα. Έτσι, αν $n_1, n_2, \ldots, n_k$ είναι θετικοί ακεραίοι, τότε η τομή H των υποομάδων $n_i\mathbb{Z}$, $i = 1, \ldots, k$, της προσθετικής ομάδας $\mathbb{Z}$ των ακέραιων είναι η υποομάδα $\varepsilon\mathbb{Z}$, όπου ε είναι το ελάχιστο κοινό πολλαπλάσιο των $n_1, n_2, \ldots, n_k$ (γιατί;).

4.4.4 Παρατήρηση. Αν το H είναι πεπερασμένο υποσύνολο, τότε η συνθήκη 3(β) δεν χρειάζεται (βλέπε 4.3.7).

Το κέντρο μιας ομάδας

Όταν μια ομάδα G δεν είναι Αβελιανή είναι σημαντικό να γνωρίζουμε ποια στοιχεία της μετατίθενται με όλα τα στοιχεία της G. Ορίζουμε λοιπόν το σύνολο

$$Z(G) = \{\, z \in G \mid zg = gz \text{ για κάθε } g \in G \,\}$$

Αυτό το σύνολο λέγεται ***κέντρο*** της G. Προφανώς $1 \in Z(G)$ και άρα $Z(G) \neq \emptyset$. Επίσης αν $z_1, z_2 \in Z(G)$ τότε $(z_1 z_2)g = z_1(z_2 g) = z_1(g z_2) = (z_1 g)z_2 = (g z_1)z_2 = g(z_1 z_2)$, για κάθε $g \in G$. Δηλαδή $z_1 z_2 \in Z(G)$. Επιπλέον, για τυχαίο $z \in Z(G)$, η σχέση "$zg = gz$, για κάθε $g \in G$" είναι ισοδύναμη με τη σχέση "$z^{-1}g^{-1} = g^{-1}z^{-1}$, για κάθε $g \in G$". Συνεπώς ισχύει $z^{-1}g = gz^{-1}$, για κάθε $g \in G$, αφού η απεικόνιση $G \to G$, $g \to g^{-1}$ είναι $1-1$ και επί (γιατί;). Άρα το κέντρο της G είναι μια υποομάδα. Για παράδειγμα, το κέντρο της S_n είναι η τετριμμένη υποομάδα $\{\, i \,\}$ αν $n \geq 3$ (βλέπε Άσκηση 4.2.17). Ας υπολογίσουμε το κέντρο $Z(D_{2n})$ της διεδρικής ομάδας τάξης $2n$. Η D_{2n} αποτελείται από τις στροφές $A(2\pi i/n)$ και τις ανακλάσεις $R(2\pi j/n)$ ενός κανονικού κυρτού πολυγώνου που έχει n κορυφές, όπως περιγράφονται στην παράγραφο 4.1 . Επειδή $R(2\pi j/n) = A(2\pi j/n)R(0)$, έχουμε $A\left(\frac{2\pi}{n}\right) R(2\pi j/n) = A\left(\frac{2\pi(j+1)}{n}\right) R(0)$, ενώ $R(2\pi j/n)A\left(\frac{2\pi}{n}\right) = A\left(\frac{2\pi(j-1)}{n}\right) R(0)$ που σημαίνει ότι το κέντρο δεν περιέχει καμιά ανάκλαση. Τώρα από τη σχέση $R(0)A\left(\frac{2\pi i}{n}\right) = A\left(\frac{-2\pi i}{n}\right) R(0)$ προκύπτει ότι το κέντρο είναι η τετριμμένη υποομάδα αν το n είναι περιττός, ενώ αν το n είναι άρτιος τότε το κέντρο έχει δύο στοιχεία: το I και η στροφή $A(\pi)$ που έχει τάξη 2 (γιατί;).

Επειδή η γενική γραμμική ομάδα $GL_n(K)$ είναι μια από τις πλέον σημαντικές ομάδες υπολογίζουμε το κέντρο της.

4.4.5 Θεώρημα. *Έστω K ένα σώμα. Το κέντρο της $GL_n(K)$ αποτελείται από όλους τους πίνακες της μορφής λI, $\lambda \in K$, $\lambda \neq 0$, ενώ το κέντρο της $SL_n(K)$*

αποτελείται από τους ίδιους πίνακες με $\lambda^n = 1$, όπου I είναι ο ταυτοτικός $n \times n$ πίνακας.

Απόδειξη. Προφανώς όλοι οι πίνακες λI, $\lambda \neq 0$, ανήκουν στο κέντρο της $GL_n(K)$ και φυσικά αν $\det(\lambda I) = \lambda^n = 1$ τότε ο $\lambda I \in Z(SL_n(K))$. Αντίστροφα, έστω $A \in Z(GL_n(K))$. Έστω $T_{ij}(\alpha)$, $\alpha \in K$, $1 \leq i, j \leq n$, $i \neq j$, ο $n \times n$ πίνακας του οποίου τα διαγώνια στοιχεία είναι ίσα με 1 όπως επίσης και το στοιχείο στη θέση ij είναι ίσο με a ενώ όλα τα άλλα είναι ίσα με μηδέν. Ο αντίστροφος πίνακας $T_{ij}(\alpha)^{-1}$ του $T_{ij}(\alpha)$ είναι ο $T_{ij}(-\alpha)$. Επειδή ο A είναι στοιχείο του κέντρου πρέπει να ισχύει $T_{ij}(1)A = AT_{ij}(1)$. Αυτή η σχέση είναι ισοδύναμη με την

$$T_{ij}(1)AT_{ij}(-1) = A \qquad (*)$$

Αν $A = (\alpha_{ij})$, υπολογίζοντας το γινόμενο στο αριστερό μέλος της $(*)$, εύκολα προκύπτει ότι $\alpha_{ii} = \alpha_{jj}$ και $\alpha_{jk} = 0$, $j, k = 1, 2, \ldots, n$, για $k \neq j$. Άρα $A = \lambda I$ για κάποιο $\lambda \in K$. Επειδή $\det T_{ij}(\alpha) = 1$, για κάθε α, ο προηγούμενος ισχυρισμός εφαρμόζεται και για έναν πίνακα A του κέντρου της $SL_n(K)$, δηλαδή και σ' αυτή τη περίπτωση πρέπει ο A να είναι της μορφής λI, αλλά επειδή $\det(\lambda I) = \lambda^n$ πρέπει $\lambda^n = 1$. ⊺

4.4.6 Παρατηρήσεις.

1. Από το προηγούμενο Θεώρημα προκύπτει ότι $Z(GL_n(K)) \cap SL_n(K) = Z(SL_n(K))$. Γενικά όμως αν $H \leq G$ δεν ισχύει $Z(G) \cap H = Z(H)$. Για παράδειγμα αν $G = S_3$ και $H = \{\, i, (123), (132) \,\}$, τότε $Z(S_3) \cap H = 1$ και $Z(H) = H$.

2. Η απεικόνιση $Z(GL_n(K)) \to K^*$, $\lambda I \to \lambda$, είναι ένας ισομορφισμός ομάδων (γιατί;). Αν K είναι ένα πεπερασμένο σώμα με q στοιχεία, από τον ισομορφισμό αυτό προκύπτει ότι το κέντρο της $GL_n(K)$ έχει $q - 1$ στοιχεία. Περισσότερα για το κέντρο της $GL_n(K)$ και $SL_n(K)$ θα δούμε στα επόμενα.

3. Αν g είναι ένα στοιχείο μιας ομάδας G τότε το σύνολο

   $$C_G(g) = \{\, x \in G \mid gx = xg \,\}$$

   είναι μια υποομάδα της G και προφανώς ισχύει η ισότητα

   $$Z(G) = \bigcap_{g \in G} C_G(g).$$

   Η υποομάδα $C_G(g)$ ονομάζεται ***κεντροποιούσα*** του g. Με αυτές τις υποομάδες θα ασχοληθούμε στην επόμενη Ενότητα.

Παραγόμενες Υποομάδες

Έστω X ένα υποσύνολο μιας ομάδας G. Είναι φανερό ότι η τομή όλων των υποομάδων που περιέχουν το X είναι η μικρότερη υποομάδα μ' αυτή την ιδιότητα. Το επόμενο λήμμα χαρακτηρίζει αυτή την υποομάδα και περιγράφει έναν από τους πιο σημαντικούς τρόπους εύρεσης υποομάδων μιας ομάδας.

4.4.7 Λήμμα. *Έστω X ένα μη κενό υποσύνολο μιας ομάδας G. Θεωρούμε το υποσύνολο $X^{-1} = \{ x^{-1} \mid x \in X \}$. Τότε το σύνολο H όλων των δυνατών πεπερασμένων γινομένων της μορφής*

$$x_1 x_2 \cdots x_n, \quad n = 0, 1, 2, 3, \ldots \qquad (*)$$

όπου τα x_i είναι οποιαδήποτε (όχι κατ' ανάγκη διακεκριμένα) στοιχεία της ένωσης $X \cup X^{-1}$, είναι μια υποομάδα της G. Επιπλέον αυτή η υποομάδα H είναι η τομή όλων των υποομάδων της G που περιέχουν το X, δηλαδή είναι η μικρότερη υποομάδα που περιέχει το X.

Απόδειξη. Προφανώς το X είναι ένα υποσύνολο του H. Έστω $y, z \in H$, τότε $y = \alpha_1 \alpha_2 \cdots \alpha_n$ και $z = \beta_1 \beta_2 \cdots \beta_m$, όπου $\alpha_i, \beta_j \in X \cup X^{-1}$, οπότε $yz = \alpha_1 \cdots \alpha_n \beta_1 \cdots \beta_m = \gamma_1 \cdots \gamma_{n+m}$, όπου $\gamma_k \in X \cup X^{-1}$. Συνεπώς $yz \in H$. Επίσης αν $x_1 \cdots x_n \in H$ με $x_i \in X \cup X^{-1}$, τότε $(x_1 \cdots x_n)^{-1} = x_n^{-1} \cdots x_1^{-1} \in H$, αφού $x_i^{-1} \in X \cup X^{-1}$. Έτσι σύμφωνα με το Λήμμα 4.4.3, το H είναι υποομάδα.

Τώρα η τομή όλων των υποομάδων που περιέχουν το X είναι η μικρότερη υποομάδα που περιέχει το X και συνεπώς αυτή περιέχεται στο H. Αλλά αφού αυτή η τομή περιέχει το X, σαν ομάδα, θα περιέχει κάθε γινόμενο στοιχείων του $X \cup X^{-1}$, οπότε περιέχει και τα στοιχεία της μορφής $(*)$, δηλαδή την H. ⊺

4.4.8 Ορισμός. *Η υποομάδα H που περιγράφεται στο Λήμμα 4.4.7 ονομάζεται* ***υποομάδα παραγόμενη από το*** *X. Επίσης λέμε ότι το X παράγει την H τα δε στοιχεία του X ονομάζονται* ***γεννήτορες*** *της H. Αυτή την υποομάδα συνήθως τη συμβολίζουμε με $\langle X \rangle$. Αν το X είναι ένα πεπερασμένο υποσύνολο $\{ x_1, \ldots, x_n \}$ τότε γράφουμε $\langle X \rangle = \langle x_1, x_2, \ldots, x_n \rangle$.*

4.4.9 Παρατηρήσεις.

1. Όλα τα γινόμενα $x_1 x_2 \cdots x_n$ της μορφής $(*)$ στο Λήμμα 4.4.7 δεν είναι, κατ' ανάγκη, διακεκριμένα. Έτσι, αν $X = \{ (1\,2), (1\,3\,2) \} \subset S_4$ βλέπουμε ότι $(1\,2)(1\,3\,2)(1\,2) = (1\,3\,2)(1\,3\,2) = (1\,3\,2)^{-1}$. Γενικά αν το X έχει περισσότερα από ένα στοιχεία, το ερώτημα πότε δυο γινόμενα της μορφής $(*)$ συμπίπτουν είναι ένα από τα πιο δύσκολα προβλήματα της θεωρίας ομάδων. Με αυτό το πρόβλημα, γνωστό ως το ***πρόβλημα της λέξης***, δε θα ασχοληθούμε στο βιβλίο αυτό.

2. Προφανώς το ουδέτερο στοιχείο μιας ομάδας G είναι γεννήτορας της τετριμμένης υποομάδας $\{1\}$ που είναι η τομή όλων των υποομάδων της G. Επειδή το κενό σύνολο είναι υποσύνολο κάθε υποομάδας, συνηθίζεται καταχρηστικά να λέμε ότι το κενό σύνολο παράγει τη τετριμμένη υποομάδα.

3. Αν H είναι υποομάδα τότε το σύνολο H όπως επίσης και το σύνολο $H - \{1\}$ είναι σύνολα γεννητόρων της. Γενικά αν K είναι γνήσια υποομάδα της H τότε το σύνολο $H - K$ είναι ένα σύνολο γεννητόρων της H. Πράγματι, αρκεί να δείξουμε ότι $K \subseteq \langle H - K \rangle$. Αλλά για $x \notin K$ το στοιχείο $xy \notin K$ όταν $y \in K$. Συνεπώς $xy \in H - K$ και $x^{-1}(xy) = y \in \langle H - K \rangle$. Άρα $\langle H - K \rangle = H$.

Συνήθως ενδιαφερόμαστε για σύνολα γεννητόρων των οποίων το πλήθος είναι όσο γίνεται μικρότερο, δηλαδή σύνολα γεννητόρων κανένα άλλο υποσύνολο των οποίων δεν είναι σύνολο γεννητόρων. Τέτοια σύνολα λέγονται ανηγμένα σύνολα γεννητόρων. Σημειώνουμε ότι γενικά δεν υπάρχουν σύνολα γεννητόρων για μια υποομάδα ως προς τα οποία κάθε στοιχείο της υποομάδας να γράφεται μοναδικά υπό την μορφή $(*)$ του 4.4.7.

4.4.10 Παραδείγματα.

1. Η προσθετική ομάδα $\mathbb{Z}$ των ακέραιων παράγεται από το μονοσύνολο $\{1\}$ όπως επίσης και από το μονοσύνολο $\{-1\}$. Εκτός από αυτά δεν υπάρχει άλλο μονοσύνολο που να παράγει την $\mathbb{Z}$ (γιατί;). Επίσης το υποσύνολο $\{2, 3\}$ παράγει την $\mathbb{Z}$, αφού κάθε ακέραιος μπορεί να γραφεί στη μορφή $2z_1+3z_2$ με $z_1, z_2 \in \mathbb{Z}$ (γιατί;). Αυτό το σύνολο $\{2, 3\}$ είναι ένα ανηγμένο σύνολο γεννητόρων (γιατί;).

2. Αν V είναι ένας πεπερασμένης διάστασης διανυσματικός χώρος επί του σώματος $\mathbb{Z}_p$, τότε κάθε στοιχείο της προσθετικής ομάδας V γράφεται στη μορφή $z_1v_1 + z_2v_2 + \cdots + z_nv_n$, όπου $\{v_1, v_2, \ldots, v_n\}$ είναι μια βάση και $z_1, \ldots, z_n$ ακέραιοι. Η βάση αυτή είναι ένα ανηγμένο σύνολο γεννητόρων (γιατί;).

3. Είναι γνωστό ότι κάθε ρητός αριθμός $\frac{a}{b}$ μπορεί να γραφεί (μοναδικά) στη μορφή
$$\frac{a}{b} = x_0 + \frac{a_1}{p_1^{\beta_1}} + \frac{a_2}{p_2^{\beta_2}} + \cdots + \frac{a_k}{p_k^{\beta_k}}$$
όπου $x_0, a_i, \beta_i \in \mathbb{Z}$ και $p_1, \ldots, p_k$ είναι πρώτοι αριθμοί με $0 < a_i < p_i$, $1 \leq i \leq k$ και $\beta_i > 0,\ 1 \leq i \leq k$. Επιπλέον όλες οι δυνάμεις $p_i^{\beta_i}$ διαιρούν το b και $p_i^{\beta_i} \neq p_j^{\beta_j},\ i \neq j$.

Συνεπώς το σύνολο $\left\{ \frac{1}{p^n} \mid n \in \mathbb{N},\ p \text{ πρώτος} \right\}$ είναι ένα σύνολο γεννητόρων της προσθετικής ομάδας $\mathbb{Q}$. Για το παράδειγμα αυτό, μπορούμε να δείξουμε ότι δεν υπάρχει κανένα ανηγμένο σύνολο γεννητόρων. Πράγματι, αν X είναι ένα σύνολο γεννητόρων τότε και κάθε υποσύνολο $X - \{\, a \,\}$, για $a \in X$, είναι ένα σύνολο γεννητόρων. Αυτό προκύπτει ως εξής: Αν $b \in X - \{\, a \,\}$ τότε, από τις στοιχειώδεις ιδιότητες των ρητών αριθμών, υπάρχουν μη μηδενικοί ακέραιοι κ, λ έτσι ώστε $\kappa a = \lambda b$ και άρα $\kappa a \in \langle\, X - \{\, a \,\} \,\rangle$. Ως ρητός αριθμός, ο $\frac{1}{\kappa} a$ μπορεί να γραφεί ως άθροισμα ακέραιων πολλαπλάσιων στοιχείων του X, δηλαδή $\frac{1}{\kappa} a = \mu a + c$ για κατάλληλα $\mu \in \mathbb{Z}$ και $c \in \langle\, X - \{\, a \,\} \,\rangle$. Άρα $a = \kappa\mu a + \kappa c = \mu\lambda b + \kappa c \in \langle\, X - \{\, a \,\} \,\rangle$, δηλαδή $\langle\, X - \{\, a \,\} \,\rangle = \langle\, X \,\rangle = \mathbb{Q}$.

4. Το σύνολο των πρώτων αριθμών αποτελεί ένα ανηγμένο σύνολο γεννητόρων της πολλαπλασιαστικής ομάδας των θετικών ρητών αριθμών (γιατί;).

5. Έστω K ένα σώμα και $SL_2(K)$ η ειδική γραμμική ομάδα των 2×2 πινάκων (με στοιχεία από το K) που έχουν ορίζουσα 1. Δείχνουμε ότι το σύνολο

$$X = \left\{ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \mid t \in K \right\}$$

είναι ένα σύνολο γεννητόρων της $SL_2(K)$.
Πράγματι, αν $c \neq 0,\ c \in K$ έχουμε

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & (a-1)c^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} 1 & (d-1)c^{-1} \\ 0 & 1 \end{pmatrix}.$$

Αν $b \neq 0$, τότε έχουμε

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ (d-1)b^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ (a-1)b^{-1} & 1 \end{pmatrix}.$$

Για την περίπτωση $b = c = 0$, έχουμε

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a^{-1} - 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a - 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a^{-1} \\ 0 & 1 \end{pmatrix}.$$

Περισσότερα περί Μεταθέσεων

Ας θεωρήσουμε την συμμετρική ομάδα S_n βαθμού n. Έχουμε δει (Θεώρημα 4.2.13) ότι κάθε μετάθεση γράφεται σαν γινόμενο κύκλων (ξένων ανά δύο μεταξύ τους). Συνεπώς το υποσύνολο όλων των κυκλικών μεταθέσεων είναι ένα σύνολο

γεννητόρων. Αυτό το σύνολο δεν είναι ανηγμένο, καθώς αν $(x_1 \ldots x_k)$ είναι ένας k-κύκλος τότε

$$(x_1\, x_2 \cdots x_k) = (x_1\, x_k)(x_1\, x_{k-1}) \cdots (x_1\, x_2)$$

και συνεπώς το σύνολο $\{\,(i,\, j) \mid 1 \leq i < j \leq n\,\}$ είναι ένα υποσύνολο γεννητόρων της S_n (γιατί;). Οι κυκλικές μεταθέσεις $(i\, j)$, $1 \leq i < j \leq n$ λέγονται ***αντιμεταθέσεις***. Κάθε αντιμετάθεση $(i\, j)$ γράφεται

$$(i\, j) \;=\; (1\, i)(1\, j)(1\, i) \;=\; (1\, j)(1\, i)(1\, j).$$

Άρα κάθε μετάθεση σ γράφεται σαν γινόμενο των αντιμεταθέσεων $(1\, i)$. Αυτό σημαίνει ότι το σύνολο $\{\;(1\, i) \mid 1 < i \leq n\,\}$ είναι ένα σύνολο γεννητόρων. Αυτό είναι ανηγμένο (γιατί;). Μπορούμε να βρούμε μικρότερα, σε πλήθος στοιχείων, υποσύνολα που παράγουν την S_n. Παραδείγματος χάρη, ισχύει $S_n = \langle\, (1\, 2),\ (1\, 2 \cdots n)\,\rangle$. Γι' αυτό αρκεί να δείξουμε ότι κάθε αντιμετάθεση $(1\, i)$ γράφεται σαν ένα γινόμενο των $(1\, 2)$ και $(1\, 2 \cdots n)$. Πράγματι, έχουμε ότι, για $i > 2$

$$(1\, i) \;=\; (i-1\, i)(i-2\, i-1) \cdots (2\, 3)(1\, 2)(2\, 3) \cdots (i-1\, i)$$

και

$$\begin{aligned}
(1\, 2 \cdots n)(1\, 2)(1\, 2 \cdots n)^{-1} &= (2\, 3)\\
(1\, 2 \cdots n)^2(1\, 2)(1\, 2 \cdots n)^{-2} &= (3\, 4)\\
&\;\;\vdots\\
(1\, 2 \cdots n)^{n-2}(1\, 2)(1\, 2 \cdots n)^{-(n-2)} &= (n-1\, n).
\end{aligned}$$

Τώρα ορίζουμε μια από τις σημαντικότερες υποομάδες της S_n την λεγόμενη ***εναλλάσουσα ομάδα***. Η ομάδα αυτή είναι ιδιαίτερα σημαντική όπως θα δούμε στην παράγραφο 4.9.

Είδαμε ότι κάθε μετάθεση γράφεται ως γινόμενο αντιμεταθέσεων. Μια μετάθεση θα λέγεται ***άρτια*** αν γράφεται σαν ένα γινόμενο άρτιου πλήθους αντιμεταθέσεων. Θα δείξουμε τώρα ότι μια άρτια μετάθεση δε μπορεί να γραφεί σαν ένα γινόμενο περιττού πλήθους αντιμεταθέσεων. Με άλλα λόγια, θα δείξουμε ότι μια μετάθεση δε μπορεί να έχει δύο παραγοντοποιήσεις ως γινόμενο αντιμεταθέσεων, με τη μία να περιλαμβάνει ένα άρτιο πλήθος και την άλλη ένα περιττό πλήθος αντιμεταθέσεων. Ας υποθέσουμε ότι αυτό το τελευταίο δεν ισχύει και έστω σ μια μετάθεση για την οποία έχουμε $\sigma = \sigma_1\sigma_2 \cdots \sigma_\lambda$, με λ άρτιο, και $\sigma = \tau_1\tau_2 \cdots \tau_s$, με s περιττό, όπου οι σ_k και οι τ_j, $i \leq k \leq \lambda$, $i \leq j \leq s$, είναι αντιμεταθέσεις. Αυτό σημαίνει ότι για την ταυτοτική μετάθεση i έχουμε $i = \sigma\sigma^{-1} = \sigma_1\sigma_2 \cdots \sigma_\lambda\tau_s\tau_{s-1} \cdots \tau_1$, δηλαδή η i γράφεται σαν γινόμενο περιττού πλήθους αντιμεταθέσεων. Αυτό όμως δεν ισχύει, διότι έχουμε το εξής αποτέλεσμα.

4.4.11 Πρόταση. *Η ταυτοτική μετάθεση i δεν μπορεί να εκφρασθεί ως το γινόμενο ενός περιττού πλήθους αντιμεταθέσεων.*

Απόδειξη. Υποθέτουμε ότι η πρόταση δεν ισχύει. Μεταξύ όλων των δυνατών εκφράσεων $i = \pi_1\pi_2\cdots\pi_t$, όπου οι π_i είναι αντιμεταθέσεις και ο t είναι περιττός, διαλέγουμε μια για την οποία ο αριθμός t είναι ο μικρότερος δυνατός. (Σημειώνουμε ότι $t \geq 3$ αφού η i δεν είναι αντιμετάθεση). Υποθέτουμε ότι $\pi_t = (\alpha\,\beta)$,
$\alpha < \beta$. Μεταξύ όλων αυτών των εκφράσεων διαλέγουμε μια που έχει το μικρότερο δυνατόν αριθμό αντιμεταθέσεων οι οποίες μεταθέτουν το α. Επειδή τώρα $i(\alpha) = \alpha$, θα πρέπει εκτός από την π_t να υπάρχει και άλλη αντιμετάθεση π_j που να μεταθέτει το α. Θεωρούμε τον μεγαλύτερο τέτοιο δείκτη j και έστω $\pi_j = (\alpha\,\gamma)$. Αν μεταξύ των $\pi_{j+1}, \ldots, \pi_{t-1}$ δεν εμφανίζεται το γ τότε η π_j μετατίθεται με όλες αυτές και στη περίπτωση αυτή μπορούμε να τη μεταφέρουμε στη θέση πριν από την π_t. Αν το γ εμφανίζεται, τότε χρησιμοποιώντας τη σχέση $(\alpha\,\gamma)(\gamma\,\delta) = (\gamma\,\delta)(\alpha\,\delta)$ πάλι μπορούμε να αφαιρέσουμε τη π_j από τη θέση της και στη θέση της π_{t-1} να εμφανίσουμε μια αντιμετάθεση της μορφής $(\alpha\,\varepsilon)$, $\varepsilon \in \{1, 2, \ldots, n\}$. Εφαρμόζοντας αυτούς τους χειρισμούς δεν επηρεάζεται ούτε το t ούτε το πλήθος των αντιμεταθέσεων που μεταθέτουν το α. Έτσι η ταυτοτική μετάθεση έχει τη μορφή

$$i = \pi_1\pi_2\cdots\pi'_j\cdots\pi'_{t-2}(\alpha\,\varepsilon)(\alpha\,\beta).$$

Αν $\varepsilon = \beta$ τότε επειδή $(\alpha\,\beta)^2 = i$, η i εκφράζεται σαν ένα γινόμενο αντιμεταθέσεων πλήθους μικρότερου του t, που είναι άτοπο. Αν το $\varepsilon \neq \beta$ τότε από τη σχέση $(\alpha\,\varepsilon)(\alpha\,\beta) = (\beta\,\varepsilon)(\alpha\,\varepsilon)$, η i θα εκφραζόταν σαν ένα γινόμενο αντιμεταθέσεων πλήθους t αλλά μεταξύ αυτών το πλήθος αυτών που μεταθέτουν το α θα ήταν μικρότερο από αυτό που υποθέσαμε. Άρα και σ' αυτή την περίπτωση οδηγούμαστε σε άτοπο. Συνεπώς η ταυτοτική μετάθεση i δεν μπορεί να γραφεί σαν ένα γινόμενο αντιμεταθέσεων περιττού πλήθους. ⊤

Τις μεταθέσεις που δεν είναι άρτιες τις λέμε ***περιττές μεταθέσεις***. Για το γινόμενο των άρτιων και περιττών μεταθέσεων ισχύει ο ίδιος κανόνας που ισχύει για το άθροισμα των άρτιων και περιττών ακεραίων αριθμών.

4.4.12 Θεώρημα.

1. Το γινόμενο δύο άρτιων μεταθέσεων είναι άρτια μετάθεση.

2. Το γινόμενο δύο περιττών μεταθέσεων είναι άρτια μετάθεση.

3. Το γινόμενο μιας άρτιας επί μιας περιττής μετάθεσης είναι περιττή μετάθεση.

4. Η αντίστροφη μετάθεση μιας άρτιας (αντίστοιχα μιας περιττής) είναι άρτια (αντίστοιχα είναι περιττή).

Απόδειξη Είναι προφανής. ⊤

4.4.13 Πόρισμα. *Το σύνολο των άρτιων μεταθέσεων βαθμού n αποτελεί μια ομάδα μεταθέσεων την οποία συμβολίζουμε A_n και ονομάζουμε* ***εναλλάσουσα ομάδα βαθμού n****.*

Έστω ότι οι άρτιες μεταθέσεις της S_n είναι οι $\sigma_1 = i, \sigma_2, \ldots, \sigma_k$. Τότε οι μεταθέσεις $(1\,2)\sigma_1, (1\,2)\sigma_2, \ldots, (1\,2)\sigma_k$ είναι όλες οι περιττές. Πράγματι, αφενός όλες οι μεταθέσεις $(1\,2)\sigma_i$, $i = 1, 2, \ldots, k$ είναι περιττές. Αφετέρου αν ρ είναι μια περιττή μετάθεση τότε η $(1\,2)\rho$ είναι άρτια, δηλαδή $(1\,2)\rho = \sigma_i$ για κάποιο $1 \leq i \leq k$, άρα η ρ πρέπει να είναι μια από τις $(1\,2)\sigma_i$, $1 \leq i \leq k$. Τότε έχουμε $2k = |S_n| = n!$. Άρα η τάξη $|A_n|$ της A_n είναι $\frac{n!}{2}$.

4.4.14 Παρατηρήσεις.

1. Ένας κύκλος μήκους k είναι άρτια (αντίστοιχα περιττή) μετάθεση αν και μόνον αν το k είναι περιττός (αντίστοιχα άρτιος) (γιατί;)

2. Από το Θεώρημα 4.4.12 βλέπουμε ότι οι περιττές μεταθέσεις δεν αποτελούν υποομάδα.

4.4.15 Θεώρημα. *Οι $n-2$ το πλήθος $3-$κύκλοι $(1\,2\,3), (1\,2\,4), \ldots, (1\,2\,n)$ παράγουν την A_n, για $n \geq 3$.*

Απόδειξη. Προηγουμένως δείξαμε ότι οι $n-1$ το πλήθος αντιμεταθέσεις $(1\,2), (1\,3), \ldots, (1\,n)$ παράγουν την S_n και ότι κάθε άρτια μετάθεση μπορεί να εκφρασθεί ως ένα γινόμενο άρτιου πλήθους αντιμεταθέσεων. Συνεπώς κάθε άρτια μετάθεση μπορεί να γραφεί ως το γινόμενο ενός άρτιου πλήθους αντιμεταθέσεων της μορφής $(1\,i)$, $2 \leq i \leq n$. Αλλά ισχύει $(1\,\beta)(1\,\alpha) = (1\,\alpha\,\beta)$, που σημαίνει ότι κάθε άρτια μετάθεση γράφεται ως ένα γινόμενο τέτοιων κύκλων. Τώρα η σχέση $(1\,\beta\,2)(1\,2\,\alpha)(1\,2\,\beta) = (1\,\alpha\,\beta)$ αποδεικνύει το Θεώρημα. ⊤

Κλείνουμε αυτή την υποπαράγραφο αναφέροντας ένα παιγνίδι που λίγο πολύ είναι γνωστό σε όλους μας το λεγόμενο παιγνίδι των 15 πλακιδίων. Αυτό το παιγνίδι είχε επινοηθεί το 1870 από το διάσημο της εποχής εκείνης κατασκευαστή "puzzles" Αμερινανό Sam Loyd και είχε προκαλέσει υστερία στους συμπολίτες του που έπαιζαν μετά μανίας αυτό το παιγνίδι.

Αυτό αποτελείται από 15 πλακίδια (τετραγωνίδια) τα οποία είναι τοποθετημένα σε ένα τετράγωνο πλαίσιο πλευράς τετραπλάσιας αυτής των πλακιδίων. Έτσι τα πλακίδια εφάπτονται το ένα με το άλλο και περισσεύει ένα κενό τετράγωνο που είναι ίσο με το μέγεθος ενός πλακιδίου. Αριθμούμε τα πλακίδια από το 1 έως το 15 όπως στο Σχήμα 1 και αφήνουμε την κάτω δεξιά γωνία κενή. Το

παιγνίδι είναι έτσι κατασκευασμένο ούτως ώστε η κίνηση των πλακιδίων να περιορίζεται στο επίπεδο του πλαισίου και να γίνεται κάθετα και οριζόντια και αυτό είναι δυνατόν επειδή περισσεύει ένα κενό τετραγωνίδιο στο πλαίσιο.

Ξεκινώντας από την κανονική θέση των πλακιδίων (Σχήμα 1), εκτελούμε μια πεπερασμένη ακολουθία επιπέδων μετακινήσεων με τέτοιο τρόπο ώστε στο τέλος το τετράγωνο στη δεξιά κάτω γωνία να είναι κενό. Δηλαδή μετά την εκτέλεση αν και τα πλακίδια θα έχουν καταλάβει νέες θέσεις, κανένα από αυτά δε θα πρέπει να βρίσκεται στη δεξιά κάτω γωνία του πλαισίου. Μια τέτοια εκτέλεση ονομάζεται "πραγματοποιήσιμη κίνηση". Αυτό σημαίνει ότι στη νέα θέση των πλακιδίων, μετά την εκτέλεση μιας ακολουθίας επιτρεπτών μετακινήσεών τους, αντιστοιχεί μια μετάθεση των 1, 2, ... , 15, δηλαδή ένα στοιχείο της S_{15}.

Κανονική θέση

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Σχήμα 1

Αν εκτελέσουμε διαδοχικά δύο πραγματοποιήσιμες κινήσεις τότε προφανώς το αποτέλεσμα είναι πάλι μια πραγματοποιήσιμη κίνηση. Συνεπώς το σύνολο G των μεταθέσεων που αντιστοιχούν στις πραγματοποιήσιμες κινήσεις είναι μια ομάδα μεταθέσεων βαθμού 15. Το ερώτημα είναι ποιες είναι όλες αυτές οι δυνατές μεταθέσεις και συνεπώς οι πραγματοποιήσιμες κινήσεις. Η απάντηση είναι η εξής.

Η ομάδα G είναι η εναλλάσσουσα ομάδα A_{15}. (Μια πλήρης και εκλεπτισμένη απόδειξη αυτού του ισχυρισμού έχει δοθεί από τον A.F. Archer [1] . Μια άλλη απόδειξη δίδεται στο βιβλίο των Mc Coy και Janusez [18]).

Πράγματι, ξεκινώντας από την κανονική θέση κατά τη διάρκεια της διαδικασίας της εκτέλεσης της πραγματοποιήσιμης κίνησης το κενό τετραγωνίδιο, το οποίο το αριθμούμε με το 16, μετακινείται οριζόντια ή κάθετα στο επίπεδο του πλαισίου. Συνεπώς μια μετακίνηση ενός πλακιδίου στη θέση ενός αμέσως παρακειμένου του επιβάλλει την εναλλαγή του 16 με κάποιο άλλο αριθμό και άρα μια τέτοια μετακίνηση αντιστοιχεί σε μια αντιμετάθεση της S_{16}. Συνεπώς αν και το αποτέλεσμα μιας πραγματοποιήσιμης κίνησης μας δίνει μια μετάθεση της S_{15}, η διαδικασία των μετακινήσεων για να πάρουμε αυτή την μετάθεση γίνεται με αντιμεταθέσεις της S_{16}. Ας φαντασθούμε το επίπεδο του πλαισίου σαν να είναι το επίπεδο μιας σκακιέρας, δηλαδή χωρισμένο σε εναλλασσόμενα μαύρα και άσπρα τετραγωνίδια. Κάθε οριζόντια ή κάθετη κίνηση κατά ένα τετραγωνίδιο

μας πηγαίνει από ένα τετραγωνίδιο ενός χρώματος σε ένα τετραγωνίδιο αντιθέτου χρώματος. Άρα ένα περιττό πλήθος τέτοιων κινήσεων θα τελειώνει επί ενός τετραγωνιδίου αντιθέτου χρώματος, ενώ ένα άρτιο πλήθος τέτοιων κινήσεων θα σταματάει σε ένα τετραγωνίδιο του ιδίου χρώματος.

Ιδιαίτερα, αν το κενό τετραγωνίδιο 16 ξεκινήσει να μετακινείται από την κάτω δεξιά γωνία (που έχει ένα συγκεκριμένο χρώμα) και επανέλθει στην αρχική του θέση (και συνεπώς στο ίδιο χρώμα) μετά από μια ακολουθία μετακινήσεων, δηλαδή εκτελεσθεί μια πραγματοποιήσιμη κίνηση, τότε η αντίστοιχη μετάθεση της S_{15} που θα προκύψει θα είναι γινόμενο άρτιου πλήθους αντιμεταθέσεων, δηλαδή μια μετάθεση της A_{16}. Αυτό σημαίνει ότι $G \leq A_{16} \cap S_{15} = A_{15}$. Για παράδειγμα, οι επόμενες ακολουθίες μετακινήσεων αποτελούν μια πραγματοποιήσιμη κίνηση.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

$\xrightarrow{(16\ 15)}$

1	2	3	4
5	6	7	8
9	10	11	12
13	14	16	15

$\xrightarrow{(11\ 16)}$

1	2	3	4
5	6	7	8
9	10	16	12
13	14	11	15

$\xrightarrow{(16\ 12)}$

1	2	3	4
5	6	7	8
9	10	12	16
13	14	11	15

$\xrightarrow{(16\ 15)}$

1	2	3	4
5	6	7	8
9	10	12	15
13	14	11	16

$(11\ 12\ 15) = (16\ 15)(16\ 12)(11\ 16)(16\ 15)$

Επίσης οι μεταθέσεις

$$\begin{aligned}
\alpha &= (6\ 7\ 8\ 12\ 15\ 14\ 10) \\
&= (16\ 15)(15\ 14)(14\ 10)(10\ 6)(6\ 7)(7\ 8)(8\ 12)(12\ 16), \\
\beta &= (1\ 2\ 3\ 4\ 8\ 12\ 15\ 14\ 13\ 9\ 5) \\
&= (16\ 15)(15\ 14)(14\ 13)(13\ 9)(9\ 5)(5\ 1)(1\ 2)(2\ 3)(3\ 4)(4\ 8)(8\ 12)(12\ 16), \\
\gamma &= (4\ 8\ 12\ 15\ 14\ 10\ 6\ 2\ 3) \\
&= (16\ 15)(15\ 14)(14\ 10)(10\ 6)(6\ 2)(2\ 3)(3\ 4)(4\ 8)(8\ 12)(12\ 16)
\end{aligned}$$

είναι στοιχεία της G.

Παρατηρούμε όμως ότι $\alpha^5(11\ 12\ 15)\alpha^{-5} = (11\ 7\ 8)$ και $\beta(7) = 7 = \gamma(7)$, $\beta(11) = 11 = \gamma(11)$. Άρα $\beta^k(11\ 7\ 8)\beta^{-k} = (11, 7, \beta^k(8))$ και $\gamma^k(11\ 7\ 8)\gamma^{-k} = (11, 7, \gamma^k(8))$, για κάθε k. Αλλά αν x είναι ένας αριθμός μεταξύ του 1 και 15

διάφορος του 11 και του 7, τότε, για κάποιο j, $x = \beta^j(8)$ ή $x = \gamma^j(8)$. Συνεπώς κάθε 3-κύκλος της μορφής $(11\ 7\ x)$ ανήκει στην G. Αλλά η A_{15} παράγεται από όλους αυτούς τους 3-κύκλους (γιατί;) και άρα $A_{15} \subseteq G$. Οπότε $G = A_{15}$.

Γινόμενα Υποομάδων

Έστω H_1, H_2 δύο υποομάδες μιας ομάδας G. Η ένωση $H_1 \cup H_2$ είναι υποομάδα αν και μόνο αν η μια από τις δύο υποομάδες περιέχεται στην άλλη. Πράγματι, έστω ότι $H_1 \nsubseteq H_2$. Εκλέγουμε ένα στοιχείο h_1 της H_1 που να μην ανήκει στην H_2. Αν η $H_1 \cup H_2$ είναι υποομάδα τότε κανένα από τα στοιχεία h_1h_2, όπου $h_2 \in H_2$, δεν μπορεί να ανήκει στην H_2 (γιατί;). Άρα όλα αυτά τα στοιχεία θα ανήκουν στην H_1. Επειδή $h_1 \in H_1$ προκύπτει ότι $H_2 \subseteq H_1$. Θεωρούμε τώρα την υποομάδα $\langle H_1 \cup H_2 \rangle$ που παράγεται από την ένωση $H_1 \cup H_2$. Συνήθως γράφουμε $\langle H_1 \cup H_2 \rangle = \langle H_1, H_2 \rangle$ και τη λέμε ***υποομάδα παραγόμενη*** από τις υποομάδες H_1 και H_2. Τα στοιχεία αυτής της υποομάδας είναι εξ ορισμού της μορφής $h_1^{\varepsilon_1}h_2^{\varepsilon_2}\cdots h_k^{\varepsilon_k}$, όπου $h_i \in H_1 \cup H_2$ και $\varepsilon_i = \pm 1$, $1 \leq i \leq k$, για κάποιο k θετικό ακέραιο. Συνεπώς, το σύνολο όλων των γινομένων hh', $h \in H_1$, $h' \in H_2$ είναι υποσύνολο της υποομάδας $\langle H_1, H_2 \rangle$. Αυτό το σύνολο ονομάζεται ***γινόμενο της*** H_1 ***επί την*** H_2 και συμβολίζεται με H_1H_2. Επίσης και το αντίστοιχο σύνολο όλων των γινομένων $h'h$, $h' \in H_2$, $h \in H_1$ είναι υποσύνολο της $\langle H_1, H_2 \rangle$ και ονομάζεται ***γινόμενο της*** H_2 ***επί την*** H_1. Γενικώς ισχύει $H_1H_2 \neq H_2H_1$. Έτσι, αν θεωρήσουμε τις υποομάδες $H_1 = \{ i, (1\,2) \}$ και $H_2 = \{ i, (1\,3) \}$ της S_3, έχουμε ότι $H_1H_2 = \{ i, (1\,2), (1\,3), (1\,3\,2) \}$ ενώ $H_2H_1 = \{ i, (1\,2), (1\,3), (1\,2\,3) \}$. Σημειώνουμε δε ότι $S_3 = \langle H_1, H_2 \rangle$ και ότι τα γινόμενα H_1H_2, H_2H_1 δεν είναι υποομάδες.

Η ισότητα $H_1H_2 = H_2H_1$ σημαίνει ότι για κάθε γινόμενο hh', $h \in H_1$, $h' \in H_2$, υπάρχει κάποιο $h_1 \in H_1$ και $h_2 \in H_2$ έτσι ώστε $hh' = h_2h_1$ (και αντιστρόφως).

4.4.16 Πρόταση. *Αν H_1 και H_2 είναι δύο υποομάδες μιας ομάδας G τότε το γινόμενο H_1H_2 είναι υποομάδα αν και μόνον αν $H_1H_2 = H_2H_1$. Στην περίπτωση αυτή έχουμε $H_1H_2 = H_2H_1 = \langle H_1, H_2 \rangle$.*

Απόδειξη. Έστω ότι $H_1H_2 = H_2H_1$. Προφανώς $1 \in H_1H_2$ και συνεπώς $H_1H_2 \neq \emptyset$. Για να δείξουμε ότι το H_1H_2 είναι υποομάδα, σύμφωνα με το 4.4.3, αρκεί να δείξουμε ότι $(h_1h_2)(h_1'h_2')^{-1} \in H_1H_2$, για κάθε $h_1, h_1' \in H_1$ και $h_2, h_2' \in H_2$. Από την υπόθεση, υπάρχουν $h \in H_1$ και $h' \in H_2$ τέτοια ώστε $h_1'h_2' = h'h$. Επομένως έχουμε

$$(h_1h_2)(h_1'h_2')^{-1} = (h_1h_2)(h'h)^{-1} = (h_1h_2)(h^{-1}h'^{-1}) = h_1(h_2h^{-1})h'^{-1}.$$

Για τον ίδιο λόγο έχουμε $h_2h^{-1} = h''h_2'$, για κάποιο $h'' \in H_1$ και $h_2' \in H_2$. Άρα

$$(h_1h_2)(h_1'h_2')^{-1} = h_1(h''h_2')h'^{-1} = (h_1h'')(h_2'h'^{-1}) \in H_1H_2.$$

Αντίστροφα, έστω ότι το H_1H_2 είναι υποομάδα. Για ένα στοιχείο $h_2h_1 \in H_2H_1$, $h_1 \in H_1$, $h_2 \in H_2$, έχουμε ότι $h_2h_1 = (h_1^{-1}h_2^{-1})^{-1} \in H_1H_2$, αφού H_1, H_2 και H_1H_2 είναι υποομάδες. Άρα $H_2H_1 \subseteq H_1H_2$.

Δείχνουμε τώρα ότι θα ισχύει και $H_1H_2 \subseteq H_2H_1$. Πράγματι, έστω $h_1h_2 \in H_1H_2$, $h_1 \in H_1$, $h_2 \in H_2$. Επειδή η εξίσωση $(h_1h_2)x = 1$ έχει λύση στην H_1H_2, το στοιχείο h_1h_2 είναι το αντίστροφο κάποιου στοιχείου h της υποομάδας H_1H_2. Έστω $h = h_1'h_2'$, $h_1' \in H_1$, $h_2' \in H_2$. Επομένως $h_1h_2 = h^{-1} = (h_1'h_2')^{-1} = h_2'^{-1}h_1'^{-1} \in H_2H_1$. Η τρίτη ισότητα προκύπτει εύκολα και αφήνεται ως άσκηση στον αναγνώστη. ⊤

Κλάσεις mod H και το Θεώρημα του Lagrange.

Έστω H μια υποομάδα μιας ομάδας G. Θα δούμε τώρα ότι μπορούμε να ταξινομήσουμε μ' έναν φυσιολογικό τρόπο, που εξαρτάται από την H, όλα τα στοιχεία της G που βρίσκονται εκτός της H.

Για ένα στοιχείο g της G θεωρούμε το υποσύνολο $gH = \{\, gh \mid h \in H \,\}$ της G. Για παράδειγμα, αν $G = S_3$ και $H = \{\, i, (1\,2\,3), (1\,3\,2) \,\}$ τότε, για $g = (1\,2)$, το $(1\,2)H$ είναι το σύνολο $\{\, (1\,2), (2\,3), (1\,3) \,\}$. Αν $G = GL_n(K)$, $H = SL_n(K)$ και A είναι ένας πίνακας στη G που έχει ορίζουσα $\lambda \in K^*$, τότε κάθε στοιχείο του συνόλου $A\,SL_n(K)$ έχει ορίζουσα λ.

4.4.17 Πρόταση. *Έστω g_1, $g_2 \in G$. Αν $g_1H \cap g_2H \neq \emptyset$ τότε $g_1H = g_2H$. Επιπλέον η ομάδα G είναι η ξένη ένωση*

$$G = \bigcup_{g \in A} gH,$$

όπου το υποσύνολο A της G περιέχει ένα μόνο στοιχείο από κάθε σύνολο gH.

Απόδειξη. Έστω $g_3 \in g_1H \cap g_2H$. Τότε υπάρχουν h_1, $h_2 \in H$ τέτοια ώστε $g_3 = g_1h_1 = g_2h_2$. Πολλαπλασιάζοντας από τα δεξιά με h_1^{-1}, παίρνουμε την ισότητα $g_1 = (g_2h_2)h_1^{-1} = g_2(h_2h_1^{-1})$. Καθώς $h_2h_1^{-1} \in H$, η τελευταία ισότητα δηλώνει ότι $g_1 \in g_2H$. Συνεπώς, για κάθε $h \in H$, όλα τα γινόμενα g_1h είναι στοιχεία του συνόλου g_2H ή με άλλα λόγια $g_1H \subseteq g_2H$. Με όμοιο τρόπο προκύπτει ότι και $g_2H \subseteq g_1H$. Άρα $g_1H = g_2H = g_3H$. Τώρα αν $g \in G$ τότε $g = g \cdot 1 \in gH$. Συνεπώς, η G είναι η ξένη ένωση $\bigcup_{g \in A} gH$. ⊤

4.4.18 Πόρισμα. *Τα υποσύνολα gH, $g \in G$, είναι όλες οι* **κλάσεις ισοδυναμίας** *που ορίζονται από την σχέση ισοδυναμίας:*

$$x, y \in G,\ x \sim y \ \text{ αν και μόνον αν } \ x^{-1}y \in H.$$

Απόδειξη. Γνωρίζουμε (βλέπε Παράρτημα 6.1) ότι υπάρχει $1-1$ αντιστοιχία μεταξύ όλων των διαμερίσεων ενός συνόλου X ως ξένη ένωση μη-κενών υποσυνόλων του και όλων των σχέσεων ισοδυναμίας επί του X. Στην συγκεκριμένη περίπτωση, στην ξένη διακεκριμένη ένωση $G = \dot{\bigcup_{g\in G}} gH$ αντιστοιχεί η σχέση ισοδυναμίας επί της G που ορίζεται ως εξής: δύο στοιχεία $x, y \in G$ είναι ισοδύναμα αν και μόνον αν και τα δύο ανήκουν στο ίδιο σύνολο gH για κάποιο $g \in G$. Είναι όμως εύκολο να δειχτεί ότι $x, y \in gH$ για κάποιο $g \in G$ αν και μόνον αν $x^{-1}y \in H$. ⊤

4.4.19 Ορισμός. *Το σύνολο gH λέγεται* **αριστερή κλάση** $\bmod H$ *στην G που περιέχει το g (ή με αντιπρόσωπο το g). Το σύνολο όλων των αριστερών κλάσεων* $\bmod H$ *το λέμε* **αριστερό σύνολο πηλίκο της** *G δια την H, ή της G* $\bmod H$ *και συμβολίζεται με G/H.*

Το υποσύνολο A της G που περιέχει από κάθε μια αριστερή κλάση $\bmod H$ μόνο ένα στοιχείο, δηλαδή αν $g_1, g_2 \in A$ τότε $g_1H \cap g_2H = \emptyset$ και $G = \dot{\bigcup_{g\in A}} gH$, λέγεται σύνολο **αντιπροσώπων** των αριστερών κλάσεων $\bmod H$.

4.4.20 Παρατήρηση. Η Πρόταση 4.4.17 ισχύει και για τα σύνολα της μορφής $Hg = \{\, hg \mid h \in H \,\}$, $g \in G$, ενώ το Πόρισμα 4.4.18 ισχύει για τα Hg αν αντί για "$x^{-1}y \in H$" γράψουμε $xy^{-1} \in H$. Τα σύνολα Hg λέγονται **δεξιές κλάσεις** $\bmod H$. Όλα τα αποτελέσματα που ισχύουν για τις αριστερές κλάσεις $\bmod H$ ισχύουν και για τις δεξιές κλάσεις $\bmod H$. Εδώ εμείς θα χρησιμοποιήσουμε τις αριστερές κλάσεις $\bmod H$. Σημειώνουμε ότι αν A είναι ένα υποσύνολο αντιπροσώπων των αριστερών κλάσεων $\bmod H$ τότε το A^{-1} που περιέχει όλα τα αντίστροφα στοιχεία του A είναι ένα υποσύνολο αντιπροσώπων των δεξιών κλάσεων $\bmod H$. Πράγματι η αντιστοιχία $xH \longrightarrow Hx^{-1}$ μεταξύ του αριστερού συνόλου πηλίκο και δεξιού συνόλου πηλίκο της G δια H είναι ένα προς ένα και επί (γιατί;).

4.4.21 Παραδείγματα.

1. Θεωρούμε τον διανυσματικό χώρο $\mathbb{R}^2$ (το επίπεδο) επί του $\mathbb{R}$ σαν μια Αβελιανή προσθετική ομάδα. Έστω $H \subseteq \mathbb{R}^2$ ένας μονοδιάστατος διανυσματικός υπόχωρος (συνεπώς μια υποομάδα). Τότε οι αριστερές κλάσεις

mod H (που εδώ συμπίπτουν με τις δεξιές) είναι όλοι οι "ομοπαραλληλικοί" υπόχωροι $v+H$, $v \in \mathbb{R}^2$, δηλαδή όλες οι ευθείες που είναι παράλληλες προς την H, όπως στο Σχήμα 4.6.1 .

Σχήμα 4.6.1

2. Απαριθμώντας τις άρτιες και τις περιττές μεταθέσεις, μετά το Πόρισμα 4.4.13, ουσιαστικά αποδείξαμε ότι οι αριστερές κλάσεις mod A_n στην S_n είναι δύο, η A_n (άρτιες μεταθέσεις) και η $(1\,2)A_n$ (περιττές μεταθέσεις).

3. Αν $G = \mathbb{Z}$ και $H = n\mathbb{Z}$, τότε οι αριστερές (ή δεξιές) κλάσεις mod $n\mathbb{Z}$ είναι ακριβώς οι κλάσεις υπολοίπων mod n.

4. Έστω $\mathbb{C}^*$ η πολλαπλασιαστική ομάδα των μιγαδικών αριθμών. Γνωρίζουμε ότι το υποσύνολο $T = \{\, z \in \mathbb{C}^* \text{με } |z| = 1 \,\} = \{\, \sigma\upsilon\nu\theta + i\,\eta\mu\theta \mid \theta \in \mathbb{R} \,\}$ είναι μια υποομάδα της $\mathbb{C}^*$ και γεωμετρικά αυτή είναι ο κύκλος ακτίνας 1 με κέντρο το O. Αν $z = \rho(\sigma\upsilon\nu\phi + i\,\eta\mu\phi)$ είναι ένας μιγαδικός αριθμός, τότε η αριστερή κλάση mod T που περιέχει το z αποτελείται από όλους τους μιγαδικούς αριθμούς που έχουν μέτρο ρ. Αυτοί βρίσκονται επί του κύκλου με κέντρο O και ακτίνα ίση με ρ. Για διαφορετικές τιμές του ρ παίρνουμε όλες τις άλλες αριστερές κλάσεις mod T (εδώ οι αριστερές και δεξιές κλάσεις mod T συμπίπτουν (γιατί;)). Έτσι όλες οι κλάσεις

mod T είναι οι ομόκεντροι κύκλοι.

1 ρ

Σχήμα 4.6.2

5. Το υποσύνολο $H = \{\, 1, -1, \omega, -\omega, \omega^2, -\omega^2 \,\}$, όπου $\omega = \frac{-1+i\sqrt{3}}{2}$, είναι μια πεπερασμένη υποομάδα της πολλαπλασιαστικής ομάδας $\mathbb{C}^*$. Η αριστερή κλάση mod H με αντιπρόσωπο το μιγαδικό αριθμό $\rho(\sigma\upsilon\nu\,\phi + i\,\eta\mu\,\phi)$ παρίσταται γεωμετρικά από τις κορυφές ενός κανονικού κυρτού εξάγωνου.

$= \rho(cos\phi + isin\phi)$

Σχήμα 4.6.3

Τώρα αποδεικνύουμε το Θεώρημα του Lagrange που είναι ένα από τα βασικότερα θεωρήματα της θεωρίας των πεπερασμένων ομάδων.

4.4.22 Θεώρημα (Lagrange). *Έστω G μια ομάδα και H μια υποομάδα της. Τότε όλες οι αριστερές (και οι δεξιές) κλάσεις* mod H *στη G έχουν το ίδιο*

πλήθος στοιχείων και ισχύει

$$|G| = |H|\,|G : H|$$

όπου με $|G : H|$ *συμβολίζουμε το πλήθος των αριστερών (ή δεξιών) κλάσεων* $\bmod H$. *Το πλήθος αυτό ονομάζεται* ***δείκτης*** *της* H *στην* G. *Συνεπώς αν η* G *είναι μια πεπερασμένη ομάδα τότε η τάξη της διαιρείται από τις τάξεις και από τους δείκτες όλων των υποομάδων της.*

Απόδειξη. Έστω $g \in G$, τότε η απεικόνιση $f : H \longrightarrow gH,\ h \longrightarrow gh$ είναι $1-1$ και επί. Πράγματι, αν $gh_1 = gh_2$ τότε $g^{-1}(gh_1) = g^{-1}(gh_2)$ ή $(g^{-1}g)h_1 = (g^{-1}g)h_2$, δηλαδή $h_1 = h_2$, άρα η f είναι $1-1$. Αυτή είναι επί, αφού το τυχόν στοιχείο $gh \in gH$ είναι εικόνα του h. Αλλά η ομάδα G είναι η ξένη ένωση των $|G : H|$ το πλήθος αριστερών κλάσεων $\bmod H$ που, όπως μόλις δείξαμε, κάθε μια έχει το ίδιο πλήθος στοιχεία. Άρα $|G| = |H|\,|G : H|$. Αν η G είναι πεπερασμένη, αυτό σημαίνει ότι

$$|\,G : H\,| = \frac{|\,G\,|}{|\,H\,|}\ .\mathsf{T}$$

4.4.23 Πόρισμα. *Σε μια πεπερασμένη ομάδα* G *η τάξη κάθε στοιχείου της* g *διαιρεί την τάξη της* G *και ισχύει* $g^{|G|} = 1$.

Απόδειξη. Θεωρούμε την υποομάδα της G που παράγεται από το στοιχείο g. Τότε η τάξη αυτής είναι ίση με τη τάξη του g. Πράγματι, έστω n η τάξη του g. Αν $g^k = g^l$ αυτό σημαίνει $g^{k-l} = 1$ και αυτό με τη σειρά του σημαίνει ότι $k \equiv l \bmod n$ (βλέπε Πρόταση 4.3.11). Δηλαδή τα στοιχεία αυτής της υποομάδας (που είναι όλες οι δυνάμεις του g) αντιστοιχούν $1-1$ με τις κλάσεις υπολοίπων $\bmod n$, των οποίων το πλήθος είναι ακριβώς n. Άρα το n διαιρεί την τάξη $|G|$ και άρα $g^{|G|} = 1$. T

4.4.24 Πόρισμα (Θεώρημα του Euler). *Έστω* a *και* m *δύο θετικοί ακέραιοι πρώτοι μεταξύ τους. Τότε* $a^{\varphi(m)} \equiv 1 \bmod m$.

Απόδειξη. Θεωρούμε την πολλαπλασιαστική ομάδα $U(\mathbb{Z}_m)$ των αντιστρέψιμων κλάσεων υπολοίπων $\bmod m$. Γνωρίζουμε ότι η τάξη της είναι $\varphi(m)$ όπου φ είναι η γνωστή συνάρτηση του Euler. Από το προηγούμενο πόρισμα παίρνουμε το αποτέλεσμα. T

4.4.25 Πόρισμα. *Αν* H_1, H_2 *είναι υποομάδες μιας πεπερασμένης ομάδας* G *και* $H_1 \leq H_2$, *τότε* $|G : H_1| = |G : H_2| \cdot |H_2 : H_1|$.

Απόδειξη. Έχουμε $|G : H_2| = \frac{|G|}{|H_2|} = \frac{|G|/|H_1|}{|H_2|/|H_1|} = \frac{|G:H_1|}{|H_2:H_1|}$. T

4.4.26 Πόρισμα. *Μια μη-τετριμμένη ομάδα G δεν έχει καμιά γνήσια υποομάδα αν και μόνον αν η τάξη της είναι ένας πρώτος αριθμός.*

Απόδειξη. Υποθέτουμε ότι αν $\{1\} \leq H < G$ τότε $H = \{1\}$. Έστω $g \neq 1$ ένα στοιχείο της G. Τότε η υποομάδα $\langle g \rangle$ που παράγεται από το g πρέπει να είναι όλη η G. Αυτή δεν μπορεί να είναι άπειρη, αφού διαφορετικά για ένα $n \in \mathbb{N}$, $n > 1$, η υποομάδα που παράγεται από τη δύναμη g^n του g θα ήταν γνήσια υποομάδα. Άρα η $\langle g \rangle = G$ πρέπει να είναι πεπερασμένης τάξης έστω m. Τώρα ο m πρέπει να είναι πρώτος, διότι διαφορετικά αν k ήταν ένας γνήσιος διαιρέτης του, το στοιχείο $g^{m/k}$ και συνεπώς η υποομάδα $\langle g^{m/k} \rangle$ θα είχαν τάξη k (γιατί;). Αντίστροφα, αν η τάξη $|G|$ είναι ένας πρώτος αριθμός, τότε από το Θεώρημα του Lagrange έπεται ότι η G δε μπορεί να έχει γνήσιες υποομάδες. ⊺

4.4.27 Παρατήρηση. Όπως θα δούμε στο επόμενο παράδειγμα, το αντίστροφο του θεωρήματος του Lagrange δεν ισχύει γενικά για πεπερασμένες ομάδες. Με άλλα λόγια, αν k είναι ένας διαιρέτης της τάξης μιας ομάδας τότε δεν είναι αναγκαίο να υπάρχει υποομάδα τάξης k. Στην επόμενη παράγραφο, θα δούμε ότι αυτό ισχύει για τις κυκλικές ομάδες. Γενικότερα, για κάθε πεπερασμένη Αβελιανή ομάδα και κάθε διαιρέτη k της τάξης της υπάρχει πάντα υποομάδα τάξης k (βλέπε Θεώρημα 4.8.1). Σημειώνουμε επίσης ότι στην επομένη Ενότητα θα αποδείξουμε το θεώρημα του Sylow, το οποίο αναφέρει ότι το αντίστροφο του θεωρήματος του Lagrange ισχύει για διαιρέτες της τάξης μιας πεπερασμένης ομάδας, οι οποίες είναι δυνάμεις πρώτων αριθμών.

Παράδειγμα. Θεωρούμε την εναλλάσουσα ομάδα A_4 που έχει τάξη 12. Από το θεώρημα του Lagrange οι πιθανές τάξεις των γνήσιων υποομάδων της A_4 είναι 2, 3, 4 και 6. Οι υποομάδες που έχουν τάξη 2, 3 και 4 είναι οι εξής.

Υποομάδες τάξης 2: $\{i, (12)(34)\}$, $\{i, (13)(24)\}$, $\{i, (14), (23)\}$.

Υποομάδες τάξης 3: $\{i, (123), (132)\}$, $\{i, (124), (142)\}$, $\{i, (134), (143)\}$, $\{i, (234), (243)\}$.

Υποομάδες τάξης 4: $\{i, (12)(34), (13)(24), (14)(23)\}$.

Ισχυριζόμαστε τώρα ότι η A_4 δεν έχει υποομάδα τάξης 6. Πράγματι, αν υποθέσουμε ότι υπήρχε μια τέτοια υποομάδα H, τότε επειδή $|H| = 6$ και η A_4 έχει 8 στοιχεία τάξης 3, μπορούμε να διαλέξουμε ένα από αυτά, έστω g, που να μην ανήκει στην H. Συνεπώς οι αριστερές κλάσεις $\bmod H$, H και gH, θα ήταν ξένες μεταξύ τους. Επειδή $|A_4 : H| = 2$, θα έπρεπε $A_4 = H \cup gH$. Συνεπώς το $g^2 \in H$ ή το $g^2 \in gH$. Αλλά $g^2 = g^{-1}$, άρα αν $g^2 \in H$ τότε το $g \in H$ και αν $g^2 = gh$, $h \in H$, πάλι προκύπτει ότι $g = h \in H$, που είναι άτοπο. Άρα δεν μπορεί να υπάρχει τέτοια υποομάδα.

Ασκήσεις 4.4

1. Περιγράψτε τις πεπερασμένες υποομάδες της προσθετικής ομάδας ενός τριδιάστατου διανυσματικού χώρου επί του σώματος των πραγματικών αριθμών.

2. Να δειχθεί ότι η D_n είναι μια υποομάδα της D_{2n} (θεωρήστε τις συμμετρίες ενός κανονικού $2n$-γωνου).

3. Δείξτε ότι τα εξής σύνολα είναι υποομάδες της γενικής γραμμικής ομάδας $GL_2(\mathbb{R})$.

   α) $H_1 = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \mid \alpha \neq 0 \right\}$ β) $H_3 = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \mid \alpha \neq 0 \right\}$

   γ) $H_2 = \left\{ \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \mid \beta \in \mathbb{R} \right\}$.

4. Έστω G ομάδα με τάξη 12. Πόσα σύνολα αριστέρων αντιπροσώπων υπάρχουν για μια υποομάδα της H με τάξη 3 ;

5. Έστω G πεπερασμένη ομάδα και a, b δύο στοιχεία της με τάξη p ένα πρώτο αριθμό. Δείξτε ότι:

   α) $\langle a \rangle \cap \langle b \rangle = 1$ ή $\langle a \rangle = \langle b \rangle$.

   β) Το πλήθος των στοιχείων τάξης p της G είναι πολλαπλάσιο του $p-1$.

6. Έστω G ομάδα με $G =< a, b, c >$ και $a^2 = b$, $b^2 = c$, $c^2 = a$. Δείξτε ότι:
   i) Η G είναι Αβελιανή.
   ii) $G =< a >=< b >=< c >$.
   iii) Να βρεθεί η τάξη της G, αν η G δεν είναι τετριμμένη.

7. Έστω ομάδα $G = \langle x, y \rangle$ με την ιδιότητα $x^{-1}yx = y^k, \quad k \in \mathbb{Z}$. Δείξτε ότι κάθε στοιχείο της G είναι της μορφής $x^m y^n$, $m, n \in \mathbb{Z}$. Αν επιπλέον τα x και y έχουν τάξεις r και s αντίστοιχα, δείξτε ότι ε.κ.π.$(r, s) \leq |G| \leq rs$.

8. Έστω G ομάδα και $a, b, c \in G$ τρία στοιχεία, τέτοια ώστε $a^3 = b^3 = c^4 = 1$, $ac = ca^{-1}$, $aba^2 = bcb^{-1}$. Δείξτε ότι η υποομάδα $\langle a, b, c \rangle$ είναι η τετριμένη υποομάδα.

9. Να βρεθούν οι αριστερές και δεξιές κλάσεις της S_3 στην S_4.

10. Να βρεθούν οι αριστερές κλάσεις $\bmod H$ στην S_4, όπου H είναι η υποομάδα που παράγεται από την μετάθεση $(1\,2\,3\,4)$.

11. Έστω $S = \{ a_1, a_2, a_3, a_4, a_5, a_6 \}$ τα στοιχεία της S_4 που έχουν τάξη 4. Δείξτε ότι το $S^2 = S \cdot S$ περιέχει όλα τα στοιχεία της A_4.

12. Έστω H, K υποομάδες μιας ομάδας G με τάξεις 5 και 8 αντίστοιχα. Δείξτε ότι $H \cap K = \{ 1 \}$.

13. Έστω G μια ομάδα μεταθέσεων βαθμού n και έστω σ μια μετάθεση που δεν ανήκει στην G. Είναι αναγκαστικά η ένωση $\sigma G \cup G$ υποομάδα της S_n ; Αν η G παράγεται από τις μεταθέσεις $\sigma_1, \sigma_2, \ldots, \sigma_k$ πώς μπορούμε να υπολογίσουμε την τάξη της υποομάδας που παράγεται από τις μεταθέσεις $\sigma_1, \sigma_2, \ldots, \sigma_k, \sigma$;

14. Έστω G Αβελιανή ομάδα με τάξη 15.
i) Να βρεθούν όλες οι υποομάδες της και όλα τα σύμπλοκα ως προς μία γνήσια υποομάδα της.
ii) Έστω $a, b \in G$ με $a^6 = b^8 = 1$. Δείξτε ότι $b = 1$ και είτε $a = 1$, είτε η τάξη του a είναι 3.

15. Έστω A, $B \leq G$ και x, $y \in G$. Δείξτε ότι το σύνολο $xA \cap yB$ είναι είτε το κενό είτε ένα αριστερό σύμπλοκο της $A \cap B$ στη G, οπότε $x(A \cap B) = xA \cap xB$.

16. Έστω G ομάδα, H υποομάδα της με δείκτη $| G : H | = n$ και $g \in G$. Δείξτε ότι υπάρχει ακέραιος m, $1 < m \leq n$, τέτοιος ώστε $g^m \in H$.

17. Έστω A, B υποομάδες της ομάδας G. Αν ο δείκτης της B στη G είναι πεπερασμένος, δείξτε ότι η $A \cap B$ έχει επίσης πεπερασμένο δείκτη στην A και μάλιστα $| A : A \cap B | \leq | G : B |$. (Αυτή η ανισότητα αναφέρεται ως Θεώρημα του Poincaré.)

18. Έστω A, B υποομάδες της ομάδας G. Δείξτε ότι:
i) Αν μ.κ.δ.$(|A|, |B|) = 1$, τότε $A \cap B = 1$.
ii) Αν μ.κ.δ.$(|G : A|, |G : B|) = 1$, τότε $|G : A \cap B| = |G : A| \cdot |G : B|$.

19. Έστω G πεπερασμένη ομάδα και H, $K \leq G$. Δείξτε ότι
α) $| \langle H, K \rangle : K | \geq | H : H \cap K |$.
β) Αν $| H : H \cap K | > 1/2 \, | G : K |$, τότε $\langle H, K \rangle = G$.
γ) Ισχύει $| H : H \cap K | = | G : K |$ αν και μόνον αν $G = HK (= KH)$.

20. Έστω A, B δύο πεπερασμένες υποομάδες της ομάδας G. Δείξτε ότι $|AB| = \frac{|A||B|}{|A \cap B|}$.

21. i) Έστω $\pi \in S_n$, δείξτε ότι είτε $< A_n, \pi >= S_n$, είτε $\pi \in A_n$.
ii) Γενικά αν G είναι μια ομάδα και $H \leq G$ με $\mid G : H \mid = p$, p πρώτος, τότε για κάθε $g \in G$ είτε $< H, g >= G$, είτε $< H, g >= H$.

22. Δείξτε ότι η A_4 είναι η μόνη υποομάδα της S_4 με τάξη 12.

23. Έστω X ένα μη κενό σύνολο και $G \leq S_X$.
α) Να δειχθεί ότι η σχέση $a \sim b \overset{o\rho}{\iff}$ υπάρχει $g \in G$ τέτοιο ώστε $b = g(a)$, για $a, b \in X$ είναι μια σχέση ισοδυναμίας στο X.
β) Το σύνολο $H_a = \{\, g \mid g \in G$ τέτοιο ώστε $g(a) = a \,\}$, όπου $a \in X$, είναι υποομάδα της G.
γ) Μπορείτε να περιγράψετε τις κλάσεις ισοδυναμίας του συνόλου X;

24. i) Έστω G ομάδα με $\mid G \mid = 121$. Δείξτε ότι η εξίσωση $x^7 = g$ έχει λύση στην G για κάθε $g \in G$.
ii) Να βρεθούν οι λύσεις των εξισώσεων $7x \equiv 28 \pmod{11}$, $x^7 \equiv 28 \pmod{11}$.

25. i) Έστω G πεπερασμένη ομάδα και $a \in G$, δώστε ικανή και αναγκαία συνθήκη έτσι ώστε η εξίσωση $x^k = a$ να έχει λύση στην G.
ii) Έστω G μια ομάδα με τάξη 100. Δείξτε ότι για κάθε $g \in G$ υπάρχει μοναδικό $x \in G$ τέτοιο ώστε $x^{11} = g$.

26. Να βρεθούν τα a, b, για τα οποία η μετάθεση

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & a & 1 & b & 6 & 7 & 3 \end{pmatrix} \in S_7$$

είναι περιττή. Εξετάστε αν η μετάθεση $(1\,3\,6)$ είναι μία δύναμη της σ.

27. Έστω $H \leq S_n$ που περιέχει τουλάχιστον μια περιττή μετάθεση. Δείξτε ότι ακριβώς τα μισά απο τα στοιχεία της H είναι περιττές μεταθέσεις.

28. Δείξτε ότι τα στοιχεία μιας Αβελιανής ομάδας τάξης 2 μαζί με το μοναδιαίο αποτελούν υποομάδα.
Ισχύει το προηγούμενο αποτέλεσμα αν η ομάδα δεν είναι Αβελιανή ;

29. Έστω G μια ομάδα άρτιας τάξης.
i) Να δειχτεί ότι η G έχει (τουλάχιστον) ένα στοιχείο τάξης 2.
ii) Αν η G έχει ακριβώς ένα στοιχείο τάξης 2, έστω το z, τότε να δειχτεί ότι $z \in Z(G)$.
iii) Να δειχτεί ότι η εξίσωση $x^2 = 1$ έχει άρτιο το πλήθος λύσεις στη G.

30. Έστω G μια Αβελιανή ομάδα με τάξη $|\,G\,| = 2\,m$, όπου ο m είναι περιττός. Δείξτε ότι η G έχει ακριβώς ένα στοιχείο τάξης 2.
Υπόδειξη: Δείξτε ότι αν μια Αβελιανή ομάδα έχει δύο στοιχεία τάξης 2, τότε η υποομάδα που παράγουν αυτά τα στοιχεία έχει τάξη 4.

31. Θεωρούμε την υποομάδα H της $GL_3(\,\mathbb{R}\,)$ των πινάκων της μορφής

$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}, \quad a \cdot b \cdot c \neq 0\,.$$

Ποιά είναι η αριστερή κλάση $\bmod H$ που περιέχει το στοιχείο
$\begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$;

32. Δείξτε ότι οι πίνακες $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ με $a,\, b,\, c,\, d \in 2\,\mathbb{Z}$ αποτελούν μια ομάδα H ως προς την πρόσθεση πινάκων. Περιγράψτε τις κλάσεις $\bmod H$, αν η H θεωρηθεί ως υποομάδα της προσθετικής ομάδας των 2×2 πινάκων με στοιχεία ακεραίους αριθμούς και αν η H θεωρηθεί ως υποομάδα της προσθετικής ομάδας των 2×2 πινάκων με στοιχεία πραγματικούς αριθμούς.

33. Να προσδιορίσετε τις υποομάδες $H = \langle\, -\frac{1}{2}\, i\,\rangle$ και $K = \langle\, 2,\, -5\,\rangle$
i) Αν θεωρηθούν ως υποομάδες της πολλαπλασιαστικής ομάδας των μιγαδικών αριθμών.
ii) Αν θεωρηθούν ως υποομάδες της προσθετικής ομάδας των μιγαδικών αριθμών.
iii) Στις δύο προηγούμενες περιπτώσεις προσδιορίστε την τομή των H και K με την πολλαπλασιαστική και προσθετική ομάδα των πραγματικών αριθμών αντίστοιχα.

34. Έστω H μια υποομάδα της ομάδας G και $f : G \longrightarrow G$ μια απεικόνιση με τις εξής ιδιότητες
$f(\,f(z)\,) = f(z)$, $z^{-1}\, f(z) \in H$, $f(zh) = f(z)$, για κάθε $z \in G$ και κάθε $h \in H$. Δείξτε ότι το σύνολο $f(G)$ αποτελεί ένα δεξιό σύνολο αντιπροσώπων της H στη G.

35. Έστω $H \leq K \leq G$. Αν R είναι ένα σύνολο αριστερών αντιπροσώπων της H στην K και S ένα σύνολο αριστερών αντιπροσώπων της K στην G, δέιξτε ότι το σύνολο $R\,S$ είναι ένα σύνολο αριστερων αντιπροσώπων της H στη G. (Σύγκρινε με το Πόρισμα 4.4.25).

36. Να βρεθούν οι υποομάδες της προσθετικής ομάδας των πολυωνύμων που παράγονται από τα:
α) x β) $1, x, x^2, x^3$ γ) x, x^3, x^5, x^7 δ) $1, x^2, x^4, x^6$ ε) $3x+1, x^2$.

37. Δείξτε ότι μια ομάδα τάξης p^m όπου p είναι ένας πρώτος αριθμός και $m = 2, 3, 4, \ldots$ περιέχει τουλάχιστον μια υποομάδα τάξης p.

38. Να βρεθεί ένα παράδειγμα μιας ομάδας G που περιέχει ένα υποσύνολο S το οποίο είναι ομάδα ως προς ένα διαφορετικό πολλαπλασιασμό από εκείνον της G αλλά να μην είναι υποομάδα της G.

39. Να δειχτεί ότι η συμμετρική ομάδα S_n έχει τουλάχιστον $\binom{n}{r}$ υποομάδες τάξης r.

40. Να δειχτεί ότι σε μια ομάδα δύο στοιχεία που μετατίθενται παράγουν μια Αβελιανή υποομάδα.

41. Δείξτε ότι οι πίνακες της μορφής $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ με $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ τέτοιοι ώστε $\alpha\delta - \beta\gamma = 1$ και $\gamma \equiv 0 \mod n$ αποτελούν μια υποομάδα της $SL_2(\mathbb{Z})$.

42. Έστω $\alpha, \beta \in \mathbb{N}$. Δείξτε ότι $\langle \bar{\alpha} \rangle = \langle \bar{\beta} \rangle \subseteq \mathcal{U}(\mathbb{Z}_{\alpha\beta-1})$ όπου $\bar{\alpha} = \alpha \mod (\alpha\beta - 1)$ και $\bar{\beta} = \beta \mod (\alpha\beta - 1)$.
Υπόδειξη: Τα α και β είναι το ένα αντίστροφο του άλλου στην $\mathcal{U}(\mathbb{Z}_{\alpha\beta-1})$.

43. Έστω E_{ij} ο τετραγωνικός $n \times n$ πίνακας που έχει σε όλες τις θέσεις 0 εκτός από τη θέση (i, j) στην οποία έχει 1. Δείξτε ότι οι πίνακες $I_n + \alpha E_{ij}$, $i \neq j$, $\alpha \in \mathbb{C}$, παράγουν την $SL_n(\mathbb{C})$. Επίσης οι πίνακες $I_n + E_{ij}$ ($n^2 - n$ το πλήθος) παράγουν την $SL_n(\mathbb{Z})$ αλλά και οι πίνακες

$$I_n + E_{12},\ E_{12} + E_{23} + \cdots + E_{n-1,n} + (-1)^{n-1} E_{n,1}$$

παράγουν την $SL_n(\mathbb{Z})$.

44. Δείξτε ότι το αντίστροφο του θεωρήματος του Lagrange ισχύει για την S_4 και D_n $n \geq 3$.

45. Έστω $f = f(x_1, \ldots, x_n)$ ένα πολυώνυμο n μεταβλητών $x_1, \ldots, x_n$ με συντελεστές από το σώμα $\mathbb{Q}$. Αν $\sigma \in S_n$, τότε ορίζουμε
$f^\sigma = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. Οι συμμετρίες αυτού του πολυωνύμου ορίζονται να είναι όλες οι μεταθέσεις $\sigma \in S_n$ τέτοιες ώστε $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n)$. Δείξτε ότι όλες οι συμμετρίες του f αποτελούν μια υποομάδα της S_n. Να βρεθούν οι συμμετρίες των πολυωνύμων.

α) $f = x_1x_2 + x_3x_4$

β) $f = x_1x_2 + x_2^4$

γ) $f = \sum_{i \le i < j \le n} x_ix_j$

Αν H είναι ομάδα των συμμετριών ενός πολυωνύμου f και $S_n = H\dot{\cup}\sigma_1H\dot{\cup}\sigma_2H\dot{\cup}\cdots\dot{\cup}\sigma_kH$ είναι η ανάλυση της S_n στις αριστερές κλάσεις $\mod H$ δείξτε ότι όλα τα πολυώνυμα f^σ είναι ακριβώς τα $f, f^{\sigma_1}, \ldots, f^{\sigma_k}$. (Προφανώς ισχύει $f^{\sigma_1\sigma_2} = (f^{\sigma_1})^{\sigma_2}$).

46. Υπάρχει ομάδα G που παράγεται από δύο στοιχεία της και περιέχει μια υποομάδα H που δεν παράγεται από 2 στοιχεία;

47. Αν μια υποομάδα της S_n περιέχει και άρτιες και περιττές μεταθέσεις, τότε το πλήθος των άρτιων ισούται με το πλήθος των περιττών.

4.5 Ομομορφισμοί Ομάδων

Το κύριο εργαλείο που χρησιμοποιείται για την εύρεση και μελέτη των κοινών ιδιοτήτων που έχουν δύο ομάδες είναι η έννοια του ομομορφισμού ομάδων.

4.5.1 Ορισμός. *Ένας* ***ομομορφισμός*** ϕ *από μια ομάδα* G *σε μια ομάδα* G' *είναι μια απεικόνιση από την* G *στην* G' *τέτοια ώστε*

$$\phi(a * b) \;=\; \phi(a) \star \phi(b), \;\; a, b \in G$$

όπου $*$ *και* $\star$ *είναι αντίστοιχα οι πράξεις της* G *και* G'.

Συνήθως δεν κάνουμε διάκριση στο συμβολισμό των πράξεων και τις παραλείπουμε, δηλαδή γράφουμε απλώς

$$\phi(a\,b) \;=\; \phi(a)\,\phi(b).$$

Επίσης, όταν δεν υπάρχει περίπτωση σύγχυσης χρησιμοποιούμε κοινό συμβολισμό για τα ουδέτερα στοιχεία των G και G' συμβολίζοντάς τα με 1.

Αν ένας ομομορφισμός είναι $1-1$ τότε λέμε ότι είναι ***μονομορφισμός*** (σ' αυτή την περίπτωση λέμε ότι η G εμφυτεύεται στη G') και αν είναι επί τότε τον λέμε ***επιμορφισμό***. Ένας ***ισομορφισμός ομάδων*** είναι ένας ομομορφισμός που είναι $1-1$ και επί. Δύο ομάδες G και H καλούνται ***ισόμορφες*** αν υπάρχει ισομορφισμός $\phi : G \longrightarrow H$. Στην περίπτωση αυτή, γράφουμε $G \cong H$.

Την εικόνα $\mathrm{Im}\phi = \{\, \phi(g) \mid g \in G \,\}$ της ϕ τη λέμε ***ομομορφική εικόνα*** της G μέσω της ϕ και γι' αυτή συχνά χρησιμοποιείται ο συμβολισμός $\phi(G)$. Επειδή, για κάθε $g \in G$, ισχύει $\phi(g) = \phi(1g) = \phi(1)\phi(g)$ και $\phi(gg^{-1}) = \phi(g)\phi(g^{-1})$, έχουμε ότι

$$\phi(1) = 1 \;\;\text{και}\;\; \phi(g^{-1}) = \phi(g)^{-1}, \;\;\text{για κάθε}\;\; g \in G.$$

Από αυτό προκύπτει (επαγωγικά) ότι $\phi(g^n) = \phi(g)^n$ για κάθε $g \in G$ και $n \in \mathbb{N}$. Ειδικά αν n είναι η τάξη του g, τότε επειδή $\phi(g)^n = 1$, η τάξη του $\phi(g)$ διαιρεί το n (γιατί ;).

Προφανώς το υποσύνολο $\phi(G)$ είναι μια υποομάδα της G' και συνεπώς ένας ομομορφισμός $\phi : G \longrightarrow G'$ ορίζει πάντα τον επιμορφισμό $\phi : G \longrightarrow \phi(G)$. Γενικότερα, αν H είναι μια υποομάδα της G, τότε η εικόνα $\phi(H)$ της H είναι μια υποομάδα της $\phi(G)$ και ο περιορισμός $\phi|_H$ της ϕ στην H είναι ένας επιμορφισμός της H στην $\phi(H)$. Επίσης είναι φανερό ότι η δομή της $\phi(G)$ καθορίζεται πλήρως από τη δομή της G και τον ομομορφισμό ϕ. Πράγματι, ο υπολογισμός των γινομένων στην $\phi(G)$ μπορεί να γίνει αφού προηγουμένως υπολογίσουμε τα (γνωστά) γινόμενα στην G και κατόπιν μέσω της ϕ τα μεταφέρουμε στην

$\phi(G)$. Αντίθετα, η δομή της G δεν καθορίζεται πλήρως από αυτή της $\phi(G)$, διότι αν g' είναι ένα στοιχείο της $\phi(G)$, η αντίστροφη εικόνα του, δηλαδή το $\phi^{-1}(g') = \{\, h \in G \mid \phi(h) = g' \,\}$, είναι ένα υποσύνολο της G που περιέχει περισσότερα από ένα στοιχεία, εκτός αν η ϕ είναι μονομορφισμός. Συνεπώς για να μελετήσουμε τη δομή της G μέσω της δομής της $\phi(G)$ πρέπει να προσδιορίσουμε τις αντίστροφες εικόνες των στοιχείων της $\phi(G)$. Δηλαδή για ένα οποιοδήποτε στοιχείο $g' \in \phi(G)$ να προσδιορίσουμε τη μορφή των στοιχείων του υποσυνόλου $\phi^{-1}(g')$. Έστω $g \in \phi^{-1}(g')$, δηλαδή $\phi(g) = g'$. Τότε

$$\begin{aligned}\phi^{-1}(g') &= \{\, h \in G \mid \phi(h) = \phi(g) \,\} = \{\, h \in G \mid \phi(g^{-1}h) = 1 \,\} \\ &= \{\, h \in G \mid h = g\,k,\ \phi(k) = 1 \,\} = \{\, gk \in G \mid \phi(k) = 1 \,\}.\end{aligned}$$

Επομένως, είναι φανερό ότι το υποσύνολο $K = \{\, k \in G \mid \phi(k) = 1 \,\} = \phi^{-1}(1)$ της G είναι αυτό που καθορίζει την αντίστροφη εικόνα του $\phi(g)$, αφού αυτή αποτελείται από όλα τα γινόμενα της μορφής gk, $k \in K$. Παρατηρούμε τώρα ότι αυτό το υποσύνολο K είναι μια υποομάδα της G. Πράγματι, επειδή $\phi(1) = 1$ και $1 = \phi(k)^{-1} = \phi(k^{-1})$, $k \in K$, το $1 \in K$ και $k^{-1} \in K$, για κάθε $k \in K$. Επίσης αν $k_1, k_2 \in K$, τότε $\phi(k_1k_2) = \phi(k_1)\phi(k_2) = 1$ και άρα $k_1k_2 \in K$. Συνεπώς η αντίστροφη εικόνα $\phi^{-1}(\phi(g))$ του $\phi(g)$ είναι η αριστερή κλάση $\mathrm{mod}K$ που περιέχει το g, δηλαδή η gK. Είναι δε φανερό ότι η εικόνα $\phi(gK)$ του υποσυνόλου gK είναι το μονοσύνολο $\{\, \phi(g) \,\}$. Αυτό δείχνει ότι η αντιστοιχία

$$\phi(g) \longrightarrow \phi^{-1}(\phi(g)) = gK$$

μεταξύ της $\phi(G)$ και του αριστερού συνόλου πηλίκο $\{\, gK \mid g \in G \,\}$ είναι $1-1$ και επί απεικόνιση. Μπορούμε δε να γράψουμε την ανάλυση της G ως προς την K στη μορφή

$$G = \bigcup_{g' \in \phi(G)} \phi^{-1}(g').$$

Στα επόμενα την υποομάδα $K = \phi^{-1}(1)$ θα την λέμε ***πυρήνα*** του ομομορφισμού ϕ και θα την συμβολίζουμε με $\ker\phi$.

Συνεπώς ο ϕ είναι ένας μονομορφισμός ομάδων αν και μόνον αν ο πυρήνας του είναι η τετριμμένη υποομάδα της G. Φυσικά σ' αυτή την περίπτωση η δομή της $\phi(G)$ μας δίνει πλήρως την δομή της G (αφού $G \cong \phi(G)$). Αντίθετα, ο λεγόμενος τετριμμένος ομομορφισμός $\tau : G \longrightarrow G'$, $\tau(g) = 1$, για κάθε $g \in G$, δεν μας προσφέρει καμιά πληροφορία για τη δομή της G, αφού ο πυρήνας του είναι η ίδια η ομάδα G. Ας θεωρήσουμε τώρα την προσθετική ομάδα $\mathbb{R}^+$ των πραγματικών αριθμών και την αντιστοιχία $\phi : \mathbb{R}^+ \longrightarrow \mathbb{C}^*$, $\phi(r) = e^{2\pi ir}$, από την $\mathbb{R}^+$ στην πολλαπλασιαστική ομάδα των μη μηδενικών μιγαδικών αριθμών. Προφανώς η ϕ είναι μια απεικόνιση και επειδή $\phi(r_1 + r_2) = e^{2\pi i(r_1+r_2)} =$

$e^{2\pi i r_1}e^{2\pi i r_2} = \phi(r_1)\phi(r_2)$, η ϕ είναι ένας ομομορφισμός. Από τις ιδιότητες των μιγαδικών αριθμών προκύπτει ότι $\phi(\mathbb{R}^+) = \{\, z \mid |z| = 1 \,\} = S^1$ (η ομάδα του μοναδιαίου κύκλου) και $\ker\phi = \{\, r \in \mathbb{R}^+ \mid e^{2\pi i r} = 1 \,\} = \mathbb{Z}$. Συνεπώς έχουμε την $1-1$ αντιστοιχία $e^{2\pi i r} = \phi(r) \longleftrightarrow r + \mathbb{Z} = \phi^{-1}(e^{2\pi i r})$ και την ανάλυση της $\mathbb{R}^+$ ως προς την υποομάδα $\mathbb{Z}$

$$\mathbb{R}^+ = \bigcup_{z\in S^1} \phi^{-1}(z).$$

Ως ένα παράδειγμα ενός ομομορφισμού μη-Αβελιανών ομάδων, θεωρούμε τη διεδρική ομάδα D_6. Αυτή παράγεται από δύο στοιχεία x και y, τέτοια ώστε $x^6 = y^2 = (yx)^2 = 1$. Έχουμε δε

$$D_6 = \{\, 1,\, x,\, x^2,\, x^3,\, x^4,\, x^5,\, y,\, yx,\, yx^2,\, yx^3,\, yx^4,\, yx^5 \,\}.$$

Μπορούμε εύκολα να ελέγξουμε ότι η αντιστοιχία $f : D_6 \longrightarrow S_3$ με

$$\begin{aligned}
&f(1) = f(x^3) = i, && f(x) = f(x^4) = (1\,2\,3)\\
&f(x^2) = f(x^5) = (1\,3\,2) && f(y) = f(yx^3) = (1\,2)\\
&f((yx) = f(yx^4) = (2\,3), && f(yx^2) = f(yx^5) = (1\,3),
\end{aligned}$$

είναι ένας επιμορφισμός ομάδων που ο πυρήνας του είναι η υποομάδα $\{\, 1, x^3 \,\}$ της D_6. Συνεπώς έχουμε:

$$\begin{aligned}
&f^{-1}(i) = \{\, 1,\, x^3 \,\}, && f^{-1}(1\,2\,3) = \{\, x,\, x^4 \,\} = xf^{-1}(i),\\
&f^{-1}(1\,3\,2) = \{\, x^2,\, x^5 \,\} = x^2 f^{-1}(i), && f^{-1}(1\,2) = \{\, y,\, yx^3 \,\} = yf^{-1}(i),\\
&f^{-1}(2\,3) = \{\, yx,\, yx^4 \,\} = yxf^{-1}(i) \quad \text{και} && f^{-1}(1\,3) = \{\, yx^2,\, yx^5 \,\} = yx^2 f^{-1}(i).
\end{aligned}$$

Άρα $D_6 = f^{-1}(i) \cup f^{-1}(1\,2\,3) \cup f^{-1}(1\,3\,2) \cup f^{-1}(1\,2) \cup f^{-1}(1\,3) \cup f^{-1}(2\,3)$.

Τώρα με βάση αυτά που προαναφέραμε αποδεικνύουμε ένα θεώρημα ανάλογο του θεωρήματος του Lagrange που αφορά τις τάξεις και τους δείκτες των ομομορφικών εικόνων των υποομάδων μιας πεπερασμένης ομάδας G.

4.5.2 Θεώρημα. *Έστω G μια πεπερασμένη ομάδα και $\phi : G \longrightarrow G'$ ένας ομομορφισμός ομάδων. Τότε για κάθε υποομάδα H της G, η τάξη της εικόνας $\phi(H)$ της H διαιρεί την τάξη της H και ο δείκτης της $\phi(H)$ στην $\phi(G)$ διαιρεί το δείκτη της H στην G. Συγκεκριμένα ισχύει*

$$|H| = |\phi(H)|\,|\ker\phi_H| \quad \textit{και} \quad |G : H| = |\phi(G) : \phi(H)|\,|\ker\phi : \ker\phi_H|$$

όπου ϕ_H συμβολίζει τον περιορισμό του ϕ στην H.

Απόδειξη. Έστω $H \leq G$. Θεωρούμε τον περιορισμό $\phi_H = \phi_{|H} : H \longrightarrow G'$ που είναι ένας ομομορφισμός με πυρήνα $\ker \phi_H = H \cap \ker \phi$ (γιατί;). Συνεπώς, όπως είδαμε πριν, υπάρχει $1-1$ και επί αντιστοιχία μεταξύ των στοιχείων της υποομάδας $\phi_H(H)$ της G' και των κλάσεων $h \ker \phi_H,\ h \in H$. Επιπλέον έχουμε

$$H = \bigcup_{h' \in \phi(H)} \phi_H^{-1}(h'),$$

όπου $h' = \phi_H(h)$, για κάποιο $h \in H$ και $\phi_H^{-1}(h') = h \ker \phi_H$. Συνεπώς, όπως και στο θεώρημα του Lagrange, επειδή $|\ker \phi_H| = |h \ker \phi_H|$, για κάθε $h \in H$, προκύπτει ότι

$$|H| = |\ker \phi_H|\ |\phi(H)|.$$

Ειδικά έχουμε

$$|G| = |\phi(G)|\ |\ker \phi|,$$

και από αυτή τη σχέση παίρνουμε

$$\begin{aligned} |G| &= |\phi(H)|\ |\phi(G) : \phi(H)|\ |\ker \phi_H|\ |\ker \phi : \ker \phi_H| \\ &= |H|\ |\phi(G) : \phi(H)|\ |\ker \phi : \ker \phi_H|. \end{aligned}$$

Οπότε $\quad |G : H| = |\phi(G) : \phi(H)|\ |\ker \phi : \ker \phi_H|.$ ⊤

4.5.3 Πόρισμα. *Αν η G είναι πεπερασμένη, τότε η τάξη της διαιρείται από τις τάξεις των ομομορφικών εικόνων της.*

Απόδειξη. Αυτό προκύπτει άμεσα από το Θεώρημα 4.5.2. ⊤

4.5.4 Παρατήρηση. Αναφέρθηκε προηγουμένως ότι η τάξη της εικόνας $\phi(g)$ ενός στοιχείου g της G διαιρεί την τάξη του g. Το Θεώρημα 4.5.2 είναι ακριβώς η γενίκευση αυτής της επισήμανσης.

4.5.5 Πόρισμα. *Έστω ότι G, H και ϕ είναι όπως στο Θεώρημα 4.5.2. Τότε η τάξη $|\phi(H)|$ της H διαιρεί τον μ.κ.δ.$(|H|, |\phi(G)|)$ και ο δείκτης $|\phi(G) : \phi(H)|$ της H στη G διαιρεί τον μ.κ.δ.$(|G : H|, |\phi(G)|)$. Ειδικά αν μ.κ.δ.$(|H|, |\phi(G)|) = 1$ τότε $H \leq \ker \phi$.*

Απόδειξη. Αυτό προκύπτει από το θεώρημα του Lagrange και το Θεώρημα 4.5.2. Αν μ.κ.δ.$(|H|, |\phi(G)|) = 1$, τότε $\phi(H) = \{\, 1 \,\}$ και άρα $H \leq \ker \phi$. ⊤

4.5.6 Πόρισμα. *Αν G και G' είναι δύο πεπερασμένες ομάδες των οποίων οι τάξεις είναι πρώτες μεταξύ τους τότε εκτός από τον τετριμμένο ομομορφισμό δεν υπάρχει άλλος ομομορφισμός από την G στην G'.*

Απόδειξη. Αν $\phi : G \longrightarrow G'$ είναι ένας ομομορφισμός, τότε η τάξη $|\phi(G)|$ διαιρεί τον μ.κ.δ.$(|G|, |G'|) = 1$ και άρα $|\phi(G)| = 1$. ⊤

4.5.7 Πρόταση. *Έστω X ένα σύνολο γεννητόρων μιας ομάδας G. Τότε*

α) $\phi(G) = \langle\, \phi(X)\,\rangle$, για κάθε ομομορφισμό ομάδων $\phi : G \longrightarrow G'$.

β) Δύο ομομορφισμοί ϕ_1 και ϕ_2 από την G σε μια ομάδα G' συμπίπτουν στο X αν και μόνον αν συμπίπτουν σε όλη τη G, δηλαδή

$$\phi_1(x) = \phi_2(x) \quad \textit{για κάθε} \quad x \in X \Longleftrightarrow \phi_1 = \phi_2\,.$$

Απόδειξη. α) Κάθε στοιχείο $g \in G$ γράφεται ως γινόμενο $g = x_{i_1}^{n_1} \cdots x_{i_k}^{n_k}$, για κάποια $x_{i_j} \in X$ και $n_j \in \mathbb{Z}$, $j = 1, \ldots, k$. Συνεπώς, επειδή κάθε στοιχείο $g' \in \phi(G)$ είναι της μορφής $g' = \phi(g)$, για κάποιο $g \in G$ θα έχουμε $g' = \phi(x_{i_1})^{n_1} \cdots$
$\phi(x_{i_k})^{n_k}$. Άρα $\phi(G) = \langle\, \phi(X)\,\rangle$.

β) Έστω $g \in G$. Όπως πριν έχουμε $g = x_{i_1}^{n_1} \cdots x_{i_k}^{n_k}$. Άρα $\phi_1(g) = \phi_1(x_{i_1})^{n_1} \cdots \phi_1(x_{i_k})^{n_k} = \phi_2(x_{i_1})^{n_1} \cdots \phi_2(x_{i_k})^{n_k} = \phi_2(g)$. Από αυτό προκύπτει το ζητούμενο. ⊤

Περισσότερες ενδιαφέρουσες ιδιότητες των ομομορφισμών ομάδων θα μελετηθούν στην επόμενη παράγραφο. Τώρα δίνουμε μερικά χρήσιμα παραδείγματα και εφαρμογές των αποτελεσμάτων που αναπτύχτησαν σ' αυτή την παράγραφο.

4.5.8 Παραδείγματα και Εφαρμογές.

1. *Ομομορφισμοί Δακτυλίων.*

   Έστω $\phi : R \longrightarrow R'$ ένας ομομορφισμός από το δακτύλιο R στο δακτύλιο R'. Υποθέτουμε ότι οι δακτύλιοι R και R' έχουν μονάδες 1_R και $1_{R'}$ αντιστοιχα και ισχύει $\phi(1_R) = 1_{R'}$. Τότε ο ϕ είναι αφενός ένας ομομορφισμός της προσθετικής ομάδας του R στην αντίστοιχη του R' και αφετέρου ένας ομομορφισμός της πολλαπλασιαστικής ομάδας $U(R)$ των αντιστρέψιμων στοιχείων του R στην αντίστοιχη $U(R')$. Για τις προσθετικές ομάδες, ο πυρήνας του ϕ είναι το υποσύνολο $\{\, r \in R \mid \phi(r) = 0\,\}$ ενώ ο πυρήνας του ϕ θεωρούμενου ως ομομορφισμού μεταξύ των πολλαπλασιαστικών ομάδων $U(R)$ και $U(R')$ είναι το υποσύνολο $\{\, r \in U(R) \mid \phi(r) = 1\,\}$.

2. *Γραμμικές Απεικονίσεις.*

   Έστω V και W δύο διανυσματικοί χώροι, επί ενός σώματος F, διαστάσεων n και m αντίστοιχα. Μια γραμμική απεικόνιση είναι ένας ομομορφισμός

$T : V \longrightarrow W$ της προσθετικής ομάδας V στην προσθετική ομάδα W που επιπλέον ικανοποιεί τη συνθήκη

$$T(\lambda v) = \lambda T(v), \quad v \in V, \quad \lambda \in F.$$

Ο πυρήνας K του T είναι η αντίστροφη εικόνα $T^{-1}(0_W) = \{\, k \in V \mid T(k) = 0_W \,\}$, όπου 0_W είναι το μηδενικό διάνυσμα του W. Γενικά αν $w \in W$, τότε $T^{-1}(w) = v + K = \{\, v + k \mid k \in K \,\}$, όπου $v \in V$ είναι ένα διάνυσμα με $T(v) = w$.

Αν θεωρήσουμε τα στοιχεία του V (αντίστοιχα του W) ως διανύσματα στήλες με συντεταγμένες που ορίζονται από μια βάση του V (αντίστοιχα μια βάση του W) και αν A είναι ο πίνακας που αντιστοιχεί στον T ως προς αυτές τις βάσεις, τότε το σύνολο των λύσεων του συστήματος $AX = 0_W$ είναι ακριβώς ο πυρήνας K του T. Το δε σύνολο των λύσεων του συστήματος $AX = b$ είναι η κλάση $v + K$ όπου v είναι μια λύση του συστήματος.

3. *Η Παράγωγος Απεικόνιση.*

Έστω $\mathbb{R}[x]$ η προσθετική ομάδα του δακτυλίου των πολυωνύμων μιας μεταβλητής με συντελεστές πραγματικούς αριθμούς. Η απεικόνιση $d : \mathbb{R}[x] \longrightarrow \mathbb{R}[x]$, $d(f(x)) = f'(x)$, όπου $f'(x)$ είναι η παράγωγος του $f(x)$ είναι ένας ομομορφισμός της $\mathbb{R}[x]$ στον εαυτό της. Επειδή τα πολυώνυμα που έχουν παράγωγο μηδέν είναι τα σταθερά πολυώνυμα, έχουμε $\ker d = \mathbb{R}$. Συνεπώς η αντίστροφη εικόνα ενός πολυώνυμου $g(x)$ μέσω της d είναι η κλάση $\mathrm{mod}\mathbb{R}$, $d^{-1}(g(x)) = f(x) + \mathbb{R}$, όπου $f(x) = \int g(x)dx$ είναι μια "παράγουσα" της $g(x)$.

4. *Η Οριζουσιακή Απεικόνιση.*

Έστω $M_n(\mathbb{F})$ το σύνολο των $n \times n$ πινάκων με στοιχεία από το σώμα $\mathbb{F}$. Γνωρίζουμε ότι το $M_n(\mathbb{F})$ είναι ένας δακτύλιος επί του οποίου ορίζεται η οριζουσιακή απεικόνιση $\det : M_n(\mathbb{F}) \longrightarrow \mathbb{F}$, όπου $\det(A)$ είναι η ορίζουσα του πίνακα $A \in M_n(\mathbb{F})$, (για τον υπολογισμό της $\det A$ βλέπε επόμενο παράδειγμα). Είναι γνωστό ότι γενικά δεν ισχύει $\det(A + B) = \det(A) + \det(B)$, δηλαδή η det δεν είναι ένας ομομορφισμός της προσθετικής ομάδας του $M_n(\mathbb{F})$. Αλλά είναι γνωστό ότι $\det(AB) = \det(A)\det(B)$. Συνεπώς, αν θεωρήσουμε την πολλαπλασιαστική ομάδα των αντιστρέψιμων πινάκων, δηλαδή την γενική γραμμική ομάδα $GL_n(\mathbb{F})$, τότε ο περιορισμός της det σ' αυτή την ομάδα είναι ένας ομομορφισμός της $GL_n(\mathbb{F})$ στην πολλαπλασιαστική ομάδα $\mathbb{F}^*$ του σώματος $\mathbb{F}$. Επειδή δε για $r \in \mathbb{F}^*$, ο πίνακας

$A = \begin{pmatrix} r & & 0 \\ & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ έχει ορίζουσα r, ο ομομορφισμός det είναι ένας επιμορφισμός. Ο πυρήνας του ομομορφισμού det είναι η ειδική γραμμική ομάδα $\ker\det = \{\, S \in GL_n(\mathbb{F}) \mid \det(S) = 1 \,\} = SL_n(\mathbb{F})$. Η αντίστροφη εικόνα του r είναι η κλάση $\det^{-1}(r) = \begin{pmatrix} r & & 0 \\ & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix} SL_n(\mathbb{F})$ και άρα έχουμε

$$GL_n(\mathbb{F}) = \bigcup_{r\in\mathbb{F}^*} \det{}^{-1}(r) = \bigcup_{r\in\mathbb{F}^*} \begin{pmatrix} r & & \\ & 1 & \\ & \ddots & \\ & & 1 \end{pmatrix} SL_n(\mathbb{F}).$$

Αυτό σημαίνει ότι κάθε αντιστρέψιμος πίνακας $B \in GL_n(\mathbb{F})$ γράφεται μοναδικά στη μορφή $B = \begin{pmatrix} r & & \\ & 1 & \\ & \ddots & \\ & & 1 \end{pmatrix} S$, όπου $\det S = 1$ και $\det B = r$.

Παρατηρούμε επίσης ότι το σύνολο $L = \left\{ \begin{pmatrix} r & & 0 \\ & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \mid r \in \mathbb{F}^* \right\}$ είναι μια υποομάδα της $GL_n(\mathbb{F})$ και ο περιορισμός $\det_{|L}$ του ομομορφισμού det στην L είναι ένας ισομορφισμός, δηλαδή $L \cong \mathbb{F}^*$. Πράγματι, για $r, t \in \mathbb{F}^*$ έχουμε

$$\begin{pmatrix} r & & 0 \\ & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \begin{pmatrix} t & & 0 \\ & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{-1} = \begin{pmatrix} rt^{-1} & & 0 \\ & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in L$$

και

$$\ker\det{}_{|L} = L \cap SL_n(\mathbb{F}) = \left\{ \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\}.$$

Συνεπώς έχουμε $GL_n(\mathbb{F}) = L \cdot SL_n(\mathbb{F})$. Αυτό είναι ένα παράδειγμα δύο υποομάδων μιας ομάδας που το γινόμενό τους είναι υποομάδα και φυσικά ισχύει $GL_n(\mathbb{F}) = \langle\, L,\, SL_n(\mathbb{F})\,\rangle = L{\cdot}SL_n(\mathbb{F}) = SL_n(\mathbb{F}){\cdot}L$, όπως έπεται και από το 4.4.16. Επισημαίνουμε εδώ ότι τα στοιχεία της L και της $SL_n(\mathbb{F})$ δεν αντιμετατίθενται αλλά η σχέση $L \cdot SL_n(\mathbb{F}) = SL_n(\mathbb{F}) \cdot L$ σημαίνει ότι για $A \in L$ και $S \in SL_n(\mathbb{F})$ υπάρχουν $A' \in L$ και $S' \in SL_n(\mathbb{F})$ τέτοια ώστε $AS = S'A'$. Στην προκειμένη περίπτωση όμως, λόγω της προηγούμενης ιδιότητας των οριζουσών, πρέπει $A = A'$. Ας επισημάνουμε επιπλέον ότι η L είναι ισόμορφη με το κέντρο Z της $GL_n(\mathbb{F})$ αφού και οι δύο είναι ισόμορφες με την $\mathbb{F}^*$ (βλέπε 4.4.5). Ισχύει δε $Z \cdot SL_n(\mathbb{F}) = SL_n(\mathbb{F}) \cdot Z$, αφού τα στοιχεία της Z αντιμετατίθενται μ' αυτά της $SL_n(\mathbb{F})$ (θα δούμε στην επόμενη παράγραφο ότι για κάθε υποομάδα H της $GL_n(\mathbb{F})$ ισχύει $H \cdot SL_n(\mathbb{F}) = SL_n(\mathbb{F}) \cdot H$). Αλλά γενικά η $Z \cap SL_n(\mathbb{F}) \neq \{\, I \,\}$. Επίσης αν το $\mathbb{F}$ δεν περιέχει τις n-οστές ρίζες όλων των στοιχείων του, τότε η $Z \cdot SL_n(\mathbb{F})$ είναι γνήσια υποομάδα της $GL_n(\mathbb{F})$ αφού αν r είναι η ορίζουσα ενός πίνακα της $Z \cdot SL_n(\mathbb{F})$, το r πρέπει να είναι η n-οστή δύναμη ενός στοιχείου $\lambda \in \mathbb{F}^*$. Έτσι, αν $\mathbb{F} = \mathbb{R}$, ο πίνακας $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ δεν ανήκει στην $Z \cdot SL_2(\mathbb{R})$, αφού δεν υπάρχει πραγματικός αριθμός που το τετράγωνό του να είναι -1.

Με αφορμή τα προηγούμενα, είναι ευκαιρία εδώ να υπολογίσουμε τις τάξεις της $GL_n(\mathbb{F})$ και της $SL_n(\mathbb{F})$, στην περίπτωση που το σώμα $\mathbb{F}$ είναι πεπερασμένο. Έστω $|\mathbb{F}| = q$. Τότε η ομάδα $GL_n(\mathbb{F})$ είναι πεπερασμένη και μπορούμε να υπολογίσουμε την τάξη της ως εξής. Ένας πίνακας $A \in M_n(\mathbb{F})$ ανήκει στην $GL_n(\mathbb{F})$ αν και μόνον αν οι στήλες του αποτελούν μία βάση του διανυσματικού χώρου $\mathbb{F}^n$. Συνεπώς η τάξη της $GL_n(\mathbb{F})$ είναι ίση με το πλήθος των βάσεων του $\mathbb{F}^n$. Έστω $\{\, e_1, \ldots, e_n \,\}$ μια βάση του $\mathbb{F}^n$. Μπορούμε να θεωρήσουμε ότι το e_1 είναι ένα οποιοδήποτε μη-μηδενικό διάνυσμα του $\mathbb{F}^n$. Συνεπώς, επειδή $|\mathbb{F}^n| = q^n$, το e_1 μπορεί να επιλεγεί με $q^n - 1$ τρόπους. Έστω e_1 ένα από αυτά τα $q^n - 1$ διανύσματα. Τότε τα μόνα διανύσματα που είναι γραμμικά εξαρτημένα από το e_1 είναι τα πολλαπλάσια του e_1, δηλαδή όλα τα διανύσματα λe_1, $\lambda \in \mathbb{F}$ που το πλήθος τους είναι q. Άρα το πλήθος των διανυσμάτων που είναι γραμμικά ανεξάρτητα από το e_1 ισούται με $q^n - q$. Έτσι, παίρνουμε συνολικά $(q^n - 1)(q^n - q)$ το πλήθος ζευγάρια διανυσμάτων που είναι γραμμικά ανεξάρτητα. Υποθέτουμε τώρα ότι το πλήθος των γραμμικά ανεξαρτήτων r διανυσμάτων είναι $(q^n - 1)(q^n - q) \cdots (q^n - q^{r-1})$, και έστω $e_1, e_2, \ldots, e_r$, r τέτοια διανύσματα. Τα διανύσματα της μορφής $\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_r e_r$, $\lambda_i \in \mathbb{F}$, είναι τα μόνα διανύσματα που είναι γραμμικά εξαρτημένα από τα $e_1, e_2, \ldots, e_r$.

Το πλήθος αυτών είναι q^r που είναι το πλήθος των r-αδων $(\lambda_1, \lambda_2, \ldots, \lambda_r)$, $\lambda_i \in \mathbb{F}$. Άρα το πλήθος των διανυσμάτων που είναι γραμμικά ανεξάρτητα από τα $e_1, e_2, \ldots, e_r$ είναι ίσο με $(q^n - q^r)$ και συνεπώς παίρνουμε συνολικά $(q^n-1)(q^n-q)\cdots(q^n-q^r)$ το πλήθος υποσύνολα $\{e_1, e_2, \ldots, e_{r+1}\}$ $r+1$ γραμμικά ανεξάρτητων διανυσμάτων. Επομένως τελικά έχουμε

$$\begin{aligned} |GL_n(\mathbb{F})| &= (q^n-1)(q^n-q)\cdots(q^n-q^{n-1}) \\ &= q^{\frac{n(n-1)}{2}}(q-1)(q^2-1)\cdots(q^n-1) \end{aligned}$$

και $$|SL_n(\mathbb{F})| = q^{\frac{n(n-1)}{2}}(q^2-1)\cdots(q^n-1),$$

αφού $\ker\det = SL_n(\mathbb{F})$ και από το Θεώρημα 4.5.2 έχουμε $|SL_n(\mathbb{F})| = |GL_n(\mathbb{F})|/|\mathbb{F}^*|$.

5. *Σύνθεση Ομομορφισμών.*

Έστω G_1, G_2 και G_3 τρεις ομάδες. Αν $\phi_1 : G_1 \longrightarrow G_2$, $\phi_2 : G_2 \longrightarrow G_3$ είναι ομομορφισμοί τότε η σύνθεσή τους $\phi_2 \circ \phi_1 : G_1 \longrightarrow G_3$ είναι ένας ομομορφισμός. Πράγματι,

$$\begin{aligned} (\phi_2 \circ \phi_1)(g_1g_2) &= \phi_2(\phi_1(g_1)\phi_1(g_2)) = \phi_2(\phi_1(g_1))\phi_2(\phi_1(g_2)) \\ &= (\phi_2 \circ \phi_1)(g_1) \cdot (\phi_2 \circ \phi_1)(g_2). \end{aligned}$$

Για τους αντίστοιχους πυρήνες και τις ομομορφικές εικόνες προκύπτει ότι

$$\ker\phi_1 \leq \ker\phi_2\circ\phi_1 \quad \text{και} \quad \mathrm{Im}(\phi_2\circ\phi_1) \leq \mathrm{Im}\phi_2.$$

Συνεπώς αν η σύνθεση $\phi_2 \circ \phi_1$ είναι μονομορφισμός τότε και ο ϕ_1 είναι μονομορφισμός. Αν ο $\phi_2 \circ \phi_1$ είναι επιμορφισμός τότε και ο ϕ_2 είναι το ίδιο.

6. *Πίνακες Μεταθέσεων*

Θεωρούμε έναν $n-$διάστατο διανυσματικό χώρο επί ενός σώματος K και μία βάση του $\{e_1, e_2, \ldots, e_n\}$ Για κάθε μετάθεση $\sigma \in S_n$ η απεικόνιση $e_i \longrightarrow e_{\sigma(i)}$, $i = 1, 2, \ldots, n$, επεκτείνεται μοναδικά σε μια γραμμική απεικόνιση του V στον εαυτό του, την οποία συμβολίζουμε με $M(\sigma)$. Για $\sigma_1, \sigma_2 \in S_n$ έχουμε $M(\sigma_1\sigma_2)(e_i) = e_{\sigma_1\sigma_2(i)} = M(\sigma_1)(e_{\sigma_2(i)}) = M(\sigma_1)(M(\sigma_2)(e_i)) = (M(\sigma_1)M(\sigma_2))(e_i)$, για κάθε $i = 1, 2, \ldots, n$. Άρα $M(\sigma_1\sigma_2) = M(\sigma_1)M(\sigma_2)$, αφού τα $e_1, e_2, \ldots, e_n$ είναι βάση του V. Επίσης καθώς τα διανύσματα $M(\sigma)(e_i)$, $i = 1, 2, \ldots, n$, αποτελούν βάση του V, η $M(\sigma)$ είναι αντιστρέψιμη απεικόνιση, ενώ η μόνη μετάθεση

σ για την οποία $M(\sigma) = 1_V$ είναι προφανώς η ταυτοτική i. Άρα η απεικόνιση $M : S_n \longrightarrow GL(V)$ με $\sigma \longrightarrow M(\sigma)$ είναι ένας μονομορφισμός ομάδων. Αν παραστήσουμε τις γραμμικές απεικονίσεις $M(\sigma), \quad \sigma \in S_n$ με πίνακες, ως προς τη βάση $\{e_1, e_2, \ldots, e_n\}$, τότε ο πίνακας $M(\sigma)$ είναι αυτός που όλα τα στοιχεία του σε κάθε γραμμή και κάθε στήλη είναι μηδέν εκτός από τα στοιχεία που βρίσκονται στις $(\sigma(i), i)$ θέσεις, για $i = 1, 2, \ldots, n$. Ο πίνακας $M(\sigma)$ καλείται ***πίνακας μετάθεση*** που αντιστοιχεί στην σ. Έτσι, αν ο V έχει διάσταση 3, τότε η ομάδα $Im\, M$ αποτελείται από τους πίνακες

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \text{ και } \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

7. *Το Πρόσημο Μετάθεσης.*

Η απεικόνιση $\pi : S_n \longrightarrow \{1, -1\}$, από τη συμμετρική ομαδα S_n στην πολλαπλασιαστική ομάδα $\{1, -1\}$, όπου

$$\pi(\sigma) = \begin{cases} 1 & \text{αν η } \sigma \text{ είναι άρτια} \\ -1 & \text{αν η } \sigma \text{ είναι περιττή} \end{cases}$$

είναι, σύμφωνα με το 4.4.12, ένας επιμορφισμός ομάδων. Ο πυρήνας $\ker \pi$ είναι η εναλλάσουσα υποομάδα A_n. Ο π λέγεται ***επιμορφισμός προσήμων*** των μεταθέσεων και η εικόνα $\pi(\sigma)$ της σ καλείται ***πρόσημο της*** σ.

Σαν μια πρώτη εφαρμογή του επιμορφισμού προσήμων των μεταθέσεων σε συνδυασμό με το Πόρισμα 4.5.4 θα δείξουμε ότι

> *"Κάθε ομάδα μεταθέσεων βαθμού n περιττής τάξης είναι υποομάδα της εναλλάσουσας ομάδας A_n".*

Πράγματι, έστω $H \leq S_n$. Καθώς $|\pi(S_n)| = 2$, από το Πόρισμα 4.5.5 έπεται ότι η τάξη $|\pi(H)|$ της εικόνας $\pi(H)$ πρέπει να διαιρεί τον μ.κ.δ.$(2, |H|)$. Αν η τάξη $|H|$ της H είναι περιττός αριθμός τότε $|\pi(H)| = 1$ και συνεπώς η H είναι υποομάδα του πυρήνα $\ker \pi = A_n$. Ειδικά, αυτό μας δηλώνει ότι "κάθε μετάθεση σ που η τάξη της είναι περιττή πρέπει να είναι άρτια

μετάθεση", αφού η υποομάδα που παράγεται από τη σ είναι περιττής τάξης. Συνεπώς κάθε περιττή μετάθεση είναι άρτιας τάξης.

Μια άλλη εφαρμογή του επιμορφισμού προσήμων είναι ο υπολογισμός της ορίζουσας ενός πίνακα. Στο παράδειγμα 6 θεωρήσαμε τον μονομορφισμό $M : S_n \longrightarrow GL_n(K), \sigma \longrightarrow M(\sigma)$, όπου $M(\sigma)$ είναι ο πίνακας μετάθεση που αντιστοιχεί στη μετάθεση σ. Αν σ είναι μια αντιμετάθεση $(i\, j)$, τότε ο πίνακας $M(\sigma)$ είναι αυτός που παίρνουμε από τόν ταυτοτικό πίνακα με εναλλαγή της i και j στήλης. Οπότε, από τις ιδιότητες των οριζουσών, η ορίζουσα $\det M(\sigma) = -1$. Συνεπώς, εκφράζοντας την σ ως ένα γινόμενο αντιμεταθέσεων, έστω $\sigma = \sigma_1\sigma_2 \cdots \sigma_k$, βλέπουμε ότι για την ορίζουσα του $M(\sigma)$ έχουμε

$$\begin{aligned}\det M(\sigma) &= \prod_{i=1}^{k} \det M(\sigma_i) \\ &= \begin{cases} 1 & \text{αν ο } k \text{ είναι άρτιος (δηλαδή } \sigma \text{ άρτια)} \\ -1 & \text{αν ο } k \text{ είναι περιττός (δηλαδή } \sigma \text{ περιττή)} \end{cases} = \pi(\sigma).\end{aligned}$$

Επομένως ο επιμορφισμός π είναι η σύνθεση $\det_{|\mathrm{Im}M} \circ M$ του M επί τον περιορισμό της ορίζουσας απεικόνισης $\det : GL_n(K) \longrightarrow K^*$ στην εικόνα $\mathrm{Im}M$.

Τώρα θα χρησιμοποιήσουμε το πρόσημο των μεταθέσεων για να δείξουμε ότι η ορίζουσα $\det A$ ενός $n \times n$ πίνακα $A = (\alpha_{ij})$ με στοιχεία α_{ij} από ένα σώμα K γράφεται στη μορφή

$$\det A = \sum_{\sigma \in S_n} \pi(\sigma) \prod_{i=1}^{n} \alpha_{\sigma_{(i),i}}.$$

Θεωρούμε τη γνωστή, από τη Γραμμική Άλγεβρα, ανάπτυξη της ορίζουσας ως προς τη j-στήλη:

$$\det A = \sum_{i=1}^{n} \alpha_{ij}\beta_{ij}$$

όπου $\beta_{ij} = (-1)^{i+j} \det A_{ij}$ και A_{ij} είναι ο $(n-1) \times (n-1)$ πίνακας που προκύπτει από τον A απαλείφοντας την i-γραμμή και j-στήλη.

Είναι φανερό ότι

$$\beta_{ij} = \det(s_1,\, s_2,\, \ldots,\, s_{j-1},\, e_i, s_{j+1},\, \ldots,\, s_n)$$

όπου s_k συμβολίζει την k-στήλη $\begin{pmatrix} \alpha_{1k} \\ \vdots \\ \alpha_{nk} \end{pmatrix}$ του πίνακα A και e_i συμβολίζει την i-στήλη του ταυτοτικού πίνακα I_n, (η οποία τοποθετείται στην j-στήλη του A). Συνεπώς, αναπτύσσοντας την ορίζουσα του A ως προς την πρώτη στήλη, έχουμε

$$\det A = \sum_{i_1=1}^{n} \alpha_{i_1 1}\beta_{i_1 1} = \sum_{i_1=1}^{n} \alpha_{i_1,1} \det(e_{i_1},\, s_2,\, s_3,\, \ldots,\, s_n).$$

Αναπτύσσουμε τώρα την ορίζουσα $\det(e_{i_1},\, s_2,\, \ldots,\, s_n)$ με τον ίδιο τρόπο ως προς τη δεύτερη στήλη και παίρνουμε

$$\det A = \sum_{i_1=1}^{n} \alpha_{i_1 1} \left(\sum_{i_2=1}^{n} \alpha_{i_2 2} \det(e_{i_1},\, e_{i_2},\, s_3, \ldots,\, s_n) \right).$$

Επαναλαμβάνοντας αυτή τη διαδικασία για όλες τις εν λόγω ορίζουσες, στο τέλος θα πάρουμε την έκφραση:

$$\begin{aligned} \det A &= \sum_{i_1=1}^{n} \cdots \sum_{i_n=1}^{n} \alpha_{i_1 1}\alpha_{i_2 2} \cdots \alpha_{i_n n} \det(e_{i_1},\, e_{i_2},\, \ldots,\, e_{i_n}) \\ &= \sum_{i_1, i_2, \ldots, i_n} \alpha_{i_1 1} \cdots \alpha_{i_n n} \det(e_{i_1},\, \ldots,\, e_{i_n}). \end{aligned}$$

Τώρα παρατηρούμε ότι αν στον πίνακα $(e_{i_1},\, e_{i_2},\, \ldots,\, e_{i_n})$ ανά δύο οι δείκτες $i_1,\, i_2,\, \ldots,\, i_n$ είναι διάφοροι τότε ο πίνακας αυτός είναι ο πίνακας μετάθεση $M(\sigma)$ που αντιστοιχεί στη μετάθεση

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}.$$

Όλες δε οι $n!$ τέτοιες επιλογές n-αδων $(i_1,\, \ldots,\, i_n)$ εμφανίζονται στο προηγούμενο άθροισμα. Επίσης σ' αυτό το άθροισμα, αν σε μια n-αδα δεικτών $(i_1,\, \ldots,\, i_n)$ δύο ή περισσότεροι δείκτες είναι ίσοι, με άλλα λόγια μια ή περισσότερες στήλες του πίνακα είναι ίσες, τότε η ορίζουσα αυτή είναι μηδέν. Επομένως τελικά έχουμε

$$\det A = \sum_{\sigma \in S_n} \alpha_{\sigma(1),1}\alpha_{\sigma(2),2} \cdots \alpha_{\sigma(n),n} \det M(\sigma) = \sum_{\sigma \in S_n} \pi(\sigma) \prod_{i=1}^{n} \alpha_{\sigma(i),i}.$$

8. *Η Ομομορφική Εικόνα των Ακεραίων.*

Από την ιδιότητα $g^m g^n = g^{m+n}$ των δυνάμεων ενός στοιχείου g μιας ομάδας G, προκύπτει ότι αν $H = \langle\, g \,\rangle = \{\, g^n \mid n \in \mathbb{Z} \,\}$ είναι η υποομάδα που παράγεται από το στοιχείο g, τότε η απεικόνιση $\phi : \mathbb{Z} \longrightarrow G,\ n \longrightarrow g^n$ είναι ένας ομομορφισμός, καθώς $\phi(m+n) = g^{m+n} = g^m g^n = \phi(m)\phi(n)$. Ισχύει δε $\mathrm{Im}\phi = H$ και

$$\ker\phi = \begin{cases} \{\, 0 \,\} & \text{αν η τάξη του } \ g \ \text{ είναι άπειρη} \\ r\mathbb{Z} & \text{αν η τάξη του } \ g \ \text{ είναι πεπερασμένη ίση με } \ r. \end{cases}$$

Ως ειδική περίπτωση του παραδείγματος αυτού, παίρνουμε τη γνωστή απεικόνιση $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_r$, $n \longrightarrow n \bmod r$, που είναι ένας επιμορφισμός με πυρήνα την υποομάδα $r\mathbb{Z}$ του $\mathbb{Z}$.

9. *Ο Ομομορφισμός $GL_n(\mathbb{Z}) \longrightarrow GL_n(\mathbb{Z}_p)$.*

Στο προηγούμενο παράδειγμα θεωρήσαμε τον επιμορφισμό $\phi : \mathbb{Z} \to \mathbb{Z}_r$, $n \to n \bmod r$. Αν το r είναι ένας πρώτος αριθμός p τότε αυτός ο επιμορφισμός ορίζει τον εξής ομομορφισμό της ομάδας $GL_n(\mathbb{Z})$ στην ομάδα $GL_n(\mathbb{Z}_p)$. Σε κάθε $n \times n$ πίνακα $A = (\,\alpha_{ij}\,)$, $\alpha_{ij} \in \mathbb{Z}$, με $\det A = \pm 1$, αντιστοιχούμε τον πίνακα $(\phi(\alpha_{ij}))$, όπου $\phi(\alpha_{ij}) = \alpha_{ij} \bmod p$. Τον πίνακα $(\phi(\alpha_{ij}))$ τον συμβολίζουμε με $\phi(A)$ Επειδή έχουμε

$$\det A = \sum_{\sigma \in S_n} \pi(\sigma) \prod_{i=1}^{n} \alpha_{\sigma(i),i} = \pm 1$$

(δες προηγούμενο παράδειγμα 5), επίσης έχουμε και

$$\begin{aligned} \det \phi(A) = \sum_{\sigma \in S_n} \pi(\sigma) \prod_{i=1}^{n} \phi(\alpha_{\sigma(i),i}) = \phi\left(\sum_{\sigma \in S_n} \pi(\sigma) \prod_{i=1}^{n} \alpha_{\sigma(i),i} \right) \\ = \phi(\pm 1) = \pm 1 \bmod p. \end{aligned}$$

Συνεπώς η αντιστοιχία $A \longrightarrow \phi(A)$ είναι μια αντιστοιχία της $GL_n(\mathbb{Z})$ στην $GL_n(\mathbb{Z}_p)$ και είναι φανερό ότι αυτή είναι μια απεικόνιση (που δεν είναι επί). Επιπλέον καθώς ο $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_p$ είναι και επιμορφισμός δακτυλίων, από τον ορισμό του γινομένου πινάκων, εύκολα προκύπτει ότι η απεικόνιση $A \longrightarrow \phi(A)$, που στο εξής θα την συμβολίζουμε πάλι με ϕ διατηρεί τον πολλαπλασιασμό πινάκων. Δηλαδή ισχύει $\phi(AB) = \phi(A)\phi(B)$ για κάθε $A, B \in GL_n(\mathbb{Z})$. Άρα η ϕ είναι ένας ομομορφισμός της $GL_n(\mathbb{Z})$ στην $GL_n(\mathbb{Z}_p)$. Με βάση αυτόν τον ομομορφισμό αποδεικνύουμε τώρα το εξής ενδιαφέρον αποτέλεσμα.

"Για κάθε $n \in \mathbb{N}$, το πλήθος των μη ισόμορφων πεπερασμένων υποομάδων της $GL_n(\mathbb{Z})$ είναι πεπερασμένο".

Πράγματι, θεωρούμε τον πυρήνα $\ker\phi$ της $\phi : GL_n(\mathbb{Z}) \longrightarrow GL_n(\mathbb{Z}_p)$. Αυτός αποτελείται από όλους τους πίνακες $A = (\alpha_{ij}) \in GL_n(\mathbb{Z})$ για τους οποίους $\phi(A) = I_n$. Αυτό σημαίνει ότι $\alpha_{ii} \equiv 1 \bmod p$, $i = 1, 2, \ldots, n$, και $\alpha_{ij} \equiv 0 \bmod p$, για $1 \leq i \neq j \leq n$. Δηλαδή ο A έχει τη μορφή $A = I_n + pA'$, για κάποιον $A' \in M_n(\mathbb{Z})$. Ισχυριζόμαστε ότι αν H είναι μια πεπερασμένη υποομάδα της $GL_n(\mathbb{Z})$ τότε, για $p \neq 2$, η τομή $H \cap \ker\phi = \{ I_n \}$ και συνεπώς η H είναι ισόμορφη με την εικόνα της $\phi(H)$ (γιατί;). Για το σκοπό αυτό, αρκεί να δείξουμε ότι όλα τα στοιχεία του $\ker\phi$, εκτός από τον ταυτοτικό πίνακα I_n, έχουν άπειρη τάξη. Υποθέτοντας το αντίθετο, έστω $A \in \ker\phi$ με $A^m = I_n$, για κάποιον θετικό ακέραιο m. Μπορούμε να εκφράσουμε τον πίνακα A στη μορφή $A = I_n + p^k A'$, για κάποιον θετικό ακέραιο k και κάποιον πίνακα $A' = (\alpha'_{ij}) \in M_n(\mathbb{Z})$ με ένα τουλάχιστον από τα στοιχεία του α'_{ij} να μην είναι ισότιμο με το $0 \bmod p$. Από το διωνυμικό ανάπτυγμα για τους πίνακες, έχουμε

$$I_n = A^m = (I_n + p^k A')^m = \sum_{i=0}^{m} \binom{m}{i} p^{ki} A'^i = I_n + \sum_{i=1}^{m} \binom{m}{i} p^{ki} A'^i$$

και επομένως

$$\sum_{i=2}^{m} \binom{m}{i} p^{ki} A'^i = -mp^k A'.$$

Αυτό είναι αδύνατο να ισχύει αφού όλοι οι όροι του αθροίσματος διαιρούνται από μια δύναμη του p που είναι μεγαλύτερη από αυτή που διαιρεί τον mp^k (γιατί;). Συνεπώς $H \cap \ker\phi = \{ I_n \}$ και άρα $H \cong \phi(H)$. Καθώς η ομάδα $GL_n(\mathbb{Z}_p)$ είναι πεπερασμένη, το πλήθος των υποομάδων της είναι φυσικά πεπερασμένο. Άρα, πρέπει να υπάρχει πεπερασμένο πλήθος μη ισόμορφων πεπερασμένων υποομάδων της $GL_n(\mathbb{Z})$.

Αναφέρουμε πληροφοριακά ότι οι κλάσεις ισομορφίας των πεπερασμένων υποομάδων της $GL_2(\mathbb{Z})$ και $GL_3(\mathbb{Z})$ έχουν ταξινομηθεί και παίζουν σημαντικό ρόλο στην κρυσταλλογραφία. Υπάρχουν 10 τέτοιες κλάσεις για την $GL_2(\mathbb{Z})$ και 32 για την $GL_3(\mathbb{Z})$ (δες το βιβλίο του P. Yale *"Geometry and Symmetry"* [33] ή το βιβλίο του H.S.M. Coxeter, *"Introduction to Geometry"* [7]).

10. *Η Ομάδα Αυτομορφισμών μιας Ομάδας.*

Ένας αυτομορφισμός μιας ομάδας G είναι μια μετάθεση του συνόλου G που ταυτόχρονα είναι και ομομορφισμός. Το υποσύνολο της συμμετρικής

ομάδας S_G του συνόλου G που είναι αυτομορφισμοί της ομάδας G θα το συμβολίζουμε με $Aut(G)$. Ένα στοιχείο του $Aut(G)$ είναι η ταυτοτική απεικόνιση $1_G : G \longrightarrow G$ και αν $\alpha_1, \alpha_2 \in Aut(G)$, τότε $\alpha_1\alpha_2^{-1} \in Aut(G)$ (γιατί;). Άρα το σύνολο $AutG$ είναι μια ομάδα μεταθέσεων του συνόλου G που ονομάζεται η ***ομάδα αυτομορφισμών της G***. Αυτή η ομάδα δίνει χρήσιμες πληροφορίες για τη δομή της G. Για παράδειγμα, ιδιαίτερο ενδιαφέρον παρουσιάζουν οι λεγόμενοι ***εσωτερικοί αυτομορφισμοί*** που ορίζονται ως εξής: Για $g \in G$ ορίζουμε την απεικόνιση

$$\tau_g : G \longrightarrow G, \;\; x \longrightarrow gxg^{-1}.$$

Καθώς $\tau_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \tau_g(x)\tau_g(y)$ και $\tau_g\tau_{g^{-1}} = \tau_{g^{-1}}\tau_g = 1_G$, προκύπτει ότι $\tau_g \in Aut(G)$. Για δύο στοιχεία $g_1, g_2 \in G$, έχουμε $(\tau_{g_1}\tau_{g_2})(x) = g_1g_2xg_2^{-1}g_1^{-1} = g_1g_2x(g_1g_2)^{-1} = \tau_{g_1g_2}(x)$ για κάθε $x \in G$ και άρα $\tau_{g_1}\tau_{g_2} = \tau_{g_1g_2}$. Είναι φανερό ότι το υποσύνολο $InnG$ όλων των εσωτερικών αυτομορφισμών της G είναι μια υποομάδα της $AutG$.

Ας προσδιορίσουμε εδώ την ομάδα αυτομορφισμών των γνωστών ομάδων S_3, $\mathbb{Q}^+$ και της ομάδας K_4 του Klein.

(α′) $Aut(S_3)$: Η S_3 έχει 6 στοιχεία, την ταυτοτική μετάθεση i, δύο στοιχεία α, β τάξης 3 και τρία στοιχεία $\gamma, \delta, \varepsilon$ τάξης 2. Ένας αυτομορφισμός μιας ομάδας διατηρεί την τάξη των στοιχείων (γιατί;). Συνεπώς ένας αυτομορφισμός της S_3 μεταθέτει ξεχωριστά τα στοιχεία α, β και ξεχωριστά τα τρία στοιχεία $\gamma, \delta, \varepsilon$. Καθώς τα στοιχεία $\gamma, \delta, \varepsilon$ παράγουν την ομάδα S_3, ένας αυτομορφισμός καθορίζεται πλήρως από την μετάθεση που αυτός επάγει στα τρία στοιχεία $\gamma, \delta, \varepsilon$. Αντίστροφα, αν σ είναι μια μετάθεση των $\gamma, \delta, \varepsilon$ τότε ορίζοντας την απεικόνιση $\phi : S_3 \longrightarrow S_3$ με $\phi(i) = i$, $\phi(\alpha) = \sigma(\gamma)\,\sigma(\delta)$, $\phi(\beta) = \sigma(\gamma)\,\sigma(\varepsilon)$ και $\phi(\gamma) = \sigma(\gamma)$, $\phi(\delta) = \sigma(\delta)$, $\phi(\varepsilon) = \sigma(\varepsilon)$, αυτή είναι ένας αυτομορφισμός της S_3. Άρα $Aut(S_3) \cong S_3$. Επίσης εύκολα προκύπτει ότι $Inn(S_3) = Aut(S_3)$.

(β′) $Aut(\,\mathbb{Q}^+\,)$: Έστω ϑ ένας αυτομορφισμός της $\mathbb{Q}^+$. Η εικόνα της μονάδας μέσω του ϑ είναι ένας μη μηδενικός ρητός αριθμός, έστω $\vartheta\,(\,1\,) = \kappa/\lambda$. Έστω το κλάσμα $1/s$, με $s \neq 0$. Τότε έχουμε $\vartheta\,(\,1/s\,) = \kappa/(s \cdot \lambda)$. Πράγματι επειδή ο ϑ είναι αυτομορφισμός, θα είναι

$$\underbrace{\vartheta\,(\,1/s\,) + \cdots + \vartheta\,(\,1/s\,)}_{s} = \vartheta\,(\,\underbrace{1/s + \cdots + 1/s}_{s}\,) = \vartheta\,(\,1\,) = \kappa/\lambda,$$

οπότε αναγκαστικά $\vartheta\,(\,1/s\,) = \kappa/(s\cdot\lambda)$. Επομένως, πάλι επειδή ο ϑ διατηρεί την πρόσθεση, η εικόνα του τυχαίου κλάσματος r/s μέσω του ϑ είναι $\vartheta\,(\,r/s\,) = (r/s)\cdot(\kappa/\lambda)$. Δηλαδή αποδείξαμε ότι ο αυτομορφισμός ϑ είναι πλήρως καθορισμένος από την εικόνα του 1.
Αντίστροφα δεν είναι δύσκολο να αποδείξουμε ότι αν κ/λ είναι ένας τυχαίος μη μηδενικός ρητός αριθμός τότε η απεικόνιση $\vartheta : \mathbb{Q} \longrightarrow \mathbb{Q}$ με $\vartheta(\,r/s\,) = (r/s)\cdot(\kappa/\lambda)$ ορίζει έναν αυτομορφισμό της $(\,\mathbb{Q}, +\,)$ με $\vartheta(\,1\,) = \kappa/\lambda$. Από τα προηγούμενα έπεται ότι η απεικόνιση $f : Aut(\,\mathbb{Q}, +\,) \longrightarrow (\,\mathbb{Q}^*, \cdot\,)$ με $f(\,\vartheta\,) = \vartheta(\,1\,)$ είναι 1 - 1 και επί. Επιπλέον η f είναι ένας ομομορφισμός ομάδων δηλαδή $f(\,\vartheta_1\circ\vartheta_2\,) = (\,\vartheta_1\circ\vartheta_2\,)(\,1\,) = \vartheta_1(\,1\,)\cdot\vartheta_2(\,1\,) = f(\,\vartheta_1\,)\cdot f(\,\vartheta_2\,)$ (γιατί;). Άρα η f είναι ένας ισομορφισμός μεταξύ της ομάδας αυτομορφισμών της προσθετικής ομάδας των ρητών και της πολλαπλασιαστικής ομάδας των ρητών ($\,Aut(\,\mathbb{Q}, +\,) \cong (\,\mathbb{Q}^*, \cdot\,)\,$).

(γ') $Aut(K_4)$: Η ομάδα K_4 του Klein αποτελείται από τέσσερα στοιχεία, το ουδέτερο e και τα $a,\ b$ και c. Μεταξύ των $a,\ b,\ c$ ισχύουν οι σχέσεις $a\cdot b = b\cdot a = c,\ a\cdot c = c\cdot a = b$ και $b\cdot c = c\cdot b = a$. Έστω ϕ μια μετάθεση των τριών συμβόλων $a,\ b,\ c$, δηλαδή $\phi \in S_3$. Τότε, επειδή $\{\,\phi(a),\ \phi(b),\ \phi(c)\,\} = \{\,a,\ b,\ c\,\}$, μεταξύ των στοιχείων $\phi(a),\ \phi(b),\ \phi(c)$ ισχύουν ακριβώς οι παραπάνω σχέσεις. Δηλαδή η ϕ ορίζει έναν αυτομορφισμό της K_4 (θέτοντας $\phi(e) = e$). Οπότε στην πραγματικότητα έχουμε αποδείξει ότι $Aut(K_4) \cong S_3$, αφού κάθε αυτομορφισμός της K_4 μεταθέτει τα στοιχεία της K_4 (διατηρώντας το ουδέτερο στοιχείο e σταθερό).

Καθώς η φύση αυτών καθ' εαυτών των στοιχείων μιας ομάδας είναι δευτερεύουσας σημασίας στην Άλγεβρα, μπορούμε να θεωρούμε ότι δύο ομάδες ταυτίζονται αν αυτές είναι ισόμορφες. Θα πρέπει να παρατηρήσουμε ότι η έννοια της ισομορφίας ορίζει μια σχέση ισοδυναμίας μεταξύ όλων των ομάδων. Πράγματι, για κάθε ομάδα G, η ταυτοτική απεικόνιση $1_G : G \longrightarrow G,\quad x \longrightarrow x$ είναι ένας ισομορφιαμός, δηλαδή πάντα ισχύει $G \cong G$. Αν $f : G_1 \longrightarrow G_2$ είναι ένας ισομορφισμός από την ομάδα G_1 στην ομάδα G_2, τότε ορίζεται η αντίστροφη απεικόνιση $f^{-1} : G_2 \longrightarrow G_1$ που είναι και αυτή ισομορφισμός (γιατί;). Δηλαδή αν $G_1 \cong G_2$ τότε $G_2 \cong G_1$. Επιπλέον αν $f_1 : G_1 \longrightarrow G_2$ και $f_2 : G_2 \longrightarrow G_3$ είναι ισομορφισμοί ομάδων, τότε και η σύνθεση $f_2\,f_1 : G_1 \longrightarrow G_3$ είναι ένας ισομορφισμός ομάδων, δηλαδή αν $G_1 \cong G_2$ και $G_2 \cong G_3$ τότε $G_1 \cong G_3$.

4.5.9 Παραδείγματα μη-ισόμορφων ομάδων.

1. Η προσθετική ομάδα των ρητών $\mathbb{Q}^+$ δεν είναι ισόμορφη με την προσθετική ομάδα των πραγματικών αριθμών, αφού το σύνολο των ρητών είναι

αριθμήσιμο ενώ το σύνολο των πραγματικών αριθμών είναι μη αριθμήσιμο.

2. Η ομάδα των ακεραίων αριθμών δεν ειναι ισόμορφη με την προσθετική ομάδα των ρητών $\mathbb{Q}^+$. Πράγματι, αν υπήρχε μια απεικόνιση $f : \mathbb{Z} \longrightarrow \mathbb{Q}^+$ που να είναι ισομορφισμός με $f(1) = a/b$, τότε η εικόνα ενός θετικού ακεραίου n θα ήταν $f(n) = n\,a/b$. Επομένως, αν p είναι ένας πρώτος που δεν διαιρεί το b, για τον ρητό $1/p$ δεν υπάρχει ακέραιος m τέτοιος ώστε $f(m) = 1/p$ (γιατί;), δηλαδή η f δεν είναι επί, άτοπο.

3. Ας συγκρίνουμε την ομάδα $\mathcal{E}_4 = \{\, e^{\frac{2\pi ik}{4}} \mid k = 0, 1, 2, 3, 4\,\}$ και την ομάδα $K_4 = \{\, 1, (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\,\}$. Παρατηρούμε ότι η $\mathcal{E}_4$ έχει ένα στοιχείο τάξης 2 και δύο στοιχεία τάξης 4, ενώ η K_4 έχει τρία στοιχεία τάξης 2 και κανένα στοιχείο τάξης 4. Άρα η $\mathcal{E}_4$ δεν είναι ισόμορφη με την K_4.

4. Η πολλαπλασιαστική ομάδα F^* ενός σώματος F δεν είναι ποτέ ισόμορφη με την προσθετική του ομάδα F^+. Πράγματι, αν $\phi : F^* \longrightarrow F^+$ ήταν ένας ισομορφισμός, τότε θα έπρεπε να έχουμε $\phi(1) = 0$. Αν η χαρακτηριστική του F είναι διάφορη του 2, τότε θα είχαμε $0 = \phi(1) = \phi((-1)\,(-1)) = \phi(-1) + \phi(-1) = 2\phi(-1)$, δηλαδή $\phi(-1) = 0$ και η ϕ δεν θα ήταν 1 - 1 . Αν η χαρακτηριστική του F είναι ίση με 2, τότε κάθε μη μηδενικό στοιχείο της F^+ είναι τάξης 2, ενώ η F^* δεν έχει, στην περίπτωση αυτή, κανένα στοιχείο τάξης 2.

4.5.10 Παραδείγματα ισόμορφων ομάδων.

1. $\mathbb{Z}^+ \cong n\,\mathbb{Z}, \quad n > 0.$

   Το σύνολο $n\,\mathbb{Z} = \{\, n\,z \mid z \in \mathbb{Z}\,\}$ των ακεραίων πολλαπλασίων ενός θετικού ακεραίου αριθμού n μαζί με την πρόσθεση των ακεραίων εύκολα διαπιστώνεται ότι αποτελεί ομάδα. Επίσης απλοί υπολογισμοί δείχνουν ότι η απεικόνιση $\mathbb{Z} \longrightarrow n\,\mathbb{Z}, \quad z \longrightarrow n\,z$ είναι ένας ισομορφισμός ομάδων. Αυτό είναι ένα παράδειγμα ομάδας που είναι ισόμορφη με γνήσιες υποομάδες της.

2. $\mathbb{Z}_n \cong \mathcal{E}_n, \quad n > 0.$

   Θεωρούμε την προσθετική ομάδα $\mathbb{Z}_n$ των κλάσεων υπολοίπων mod$n$ και την πολλαπλασιαστική ομάδα $\mathcal{E}_n$ των $n-$οστών ριζών της μονάδας. Η αντιστοιχία $\phi : \mathbb{Z}_n \longrightarrow \mathcal{E}_n, \quad k \bmod n \longrightarrow e^{\frac{2\pi ki}{n}}$ είναι απεικόνιση, αφού αν $k_1 \equiv k_2 \pmod n$, τότε $e^{\frac{2\pi(k_1-k_2)i}{n}} = 1$, δηλαδή $e^{\frac{2\pi k_1 i}{n}} = e^{\frac{2\pi k_2 i}{n}}$. Παρόμοιος ισχυρισμός δείχνει ότι η ϕ είναι 1 - 1. Επίσης η ϕ διατηρεί

τις πράξεις, αφού $\phi(\,k_1 \bmod n \,+\, k_2 \bmod n\,) \,=\, \phi(\,(k_1+k_2) \bmod n\,) \,=\, e^{\frac{2\pi(k_1+k_2)i}{n}} \,=\, e^{\frac{2\pi k_1 i}{n}} \cdot e^{\frac{2\pi k_2 i}{n}}$. Καθώς η ϕ είναι επί, συμπεραίνουμε ότι αυτή είναι ισομορφισμός.

3. $\mathbb{R}^{\times}_{>0} \cong \mathbb{R}^{+}$.

   Από τη στοιχειώδη ανάλυση είναι γνωστό ότι η λογαριθμική απεικόνιση $\log : \mathbb{R}^{\times}_{>0} \longrightarrow \mathbb{R}^{+}$ είναι 1 - 1 και επί, επίσης $\log(\,x\,y\,) = \log x + \log y$, με $\log 1 = 0$ και $\log \frac{1}{x} = -\log x$. Η αντίστροφη απεικόνιση της log είναι η εκθετική απεικόνιση $\mathbb{R}^{+} \longrightarrow \mathbb{R}^{\times}_{>0}$ με $x \longrightarrow e^{x}$. Ο ισομορφισμός αυτός φανερώνει ότι η πρόσθεση πραγματικών αριθμών από αλγεβρικής πλευράς είναι ουσιαστικά ίδια με τον πολλαπλασιασμό θετικών πραγματικών αριθμών και η μετάβαση από τη μία στην άλλη γίνεται μέσω του γνωστού "λογαριθμικού κανόνα". Ας σημειωθεί ότι το ίδιο δεν συμβαίνει για τους ρητούς αριθμούς, δηλαδή η πολλαπλασιαστική ομάδα των θετικών ρητών δεν είναι ισόμορφη με την προσθετική ομάδα των ρητών. Πράγματι, έστω ότι υπάρχει ένας ισομορφισμός $\phi : \mathbb{Q}^{+} \longrightarrow \mathbb{Q}^{\times}_{>0}$ και έστω $x \in \mathbb{Q}^{+}$ τέτοιο ώστε $\phi(x) = 2$. Τότε όμως, αν $u \in \mathbb{Q}^{\times}_{>0}$ είναι η εικόνα του $x/2$ μέσω του ϕ, δηλαδή αν $\phi(x/2) = u$, τότε θα έχουμε $2 = \phi(x) = \phi(\,x/2 + x/2\,) = \phi(x/2) \cdot \phi(x/2) = u^2$. Δηλαδή το 2 είναι το τετράγωνο ενός ρητού αριθμού, άτοπο.

4. $SO_2(\,\mathbb{R}\,) \cong S^1$.

   Θεωρούμε το σύνολο $S^1 = \{\, z \in \mathbb{C} \mid \;\mid z \mid = 1\,\}$ του $\mathbb{C}$, το οποίο είναι ομάδα ως προς τον πολλαπλασιασμό μιγαδικών αριθμών. Κάθε στοιχείο του S^1, παριστώμενο στο μιγαδικό επίπεδο, είναι ένα σημείο του κύκλου με κέντρο την αρχή των αξόνων και ακτίνα ίση με ένα. Για το λόγο αυτό η ομάδα S^1 ονομάζεται ***ομάδα του μοναδιαίου κύκλου***. Ας θεωρήσουμε την ειδική ορθογώνια ομάδα $SO_2(\,\mathbb{R}\,)$, που περιγράψαμε στην Παράγραφο 4.1 και την απεικόνιση $SO_2(\,\mathbb{R}\,) \longrightarrow S^1$, $A(\theta) \longrightarrow e^{i\theta}$. Επειδή $A(\theta) = A(\theta + 2k\pi)$ και $A(\theta)\,A(\theta') = A(\theta+\theta') \longrightarrow e^{i(\theta+\theta')} = e^{\theta}\,e^{\theta'}$, η απεικόνιση αυτή είναι ένας ισομορφισμός ομάδων.

5. $\mathbb{Q}^{\times} \cong \mathbb{Q}^{\times}_{>0} \times C_2$, $\mathbb{R}^{\times} \cong \mathbb{R}^{\times}_{>0} \times C_2$, $\mathbb{C}^{\times} \cong \mathbb{R}^{\times}_{>0} \times S^1$.

   Με C_2 παριστάνουμε την πολλαπλασιαστική ομάδα $\{\,1,\,-1\,\}$, οπότε οι αντιστοιχίες $\mathbb{Q} \longrightarrow \mathbb{Q}^{\times}_{>0} \times C_2$ και $\mathbb{R}^{\times} \longrightarrow \mathbb{R}^{\times}_{>0} \times C_2$ με $q \longrightarrow (\,q,\,1\,)$ αν $q > 0$ και $q \longrightarrow (\,\mid q \mid, -1\,)$ αν $q < 0$, όπου $q \in \mathbb{Q}^{\times}$, (αντίστοιχα $q \in \mathbb{R}^{\times}$) είναι προφανώς ισομορφισμοί ομάδων. Επίσης η απεικόνιση $r\,e^{i\theta} \longrightarrow (\,r,\,e^{i\theta}\,)$ είναι ένας ισομορφισμός μεταξύ των ομάδων $\mathbb{C}^{\times}$ και $\mathbb{R}^{\times}_{>0} \times S^1$.
   Ας σημειωθεί όμως ότι υπάρχει ισομορφισμός $\mathbb{C}^{\times} \cong S^1$, ο οποίος δεν

μπορεί να εκφρασθεί μέσω ενός συγκεκριμένου τύπου, αν και αποδεικνύεται η ύπαρξή του. Η απόδειξη της ύπαρξης αυτού του ισομορφισμού απαιτεί γνώσεις που είναι πέρα απ΄ το σκοπό αυτού του βιβλίου. Επίσης σημειώνουμε ότι υπάρχει ισομορφισμός $\mathbb{C}^+ \cong \mathbb{R}^+$, ο οποίος επίσης δεν μπορεί να εκφρασθεί μέσω ενός συγκεκριμένου τύπου.

6. $\mathbb{Q}^\times_{>0} \cong \mathbb{Z}[x]$.

   Με $\mathbb{Z}[x]$ παριστάνουμε την προσθετική ομάδα των πολυωνύμων μιας μεταβλητής με ακεραίους συντελεστές. Από το Θεμελιώδες Θεώρημα της Αριθμητικής γνωρίζουμε ότι κάθε ρητός $\frac{\alpha}{\beta} > 0$ γράφεται μοναδικά στη μορφή $\frac{\alpha}{\beta} = q_0^{\alpha_0} q_1^{\alpha_1} \cdots q_i^{\alpha_i} \cdots$, όπου $q_0 < q_1 < q_2 < \cdots$ είναι όλοι οι πρώτοι και α_i είναι ακέραιοι αριθμοί όλοι μηδέν εκτός από πεπερασμένο πλήθος. Είναι φανερό ότι η απεικόνιση

$$f(x) = \alpha_n x^n + \cdots + \alpha_0 \longrightarrow q_0^{\alpha_0} q_1^{\alpha_1} \cdots q_n^{\alpha_n}$$

   είναι ένας ισομορφισμός μεταξύ των ομάδων $\mathbb{Z}[x]$ και $\mathbb{Q}^\times_{>0}$.

7. $S_n \cong S_X, \quad |\, X \,| = n$.

   Ήδη έχουμε αναφέρει στην παράγραφο 4.2 ότι αν X και Y είναι δύο σύνολα με το ίδιο πλήθος στοιχεία, τότε οι ομάδες S_X και S_Y μπορούν να ταυτισθούν με την ομάδα S_n, όπου $n = |\, X \,|$. Πράγματι, θεωρούμε μία 1 - 1 αντιστοιχία $\alpha : X \longrightarrow Y$. Τότε για κάθε $\sigma \in S_X$ η απεικόνιση $\alpha \circ \sigma \circ \alpha^{-1} : Y \longrightarrow Y$ είναι μια μετάθεση του Y (γιατί;), όπου α^{-1} είναι η αντίστροφη απεικόνιση $Y \longrightarrow X$ της α. Τώρα η απεικόνιση $f : S_X \longrightarrow S_Y$ με $\sigma \longrightarrow \alpha \circ \sigma \circ \alpha^{-1}$ είναι ένας ισομορφισμός ομάδων, αφού $\alpha \circ \sigma_1 \circ \alpha^{-1} = \alpha \circ \sigma_2 \circ \alpha^{-1}$ αν και μόνο αν $\sigma_1 = \sigma_2$ και επιπλέον $f(\,\sigma_1\,\sigma_2\,) = \alpha \circ \sigma_1\,\sigma_2 \circ \alpha^{-1} = \alpha \circ \sigma_1 \circ \alpha^{-1}\,\alpha \circ \sigma_2 \circ \alpha^{-1} = f(\,\sigma_1\,)\,f(\,\sigma_2\,)$. Εδώ παρατηρούμε ότι αν β ήταν μια άλλη 1 - 1 απεικόνιση από το X στο Y, τότε και η απεικόνιση $S_X \ni \sigma \longrightarrow \beta\,\sigma\,\beta^{-1} \in S_Y$ είναι ένας άλλος ισομορφισμός της S_X στην S_Y. Αυτό δείχνει ότι αν G και H είναι δυο ισόμορφες ομάδες, τότε γενικά υπάρχουν πολλοί ισομορφισμοί από τη G στην H. Αυτό θα το δούμε και στο Παράδειγμα 9, όπου σε κάθε βάση ενός n-διάστατου διανυσματικού χώρου V αντιστοιχούμε έναν ισομορφισμό της $GL(\,V\,)$ στην $GL_n(\,K\,)$.

8. $GL_2(\,\mathbb{Z}_2\,) \cong S_3$.

   Η ομάδα $GL_2(\,\mathbb{Z}_2\,)$ αποτελείται από τους 2×2 αντιστρέψιμους πίνακες με στοιχεία από το σώμα $\mathbb{Z}_2$ ή, ισοδύναμα, από τους 2×2 πίνακες των οποίων οι στήλες είναι γραμμικά ανεξάρτητα διανύσματα του διανυσματικού χώρου $\mathbb{Z}_2^2$. Ο χώρος $\mathbb{Z}_2^2$ αποτελείται από τα διανύσματα $\binom{0}{0}$, $\binom{1}{0}$, $\binom{0}{1}$ και $\binom{1}{1}$.

Τα ζεύγη $\left\{ \binom{1}{0}, \binom{0}{1} \right\}$, $\left\{ \binom{1}{0}, \binom{1}{1} \right\}$ και $\left\{ \binom{0}{1}, \binom{1}{1} \right\}$ είναι τα μόνα γραμμικά ανεξάρτητα ζεύγη διανυσμάτων. Άρα τα στοιχεία της $GL_2(\mathbb{Z}_2)$ είναι τα εξής: $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\Gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\Delta = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, $E = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Αν θέσουμε $v_1 = \binom{1}{0}$, $v_2 = \binom{0}{1}$, $v_3 = \binom{1}{1}$, βλέπουμε ότι
$A(v_1) = v_2$, $A(v_2) = v_1$, $A(v_3) = v_3$
$B(v_1) = v_3$, $B(v_2) = v_2$, $B(v_3) = v_1$
$\Gamma(v_1) = v_1$, $\Gamma(v_2) = v_3$, $\Gamma(v_3) = v_2$
$\Delta(v_1) = v_2$, $\Delta(v_2) = v_3$, $\Delta(v_3) = v_1$
$E(v_1) = v_3$, $E(v_2) = v_1$, $E(v_3) = v_2$.
Συνεπώς έχουμε την αντιστοιχία $A \longleftrightarrow (12)$, $B \longleftrightarrow (13)$, $\Gamma \longleftrightarrow (23)$, $\Delta \longleftrightarrow (123)$, $E \longleftrightarrow (132)$ και $I \longleftrightarrow 1$. Απλοί υπολογισμοί δείχνουν ότι η αντιστοιχία αυτή διατηρεί και τις πράξεις και επομένως $GL_2(\mathbb{Z}_2) \cong S_3$.

9. $GL(V) \cong GL_n(K)$.
Έστω V ένας $n-$διάστατος διανυσματικός χώρος επί του σώματος K και $\{e_1, e_2, \ldots, e_n\}$ μία βάση του. Θεωρούμε την ομάδα $GL(V)$ όλων των αντιστρέψιμων γραμμικών απεικονίσεων από τον V στον εαυτό του. Από τη Γραμμική Άλγεβρα γνωρίζουμε ότι ως προς τη βάση $\{e_1, e_2, \ldots, e_n\}$ υπάρχει μία 1 - 1 και επί αντιστοιχία μεταξύ των στοιχείων της $GL(V)$ και της γενικής γραμμικής ομάδας $GL_n(K)$. Επιπλέον η αντιστοιχία αυτή διατηρεί το γινόμενο, δηλαδή αν $f_1, f_2 \in GL(V)$, τότε ο πίνακας που αντιστοιχεί στη σύνθεση $f_1 \circ f_2$ είναι το γινόμενο των αντιστοίχων πινάκων. Συνεπώς η αντιστοιχία αυτή είναι ένας ισομορφισμός από την $GL(V)$ στην $GL_n(K)$ που εξαρτάται από τη βάση $\{e_1, e_2, \ldots, e_n\}$ του V. Δηλαδή για κάθε επιλογή βάσης παίρνουμε και έναν διαφορετικό ισομορφισμό.

10. *Η άλγεβρα του Boole.*

Έστω G μία πεπερασμένη ομάδα για την πράξη της οποίας θα χρησιμοποιούμε τον συμβολισμό της πρόσθεσης. Υποθέτουμε ότι $a + a = 0$ (το 0 είναι το ουδέτερο στοιχείο), δηλαδή $2a = 0$, για κάθε $a \in G$. Τότε $2(a + b) = 0$ για $a, b \in G$, ή ισοδύναμα $a + b = -(a + b) = -b - a$. Αλλά επειδή $a = -a$ και $b = -b$, έχουμε ότι $a + b = b + a$, δηλαδή η G είναι Αβελιανή ομάδα. Επίσης παρατηρούμε ότι η ομάδα G μπορεί να θεωρηθεί ένας διανυσματικός χώρος επί του σώματος $\mathbb{Z}_2$ και επειδή είναι πεπερασμένη, ως διανυσματικός χώρος, έχει πεπερασμένη διάσταση, έστω n. Συνεπώς, αν $\{e_1, e_2, \ldots, e_n\}$ είναι μία βάση του διανυσματικού χώ-

ρου G τότε κάθε στοιχείο a του G μπορεί να παρασταθεί (ως προς τη βάση αυτή) σαν μια $n-$άδα $(a_1, \ldots, a_n)$, $a_i \in \mathbb{Z}_2$. Οπότε, με την βοήθεια του πολλαπλασιασμού των στοιχείων του $\mathbb{Z}_2$, ορίζεται ο εξής πολλαπλασιασμός στη G, $a\,b = (a_1, \ldots, a_n)\cdot(b_1, \ldots, b_n) = (a_1b_1, \ldots, a_nb_n)$, κάθε $a, b \in G$. Άρα, για κάθε $a \in G$, ισχύει $a^2 = a$. Ο διανυσματικός χώρος G με τον πολλαπλασιασμό αυτό λέγεται ***άλγεβρα του Boole***.

Η ομάδα G είναι ισόμορφη με την ομάδα του Παραδείγματος 4.3.5 (4), δηλαδή την ομάδα $\mathcal{P}(X)$ που είναι εφοδιασμένη με την πράξη $\triangle$ (τη συμμετρική διαφορά), όπου $\mathcal{P}(X)$ είναι το δυναμοσύνολο ενός συνόλου X με n στοιχεία. Πράγματι, για κάθε $A \in \mathcal{P}(X)$ ισχύει $A \triangle A = \emptyset$ και αν $A_1, A_2, \ldots, A_n$ είναι τα μονοσύνολα $A_1 = \{e_1\}$, $A_2 = \{e_2\}, \ldots, A_n = \{e_n\}$ της G, τότε η απεικόνιση $G \longrightarrow \mathcal{P}(X)$, με $e_i \longrightarrow A_i$ ορίζει έναν ισομορφισμό (γιατί;). Ο πολλαπλασιασμός, που ορίστηκε στην G, στο $\mathcal{P}(X)$ "αντιστοιχεί" στην τομή $A \cap B$ δύο στοιχείων A, $B \in \mathcal{P}(X)$. Η θεώρηση της G ως το δυναμοσύνολο ενός συνόλου X απετέλεσε το μαθηματικό μοντέλο του Άγγλου μαθηματικού George Boole (1815 - 1864) για τους "τυπικούς ισχυρισμούς" (συνεπαγωγές) που ισχύουν στη Μαθηματική Λογική [19].

Στην αρχή της Παραγράφου 4.2 τονίσαμε ότι ένας λόγος που οι συμμετρικές ομάδες παίζουν σημαντικό ρόλο σε όλη τη θεωρία ομάδων οφείλεται στο επόμενο θεώρημα του Cayley:

4.5.11 Θεώρημα. *Κάθε πεπερασμένη ομάδα G είναι ισόμορφη με μια ομάδα μεταθέσεων.*

Απόδειξη. Για κάθε $g \in G$ θεωρούμε την απεικόνιση $L_g : G \longrightarrow G$ με $x \longrightarrow gx$, η οποία είναι 1-1 και επί. Αν $g_1, g_2, x \in G$, τότε έχουμε $L_{g_1g_2}(x) = (g_1\,g_2)\,x = g_1\,(g_2\,x) = g_1\,(L_{g_2}(x)) = L_{g_1}\,(L_{g_2}(x)) = (L_{g_1}\,L_{g_2})\,(x)$ και άρα $L_{g_1g_2} = L_{g_1}\,L_{g_2}$. Συνεπώς η απεικόνιση

$$L : G \longrightarrow S_{|G|}, \quad g \longrightarrow L_g$$

είναι ένας ομομορφισμός ομάδων. Επιπλέον η L είναι 1-1, αφού για κάθε δύο στοιχεία $g_1, g_2 \in G$ με $g_1 \neq g_2$ έχουμε $L(g_1) = L_{g_1} \neq L_{g_2} = L(g_2)$. Συνεπώς $G \cong Im\,L$, όπου $Im\,L$ είναι μια ομάδα μεταθέσεων. ⊺

Θα ολοκληρώσουμε την παράγραφο αυτή, ταξινομώντας όλες τις ομάδες G που έχουν τάξη ≤ 7.

Από το Πόρισμα 4.4.26 προκύπτει ότι αν η τάξη της G είναι $2, 3, 5$ ή 7 τότε η G παράγεται από ένα στοιχείο της g και είναι ισόμορφη με την ομάδα $\mathbb{Z}_n$,

$n = 2, 3, 5$ και 7 αντίστοιχα. Ένας ισομορφισμός είναι η απεικόνιση $g^k \longrightarrow k \mod n$.

Έστω τώρα ότι $|G| = 4$. Αν η G παράγεται από ένα στοιχείο τότε όπως πριν $G \cong \mathbb{Z}_4$. Έστω ότι η G δεν παράγεται από ένα στοιχείο. Τότε από το Πόρισμα 4.4.23 έπεται ότι κάθε στοιχείο της διάφορο του 1 πρέπει να είναι τάξης 2. Αν $g_1, g_2 \in G \setminus \{1\}$, $g_1 \neq g_2$ και $g_1^2 = g_2^2 = 1$, τότε το στοιχείο της g_1g_2 είναι διάφορο από τα $1, g_1, g_2$, αφού η σχέση $g_1g_2 = g_1$ ή η σχέση $g_1g_2 = g_2$ θα έδινε $g_2 = 1$ ή $g_1 = 1$ και η σχέση $g_1g_2 = g_1^2$ ή η σχέση $g_1g_2 = g_2^2$ θα έδινε $g_1 = g_2$. Συνεπώς η ομάδα $G = \{1, g_1, g_2, g_1g_2\}$ είναι ισόμορφη με την ομάδα $\{i, (12)(34), (13)(24), (14)(23)\}$ (γιατί;).

Έστω τώρα ότι η G έχει τάξη 6. Από το 4.4.23 οι πιθανές τάξεις των μη τετριμμένων στοιχείων της G είναι 2,3 και 6. Αν η G έχει ένα στοιχείο g τάξης 6 τότε αυτή παράγεται από το g και είναι ισόμορφη με τη $\mathbb{Z}_6$. Σ' αυτή τη περίπτωση τα στοιχεία g^2 και g^4 είναι τάξης 3 και το στοιχείο g^3 είναι τάξης 2 ενώ το στοιχείο g^5 είναι τάξης 6. Υποθέτουμε ότι η G δεν παράγεται από ένα στοιχείο της, δηλαδή ότι η G δεν έχει ένα στοιχείο τάξης 6. Συνεπώς όλα τα διάφορα του 1 στοιχεία της G είναι τάξης 2 ή 3. Αν όλα αυτά ήταν τάξης 2 και g_1, g_2 ήταν δύο από αυτά τότε και το γινόμενό τους g_1g_2 θα ήταν τάξης 2. Γι' αυτό το γινόμενο ισχύει όμως ότι $g_1g_2 = (g_1g_2)^{-1} = g_2^{-1}g_1^{-1} = g_2g_1$, που σημαίνει ότι το υποσύνολο $\{1, g_1, g_2, g_1g_2\}$ θα ήταν μια υποομάδα τάξης 4 που είναι αδύνατο, σύμφωνα με το θεώρημα του Lagrange. Άρα η G πρέπει να έχει ένα στοιχείο τάξης 3. Αλλά επίσης στη G δεν μπορούν όλα τα μη-ουδέτερα στοιχεία να είναι τάξης 3, αφού για καθένα από αυτά το αντίστροφό του θα ήταν τάξης 3 οπότε η G δεν θα ήταν τάξης 6. Άρα η G πρέπει να έχει και ένα στοιχείο τάξης 2. Έστω λοιπόν a και b δύο στοιχεία τάξης 2 και τάξης 3 αντίστοιχα. Συνεπώς $a \notin \langle b \rangle = \{1, b, b^2\}$ και έχουμε $G = \langle b \rangle \cup a\langle b \rangle = \{1, b, b^2, a, ab, ab^2\}$. Επειδή η G είναι ομάδα, το $ba \in G$ και θα πρέπει ή $ba = ab$ ή $ba = ab^2$ (γιατί;). Στην πρώτη περίπτωση μπορεί εύκολα να ελεγθεί ότι η τάξη του ba είναι 6 και άρα απορρίπτεται αφού υποθέσουμε ότι η G δεν έχει στοιχείο τάξης 6. Στη δεύτερη περίπτωση, μπορούμε εύκολα να δούμε ότι η ομάδα G είναι ισόμορφη με την S_3.

Ασκήσεις 4.5

1. Δίνονται οι ομάδες $G = \left\{ \begin{pmatrix} 1 & \nu \\ 0 & 1 \end{pmatrix} \mid \nu \in \mathbb{Z} \right\}$ και $H = \{1, i, -1, -i\}$ με τις γνωστές πράξεις και $\vartheta : G \longrightarrow H$ με $\begin{pmatrix} 1 & \nu \\ 0 & 1 \end{pmatrix} \xrightarrow{\vartheta} i^\nu$. Δείξτε ότι ο ϑ είναι επιμορφισμός ομάδων. Να βρεθεί ο πυρήνας του ϑ.

2. α) Δείξτε ότι η $f : Z \times Z \longrightarrow Z$, $f(x,y) = x - 2y$ είναι ένας ομομορφισμός προσθετικών ομάδων και βρείτε την $f(Z \times Z) = Imf$.
β) Έστω G μια ομάδα και $g \in G$. Δείξτε ότι η $f : Z \longrightarrow G$ με $f(k) = g^{2k}$ είναι ένας ομομορφισμός. Ποια είναι η Imf αν η τάξη του g είναι 6 ή 7;

3. Δινονται οι παρακάτω απεικονίσεις από την πολλαπλασιαστική ομάδα των πραγματικών αριθμών στον εαυτό της

   (α′) $x \longrightarrow -x$
   (β′) $x \longrightarrow x^2$
   (γ′) $x \longrightarrow x^3$
   (δ′) $x \longrightarrow x^4$
   (ε′) $x \longrightarrow x^{-1}$
   (ϛ′) $x \longrightarrow -x^2$
   (ζ′) $x \longrightarrow 2x$
   (η′) $x \longrightarrow 3x$
   (ϑ′) $x \longrightarrow -\frac{1}{x}$
   (ι′) $x \longrightarrow 10^x$
   (ια′) $x \longrightarrow \sqrt{|\, x \,|}$

   Ποιες από αυτές είναι ομομορφισμοί ομάδων; Απ' τους ομομορφισμούς, ποιοι είναι ισομορφισμοί ;

4. Ποιες από τις παρακάτω απεικονίσεις από την πολλαπλασιαστική ομάδα των μιγαδικών στον εαυτό της είναι ομομορφισμοί ;

   (α′) $z \longrightarrow z^6$
   (β′) $z \longrightarrow z^8$
   (γ′) $z \longrightarrow \bar{z}$
   (δ′) $z \longrightarrow 2z + 1$
   (ε′) $z \longrightarrow \frac{1}{z}$

   Στην περίπτωση που μια απεικόνιση είναι ομομορφισμός προσδιορίστε τον πυρήνα της.

5. Έστω $\mathbb{Q}[x]$ η προσθετική ομάδα των πολυωνύμων με ρητούς συντελεστές και $G = \{\, \alpha x + \beta \mid \alpha, \beta \in \mathbb{Q} \,\}$ η προσθετική ομάδα των γραμμικών πολυωνύμων. Θεωρούμε την αντιστοιχία $\mathbb{Q}[x] \longrightarrow G,\ f(x) \longrightarrow \alpha x + \beta$, όπου $\alpha x + \beta$ είναι το υπόλοιπο της διαίρεσης του $f(x)$ δια του $x^2 + 1$. Δείξτε ότι αυτός είναι ένας ομομορφισμός ομάδων. Ποιος είναι ο πυρήνας του; Είναι η απεικόνιση αυτή " επί ";

6. Έστω V ένας τρισδιάστατος πραγματικός διανυσματικός χώρος με εσωτερικό γινόμενο και $v \in V$. Ορίζουμε την απεικόνιση $V \longrightarrow \mathbb{R}^+$ με $x \longrightarrow \langle\, x,\, a \,\rangle$, όπου $\langle\, ,\, \rangle$ συμβολίζει το εσωτερικό γινόμενο. Δείξτε ότι η απεικόνιση αυτή είναι ομομορφισμός ομάδων. Ποιος είναι ο πυρήνας της;

7. Έστω $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R},\ a \cdot c \neq 0 \right\}$ και $\phi : G \longrightarrow \mathbb{R}^+$ με $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \longrightarrow \log(a \cdot c)$. Δείξτε ότι η ϕ είναι ομομορφισμός ομάδων. Ποιος είναι ο πυρήνας της;

8. Να βρεθούν όλοι οι ομομορφισμοί ϕ από την πολλαπλασιαστική ομάδα των ρητών στον εαυτό της τέτοιοι ώστε $Im\phi \subseteq \{\, -2, -1, 0, 1, 2 \,\}$.

9. $\alpha\,)$ Δείξτε ότι η απεικόνιση $\lambda_r(\, x\,) = r \cdot x,\ r \in \mathbb{Q}$ είναι ένας ενδομορφισμός της προσθετικής ομάδας των ρητών.
   $\beta\,)$ Δείξτε ότι κάθε ενδομορφισμός της προσθετικής ομάδας των ρητών είναι της παραπάνω μορφής.
   $\gamma\,)$ Δείξτε ότι κάθε μη-μηδενικός ενδομορφισμός της προσθετικής ομάδας των ρητών είναι αυτομορφισμός.

10. Έστω $G = GL_2(\mathbb{Q})$, $A \in G$ και $d = \frac{m}{n}\, 2^{\ell_A}$ η ορίζουσα του πίνακα A, όπου m, n είναι περιττοί ακέραιοι και ℓ_A ακέραιος (που εξαρτάται από τον πίνακα A). Δείξτε ότι η αντιστοιχία $f : A \longrightarrow \begin{pmatrix} 1 & \ell_A \\ 0 & 1 \end{pmatrix}$ ορίζει έναν ενδομορφισμό της G. Βρείτε τον πυρήνα της. Δείξτε ότι αν και ο πίνακας $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ ανήκει στο κέντρο της G, η εικόνα του μέσω της f δεν ανήκει στο κέντρο.

11. i) Πόσοι ομομορφισμοί ομάδων $\mathbb{Z}_{20} \longrightarrow \mathbb{Z}_8$ υπάρχουν ;
    ii) Υπάρχει μη τετριμμένος ομομορφισμός ομάδων $\mathbb{Z}_{20} \longrightarrow \mathbb{Z}_{27}$;

12. Έστω $\phi : G_1 \longrightarrow G_2$ ένας επιμορφισμός πεπερασμένων ομάδων. Αν η ομάδα G_2 περιέχει στοιχείο τάξης m, τότε δείξτε ότι η ομάδα G_1 περιέχει επίσης στοιχείο τάξης m.

13. i) Για ποια n υπάρχει επιμορφισμός ομάδων $G \longrightarrow S_n$, αν η ομάδα G είναι Αβελιανή;

    ii) Για ποια n υπάρχει μονομορφισμός ομάδων $S_n \longrightarrow G$, αν η ομάδα G είναι Αβελιανή;

14. Έστω G πεπερασμένη ομάδα με τάξη n και $\phi : G \longrightarrow \mathbb{Z}_{15}$ ομομορφισμός ομάδων. Ποιες από τις παρακάτω προτάσεις είναι σωστές και ποιες λάθος; (Τεκμηριώστε την απάντησή σας).

    (α′) Το 15 διαιρεί το n.

    (β′) Το n διαιρεί το 15.

    (γ′) Αν ο ϕ είναι μονομορφισμός, τότε το 15 διαιρεί το n.

    (δ′) Αν ο ϕ είναι επιμορφισμός, τότε το 15 διαιρεί το n.

    (ε′) Αν ο ϕ είναι μονομορφισμός, τότε το n διαιρεί το 15.

    (ϛ′) Αν ο ϕ είναι επιμορφισμός, τότε το n διαιρεί το 15.

    (ζ′) Αν $n = 15$, τότε ο ϕ είναι ισομορφισμός.

15. Έστω G ομάδα, $a, b \in G$ δύο στοιχεία της και $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow G$ η απεικόνιση με $f((x, y)) = a^x b^y$.
    i) Διατυπώστε και αποδείξτε ικανή και αναγκαία συνθήκη που πρέπει να πληρούν τα a και b ώστε η f να είναι ομομορφισμός ομάδων.
    ii) Αν η ομάδα G είναι Αβελιανή και τα a, b πεπερασμένης τάξης με τάξεις m και n αντίστοιχα, προσδιορίστε τον πυρήνα της f, την $Im\, f$ και το δείκτη του $\ker f$ στην ομάδα $\mathbb{Z} \times \mathbb{Z}$.
    Υπόδειξη: Εξετάστε πρώτα την περίπτωση όπου μ.κ.δ.$(m, n) = 1$.

16. Έστω $f : G \longrightarrow G$ ενδομορφισμός ομάδων με $f^2 = f$. Δείξτε ότι:
    i) Αν ο f δεν είναι ο ταυτοτικός, τότε ο f δεν είναι επί.
    ii) $G = ker\, f \cdot Im\, f$ και $ker\, f \cap Im\, f = \{1\}$.

17. Έστω G μια Αβελιανή ομάδα και $\alpha \in Aut(G)$ με $\alpha^2 = 1_G$. Αν η G έχει περιττή τάξη δείξτε ότι κάθε στοιχείο $x \in G$ γράφεται ως $x = yz$ όπου $\phi(y) = y$ και $\phi(z) = z^{-1}$.

18. Αν G είναι μια πεπερασμένη ομάδα και $\phi : G \to G$ είναι ένας αυτομορφισμός τέτοιος ώστε $\phi(x) = x^{-1}$ για περισσότερα από τα $3/4$ των στοιχείων της G τότε δείξτε ότι η G είναι Αβελιανή.

19. Αν $g_1, g_2, \ldots, g_n$ είναι τα στοιχεία μιας ομάδας G, θέτουμε $g_\kappa g_\lambda = g_{\psi(\kappa,\lambda)}$, $\kappa, \lambda = 1, \ldots, n$.

i) Δείξτε ότι η απεικόνιση ϕ που ορίζεται από τον τύπο $(\phi(g_\kappa))(\lambda) = \psi(\kappa, \lambda)$ είναι ένας μονομορφισμός της G στην S_n.
ii) Βρείτε αν υπάρχει ομάδα G με $\mid G \mid = 16$, τέτοια ώστε να υπάρχει στοιχείο $g \in G$ με $\phi(g) = (1\,2\,3\,4)(5\,6\,7\,8\,9\,10\,11\,12\,13\,14\,15\,16)$, όπου ϕ είναι η απεικόνιση που ορίστηκε παραπάνω. Απαντήστε το ίδιο για $\phi(g) = (1\,2) \in S_{16}$.

20. α) Υπάρχει ομάδα G τέτοια ώστε $G \times K_4 \cong A_4$, όπου K_4 είναι η ομάδα του Klein;

    β) Υπάρχει ομάδα G τέτοια ώστε $G \times K_4 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$;

21. Έστω S_n η συμμετρική ομάδα βαθμού n και $a_1, \ldots, a_m \in \{\, 1, 2, \ldots, n \,\}$. Έστω G το σύνολο όλων των μεταθέσεων $\sigma \in S_n$ με την ιδιότητα $\sigma(a_i) = a_i$, για κάθε $i = 1, \ldots, m$. Δείξτε ότι το G είναι μια ομάδα μεταθέσεων ισόμορφη με την S_k, όπου $k = n - m$.

22. Έστω V_1, V_2 δύο διανυσματικοί χώροι πεπερασμένης διάστασης επί του ιδίου σώματος. Θεωρούμε τους δύο χώρους ως Αβελιανές ομάδες με πράξη την πρόσθεση. Δείξτε ότι οι ομάδες αυτές είναι ισόμορφες αν οι δύο χώροι έχουν την ίδια διάσταση. Ισχύει το αντίστροφο;

23. Δείξτε ότι το σύνολο $G = \{\, 2^m 3^n \mid m, n \in \mathbb{Z} \,\}$ είναι ομάδα με πράξη τον πολλαπλασιασμό ισόμορφη με την $\mathbb{Z} \times \mathbb{Z}$.

24. Έστω G μια ομάδα με μια πράξη $*$, X ένα σύνολο και $\vartheta : G \longrightarrow X$ μια απεικόνιση που είναι $1-1$ και επί. Στο σύνολο X ορίζουμε μια πράξη ως εξής $\vartheta(a) \circ \vartheta(b) = \vartheta(\, a * b \,)$, για κάθε a, $b \in G$. Δείξτε ότι το σύνολο X με την πράξη $\circ$ είναι ομάδα ισόμορφη με την ομάδα G.

25. Γιατί δεν μπορούμε να βρούμε έναν ισομορφισμό μεταξύ των ομάδων
    $\alpha)$ Της προσθετικής ομάδας των ακεραίων και της $\mathbb{Z}_n$, $n \neq 0$.

    $\beta)$ Της πολλαπλασιαστικής ομάδας των μιγαδικών αριθμών και της $\mathbb{R}^+ \times \mathbb{R}^+$, όπου $\mathbb{R}^+$ είναι η προσθετική ομάδα των πραγματικών αριθμών.

    $\gamma)$ Της ομάδας συμμετρίας ενός ισοπλεύρου τριγώνου και της ομάδας των στροφών ενός εξαγώνου.

26. Έστω p ένας περιττός πρώτος αριθμός. Δείξτε ότι οι πολλαπλασιαστικές ομάδες $U(\, \mathbb{Z}_p \,)$ και $U(\, \mathbb{Z}_{2p} \,)$ είναι ισόμορφες.

4.6 Κυκλικές Ομάδες

Μια ομάδα που παράγεται από ένα στοιχείο ονομάζεται κυκλική. Σ' αυτή την παράγραφο αφού ταξινομήσουμε όλες τις κυκλικές ομάδες θα μελετήσουμε τη δομή τους και θα δούμε ότι αυτή καθορίζεται πλήρως από την τάξης τους. Εφαρμογή αυτού του αποτελέσματος θα μας οδηγήσει στη λύση προβλημάτων της Θεωρίας Αριθμών. Ένας λόγος που αυτές οι ομάδες θεωρούνται σημαντικές είναι γιατί εμφανίζονται σαν υποομάδες μέσα σε κάθε ομάδα αφού κάθε στοιχείο μιας ομάδας παράγει μια υποομάδα που είναι κυκλική.

Έχουμε ήδη συναντήσει αρκετά παραδείγματα κυκλικών ομάδων. Ένα από αυτά είναι η προσθετική ομάδα $\mathbb{Z}$ των ακέραιων που παράγεται από το 1 (ή από το -1). Ένα άλλο είναι η προσθετική ομάδα $\mathbb{Z}_n$ των κλάσεων υπολοίπων $\bmod n$ που παράγεται από την κλάση $1 \bmod n$. Επίσης, η πολλαπλασιαστική ομάδα $\mathcal{E}_n$ των n-οστών ριζών της μονάδας είναι κυκλική.

Αν $G = \langle x \rangle$ είναι μια κυκλική ομάδα που παράγεται από ένα στοιχείο x, τότε κάθε στοιχείο της y είναι μια δύναμη x^r, $r \in \mathbb{Z}$ του x. Διακρίνουμε δύο περιπτώσεις. Μια περίπτωση είναι όλες οι δυνάμεις του x ανά δύο να είναι διάφορες, οπότε η G έχει άπειρο πλήθος στοιχεία και λέγεται ***άπειρη κυκλική ομάδα***. Συμβολίζεται δε με C_∞. Η άλλη περίπτωση είναι για κάποιους $r, s \in \mathbb{Z}$ να έχουμε $x^r = x^s$. Τότε $x^{r-s} = 1$ (υποθέτουμε $r > s$). Από το Αξίωμα του Ελαχίστου, το σύνολο $\{\, r \in \mathbb{N} \mid x^r = 1 \,\}$ έχει έναν ελάχιστο θετικό ακέραιο n. Σ' αυτή την περίπτωση, η G είναι το σύνολο $\{\, 1, x, x^2, \ldots, x^{n-1} \,\}$ με

$$x^r x^s = \begin{cases} x^{r+s} & \text{αν } r+s < n \\ x^{r+s-n} & \text{αν } r+s \geq n \end{cases}$$

και λέγεται ***πεπερασμένη κυκλική ομάδα*** τάξης n. Συμβολίζεται δε με C_n. Πράγματι, αφ' ενός τα n στοιχεία $1, x, \ldots, x^{n-1}$ είναι ανά δύο διάφορα (γιατί αν $x^r = x^s$ με $0 \leq s < r < n$, τότε $x^{r-s} = 1$ που είναι άτοπο, καθώς $r - s < n$), αφ' ετέρου για κάθε στοιχείο x^k, $x \in \mathbb{Z}$, της G υπάρχει κάποιο $i = 0, 1, \ldots, n-1$, τέτοιο ώστε $x^k = x^i$ (αν $k = n\,s + v$ με $0 \leq v < n$, τότε $x^k = (x^n)^s x^v = x^v$).

Τέλος παρατηρούμε ότι αν $m > n$, τότε $x^m = x^{m-n}$ και ότι η τάξη του στοιχείου x είναι ίση με την τάξη της G.

4.6.1 Θεώρημα. *(Ταξινόμησης Κυκλικών Ομάδων). Κάθε κυκλική ομάδα G είναι ισόμορφη με την προσθετική ομάδα $\mathbb{Z}_n$ των κλάσεων υπολοίπων modulo n για κάποιο $n = 0, 1, \ldots$. Συγκεκριμένα, αν $G = C_n$, για κάποιο θετικό ακέραιο n, τότε $C_n \cong \mathbb{Z}_n$ και αν $G = C_\infty$, τότε $C_\infty \cong \mathbb{Z}_0 = \mathbb{Z}$.*

Απόδειξη. Έστω $C_\infty = \langle x \rangle$. Θεωρούμε την αντιστοιχία

$$\phi : C_\infty \longrightarrow \mathbb{Z}, \quad x^r \longrightarrow r.$$

Από τον ορισμό της ϕ αυτή είναι απεικόνιση και μάλιστα $1-1$ και επί. Επιπλέον ισχύει $\phi(x^{r_1}x^{r_2}) = \phi(x^{r_1+r_2}) = r_1 + r_2 = \phi(x^{r_1}) + \phi(x^{r_2})$. Άρα η ϕ είναι ένας ισομορφισμός. Θεωρούμε τώρα την πεπερασμένη κυκλική ομάδα $C_n = \{1, x, \ldots, x^{n-1}\}$ τάξης $n \geq 1$. Πάλι εδώ η αντιστοιχία

$$\phi : C_n \longrightarrow \mathbb{Z}_n, \quad x^r \longrightarrow r \bmod n$$

από τον ορισμό της είναι μια $1-1$ και επί απεικόνιση, αφού
$\mathbb{Z}_n = \{0 \bmod n, 1 \bmod n, \ldots, (n-1) \bmod n\}$. Επιπλέον έχουμε

$$\begin{aligned}
\phi(x^{r_1}x^{r_2}) &= \begin{cases} \phi(x^{r_1+r_2}) & \text{αν} \quad r_1 + r_2 < n \\ \phi(x^{r_1+r_2-n}) & \text{αν} \quad r_1 + r_2 \geq n \end{cases} \\
&= \begin{cases} (r_1 + r_2) \bmod n & \text{αν} \quad r_1 + r_2 < n \\ (r_1 + r_2 - n) \bmod n & \text{αν} \quad r_1 + r_2 \geq n \end{cases} \\
&= (r_1 + r_2) \bmod n \\
&= r_1 \bmod n + r_2 \bmod n \\
&= \phi(x^{r_1}) + \phi(x^{r_2}).
\end{aligned}$$

Επομένως $C_n \cong \mathbb{Z}_n$. ⊤

4.6.2 Παράδειγμα. Έστω $n = 12$. Η κυκλική ομάδα C_{12} μπορεί να θεωρηθεί ότι είναι η $\mathbb{Z}_{12}$ ή η $\mathcal{E}_{12}$ ή η $U(\mathbb{Z}_{13})$ ή η ομάδα όλων των στροφών ενός δωδεκάγωνου (που είναι υποομάδα της D_{12} δείκτου 2), δηλαδή αυτή που αποτελείται από τις στροφές κατά γωνία 0, $30°$, $60°$, $\ldots$, $330°$.

Τα στοιχεία όλων αυτών των ομάδων μπορούν να ταυτισθούν με τις κορυφές ενός κυρτού κανονικού δωδεκαγώνου.

Σχήμα 4.6.1

Η κορυφή k, για την $\mathbb{Z}_{12}$, παριστά την κλάση $k \bmod 12$, για την $\mathcal{E}_{12}$ τη δωδέκατη ρίζα $e^{2k\pi i/12}$, για την $U(\mathbb{Z}_{13})$ την κλάση $2^k \bmod 13$, για τις στροφές την $A(30^\circ)^k$ και για τις μεταθέσεις την $(\,0\,1\,2\,\ldots\,11)^k$. Εδώ έχουμε θεωρήσει τους γεννήτορες $1 \bmod 12$, $e^{2\pi i/12}$, $2 \bmod 13$, $A(30^\circ)$ και $(\,0\,1\,2\,\ldots\,11\,)$, αντίστοιχα των εν λόγω ομάδων. Αρχίζοντας από την κορυφή 0, για την ομάδα $\mathbb{Z}_{12}$, για να πάμε στην κορυφή k, προσθέτουμε k φορές το γεννήτορα $1 \bmod 12$ στο 0, ενώ για την ομάδα, $U(\mathbb{Z}_{13})$ πολλαπλασιάζουμε k φορές το γεννήτορα $2 \bmod 13$. Μ' αυτόν τον τρόπο παίρνουμε όλες τις κορυφές του δωδεκαγώνου.

Οι Υποομάδες μιας Κυκλικής Ομάδας

Τώρα θα μελετήσουμε τη δομή όλων των υποομάδων μιας κυκλικής ομάδας και θα δούμε ότι το αντίστροφο του Θεωρήματος του Lagrange, που δεν ισχύει γενικά, ισχύει για τις πεπερασμένες κυκλικές ομάδες.

Έστω H μια υποομάδα μιας κυκλικής ομάδας $G = \langle\, g \,\rangle$ (άπειρης ή πεπερασμένης). Αν $h \in H$, τότε $h = g^k$, για κάποιο $k \in \mathbb{Z}$, οπότε και $h^{-1} = g^{-k} \in H$. Αυτό σημαίνει ότι η H περιέχει δυνάμεις g^t του g με $t \in \mathbb{N}$. Έστω m ο μικρότερος θετικός ακέραιος αριθμός, για τον οποίο $g^m \in H$. Τότε κάθε στοιχείο της H είναι της μορφής $(g^m)^s,\ s \in \mathbb{Z}$. Πράγματι, αν $g^k \in H$, διαιρώντας το k με το m, έχουμε $k = ms + v,\ 0 \le v < m$, οπότε $g^k = (g^m)^s g^v$ ή ισοδύναμα $g^v = g^k (g^{-m})^s$. Αλλά g^k, $(g^{-m})^s \in H$ και συνεπώς $g^v \in H$. Από την υπόθεση που κάναμε για το m, το g^v είναι στοιχείο της H μόνον αν $v = 0$. Αυτό σημαίνει ότι όλα τα στοχεία της H είναι της μορφής $(g^m)^s,\ s \in \mathbb{Z}$. Δηλαδή η H είναι η κυκλική ομάδα $H = \langle\, g^m \,\rangle$ που παράγεται από το στοιχείο g^m. Άρα κάθε υποομάδα μιας κυκλικής ομάδας είναι κυκλική.

Στην περίπτωση που η G είναι άπειρη, το προηγούμενο αποτέλεσμα μας επιτρέπει να αποδείξουμε τον εξής ισχυρισμό: Υπάρχει $1-1$ και επί αντιστοιχία μεταξύ του συνόλου των φυσικών αριθμών $\mathbb{N}$ και των υποομάδων της G, η αντιστοιχία αυτή είναι $k \longrightarrow \langle\, g^k \,\rangle$. Αυτή είναι $1-1$, διότι αν $k_1 \neq k_2$ τότε $\langle\, g^{k_1} \,\rangle \neq \langle\, g^{k_2} \,\rangle$. Τώρα αν H είναι μια υποομάδα της G, όπως δείξαμε υπάρχει κάποιος φυσικός αριθμός k τέτοιος ώστε $H = \langle\, g^k \,\rangle$ και άρα η εν λόγω αντιστοιχία είναι επί. Με άλλα λόγια για την άπειρη κυκλική ομάδα $G = \langle\, g \,\rangle$ οι υποομάδες $\langle\, g^k \,\rangle$, $k \in \mathbb{N}$, είναι ακριβώς όλες οι υποομάδες της G. Έτσι, στην προκειμένη περίπτωση, όλες οι μη-τετριμμένες υποομάδες της G είναι ισόμορφες με την ίδια την G (γιατί;).

Στην περίπτωση που η G είναι πεπερασμένης τάξης n, τότε η αντιστοιχία $k \longrightarrow \langle\, g^{n/k} \,\rangle$ είναι μία $1-1$ και επί αντιστοιχία μεταξύ όλων των διαιρετών του n και όλων των υποομάδων της G. Πράγματι, αν $k \mid n$, η υποομάδα που παράγεται από το $g^{n/k}$ έχει τάξη ίση με $\frac{n}{\text{μ.κ.δ.}(n,n/k)} = k$ (βλ. Πρόταση 4.3.11).

Επομένως για δύο διαφορετικούς διαιρέτες του n οι αντίστοιχες υποομάδες είναι διακεκριμένες αφού έχουν διαφορετικές τάξεις.

Τώρα αν H είναι μια υποομάδα της G, όπως είδαμε προηγουμένως, αυτή πρέπει να παράγεται από μια δύναμη g^m του g. Ισχυριζόμαστε ότι $m = n/k$, για κάποιο διαιρέτη k του n. Έστω k η τάξη της H. Τότε $(g^m)^k = 1$ και άρα ο $n \mid mk$, δηλαδή $mk = \lambda n$, $\lambda \in \mathbb{N}$. Από το Θεώρημα 4.4.22, έπεται ότι $k \mid n$ και συνεπώς έχουμε $mk = \lambda n = \lambda \left(\frac{n}{k}\right) k$, οπότε $m = \lambda \frac{n}{k}$. Επομένως $g^m = (g^{n/k})^\lambda$. Αυτό σημαίνει ότι η $H \leq \langle\, g^{n/k} \,\rangle$. Επειδή όμως $|H| = k = |\langle\, g^{n/k} \,\rangle|$, τελικά έχουμε $H = \langle\, g^{n/k} \,\rangle$. Με άλλα λόγια, αυτό που δείξαμε είναι ότι για κάθε διαιρέτη k της τάξης της G υπάρχει μια μοναδική υποομάδα τάξης k και αυτή είναι η $\langle\, g^{n/k} \,\rangle$. Ας παρατηρηθεί εδώ ότι ο n/k είναι ο μικρότερος φυσικός αριθμός μεταξύ όλων των φυσικών m για τους οποίους $g^m \in \langle\, g^{n/k} \,\rangle$.

Γεννάται τώρα το εξής εύλογο ερώτημα: Ποιά άλλα στοιχεία της $\langle\, g^{n/k} \,\rangle$, εκτός από το $g^{n/k}$, παράγουν την $\langle\, g^{n/k} \,\rangle$. Για παράδειγμα, αν $G = \mathbb{Z}_{12}$ και $H = \langle\, 3 \bmod 12 \,\rangle = \{\, 0 \bmod 12, 3 \bmod 12, 6 \bmod 12, 9 \bmod 12 \,\}$ τότε εύκολα βλέπουμε ότι και το στοιχείο $9 \bmod 12$ παράγει την H.

Γνωρίζουμε (βλέπε Πρόταση 4.3.11 (ii)) ότι

$$\langle\, g^m \,\rangle = \langle\, g^{n/k} \,\rangle \text{ αν και μόνον αν } k = \frac{n}{\text{μ.κ.δ.}(m,n)}.$$

Δηλαδή $\text{μ.κ.δ}(m,n) = \text{μ.κ.δ.}\,(n/k, n) = n/k$. Αυτό σημαίνει ότι οι δυνάμεις g^m είναι γεννήτορες της $\langle\, g^{n/k} \,\rangle$ για όλους τους m, $1 \leq m \leq n$, που ικανοποιούν την συνθήκη $\text{μ.κ.δ.}(m,n) = n/k$. Γράφοντας αυτούς τους m στη μορφή $m = \frac{n}{k}\lambda$ έχουμε $1 \leq \lambda \leq k$ και $\text{μ.κ.δ}(m,n) = \text{μ.κ.δ}\left(\lambda\frac{n}{k}, \frac{n}{k}k\right) = n/k$, δηλαδή $\text{μ.κ.δ.}(\lambda, k) = 1$. Αντίστροφα, αν $1 \leq \lambda \leq k$ και $\text{μ.κ.δ.}(\lambda,k) = 1$ έχουμε $n/k = \frac{n}{k}\text{μ.κ.δ}(\lambda,k) = \text{μ.κ.δ}\left(\frac{n}{k}\lambda, n\right)$, δηλαδή ο $g^{\frac{n}{k}\lambda}$ είναι ένας γεννήτορας της $\langle\, g^{n/k} \,\rangle$. Το πλήθος αυτών είναι $\varphi(k)$ όπου φ είναι η συνάρτηση του Euler, αφού αυτό το πλήθος είναι το πλήθος των λ, $1 \leq \lambda \leq k$ με $\text{μ.κ.δ}(\lambda,k) = 1$. Ιδιαίτερα, από αυτό προκύπτει ότι μια δύναμη g^m του g είναι γεννήτορας της $\langle\, g \,\rangle$ αν και μόνον αν $\text{μ.κ.δ}(m,n) = 1$ και το πλήθος αυτών είναι $\varphi(n)$. Ας σημειωθεί ότι ο $\varphi(n)$ είναι η τάξη της ομάδας $U(\mathbb{Z}_n)$ των αντιστρέψιμων στοιχείων του δακτυλίου Z_n. Αυτά τα στοιχεία, όπως είδαμε μόλις πριν, είναι οι γεννήτορες της ομάδας $\mathbb{Z}_n$.

Τέλος, έστω H μια υποομάδα μιας κυκλικής ομάδας $G = \langle\, g \,\rangle$ (πεπερασμένης ή άπειρης). Θεωρούμε το μικρότερο φυσικό αριθμό m για τον οποίο $g^m \in H$. Για κάθε $t \in \mathbb{Z}$, υπάρχουν μοναδικοί ακέραιοι s και v τέτοιοι ώστε $t = s\,m + v$, $0 \leq v \leq m-1$. Αυτό δείχνει ότι ένα οποιοδήποτε στοιχείο $g^t = (g^m)^s g^v$ της $\langle\, g \,\rangle$ έχει μια μοναδική παράσταση της μορφής $g^t = u g^\beta$ με $u \in \langle\, g^m \,\rangle$, $0 \leq \beta \leq n-1$.

Συνεπώς η ανάλυση της $G = \langle g \rangle$ ως προς την $\langle g^m \rangle$ είναι η

$$G = \langle g^m \rangle \cup g\langle g^m \rangle \cup \cdots \cup g^{m-1}\langle g^m \rangle.$$

Επιπλέον υπάρχει μια $1-1$ αντιστοιχία μεταξύ των αριστερών κλάσεων mod $\langle g^m \rangle$ και των κλάσεων υπολοίπων mod$m$.

Συνοψίζουμε τα προηγούμενα αποτελέσματα στο επόμενο θεώρημα το οποίο θα ονομάζουμε ***Θεώρημα δομής των κυκλικών ομάδων***.

4.6.3 Θεώρημα. *Έστω G μια κυκλική ομάδα που παράγεται από ένα στοιχείο g. Τότε ισχύουν τα εξής.*

α) Κάθε υποομάδα της G είναι κυκλική.

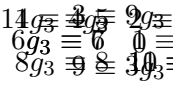
β) Αν η G είναι άπειρη, οι μόνες υποομάδες της είναι της μορφής $\langle g^m \rangle$, $m \in \mathbb{N}$. Όλες αυτές είναι διακεκριμένες, έχουμε δε $|\langle g \rangle : \langle g^m \rangle| = m$, δηλαδή ο δείκτης μιας μη-τετριμμένης υποομάδας της G στην G είναι πάντα πεπερασμένος.

γ) Αν η G είναι πεπερασμένη τάξης n, τότε για κάθε διαιρέτη k του n υπάρχει μια μοναδική υποομάδα της G τάξης k. Επιπλέον, αυτή είναι η $\langle g^{n/k} \rangle$, η οποία έχει δείκτη $|\langle g \rangle : \langle g^{n/k} \rangle| = n/k$. Ένα στοιχείο της $\langle g^{n/k} \rangle$ είναι γεννήτοράς της αν και μόνον αν αυτό ανήκει στο σύνολο

$$\{\, (g^{n/k})^\lambda \mid 1 \leq \lambda \leq k,\ \mu.\kappa.\delta.(\lambda, k) = 1 \,\}.$$

Συνεπώς, το πλήθος των γεννητόρων της είναι $\varphi(k)$. Ιδιαίτερα, το πλήθος των γεννητόρων της G είναι $\varphi(n)$ και μια δύναμη g^m του g είναι γεννήτορας αν και μόνον αν $\mu.\kappa.\delta(m, n) = 1$, όπου φ είναι η συνάρτηση του Euler.

4.6.4 Παράδειγμα. Στο προηγούμενο παράδειγμα είχαμε ταυτίσει τα στοιχεία της κυκλικής ομάδας $\mathbb{Z}_{12}$ με τις κορυφές ενός δωδεκάγωνου. Από το Θεώρημα 4.6.3, έπεται ότι οι γεννήτορες της $\mathbb{Z}_{12}$ είναι τα στοιχεία $g_1 = 1 \bmod 12$,, $g_2 = 5 \bmod 12$, $g_3 = 7 \bmod 12$ και $g_4 = 11 \bmod 12$. Για το δωδεκάγωνο αυτό σημαίνει ότι αν θεωρήσουμε έναν γεννήτορα g_i τότε κάθε κορυφή του είναι ένα πολλαπλάσιο του g_i. Η σειρά με την οποία παίρνουμε τις κορυφές εξαρτάται από το g_i. Αρχίζοντας από το 0 η επόμενη κορυφή είναι η g_i, μετά η κορυφή $2g_i$ και ούτω καθ' εξής. Έτσι, αν $i = 3$, το δωδεκάγωνο που θα προκύψει είναι αυτό στο Σχήμα.



Σχήμα 4.6.2

Οι διαιρέτες 2, 3, 4 και 6 καθορίζουν τις υποομάδες της $\mathbb{Z}_{12}$. Για καθένα από αυτούς υπάρχει μόνο μια υποομάδα της $\mathbb{Z}_{12}$ με την αντίστοιχη τάξη. Για το δωδεκάγωνο αυτό σημαίνει ότι τα μόνα κανονικά πολύγωνα που οι κορυφές τους είναι κορυφές του δωδεκαγώνου αρχίζοντας από το 0 είναι το ευθύγραμμο τμήμα $\{\,0,\,6\,\}$, το τρίγωνο $\{\,0,\,4,\,8\,\}$, το τετράγωνο $\{\,0,\,3,\,6,\,9\,\}$ και το εξάγωνο $\{\,0,\,2,\,4,\,6,\,8,\,10\,\}$. Αυτά καθορίζονται από τις υποομάδες $H_1 = \langle\, 6 \bmod 12 \,\rangle$, $H_2 = \langle\, 4 \bmod 12 \,\rangle$, $H_3 = \langle\, 3 \bmod 12 \,\rangle$ και $H_4 = \langle\, 2 \bmod 12 \,\rangle$.

4.6.5 Πόρισμα. *Για κάθε θετικό ακέραιο n ισχύει*

$$\sum_{k|n} \varphi(k) = n$$

όπου το k διατρέχει όλους τους θετικούς διαιρέτες του n.

Απόδειξη. Έστω $G = \langle\, g \,\rangle$ μια κυκλική ομάδα τάξης n. Για κάθε διαιρέτη k του n θεωρούμε το σύνολο $H_k = \left\{ \left(g^{n/k}\right)^{\lambda} \mid 1 \le \lambda \le k, \mu.κ.δ(\lambda, k) = 1 \right\}$. Προφανώς $|\, H_k \,| = \varphi(k)$. Από το Θεώρημα 4.6.3 έπεται ότι η ένωση $\bigcup_{k|n} H_k$ είναι διακεκριμένη και εξαντλεί την G, αφού αν $h \in G$, με $|\langle\, h \,\rangle| = s$, τότε θα πρέπει $h = \left(g^{n/s}\right)^{\lambda}$, για κάποιο λ, $1 \le \lambda \le s$ και $\mu.κ.δ(\lambda, s) = 1$, δηλαδή $h \in H_s$. Συνεπώς $|\, G \,| = \sum_{k|n} |\, H_k \,| = \sum_{k|n} \varphi(k)$. ⊺

4.6.6 Θεώρημα. *Μια πεπερασμένη ομάδα G τάξης n είναι κυκλική αν και μόνον αν για κάθε διαιρέτη k του n υπάρχει το πολύ μια κυκλική υποομάδα της G που έχει τάξη k.*

Απόδειξη. Αν η G είναι κυκλική τότε από το Θεώρημα 4.6.3 έπεται ότι για κάθε διαιρέτη k του n υπάρχει ακριβώς μια κυκλική υποομάδα της G τάξης k.

Αντίστροφα, κάθε στοιχείο της G έχει κάποια τάξη s που διαιρεί το n. Αλλά από την υπόθεση υπάρχει το πολύ μια κυκλική υποομάδα τάξης s και συνεπώς υπάρχει ακριβώς μια, αυτή που παράγεται από το στοιχείο τάξης s. Οπότε αν k είναι ένας διαιρέτης του n ή δεν υπάρχει κανένα στοιχείο τάξης k ή υπάρχουν ακριβώς $\varphi(k)$ το πλήθος στοιχεία τάξης k, από το Θεώρημα 4.6.3 γ) . Αλλά από το Πόρισμα 4.6.5 έχουμε ότι $|G| = n = \sum_{k|n} \varphi(k)$. Επομένως δεν μπορεί να μην υπάρχει ένα στοιχείο τάξης k για κάθε διαιρέτη k του n, διότι διαφορετικά θα είχαμε $|G| < \sum_{k|n} \varphi(k)$. Άρα, για το n, ως διαιρέτης του εαυτού του, υπάρχει στοιχείο τάξης n (και μάλιστα υπάρχουν $\varphi(n)$ τέτοια στοιχεία) και συνεπώς η G είναι κυκλική. ⊺

Έστω τώρα $G_1, G_2, \ldots, G_k$ k το πλήθος ομάδες. Στο παράδειγμα 4.3.5 (10) είχαμε θεωρήσει το καρτεσιανό γινόμενο $G = G_1 \times G_2 \times \cdots \times G_k$ στο οποίο ορίζεται η πράξη

$$(g_1, \ldots, g_k)(g_1', \ldots, g_k') = (g_1 g_1', \ldots, g_k g_k')$$

και ως προς την οποία το G είναι ομάδα. Αν οι ομάδες G_i είναι κυκλικές τότε γενικά η ομάδα G δεν είναι κυκλική. Παραδείγματος χάρη, οι ομάδες $\mathbb{Z} \times \mathbb{Z}$ και $\mathbb{Z}_3 \times \mathbb{Z}_3$ δεν είναι κυκλικές ομάδες (γιατί;). Ισχύει όμως το εξής.

4.6.7 Θεώρημα. *Η ομάδα $G = C_{m_1} \times C_{m_2} \times \cdots \times C_{m_k}$ είναι κυκλική ομάδα τάξης m, όπου $m = m_1 \cdot \cdots \cdot m_k$, αν και μόνο αν μ.κ.δ.$(m_i, m_j) = 1$ για κάθε $i \leq i, j \leq k$ με $i \neq j$. Σ' αυτή την περίπτωση ένα στοιχείο $g = (g_1, \ldots, g_k)$ της G είναι γεννήτορας αν και μόνον αν το g_i, $i = 1, \ldots, k$, είναι γεννήτορας της C_{m_i}.*

Απόδειξη. Η τάξη της G είναι ίση με $m = m_1 m_2 \cdots m_k$. Έστω ότι για κάθε $1 \leq i, j \leq k$ ισχύει μ.κ.δ.$(m_i, m_j) = 1$ και έστω $C_{m_i} = \langle g_i \rangle$. Θεωρούμε το στοιχείο $g = (g_1, \ldots, g_k)$. Επειδή $|G| = m$, ισχύει $g^m = (1, \ldots, 1)$. Αν n είναι η τάξη του g, πρέπει $n \mid m$. Αλλά, επειδή $g^n = (g_1^n, \ldots, g_k^n) = (1, \ldots, 1)$, δηλαδή $g_i^n = 1$, $i = 1, \ldots, k$, πρέπει $m_i \mid n$, $i = 1, \ldots, k$. Συνεπώς θα πρέπει $m \mid n$, αφού μ.κ.δ.$(m_i, m_j) = 1$, $1 \leq i, j \leq k$. Άρα $m = n$. Δηλαδή το στοιχείο g είναι γεννήτορας της G και άρα $G \cong C_m$.

Αντίστροφα, υποθέτουμε ότι η G είναι κυκλική και έστω $g = (g_1, \ldots, g_k)$ ένας γεννήτορας. Τότε κάθε στοιχείο της είναι της μορφής $g^\lambda = (g_1^\lambda, \ldots, g_k^\lambda)$.

Αυτό σημαίνει ότι κάθε στοιχείο της C_{m_i} είναι της μορφής g_i^{λ}, δηλαδή το g_i είναι γεννήτορας της C_{m_i} και άρα είναι τάξης m_i. Καθώς η ομάδα G είναι Αβελιανή, η τάξη του $g = (g_1, \ldots, g_k) = (g_1, 1, \ldots, 1)(1, g_2, \ldots, 1)(1, \ldots, 1, g_k)$ είναι το ε.κ.π.$(m_1, m_2, \ldots, m_k)$ (βλέπε Άσκηση 4.6.7). Αλλά υποθέσαμε ότι το g είναι γεννήτορας της G και άρα η τάξη του είναι m. Συνεπώς $m = m_1 \cdots m_k =$ ε.κ.π.$(m_1, \ldots, m_k)$. Από τον ορισμό του ε.κ.π. προκύπτει τελικά ότι τα $m_i \;\; i = 1, \ldots, k$ πρέπει να είναι ανά δύο πρώτα μεταξύ τους. ⊤

4.6.8 Εφαρμογές.

1. Επειδή όλες οι κυκλικές ομάδες τάξης n είναι ισόμορφες με την προσθετική ομάδα $\mathbb{Z}_n$ των κλάσεων υπολοίπων modulo n, είναι αναμενόμενο τα προηγούμενα αποτελέσματα να έχουν εφαρμογές στη θεωρία αριθμών. Έτσι, αν ένας φυσικός αριθμός k διαιρεί τον n τότε από το Θεώρημα 4.6.3 γ) προκύπτει ότι η μοναδική υποομάδα της $\mathbb{Z}_n$ που έχει τάξη k είναι το σύνολο $\{\, x \bmod n \mid kx \equiv 0 \bmod n \,\}$ (γιατί;). Με άλλα λόγια αυτό σημαίνει ότι η εξίσωση $kx \equiv 0 \bmod n$ έχει ακριβώς k λύσεις modulo n. Πιο γενικά, αν $k \in \mathbb{N}$, τότε το σύνολο των λύσεων της εξίσωσης $kx \equiv 0 \bmod n$ είναι ακριβώς το σύνολο των λύσεων της $\delta x \equiv 0 \bmod n$, όπου $\delta =$ μ.κ.δ.(k, n). Δηλαδή ισχύει $kx \equiv 0 \bmod n$ αν και μόνον αν $\delta x \equiv 0 \bmod n$. Πράγματι, η $\delta x \equiv 0 \bmod n$ δίνει $kx \equiv 0 \bmod n$ αφού $\delta \mid k$. Επίσης υπάρχουν $s, t \in \mathbb{Z}$ τέτοια ώστε $\delta = sn + tk$ και άρα $\delta x \equiv (snx + tkx) \bmod n = tkx \bmod n$. Άρα η εξίσωση $kx \equiv 0 \bmod n$ δίνει $\delta x \equiv 0 \bmod n$.

Επίσης η πολλαπλασιαστική ιδιότητα της συνάρτησης φ του Euler (βλ. Παράγραφο 1.6) προκύπτει άμεσα εφαρμόζοντας τα 4.6.3 και 4.6.7. Πράγματι, από το 4.6.3, το πλήθος των γεννητόρων της κυκλικής ομάδας C_m είναι ίσο με $\varphi(m)$. Άρα το πλήθος αυτό είναι ίσο με το γινόμενο $\varphi(m_1)\varphi(m_2)\cdots\varphi(m_k)$ αν και μόνον αν $C_m \cong C_{m_1} \times \cdots \times C_{m_k}$ που αυτό ισχύει αν και μόνον αν $(m_i, m_j) = 1$, $1 \le i, j \le k$, από το 4.6.7.

Μια άλλη εφαρμογή του Θεωρήματος 4.6.7 είναι το Κινέζικο Θεώρημα (Άσκηση 2.6 (20)) για την ύπαρξη λύσης ενός συστήματος ισοτιμιών της μορφής $x = \alpha_i \bmod m_i, \;\; i = 1, \ldots, k$, όπου $\alpha_i \in \mathbb{Z}$ και $(m_i, m_j) = 1, \;\; i \le i, j \le k$. Πράγματι, αν θεωρήσουμε τις κυκλικές ομάδες $\mathbb{Z}_{m_i}, \;\; i = 1, \ldots, k$, τότε από το 4.6.7, το στοιχείο $x_0 = (1 \bmod m_1, \ldots, 1 \bmod m_k)$ είναι ένας γεννήτορας της κυκλικής ομάδας $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$. Συνεπώς το στοιχείο $(\alpha_1 \bmod m_1, \ldots, \alpha_k \bmod m_k)$ είναι ένα πολλαπλάσιο (δηλαδή μια δύναμη) λx_0 του x_0, δηλαδή $\lambda x_0 = (\lambda \bmod m_1, \ldots, \lambda \bmod m_k) = (\alpha_1 \bmod m_1, \ldots, \alpha_k \bmod m_k)$. Συνεπώς $\lambda \equiv \alpha_i \bmod m_i, \;\; i = 1, 2, \ldots, k$.

2. Στη δεύτερη Ενότητα είδαμε αφενός ότι για κάθε πρώτο αριθμό p ο δακτύλιος $\mathbb{Z}_p$ είναι σώμα και αφετέρου ότι κάθε πεπερασμένο σώμα F περιέχει ένα υπόσωμα που είναι ισόμορφο με το $\mathbb{Z}_p$ για κάποιο πρώτο p. Συνεπώς

μπορούμε να υποθέσουμε ότι $\mathbb{Z}_p \leq F$ και έτσι το σώμα F να θεωρηθεί ένας διανυσματικός χώρος πεπερασμένης διάστασης επί του $\mathbb{Z}_p$, έστω n (αφού το F είναι πεπερασμένο). Αν $v_1, \ldots, v_n$ είναι μια βάση του F επί του $\mathbb{Z}_p$ τότε έχουμε το ευθύ άθροισμα

$$F = \mathbb{Z}_p v_1 \oplus \cdots \oplus \mathbb{Z}_p v_n$$

όπου $\mathbb{Z}_p v_i$ είναι ο μονοδιάστατος υπόχωρος που παράγεται από το διάνυσμα v_i, $i = 1, 2, \ldots, n$. Επίσης ο $\mathbb{Z}_p v_i$ είναι η κυκλική υποομάδα της προσθετικής ομάδας F που παράγεται από το στοιχείο v_i του F και έχει τάξη p. Είναι τώρα φανερό ότι το σώμα F έχει p^n στοιχεία. Σημειώνουμε, ότι αν ο $n \neq 1$ τότε η προσθετική ομάδα F δεν μπορεί να είναι κυκλική, καθώς κάθε μη μηδενικό στοιχείο του F έχει τάξη p (γιατί;) και η F έχει περισσότερα από p στοιχεία.

Τώρα θα δείξουμε ότι η πολλαπλασιαστική ομάδα F^* του F είναι μια κυκλική ομάδα τάξης $p^n - 1$. Γι' αυτό θα δώσουμε δύο αποδείξεις γιατί θεωρούμε ότι η κάθε μια έχει ξεχωριστή αξία καθότι η μια είναι άμεση συνέπεια του 4.6.6 ενώ η άλλη αποκαλύπτει περισσότερα στοιχεία για τη δομή της F^* που είναι Αβελιανή αλλά γενικά δεν είναι κυκλική όταν το F είναι άπειρο σώμα.

Η πρώτη απόδειξη δίνει κάτι περισσότερο από αυτό που θέλουμε να δείξουμε. Ισχυριζόμαστε ότι αν F είναι ένα οποιοδήποτε σώμα (άπειρο ή πεπερασμένο) τότε κάθε πεπερασμένη υποομάδα της πολλαπλασιαστικής ομάδας F^* είναι κυκλική (κάτι ανάλογο είχαμε δει στο Παράδειγμα 4.3.5 (8) για το σώμα των μιγαδικών $\mathbb{C}$). Πράγματι, έστω G μια τέτοια ομάδα τάξης, έστω m. Αν $\alpha \in G$ με $\alpha^k = 1$ όπου $k \mid m$, τότε το α είναι μια ρίζα του πολυωνύμου $x^k - 1 \in F[x]$. Το $x^k - 1$ όμως έχει το πολύ k ρίζες στο F. Συνεπώς για κάθε διαιρέτη k του m υπάρχει το πολύ μια κυκλική υποομάδα τάξης k και άρα από το Θεώρημα 4.6.6 η G είναι κυκλική. Στην περίπτωση που η ίδια η F^* είναι πεπερασμένη, αυτή πρέπει να είναι κυκλική.

Στη δεύτερη απόδειξη η επιχειρηματολογία είναι η εξής. Κατ' αρχήν, για κάθε διαιρέτη k του $p^n - 1$ η εξίσωση $x^k - 1$ έχει ακριβώς k λύσεις στην $\mathbb{F}^*$. Πράγματι, ισχύει η ταυτότητα

$$x^{p^n - 1} - 1 = (x^k - 1)(x^{k(\lambda-1)} + x^{k(\lambda-2)} + \cdots + x^k + 1)$$

όπου $p^k - 1 = k\lambda$. Το πολυώνυμο $x^{k(\lambda-1)} + \cdots + x^k + 1$ έχει το πολύ $k\lambda - k$ μη μηδενικές λύσεις στο $\mathbb{F}^*$ και από την 2.7.9 το πολυώνυμο $x^{p^n-1} - 1$ έχει ακριβώς $p^n - 1$ λύσεις στην $\mathbb{F}^*$. Άρα το πολυώνυμο $x^k - 1$ έχει τουλάχιστον k μη μηδενικές λύσεις στο F, οπότε έχει k ακριβώς λύσεις. Έστω τώρα

$$p^n - 1 = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$$

η ανάλυση του $p^n - 1$ σε πρώτους. Επειδή $p_i^{n_i} \mid p^n - 1$, σύμφωνα με τα προηγούμενα η εξίσωση $x^{p_i^{n_i}} - 1 = 0$ έχει ακριβώς $p_i^{n_i}$ ρίζες στο F. Από αυτές τις ρίζες, οι

$p_i^{n_i-1}$ είναι όλες ακριβώς οι ρίζες της εξίσωσης $x^{p_i^{n_i-1}}-1=0$. Από τις υπόλοιπες ρίζες της $x^{p_i^{n_i}}-1=0$, των οποίων το πλήθος είναι $p_i^{n_i}-p_i^{n_i-1}=p_i^{n_i}\left(1-\frac{1}{p_i}\right)$, διαλέγουμε μια, έστω τη ϱ_i. Το ϱ_i είναι στοιχείο της F^* με τάξη $p_i^{n_i}$, αφού $\varrho_i^{p_i^{n_i}}=1$ και $\varrho_i^{p_i^{n_i-1}}\neq 1$. Το στοιχείο $\varrho_1\varrho_2\cdots\varrho_s$ είναι ένα στοιχείο της F^* με τάξη p^n-1 (γιατί;) και άρα η F^* είναι κυκλική.

Σημειώνουμε ότι το γινόμενο $\prod_{i=1}^{s}(p_i^{n_i}-p_i^{n_i-1})=(p^n-1)\prod_{i=1}^{s}\left(1-\frac{1}{p_i}\right)=\varphi(p^n-1)$ μας δίνει το πλήθος των δυνατών επιλογών των γινομένων $\varrho_1\varrho_2\cdots\varrho_s$, δηλαδή το πλήθος των στοιχείων της F^* που έχουν τάξη p^n-1, που είναι ακριβώς αυτό που αναφέρεται και στο Θεώρημα 4.6.3 γ).

Ισχύει και το αντίστροφο, δηλαδή: *"Αν F είναι ένα σώμα για το οποίο η πολλαπλασιαστική ομάδα F^* είναι κυκλική τότε το F είναι πεπερασμένο"*.

Πράγματι, αν η F^* είναι πεπερασμένη κυκλική, τότε και το σώμα $F=F^*\cup\{0\}$ είναι πεπερασμένο. Υποθέτουμε ότι η F^* είναι άπειρη κυκλική. Τότε το σώμα έχει χαρακτηριστική μηδέν και άρα περιέχει το σώμα των ρητών ως υπόσωμα (βλέπε Θεώρημα 2.8.7), δηλαδή η πολλαπλασιαστική ομάδα $\mathbb{Q}^*$ είναι κυκλική, σαν υποομάδα της πολαπλασιαστικής ομάδας του σώματος που έχουμε υποθέσει ότι είναι κυκλική, αυτό είναι άτοπο.

Επίσης χρησιμοποιώντας το Θεώρημα 4.6.3 γ) και βασικά στοιχεία της θεωρίας σωμάτων μπορούμε εύκολα να δείξουμε ότι εάν σε κάθε υποομάδα της πολλαπλασιαστικής ομάδας F^* ενός σώματος F με p^n στοιχεία επισυνάψουμε το μηδενικό στοιχείο 0 του F τότε παίρνουμε όλα τα υποσώματα του F που καθένα από αυτά έχει p^k στοιχεία για κάποιο διαιρέτη k του n. Όπως είδαμε στην Παράγραφο 2.7, αυτό μας λέει ότι για κάθε διαιρέτη k του n υπάρχει ένα μοναδικό υπόσωμα του F που έχει p^k στοιχεία και ότι όλα αυτά εξαντλούν όλα τα υποσώματα του F. Ιδιαίτερα το F έχει μόνο ένα υπόσωμα με p στοιχεία, το $\mathbb{Z}_p$.

3. Από το Θεώρημα 4.6.3 γ) προκύπτει ότι αν k είναι ένας διαιρέτης της τάξης μιας πεπερασμένης ομάδας $G=\langle g\rangle$ τότε η υποομάδα που έχει τάξη k είναι το υποσύνολο $\{\alpha\in G\mid \alpha^k=1\}$. Τώρα θα δείξουμε ότι αν n είναι ένας οποιοσδήποτε φυσικός αριθμός το σύνολο $G_n=\{\alpha\in G\mid \alpha^n=1\}$, που προφανώς είναι υποομάδα, έχει τάξη $\delta=$ μ.κ.δ.$(n,|G|)$ και συνεπώς $G_n=\{1,g^r,g^{2r},\ldots,g^{(\delta-1)r}\}$ όπου $|G|=\delta r$. Αυτό μας λέει ότι η εξίσωση $x^n=1$ έχει ακριβώς δ λύσεις στην G.

Έστω $\alpha\in G_n$. Από την Ευκλείδεια διαίρεση έχουμε $n=|G|\lambda+n_1$, $0\leq n_1<|G|$ και συνεπώς $\alpha^{n_1}=1$. Αν $|G|=n_1\lambda_1+n_2$, $0\leq n_2<n$ παίρνουμε $\alpha^{n_2}=1$ και προχωρώντας με τον ίδιο τρόπο, από τον αλγόριθμο του Ευκλείδη θα βρούμε ένα i για το οποίο $n_i=0$ και $\delta=n_{i-1}$ θα έχουμε λοιπόν $\alpha^\delta=1$.

Φυσικά, αν $\alpha \in G$ με $\alpha^\delta = 1$ τότε και $\alpha^n = 1$, δηλαδή $\alpha \in G_n$. Αυτό σημαίνει ότι $G_n = \{\, \alpha \in G \mid \alpha^\delta = 1 \,\} = \langle\, g^{|G|/\delta} \,\rangle = \{\, 1, g^r, g^{2r}, \ldots, g^{(\delta-1)r} \,\}$ όπου $|G| = \delta r$.

Ιδιαίτερα έστω F ένα πεπερασμένο σώμα με q στοιχεία, τότε η εξίσωση $x^n = 1$ έχει ακριβώς $\delta = \mu.κ.δ.(\, n,\, q-1\,)$ λύσεις στο F. Αυτό μας λέει επίσης ότι η τάξη του κέντρου $Z(SL_n(F))$, της ειδικής γραμμικής ομάδας των $n \times n$ πινάκων πάνω από το F, έχει τάξη δ. Πράγματι, η υποομάδα $Z(SL_n(F))$ αποτελείται από τους $n \times n$ πίνακες $\begin{pmatrix} \lambda & & \\ & \ddots & \\ & & \lambda \end{pmatrix}$ με $\lambda \in F^*$ και $\lambda^n = 1$ (βλέπε Θεώρημα 4.4.5). Συνεπώς αυτή είναι ισόμορφη με την $F_n^* = \{\, \lambda \in F^* \mid \lambda^n = 1 \,\}$ που η τάξη της όπως είδαμε είναι $\delta = (n,\, q-1)$. Άρα $|Z(SL_n(F))| = \delta$.

Ομομορφισμοί Κυκλικών Ομάδων

Η Πρόταση 4.5.6 μας λέει ότι αν G είναι μια κυκλική ομάδα που παράγεται από το στοιχείο g τότε ένας ομομορφισμός $\phi : G \longrightarrow G'$ καθορίζεται από την εικόνα $\phi(g)$ του g, ενώ η εικόνα $\mathrm{Im}\phi$ παράγεται από το στοιχείο $\phi(g)$. Αν η τάξη του $\phi(g)$ είναι άπειρη τότε $G \cong \mathrm{Im}\phi$. Αν η G είναι άπειρη και το $\phi(g)$ έχει τάξη πεπερασμένη r, τότε ο πυρήνας είναι η υποομάδα $\langle\, g^r \,\rangle$. Αν η G είναι πεπερασμένης τάξης n, τότε και η εικόνα $\mathrm{Im}\phi$ είναι πεπερασμένης τάξης και η τάξη της διαιρεί το n. Συνεπώς αν η ομάδα G' έχει στοιχεία που η τάξη τους διαιρεί την τάξη n του g αυτά είναι υποψήφιες εικόνες του g.

Για παράδειγμα, αν $G = \mathbb{Z}_{12}$ και $G' = \mathbb{Z}_{32}$ τότε εξετάζουμε τις πιθανές εικόνες του $1 \bmod 12$, δηλαδή τους πιθανούς ομομορφισμούς $\phi : \mathbb{Z}_{12} \longrightarrow \mathbb{Z}_{32}$. Αν $\phi(1 \bmod 12) = \alpha \bmod 32$, τότε $\phi(k \bmod 12) = k\alpha \bmod 32$ και η τάξη του $\alpha \bmod 32$ πρέπει να διαιρεί το 12 (Παρατήρηση 4.5.3) αλλά επίσης από το θεώρημα του Lagrange πρέπει να διαιρεί και το 32. Άρα θα πρέπει η τάξη του $\alpha \bmod 32$ να διαιρεί τον $\mu.κ.δ.(12, 32) = 4$, δηλαδή θα πρέπει να είναι 1, 2 ή 4.

Στη γενική περίπτωση, για τυχαίους θετικούς ακεραίους m και n, ο ίδιος ισχυρισμός του παραδείγματος δίνει ότι το πλήθος των διακεκριμένων ομομορφισμών $\phi : \mathbb{Z}_m \longrightarrow \mathbb{Z}_n$ είναι το άθροισμα $\sum \varphi(\delta)$, όπου δ διατρέχει όλους τους διαιρέτες του $\mu.κ.δ.(m, n) = d$ (μάλιστα από το Πόρισμα 4.6.5 έχουμε ότι $\sum \varphi(\delta) = d$).

Στο παράδειγμά μας, αν θεωρήσουμε τον ομομορφισμό που στέλνει το $1 \bmod 12$ στο $8 \bmod 32$, τότε η ομομορφική εικόνα της $\mathbb{Z}_{12}$ είναι η υποομάδα $\{\, 0 \bmod 32, 8 \bmod 32, 16 \bmod 32, 24 \bmod 32 \,\}$ της $\mathbb{Z}_{32}$ που παράγεται από το $8 \bmod 32$. Η ίδια ομομορφική εικόνα προκύπτει από τον ομομορφισμό που στέλνει το $1 \bmod 12$ στο $24 \bmod 32$.

4.6.9 Παρατήρηση. Στην ειδική περίπτωση όπου $m = n$, το πλήθος των ενδομορφισμών της ομάδας $\mathbb{Z}_m$ είναι m. Μάλιστα, το σύνολο των ενδομορφισμών αυτών, το οποίο συμβολίζουμε με $End(\mathbb{Z}_m)$, αποτελεί δακτύλιο ισόμορφο με τον $\mathbb{Z}_m$. Πράγματι, η σύνθεση ενδομορφισμών ορίζει τον πολλαπλασιασμό στο $End(\mathbb{Z}_m)$ και η πρόσθεση δύο ενδομορφισμών ϕ_1 και ϕ_2 του $\mathbb{Z}_m$ ορίζεται θέτοντας

$$(\phi_1 + \phi_2)(\alpha) = \phi_1(\alpha) + \phi_2(\alpha).$$

Επίσης, για $k \in \mathbb{Z}$, θεωρούμε τον ενδομορφισμό $\phi_k : \mathbb{Z}_m \longrightarrow \mathbb{Z}_m$, $1 \bmod m \longrightarrow k \bmod m$. Καθώς η απεικόνιση $\mathbb{Z} \longrightarrow End(\mathbb{Z}_m)$, $k \longrightarrow \phi_k$, είναι ένας επιμορφισμός δακτυλίων με πυρήνα το ιδεώδες που παράγεται από το m (γιατί;), συμπεραίνουμε ότι $\mathbb{Z}/m\mathbb{Z} \cong End(\mathbb{Z}_m)$.

Τα αντιστρέψιμα στοιχεία του δακτυλίου $End(\mathbb{Z}_n)$ είναι ακριβώς οι αυτομορφισμοί της ομάδας $\mathbb{Z}_n$. Αλλά τα αντιστρέψιμα στοιχεία του δακτυλίου $\mathbb{Z}/n\mathbb{Z}$ είναι όλες οι αντιστρέψιμες κλάσεις υπολοίπων modulo n, δηλαδή όλες οι κλάσεις $\lambda \bmod n$, $(\lambda, n) = 1$, που αποτελούν την πολλαπλασιαστική ομάδα $U_n = Aut(\mathbb{Z}_n)$. Ας παρατηρήσουμε επίσης ότι ένας αυτομορφισμός θ της $\mathbb{Z}_n$ είναι πλήρως καθορισμένος αν γνωρίζουμε την εικόνα $\theta(k \bmod n) = \lambda k \bmod n$ ενός γεννήτορα k της $\mathbb{Z}_n$, η οποία πρέπει να είναι γεννήτορας της $\mathbb{Z}_n$. Αυτό σημαίνει ότι $(\lambda, n) = 1$. Στην ειδική περίπτωση $n = 0$, η πολλαπλασιαστική ομάδα των αντιστρέψιμων στοιχείων του $End(\mathbb{Z}) \cong \mathbb{Z}$ είναι η $\{1, -1\}$ και άρα η προσθετική ομάδα των ακέραιων έχει μόνο δύο αυτομορφισμούς, τον ταυτοτικό $\mathbb{Z} \longrightarrow \mathbb{Z}$, $x \longrightarrow x$ και την απεικόνιση $\mathbb{Z} \longrightarrow \mathbb{Z}$, $x \longrightarrow -x$. Αυτό προκύπτει και από το γεγονός ότι η $\mathbb{Z}$ έχει μόνο δύο γεννήτορες το 1 και το -1.

Ενημερωτικά αναφέρουμε εδώ, και θα αποδείξουμε στην Εφαρμογή 4.8.3, ότι ο Gauss το 1801 απέδειξε ότι: Αν p είναι πρώτος διάφορος του 2 τότε για κάθε n η ομάδα U_{p^n} είναι κυκλική ισόμορφη με την $\mathbb{Z}_{p^n - p^{n-1}}$, δηλαδή $Aut(\mathbb{Z}_{p^n}) \cong \mathbb{Z}_{p^n - p^{n-1}}$. Αυτό το αποτέλεσμα είναι πολύ χρήσιμο σήμερα στην κρυπτογραφία.

Ασκήσεις 4.6

1. Έστω α ένα στοιχείο μιας ομάδας G. Αν η τάξη του α είναι 12 να βρεθούν όλα τα στοιχεία της $< \alpha >$. Να βρεθούν στην $< \alpha >$ τα στοιχεία α^{32}, α^{47}, α^{70}.

2. Υπάρχουν γνήσιες υποομάδες της S_3 που δεν είναι κυκλικές;

3. Αν κάθε γνήσια υποομάδα μιας ομάδας G, είναι κυκλική είναι η G κυκλική;

4. Έστω H_1, H_2 δύο κυκλικές υποομάδες μιας Αβελιανής ομάδας G με $| H_1 | = 10$ και $| H_2 | = 28$. Δείξτε ότι η G έχει μια κυκλική υποομάδα τάξης 140.

5. Έστω G μια κυκλική ομάδα τάξης 15. Να βρεθούν όλες οι υποομάδες της και όλες οι κλάσεις modulo H για κάθε υποομάδα H.

6. Έστω G μια πεπερασμένη ομάδα τάξης m. Έστω $g \in G$. Υποθέτουμε ότι για κάθε πρώτο διαιρέτη p του m είναι $g^{\frac{m}{p}} \neq e$. Δείξτε ότι η G είναι κυκλική παραγόμενη από το g.

7. Έστω G μια ομάδα και $a,\ b \in G$ πεπερασμένης τάξης τέτοια ώστε $a\,b = b\,a$. Υποθέτουμε ότι $\langle a \rangle \cap \langle b \rangle = 1$. Δείξτε ότι το στοιχείο $a\,b$ έχει πεπερασμένη τάξη ίση με το ε.κ.π. των τάξεων του a και b.

8. Έστω G μια κυκλική ομάδα τάξης p^n, όπου p-πρώτος και H, K υποομάδες της G. Δείξτε ότι είτε $H \subseteq K$ είτε $K \subseteq H$. Ισχύει το αντίστροφο;

9. i) Έστω $\pi,\ \tau \in S_n$ δύο κύκλοι ξένοι μεταξύ τους με μήκη n, m αντίστοιχα και n, m σχετικά πρώτοι. Δείξτε ότι η υποομάδα K που παράγεται από τις μεταθέσεις π και τ είναι κυλική.
   ii) Έστω G ομάδα και $a, b \in G$ με $a \cdot b = b \cdot a$. Αν $a^m = b^n = 1$ με $(m,\, n) = 1$, τότε η υποομάδα που παράγεται από τα a, b είναι κυκλική. Να βρεθεί ένα στοιχείο $c \in G$, τέτοιο ώστε $< c > = < a,\, b >$.

10. i) Δείξτε ότι κάθε Αβελιανή ομάδα με τάξη ίση με pq, όπου p, q είναι διαφορετικοί πρώτοι είναι κυκλική.
    ii) Δείξτε ότι η πολλαπλασιαστική ομάδα του δακτυλίου $\mathbb{Z}_{18}$ είναι κυκλική.

11. Θεωρούμε την ομάδα $U(\,\mathbb{Z}_{26}\,)$ των αντιστρέψιμων στοιχείων του $\mathbb{Z}_{26}$. Να δειχτεί ότι $U(\,\mathbb{Z}_{26}\,)$ είναι κυκλική και να βρεθούν όλοι οι γεννήτορές της.

12. Γνωρίζουμε (Εφαρμογή 4.6.8 (2)) ότι η πολλαπλασιαστική ομάδα $\mathbb{Z}_p^*$ είναι κυκλική. Να βρεθούν όλοι οι πρώτοι $p < 1000$ για τους οποίους το $2 \bmod p$ είναι γεννήτορας.[3]

13. Δείξτε ότι μία ομάδα είναι άπειρη κυκλική αν και μόνο αν είναι ισόμορφη με κάθε μη τετριμμένη υποομάδα της.

14. Έστω $a > 1$ φυσικός αριθμός πρώτος προς τον 9 και G κυκλική ομάδα με τάξη $n = a^{11} - a^7 - a^5 + a$. Δείξτε ότι υπάρχει υποομάδα της G με τάξη 45.

15. Έστω η κυκλική ομάδα $G = < a >$ με τάξη 120.
    i) Δείξτε ότι $< a^{54} > = < a^6 >$.

[3] Υπάρχει μια εικασία του Artin, η οποία δεν έχει αποδειχθεί μέχρι σήμερα, σύμφωνα με την οποία υπάρχουν άπειροι πρώτοι p για τους οποίους το $2 \bmod p$ παράγει την $\mathbb{Z}_p^*$.

ii) Να βρεθεί ο μικρότερος θετικός ακέραιος ν έτσι ώστε
$< a^{26} >=< a^{\nu} >$.

16. Μια ομάδα G έχει ακριβώς τρείς υποομάδες. Δείξτε ότι η G είναι κυκλική με τάξη ίση με το τετράγωνο ενός πρώτου αριθμού.

17. Να βρεθούν οι κοινές λύσεις των εξισώσεων $x^{25} = 1$ και $x^3 = 1$ στην ομάδα G, όπου G κυκλική με τάξη 100.

18. Δείξτε ότι κάθε ομάδα G που περιέχει τουλάχιστον τρία στοιχεία τάξης 6 δεν είναι κυκλική.

19. Γιατί η ομάδα $U(\mathbb{Z}_{3^{10}}) \times U(\mathbb{Z}_{5^{20}})$ δεν είναι κυκλική ;

20. Έστω G μια ομάδα με $|G| \leq 180$. Υποθέτουμε ότι υπάρχουν δυο υποομάδες με τάξεις 7 και 13 αντίστοιχα. Δείξτε ότι κάθε γνήσια υποομάδα της είναι κυκλική. Αν επιπλέον η G είναι Αβελιανή, τότε είναι κυκλική. Είναι δυνατόν η G να περιέχει στοιχείο τάξης 2 ;

21. Έστω G μια πεπερασμένη Αβελιανή ομάδα με τάξη που δεν διαιρείται από το τετράγωνο κανενός ακεραίου μεγαλυτέρου του 1. Δείξτε ότι η G είναι κυκλική.

22. Έστω $G =< g >$ με $|G| = 20$. Να βρεθούν δύο διακεκριμένες υποομάδες $H_1, H_2 \neq \{1\}$ με $H_1 \lneq H_2$ όπου $g^4 \notin H_2$.

23. Δείξτε ότι στην ομάδα $U(\mathbb{Z}_p)$, όπου p πρώτος, το μόνο στοιχείο που έχει τάξη 2 είναι το $p-1$. Από αυτό δείξτε το θεώρημα του Wilson:

    $(p-1)! \equiv -1 \mod p$.

24. Για την ομάδα $U(\mathbb{Z}_{100})$ να βρεθούν

    α) η τάξη της

    β) η τάξη του 73 mod 100

    γ) το αντίστροφο του 19 mod 100

    δ) Να δειχθεί ότι αν ο $n \in \mathbb{N}$ είναι τέτοιος ώστε ο $2n+1$ και ο $2n$ δεν διαιρούνται με το 5 τότε $(2n+1)^{20} \equiv 1 \mod 100$ και $(2n)^{20} \equiv 76 \mod 100$.
    Υπόδειξη: Παρατηρήστε ότι $3^{20} = (10-1)^{10} \equiv 1 \mod 100$ και άρα η τάξη του 3 είναι 20. Συνεπώς η $U(\mathbb{Z}_{100})$ δεν μπορεί να είναι κυκλική διότι θα έπρεπε να υπήρχε ένας αριθμός που το τετράγωνό του να είναι 3. Άρα $U(\mathbb{Z}_{100}) \cong C_{20} \times C_2$. Επίσης παρατηρήστε ότι αν $2n = 2^k(2m+1)$, τότε

$(2n)^{20} = 2^{20k}(2m+1)^{20} = (2^{20})^k\,(2m+1)^{20} = 76^k \cdot 1 \equiv 76 \bmod 100$. Σημειώστε ότι το 76 είναι το ταυτοτικό στοιχείο της πολλαπλασιαστικής ομάδας $\{\,76,\ 4,\ 16,\ 64,\ 56,\ 24,\ 96,\ 84,\ 36,\ 44\,\} \bmod 100$.

4.7 Κανονικές Υποομάδες και Ομάδες Πηλίκα

Θεωρούμε έναν ομομορφισμό ομάδων $\phi : G \longrightarrow G'$ με πυρήνα K. Έχουμε δει ότι αν $g' \in \phi(G)$ τότε το σύνολο των στοιχείων της G που απεικονίζονται στο g' μέσω του ϕ είναι η αριστερή κλάση gK του g μοδυλο K, για κάποιο $g \in G$ τέτοιο ώστε $\phi(g) = g'$.

Παρατηρούμε ότι, ορίζοντας το γινόμενο δύο μη κενών υποσυνόλων H_1, H_2 της G ως το σύνολο $H_1H_2 = \{\, h_1h_2 \mid h_1 \in H_1,\ h_2 \in H_2 \,\}$, το γινόμενο δύο κλάσεων g_1K, g_2K είναι η κλάση g_1g_2K. Πράγματι, κάθε στοιχείο της g_1g_2K είναι της μορφής $g_1 1 \cdot g_2 h$, $h \in K$, και συνεπώς $g_1g_2K \subseteq g_1Kg_2K$. Αντίστροφα, αν $h_1, h_2 \in K$ τότε $\phi(g_1h_1g_2h_2) = \phi(g_1)\phi(h_1)\phi(g_2)\phi(h_2) = \phi(g_1)\phi(g_2) = \phi(g_1g_2)$. Αυτό δηλώνει ότι για κάθε $h_1, h_2 \in K$ τα γινόμενα $g_1h_1g_2h_2$ ανήκουν στην αριστερή κλάση $\mathrm{mod}K$ που ορίζεται από το γινόμενο g_1g_2, δηλαδή $g_1h_1g_2h_2 \in g_1g_2K$. Επιπλέον, αν $g_1'K = g_1K$ και $g_2'K = g_2K$, τότε $g_1g_2K = g_1Kg_2K = g_1'Kg_2'K = g_1'g_2'K$.

Έτσι, βλέπουμε ότι η αντιστοιχία

$$G/K \times G/K \longrightarrow G/K, \quad (g_1K, g_2K) \longrightarrow g_1Kg_2K = g_1g_2K$$

είναι μια απεικόνιση, δηλαδή μια πράξη επί του G/K. Η πράξη αυτή ικανοποιεί τις τρεις βασικές ιδιότητες για να αποτελεί το σύνολο G/K ως προς αυτή την πράξη ομάδα:

1. Η κλάση K είναι το ουδέτερο στοιχείο, αφού $KK = K$, έχουμε $gKK = gK$, για κάθε $g \in G$.

2. Το αντίστροφο στοιχείο της gK είναι το $g^{-1}K$, αφού $gKg^{-1}K = gg^{-1}K = K$.

3. Η προσεταιριστική ιδιότητα ικανοποιείται αφού αυτή ικανοποιείται στην G:

$$\begin{aligned} g_1K(g_2Kg_3K) &= g_1K(g_2g_3K) = g_1(g_2g_3)K \\ &= (g_1g_2)g_3K = (g_1g_2K)g_3K \\ &= (g_1Kg_2K)g_3K. \end{aligned}$$

Αποδεικνύουμε τώρα ότι ισχύει και το αντίστροφο. Δηλαδή αν K είναι μια υποομάδα της G για την οποία ισχύει $g_1Kg_2K = g_1g_2K$ (και συνεπώς, όπως πριν, το G/K ως προς την πράξη $G/K \times G/K \longrightarrow G/K$ είναι ομάδα) τότε η K είναι ο πυρήνας ενός ομομορφισμού της G. Πράγματι, η αντιστοιχία $\phi : G \longrightarrow G/K$, $g \longrightarrow gK$ είναι ένας ομομορφισμός ομάδων, αφού από τον ορισμό της είναι μια απεικόνιση και ισχύει

$$\phi(g_1g_2) = g_1g_2K = g_1Kg_2K = \phi(g_1)\phi(g_2).$$

Ο πυρήνας είναι

$$\ker\phi = \{\, g \in G \mid \phi(g) = K \,\} = \{\, g \in G \mid gK = K \,\} = \{\, g \in G \mid g \in K \,\} = K,$$

αφού $gK = K$ αν και μόνον αν $g \in K$.

Έχοντας υπόψη τα προαναφερθέντα, οι υποομάδες μιας ομάδας G που είναι πυρήνες ομομορφισμών της χαρακτηρίζονται στο επόμενο θεώρημα.

4.7.1 Θεώρημα. *Μια υποομάδα K μιας ομάδας G είναι ο πυρήνας ενός ομομορφισμού της G αν και μόνον αν το γινόμενο κάθε δύο αριστερών κλάσεων* $\mathrm{mod}K$ *είναι μια αριστερή κλάση* $\mathrm{mod}K$. *Με άλλα λόγια, η K είναι ο πυρήνας ενός ομομορφισμού της G αν και μόνον αν η αντιστοιχία*

$$G/K \times G/K \longrightarrow G/K,\ (g_1K, g_2K) \longrightarrow g_1Kg_2K$$

είναι μια πράξη επί του G/K. Σ' αυτή την περίπτωση το G/K ως προς αυτή την πράξη είναι ομάδα και ονομάζεται ***ομάδα πηλίκο της*** G ***δια*** K *ή της* $G \bmod K$.

Απόδειξη. Αν η K είναι ο πυρήνας ενός ομομορφισμού της G, τότε δείξαμε, μόλις πριν, ότι η αντιστοιχία που αναφέρεται στο θεώρημα είναι μια πράξη επί του G/K ως προς την οποία το G/K είναι ομάδα. Αντίστροφα, έστω ότι $g_1Kg_2K \in G/K$ για κάθε $g_1, g_2 \in K$. Δηλαδή για κάθε $g_1, g_2 \in G$, υπάρχει $g_3 \in G$ τέτοιο ώστε $g_1Kg_2K = g_3K$. Αυτό σημαίνει ότι για κάθε δύο στοιχεία $h_1, h_2 \in K$ υπάρχει $h_3 \in K$ τέτοιο ώστε $g_1h_1g_2h_2 = g_3h_3$. Συνεπώς για $h_1 = h_2 = 1 \in K$, υπάρχει $h \in K$ τέτοιο ώστε $g_1g_2 = g_3h$. Δηλαδή $g_1g_2 \in g_3K$ ή ισοδύναμα $g_1g_2K = g_3K = g_1Kg_2K$. Συνεπώς το γινόμενο g_1Kg_2K καθορίζεται πλήρως από το γινόμενο g_1g_2. Λόγω αυτών που αναφέρθηκαν προηγουμένως, ως προς αυτό το γινόμενο το σύνολο G/K είναι ομάδα, ενώ ο πυρήνας του ομομορφισμού $\phi : G \longrightarrow G/K$, $g \longrightarrow gK$ είναι η υποομάδα K. ⊤

Παρατηρούμε ότι αν K είναι ο πυρήνας ενός ομομορφισμού $\phi : G \longrightarrow G'$ τότε για κάθε στοιχείο $g \in G$ όλα τα στοιχεία της μορφής gkg^{-1}, $k \in K$, είναι στοιχεία του K, αφού

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = 1\,.$$

Δηλαδή το υποσύνολο gKg^{-1} είναι υποσύνολο του K, για κάθε $g \in G$. Αλλά $gKg^{-1} = \tau_g(K)$, όπου τ_g είναι ο εσωτερικός αυτομορφισμός που ορίζεται από το g. Συνεπώς κάθε υποομάδα K της G που είναι πυρήνας ενός αυτομορφισμού της G είναι αναλλοίωτη από όλους τους εσωτερικούς αυτομορφισμούς της G. Ισχύει και το αντίστροφο. Έστω $K \leq G$ τέτοια ώστε $\tau_g(K) = gKg^{-1} \subseteq K$, για κάθε $g \in G$. Θα δείξουμε ότι $g_1Kg_2K = g_1g_2K$ για κάθε $g_1, g_2 \in G$. Πράγματι,

επειδή $\tau_{g_2^{-1}}(k) = g_2^{-1}kg_2 \in K$, υπάρχει $k' \in K$, με $g_2^{-1}kg_2 = k'$ ή ισοδύναμα $kg_2 = g_2k'$. Άρα κάθε στοιχείο $g_1k_1g_2k_2, \quad k_1, k_2 \in K$, γράφεται στη μορφή $g_1g_2k_1'k_2$ με $k_1' \in K$. Αυτό σημαίνει ότι $g_1Kg_2K \subseteq g_1g_2K$. Με τον ίδιο τρόπο συμπεραίνουμε ότι $g_1g_2K \subseteq g_1Kg_2K$ και άρα $g_1Kg_2K = g_1g_2K$.

Επομένως μια υποομάδα K μιας ομάδας G είναι πυρήνας ενός ομομορφισμού της G αν και μόνον αν η K είναι αναλλοίωτη από όλους τους εσωτερικούς αυτομορφισμούς της G. Έχει επικρατήσει αυτές τις υποομάδες να τις καλούμε ***κανονικές υποομάδες*** της G. Έτσι οι λέξεις κανονική υποομάδα και πυρήνας ενός ομομορφισμού της G είναι ταυτόσημες. Για να δηλώσουμε ότι μια υποομάδα K είναι κανονική γράφουμε $K \trianglelefteq G$.

4.7.2 Πρόταση. *Έστω K μια υποομάδα μιας ομάδας G. Τότε τα εξής είναι ισοδύναμα.*

1. *η K είναι κανονική υποομάδα.*
2. *$gKg^{-1} = K$, για κάθε $g \in G$.*
3. *$gK = Kg$, για κάθε $g \in G$.*

Απόδειξη. Αν η K είναι κανονική, τότε, για κάθε $g \in G$, από τη σχέση $gKg^{-1} \subseteq K$ προκύπτει $g^{-1}(gKg^{-1})g \subseteq g^{-1}Kg$ ή $K \subseteq g^{-1}Kg$. Αλλά όταν το g διατρέχει όλα τα στοιχεία της G το g^{-1} διατρέχει και αυτό όλα τα στοιχεία της G. Συνεπώς $K \subseteq (g^{-1})^{-1}Kg^{-1} = gKg^{-1}$. Άρα $K = gKg^{-1}$. Υποθέτουμε ότι ισχύει η 2. Τότε $(gKg^{-1})g = Kg$ ή ισοδύναμα $gK = Kg$. Υποθέτοντας ότι ισχύει η τελευταία σχέση, δείχνουμε ότι $g_1Kg_2K = g_1g_2K$ για κάθε $g_1g_2 \in G$. Πράγματι $g_1Kg_2K = g_1(Kg_2)K = g_1(g_2K)K = g_1g_2KK = g_1g_2K$. ⊤

4.7.3 Παρατήρηση. Τονίζουμε ότι η ισοδυναμία

$$gKg^{-1} = K \iff gKg^{-1} \subseteq K$$

δεν ισχύει για όλα τα $g \in G$. Φυσικά αν για κάποιο $g \in G$ ισχύει $gKg^{-1} = K$ τότε ισχύει και $gKg^{-1} \subseteq K$. Αλλά αν για κάποιο $g \in G$ ισχύει $gKg^{-1} \subseteq K$ αυτό δεν συνεπάγεται γενικά ότι θα ισχύει και $gKg^{-1} = K$. Για παράδειγμα, αν θεωρήσουμε το σύνολο G όλων των απεικονίσεων $f_{\alpha,\beta} : \mathbb{R} \longrightarrow \mathbb{R}$, όπου $f_{\alpha,\beta}(x) = \alpha x + \beta$ με $\alpha \neq 0$, $\alpha, \beta \in \mathbb{R}$, τότε το G με πράξη τη σύνθεση απεικονίσεων είναι μια μη-Αβελιανή ομάδα, γνωστή ως η ομοπαραλληλική ομάδα της ευθείας. Το υποσύνολο

$$K = \{\, f_{1,z} \mid z \in \mathbb{Z} \,\}$$

είναι υποομάδα (ισόμορφη με τη προσθετική ομάδα $\mathbb{Z}$).
Το αντίστροφο ενός στοιχείου $f_{\alpha,\beta} \in G$ είναι η απεικόνιση $f_{\frac{1}{\alpha},-\frac{\beta}{\alpha}}$. Αν θεωρήσουμε το στοιχείο $f_{\frac{1}{k},\beta}$, όπου $k \in \mathbb{Z}$, $\beta \in \mathbb{R}$, τότε επειδή

$$f_{k,-k\beta} \circ f_{1,z} \circ f_{\frac{1}{k},\beta} = f_{1,kz}$$

ισχύει $f_{\frac{1}{k},\beta}^{-1} K f_{\frac{1}{k},\beta} \subsetneq K$, αφού το $f_{\frac{1}{k},\beta}^{-1} K f_{\frac{1}{k},\beta}$ είναι μια υποομάδα (ισόμορφη με την $k\mathbb{Z}$) και δεν περιέχει, για παράδειγμα, το $f_{1,1} \in K$. Συνεπώς η K δεν είναι κανονική υποομάδα της G. Άλλωστε το συμπέρασμα προκύπτει αμέσως από το γεγονός ότι

$$f_{\alpha,\beta}^{-1} \circ f_{1,z} \circ f_{\alpha,\beta} = f_{1,\frac{z}{\alpha}} \notin K,$$

για $z \in \mathbb{Z}$ και $\frac{z}{\alpha} \notin \mathbb{Z}$.

4.7.4 Πρόταση. *α) Αν g είναι ένα στοιχείο μιας ομάδας G και K είναι μια κανονική υποομάδα της G, τότε η τάξη του στοιχείου gK της G/K είναι ο μικρότερος θετικός ακέραιος k για τον οποίο $g^k \in K$.*

β) Κάθε υποομάδα K μιας Αβελιανής ομάδας G είναι κανονική και η ομάδα G/K είναι Αβελιανή.

γ) Αν G είναι μια κυκλική ομάδα, τότε η G/K είναι κυκλική για κάθε υποομάδα της K.

Απόδειξη. α) Έστω k η τάξη του στοιχείου gK. Εξ' ορισμού το k είναι ο μικρότερος θετικός ακέραιος για τον οποίο $(gK)^k = K$. Αλλά $(gK)^k = g^k K$ και $g^k K = K$ αν και μόνον αν $g^k \in K$.

β) Έστω K μια υποομάδα της G και $g_1, g_2 \in G$. Επειδή $(g_1k_1)(g_2k_2) = g_1g_2k_1k_2 = g_2g_1k_1k_2 = g_2k_2g_1k_1$, έχουμε ότι $g_1Kg_2K = g_1gK = g_2Kg_1K$ που είναι το ζητούμενο.

γ) Αφήνεται σαν άσκηση. ⊺

4.7.5 Παραδείγματα.

1. Έστω $D_6 = \{ 1, x, x^2, x^3, x^4, x^5, y, yx, yx^2, yx^3, yx^4, yx^5 \}$ η διεδρική ομάδα. Θεωρούμε την υποομάδα $K = \{ 1, x^3 \}$ της D_6 και το σύνολο πηλίκο $D_6/K = \{ K, xK, x^2K, yK, yxK, yx^2K \}$. Είναι εύκολο να δειχτεί ότι η K είναι κανονική και άρα από το Θεώρημα 4.7.1 έπεται ότι το σύνολο D_6/K είναι ομάδα ως προς τον πολλαπλασιασμό των κλάσεων $\mathrm{mod} K$. Η D_6/K έχει έξι στοιχεία και δεν είναι Αβελιανή ομάδα, αφού, για παράδειγμα, $xKyK = xyK = yx^{-1}K = yx^5K \neq yxK = yKxK$. Επομένως, σύμφωνα με την ταξινόμηση των μη ισόμορφων ομάδων τάξης 6 (που έγινε στο τέλος της Παραγράφου 4.5), η D_6/K είναι ισόμορφη με την S_3.

2. Εφαρμόζοντας το θεώρημα του Cayley (Θεώρημα 4.5.11) για την ομάδα D_6/K, έχουμε τον μονομορφισμό

$$T : D_6/K \longrightarrow S_6, \quad gK \longrightarrow T_{gK}$$

με $T_{gK}(g'K) = gg'K$. Συμβολίζοντας τις κλάσεις K, xK, x^2K, yK, yxK και yx^2K με $1, 2, 3, 4, 5$ και 6 αντίστοιχα, βλέπουμε ότι $T_{xK} = (1\,2\,3)(4\,6\,5)$ και $T_{yK} = (1\,4)(2\,5)(3\,6)$.

Θεωρώντας τώρα τον επιμορφισμό $\phi : D_6 \longrightarrow D_6/K, \quad g \longrightarrow gK$, παίρνουμε τη σύνθεση $f' = T \circ \phi : D_6 \longrightarrow S_6$. Έτσι, έχουμε $f'(x) = (1\,2\,3)(4\,6\,5)$ και $f'(y) = (1\,4)(2\,5)(3\,6)$.

Στο επόμενο διάγραμμα παραθέτουμε όλες τις υποομάδες της D_6. Κάθε μια από αυτές παρίσταται με γεννήτορες. Οι ευθείες που συνδέουν αυτές υποδεικνύουν ότι η υποομάδα που βρίσκεται στο άνω άκρο αυτής περιέχει την υποομάδα που βρίσκεται στο κάτω άκρο της ευθείας. Οι υποομάδες $\{1\}$, $\langle x^3 \rangle$, $\langle x^2 \rangle$, $\langle x \rangle$, $\langle x^2, y \rangle$, $\langle x^2, yx \rangle$ και D_6 είναι οι μόνες κανονικές υποομάδες της D_6. Έχουμε δε $\langle x^3 \rangle \cong C_2$, $\langle x^2 \rangle \cong C_3$, $\langle x \rangle \cong C_6$, $\langle x^2, y \rangle \cong \langle x^2, yx \rangle \cong S_3$. Επίσης έχουμε $\langle x^3, y \rangle \cong \langle x^3, yx^4 \rangle \cong \langle x^3, yx^2 \rangle \cong C_2 \times C_2$ και όλες οι υπόλοιπες υποομάδες είναι ισόμορφες με την C_2.

$$D_6 =< x, y >$$

$$< x >\quad < x^3, y >\qquad\qquad < x^2, y >\ < x^3, yx^4 >\ < x^3, yx^2 >< x^2, yx >$$

$$< x^2 >< x^3 >\ \ < y >\ \ < yx >< yx^2 >\qquad < yx^3 >\qquad < yx^4 >\qquad < yx^5 >$$

$$\{1\}$$

Το επόμενο θεώρημα είναι το πρώτο βασικό θεώρημα των ομομορφισμών.

4.7.6 Θεώρημα. ***Πρώτο Θεώρημα Ισομορφισμών***
Έστω $\phi : G \longrightarrow G'$ ένας ομομορφισμός ομάδων. Τότε ισχύει

$$G/\ker\phi \cong \phi(G).$$

Απόδειξη. Έστω $K = \ker\phi$. Θεωρούμε την αντιστοιχία

$$\bar{\phi} : G/K \longrightarrow \phi(G), \quad gK \longrightarrow \phi(g).$$

Αρχικά παρατηρούμε ότι η αντιστοιχία αυτή είναι μια απεικόνιση. Πράγματι, αν $g, g' \in G$ είναι δύο στοιχεία με $gK = g'K$, τότε $g^{-1}g'K = K$ και άρα $g^{-1}g' \in K$. Τότε όμως έχουμε $\phi(g^{-1}g') = 1$ και άρα $\phi(g) = \phi(g')$. Τα παραπάνω επιχειρήματα αντιστρέφονται και δείχνουν ότι η απεικόνιση $\bar{\phi}$ είναι $1-1$. Επιπλέον, η $\bar{\phi}$ είναι επί, αφού για κάθε $g' \in \phi(G)$ υπάρχει ένα $g \in G$ με $\phi(g) = g'$ και έχουμε $\bar{\phi}(gK) = \phi(g) = g'$. Τέλος, ισχύει

$$\bar{\phi}(g_1Kg_2K) = \bar{\phi}(g_1g_2K) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \bar{\phi}(g_1K)\bar{\phi}(g_2K),$$

δηλαδή ο $\bar{\phi}$ είναι ομομορφισμός. ⊺

4.7.7 Παρατηρήσεις.

1. Το Θεώρημα 4.7.6 μας υποδεικνύει μια διαδικασία να βρίσκουμε ομομορφισμούς από μια ομάδα G σε μια άλλη G' ως εξής. Μπορούμε πρώτα να βρούμε τις υποομάδες K της G για τις οποίες η G/K είναι ομάδα και μετά να δούμε αν η G' έχει κάποια υποομάδα H που είναι ισόμορφη με μια ομάδα πηλίκο G/K. Έτσι θα έχουμε τη σύνθεση $G \longrightarrow G/K \xrightarrow{\sim} H$. Για παράδειγμα, αν $G = D_6$ και $G' = A_4$ έχουμε δει στο Παράδειγμα 3.9.2 (2) ότι για την D_6 οι δυνατές ομάδες πηλίκα είναι οι $D_6/\langle x^3\rangle$, $D_6/\langle x^2\rangle$, $D_6/\langle x\rangle$, $D_6/\langle x^2, y\rangle$ και $D_6\langle x^2, yx\rangle$ (και φυσικά οι D_6/D_6 και $D_6/\{1\}$).
   Για τη δομή της

   $$D_6/\langle x^2\rangle = \{\langle x^2\rangle, x\langle x^2\rangle, y\langle x^2\rangle, yx\langle x^2\rangle\}$$

   βλέπουμε ότι, επειδή $y^2 = (yx)^2 = x^4 = 1$, έχουμε $(x\langle x^2\rangle)^2 = (y\langle x^2\rangle)^2 = (yx\langle x^2\rangle)^2 = \langle x^2\rangle$ και συνεπώς η $D_6/\langle x^2\rangle$ είναι ισόμορφη με την $C_2 \times C_2$. Η A_4 περιέχει την υποομάδα $H = \{i, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ που είναι ισόμορφη με την $C_2 \times C_2$. Ένας ισομορφισμός της $D_6/\langle x^2\rangle$ στην H είναι η απεικόνιση $f : D_6/\langle x^2\rangle \longrightarrow H$, $x\langle x^2\rangle \longrightarrow (1\,2)(3\,4)$, $y\langle x^2\rangle \longrightarrow (1\,3)(2\,4)$, η οποία δίνει τον ομομορφισμό $\phi : D_6 \longrightarrow D_6/\langle x^2\rangle \longrightarrow A_4$, $\phi(x) = (1\,2)(3\,4)$, $\phi(y) = (1\,3)(2\,4)$, με πυρήνα την υποομάδα $\langle x^2\rangle$.
   Έχουμε δει ότι η ομάδα πηλίκο $D_6/\langle x^3\rangle$ είναι ισόμορφη με την S_3, ενώ η A_4 δεν έχει καμιά υποομάδα τάξης 6 (βλέπε το Παράδειγμα μετά Παρατήρηση 4.4.27). Άρα δεν υπάρχει ομομορφισμός της D_6 στην A_4 με πυρήνα την $\langle x^3\rangle$. Από τις ομάδες πηλίκα $D_6/\langle x\rangle$, $D_6/\langle x^2, y\rangle$ και $D_6/\langle x^2, yx\rangle$ που είναι ισόμορφες με την C_2 παίρνουμε ομομορφισμούς της D_6 στην A_4 καθώς η A_4 έχει υποομάδες τάξης 2.

2. Έχουμε δει ότι σε κάθε ομομορφισμό ϕ μιας ομάδας G αντιστοιχεί ο πυρήνας K του ϕ για τον οποίο το σύνολο G/K είναι ομάδα και αντίστροφα σε κάθε υποομάδα K για την οποία το σύνολο G/K είναι ομάδα αντιστοιχεί ένας ομομορφισμός της G. Θα θέλαμε να τονίσουμε εδώ, για να μην υπάρχει σύγχυση, ότι αυτή η αντιστοιχία δεν είναι ένα προς ένα. Όπως είδαμε, μόλις προηγουμένως, ο ομομορφισμός $G \longrightarrow G/K$ και ένας μονομορφισμός από την G/K σε μια ομάδα H δίνουν ένα ομομορφισμό της G στην H με πυρήνα τον K.
Επίσης θα θέλαμε να τονίσουμε ότι μπορούμε να έχουμε δύο ομομορφισμούς ϕ_1 και ϕ_2 μιας ομάδας G για τους οποίους οι πυρήνες K_1 και K_2 αντίστοιχα είναι ισόμορφες υποομάδες αλλά οι αντίστοιχες ομάδες πηλίκα να μην είναι ισόμορφες. Για παράδειγμα, οι ομομορφισμοί $\mathbb{Z} \longrightarrow \mathbb{Z}_n$, $z \longrightarrow z \bmod n$ και $\mathbb{Z} \longrightarrow \mathbb{Z}_m$, $z \longrightarrow z \bmod m$, έχουν ισόμορφους πυρήνες αφού αυτοί είναι οι υποομάδες $n\mathbb{Z}$ και $m\mathbb{Z}$ αντίστοιχα. Αλλά $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \ncong \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.
Αλλά και αντίστροφα, μπορούμε να έχουμε δύο ομομορφισμούς ϕ_1 και ϕ_2 με πεδίο ορισμού την G, των οποίων οι πυρήνες K_1 και K_2 δεν είναι ισόμορφες ομάδες, αλλά οι ομάδες πυλίκα G/K_1, G/K_2 είναι ισόμορφες. Για παράδειγμα, είδαμε ότι οι υποομάδες $\langle\, x \,\rangle$ και $\langle\, x^2, y \,\rangle$ της D_6 είναι κανονικές και $D_6/\langle\, x \,\rangle \cong D_6/\langle\, x^2,\, y \,\rangle \cong C_2$, αλλά $\langle\, x \,\rangle \cong C_6$ και $\langle\, x^2,\, y \,\rangle \cong S_3$.
Μια άλλη περίπτωση που πρέπει να τονιστεί είναι η εξής. Μπορούμε να έχουμε δύο μη ισόμορφες ομάδες G_1 και G_2 οι οποίες έχουν υποομάδες K_1 και K_2 αντίστοιχα που είναι πυρήνες ομομορφισμών και ισχύει $K_1 \cong K_2$ και $G_1/K_1 \cong G_2/K_2$. Για παράδειγμα,

$$\mathbb{Z}_4/\mathbb{Z}_2 \cong (\mathbb{Z}_2 \times \mathbb{Z}_2)/(\mathbb{Z}_2 \times \{\,1\,\}) \cong \mathbb{Z}_2\,.$$

4.7.8 Παραδείγματα και Εφαρμογές.

1. Το κέντρο $Z(G) = \{\, z \in G \mid gz = zg,\ g \in G \,\}$ είναι μια κανονική υποομάδα της G. Από τον ορισμό του κέντρου είναι φανερό ότι η G είναι Αβελιανή αν και μόνον αν $G = Z(G)$. Στο άλλο άκρο, έχουμε δει στην Παράγραφο 4.2 ότι η συμμετρική ομάδα S_n για $n > 2$ έχει τετριμμένο κέντρο. Συνεπώς, η μελέτη της ομάδας πηλίκο $G/Z(G)$ μπορεί να δώσει πληρφορίες για τη μη-μεταθετικότητα της G. Ισχύει το εξής κριτήριο (βλέπε Άσκηση 4.7.18): Η ομάδα G είναι Αβελιανή αν και μόνον αν η $G/Z(G)$ είναι κυκλική ομάδα. Η πιο συνήθης διατύπωση του προηγούμενου αποτελέσματος που χρησιμοποιείται στην πράξη είναι η εξής. Η ομάδα G δεν είναι Αβελιανή αν και μόνον αν η $G/Z(G)$ δεν είναι κυκλική. Για παράδειγμα, αν η G δεν είναι Αβελιανή και έχει τάξη pq για p και q πρώτους, τότε αυτή έχει τετριμμένο κέντρο. Πράγματι, αφού η G δεν είναι Αβελιανή σύμφωνα με τα προηγούμενα η $G/Z(G)$ δεν είναι κυκλική και άρα το κέντρο $Z(G)$ πρέπει

να είναι η τετριμμένη υποομάδα (γιατί;).

Ένα άλλο ενδιαφέρον αποτέλεσμα που αναφέρεται στο πηλίκο $G/Z(G)$ είναι το εξής (βλέπε Άσκηση 4.7.19): Για κάθε ομάδα G ισχύει

$$G/Z(G) \cong Inn(G).$$

Από αυτό και το προηγούμενο αποτέλεσμα προκύπτει ότι η ομάδα των εσωτερικών αυτομορφισμών μιας μη Αβελιανής ομάδας δεν είναι κυκλική. Αν η ομάδα G είναι Αβελιανή τότε $Inn(G) = \{1\}$. Επίσης από το προηγούμενο αποτέλεσμα προκύπτει άμεσα ότι $Inn(S_n) \cong S_n$ για $n > 2$. Η πλήρης εικόνα της δομής των αυτομορφισμών της S_n δίνεται από το εξής αποτέλεσμα:

$$S_n \cong Aut(S_n) = Inn(S_n)\,,$$

για $n \geq 3$ και $n \neq 6$. Για $n = 6$ ο δείκτης $\mid Aut(S_6) : Inn(S_6) \mid = 2$. Η απόδειξη του αποτελέσματος αυτού είναι πέρα από τους σκοπούς αυτού του βιβλίου.

2. Αν x, y είναι δύο στοιχεία μιας ομάδας G τότε το στοιχείο $x^{-1}y^{-1}xy$ που το συμβολίζουμε με $[x, y]$ λέγεται **μεταθέτης** των x και y και λέγεται έτσι επειδή $xy = yx[x, y]$. Η υποομάδα της G που παράγεται από όλους τους μεταθέτες $[x, y]$, $x, y \in G$ ονομάζεται **υποομάδα των μεταθετών** της G και συμβολίζεται συνήθως με $[G, G]$. Είναι φανερό ότι η G είναι Αβελιανή αν και μόνον αν $[G, G] = \{1\}$. Επίσης, για κάθε ομομορφισμό ε της G στον εαυτό της ισχύει $\varepsilon[x, y] = [\varepsilon(x), \varepsilon(y)]$, δηλαδή

$$\varepsilon([G,G]) \subseteq [\varepsilon(G), \varepsilon(G)] \subseteq [G, G]\,.$$

Ειδικά, για κάθε $g \in G$ ισχύει

$$\tau_g([G, G]) \subseteq [\tau_g(G), \tau_g(G)] = [G, G]\,,$$

δηλαδή $g[G, G]g^{-1} \subseteq [G, G]$. Αυτό σημαίνει ότι η $[G, G]$ είναι κανονική υποομάδα της G. Είναι δε η μικρότερη κανονική υποομάδα της G μεταξύ όλων των υποομάδων K για τις οποίες η ομάδα πηλίκο G/K είναι Αβελιανή ομάδα. Με άλλα λόγια, ισχύει το εξής:

"Αν $K \trianglelefteq G$, τότε η G/K είναι Αβελιανή αν και μόνον αν $[G, G] \subseteq K$".

Πράγματι, η ομάδα G/K είναι Αβελιανή αν και μόνο αν $g_1Kg_2K = g_2Kg_1K$ ή, ισοδύναμα, αν και μόνο αν $g_1g_2K = g_2g_1K$. Η τελευταία συνθήκη σημαίνει ακριβώς ότι $g_1^{-1}g_2^{-1}g_1g_2K = K$, δηλαδή ότι $[g_1, g_2] \in K$ για κάθε $g_1, g_2 \in G$.

Για παράδειγμα, αν $\phi : G \longrightarrow G'$ είναι ένας ομομορφισμός από την G σε μια Αβελιανή ομάδα G' τότε $[G, G] \subseteq \ker\phi$ αφού το πηλίκο $G/\ker\phi \cong \phi(G)$

είναι Αβελιανή ομάδα. Όπως είδαμε οι ορισμοί του κέντρου και της υποομάδας μεταθετών μιας ομάδας G δίνουν την ισοδυναμία "$G = Z(G)$ αν και μόνον αν $[G, G] = \{1\}$". Αν και ισχύει αυτή η ισοδυναμία, δεν υπάρχει κάποιο είδος δυϊκότητας μεταξύ του κέντρου και της υποομάδας μεταθετών. Πράγματι, αν το κέντρο $Z(G)$ μιας ομάδας G είναι τετριμμένο, δεν έπεται κατ' ανάγκη ότι θα ισχύει $G = [G, G]$. Για παράδειγμα, έχουμε $Z(S_3) = \{i\}$ και $[S_3, S_3] = A_3$ (γιατί;). Επίπλέον, δεν ισχύει ούτε η αντίστροφη συνεπαγωγή: Με άλλα λόγια, είναι δυνατό να έχουμε $G = [G, G]$ και $Z(G) \neq \{1\}$. Για παράδειγμα, αν $G = SL_3(\mathbb{Z}_7)$ τότε το κέντρο $Z(G)$ δεν είναι τετριμμένο (βλέπε Θεώρημα 4.4.5), αλλά μπορεί να αποδειχτεί ότι $G = [G, G]$ (βλέπε Άσκηση 4.7.22).

Σημειώνουμε ότι η έννοια της υποομάδας μεταθετών παίζει σημαντικό ρόλο στην επιλυσημότητα των αλγεβρικών εξισώσεων, όπως αυτή αναπτύχθηκε από τον E. Galois.

3. Η εναλλάσουσα υποομάδα A_n των άρτιων μεταθέσεων βαθμού n είναι κανονική υποομάδα της S_n. Πράγματι, χρησιμοποιώντας τον ορισμό, πρέπει να δείξουμε ότι $\sigma A_n \sigma^{-1} \subseteq A_n$ για κάθε $\sigma \in S_n$, δηλαδή ότι για κάθε $\sigma \in S_n$ και $\pi \in A_n$ ισχύει $\sigma\pi\sigma^{-1} \in A_n$. Αλλά, εκφράζοντας την άρτια μετάθεση π ως γινόμενο άρτιου πλήθους αντιμεταθέσεων, $\pi = \pi_1\pi_2\cdots\pi_k$, έχουμε $\sigma\pi\sigma^{-1} = \sigma\pi_1\sigma^{-1}\sigma\pi_2\sigma^{-1}\cdots\sigma\pi_k\sigma^{-1}$, όπου $\sigma\pi_i\sigma^{-1}$ είναι, ως γνωστόν, αντιμετάθεση. Έτσι, και η $\sigma\pi\sigma^{-1}$ είναι γινόμενο άρτιου πλήθους αντιμεταθέσεων. Εναλλακτικά, η κανονικότητα της A_n στην S_n έπεται αφού αυτή είναι ο πυρήνας του "προσήμου μεταθέσεων" (Παράδειγμα 4.5.8 (7)). Καθώς $\mid S_n : A_n \mid = 2$, η κανονικότητα της A_n στην S_n έπεται επίσης από το εξής γενικό αποτέλεσμα:

4.7.9 Λήμμα. *Κάθε υποομάδα K μιας ομάδας G δείκτου 2 είναι κανονική.*

Απόδειξη. Πράγματι, αν $g \notin K$, $g \in G$, τότε η $G = K \cup gK = K \cup Kg$ είναι η ανάλυση της G σε αριστερές και δεξιές κλάσεις $\mathrm{mod} K$. Επειδή η ένωση είναι ξένη, πρέπει $gK = Kg = G \setminus K$. ⊺

Καθώς $S_n/A_n \cong C_2$, από το το προηγούμενο παράδειγμα προκύπτει ότι $[S_n, S_n] \leq A_n$. Αλλά, για $n \geq 3$, το Θεώρημα 4.4.15 δείχνει ότι η A_n παράγεται από τις μεταθέσεις $(1\,a\,b)$, $2 \leq a,\ b \leq n$, ενώ η S_n παράγεται από τις αντιμεταθέσεις $(1\,a)$. Είναι δε $(1\,a)^{-1}(1\,b)^{-1}(1\,a)(1\,b) = (1\,a\,b)$. Συνεπώς $A_n \leq [S_n, S_n]$ και άρα $A_n = [S_n, S_n]$.

4. Η ειδική γραμμική ομάδα $SL_n(K)$ είναι κανονική υποομάδα της γενικής γραμμικής ομάδας $GL_n(K)$, όπου K είναι ένα σώμα. Αυτό προκύπτει από την ιδιότητα των οριζουσών: $\det(ABA^{-1}) = \det B$. Επίσης αυτό προκύπτει και από το γεγονός ότι η $SL_n(K)$ είναι ο πυρήνας του ομομορφισμού

$$\det : GL_n(K) \longrightarrow K^*.$$

5. Η υποομάδα $K = \langle \phi \rangle$ της διεδρικής ομάδας D_n που παράγεται από τη στροφή του κανονικού n-γώνου κατά γωνία $2\pi/n$, είναι κανονική. Η D_n παράγεται από την ϕ και μια ανάκλαση τ και ισχύει $\tau^{-1}\phi\tau = \phi^{n-1}$. Η κανονικότητα της K προκύπτει και από το γεγονός ότι $\mid D_n : K \mid = 2$.

6. Έστω $G = \mathbb{R}^*$ και $K = \mathbb{R}^*_{>0}$ (θετικοί πραγματικοί αριθμοί). Προφανώς η K είναι κανονική υποομάδα αφού είναι υποομάδα μιας Αβελιανής ομάδας. Έχουμε δε $G = K \cup (-1)K$, δηλαδή η ομάδα G/K έχει τάξη δύο και τα δύο στοιχεία της τα συμβολίζουμε με $\bar{1}(= K)$ και $-\bar{1} = ((-1)K)$. Ισχύει δε $\bar{1}\cdot -\bar{1} = -\bar{1}$ και $-\bar{1}\cdot -\bar{1} = \bar{1}$. Αν θεωρήσουμε τον επιμορφισμό

$$\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$$

και το υποσύνολο $GL_n(\mathbb{R})^+$ όλων των πινάκων της $GL_n(\mathbb{R})$ που η ορίζουσά τους είναι θετικός αριθμός, αυτό είναι μια κανονική υποομάδα που η ομομορφική της εικόνα $\det(GL_n(\mathbb{R})^+)$ είναι η $\mathbb{R}^*_{>0}$.

7. Μια χρήσιμη εφαρμογή της ομάδας πηλίκο είναι ότι πολλές φορές μας επιτρέπει να χρησιμοποιήσουμε τη μαθηματική επαγωγή για να αποδείξουμε ιδιότητες που ικανοποιούνται από συγκεκριμένες ομάδες. Για παράδειγμα, δείχνουμε ότι κάθε πεπερασμένη Αβελιανή ομάδα G της οποίας η τάξη διαιρείται από ένα πρώτο αριθμό p έχει ένα στοιχείο τάξης p (όπως θα δούμε στην επόμενη Ενότητα αυτό ισχύει για κάθε πεπερασμένη ομάδα).

Σύμφωνα με το Πόρισμα 4.4.26, αν η G δεν έχει γνήσιες υποομάδες αυτή είναι κυκλική τάξης p, οπότε κάθε (μη τετριμένο) στοιχείο της είναι τάξης p. Υποθέτουμε ότι H είναι μια γνήσια υποομάδα της G. Αν το p διαιρεί την τάξη της H τότε επαγωγικά η H έχει ένα στοιχείο τάξης p που βέβαια ανήκει στην G. Αν το p δεν διαιρεί την τάξη της H, τότε από το Θεώρημα του Lagrange το p πρέπει να διαιρεί την τάξη της G/H και επαγωγικά η G/H έχει ένα στοιχείο gH τάξης p, δηλαδή $g^p \in H$ (βλέπε 4.7.4α)). Επίσης ισχύει $(gH)^{|H|} \neq H$, αφού διαφορετικά, επειδή η τάξη του gH είναι p, θα έπρεπε το p να διαιρούσε την τάξη $\mid H \mid$ της H. Επειδή $g^p \in H$, σύμφωνα με το 4.4.23, ισχύει $(g^p)^{|H|} = 1$. Άρα το στοιχείο $g^{|H|}$ έχει τάξη p.

8. *Χαρακτήρες Πεπερασμένων Κυκλικών Ομάδων*

Έστω G μια κυκλική ομάδα τάξης n. Ένας ομομορφισμός $\mathcal{X} : G \longrightarrow S^1$, όπου $S^1 = \{\, z \in \mathbb{C} \mid \ \mid z \mid = 1 \,\}$ λέγεται **χαρακτήρας** της G. Αν g είναι ένας γεννήτορας της G τότε η απεικόνιση

$$\mathcal{X}_t : G \longrightarrow S^1,\ g^r \longrightarrow e^{2\pi irt/n}, \quad t \in \mathbb{Z}$$

είναι ένας χαρακτήρας της G και όλοι οι χαρακτήρες της G είναι ακριβώς αυτοί. Πράγματι, αν $\mathcal{X}$ είναι ένας χαρακτήρας τότε ο $\mathcal{X}(g)$ είναι μια n-οστή ρίζα της μονάδας, έστω $\mathcal{X}(g) = e^{2\pi ik/n}$, και άρα $\mathcal{X} = \mathcal{X}_k$. Αν $\mathcal{X}_k$, $\mathcal{X}_\ell$ είναι δύο χαρακτήρες, τότε ορίζουμε το γινόμενο $\mathcal{X}_k\mathcal{X}_\ell$ θέτοντας $(\mathcal{X}_k\mathcal{X}_\ell)(g) = \mathcal{X}_k(g)\mathcal{X}_\ell(g)$ και άρα

$$\mathcal{X}_k\mathcal{X}_\ell = \mathcal{X}_{(k+\ell) \bmod n} = \begin{cases} \mathcal{X}_{k+\ell} & \text{αν} \quad k+\ell < n \\ \mathcal{X}_{k+\ell} - n & \text{αν} \quad k+\ell \geq n. \end{cases}$$

Το σύνολο $\hat{G} = \{\, \mathcal{X}_0, \mathcal{X}_1, \ldots, \mathcal{X}_{n-1} \,\}$, όλων των χαρακτήρων της G, ως προς αυτό το γινόμενο είναι μια ομάδα. Το ουδέτερο στοιχείο είναι ο χαρακτήρας $\mathcal{X}_0$ και το αντίστροφο στοιχείο του $\mathcal{X}_k$ είναι ο χαρακτήρας $\mathcal{X}_{-k} = \mathcal{X}_{n-k}$. Παρατηρούμε ότι ο $\mathcal{X}_1$ έχει τάξη n και άρα η $\hat{G}$ είναι ισόμορφη με την G. Η απεικόνιση $G \longrightarrow \hat{G}$, $g^k \longrightarrow \mathcal{X}_k$, είναι ένας ισομορφισμός (που όμως εξαρτάται από το γεννήτορα g της G).

Έστω τώρα H μια υποομάδα της G. Θεωρούμε το σύνολο

$$M(H) = \{\mathcal{X} \in \hat{G} \mid \mathcal{X}(h) = 1,\ \text{για κάθε } h \in H\}.$$

Είναι φανερό ότι το $M(H)$ είναι μια υποομάδα της $\hat{G}$ και ισχύει $M(H) \cong G/H$. Πράγματι, η αντιστοιχία $M(H) \longrightarrow \widehat{(G/H)}$, $\mathcal{X} \longrightarrow \vartheta_{\mathcal{X}}$, όπου $\vartheta_{\mathcal{X}}(g^iH) = \mathcal{X}(g^i)$ είναι μια απεικόνιση που από τον ορισμό της είναι $1-1$. Αν $\vartheta \in \widehat{(G/H)}$, τότε ο χαρακτήρας $\mathcal{X}$ της G για τον οποίο $\mathcal{X}(g) = \vartheta(gH)$ προφανώς ανήκει στην $M(H)$. Δηλαδή η απεικόνιση αυτή είναι και επί. Έχουμε δε

$$\begin{aligned} \vartheta_{\mathcal{X}_1\mathcal{X}_2}(g^iH) &= \mathcal{X}_1\mathcal{X}_2(g^i) = \mathcal{X}_1(g^i)\mathcal{X}_2(g^i) = \vartheta_{\mathcal{X}_1}(g^iH)\vartheta_{\mathcal{X}_2}(g^iH) \\ &= \vartheta_{\mathcal{X}_1}\vartheta_{\mathcal{X}_2}(g^iH). \end{aligned}$$

Συνεπώς $\mathcal{X}_1\mathcal{X}_2 \longrightarrow \vartheta_{\mathcal{X}_1}\vartheta_{\mathcal{X}_2}$, δηλαδή αυτή η απεικόνιση είναι ένας ισομορφισμός. Επειδή $\widehat{(G/H)} \cong G/H$ θα είναι και $M(H) \cong G/H$.

Οι χαρακτήρες των κυκλικών ομάδων έχουν εφαρμογές στη Θεωρία Αριθμών.

Το επόμενο αποτέλεσμα αναφέρεται στις ομομορφικές εικόνες των υποομάδων μιας ομάδας.

4.7.10 Θεώρημα (Θεώρημα Αντιστοιχίας). *Έστω $\phi : G \longrightarrow G'$ ένας επιμορφισμός ομάδων με πυρήνα $K = \ker\phi$. Τότε ο ϕ επάγει μια $1-1$ και επί αντιστοιχία Φ μεταξύ του συνόλου $S(G,K)$ όλων των υποομάδων της G που περιέχουν την K και του συνόλου $S(G')$ όλων των υποομάδων της G'. Ισχύει δε*

1. *$K \leq H_1 \leq H_2 \leq G$ αν και μόνον αν $\Phi(H_1) \leq \Phi(H_2)$. Στην περίπτωση αυτή είναι $\mid H_2 : H_1 \mid = \mid \Phi(H_2) : \Phi(H_1) \mid$*

2. *$K \leq H_1 \trianglelefteq H_2$ αν και μόνον αν $\Phi(H_1) \trianglelefteq \Phi(H_2)$. Στην περίπτωση αυτή είναι $H_2/H_1 \cong \Phi(H_2)/\Phi(H_1)$.*

Απόδειξη. Γνωρίζουμε ότι η ομομορφική εικόνα $\phi(H)$ μιας υποομάδας H της G είναι υποομάδα της G'. Επιπλέον αν H' είναι μια υποομάδα της G' τότε η αντίστροφη εικόνα της H' που ορίζεται ως το υποσύνολο

$$\phi^{-1}(H') = \{\, g \in G \mid \phi(g) \in H' \,\}$$

της G είναι υποομάδα της G. Πράγματι, αν $g_1, g_2 \in \phi^{-1}(H')$ τότε, επειδή $\phi(g_1 g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1} \in H'$ το $g_1 g_2^{-1} \in \phi^{-1}(H')$. Επίσης έχουμε δει ότι $\phi^{-1}(1) = K$ και άρα $K \subseteq \phi^{-1}(H')$.

Τώρα θα δείξουμε ότι η αντιστοιχία

$$\Phi : S(G,K) \longrightarrow S(G'),\ H \longrightarrow \phi(H),$$

είναι $1-1$ και επί απεικόνιση. Όπως μόλις είδαμε η αντιστοιχία

$$\Phi^{-1} : S(G') \longrightarrow S(G,K),\ H' \longrightarrow \phi^{-1}(H')$$

είναι μια απεικόνιση. Θα δείξουμε ότι η σύνθεση $\Phi^{-1}\Phi$ και η $\Phi\Phi^{-1}$ είναι η ταυτοτική απεικόνιση $1_{S(G,K)}$ και η $1_{S(G')}$ αντίστοιχα. Πράγματι, αν $H \in S(G,K)$ τότε

$$\Phi^{-1}(\Phi(H)) = \phi^{-1}(\phi(H)) = \{\, g \in G \mid \phi(g) \in \phi(H) \,\}$$

και άρα $H \subseteq \phi^{-1}(\phi(H))$. Έστω $g \in \phi^{-1}(\phi(H))$. Τότε $\phi(g) \in \phi(H)$, δηλαδή υπάρχει ένα $h \in H$ τέτοιο ώστε $\phi(g) = \phi(h)$ ή ισοδύναμα $\phi(gh^{-1}) = 1$ που σημαίνει ότι $gh^{-1} \in K$, δηλαδή $g \in hK$. Επειδή $K \subseteq H$ έπεται ότι $g \in H$. Επομένως $(\Phi^{-1}\Phi)(H) = H$, για κάθε $H \in S(G,K)$. Άρα $\Phi^{-1}\Phi = 1_{S(G,K)}$. Η ισότητα $\Phi\Phi^{-1} = 1_{S(G')}$ προκύπτει από την υπόθεση ότι η ϕ είναι επί απεικόνιση: Αν $H' \in S(G')$ και $h' \in H'$ τότε υπάρχει $g \in G$ με $\phi(g) = h'$ που σημαίνει ότι $g \in \phi^{-1}(H')$ και συνεπώς $h' = \phi(g) \in \phi(\phi^{-1}(H'))$, δηλαδή $H' \subseteq \phi(\phi^{-1}(H'))$. Επειδή προφανώς ισχύει $\phi(\phi^{-1}(H')) \subseteq H'$, έχουμε $\phi(\phi^{-1}(H')) = H'$ για κάθε $H' \in S(G')$.

Τώρα η συνθήκη 1. είναι προφανής από τον ορισμό των υποομάδων $\phi(H)$ και $\phi^{-1}(H')$. Για την ισότητα

$$| H_2 : H_1 | = | \Phi(H_2) : \Phi(H_1) |$$

αρκεί να δείξουμε ότι υπάρχει μια $1-1$ και επί απεικόνιση μεταξύ των αριστερών συνόλων πηλίκο H_2/H_1 και $\phi(H_2)/\phi(H_1)$. Μια τέτοια είναι η αντιστοιχία $hH_1 \longrightarrow \phi(h)\phi(H_1)$. Πράγματι, αν $hH_1 \neq h'H_1$, $h, h' \in H_2$, δηλαδή $hH_1 \cap h'H_1 = \emptyset$, τότε $\phi(h)\phi(H_1) \cap \phi(h')\phi(H_1) = \emptyset$. Διότι αν $g' = \phi(h)\phi(h_1) = \phi(h')\phi(h'_1)$, για $h_1, h'_1 \in H_1$, τότε $\phi(h^{-1}h'h'_1h_1^{-1}) = 1$, δηλαδή $h^{-1}h'h'_1h_1^{-1} \in K \subset H_1$ και άρα $h^{-1}h' \in H_1$ που είναι άτοπο. Άρα η f είναι $1-1$. Είναι δε φανερό ότι είναι και επί.

Για τη συνθήκη 2., υποθέτουμε ότι $H_1 \trianglelefteq H_2$, δηλαδή $hH_1h^{-1} = H_1$, για κάθε $h \in H_2$. Τότε έχουμε $\phi(h)\phi(H_1)\phi(h)^{-1} = \phi(H_1)$, δηλαδή $h'\phi(H_1)h'^{-1} = \phi(H_1)$ για κάθε $h' \in \phi(H_2)$. Άρα $\phi(H_1) \trianglelefteq \phi(H_2)$. Αντίστροφα, έστω
$K \leq H_1 \leq H_2 \leq G$ όπου $\phi(H_1) \trianglelefteq \phi(H_2)$. Τότε έχουμε

$$\phi(hH_1h^{-1}) = \phi(h)\phi(H_1)\phi(h)^{-1} = \phi(H_1)\,,$$

για κάθε $h \in H_2$. Αλλά $hH_1h^{-1} \in S(G,K)$, αφού από τη σχέση $K \leq H_1$ προκύπτει $K = hKh^{-1} \leq hH_1h^{-1}$. Άρα

$$\Phi^{-1}(\phi(hH_1h^{-1})) = \Phi^{-1}(\phi(H_1))$$

και όπως είδαμε πριν έπεται ότι $hH_1h^{-1} = H_1$, δηλαδή $H_1 \trianglelefteq H_2$.

Για να δείξουμε την ύπαρξη του ισομορφισμού

$$H_2/H_1 \cong \phi(H_2)/\phi(H_1)$$

θεωρούμε τους ομομορφισμούς ομάδων $\rho : \phi(H_2) \longrightarrow \phi(H_2)/\phi(H_1)$, $\phi(h) \longrightarrow \phi(h)\phi(H_1)$, και $\phi\mid_{H_2}\colon H_2 \longrightarrow \phi(H_2)$ με πυρήνες $\phi(H_1)$ και K αντίστοιχα. Η σύνθεση $\rho \circ \phi\mid_{H_2}$ είναι ένας ομομορφισμός (βλέπε Παράδειγμα 4.5.8.5) και μάλιστα επιμορφισμός, αφού $\rho \circ \phi\mid_{H_2}(H_2) = \rho(\phi\mid_{H_2}(H_2)) = \phi(H_2)/\phi(H_1)$, του οποίου ο πυρήνας είναι

$$\begin{aligned}
\ker(\rho \circ \phi\mid_{H_2}) &= \{\, h_2 \in H_2 \mid \rho \circ \phi\mid_{H_2}(h_2) = \phi(H_1) \,\} \\
&= \{\, h_2 \in H_2 \mid \phi\mid_{H_2}(h_2)\phi(H_1) = \phi(H_1 \,\} \\
&= \{\, h_2 \in H_2 \mid \phi(h_2) \in \phi(H_1) \,\} \\
&= \phi^{-1}(\phi(H_1)) \\
&= H_1
\end{aligned}$$

Επομένως το αποτέλεσμα έπεται από το Θεώρημα 4.7.6. ⊺

4.7.11 Πόρισμα. *Αν $K \trianglelefteq G$, τότε κάθε υποομάδα της ομάδας πηλίκο G/K είναι της μορφής H/K για κάποια μοναδική υποομάδα H της G που περιέχει την K. Επιπλέον, αν $L \trianglelefteq G$ και $K \leq L$, τότε*

$$\frac{G}{L} \cong \frac{G/K}{L/K}$$

Απόδειξη. Θεωρούμε τον επιμορφισμό $\phi : G \longrightarrow G/K$, $g \longrightarrow gK$. Αν $H \leq G$ με $K \leq H$ τότε

$$\phi(H) = \{\, hK \mid h \in H \,\} = H/K\,.$$

Επομένως, σύμφωνα με το προηγούμενο θεώρημα, όλες οι υποομάδες της G/K είναι αυτής της μορφής και $H_1/K \neq H_2/K$ αν και μόνον αν $H_1 \neq H_2$. Ειδικά, στις υποομάδες G και L αντιστοιχούν οι υποομάδες G/K και L/K και ισχύει ο ισομορφισμός $\frac{G}{L} \cong \frac{G/K}{L/K}$ που αναφέρεται στο Πόρισμα. ⊺

Στην περίπτωση που μια υποομάδα H της G δεν περιέχει την κανονική υποομάδα K, τότε η ομομορφική εικόνα $\phi(H)$, όπου $\phi : G \longrightarrow G/K$, δίδεται στο επόμενο θεώρημα το οποίο συνήθως ονομάζεται "Δεύτερο Θεώρημα Ισομορφισμών".

4.7.12 Θεώρημα (Δεύτερο Θεώρημα Ισομορφισμών). *Έστω K μια κανονική υποομάδα μιας ομάδας G. Θεωρούμε τον επιμορφισμό*

$$\phi : G \longrightarrow \frac{G}{K},\ g \longrightarrow gK.$$

Τότε για κάθε $H \leq G$, το γινόμενο HK είναι υποομάδα της G και $\phi(H) = \frac{HK}{K}$. Επιπλέον η τομή $H \cap K$ είναι κανονική υποομάδα της H και ισχύει

$$\frac{HK}{K} \cong \frac{H}{H \cap K}.$$

Απόδειξη. Καθώς η $\phi(H)$ είναι υποομάδα της G/K, από το Πόρισμα 4.7.11 υπάρχει μια μοναδική υποομάδα M της G που περιέχει την K για την οποία θα έχουμε

$$\phi(H) = \frac{M}{K}.$$

Από το Θεώρημα αντιστοιχίας 4.7.10 μπορούμε να προσδιορίσουμε ποια είναι η M. Πράγματι, η $\Phi^{-1}(\phi(H)) = \phi^{-1}(\phi(H))$ είναι η υποομάδα της G που

περιέχει την K (που είναι ο πυρήνας της ϕ) και αντιστοιχεί στην $\phi(H)$. Αλλά $\phi^{-1}(\phi(H)) = \{\, \phi^{-1}(\phi(h)) \mid h \in H \,\} = \{\, hK \mid h \in H \,\} = HK$, αφού

$$\begin{aligned}\phi^{-1}(\phi(h)) &= \{\, g \in G \mid \phi(g) = \phi(h) \,\} = \{\, g \in G \mid gK = hK \,\} \\ &= \{\, g \in G \mid g \in hK \,\} = hK.\end{aligned}$$

Συνεπώς η HK είναι υποομάδα της G (αυτό προκύπτει και από το γεγονός ότι $HK = \{\, hK \mid h \in H \,\} = \{\, Kh' \mid h' \in H \,\} = KH$). Επομένως, αφού στην $\phi(H)$ αντιστοιχεί μέσω της Φ^{-1} η υποομάδα HK, αυτή είναι η μοναδική υποομάδα M της G για την οποία έχουμε $\phi(H) = HK/H$.

Τώρα, όπως και στην απόδειξη του Θεωρήματος 4.5.2, θεωρούμε τον περιορισμό ϕ_H της ϕ στην H και έχουμε $\ker \phi_H = H \cap \ker \phi = H \cap K$. Καθώς $\phi_H(H) = \phi(H)$, από το θεώρημα 4.7.6 έπεται ότι

$$\phi(H) = \frac{HK}{K} \cong \frac{H}{H \cap K},$$

με τον ισομορφισμό $HK/K \longrightarrow H/H \cap K$ να δίνεται από την αντιστοιχία $hK \longrightarrow h(H \cap K)$. ⊺

4.7.13 Παρατήρηση. Θα θέλαμε να σημειώσουμε ότι από το Θεώρημα 4.7.10(2) έπεται ότι το Πόρισμα 4.7.11 ισχύει και για τις κανονικές υποομάδες. Δηλαδή, οι κανονικές υποομάδες της G/K είναι της μορφής H/K, όπου $H \trianglelefteq G$ με $K \leq H$. Γενικότερα, αν $\phi : G \longrightarrow G'$ είναι ένας επιμορφισμός ομάδων με πυρήνα την υποομάδα K και $H \trianglelefteq G$, τότε η υποομάδα $\phi(H)$ της G' είναι κανονική, ανεξάρτητα αν η H περιέχει ή όχι την K, αφού, για κάθε $g' \in G'$ και $\phi(h) \in \phi(H)$ έχουμε $g'\,\phi(h)\,g'^{-1} = \phi(ghg^{-1}) \in \phi(H)$, όπου $g \in G$ με $\phi(g) = g'$. Το αντίστροφο δεν ισχύει, δηλαδή μπορεί να ισχύει $\phi(H) \trianglelefteq G'$, αλλά η H να μην είναι κανονική υποομάδα της G. Πράγματι, η σχέση $\phi(ghg^{-1}) \in \phi(H)$ δεν σημαίνει ότι $ghg^{-1} \in H$, αλλά ότι $ghg^{-1} \in \phi^{-1}(\,\phi(H)\,)$ και γενικά ισχύει $H \subseteq \phi^{-1}(\,\phi(H)\,) = H \ker \phi$.

Αν όμως $H' \trianglelefteq G'$, τότε $\phi^{-1}(H') \trianglelefteq G$ και ισχύει $G/\phi^{-1}(H') \cong G'/H'$. Πράγματι, θεωρούμε τον επιμορφισμό $\phi' : G' \longrightarrow G'/H'$, οπότε η σύνθεση των επιμορφισμών $\phi' \circ \phi : G \longrightarrow G'/H'$ έχει πυρήνα

$$\ker(\phi' \circ \phi) = \{\, g \in G \mid \phi' \circ \phi(g) = H' \,\} = \{\, g \in G \mid \phi(g)H' = H' \,\} =$$

$$\{\, g \in G \mid \phi(g) \in H' \,\} = \phi^{-1}(H').$$

Οπότε στο Θεώρημα 4.7.12 αν η υποομάδα H της G είναι κανονική, τότε και το γινόμενο HK είναι κανονική υποομάδα της G.

4.7.14 Πόρισμα. *Έστω G μια πεπερασμένη ομάδα και K μια κανονική υποομάδα τέτοια ώστε ο μ.κ.δ.$(|\ K\ |, |\ G/K\ |) = 1$. Τότε η K είναι η μοναδική υποομάδα τάξης $|\ K\ |$ της G.*

Απόδειξη. Έστω H μια υποομάδα της G με τάξη $|\ K\ |$. Επειδή η τάξη της HK/K διαιρεί την τάξη $|\ G/K\ |$, θα έχουμε μ.κ.δ.$(|\ K\ |, |\ HK/K\ |) = 1$. Αλλά $HK/K \cong H/K \cap H$ και άρα μ.κ.δ.$(|\ K\ |, |\ H\ |\ /\ |\ K \cap H\ |) = 1$. Επειδή $|\ K\ | = |\ H\ |$, θα πρέπει $|\ K \cap H\ | = |\ H\ |$, δηλαδή $H = K$. ⊤

4.7.15 Παραδείγματα.

1. Θεωρούμε τη διεδρική ομάδα $D_4 = \langle\, x, y \mid x^4 = y^2 = (yx)^2 \,\rangle = \{\, y^i x^j \mid 0 \le i \le 1, 0 \le j \le 3 \,\}$ και την ομάδα $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{\, (i, j) \mid 0 \le i, j \le 1 \,\}$ με πράξη την πρόσθεση $(i_1, j_1) + (i_2, j_2) = (i_1 + i_2, j_1 + j_2)$. Ορίζουμε την αντιστοιχία

$$\phi : D_4 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2, \quad y^i x^i \longrightarrow (i, j)$$

η οποία είναι ένας ομομορφισμός του οποίου ο πυρήνας είναι η υποομάδα $K = \{\, 1, x^2 \,\}$ (γιατί;). Οι υποομάδες της $\mathbb{Z}_2 \times \mathbb{Z}_2$ είναι οι $H_1 = \mathbb{Z}_2 \times \{\, 0 \,\}$, $H_2 = \{\, 0 \,\} \times \mathbb{Z}_2$, $H_3 = \{\, (0, 0), (1, 1) \,\}$, $H_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$ και $H_5 = \{\, (0, 0) \,\}$ και έχουμε

$$\begin{array}{ll} \phi^{-1}(H_1) = \{\, 1, x^2, y, yx^2 \,\} & \phi^{-1}(H_4) = D_4 \\ \phi^{-1}(H_2) = \{\, 1, x, x^2, x^3 \,\} & \phi^{-1}(H_5) = \{\, 1, x^2 \,\}. \\ \phi^{-1}(H_3) = \{\, 1, x^2, yx, yx^3 \,\} & \end{array}$$

Συνεπώς οι υποομάδες της D_4, σύμφωνα με το 4.7.10, που περιέχουν την K είναι οι $\phi^{-1}(H_i)$, $i = 1, 2, 3, 4, 5$. Αυτές είναι όλες κανονικές υποομάδες της D_4, αφού όλες οι υποομάδες της $\mathbb{Z}_2 \times \mathbb{Z}_2$ είναι κανονικές (αυτό βέβαια είναι φανερό και από το ότι οι $\phi^{-1}(H_i)$, $i = 1, 2, 3$ είναι δείκτου 2 και η $\phi^{-1}(H_5)$ είναι ο πυρήνας του ϕ. Στην περίπτωση αυτή, συμβαίνει να είναι αυτές οι μόνες μη-τετριμμένες κανονικές υποομάδες της D_4 ενώ οι υπόλοιπες υποομάδες της D_4 είναι οι $\{\, 1, y \,\}$, $\{\, 1, yx \,\}$, $\{\, 1, yx^2 \,\}$ και $\{\, 1, yx^3 \,\}$.

Από το Πόρισμα 4.7.11 προκύπτει ότι οι υποομάδες της D_4/K είναι ακριβώς οι $\phi^{-1}(H_i)/K$, $i = 1, 2, 3, 4, 5$, ενώ από το Θεώρημα 4.7.12 παίρνουμε

$$\begin{aligned} \phi(\{\, 1, y \,\}) &= \frac{\{\, 1, y \,\}\{\, 1, x^2 \,\}}{\{\, 1, x^2 \,\}} = \frac{\{\, 1, x^2, y, yx^2 \,\}}{\{\, 1, x^2 \,\}} \\ &= \frac{\phi^{-1}(H_1)}{K} \cong \frac{\{\, 1, y \,\}}{\{\, 1, y \,\} \cap \{\, 1, x^2 \,\}} = \frac{\{\, 1, y \,\}}{\{\, 1 \,\}} \cong C_2. \end{aligned}$$

$$\phi(\{\,1,\, yx\,\}) = \frac{\phi^{-1}(H_3)}{K} \cong C_2 \quad \text{και}$$
$$\phi(\{\,1,\, yx^2\,\}) = \frac{\phi^{-1}(H_1)}{K} \cong C_2$$
$$\phi(\{\,1,\, yx^3\,\}) = \frac{\phi^{-1}(H_3)}{K} \cong C_2$$

2. Θεωρούμε την προσθετική ομάδα $\mathbb{Z}$ των ακέραιων. Γνωρίζουμε ότι όλες οι υποομάδες της $\mathbb{Z}$ είναι της μορφής $n\mathbb{Z}$, $n \in \mathbb{N}$. Συνεπώς, από το Πόρισμα 4.7.11, όλες οι υποομάδες της $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ είναι της μορφής $m\mathbb{Z}/n\mathbb{Z}$, όπου $n\mathbb{Z} \subseteq m\mathbb{Z}$, δηλαδή $n = m \cdot k$. Συνεπώς από το ίδιο πόρισμα έχουμε ότι

$$\mathbb{Z}_m = \frac{\mathbb{Z}}{m\mathbb{Z}} \cong \frac{\frac{\mathbb{Z}}{n\mathbb{Z}}}{\frac{m\mathbb{Z}}{n\mathbb{Z}}} = \frac{\mathbb{Z}_n}{\frac{m\mathbb{Z}}{n\mathbb{Z}}}.$$

Αλλά η αντιστοιχία $m\mathbb{Z} \longrightarrow \mathbb{Z}_k$, $mz \longrightarrow z + k\mathbb{Z}$, είναι ένας επιμορφισμός ομάδων που ο πυρήνας του είναι το σύνολο $n\mathbb{Z}$ και επομένως $m\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_k$. Άρα $\mathbb{Z}_m \cong \mathbb{Z}_{m\cdot k}/\mathbb{Z}_k$ (αυτό το έχουμε ξαναδεί στο θεώρημα της δομής των κυκλικών ομάδων).

3. Είδαμε στο Παράδειγμα 4.7.8(4) ότι $SL_n(K) \trianglelefteq GL_n(K)$. Συνεπώς για κάθε υποομάδα H της $GL_n(K)$ το γινόμενο $H \cdot SL_n(K)$ είναι υποομάδα της $GL_n(K)$. Στο Παράδειγμα 4.5.8(4) είχαμε δει ότι $L \cdot SL_n(K) = GL_n(K)$, όπου

$$L = \left\{ \begin{pmatrix} r & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \text{με } r \in K^* \right\}$$

και $L \cap SL_n(K) = \{I\}$. Επίσης αν D είναι η υποομάδα όλων των διαγωνίων πινάκων της $GL_n(K)$ πάλι έχουμε $D \cdot SL_n(K) = GL_n(K)$ αλλά $D \cap SL_n(K) \neq \{\,I\,\}$. Εφαρμόζοντας το Θεώρημα 4.7.12, παίρνουμε

$$K^* \cong L \cong \frac{L}{SL_n(K) \cap L} \cong \frac{GL_n(K)}{SL_n(K)} \cong \frac{D}{D \cap SL_n(K)}.$$

Αν Z είναι το κέντρο της $GL_n(K)$ τότε η υποομάδα $Z \cdot SL_n(K)$ είναι κανονική αφού και οι δύο υποομάδες Z και $SL_n(K)$ είναι κανονικές. Παρατηρούμε ότι οι υποομάδες D και L δεν είναι κανονικές υποομάδες (γιατί;) αλλά τα γινόμενα $D \cdot SL_n(K)$ και $L \cdot SL_n(K)$ είναι κανονικές υποομάδες.

4. Είναι εύκολο να δειχτεί ότι υπάρχει ένας μοναδικός επιμορφισμός ομάδων $\phi : S_4 \longrightarrow S_3$ με $(1\,2) \longrightarrow (1\,2)$ και $(1\,3\,4) \longrightarrow (1\,2\,3)$. Ο πυρήνας του

ϕ είναι η υποομάδα $K = \{\,1,\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\,\}$ του Klein. Έτσι έχουμε

$$\phi^{-1}(\{\,i\,\}) = K$$

$$\phi^{-1}(\{\,i,\ (1\,2)\,\}) = K \cup (1\,2)K$$

$$\phi^{-1}(\{\,i,\ (1\,3)\,\}) = K \cup (1\,3)K$$

$$\phi^{-1}(\{\,i,\ (2\,3)\,\}) = K \cup (2\,3)K$$

$$\phi^{-1}(\{\,i,\ (1\,2\,3),\ (1\,3\,2)\,\}) = K \cup (1\,2\,3)K \cup (1\,3\,2)K = A_4$$

$$\phi^{-1}(S_3) = S_4.$$

Συνεπώς οι μόνες κανονικές υποομάδες της S_4 που περιέχουν την K είναι οι K, A_4 και S_4. Θα δείξουμε ότι αυτές είναι οι μόνες κανονικές υποομάδες της S_4. Επειδή η S_4 είναι σχετικά μικρή ομάδα θα μπορούσαμε να βρούμε όλες τις υποομάδες της και να εξετάζαμε ποιες από αυτές είναι κανονικές. Ένας άλλος πιο κομψός τρόπος είναι ο εξής. Αν $\{\,i\,\} \neq H \trianglelefteq S_4$, τότε $K \leq H$. Πράγματι, αν $K \not\leq H$ τότε $K \cap H \neq \{\,i\,\}$ ή $K \cap H = \{\,i\,\}$. Αλλά αν $\sigma \in K \cap H$ με $\sigma \neq i$, επειδή όλες οι μεταθέσεις, οι διάφορες της ταυτοτικής, που ανήκουν στην K είναι του ίδιου τύπου και είναι οι μόνες μεταθέσεις αυτού του τύπου στην S_4, θα πρέπει όλες αυτές να ανήκουν στην $H \cap K$ (γιατί;). Συνεπώς $H \cap K = K$, δηλαδή $K \leq H$. Έστω ότι $H \cap K = \{\,i\,\}$. Επειδή και οι δύο είναι κανονικές υποομάδες, η KH είναι κανονική υποομάδα που περιέχει την K άρα η KH θα είναι η A_4 ή όλη η ομάδα S_4. Επειδή $\mid KH \mid = \mid K \mid\mid H \mid$, θα πρέπει $\mid H \mid = 3$ ή 6. Αν $\mid H \mid = 3$, τότε η H περιέχει ένα 3-κύκλο και επειδή είναι κανονική θα πρέπει να περιέχει όλους τους 3-κύκλους (γιατί;). Άρα δεν μπορεί να είναι $\mid H \mid = 3$ και συνεπώς $KH \neq A_4$. Αν ήταν $\mid H \mid = 6$, δηλαδή $KH = S_4$, επειδή $S_4/K \cong S_3$, θα είχαμε $KH/K \cong H/K \cap H \cong H \cong S_3$. Μια υποομάδα της S_4 που είναι ισόμορφη με την S_3 θα πρέπει να περιέχει δύο μόνο 3-κύκλους (ο ένας αντίστροφος του άλλου). Αλλά όλοι οι 3-κύκλοι είναι συζυγείς μεταθέσεις (βλέπε Θεώρημα 4.2.15). Συνεπώς μια τέτοια υποομάδα δεν μπορεί να είναι κανονική. Αυτές οι υποομάδες είναι, προς χάρη της πληρότητας, οι εξής:

$$\{\,1,\ (1\,2\,3),\ (1\,3\,2),\ (1\,2),\ (1\,3),\ (2\,3)\,\}$$

$$\{\,1,\ (1\,2\,4),\ (1\,4\,2),\ (1\,2),\ (1\,4),\ (2\,4)\,\}$$

$$\{\,1,\ (1\,3\,4),\ (1\,4\,3),\ (1\,3),\ (1\,4),\ (4\,3)\,\}$$

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

Ασκήσεις 4.7

1. Έστω ότι η H είναι η μοναδική υποομάδα τάξης m μιας ομάδας G. Δείξτε ότι η H είναι κανονική στη G.

2. Έστω G μια ομάδα και $a \in G$ με $\langle a \rangle$ τη μοναδική υποομάδα τάξης 3. Δείξτε ότι $g^2 \cdot a = a \cdot g^2$, για κάθε $g \in G$.

3. Έστω $\pi = (12345)$, $\tau = (25)\cdot(34) \in S_5$. Δείξτε ότι:
   i) $\tau \cdot \pi \cdot \tau = \pi^{-1}$.
   ii) $< \pi > \lhd < \pi, \tau >$.
   iii) $D_5 \cong < \pi, \tau >$.

4. Έστω G ομάδα και H, K κανονικές υποομάδες της με $H \cap K = \{1\}$. Δείξτε ότι $hk = kh$, για όλα τα $h \in H$ και $k \in K$.

5. Έστω G ομάδα με τάξη 26. Να βρεθούν όλες οι κανονικές υποομάδες της.

6. Έστω G ομάδα με τάξη 210 και K κανονική υποομάδα της G με τάξη 7.
   i) Δείξτε ότι $x^{30} \in K$ για κάθε $x \in G$.
   ii) Αν $x \in G$ με $x^7 \in K$, τότε $x \in K$.
   iii) Δείξτε ότι για το στοιχείο $g \in G$ ισχύει η ισοδυναμία
   $g \in K \iff g^{37} \in K$.
   iv) Αν $M \lhd G$ με $|M| = 6$. Δείξτε ότι $KM \lhd G$. Ποιός είναι ο δείκτης της KM στην G; Γιατί η G/KM είναι κυκλική;

7. Έστω G ομάδα και a ένα στοιχείο άπειρης τάξης, ώστε $<a> \lhd G$. Δείξτε ότι $g^2 \cdot a = a \cdot g^2$ για κάθε $g \in G$.

8. Έστω G ομάδα και M κανονική υποομάδα της έτσι ώστε το πηλίκο G/M να είναι άπειρη κυκλική. Δείξτε ότι για κάθε θετικό ακέραιο n υπάρχει κανονική υποομάδα N_n της G με $|G : N_n| = n$.

9. Να βρεθεί η ομάδα πηλίκο G/H, όπου $G = Q_8$ είναι η ομάδα των quaternions και $H = Z(Q_8)$. Όμοια αν $G = D_4$ και $H = Z(D_4)$.

10. Έστω $G = \langle 2^x 3^y 5^z \ x, y, z \in \mathbb{Z} \rangle$ και $H = \langle 2^x, \ x \in \mathbb{Z} \rangle$. Περιγράψτε την ομάδα πηλίκο G/H.

11. Έστω G ομάδα και H κανονική υποομάδα της. Δείξτε ότι η G έχει ένα στοιχείο άπειρης τάξης αν και μόνο η H ή η G/H έχει ένα στοιχείο άπειρης τάξης.

12. Έστω G ομάδα και N_1, N_2 κανονικές υποομάδες της. Δίνεται η απεικόνιση $\varphi : G \longrightarrow G/N_1 \times G/N_2$ με $g \longrightarrow (gN_1, gN_2)$. Δείξτε ότι η φ είναι ένας ομομορφισμός ομάδων και ότι η φ είναι μονομορφισμός αν και μόνο αν $N_1 \cap N_2 = 1$.

13. Έστω G μια ομάδα και A κανονική υποομάδα της τάξης 2. Υποθέτουμε ότι το πηλίκο G/A είναι κυκλικό. Δείξτε ότι η G είναι Αβελιανή.
Υπόδειξη: Δείξτε ότι η A είναι υποομάδα του κέντρου της G.

14. Έστω G μια μη Αβελιανή ομάδα. Δείξτε ότι η ομάδα αυτομορφισμών $AutG$ της G δεν είναι κυκλική.

15. Έστω G μια ομάδα και N μια υποομάδα της με την ιδιότητα $N \cap G' = 1$, όπου G' είναι η ομάδα μεταθετών της G. Δείξτε ότι η N είναι Αβελιανή. Αν επιπλέον η N είναι κανονική υποομάδα δείξτε ότι $N \leq Z(G)$, όπου $Z(G)$ ειναι το κέντρο της G.

16. Θεωρούμε την ομάδα $U(\mathbb{Z}_{16})$. Δείξτε ότι το 16 διαιρεί τον αριθμό $m^4 - 1$ για κάθε περιττό αριθμό m.

17. Δείξτε ότι αν H είναι μια κυκλική κανονική υποομάδα μιας ομάδας τότε κάθε υποομάδα της H είναι κανονική υποομάδα της G.

18. Έστω G μια ομάδα και H μια υποομάδα της, η οποία περιέχεται στο κέντρο $Z(G)$ της G. Αν η ομάδα πηλίκο G/H είναι κυκλική, δείξτε ότι η ομάδα G είναι Αβελιανή.

19. Έστω G μια ομάδα.

    α) Να δειχτεί όι η ομάδα $Inn(G)$ των εσωτερικών αυτομορφισμών της G είναι κανονική υποομάδα της ομάδας όλων των αυτομορφισμών της G.

    β) Αν $Z(G)$ είναι το κέντρο της G, να δειχτεί ότι η ομάδα πηλίκο $G/Z(G)$ είναι ισόμορφη με την ομάδα $Inn(G)$.
    Υπόδειξη: Θεωρήστε την απεικόνιση $G \longrightarrow Aut(G)$, $g \longrightarrow \tau_g$, όπου τ_g είναι ο εσωτερικός αυτομορφισμός $\tau_g(x) = gxg^{-1}$, $x \in G$.

20. Έστω G μια ομάδα. Δείξτε ότι $[G, G] = \{\, \alpha_1\alpha_2\cdots\alpha_n\alpha_1^{-1}\cdots\alpha_n^{-1} \mid \alpha_i \in G,\ i = 1, 2, \ldots, n,\ n \geq 2\}$.

21. Δίνεται μια ομάδα G. Υποθέτουμε ότι για κάποιο $n > 1$ και για όλα τα $\alpha, \beta \in G$ ισχύει $(\alpha\beta)^n = \alpha^n\beta^n$. Τότε δείξτε ότι

    α) $\{x^n \mid x \in G\} \trianglelefteq G$ και $\{x^{n-1} \mid x \in G\} \trianglelefteq G$.

    β) $\alpha^{n-1}\beta^n = \beta^n\alpha^{n-1}$, για όλα τα α, $\beta \in G$.

γ) $(\alpha\beta\alpha^{-1}\beta^{-1})^{n(n-1)} = 1$, για όλα τα $\alpha, \beta \in G$.

22. Έστω E_{ij} ο τετραγωνικός $n \times n$ πίνακας που έχει σε όλες τις θέσεις 0 εκτός από τη θέση (i, j) στην οποία έχει 1 και $diag(\beta_1, \ldots, \beta_n)$ ο διαγώνιος πίνακας με στοιχεία στην κύρια διαγώνιο τα $\beta_1, \ldots, \beta_n$. Δείξτε ότι για $i \neq j$ και $\beta_1 \cdot \ldots \cdot \beta_n \neq 0$

$$[I_n + \alpha E_{ij}, diag(\beta_1, \ldots, \beta_n)] = I_n + \frac{\alpha(\beta_j - \beta_i)}{\beta_i} E_{ij}$$

και επιπλέον ότι για $i \neq j \neq k$

$$[I_n + \alpha E_{ij}, I_n + \beta E_{jk}] = I_n + \alpha\beta E_{ik}.$$

Επίσης δείξτε ότι αν $n \geq 3$

$$[GL_n(\mathbb{C}), GL_n(\mathbb{C})] = SL_n(\mathbb{C}) = [SL_n(\mathbb{C}), SL_n(\mathbb{C})].$$

23. Αποδείξτε την εξής γενίκευση του Θεωρήματος 4.7.12: Αν K, H και L είναι υποομάδες της G και $K \trianglelefteq G$, $H \trianglelefteq L$, τότε υπάρχει ένας ισομορφισμός $L\,K/H\,K \cong L/(L \cap K)\,H$.

4.8 Εφαρμογή: Πεπερασμένες Αβελιανές Ομάδες

Εφαρμόζοντας τα προηγούμενα αποτελέσματα μπορούμε τώρα να ταξινομήσουμε όλες τις πεπερασμένες Αβελιανές ομάδες. Δηλαδή μπορούμε να απαντήσουμε στο βασικό ερώτημα πότε δύο τέτοιες ομάδες είναι ισόμορφες ή όχι, δίνοντας έναν κατάλογο όλων των μη ισόμορφων Αβελιανών πεπερασμένων ομάδων μιας δεδομένης τάξης. Όπως θα δούμε, αυτός ο κατάλογος αποτελείται από ομάδες της μορφής

$$C_{p_1^{n_1}} \times C_{p_2^{n_2}} \times \cdots \times C_{p_s^{n_s}},$$

όπου τα p_i είναι πρώτοι αριθμοί όχι κατ' ανάγκη διακεκριμένοι.

Κατ' αρχήν αποδεικνύουμε ότι για τις πεπερασμένες Αβελιανές ομάδες ισχύει το αντίστροφο του θεωρήματος του Lagrange.

4.8.1 Θεώρημα. *Έστω G μια πεπερασμένη Αβελιανή ομάδα τάξης n. Τότε ισχύουν τα εξής.*

1. *Για κάθε διαιρέτη m του n υπάρχει μια υποομάδα της G που έχει τάξη m.*
2. *Αν $n = m_1 m_2$, όπου ο μ.κ.δ.$(m_1, m_2) = 1$, τότε η G έχει δύο μοναδικές υποομάδες G_1, G_2 τάξεων m_1, m_2 αντίστοιχα και ισχύει*

$$G = G_1 G_2 \quad \text{και} \quad G_1 \cap G_2 = \{1\}.$$

Σ' αυτή την περίπτωση κάθε στοιχείο g της G γράφεται μοναδικά στη μορφή $g = g_1 g_2$, $g_1 \in G_1$, $g_2 \in G_2$ και η G είναι ισόμορφη με το καρτεσιανό γινόμενο $G_1 \times G_2$.

Απόδειξη. Εφαρμόζουμε επαγωγή στο n. Η περίπτωση $n = 1$ είναι τετριμμένη. Επίσης αν ο n είναι ένας πρώτος αριθμός οι μόνες υποομάδες της G είναι η $\{1\}$ και η G (βλέπε 4.4.26). Υποθέτουμε ότι ο n είναι σύνθετος αριθμός και έστω m ένας γνήσιος διαιρέτης του n, $1 < m < n$. Τότε, σύμφωνα με το Παράδειγμα 4.7.8 (7)), αν p είναι ένας πρώτος διαιρέτης του m, η G έχει ένα στοιχείο g τάξης p. Η ομάδα πηλίκο $G/\langle g \rangle$ έχει τάξη $\frac{n}{p}$ και συνεπώς επαγωγικά η $G/\langle g \rangle$ έχει μια υποομάδα τάξης $\frac{m}{p}$. Αυτή η υποομάδα, σύμφωνα με το Πόρισμα 4.7.11, είναι της μορφής $H/\langle g \rangle$ για μια (μοναδική) υποομάδα H της G που περιέχει την $\langle g \rangle$. Συνεπώς $|H/\langle g \rangle| = \frac{m}{p}$ που σημαίνει ότι $|H| = m$.

Έστω τώρα ότι $n = m_1 m_2$ όπου ο μ.κ.δ.$(m_1, m_2) = 1$. Όπως μόλις δείξαμε υπάρχουν δύο υποομάδες G_1, G_2 με $|G_1| = m_1$ και $|G_2| = m_2$. Άρα $|G : G_1| = m_2$ και $|G : G_2| = m_1$. Σύμφωνα με το Πόρισμα 4.7.14, οι G_1 και G_2 είναι μοναδικές. Έστω $h \in G_1 \cap G_2$. Επειδή $h \in G_1$ και $h_2 \in G_2$, σύμφωνα με το 4.4.23, θα πρέπει $h^{m_1} = h^{m_2} = 1$. Αλλά η τάξη του h θα πρέπει να διαιρεί

το m_1 και το m_2 (βλέπε 4.3.11). Συνεπώς $h = 1$, αφού ο μ.κ.δ.$(m_1, m_2) = 1$. Επομένως $G_1 \cap G_2 = \{1\}$. Έτσι έχουμε $|G_1G_2| = |G_1| \frac{|G_2|}{|G_1 \cap G_2|} = |G_1||G_2| = m_1m_2 = |G|$ και άρα $G = G_1G_2$.

Στην προκειμένη περίπτωση, έστω $s \in G$, $s = g_1g_2$, $g_1 \in G_1$, $g_2 \in G_2$ και $s = g_1'g_2'$, $g_1' \in G_1$, $g_2' \in G_2$. Τότε $g_1^{-1}g_1'g_2'g_2^{-1} = 1$, άρα $g_2'g_2^{-1} \in G_1$, αφού $g_1^{-1}g_1' \in G_1$. Δηλαδή $g_2'g_2^{-1} \in G_1 \cap G_2 = \{1\}$ που σημαίνει $g_2 = g_2'$. Όμοια $g_1 = g_1'$. Από το γεγονός αυτό προκύπτει ότι ο ομομορφισμός

$$G_1 \times G_2 \longrightarrow G,\ (g_1, g_2) \longrightarrow g_1g_2,$$

είναι ένας ισομορφισμός ομάδων. ⊤

4.8.2 Παράδειγμα. Έστω G μια Αβελιανή ομάδα τάξης 12. Οι γνήσιοι διαιρέτες του 12 είναι 2, 3, 4 και 6. Αν η G είναι κυκλική, σύμφωνα με το θεώρημα δομής των κυκλικών ομάδων, η G έχει μοναδικές υποομάδες τάξης 2, 3, 4 και 6, την ύπαρξη των οποίων αναφέρει και το προηγούμενο θεώρημα. Αν $G = \langle g \rangle$, τότε αυτές είναι οι $\langle g^6 \rangle$, $\langle g^4 \rangle$, $\langle g^3 \rangle$ και $\langle g^2 \rangle$ αντίστοιχα. Ισχύει δε

$$\langle g \rangle = \langle g^4 \rangle \langle g^3 \rangle \cong \langle g^4 \rangle \times \langle g^3 \rangle \cong C_3 \times C_4.$$

Έστω ότι η G δεν είναι κυκλική. Αυτή έχει ένα στοιχείο g τάξης 2 και ένα στοιχείο h τάξης 3. Οπότε το γινόμενό τους $s = gh$ έχει τάξη 6 (γιατί;) και έχουμε $\langle s \rangle = \langle g \rangle \langle h \rangle \cong \langle g \rangle \times \langle h \rangle \cong C_2 \times C_3$. Το στοιχείο $h = s^2$ είναι το μοναδικό στοιχείο της G τάξης 3. Πράγματι, αυτό είναι το μοναδικό στοιχείο τάξης 3 της $\langle s \rangle$. Αν t είναι ένα άλλο στοιχείο της G τάξης 3, τότε $G = \langle s \rangle \dot{\cup} t\langle s \rangle$. Συνεπώς $t^2 = t^{-1} \in \langle s \rangle$ που σημαίνει ότι $t \in \langle s \rangle$ που είναι άτοπο. Επίσης η G εκτός από το g, που είναι το μοναδικό στοιχείο της $\langle s \rangle$ τάξης 2, θα πρέπει να έχει και άλλο στοιχείο τάξης 2. Διότι διαφορετικά τα στοιχεία του υποσυνόλου $G \setminus \langle s \rangle$, που είναι πλήθους 6, θα έπρεπε να είναι τάξης 4 ή 6. Επειδή η G δεν είναι κυκλική, αυτή δεν έχει κανένα στοιχείο τάξης 4 (γιατί;). Από την άλλη πλευρά, αν $s' \in G \setminus \langle s \rangle$ είχε τάξη 6 τότε το $s'^3 \in \langle s \rangle$ και $s'^2 \in \langle s \rangle$ και άρα $\langle s' \rangle = \langle s \rangle$ που είναι άτοπο. Επομένως υπάρχει $w \in G$ που δεν ανήκει στην $\langle s \rangle$ και έχει τάξη 2. Άρα έχουμε $G = \langle w \rangle \langle g \rangle \langle h \rangle \cong \langle w \rangle \times \langle g \rangle \times \langle h \rangle \cong C_2 \times C_2 \times C_3$. Αυτό το αποτέλεσμα προκύπτει άμεσα από το Θεώρημα 4.8.1, καθώς είναι $12 = 3 \cdot 4$ και συνεπώς υπάρχουν δύο μοναδικές υποομάδες της G τάξης 3 και 4. Αυτή που είναι τάξης 4 αν δεν είναι κυκλική είναι ισόμορφη με το καρτεσιανό γινόμενο $C_2 \times C_2$ και συνεπώς η G είναι ισόμορφη με την $C_4 \times C_3$ ή με την $C_2 \times C_2 \times C_3$.

4.8.3 Εφαρμογή. Ως εφαρμογή του Θεώρήματος 4.8.1 θα δείξουμε ότι μεταξύ των Αβελιανών ομάδων $U(\mathbb{Z}_m)$ οι μόνες κυκλικές είναι αυτές για τις οποίες το m είναι 2, 4 ή της μορφής $2p^n$ ή p^n, όπου p είναι ένας περιττός πρώτος αριθμός

και n ένας οποιοσδήποτε φυσικός αριθμός. Αυτό το αποτέλεσμα έχει εφαρμογές στη Θεωρία Αριθμών, όπως για παράδειγμα στη δεκαδική παράσταση ενός ρητού αριθμού.

Κατ' αρχήν έχουμε $U(\mathbb{Z}_2) = \{1\}$ και $U(\mathbb{Z}_4) \cong C_2$. Έστω τώρα p ένας περιττός πρώτος αριθμός. Τότε γνωρίζουμε (βλέπε Θεώρημα 4.6.7 και Άσκηση 2.1 13)) ότι

$$U(\mathbb{Z}_{2p^n}) \cong U(\mathbb{Z}_2 \times \mathbb{Z}_{p^n}) = U(\mathbb{Z}_2) \times U(\mathbb{Z}_{p^n}) \cong U(\mathbb{Z}_{p^n}).$$

Αρκεί λοιπόν να δειχτεί ότι η ομάδα $U(\mathbb{Z}_{p^n})$ είναι κυκλική. Μπορούμε να περιοριστούμε στην περίπτωση όπου $n \geq 2$, αφού, όπως έχουμε δείξει στην Εφαρμογή 4.6.8(2), η ομάδα $U(\mathbb{Z}_p) = \mathbb{Z}_p^*$ είναι κυκλική.

Η τάξη της ομάδας $U(\mathbb{Z}_{p^n})$ είναι ίση με $\varphi(p^n) = p^{n-1}(p-1)$ και έτσι, καθώς οι ακέραιοι p^{n-1} και $p-1$ είναι σχετικά πρώτοι, υπάρχουν μοναδικές υποομάδες G_1 και G_2 με $|G_1| = p^{n-1}$, $|G_2| = p-1$ για τις οποίες έχουμε $U(\mathbb{Z}_{p^n}) = G_1G_2$, $G_1 \cap G_2 = \{1\}$. Αν δείξουμε ότι αυτές οι δύο υποομάδες είναι κυκλικές τότε η $U(\mathbb{Z}_{p^n})$ είναι κυκλική (γιατί;).

Καθώς η G_1 είναι η μοναδική υποομάδα τάξης p^{n-1}, αν βρούμε μια κλάση υπολοίπων modulo p^n που έχει τάξη p^{n-1}, τότε αυτή θα παράγει την G_1. Δείχνουμε επαγωγικά ότι για κάθε $t \in \mathbb{N}$ ισχύει $(1+p)^{p^t} \equiv 1 \bmod p^{t+1}$ αλλά $(1+p)^{p^t} \not\equiv 1 \bmod p^{t+2}$. Για $t = 0$ έχουμε $(1+p) \equiv 1 \bmod p$ ενώ $(1+p) \not\equiv 1 \bmod p^2$. Από την υπόθεση της επαγωγής έχουμε ότι $(1+p)^{p^t} \equiv 1 + rp^{t+1}$ αλλά $r \not\equiv 0 \bmod p$. Έτσι έχουμε

$$(1+p)^{p^{t+1}} = (1+rp^{t+1})^p = 1 + rp^{t+2} + \sum_{i=2}^{p} \binom{p}{i} (rp^{t+1})^i = 1 + rp^{t+2} + sp^{t+3},$$

αφού $p \geq 3$ και $\binom{p}{i} \equiv 0 \bmod p$, $i \leq i \leq p-1$. Αυτό δείχνει ότι $(1+p)^{p^{t+1}} \equiv 1 \bmod p^{t+2}$ αλλά $(1+p)^{p^{t+1}} \not\equiv 1 \bmod p^{t+3}$. Ειδικότερα, θα ισχύει $(1+p)^{p^{n-1}} \equiv 1 \bmod p^n$ ενώ $(1+p)^{p^{n-2}} \not\equiv 1 \bmod p^n$. Με άλλα λόγια, η κλάση modulo p^n του $1+p$ έχει τάξη p^{n-1} και άρα, όπως εξηγήσαμε παραπάνω, αυτή θα παράγει την ομάδα G_1.

Τώρα, λόγω του Θεωρήματος 4.7.12, έχουμε

$$U(\mathbb{Z}_{p^n})/G_1 = G_1G_2/G_1 \cong G_2/G_1 \cap G_2 \cong G_2.$$

Παρατηρούμε όμως ότι η αντιστοιχία

$$\phi : U(\mathbb{Z}_{p^n}) \longrightarrow U(\mathbb{Z}_p),\ r \bmod p^n \longrightarrow r \bmod p,$$

είναι ένας επιμορφισμός ομάδων με πυρήνα την υποομάδα G_1. Πράγματι, η αντιστοιχία αυτή είναι μια καλά ορισμένη απεικόνιση, η οποία είναι επί (γιατί;).

Επιπλέον, ισχύει $\phi(r_1 r_2 \bmod p^n) = \phi(r_1 \bmod p)\phi(r_2 \bmod p)$ και άρα η ϕ είναι ομομορφισμός. Είναι δε $\ker\phi = \{r \bmod p^n \in U(\mathbb{Z}_{p^n}) \mid r \equiv 1 \bmod p\}$ και άρα $(1+p) \bmod p^n \in \ker\phi$, δηλαδή $G_1 \subseteq \ker\phi$. Καθώς

$$|U(\mathbb{Z}_{p^n})/G_1| = p - 1 = |U(\mathbb{Z}_{p^n})/\ker\phi|,$$

θα πρέπει $G_1 = \ker\phi$ και άρα η ομάδα $G_2 \cong U(\mathbb{Z}_{p^n})/G_1 \cong U(\mathbb{Z}_p) = \mathbb{Z}_{p-1}$ είναι επίσης κυκλική.

Απομένει τώρα να αποδείξουμε ότι ισχύει και το αντίστροφο, δηλαδή ότι αν το m δεν είναι 2, 4 ή της μορφής p^n ή $2p^n$, όπου p περιττός πρώτος, τότε η ομάδα $U(\mathbb{Z}_m)$ δεν είναι κυκλική. Κατ' αρχήν, παρατηρούμε ότι αν η ανάλυση του m σε διακεκριμένους πρώτους είναι της μορφής $2^\alpha p_1^{m_1}\cdots p_k^{m_k}$, όπου $k \geq 2$, $\alpha = 0, 1, 2$, τότε η $U(\mathbb{Z}_m)$ είναι ισόμορφη με το γινόμενο $C_{(p_1-1)p_1^{m_1-1}} \times \cdots \times C_{(p_k-1)p_k^{m_k-1}}$ για $\alpha = 0, 1$ και με το γινόμενο $C_2 \times C_{(p_1-1)p_1^{m_1-1}} \times \cdots \times C_{(p_k-1)p_k^{m_k-1}}$ για $\alpha = 2$ και άρα δεν είναι κυκλική (γιατί;). Αν αποδείξουμε ότι η ομάδα $U(\mathbb{Z}_{2^\alpha})$ για $\alpha \geq 3$ δεν είναι κυκλική, τότε και η $U(\mathbb{Z}_m)$ δεν θα είναι κυκλική για $m = 2^\alpha p_1^{m_1}\cdots p_k^{m_k}$ με $\alpha \geq 3$.

Έστω λοιπόν $m = 2^\alpha$, $\alpha \geq 3$. Αποδεικνύουμε επαγωγικά ότι η τάξη κάθε στοιχείου της $U(\mathbb{Z}_m)$ είναι μικρότερη από την τάξη $2^{\alpha-1}$ της $U(\mathbb{Z}_m)$. Για $\alpha = 3$ θεωρούμε μια κλάση $r \bmod 8 \in U(\mathbb{Z}_8)$. Τότε, $r = 4k+1$ ή $r = 4k-1$ και άρα $r^2 = 1 \pm 8k + 16k^2$. Συνεπώς, $r^2 \equiv 1 \bmod 8$, ενώ η ομάδα $U(\mathbb{Z}_8)$ έχει τάξη 4. Υποθέτουμε ότι $r^{2^{t-2}} \equiv 1 \bmod 2^t$, δηλαδή ότι $r^{2^{t-2}} = 1 + \lambda 2^t$ για κάποιον ακέραιο λ. Τότε $(r^{2^{t-2}})^2 = r^{2^{t-1}} = 1 + \lambda 2^{t+1} + \lambda^2 2^{2t}$ και συνεπώς $r^{2^{t-1}} \equiv 1 \bmod 2^{t+1}$. Άρα για κάθε $r \bmod 2^\alpha \in U(\mathbb{Z}_{2^\alpha})$ ισχύει $r^{2^{\alpha-2}} \equiv 1 \bmod 2^\alpha$, και συνεπώς η $U(\mathbb{Z}_{2^\alpha})$ για $\alpha \geq 3$ δεν είναι κυκλική.[4]

4.8.4 Παρατήρηση. Θα θέλαμε να τονίσουμε εδώ ότι η συνθήκη 2) στο Θεώρημα 4.8.1 είναι και αναγκαία. Δηλαδή αν G_1 και G_2 είναι μοναδικές υποομάδες τάξης m_1 και m_2 αντίστοιχα, τέτοιες ώστε $G = G_1 G_2$, $G_1 \cap G_2 = \{1\}$, τότε μ.κ.δ.$(m_1, m_2) = 1$. Πράγματι, υπάρχει υποομάδα H της G με τάξη ίση με το ε.κ.π.(m_1, m_2) (βλέπε Άσκηση 4.9.5). Επειδή οι m_1 και m_2 διαιρούν την τάξη $|H|$ της H, σύμφωνα με το 1) του Θεωρήματος, υπάρχουν υποομάδες της H τάξης m_1 και m_2. Επειδή οι G_1 και G_2 είναι μοναδικές με αυτές τις τάξεις, θα πρέπει $H = G$ και άρα μ.κ.δ$(m_1, m_2) = 1$.

[4] Δεν είναι δύσκολο να βρούμε μια κλάση που έχει τάξη $2^{\alpha-2}$. Η κλάση $3 \bmod 2^\alpha$ είναι μια από αυτές, αφού ισχύει $3^{2^{\alpha-3}} \not\equiv 1 \bmod 2^\alpha$. Πράγματι, για $\alpha = 3$, έχουμε $3 = (-1+4) \bmod 8 \not\equiv 1 \bmod 8$ και αν υποθέσουμε ότι $3^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \bmod 2^\alpha$, δηλαδή $3^{2^{\alpha-3}} \equiv 1+2^{\alpha-1}+\lambda 2^\alpha$, τότε $3^{2^{\alpha-2}} = (1+2^{\alpha-1})^2 + \lambda^2 2^{2\alpha} + \lambda(1+2^{\alpha-1})2^{\alpha+1} \equiv (1+2^{\alpha-1})^2 \bmod 2^{\alpha+1} = (1+2^\alpha+2^{2\alpha-2}) \bmod 2^{\alpha+1} \equiv (1+2^\alpha) \bmod 2^{\alpha+1}$. Με βάση την παρατήρηση αυτή και το Λήμμα 4.8.6 παρακάτω, προκύπτει ότι $U(\mathbb{Z}_{2^\alpha}) \cong C_2 \times C_{2^{\alpha-2}}$ για $\alpha \geq 3$.

Επομένως, αν $G = G_1G_2$ με $G_1 \cap G_2 = \{1\}$ και μ.κ.δ.$(|G_1|, |G_2|) \neq 1$, τότε υπάρχουν και άλλες υποομάδες της G με τάξη ίση με $|G_1|$ ή $|G_2|$. Για παράδειγμα, για την ομάδα του Klein $K_4 = \{i, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ έχουμε $K_4 = G_1G_2,\ G_1 \cap G_2 = \{1\}$, όπου $G_1 = \langle (1\,2)(3\,4) \rangle$, $G_2 = \langle (1\,3)(2\,4) \rangle$ και υπάρχει η υποομάδα $G_3 = \langle (1\,4)(2\,3) \rangle$ που είναι διάφορη των G_1 και G_2, είναι δε $|\, G_1 \,| = |\, G_2 \,| = |\, G_3 \,| = 2$.

4.8.5 Πόρισμα. *Έστω G μια πεπερασμένη Αβελιανή ομάδα τάξης $n = n_1 \cdots n_k$, όπου οι n_i είναι ανά δύο σχετικά πρώτοι. Τότε υπάρχουν μοναδικές υποομάδες $G_i,\ i = 1, \ldots, k$ τάξης n_i τέτοιες ώστε*

$$G = G_1 \cdots G_k \quad \textit{και} \quad G_i \cap G_1 \cdots G_{i-1}G_{i+1} \cdots G_k = \{1\},$$

για $i = 1, \ldots, k$. Συνεπώς, αν $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, όπου οι p_i, $i = 1, \ldots, s$, είναι διακεκριμένοι πρώτοι αριθμοί, τότε

$$G = P_1 \cdots P_s \quad \textit{και} \quad P_i \cap P_1 \cdots P_{i-1}P_{i+1} \cdots P_s = \{1\},$$

όπου P_i είναι η μοναδική υποομάδα της G τάξης $p_i^{\alpha_i}$, $i = 1, 2, \ldots, s$.

Απόδειξη. Η ύπαρξη και η μοναδικότητα των υποομάδων G_i με $|G_i| = n_i$ προκύπτει από το προηγούμενο θεώρημα. Τώρα, το γινόμενο $G_1 \cdots G_k$ είναι μια υποομάδα της G, της οποίας η τάξη της διαιρείται με το n_i, αφού $G_i \subseteq G_1 \cdots G_k$. Συνεπώς, έχουμε $|\, G_1 \cdots G_k \,| \geq |\, G \,|$ και άρα $G_1 \cdots G_k = G$. Απομένει να δείξουμε ότι $G_i \cap G_1 \cdots G_{i-1}G_{i+1} \cdots G_k = \{1\}$ για κάθε $i = 1, \ldots, k$. Πράγματι, καθώς η τάξη κάθε στοιχείου της υποομάδας $G_1 \cdots G_{i-1}G_{i+1} \cdots G_k$ διαιρεί το γινόμενο $n_1 \cdots n_{i-1}n_{i+1} \cdots n_k$, η τάξη αυτή είναι σχετικά πρώτη προς το n_i. Από αυτό, έπεται άμεσα ότι η υποομάδα $G_i \cap G_1 \cdots G_{i-1}G_{i+1} \cdots G_k$ είναι τετριμμένη. ⊤

Ας θεωρήσουμε τώρα δύο πεπερασμένες Αβελιανές ομάδες G, H που έχουν την ίδια τάξη n. Έστω $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ η ανάλυση του n σε γινόμενο διακεκριμένων πρώτων και P_i, Q_i οι μοναδικές υποομάδες των G και H αντίστοιχα που έχουν τάξη $p_i^{\alpha_i}$, $i = 1, \ldots, s$. Τότε, $G \cong H$ αν και μόνον αν $P_i \cong Q_i$ για κάθε $i = 1, 2, \ldots, s$. Πράγματι, αν $\phi : G \longrightarrow H$ είναι ένας ισομορφισμός, τότε $|\, \phi(P_i) \,| = p_i^{\alpha_i}$ (γιατί;) και άρα $\phi(P_i) = Q_i$. Άρα ο περιορισμός της ϕ στην P_i είναι ένας ισομορφισμός της P_i στην Q_i. Αντίστροφα αν $\phi_i : P_i \longrightarrow Q_i$, $i = 1, 2, \ldots, s$ είναι ένας ισομορφισμός τότε η αντιστοιχία $\phi : G \longrightarrow H$, $g_1g_2 \cdots g_s \longrightarrow \phi_1(g_1) \cdots \phi_s(g_s)$, όπου $g_i \in P_i$, $i = 1, 2, \ldots, s$, είναι ένας ισομορφισμός. Πράγματι, όπως και στην απόδειξη του Θεωρήματος 4.8.1, προκύπτει εύκολα ότι κάθε στοιχείο g της G γράφεται μοναδικά στη μορφή $g = g_1g_2 \cdots g_s$.

Συνεπώς η ϕ είναι απεικόνιση. Έχουμε δε

$$\begin{aligned}\phi(gg') &= \phi(g_1 \cdots g_s g'_1 \cdots g'_s)\\ &= \phi(g_1 g'_1 \cdots g_s g'_s)\\ &= \phi_1(g_1 g'_1) \cdots \phi_s(g_s g'_s)\\ &= \phi_1(g_1) \cdots \phi_s(g_s)\phi_1(g'_1) \cdots \phi_s(g'_s)\\ &= \phi(g)\phi(g'),\end{aligned}$$

όπου $g = g_1 \cdots g_s$ και $g' = g'_1 \cdots g'_s$ είναι οι μοναδικές εκφράσεις δύο στοιχείων $g, g' \in G$ ως γινόμενα στοιχείων των $P_i,\ i = 1, 2, \ldots, s$.

Είναι φανερόν λοιπόν ότι η ταξινόμηση των πεπερασμένων Αβελιανών ομάδων ανάγεται στην ταξινόμηση των Αβελιανών ομάδων G των οποίων η τάξη είναι μια δύναμη ενός πρώτου αριθμού p, δηλαδή $|G| = p^n$ για κάποιο $n \in \mathbb{N}$.

Κατ' αρχήν εξετάζουμε το απλούστερο είδος Αβελιανών ομάδων που είναι οι κυκλικές. Υποθέτουμε ότι η G είναι κυκλική τάξης p^n. Τότε γνωρίζουμε ότι $G \cong C_{p^n}$. Επίσης για κάθε διαιρέτη $p^i,\ i = 0, 1, \ldots, n$, του p^n υπάρχει μια μοναδική υποομάδα τάξης p^i και αυτή είναι η $\langle\, g^{p^{n-i}} \,\rangle$, όπου g είναι ένας γεννήτορας της G. Για $i, j \neq 0$, οι υποομάδες $\langle\, g^{p^{n-i}} \,\rangle$ και $\langle\, g^{p^{n-j}} \,\rangle$ περιέχουν την $\langle\, g^{p^{n-1}} \,\rangle$. Δηλαδή η G δεν μπορεί να γραφεί ως γινόμενο γνήσιων υποομάδων της. Συνεπώς αν G είναι μια κυκλική ομάδα τάξης m και $m = p_1^{n_1} \cdots p_s^{n_s}$ είναι η ανάλυση του m σε γινόμενο δυνάμεων διακεκριμένων πρώτων, τότε η ανάλυση της G ως γινόμενο υποομάδων της που ικανοποιούν την ιδιότητα που αναφέρεται στο Πόρισμα 4.8.5 με τους όσο το δυνατόν περισσότερους παράγοντες είναι η $G = P_1 \cdots P_s$ όπου $|P_i| = p_i^{n_i}$. Αυτό είχε δειχτεί και στο Θεώρημα 4.6.7. ⊺

Το επόμενο Λήμμα είναι το σημαντικότερο βήμα για την ταξινόμηση όλων των πεπερασμένων Αβελιανών ομάδων.

4.8.6 Λήμμα. *Έστω G μια Αβελιανή ομάδα τάξης p^n, όπου p πρώτος. Αν g είναι ένα στοιχείο της G μέγιστης τάξης και η ομάδα πηλίκο $G/\langle\, g \,\rangle$ είναι κυκλική τάξης p^m, τότε υπάρχει ένα $h \in G$ τέτοιο ώστε η κλάση $h\langle\, g \,\rangle$ να παράγει την $G/\langle\, g \,\rangle$ και η τάξη του h να είναι ίση με p^m. Στην περίπτωση αυτή είναι $G = \langle\, h \,\rangle\langle\, g \,\rangle$ και $\langle\, h \,\rangle \cap \langle\, g \,\rangle = \{\, 1 \,\}$.*

Απόδειξη. Έστω p^k η τάξη του g. Τότε για κάθε στοιχείο $x \in G$ ισχύει $x^{p^k} = 1$ (γιατί;). Έστω $f\langle\, g \,\rangle$ ένας γεννήτορας της $G/\langle\, g \,\rangle$, οπότε $f^{p^m} = g^\lambda$, για κάποιο $\lambda \in \mathbb{N}$, όπου $m = n - k$. Σημειώνουμε ότι $k \geq m$, αφού η τάξη του $f\langle\, g \,\rangle$ είναι p^m και $f^{p^k} = 1 \in \langle\, g \,\rangle$. Έτσι έχουμε

$$1 = (f^{p^m})^{p^{k-m}} = g^{\lambda p^{k-m}}.$$

Άρα το p^k διαιρεί το λp^{k-m}, έστω $rp^k = \lambda p^{k-m}$. Θέτοντας $h = fg^{-r}$, έχουμε ότι $h^{p^m} = f^{p^m} g^{-rp^m} = g^\lambda g^{-\lambda} = 1$ και $h\langle g\rangle = f\langle g\rangle$, όπως απαιτείται. Από αυτό προκύπτει ότι $\langle h\rangle \cap \langle g\rangle = \{1\}$, διότι μια σχέση $h^\ell = g^t$ σημαίνει ότι $(h\langle g\rangle)^\ell = \langle g\rangle$ και άρα το p^m διαιρεί το ℓ, οπότε $h^\ell = 1$.

Τέλος είναι φανερό ότι κάθε στοιχείο $x \in G$ γράφεται ως γινόμενο $x = h^i g^j$ και άρα $G = \langle h\rangle\langle g\rangle$. ⊤

4.8.7 Παράδειγμα. Έστω G μια ομάδα τάξης p^3, όπου p είναι πρώτος. Υποθέτουμε ότι η G είναι Αβελιανή, αλλά όχι κυκλική. Γνωρίζουμε ότι η G έχει τουλάχιστον μια υποομάδα τάξης p. Αν η G έχει ένα στοιχείο g τάξης p^2, τότε η $G/\langle g\rangle$ είναι κυκλική τάξης p και σύμφωνα με το προηγούμενο Λήμμα η G έχει ένα στοιχείο h τάξης p τέτοιο ώστε η κλάση $h\langle g\rangle$ παράγει την $G/\langle g\rangle$. Άρα $G = \langle h\rangle\langle g\rangle$ με $\langle h\rangle \cap \langle g\rangle = \{1\}$. Συνεπώς $G \cong C_p \times C_{p^2}$.

Τώρα, αν η G δεν έχει κανένα στοιχείο τάξης p^2, τότε όλα τα μη ουδέτερα στοιχεία της είναι τάξης p. Έστω $g \neq 1$ ένα στοιχείο της G. Η ομάδα πηλίκο $G/\langle g\rangle$ έχει τάξη p^2 και δεν μπορεί να είναι κυκλική, διότι διαφορετικά η G θα είχε ένα στοιχείο h τάξης p^2 τέτοιο ώστε η κλάση $h\langle g\rangle$ θα παρήγαγε την $G/\langle g\rangle$. Συνεπώς όλα τα στοιχεία, εκτός από το ουδέτερο, της $G/\langle g\rangle$ είναι τάξης p. Έστω $h\langle g\rangle$ ένα τέτοιο στοιχείο. Τότε $h^p = 1$ και συνεπώς $\langle h\rangle \cap \langle g\rangle = \{1\}$. Από το Θεώρημα 4.7.12 στην υποομάδα $\langle h\rangle\langle g\rangle$ της G αντιστοιχεί η υποομάδα $\langle h\rangle\langle g\rangle/\langle g\rangle$ της $G/\langle g\rangle$ που είναι η υποομάδα που παράγεται από το στοιχείο της $h\langle g\rangle$. Τώρα η ομάδα πηλίκο

$$\frac{\dfrac{G}{\langle g\rangle}}{\dfrac{\langle h\rangle\langle g\rangle}{\langle g\rangle}} \cong \frac{G}{\langle h\rangle\langle g\rangle}$$

είναι τάξης p και παράγεται από κάθε μη ουδέτερο στοιχείο της $f\langle h\rangle\langle g\rangle$ όπου $f^p = 1$ και $\langle f\rangle \cap \langle h\rangle\langle g\rangle = 1$. Τελικά βλέπουμε ότι αν όλα τα μη ουδέτερα στοιχεία της G έχουν τάξη p, τότε υπάρχουν στοιχεία g, h, $f \in G$ τέτοια ώστε $G = \langle g\rangle\langle h\rangle\langle f\rangle$ και $\langle g\rangle \cap \langle h\rangle\langle f\rangle = \langle h\rangle \cap \langle f\rangle\langle g\rangle = \langle f\rangle \cap \langle h\rangle\langle g\rangle = \{1\}$ (γιατί;). Αυτό συνάγεται άμεσα και από την επόμενη πρόταση.

4.8.8 Πρόταση. *Έστω G μια Αβελιανή ομάδα τάξης p^n, όπου p πρώτος. Τότε υπάρχουν κυκλικές υποομάδες $G_1, G_2, \ldots, G_k$ της G τέτοιες ώστε κάθε στοιχείο g της G γράφεται μοναδικά στη μορφή*

$$g = g_1 g_2 \cdots g_k, \quad g_i \in G_i, \quad i = 1, 2, \ldots, k.$$

Απόδειξη. Εφαρμόζουμε επαγωγή στην τάξη $|G|$ της G (δηλαδή στο n). Για $n = 1$, είναι γνωστό ότι η G είναι κυκλική. Υποθέτουμε ότι η Πρόταση

ισχύει για όλες τις ομάδες τάξης μικρότερης από p^n. Έστω g ένα στοιχείο της G που έχει μέγιστη τάξη, έστω p^m. Αν $m = n$ τότε η G είναι κυκλική και η Πρόταση ισχύει. Έστω $m < n$. Τότε η Πρόταση ισχύει για την ομάδα πηλίκο $G/\langle g \rangle = H$ που έχει τάξη p^{n-m}. Δηλαδή υπάρχουν κυκλικές υποομάδες $H_1, H_2, \ldots, H_s$ της H τέτοιες ώστε το κάθε στοιχείο $h\langle g \rangle$, $h \in G$, της H να γράφεται μοναδικά στη μορφή

$$h\langle g \rangle = h_1\langle g \rangle \cdots h_k\langle g \rangle,\ h_i\langle g \rangle \in H_i.$$

Συνεπώς $h = h_1 h_2 \cdots h_k g^\lambda$, για κάποιο $\lambda \in \mathbb{N},\ \lambda < p^m$. Από το Πόρισμα 4.7.11 υπάρχει μοναδική υποομάδα G_i της G τέτοια ώστε $H_i = G_i/\langle g \rangle$, $i = 1, 2, \ldots, s$. Από το προηγούμενο Λήμμα, επειδή η G_i έχει τάξη μια δύναμη του p και η $G_i/\langle g \rangle$ είναι κυκλική, υπάρχει ένα στοιχείο $g_i \in G_i$ που η κλάση $g_i\langle g \rangle$ παράγει την $G_i/\langle g \rangle$ και η τάξη του g_i είναι ίση με $|\, G_i/\langle g \rangle \,|$. Επομένως το κάθε στοιχείο $h \in G$ γράφεται στη μορφή

$$h = g_1^{\alpha_1} g_2^{\alpha_2} \cdots g_s^{\alpha_s} g^\lambda,\ 0 \le \alpha_i < \left| \frac{G_i}{\langle g \rangle} \right|,\ 0 \le \lambda < p^m$$

και αυτή η έκφραση του h είναι μοναδική. Πράγματι, αν είχαμε

$$g_1^{\alpha_1} g_2^{\alpha_2} \cdots g_s^{\alpha_s} g^\lambda = g_1^{\beta_1} g_2^{\beta_2} \cdots g_s^{\beta_s} g^\mu\,,$$

δηλαδή $g_1^{\alpha_1-\beta_1} g_2^{\alpha_2-\beta_2} \cdots g_s^{\alpha_s-\beta_s} g^{\lambda-\mu} = 1$, τότε έπεται ότι

$$g_1^{\alpha_1-\beta_1}\langle g \rangle \cdots g_s^{\alpha_s-\beta_s}\langle g \rangle = \langle g \rangle\,.$$

Αλλά από την επαγωγική υπόθεση το ουδέτερο στοιχείο $\langle g \rangle$ της $G/\langle g \rangle$ έχει τη μοναδική έκφραση $\langle g \rangle = \langle g \rangle \cdots \langle g \rangle$ (k φορές). Δηλαδή $g_i^{\alpha_i-\beta_i}\langle g \rangle = \langle g \rangle$ ή ισοδύναμα $g_i^{\alpha_i-\beta_i} \in \langle g \rangle$. Αλλά η τάξη του g_i είναι ίση με την τάξη του $g_i\langle g \rangle$ και άρα πρέπει $g_i^{\alpha_i-\beta_i} = 1$. Αυτό μπορεί να συμβεί μόνο αν $\alpha_i = \beta_i$, $i = 1, 2, \ldots, s$, οπότε $\lambda = \mu$. ⊺

4.8.9 Λήμμα. *Έστω $n_1, n_2, \ldots, n_k$ και $m_1, m_2, \ldots, m_s$ δυνάμεις ενός πρώτου αριθμού p τέτοιες ώστε $n_1 \ge n_2 \ge \cdots \ge n_k > 1$ και $m_1 \ge m_2 \ge \cdots \ge m_s > 1$. Τότε τα καρτεσιανά γινόμενα*

$$G = C_{m_1} \times \cdots \times C_{n_k} \quad \textit{και} \quad H = C_{m_1} \times \cdots \times C_{m_s}$$

είναι ισόμορφες ομάδες αν και μόνον αν $k = s$ και $n_i = m_i$ για κάθε i, $1 \le i \le k$.

Απόδειξη. Αν $k = s$ και $n_i = m_i$, για κάθε i, $1 \leq i \leq k$ τότε $G = H$ (οπότε $G \cong H$). Αντίστροφα, υποθέτουμε ότι $G \cong H$. Τότε $\mid G \mid = \mid H \mid = p^n$, για κάποιο n, αφού η τάξη της G διαιρείται μόνο από δυνάμεις του p (γιατί;). Έστω $n_i = p^{\alpha_i},\ 1 \leq i \leq k$ και $m_j = p^{\beta_j},\ 1 \leq j \leq s$. Τότε $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_k \geq 1$ και $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_s \geq 1$, ενώ $\alpha_1 + \alpha_2 + \cdots + \alpha_k = n = \beta_1 + \beta_2 + \cdots + \beta_s$. Θεωρούμε τα υποσύνολα $G^p = \{\, g^p \mid g \in G \,\}$ και $H^p = \{\, h^p \mid h \in H \,\}$ τα οποία είναι υποομάδες της G και H αντίστοιχα (γιατί;). Είναι δε

$$G^p = C^p_{n_1} \times \cdots \times C^p_{n_k} \quad \text{και} \quad H^p = C^p_{m_1} \times \cdots \times C^p_{m_s}\,.$$

Πράγματι, αν $g \in G$, τότε για κάποια $g_i \in C_{n_i}$, έχουμε $g = (g_1, \ldots, g_k)$, οπότε $g^p = (g_1, \ldots, g_k)^p = (g_1, \ldots, g_k) \cdots (g_1, \ldots, g_k) = (g_1^p, \ldots, g_k^p)$. Γνωρίζουμε ότι αν x είναι ένας γεννήτορας της κυκλικής ομάδας C_{p^r}, τότε το στοιχείο x^p είναι γεννήτορας της υποομάδας

$$C_{p^{r-1}} = \langle\, x^p \,\rangle = \{\, (x^p)^i = (x^i)^p \mid x^i \in C_{p^r} \,\} = C^p_{p^r}\,.$$

Άρα $\mid G^p \mid = p^{(\alpha_1-1)+\cdots+(\alpha_k-1)}$ και $\mid H^p \mid = p^{(\beta_1-1)+\cdots+(\beta_s-1)}$. Ας θεωρήσουμε έναν ισομορφισμό $\phi : G \longrightarrow H$. Επειδή $\phi(g^p) = \phi(g)^p$ για κάθε $g \in G$ και $H = \{\, \phi(g) \mid g \in G \,\}$, έπεται ότι $\phi(G^p) = H^p$ και άρα $G^p \cong H^p$. Εφαρμόζουμε τώρα επαγωγή στην τάξη $\mid G \mid = \mid H \mid$ της G, δηλαδή στο n. Αν $n = 1$, τότε $G = C_p = H$ και $\alpha_1 = 1 = \beta_1$, $k = 1 = s$. Έστω ότι $n > 1$. Αν $\alpha_1 = 1$, τότε $\alpha_2 = \cdots = \alpha_k = 1$ και άρα όλα τα μη-ουδέτερα στοιχεία της G είναι τάξης p (γιατί;). Συνεπώς, θα πρέπει και όλα τα $\beta_j,\ j = 1, \ldots, s$ να είναι ίσα με 1 (γιατί;). Επειδή τότε $p^k = \mid G \mid = \mid H \mid = p^s$, προκύπτει ότι $k = s$. Υποθέτουμε ότι $\alpha_1 \neq 1$ και έστω r ο μεγαλύτερος δείκτης i με $\alpha_i \neq 1$, οπότε $\alpha_{r+1} = \alpha_{r+2} = \cdots = \alpha_k = 1$. Επίσης έστω t ο μεγαλύτερος δείκτης j με $\beta_j \neq 1$ οπότε $\beta_{t+1} = \cdots = \beta_s = 1$. Επομένως έχουμε

$$G^p = C^p_{n_1} \times \cdots \times C^p_{n_r} = C_{p^{\alpha_1-1}} \times \cdots \times C_{p^{\alpha_r-1}}$$

και

$$H^p = C^p_{m_1} \times \cdots \times C^p_{m_t} = C_{p^{\beta_1-1}} \times \cdots \times C_{p^{\beta_t-1}}\,.$$

Επειδή $G^p \cong H^p$, η υπόθεση της επαγωγής δίνει $\alpha_1 - 1 = \beta_1 - 1, \ldots, \alpha_r - 1 = \beta_t - 1$ και άρα $n_1 = m_1, \ldots, n_r = m_t$ και $r = t$ (αφού $\mid G^p \mid = \mid H^p \mid < \mid G \mid$). Ισχύει όμως $p^{\alpha_1+\alpha_2+\cdots+\alpha_r+(k-r)} = \mid G \mid = \mid H \mid = p^{\alpha_1+\cdots+\alpha_r+(s-r)}$. Συνεπώς $s = k$. Αυτό σημαίνει τελικά ότι $G = H$. ⊺

4.8.10 Πόρισμα. *Κάθε Αβελιανή ομάδα G τάξης p^n έχει μια μοναδική ανάλυση ως γινόμενο κυκλικών υποομάδων της όπως αυτή περιγράφεται στην Πρόταση 4.8.10.*

Απόδειξη. Έστω $G = G_1 \cdots G_k = G'_1 \cdots G'_s$, όπου G_i για $i = 1, \ldots, k$ και G'_j για $j = 1, \ldots, s$ είναι κυκλικές υποομάδες, τέτοιες ώστε κάθε στοιχείο g της G γράφεται μοναδικά στις μορφές

$$g = g_1 \cdots g_k \ \text{ και } \ g = g'_1 \cdots g'_s,\ g_i \in G_i,\ g'_j \in G'_j.$$

Θα δείξουμε ότι $k = s$ και μετά από μια κατάλληλη αρίθμηση $G_i \cong G'_i$, $i = 1, \ldots, k$. Θεωρούμε τα καρτεσιανά γινόμενα $H = G_1 \times \cdots \times G_k$ και $E = G'_1 \times \cdots \times G'_s$. Τότε οι αντιστοιχίες

$$G \longrightarrow H,\ g_1 \cdots g_k \longrightarrow (g_1, \ldots, g_k),\ g_i \in G_i,\ i = 1, \ldots, k$$

και

$$G \longrightarrow E,\ g'_1 \cdots g'_k \longrightarrow (g'_1, \ldots, g'_k),\ g'_j \in G_j,\ j = 1, \ldots, s$$

είναι ισομορφισμοί ομάδων και άρα $H \cong E$. Αν είναι αναγκαίο, διατάσσουμε τις G_i και G'_j έτσι ώστε $|G_1| \geq \cdots \geq |G_k|$ και $|G'_1| \geq \cdots \geq |G'_s|$. Τότε, λόγω του προηγούμενου Λήμματος, θα πρέπει $k = s$ και $G_i \cong G'_i$, $i = 1, \ldots, k$. ⊤

Από το Πόρισμα αυτό και το Λήμμα 4.8.11 συμπεραίνουμε ότι κάθε Αβελιανή ομάδα G τάξης p^n είναι ισόμορφη με ένα και μόνο ένα καρτεσιανό γινόμενο της μορφής

$$C_{p^{\alpha_1}} \times C_{p^{\alpha_2}} \times \cdots \times C_{p^{\alpha_k}}$$

όπου $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_k \geq 1$ και $\alpha_1 + \alpha_2 + \cdots + \alpha_k = n$. Οι κυκλικές ομάδες $C_{p^{\alpha_i}}$ ονομάζονται συνήθως ***στοιχειώδεις κυκλικοί παράγοντες*** της G και οι τάξεις των p^{α_i} ονομάζονται ***στοιχειώδεις διαιρέτες*** της G.

Με αυτή την ορολογία μπορούμε να διατυπώσουμε το εξής βασικό θεώρημα.

4.8.11 Θεώρημα. *Δυό Αβελιανές ομάδες G και H της ίδιας τάξης p^n είναι ισόμορφες αν και μόνον αν έχουν τους ίδιους στοιχειώδεις διαιρέτες.*

Έστω τώρα G και G' δύο πεπερασμένες Αβελιανές ομάδες τάξης n και $n = p_1^{n_1} \cdots p_k^{n_k}$ η ανάλυση του n σε γινόμενο δυνάμεων διακεκριμένων πρώτων. Αν P_i και Q_i είναι οι μοναδικές υποομάδες των G και G' τάξης $p_i^{n_i}$ (Πόρισμα 4.8.5) έχουμε δει ότι $G \cong G'$ αν και μόνον αν $P_i \cong Q_i,\ i = 1, 2, \ldots, k$. Συνεπώς $G \cong G'$ αν και μόνον αν οι P_i και Q_i έχουν τους ίδιους στοιχειώδεις διαιρέτες για κάθε $i = 1, \ldots, k$. Επομένως κάθε κλάση ισοδυναμίας ισόμορφων Αβελιανών πεπερασμένων ομάδων τάξης n καθορίζεται πλήρως από ένα σύνολο δυνάμεων $p_i^{n_{ij}}$ των $p_i,\ \ i = 1, \ldots, k$, όπου $n_{i1} \geq n_{i2} \geq \cdots \geq n_{is_i} \geq 1$ και $\sum_{j=1}^{s_i} n_{ij} = n_i$. Αν s είναι ο μεγαλύτερος δείκτης μεταξύ των $s_1, \ldots, s_k$, τότε μαζί με τις

προηγούμενες δυνάμεις του p_i, αν είναι αναγκαίο, θεωρούμε και τις δυνάμεις $p_i^{n_{i,s_i+1}}, \ldots, p_i^{n_{i,s}}$, όπου $n_{i,s_i+1} = n_{i,s_i+2} = \cdots = n_{i,s} = 0$.

Έστω

$$m_j = p_1^{n_{1j}} \cdots p_k^{n_{kj}},\ j = 1, 2, \ldots, s \tag{1}$$

$$n = m_1 m_2 \cdots m_s \ \text{ και } \ m_j \mid m_{j-1},\ j = 2, 3, \ldots, s. \tag{2}$$

Αντίστροφα αν ο n αναλύεται όπως στην (2) τότε τα m_j έχουν τη μορφή (1). Τώρα από το Θεώρημα 4.6.7 ή από τα προηγούμενα αποτελέσματα, έχουμε ότι

$$C_{m_j} \cong C_{p_1^{n_{1j}}} \times \cdots \times C_{p_k^{n_{kj}}}.$$

Επομένως, λαμβάνοντας υπόψιν ότι όλα τα καρτεσιανά γινόμενα $G_{\sigma(1)} \times \cdots \times G_{\sigma(r)}$, είναι ισόμορφα, για κάθε $\sigma \in S_n$, όπου $G_i,\ i = 1, \ldots, r$, είναι οποιεσδήποτε ομάδες (γιατί;), κάθε κλάση ισοδυναμίας ισόμορφων πεπερασμένων Αβελιανών ομάδων τάξης n αντιπροσωπεύεται από ένα καρτεσιανό γινόμενο

$$C_{m_1} \times C_{m_2} \times \cdots \times C_{m_s} \tag{3}$$

όπου $n = m_1 m_2 \cdots m_s$ και $m_2 | m_1$, $m_3 | m_2$, $\ldots$, $m_s | m_{s-1}$. Οι φυσικοί αριθμοί $m_1, \ldots, m_s$ σ' αυτή την περίπτωση ονομάζονται ***αναλλοίωτοι παράγοντες*** και οι κυκλικές ομάδες C_{m_j}, $j = 1, \ldots, s$, ***αναλλοίωτοι κυκλικοί παράγοντες*** κάθε Αβελιανής ομάδας που είναι ισόμορφη με το καρτεσιανό γινόμενο (3). Συνεπώς μπορούμε να πούμε ότι οι κλάσεις ισομορφίας των Αβελιανών ομάδων τάξης $n = p_1^{n_1} \cdots p_k^{n_k}$ βρίσκονται σε $1-1$ αντιστοιχία με τους πίνακες της μορφής

$$P = \begin{pmatrix} p_1^{n_{11}} p_1^{n_{12}} \cdots p_1^{n_{1s}} \\ p_2^{n_{21}} p_2^{n_{21}} \cdots p_2^{n_{2s}} \\ \cdots \ \cdots \\ p_k^{n_{k1}} p_k^{n_{k2}} \cdots p_k^{n_{ks}} \end{pmatrix}$$

όπου τα n_{ij} ορίζονται όπως περιγράψαμε μόλις πριν. Αν G είναι μια Αβελιανή ομάδα τάξης n και P είναι ο πίνακας που αντιστοιχεί στην κλάση ισομορφίας στην οποία ανήκει η G τότε τα διάφορα του 1 στοιχεία της i γραμμής είναι οι στοιχειώδεις διαιρέτες της μοναδικής υποομάδας P_i της G που έχει τάξη $p_i^{n_i}$. Τα δε γινόμενα των στοιχείων κάθε στήλης είναι οι αναλλοίωτοι παράγοντες της G.

Συνοψίζοντας τώρα μπορούμε να διατυπώσουμε το Θεμελιώδες Θεώρημα των Πεπερασμένων Αβελιανών Ομάδων.

4.8.12 Θεώρημα. *Δύο Αβελιανές πεπερασμένες ομάδες είναι ισόμορφες αν και μόνον αν έχουν τους ίδιους αναλλοίωτους παράγοντες .*

4.8.13 Παραδείγματα.

1. Έστω $n = 5^3$. Τότε οι προηγούμενοι δυνατοί πίνακες είναι οι εξής.

$$(5^3),\ (5^2, 5)\ \text{ και }\ (5, 5, 5).$$

Οι αντίστοιχες κλάσεις ισομορφίας των Αβελιανών ομάδων τάξης 125 αντιπροσωπεύονται από τα καρτεσιανά γινόμενα

$$C_{5^3},\ C_{5^2} \times C_5\ \text{ και }\ C_5 \times C_5 \times C_5$$

2. Έστω $n = 2^3 \cdot 3^2 \cdot 7$. Οι εν λόγω πίνακες P είναι οι εξής 6.

$$\begin{pmatrix} 2^3 \\ 3^2 \\ 7 \end{pmatrix},\ \begin{pmatrix} 2^3 & 1 \\ 3 & 3 \\ 7 & 1 \end{pmatrix},\ \begin{pmatrix} 2^2 & 2 \\ 3^2 & 1 \\ 7 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 2^2 & 2 \\ 3 & 3 \\ 7 & 1 \end{pmatrix},\ \begin{pmatrix} 2 & 2 & 2 \\ 3^2 & 1 & 1 \\ 7 & 1 & 1 \end{pmatrix},\ \begin{pmatrix} 2 & 2 & 2 \\ 3 & 3 & 1 \\ 7 & 1 & 1 \end{pmatrix}$$

Οι αντίστοιχοι αντιπρόσωποι των κλάσεων ισομορφίας είναι τα καρτεσιανά γινόμενα

$$\begin{aligned}
&C_{2^3} \times C_{3^2} \times C_7 \cong C_{504},\\
&C_{2^3} \times C_3 \times C_7 \times C_3 \cong C_{168} \times C_3\\
&C_{2^2} \times C_{3^2} \times C_7 \times C_2 \cong C_{252} \times C_2,\\
&C_{2^2} \times C_3 \times C_7 \times C_2 \times C_3 \cong C_{84} \times C_6\\
&C_2 \times C_{3^2} \times C_7 \times C_2 \times C_2 \cong C_{126} \times C_2 \times C_2,\\
&C_2 \times C_3 \times C_7 \times C_2 \times C_3 \times C_2 \cong C_{56} \times C_6 \times C_2
\end{aligned}$$

Συνεπώς δύο Αβελιανές ομάδες τάξης 504 είναι ισόμορφες αν και μόνον αν οι αναλλοίωτοι παράγοντές τους είναι το 504 ή το 168 και το 3 ή το 252 και το 2 ή το 84 και το 6 ή το 126, το 2 και το 2 ή το 56, το 6 και το 2. Οι αντίστοιχες αναλύσεις του 504 σε γινόμενο $m_1\, m_2 \cdots m_s$, όπου $m_j \mid m_{j-1}$, $j = 2, \ldots, s$, είναι 504, $168 \cdot 3$, $254 \cdot 2$, $84 \cdot 6$, $126 \cdot 2 \cdot 2$ και $56 \cdot 6 \cdot 2$. Αυτές είναι οι μόνες δυνατές.

4.8.14 Παρατηρήσεις.

1. Από τον ορισμό των αναλλοιώτων παραγόντων και των στοιχειωδών διαιρετών μιας πεπερασμένης Αβελιανής ομάδας G, είναι φανερό ότι η G έχει τάξη p^n, p πρώτος, αν και μόνον αν οι αναλλοίωτοι παράγοντες και οι

στοιχειώδεις διαιρέτες συμπίπτουν. Σ' αυτή την περίπτωση όταν οι στοιχειώδεις διαιρέτες είναι όλοι ίσοι με p, η ομάδα λέγεται ***στοιχειώδης Αβελιανή ομάδα***. Μια τέτοια ομάδα G χαρακτηρίζεται από την ιδιότητα $G^p = \{ e \}$. Αν $\mathbb{F}$ είναι ένα πεπερασμένο σώμα, τότε η προσθετική ομάδα $\mathbb{F}^+$ του $\mathbb{F}$ είναι μια στοιχειώδης Αβελιανή ομάδα αφού $p\mathbb{F}^+ = 0$ και άρα $\mathbb{F}^+ \cong C_p \times C_p \times \cdots \times C_p$ (n φορές), όπου $|\mathbb{F}^+| = p^n$.

2. Αν $m_1, m_2, \ldots, m_s$ είναι οι αναλλοίωτοι παράγοντες μιας Αβελιανής ομάδας G τάξης n, με $m_s \mid m_{s-1}, \ldots, m_2 \mid m_1$, τότε όλα τα στοιχεία της G ικανοποιούν την εξίσωση $x^{m_1} = 1$ (γιατί;). Για το λόγο αυτό ο ακέραιος m_1 ονομάζεται ***εκθέτης*** της G. Επομένως η G είναι κυκλική αν και μόνον αν ο εκθέτης της είναι η τάξη της $|G|$ (γιατί;). Αν $\mathbb{F}^*$ είναι η πολλαπλασιαστική ομάδα ενός πεπερασμένου σώματος, από το θεμελιώδες θεώρημα των Αβελιανών ομάδων έχουμε $\mathbb{F}^* \cong C_{m_1} \times C_{m_2} \times \cdots \times C_{m_s}$ όπου $m_1, \ldots, m_s$ είναι οι αναλλοίωτοι παράγοντες της $\mathbb{F}^*$ με $m_k \mid m_{k-1}$, $k = 2, \ldots, s$ και ισχύει $\alpha^{m_1} = 1$ για κάθε $\alpha \in \mathbb{F}^*$. Καθώς κάθε πολυώνυμο του $\mathbb{F}[x]$ έχει το πολύ n ρίζες όπου n είναι ο βαθμός του πολυωνύμου, το πολυώνυμο $x^{m_1} - 1$ έχει το πολύ m_1 ρίζες στο $\mathbb{F}$. Επειδή κάθε στοιχείο του $\mathbb{F}$ εκτός του μηδενικού είναι ρίζα αυτού του πολυωνύμου πρέπει $m_1 = |\mathbb{F}^*|$ και άρα η $\mathbb{F}^*$ είναι κυκλική. Αυτό μας δίνει μια άλλη απόδειξη της κυκλικότητας της $\mathbb{F}^*$ (βλέπε Εφαρμογή 4.6.8 (2)).

Ασκήσεις 4.9

1. Έστω G μια Αβελιανή ομάδα τάξης p^n με αναλλοίωτους παράγοντες $p, p, \ldots, p$ (n φορές) και $\{g_1, \ldots, g_n\}$ ένα υποσύνολο της G τέτοιο ώστε $G = < g_1 >< g_2 > \cdots < g_n >$ με

$$< g_i > \cap < g_1 > \cdots < g_{i-1} >< g_{i+1} > \cdots < g_n > = \{1\}$$

για $i = 1, \ldots, n$. Ένα τέτοιο υποσύνολο λέγεται βάση της G.

α) Δείξτε ότι το πλήθος όλων των βάσεων της G είναι ίσο με

$$(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) .$$

β) Δείξτε επίσης ότι το πλήθος όλων των υποομάδων της G που έχουν τάξη p^m, $1 \leq m \leq n$ είναι

$$\frac{(p^n - 1)(p^{n-1} - 1) \cdots (p^{n-m+1} - 1)}{(p^m - 1)(p^{m-1} - 1) \cdots (p - 1)} .$$

Συνεπώς το πλήθος των υποομάδων της G που έχουν τάξη p ισούται με το πλήθος των υποομάδων της G που έχουν δείκτη p στην G. Τί μπορείτε να συμπεράνετε για έναν διανυσματικό χώρο διάστασης n πάνω από ένα σώμα με p στοιχεία;

2. Περιγράψτε όλες τις Αβελιανές ομάδες τάξης 3240 και 2004.

3. Αν G είναι μια Αβελιανή ομάδα τάξης $\mid G \mid = p^n$ με αναλλοίωτους παράγοντες $m_1 \geq m_2 \geq \cdots \geq m_k > 0$ και H είναι υποομάδα της με αναλλοίωτους παράγοντες $\ell_1 \geq \ell_2 \geq \cdots \geq \ell_s > 0$ δείξτε ότι $k \geq s$ και $\ell_i \leq m_i$, $i = 1, 2, \ldots, s$.

4. Έστω G μια Αβελιανή ομάδα τάξης p^5 όπου p πρώτος. Αν οι αναλλοίωτοι παράγοντες είναι ο p^3 και ο p^2 πόσες υποομάδες τάξης p^2 έχει η G;

5. Αν G είναι μια πεπερασμένη Αβελιανή ομάδα και A, B είναι υποομάδες της τάξης n και m τότε η G έχει μια υποομάδα Γ τάξης ίσης με το ε.κ.π.(m, n).

4.9 Απλές Ομάδες

Όπως έχουμε ήδη αναφέρει, η έννοια της ομάδας πρωτοεμφανίστηκε στις εργασίες του Evariste Galois (1811-1832). Το θεμελειώδες έργο του Galois ουσιαστικά περιλαμβάνεται στο γράμμα που έστειλε αυτός σε ένα φίλο του, τον Auguste Chevalier, το τελευταίο βράδυ της ζωής του (29 Μαΐου 1832). Γι' αυτό το γράμμα, ο μεγάλος μαθηματικός Hermann Weyl αναφέρει στο βιβλίο του *"Symmetry"* [30] το εξής.

> "This letter, if judged by the novelty and profundity of ideas it contains, is perhaps the most substantial piece of writing in the whole literature of mankind"

Η βασική ιδέα του Galois ήταν η θεώρηση μιας ειδικής ομάδας μεταθέσεων του συνόλου των ριζών ενός ανάγωγου πολυωνύμου $f(x)$ με ρητούς συντελεστές. Η ομάδα αυτή λέγεται σήμερα ομάδα του Galois του πολυωνύμου $f(x)$. Η άκρη του νήματος που οδήγησε τον Galois στον ακατανόητο και μυστήριο, για την εποχή εκείνη, ορισμό της ομάδας βρίσκεται στη σημαντική ανακάλυψή του ότι η ομάδα A_n των άρτιων μεταθέσεων βαθμού n, για $n \neq 4$, δεν έχει κανονικές υποομάδες εκτός από την τετριμμένη και τον εαυτό της. Ως εφαρμογή αυτού του αποτελέσματος απέδειξε ότι είναι αδύνατον να λυθεί με ριζικά η γενική εξίσωση της μορφής

$$\alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_0 = 0$$

όταν $n \geq 5$. Αυτό ήταν ένα από τα κεντρικότερα μαθηματικά προβλήματα την εποχή εκείνη και είχε σχεδόν ταυτόχρονα λυθεί από τον Niels Kewrik Abel (1802-1829) με υπολογιστικές μεθόδους σε αντίθεση με τις ομαδοθεωρητικές μεθόδους του Galois, οι οποίες απετέλεσαν το ξεκίνημα της σύγχρονης άλγεβρας, δηλαδή της μελέτης των αλγεβρικών δομών. Αξίζει να τονιστεί ότι ο Abel και ο Galois χρησιμοποίησαν κατά ουσιαστικό τρόπο τις μεθόδους που ήδη είχε αναπτύξει για τον ίδιο σκοπό ο Joseph-Louis Lagrange (1736-1813).

Το 1869 ο Jordan υιοθέτησε τον όρο ***απλή*** ομάδα για μια ομάδα μεταθέσεων που δεν έχει μη-τετριμμένες γνήσιες κανονικές υποομάδες και αυτός ο όρος χρησιμοποιείται και σήμερα για μια οποιαδήποτε ομάδα που έχει αυτή την ιδιότητα. Έχουμε ήδη συναντήσει τέτοιες ομάδες. Οι ομάδες που η τάξη τους είναι ένας πρώτος αριθμός δεν έχουν καμιά μη-τετριμμένη γνήσια υποομάδα και κάθε Αβελιανή ομάδα που είναι απλή είναι μια κυκλική ομάδα που έχει τάξη έναν πρώτο αριθμό (γιατί;).

Έχουμε ορίσει τις κανονικές υποομάδες μιας ομάδας G να είναι οι πυρήνες των ομομορφισμών της G. Συνεπώς η G είναι μια απλή ομάδα αν και μόνον αν κάθε μη-τετριμμένος ομομορφισμός της είναι ένας μονομορφισμός.

Από αυτό το γεγονός θα μπορούσαμε να φανταστούμε την εμφάνιση των απλών ομάδων μεταξύ των άλλων ομάδων όπως οι πρώτοι αριθμοί εμφανίζονται μεταξύ των φυσικών αριθμών. Αυτό εξηγείται ως εξής. Θεωρούμε όλες τις ομάδες G για τις οποίες κάθε ακολουθία υποομάδων της

$$G \gneqq G_1 \gneqq G_2 \gneqq \cdots \gneqq G_k \gneqq \cdots$$

είναι πεπερασμένη, δηλαδή για κάθε τέτοια ακολουθία υπάρχει κάποιο k έτσι ώστε $G_k = \{1\}$. Σ' αυτή την περίπτωση λέμε ότι η G είναι μια ομάδα πεπερασμένου μήκους. Για παράδειγμα, κάθε πεπερασμένη ομάδα είναι πεπερασμένου μήκους ενώ η προσθετική ομάδα $\mathbb{Z}$ των ακέραιων δεν είναι (γιατί;).

Αν η G δεν είναι απλή και K είναι μια μη-τετριμμένη γνήσια κανονική υποομάδα της G, τότε θεωρούμε την ομάδα πηλίκο G/K από την οποία παίρνουμε τον επιμορφισμό

$$G \to G/K,\ g \longrightarrow gK\,,$$

που έχει πυρήνα την K. Αν η G/K δεν είναι απλή, από το θεώρημα της αντιστοιχίας υπάρχει γνήσια κανονική υποομάδα N της G που περιέχει γνήσια την K. Συνεχίζοντας αυτή τη διαδικασία, αν η G είναι πεπερασμένου μήκους, θα πρέπει να πάρουμε μια ομάδα πηλίκο G/L_1 η οποία να είναι απλή ομάδα. Αυτό σημαίνει ότι η L_1 είναι μια γνήσια κανονική υποομάδα της G η οποία δεν περιέχεται γνήσια σε καμιά άλλη γνήσια κανονική υποομάδα της G. Επαναλαμβάνοντας την ίδια διαδικασία για την ομάδα L_1, μπορούμε να βρούμε μια γνήσια κανονική υποομάδα L_2 της L_1 τέτοια ώστε η L_1/L_2 να είναι απλή. Συνεχίζοντας μ' αυτό τον τρόπο παίρνουμε μια πεπερασμένη ακολουθία

$$L_0 = G \rhd L_1 \rhd L_2 \rhd \cdots \rhd L_n \rhd L_{n+1} = \{1\} \qquad (*)$$

υποομάδων L_i της G τέτοιων ώστε οι ομάδες πηλίκα $L_i/L_{i+1},\ i = 0, \ldots, n$, να είναι απλές ομάδες.

Στην προηγούμενη διαδικασία θα μπορούσαν αντί για τις υποομάδες L_i να είχαν επιλεγεί άλλες υποομάδες L'_j για τις οποίες να είχαμε την ακολουθία

$$(**) \qquad L'_0 = G \rhd L'_1 \rhd L'_2 \rhd \cdots \rhd L'_m \rhd L'_{m+1} = \{1\}$$

στην οποία τα πηλίκα $L'_j/L'_{j+1},\ j = 0, \ldots, m$, να είναι απλές ομάδες. Ισχύει όμως το εξής σημαντικό αποτέλεσμα των Jordan και Hölder, του οποίου η απόδειξη δεν είναι μέσα στους σκοπούς αυτού του βιβλίου.

4.9.1 Θεώρημα. *Για οποιεσδήποτε δύο ακολουθίες υποομάδων της G της μορφής $(*)$ και $(**)$ ισχύει $m = n$ και $L_i/L_{i+1} \cong L_{\sigma(j)}/L_{\sigma(j)+1}$ για κάποια μετάθεση $\sigma \in S_n$.*

Επομένως για μια ομάδα G πεπερασμένου μήκους οι απλές ομάδες πηλίκα L_i/L_{i+1} μαζί με τις πολλαπλότητες με τις οποίες εμφανίζονται σε μια ακολουθία $(*)$ υποομάδων της G αποτελούν αναλλοίωτα στοιχεία της G. Αν η G είναι πεπερασμένη και $M_1, M_2, \ldots, M_s$ είναι οι ανά δύο μη-ισόμορφες απλές ομάδες L_i/L_{i+1} που εμφανίζονται στην εν λόγω ακολουθία $(*)$ τότε εύκολα προκύπτει από το θεώρημα του Lagrange ότι η τάξη της G είναι ίση με

$$|G| = |M_1|^{m_1} \cdot |M_2|^{m_2} \cdot \ldots \cdot |M_s|^{m_s}$$

όπου $m_i,\ i = 1, \ldots, s$, είναι η πολλαπλότητα, με την οποία εμφανίζεται η M_i στην ακολουθία $(*)$. Αυτό το δείχνουμε σχηματικά ως εξής

G	G/L_1
L_1	L_1/L_2
L_2	L_2/L_3
L_3	
	$\cdots$
	$\cdots$
	$\cdots$
L_n	
$\{1\}$	L_n

Για παράδειγμα, αν θεωρήσουμε την κυκλική ομάδα $G = < x >$ τάξης n, όπου $n = p_1 p_2 \cdots p_t$, p_i πρώτοι αριθμοί, τότε η ακολουθία

$$G = < x > \rhd < x^{p_1} > \rhd < x^{p_1 p_2} > \rhd \cdots \rhd < x^{p_1 \cdots p_{t-1}} > \rhd \{1\}$$

είναι μια ακολουθία της μορφής $(*)$. Οι αντίστοιχες απλές ομάδες L_i/L_{i+1} εδώ είναι οι $G/ < x^{p_1} > \cong C_{p_1}$, $< x^{p_1} > / < x^{p_1 p_2} > \cong C_{p_2}$, $\ldots$, $< x^{p_1 \cdots p_{t-1}} > \cong C_{p_t}$.

Μια άλλη ακολουθία της ίδιας μορφής είναι η

$$G = < x > \rhd < x^{p_2} > \rhd < x^{p_1 p_2} > \rhd \cdots \rhd < x^{p_1 \cdots p_{t-1}} > \rhd \{1\}.$$

Συγκρίνοντάς την με την προηγούμενη, βλέπουμε ότι

$$G/ < x^{p_2} > \cong < x^{p_1} > / < x^{p_1 p_2} > \cong C_{p_2},$$

$$< x^{p_2} > / < x^{p_1 p_2} > \cong G/ < x^{p_1} > \cong C_{p_1}$$

και όλα τα άλλα πηλίκα συμπίπτουν. Αυτό ακριβώς αναφέρει το Θεώρημα 4.9.1 των Jordan και Hölder, δηλαδή ότι οι ομάδες πηλίκα που προκύπτουν από μια ακολουθία υποομάδων της G της μορφής $(*)$ είναι ανεξάρτητες από την ακολουθία και εξαρτώνται μόνο από την ίδια την G. Αυτό μας δίνει και μια άλλη απόδειξη της μοναδικότητας της ανάλυσης του n σε γινόμενο πρώτων αριθμών. Επίσης το ότι κάθε φυσικός αριθμός αναλύεται σε γινόμενο πρώτων αριθμών προκύπτει από το γεγονός ότι για την κυκλική ομάδα C_n τάξης n μπορούμε να θεωρήσουμε μια ακολουθία υποομάδων

$$L_0 = C_n > L_1 > L_2 > \cdots > L_k = \{1\}$$

έτσι ώστε μεταξύ της L_i και της L_{i+1}, $i = 0, , 1, \ldots , k-1$, δεν υπάρχει καμιά υποομάδα της G. Με άλλα λόγια, η ομάδα πηλίκο L_i/L_{i+1} είναι απλή Αβελιανή και άρα τάξης p, όπου p πρώτος. Συνεπώς ο n θα πρέπει να είναι γινόμενο δυνάμεων πρώτων αριθμών.

Από αυτά που αναφέρθηκαν, είναι φανερό ότι οι απλές ομάδες παίζουν σημαντικότατο ρόλο σε όλη τη θεωρία ομάδων. Από την εποχή του Jordan και κυρίως τον 20ο αιώνα πολλοί κορυφαίοι μαθηματικοί ασχολήθηκαν με το πρόβλημα της ταξινόμησης των πεπερασμένων απλών ομάδων. Το 1963 οι μαθηματικοί Feit και Thompson απέδειξαν ότι αν μια μη-Αβελιανή ομάδα έχει περιττή τάξη αυτή δεν είναι απλή.[5] Αυτό το αποτέλεσμα το είχε εικάσει το 1900 ένας από τους θεμελιωτές της Θεωρίας Ομάδων ο W. Burnside. Το αποτέλεσμα αυτό και κυρίως η τεχνική που χρησιμοποιείται για την απόδειξή του οδήγησαν τελικά στη λύση του προβλήματος της ταξινόμησης των απλών ομάδων.

4.9.2 Πρόταση. *Αν K είναι μια κανονική υποομάδα της A_n που περιέχει έναν 3-κυκλο, τότε $K = A_n$.*

Απόδειξη. Καθώς $A_1 = A_2 = \{1\}$ και $A_3 = \{1, (1\,2\,3), (1\,3\,2)\}$, μπορούμε να υποθέσουμε ότι $n \geq 4$. Έστω $(\alpha\,\beta\,\gamma) \in K$. Τότε, αν $\delta \neq \alpha, \beta, \gamma$, έχουμε $(\,(\alpha\,\beta)(\gamma\,\delta)\,)(\alpha\,\gamma\,\beta)(\,(\alpha\,\beta)(\gamma\,\delta)\,)^{-1} = (\alpha\,\beta)(\gamma\,\delta)(\alpha\,\gamma\,\beta)(\gamma\,\delta)(\alpha\,\beta) = (\alpha\,\beta\,\delta)$. Αλλά $(\alpha\,\gamma\,\beta) = (\alpha\,\beta\,\gamma)^2 \in K$ και $(\alpha\,\beta)(\gamma\,\delta)K(\,(\alpha\,\beta)(\gamma\,\delta)\,)^{-1} = K$, αφού $(\alpha\,\beta)(\gamma\,\delta) \in A_n$. Συνεπώς $(\alpha\,\beta\,\delta) \in K$, για κάθε $\delta \neq \alpha, \beta$. Αλλά, αντικαθιστώντας στο Θεώρημα 4.4.15 τα 1 και 2 με α και β αντίστοιχα βλέπουμε ότι όλοι οι 3-κυκλοι $(\alpha\,\beta\,\delta)$ παράγουν την A_n και άρα $K = A_n$. ⊤

4.9.3 Παρατήρηση. Χρησιμοποιώντας την παραπάνω Πρόταση, προκύπτει άμεσα το αποτέλεσμα του Παραδείγματος που ακολουθεί την Παρατήρησης 4.4.27.

[5] Για την εργασία αυτή οι Feit και Thompson βραβεύθηκαν το 1965, με το "Cole Prize" στα μαθηματικά, ενώ το 1970 απονεμήθηκε στον Thompson το Fields Medal, το μεγαλύτερο βραβείο που απονέμεται κάθε τέσσερα χρόνια στα μαθηματικά.

Πράγματι, η A_4 δεν μπορεί να έχει καμιά γνήσια υποομάδα τάξης 6, αφού αφενός μια τέτοια υποομάδα θα ήταν κανονική και αφετέρου θα περιείχε έναν 3-κυκλο καθώς η A_4 έχει 8 3-κύκλους.

4.9.4 Θεώρημα (Galois). *Για κάθε $n \neq 4$, η A_n είναι απλή ομάδα. Επιπλέον για $n = 3$ και $n \geq 5$ η A_n είναι η μόνη μη-τετριμμένη κανονική υποομάδα της S_n. Για την περίπτωση $n = 4$, η S_4 περιέχει μόνο δύο κανονικές μη-τετριμμένες υποομάδες: την A_4 και την υποομάδα $K_4 = \{\, 1,\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\,\}$ του Klein.*

Απόδειξη. Είναι φανερό ότι η K_4 είναι μια κανονική υποομάδα της S_4. Επίσης είναι φανερό ότι η A_3 είναι απλή ομάδα και ότι είναι η μόνη μη-τετριμμένη κανονική υποομάδα της S_3.

Έστω $n \geq 5$. Υποθέτουμε ότι K είναι μια μη-τετριμμένη κανονική υποομάδα της A_n. Θα δείξουμε ότι η K περιέχει έναν 3-κυκλο, οπότε από την προηγούμενη πρόταση θα πρέπει $K = A_n$. Χρησιμοποιώντας το Αξίωμα του Ελαχίστου, μπορούμε να θεωρήσουμε μεταξύ των μη-ταυτοτικών μεταθέσεων που ανήκουν στην K μια μετάθεση σ τέτοια ώστε το πλήθος των συμβόλων που δεν μένουν σταθερά κάτω από την σ να είναι το ελάχιστο δυνατό. Έστω m αυτό το πλήθος. Αφού η σ είναι άρτια θα πρέπει $m \geq 3$. Υποθέτουμε ότι $m > 3$ και διακρίνουμε δύο περιπτώσεις.

Περίπτωση 1η. Η σ γράφεται ως γινόμενο ξένων ανά δύο αντιμεταθέσεων

$$\sigma \,=\, (\alpha_1\,\alpha_2)(\alpha_3\,\alpha_4)\cdots .$$

Έστω α_5 ένα σύμβολο διάφορο των α_i, $i = 1, 2, 3, 4$. Καθώς έχουμε $K \trianglelefteq A_n$, θα πρέπει η μετάθεση

$$\sigma' \,=\, (\alpha_3\,\alpha_4\,\alpha_5)\,\sigma\,(\alpha_3\,\alpha_5\,\alpha_4) \,=\, (\alpha_1\,\alpha_2)(\alpha_4\,\alpha_5)\cdots$$

να είναι στοιχείο της K. Τότε όμως θα έχουμε $\sigma'' = \sigma^{-1}\sigma' \in K$ και $\sigma'' \neq i$, αφού $\sigma \neq \sigma'$. Αλλά το μόνο σύμβολο που δεν μένει σταθερό από τη σ'' και μένει σταθερό από τη σ είναι ίσως το α_5. Καθώς όμως η σ'' αφήνει σταθερά τα σύμβολα α_1 και α_2, έπεται ότι αυτή αφήνει σταθερά περισσότερα σύμβολα από όσα αφήνει η σ. Αυτό είναι άτοπο.

Περίπτωση 2η. Η έκφραση της σ ως γινόμενο ξένων ανά δύο κύκλων περιέχει τουλάχιστον έναν κύκλο που δεν είναι αντιμετάθεση, έστω

$$\sigma = (\alpha_1\,\alpha_2\,\alpha_3\,\cdots)\cdots .$$

Καθώς η σ είναι άρτια και δεν αφήνει σταθερά $m > 3$ σύμβολα, υπάρχουν τουλάχιστον δύο άλλα σύμβολα, έστω τα α_4 και α_5, τα οποία η σ δεν αφήνει σταθερά. Τότε, έχουμε $\sigma'' = \sigma^{-1}\sigma' \in K$, όπου

$$\sigma' \,=\, (\alpha_3\,\alpha_4\,\alpha_5)\,\sigma\,(\alpha_3\,\alpha_5\,\alpha_4) \,=\, (\alpha_1\,\alpha_2\,\alpha_4\,\cdots)\,\cdots\,.$$

Είναι φανερό ότι όλα τα σύμβολα που μένουν σταθερά κάτω από τη σ, μένουν σταθερά και από τη σ'', ενώ η σ'' αφήνει σταθερό το σύμβολο α_1 που δεν το αφήνει σταθερό η σ. Αυτό είναι και πάλι άτοπο.

Θεωρούμε τώρα μια μη-τετριμμένη κανονική υποομάδα K της S_n. Η τομή $K \cap A_n$ είναι κανονική υποομάδα της A_n και άρα, σύμφωνα με τα προηγούμενα, πρέπει $K \cap A_n = A_n$ ή $\{1\}$. Αν $K \cap A_n = A_n$, δηλαδή $A_n \subseteq K$, τότε, επειδή $|\,S_n : A_n\,| = 2$, θα πρέπει να είναι $K = A_n$ ή $K = S_n$. Αν $K \cap A_n = \{1\}$, τότε, επειδή $|\,K\,A_n\,| = |\,K\,|\,|\,A_n\,| = \dfrac{n!}{2}\,|\,K\,| \leq n!$ και $|\,K\,| \neq 1$, θα πρέπει $|\,K\,| = 2$. Έστω $K = \{\,i,\,\tau\,\}$. Καθώς η K είναι κανονική υποομάδα της S_n, θα πρέπει να ισχύει $\rho\tau\rho^{-1} = \tau$ για κάθε $\rho \in S_n$. Τότε όμως είναι $\tau \in Z(S_n) = \{i\}$. ⊺

4.9.5 Παρατήρηση. Από το γεγονός ότι η A_n είναι απλή, μπορούμε να κατασκευάσουμε μια άπειρη απλή ομάδα ως εξής. Θεωρούμε τη συμμετρική ομάδα $S_{\mathbb{N}}$ όλων των μεταθέσεων επί των φυσικών αριθμών. Έστω G η υποομάδα της $S_{\mathbb{N}}$ όλων των μεταθέσεων που αφήνουν μόνο πεπερασμένο πλήθος σύμβολα μη-σταθερά. Για κάθε $n \in \mathbb{N}$, η υποομάδα

$$G_n = \{\sigma \in G \mid \sigma(m) = m \text{ για κάθε } \; m \in \mathbb{N},\; m > n\,\}$$

είναι ισόμορφη με την S_n και $G_n < G_{n+1}$. Έχουμε δε $G = \bigcup\limits_{n=1}^{\infty} G_n$. Τώρα έστω H_n, για $n > 1$, η μοναδική υποομάδα της G_n που έχει δείκτη 2 στην G_n, δηλαδή η υποομάδα H_n της G_n είναι ισόμορφη με την A_n. Τότε η άπειρη ένωση $H = \bigcup\limits_{i=1}^{\infty} H_i$ είναι μια υποομάδα της G, αφού $H \neq \emptyset$ και για $h_1,\, h_2 \in H$ υπάρχουν δείκτες $i_1,\, i_2$ τέτοιοι ώστε $h_1 \in H_{i_1},\;\; h_2 \in H_{i_2}$, οπότε για $j = \max\{\,i_1,\, i_2\,\}$, $H_{i_1} \leq H_j$ και $H_{i_2} \leq H_j$ και άρα $h_1 h_2^{-1} \in H_j$. Ισχύει δε $|\,G : H\,| = 2$ (γιατί;). Αν $K \trianglelefteq H$, τότε για κάθε j ισχύει $K \cap H_j \trianglelefteq H_j$ και άρα από το προηγούμενο θεώρημα για $j \geq 5$ $\;K \cap H_j = H_j$ ή $\{\,i\,\}$. Αν $K \cap H_j = \{\,i\,\}$ για κάθε j, τότε $K = \{\,i\,\}$. Αν $K \cap H_j = H_j \neq \{\,i\,\}$ για κάποιο j, τότε $K \cap H_j = H_j$ για κάθε j και άρα $K \,=\, H$.

Κλείνουμε αυτή την παράγραφο με μια γενίκευση του θεωρήματος του Cayley μέσω της οποίας μπορούμε να εξετάζουμε αν μια ομάδα είναι απλή ή όχι.

Έστω H μια υποομάδα μιας ομάδας G και G/H το αριστερό σύνολο πηλίκο. Τότε κάθε στοιχείο $g \in G$ ορίζει την μετάθεση τ_g επί του G/H με $xH \longrightarrow gxH$. Έτσι έχουμε την αντιστοιχία

$$\rho_H : G \longrightarrow S_{|G/H|},\ g \longrightarrow \tau_g$$

η οποία είναι προφανώς μια απεικόνιση. Επιπλέον ισχύει $\tau_{g_1 g_2} = \tau_{g_1}\tau_{g_2}$, καθώς

$$\tau_{g_1 g_2}(xH) = g_1 g_2 xH = \tau_{g_1}(\tau_{g_2}(xH)) = \tau_{g_1}\tau_{g_2}(xH).$$

Δηλαδή η ρ_H είναι ένας ομομορφισμός. Για τον πυρήνα $K = \ker \rho_H$, έχουμε

$$\begin{aligned} K &= \{ g \in G \mid \tau_g = i \} = \{ g \in G \mid \tau_g(xH) = xH \text{ για όλα τα } x \in G \} \\ &= \{ g \in G \mid gxH = xH \text{ για όλα τα } x \in G \} \\ &= \{ g \in G \mid x^{-1}gxH = H \text{ για όλα τα } x \in G \} \\ &= \{ g \in G \mid x^{-1}gx \in H \text{ για όλα τα } x \in G \} \\ &= \{ g \in G \mid g \in xHx^{-1} \text{ για όλα τα } x \in G \} = \bigcap_{x \in G} xHx^{-1} . \end{aligned}$$

Συνεπώς ο πυρήνας K περιέχεται στην H.[6] Επιπλέον αυτός ο πυρήνας περιέχει κάθε κανονική υποομάδα της G που περιέχεται στην H. Πράγματι, έστω $N \lhd G$ με $N \leq H$. Αυτό σημαίνει ότι για κάθε $g \in G$ και $y \in N$ ισχύει $g^{-1}yg \in H$. Τότε, $y \in \bigcap_{g \in G} gHg^{-1} = K$ για κάθε $y \in N$ και άρα $N \leq K$.

4.9.6 Θεώρημα. *Έστω G μια ομάδα και H μια υποομάδα της G που έχει πεπερασμένο δείκτη $|G : H| = \delta_H$. Τότε, υπάρχει μια κανονική υποομάδα K της G που περιέχεται στην H τέτοια ώστε ο δ_H διαιρεί τον δείκτη $|G : K| = \delta_K$ και ο δ_K διαιρεί το $\delta_H!$.*

Αν η G είναι πεπερασμένη και η τάξη της $|G|$ δεν διαιρεί το $\delta_H!$ για μια γνήσια υποομάδα H της G, τότε η G έχει μια μη-τετριμμένη κανονική υποομάδα που περιέχεται στην H και άρα η G δεν είναι απλή.

Απόδειξη. Θεωρούμε τον προηγούμενο ομομορφισμό ρ_H, για τον πυρήνα K του οποίου έχουμε

$$|G/K| = |G/K : H/K|\,|H/K|$$

όπου $|G/K : H/K| = |G : H| = \delta_H$, από το Θεώρημα της Αντιστοιχίας 4.7.10. Επίσης, από το Θεώρημα 4.7.12, η εικόνα $\rho_H(G)$ είναι ισόμορφη με την G/K

[6] Σημειώνουμε εδώ ότι για $H = \{1\}$ παίρνουμε το θεώρημα του Cayley (Θεώρημα 4.5.11).

και άρα η τάξη $|G/K| = |G : K| = \delta_K$ διαιρεί την τάξη $\delta_H! = |S_{|G/H|}|$, αφού η $\rho_H(G)$ είναι υποομάδα της $S_{|G/H|}$. Τώρα, υποθέτουμε ότι η G είναι πεπερασμένη και ότι $H \lneq G$. Η υπόθεση ότι η τάξη $|G|$ της G δεν διαιρεί το $\delta_H!$, σημαίνει ότι ο ομομορφισμός ρ_H δεν μπορεί να είναι ένας μονομορφισμός διότι διαφορετικά η εικόνα $\rho_H(G)$ θα ήταν ισόμορφη με την G και θα έπρεπε η τάξη $|G|$ να διαιρούσε την τάξη $\delta_H!$ της $S_{|G/H|}$. Άρα η G έχει μια τετριμμένη κανονική υποομάδα, τον πυρήνα K της ρ_H, που περιέχεται στην H. Συνεπώς η G δεν είναι απλή. ⊤

4.9.7 Πόρισμα. *Έστω G μια πεπερασμένη ομάδα και p ο μικρότερος πρώτος που διαιρεί την τάξη της G. Αν η G έχει μια υποομάδα H που έχει δείκτη p τότε η H είναι μια κανονική υποομάδα της G.*

Απόδειξη. Από το προηγούμενο θεώρημα υπάρχει μια κανονική υποομάδα K της G που ο δείκτης της δ_K διαιρεί το $p! = |G : H|!$. Αλλά ο δείκτης δ_K διαιρεί και την τάξη $|G|$ της G. Συνεπώς ο δ_K θα διαιρεί τον μ.κ.δ.$(p!, |G|)$. Αλλά επειδή ο p είναι ο μικρότερος πρώτος διαιρέτης της $|G|$, θα πρέπει μ.κ.δ.$(p!, |G|) = p$. Άρα $\delta_K = p = \delta_H$. Επειδή $K \leq H$ θα πρέπει τελικά να είναι $K = H$. ⊤

4.9.8 Παραδείγματα. Χρησιμοποιώντας το προηγούμενο Θεώρημα, μπορούμε να δείξουμε ότι κάθε ομάδα G τάξης p^2, όπου p είναι ένας πρώτος αριθμός, είναι Αβελιανή. Πράγματι, αρκεί να θεωρήσουμε την περίπτωση κατά την οποία όλα τα μη-ουδέτερα στοιχεία της έχουν τάξη p. Τότε, η G έχει $p+1$ μη-τετριμμένες υποομάδες η κάθε μια τάξης p (γιατί;). Έστω $h \neq 1$ ένα στοιχείο της G και $H = \langle h \rangle$. Επειδή το p^2 δεν διαιρεί το $p! = |G : H|!$, η H είναι κανονική υποομάδα της G. Έστω $g \in G$. Τότε $ghg^{-1} = h^k$, για κάποιο k με $1 \leq k < p$. Από αυτό προκύπτει ότι

$$g^2hg^{-2} = gh^kg^{-1} = \left(ghg^{-1}\right)^k = \left(h^k\right)^k = h^{k^2}$$

και επαγωγικά έχουμε ότι $h = g^phg^{-p} = h^{k^p}$. Τότε, θα είναι $h^{k^p-1} = 1$ και άρα $k^p \equiv 1 \mod p$. Συνεπώς, θα πρέπει $k = 1$ (γιατί;). Αυτό σημαίνει ότι το h μετατίθεται με το g και επειδή το g είναι ένα οποιοδήποτε στοιχείο της G το h μετατίθεται με όλα τα στοιχεία της G. Καθώς το πηλίκο G/H είναι κυκλική ομάδα, υπάρχει $g \in G$ ώστε $G/H = \langle gH \rangle$. Έτσι, αν $g_1, g_2 \in G$ με $g_1 = g^ih^j$ και $g_2 = g^th^k$, τότε θα έχουμε $g_1\,g_2 = g^ih^jg^th^k = g^th^kg^ih^j = g_2\,g_1$.

Ασκήσεις 4.9

1. Δείξτε ότι μια άπειρη απλή ομάδα G δεν μπορεί να έχει μια υποομάδα H πεπερασμένου δείκτη.
   Υπόδειξη: Αν είχε, θα υπήρχε ένας ομομορφισμός $\phi : G \to S_{|G:H|}$ με πυρήνα μια μη-τετριμμένη υποομάδα K, αφού $G/K \cong \phi(G) \leq S_{|G:H|}$.

2. Έστω G μια ομάδα τάξης 143. Υποθέτουμε ότι η G έχει ένα στοιχείο τάξης 11. Δείξτε ότι η G δεν είναι απλή.

3. Δείξτε ότι αν G είναι μια απλή πεπερασμένη ομάδα και H μια υποομάδα της που έχει δείκτη ένα πρώτο αριθμό p, τότε ο p είναι ο μεγαλύτερος πρώτος που διαιρεί την τάξη $|G|$ της G και ο p^2 δεν διαιρεί την $|\, G\,|$.

4. Θεωρούμε την ομάδα $G = GL_2(\mathbb{Z}_3)$, οπότε $|G| = 48$. Έστω K το κέντρο $Z(G)$, οπότε $|K| = 2$. Επίσης θεωρούμε την υποομάδα

$$H = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \,|\, \alpha,\, \beta,\, \gamma \in \mathbb{Z}_3,\, \alpha\gamma \neq 0 \right\}$$

   α) Δείξτε ότι $|H| = 12$ και ότι $K = \bigcap_{x \in G} xHx^{-1}$

   β) Δείξτε ότι $G/K \cong S_4$.

   Υπόδειξη: Χρησιμοποιήστε τον ομομορφισμό $\phi : G \to S_{|G:H|}$.

5 Δράσεις Ομάδων

Η σπουδαιότητα της θεωρίας ομάδων, και γενικότερα των μαθηματικών, υποδηλώνεται από τις δυνατότητες εφαρμογής της σε διάφορους επιστημονικούς κλάδους. Μετά τον Evariste Galois, ο οποίος όρισε, όπως είδαμε, την έννοια της ομάδας και ταυτόχρονα την χρησιμοποίησε για την διερεύνηση των λύσεων μιας αλγεβρικής εξίσωσης, ένας από αυτούς που συνέδεσε το όνομά του με τη Θεωρία Ομάδων είναι ο Felix Klein (1849-1925). Αυτός το 1872 στην εναρκτήριο ομιλία ως καθηγητής του Πανεπιστημίου Erlangen της Γερμανίας (γνωστής ως "Πρόγραμμα Erlangen") έκανε την ταξινόμηση των διάφορων τύπων "γεωμετρίας" μέσα σε ένα χώρο, χρησιμοποιώντας τις ομάδες μετασχηματισμών του χώρου οι οποίοι αφήνουν αναλλοίωτες ορισμένες γεωμετρικές ιδιότητές του. Οι περισσότερες εφαρμογές της θεωρίας ομάδων εκφράζονται μέσω αυτής ακριβώς της θεώρησης του Klein, την οποία σήμερα ονομάζουμε "δράση" ομάδας πάνω σε χώρους και γενικότερα πάνω σε σύνολα. Μέσω αυτής της θεώρησης μπορεί να μελετηθεί η δομή αυτής καθ' εαυτής της ομάδας. Επιπλέον μας παρέχονται αποτελεσματικά εργαλεία για τη λύση συνδυαστικών προβλημάτων. Σε αυτή την τελευταία Ενότητα του βιβλίου αναπτύσσουμε ορισμένα στοιχεία αυτής της θεωρίας. Μία από τις σημαντικές εφαρμογές της έννοιας της "δράσης" είναι η σύντομη και κομψή απόδειξη του Helmut Wielandt [31] των θεωρημάτων του Sylow, όπως αυτή δίνεται στην παράγραφο 5.3.

5.1 Ορισμοί και Παραδείγματα

Έστω G μια ομάδα και X ένα μη κενό σύνολο. Θα λέμε ότι η G ***δρα*** πάνω στο X αν έχουμε μια απεικόνιση

$$\delta : G \times X \longrightarrow X, \quad (g, x) \longrightarrow \delta(g, x)$$

που ικανοποιεί τις εξής ιδιότητες.

α) $\delta(1, x) = x$

β) $\delta(g_1, \delta(g_2, x)) = \delta(g_1 g_2, x)$, για κάθε $g_1, g_2 \in G$ και $x \in X$.

Μια τέτοια απεικόνιση δ ονομάζεται ***δράση*** της G πάνω στο X. Συνήθως την εικόνα $\delta(g, x)$ του στοιχείου (g, x) την συμβολίζουμε με $g \cdot x$. Έτσι οι ιδιότητες α) και β) γράφονται $1 \cdot x = x$ και $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ αντίστοιχα.

5.1.1 Παρατηρήσεις. Όταν μια ομάδα G δρα πάνω στο σύνολο X, τότε κάθε στοιχείο $g \in G$ ορίζει μια $1-1$ και επί απεικόνιση του X στον εαυτό του. Πράγματι, η απεικόνιση

$$\sigma_g : X \longrightarrow X, \quad \sigma_g(x) = g \cdot x, \ x \in X,$$

είναι $1-1$ και επί, αφού αν $g \cdot x = g \cdot x'$, τότε $g^{-1}(g \cdot x) = g^{-1} \cdot (g \cdot x')$ ή $(g^{-1}g) \cdot x = (g^{-1} \cdot g) \cdot x'$, δηλαδή $1 \cdot x = 1 \cdot x'$ και συνεπώς $x = x'$. Επιπλέον κάθε στοιχείο $x \in X$ είναι εικόνα του στοιχείου $g^{-1} \cdot x$. Δηλαδή η απεικόνιση σ_g είναι ένα στοιχείο της συμμετρικής ομάδας S_X του X. Τις απεικονίσεις $\sigma_g, g \in G$, συνήθως τις λέμε ***μετασχηματισμούς*** του X οριζόμενους από τα στοιχεία της G. Αν τώρα ορίσουμε την αντιστοιχία

$$\vartheta : G \longrightarrow S_X, \quad \vartheta(g) = \sigma_g,$$

τότε η ϑ είναι ένας ομομορφισμός ομάδων του οποίου ο πυρήνας ονομάζεται ***πυρήνας της δράσης*** της G πάνω στο X. Πράγματι έχουμε

$$\begin{aligned} \vartheta(g_1 g_2) =& \sigma_{g_1 g_2} = \sigma_{g_1} \circ \sigma_{g_2} = \vartheta(g_1) \circ \vartheta(g_2), \text{ καθώς} \\ \sigma_{g_1 g_2}(x) =& (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = g_1 \cdot \sigma_{g_2}(x) = \sigma_{g_1}(\sigma_{g_2}(x)) \\ =& (\sigma_{g_1} \circ \sigma_{g_2})(x), \text{ για κάθε } x \in X. \end{aligned}$$

Αντίστροφα, κάθε ομομορφισμός $\vartheta : G \to S_X$ ορίζει μια δράση της G πάνω στο X θέτοντας $\vartheta(g)(x) = g \cdot x$, για κάθε $x \in X$ και $g \in G$, αφού

$$\begin{aligned} (g_1 g_2) \cdot x &= \vartheta(g_1 g_2)(x) = (\vartheta(g_1) \circ \vartheta(g_2))(x) = \vartheta(g_1)(\vartheta(g_2)(x)) \\ &= \vartheta(g_1)(g_2 \cdot x) = g_1 \cdot (g_2 \cdot x) \end{aligned}$$

και $1 \cdot x = \vartheta(1)(x) = 1_X(x) = x$.

5.1.2 Παραδείγματα.

1. Για οποιαδήποτε ομάδα G και οποιοδήποτε σύνολο $X \neq \emptyset$ ορίζουμε τη δράση $g \cdot x = x$, για κάθε $g \in G$ και $x \in X$. Αυτή ονομάζεται ***τετριμμένη δράση***. Ο πυρήνας αυτής της δράσης είναι όλη η ομάδα G.

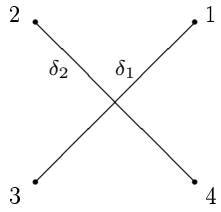
2. Αν $X = \{1, 2, \ldots, n\}$ και G είναι μια ομάδα μεταθέσεων βαθμού n, τότε η G δρα προφανώς πάνω στο X. Πράγματι, η ταυτοτική μετάθεση αφήνει σταθερό κάθε στοιχείο του X, ενώ η σύνθεση των μεταθέσεων ικανοποιεί την ιδιότητα β) του ορισμού της δράσης. Εδώ, ο πυρήνας της δράσης είναι η τετριμμένη υποομάδα της G.

3. Έστω V ένας μη μηδενικός διανυσματικός χώρος επί ενός σώματος $\mathbb{F}$. Τότε το βαθμωτό γινόμενο λv, $\lambda \in \mathbb{F}$, $v \in V$, είναι μια δράση της πολλαπλασιαστικής ομάδας $\mathbb{F}^*$ του $\mathbb{F}$ πάνω στο σύνολο V. Ο πυρήνας αυτής της δράσης είναι η τετριμμένη υποομάδα $\{1\}$ της $\mathbb{F}^*$ (γιατί;). Αν θεωρούσαμε την προσθετική ομάδα $\mathbb{F}^+$ του $\mathbb{F}$, τότε το βαθμωτό γινόμενο δεν είναι μια δράση της $\mathbb{F}^+$ πάνω στο V, αφού $0v = 0$, για κάθε $v \in V$.

   Επίσης, η πολλαπλασιαστική ομάδα των αντιστρέψιμων γραμμικών απεικονίσεων του V (όπως και κάθε υποομάδα της) δρα με προφανή τρόπο πάνω στο V. Πάλι εδώ ο πυρήνας της δράσης είναι η τετριμμένη υποομάδα, αφού αν T είναι μια γραμμική απεικόνιση του V, τότε $T \cdot x = T(x) = x$, για κάθε $x \in V$, αν και μόνον αν $T = 1_V$.

4. Έστω G η διεδρική ομάδα D_n και X το σύνολο των κορυφών ενός κανονικού κυρτού n-γωνου. Όπως έχουμε δει στην Παράγραφο 3.1, η ομάδα D_n δρα επί του X και αυτή η δράση δίνει έναν μονομορφισμό της D_n στην S_n. Συνεπώς η D_n είναι ουσιαστικά μια υποομάδα της S_n. Το ίδιο ισχύει και για κάθε υποομάδα της D_n. Έτσι, έστω $G = \{1, \rho, \rho^2\}$ όπου ρ είναι η στροφή κατά 120° και έστω $X = \{1, 2, 3, 4, 5, 6\}$ οι κορυφές ενός εξαγώνου. Τότε η G μπορεί να "αναπαρασταθεί" από την υποομάδα $\{i, (1\ 3\ 5)(2\ 4\ 6), (1\ 5\ 3)(2\ 6\ 4)\}$ της S_6.

5. Θεωρούμε τη διεδρική ομάδα D_4 η οποία όπως είδαμε δρα πάνω στις κορυφές ενός τετραγώνου και ο πυρήνας της δράσης είναι η τετριμμένη υποομάδα. Μπορούμε όμως να θεωρήσουμε την D_4 να δρα πάνω στο σύνολο $X = \{\delta_1, \delta_2\}$ των διαγωνίων του τετραγώνου:



Ο πυρήνας αυτής της δράσης δεν είναι η τετριμμένη υποομάδα, αλλά η υποομάδα $\{1, \rho^2, \alpha_1, \alpha_2\}$, όπου ρ είναι η στροφή κατά 90° και α_i η ανάκλαση ως προς τη διαγώνιο δ_i.

6. Όταν θέλουμε να μελετήσουμε τη δομή μιας ομάδας G συνήθως τη θεωρούμε να δρα πάνω στον εαυτό της, δηλαδή το σύνολο X είναι η ίδια η G. Ένας τρόπος δράσης είναι αν θέσουμε $g \cdot x = gx$ (ο πολλαπλασιασμός της G). Οπότε ο αντίστοιχος ομομορφισμός $G \to S_G$ είναι αυτός ακριβώς που θεωρήθηκε στο θεώρημα του Cayley 3.5.4 Ένας άλλος τρόπος είναι αν θέσουμε
$$g \cdot x = gxg^{-1}, \quad g, x \in G.$$
Αυτή η δράση ονομάζεται ***δράση συζυγίας***. (Είναι δράση, καθώς $1 \cdot x = x$, $(g_1 g_2) \cdot x = g_1 g_2 x g_2^{-1} g_1^{-1} = g_1 \cdot (g_2 \cdot x)$). Στην πρώτη περίπτωση ο πυρήνας της δράσης είναι η τετριμμένη υποομάδα ενώ στη δεύτερη είναι το κέντρο $Z(G)$ της G (γιατί;).

7. Έστω $X = \mathcal{P}(G)$ το δυναμοσύνολο (σύνολο όλων των υποσυνόλων) της ομάδας G. Αν ορίσουμε $g \cdot \mathcal{U} = g\mathcal{U} = \{gu \mid u \in \mathcal{U}\}$ για κάθε $\mathcal{U} \in X$, $g \in G$ τότε αυτή είναι μια δράση πάνω στο X, ενώ αν θέσουμε $g \cdot \mathcal{U} = \mathcal{U}g = \{\, ug \mid u \in \mathcal{U}\,\}$ τότε αυτή δεν είναι δράση (αν η ομάδα δεν είναι Αβελιανή) αφού $g_1 \cdot (g_2 \cdot \mathcal{U}) = g_1 \cdot (\mathcal{U} g_2) = \mathcal{U} g_2 g_1 = (g_2 g_1) \cdot \mathcal{U}$.

8. Έστω $X = G/H$ το σύνολο των αριστερών κλάσεων μιας υποομάδας H μιας ομάδας G. Ορίζουμε μια δράση της G στο X, θέτοντας $g \cdot (xH) = (gx)H$ για κάθε $g \in G$ και $xH \in G/H$. Εδώ, ο αντίστοιχος ομομορφισμός $G \to S_{G/H}$ (τον οποίο θεωρήσαμε στην Παράγραφο 4.9) έχει πυρήνα την τομή $\bigcap\limits_{x \in G} xHx^{-1}$.

Ως ένα πρώτο αποτέλεσμα, αποδεικνύουμε τώρα, χρησιμοποιώντας την έννοια της δράσης μιας ομάδας, το εξής.

5.1.3 Πρόταση. *Κάθε ομάδα G με τάξη $2m$, όπου ο $m > 1$ είναι περιττός, δεν είναι απλή.*

Απόδειξη. Αρχικά, θα δείξουμε ότι η G έχει ένα στοιχείο τάξης 2. Πράγματι, έστω $G_1 = \{g \in G \mid g^2 = 1\}$ και $G_2 = \{g \in G \mid g^2 \neq 1\}$, οπότε $G = G_1 \dot{\cup} G_2$. Αν $G_2 = \emptyset$, τότε βέβαια ο ισχυρισμός είναι προφανής. Έστω ότι $G_2 \neq \emptyset$. Τότε, για κάθε $g \in G_2$, $g \neq g^{-1}$ και $g^{-1} \in G_2$. Άρα το πλήθος $|\,G_2\,|$ των στοιχείων του υποσυνόλου G_2 είναι άρτιο. Επειδή $|\,G\,| = 2m = |\,G_1\,| + |\,G_2\,|$, θα πρέπει το πλήθος $|\,G_1\,|$ των στοιχείων του υποσυνόλου G_1 να είναι επίσης άρτιο. Καθώς $1 \in G_1$, θα πρέπει $|\,G_1\,| \geq 2$ και άρα υπάρχει $g \in G$ με $g^2 = 1$ και $g \neq 1$.

Θεωρούμε τώρα τη G να δρα πάνω στον εαυτό της G με $g \cdot x = gx$ για κάθε $g, x \in G$. Καθώς $g \neq 1$, ισχύει $g \cdot x \neq x$ για κάθε $x \in G$. Άρα η μετάθεση $\sigma_g \in S_G$ δεν αφήνει κανένα στοιχείο της G σταθερό. Θεωρώντας την έκφραση της σ_g σε γινόμενο ξένων ανά δύο κύκλων, βλέπουμε ότι αυτοί οι κύκλοι πρέπει να είναι όλοι αντιμεταθέσεις ή 1-κύκλοι αφού $\sigma_g^2 = i$ και άρα $2 =$ε.κ.π.(των μηκών των κύκλων). Καθώς όμως η σ_g δεν αφήνει κανένα στοιχείο σταθερό, θα πρέπει οι προηγούμενοι κύκλοι να είναι μόνο αντιμεταθέσεις. Συνεπώς το πλήθος τους πρέπει να είναι περιττό (ίσο με m), αφού το πλήθος των συμβόλων που περιλαμβάνονται σε αυτές είναι $2m$. Έτσι, η σ_g είναι μια περιττή μετάθεση και άρα για το πρόσημό της θα ισχύει $\pi(\sigma_g) = -1$. Έτσι, ο ομομορφισμός $\pi \circ L : G \to \{1, -1\}$, όπου $L : G \to S_G$ είναι ο ομομορφισμός που ορίστηκε στο θεώρημα του Cayley (δηλαδή $L(g)(g') = gg'$ για κάθε $g, g' \in G$), είναι επί και άρα ο πυρήνας του έχει δείκτη 2. ⊤

Ασκήσεις 5.1

1. Έστω G μια ομάδα και H μια κανονική υποομάδα της. Δείξτε ότι η αντιστοιχία
$$\begin{aligned} G \times \mathcal{P}(H) &\longrightarrow \mathcal{P}(H) \\ (g, \mathcal{U}) &\longrightarrow g\mathcal{U}g^{-1} \end{aligned}$$
είναι δράση.

2. Έστω X_1 και X_2 δύο σύνολα πάνω στα οποία δρα η ίδια ομάδα G. Υποθέτουμε ότι $X_1 \cap X_2 = \emptyset$. Να ορίσετε μια "φυσιολογική" δράση της G πάνω στο σύνολο $X = X_1 \cup X_2$.

3. Έστω $G = O_2(\mathbb{R})$. Δείξτε ότι για κάθε δύο σημεία P και Q του επίπεδου $\mathbb{R}^2$ υπάρχει $A \in G$ τέτοιο ώστε $A(P) = Q$ αν και μόνον αν το P και το Q είναι σημεία του ίδιου κύκλου $x^2 + y^2 = r^2$ για κάποιο $r \geq 0$.

5.2 Τροχιές και Σταθεροποιούσες Υποομάδες

Θεωρούμε μια ομάδα G η οποία δρα πάνω σε ένα σύνολο X. Για ένα στοιχείο $x \in X$, το υποσύνολο $T_x = \{g \cdot x \mid g \in G\}$ του X ονομάζεται ***τροχιά*** του στοιχείου x κάτω από τη δράση της G. Αποδεικνύουμε τώρα ότι οι τροχιές των στοιχείων του X αποτελούν μια διαμέριση του X. Είναι φανερό ότι $X = \bigcup_{x \in X} T_x$. Αρκεί λοιπόν να δείξουμε ότι αν $x, y \in X$, τότε η $T_x \cap T_y = \emptyset$ ή $T_x = T_y$. Πράγματι, αν $z \in T_x \cap T_y$, τότε $z = g \cdot x = g' \cdot y$ για κάποια $g, g' \in G$. Αυτό σημαίνει ότι $(g^{-1}g') \cdot y = x$, δηλαδή $x \in T_y$ και άρα $T_x \subseteq T_y$. Όμοια προκύπτει ότι $T_y \subseteq T_x$, οπότε $T_x = T_y$. Συνεπώς έχουμε την ξένη ένωση

$$X = \dot{\bigcup_{x \in L}} T_x \,,$$

όπου L είναι ένα υποσύνολο του X που περιέχει ένα μόνο στοιχείο από κάθε τροχιά. Έτσι οι τροχιές είναι οι κλάσεις ισοδυναμίας που ορίζονται από την σχέση ισοδυναμίας που αντιστοιχεί στην παραπάνω διαμέριση του X. Συνεπώς δύο στοιχεία $x, y \in X$ είναι ισοδύναμα ως προς τη δράση της G αν και μόνον αν $x = g \cdot y$ για κάποιο $g \in G$. Έτσι, αν θεωρήσουμε την ομάδα D_4 να δρα πάνω στις κορυφές 1, 2, 3, 4 του τετραγώνου, τότε η τροχιά T_1 της κορυφής 1 είναι όλο το σύνολο X και συνεπώς όλες οι κορυφές είναι ισοδύναμες ως προς αυτή τη δράση. Αν H είναι μια υποομάδα μιας ομάδας G και ορίσουμε τη δράση της H πάνω στο σύνολο G με $h \cdot g = gh^{-1}$, $h \in H$, $g \in G$, τότε είναι φανερό ότι οι τροχιές αυτής της δράσης είναι οι αριστερές κλάσεις $\mod H$ στη G.

Τώρα θεωρούμε τη δράση συζυγίας μιας ομάδας G. Γι' αυτή τη δράση, η τροχιά ενός στοιχείου $g \in G$ ονομάζεται ***κλάση συζυγίας*** του g και συμβολίζεται συνήθως με

$$C\ell(g) = \{xgx^{-1} \mid x \in G\}.$$

Για την ομάδα S_n, οι κλάσεις συζυγίας έχουν ήδη καθοριστεί στην Παράγραφο 4.2. Για την ομάδα $GL_n(\mathbb{C})$, οι κλάσεις συζυγίας είναι γνωστές από τη Γραμμική Άλγεβρα. Πράγματι, αν A είναι ένας $n \times n$ μιγαδικός πίνακας με $\det A \neq 0$, τότε η κλάση συζυγίας του αποτελείται από όλους τους όμοιους με τον A πίνακες. Συνεπώς, η $C\ell(A)$ καθορίζεται από τη μορφή Jordan του A. Επίσης είναι φανερό ότι μια υποομάδα K μιας ομάδας G είναι κανονική αν και μόνο αν η κλάση συζυγίας κάθε στοιχείου της K είναι υποσύνολο της K. Με άλλα λόγια, η K είναι κανονική αν και μόνο αν αυτή είναι ένωση κλάσεων συζυγίας. Από αυτές τις επισημάνσεις, έπεται ότι οι κλάσεις συζυγίας παίζουν σημαντικό ρόλο στη μελέτη της δομής μιας ομάδας, καθώς επίσης και στις εφαρμογές της Θεωρίας Ομάδων.

Η τροχιά ενός στοιχείου x του X έχει άμεση σχέση με τη λεγόμενη ***σταθεροποιούσα υποομάδα*** του x της G. Αυτή ορίζεται ως το υποσύνολο

$$G_x = \{g \in G \mid g \cdot x = x\}$$

της G, δηλαδή το υποσύνολο που αποτελείται από όλα τα στοιχεία της G που αφήνουν σταθερό το x κάτω από τη δοσμένη δράση. Είναι προφανές ότι το G_x είναι μια υποομάδα της G και ο πυρήνας της δράσης είναι η τομή $\bigcap_{x \in X} G_x$. Ισχύει δε το εξής βασικό αποτέλεσμα, γνωστό ως Θεώρημα των τροχιών.

5.2.1 Θεώρημα. *Υποθέτουμε ότι μια ομάδα G δρα πάνω σε ένα σύνολο X και έστω T_x η τροχιά ενός στοιχείου x. Τότε*

$$|T_x| = |G : G_x|$$

Ιδιαίτερα, αν η G είναι πεπερασμένη, έχουμε

$$|G| = |T_x|\,|G_x|$$

και άρα το πλήθος των στοιχείων μιας τροχιάς διαιρεί την τάξη της ομάδας.

Απόδειξη. Θεωρούμε το σύνολο G/G_x των αριστερών κλάσεων $\bmod G_x$ στην G και την αντιστοιχία $\vartheta : G/G_x \longrightarrow T_x$ με $\vartheta(gG_x) \longrightarrow g \cdot x$. Αυτή είναι μια απεικόνιση, αφού αν $g_1G_x = g_2G_x$, $g_1, g_2 \in G$ τότε $g_1^{-1}g_2 \in G_x$ και άρα $(g_1^{-1}g_2) \cdot x = x$, δηλαδή $g_1 \cdot x = g_2x$. Τώρα για ένα $y \in T_x$, υπάρχει η αριστερή κλάση gG_x για την οποία $\vartheta(gG_x) = y$, όπου $g \cdot x = y$. Απομένει να δείξουμε ότι η ϑ είναι $1-1$. Έστω $g_1, g_2 \in G$ με $\vartheta(g_1G_x) = \vartheta(g_2G_x)$. Τότε $g_1 \cdot x = g_2 \cdot x$ που σημαίνει $g_1^{-1}g_2 \in G_x$, δηλαδή $g_1G_x = g_2G_x$. ⊺

5.2.2 Παρατήρηση. Το παραπάνω Θεώρημα μπορεί να θεωρηθεί ως μια γενίκευση του Θεωρήματος του Lagrange. Πράγματι,το Θεώρημα 4.4.22 προκύπτει από το 5.2.1, εφαρμόζοντάς το για τη δράση που δίνεται στο Παράδειγμα 5.1.2.8.

Μια χρήσιμη πληροφορία που μας δίνουν οι κλάσεις συζυγίας είναι ότι η τάξη μιας ομάδας G είναι το άθροισμα των τάξεων των κλάσεων συζυγίας της:

$$|G| = \sum_i |C\ell(g_i)|$$

όπου $g_1, g_2, \ldots, g_k$ είναι στοιχεία της G ανά δύο μη συζυγή τέτοια ώστε για κάθε $g \in G$ υπάρχει i για το οποίο $g \in C\ell(g_i)$. Η χρησιμότητα αυτής της εξίσωσης έγκειται στο γεγονός ότι κάθε προσθετέος είναι διαιρέτης της $|G|$. Μια

πιο εύχρηστη μορφή της εξίσωσης αυτής προκύπτει αν θεωρήσουμε το κέντρο $Z(G)$, το οποίο αποτελείται από όλα τα στοιχεία της G των οποίων η κλάση συζυγίας αποτελείται μόνο από ένα στοιχείο. Έτσι, έχουμε

$$|G| = |Z(G)| + \sum_i |C\ell(g_i)|$$

όπου τα g_i έχουν επιλεγεί από κλάσεις συζυγίας που έχουν περισσότερα του ενός στοιχεία. Αυτή η εξίσωση λέγεται ***εξίσωση κλάσεων*** της G.

Η σταθεροποιούσα υποομάδα ενός στοιχείου $g \in G$ για τη δράση συζυγίας πάνω στην G συνήθως ονομάζεται ***κεντροποιούσα υποομάδα*** του g και συμβολίζεται με $C_G(g)$. Αν $g_1, g_2 \in G$ είναι δύο συζυγή στοιχεία, έστω $g_1 = xg_2x^{-1}$, τότε εύκολα προκύπτει ότι $C_G(g_1) = xC_G(g_2)x^{-1}$. Με άλλα λόγια, οι κεντροποιούσες υποομάδες συζυγών στοιχείων είναι συζυγείς. Επίσης, παρατηρούμε ότι ο πυρήνας της δράσης συζυγίας είναι το κέντρο $Z(G) = \bigcap_{g\in G} C_G(g)$.

5.2.3 Παράδειγμα. Ας υπολογίσουμε την τάξη της κεντροποιούσας υποομάδας μιας μετάθεσης σ της S_n. Με βάση το Θεώρημα 5.2.1, αρκεί να υπολογίσουμε το πλήθος των μεταθέσεων που είναι συζυγείς με τη σ. Γνωρίζουμε ότι δύο μεταθέσεις είναι συζυγείς αν και μόνον αν είναι του ιδίου τύπου. Έστω ότι ο τύπος αυτός είναι η διαμέριση του n

$$(\lambda_1, \lambda_2, \ldots, \lambda_s),\ \lambda_1 \le \lambda_2 \le \cdots \le \lambda_s,\ \lambda_1 + \lambda + \cdots + \lambda_s = n.$$

Αυτό σημαίνει ότι αν $\sigma = \sigma_1\sigma_2\cdots\sigma_s$ είναι η έκφραση της σ ως γινόμενο ξένων ανά δύο κύκλων (συμπεριλαμβάνοντας και τους 1-κύκλους), η σ_k έχει μήκος λ_k. Υποθέτουμε ότι το πλήθος των σ_k που έχουν μήκος λ_k είναι α_k. Συνεπώς θέλουμε να βρούμε το πλήθος των μεταθέσεων των οποίων οι εκφράσεις ως γινόμενα ξένων ανά δύο κύκλων περιλαμβάνουν α_1 1-κύκλους, α_2 2-κύκλους $, \ldots,$ α_t t-κύκλους. Με άλλα λόγια όλες, αυτές μπορούν να παρασταθούν με το εξής σχήμα

$$\underbrace{(\bullet)(\bullet)\cdots(\bullet)}_{\alpha_1}\underbrace{(\bullet\bullet)(\bullet\bullet)\cdots(\bullet\bullet)}_{\alpha_2}\cdots\cdots\underbrace{\overbrace{(\bullet\bullet\bullet\cdots\bullet)}^{t}}_{\alpha_t}$$

Σε αυτό το σχήμα, οι τελείες αντικαθίστανται από τα σύμβολα $1, 2, \ldots, n$ με $n!$ τρόπους. Αλλά, οι μεταθέσεις που προκύπτουν δεν είναι όλες διακεκριμένες αφού οι α_i i-κύκλοι μπορούν να μετατεθούν μεταξύ τους χωρίς να αλλάξει η μετάθεση. Συνεπώς το πλήθος των αντικαταστάσεων των συμβόλων $1, 2, \ldots, n$ που μας δίνουν την ίδια μετάθεση με αυτό τον τρόπο είναι $\alpha_1!\alpha_2!\ldots\alpha_t!$. Επίσης ένας i-κύκλος μπορεί να γραφεί με i διαφορετικούς τρόπους χωρίς να αλλάξει η

μετάθεση. Επομένως το συνολικό πλήθος των αντικαταστάσεων των συμβόλων 1, 2, ..., n που μας δίνουν την ίδια μετάθεση είναι

$$1^{\alpha_1}\alpha_1!2^{\alpha_2}\alpha_2!\dots t^{\alpha_t}\alpha_t!$$

Άρα αν αντικαταστήσουμε στο προηγούμενο σχήμα τις τελείες με τα σύμβολα 1, 2, ..., n, θα πάρουμε

$$\frac{n!}{1^{\alpha_1}\alpha_1!2^{\alpha_2}\alpha_2!\dots t^{\alpha_t}\alpha_t!}$$

διαφορετικές μεταθέσεις οι οποίες είναι όλες οι συζυγείς μεταθέσεις που έχουν τον προηγούμενο τύπο. Άρα η κεντροποιούσα υποομάδα κάθε τέτοιας μετάθεσης έχει τάξη $1^{\alpha_1}\alpha_1!2^{\alpha_2}\alpha_2!\dots t^{\alpha_t}\alpha_t!$

Για παράδειγμα, αν $n = 5$, οι τάξεις των κεντροποιουσών υποομάδων δίνεται στον επόμενο πίνακα

Τύπος μετάθεσης	Τάξη κεντροποιούσας
1 1 1 1 1	$1^5 \cdot 5! \quad = 5!$
1 1 1 2	$1^3 \cdot 3! \quad 2^1 \cdot 1! = 12$
1 1 3	$1^2 \cdot 2! \quad 3^1 \cdot 1! = 6$
1 2 2	$1^1 \cdot 1! \quad 2^2 \cdot 2! = 8$
1 4	$1^1 \cdot 1! \quad 4^1 \cdot 1! = 4$
2 3	$2^1 \cdot 1! \quad 3^1 \cdot 1! = 6$
5	$5^1 \cdot 1! \quad = 5$

Από το Θεώρημα 5.2.1 έχουμε για μια πεπερασμένη ομάδα G,

$$|C\ell(g)| = \frac{|G|}{|C_G(g)|}.$$

Άρα η εξίσωση κλάσεων γίνεται

$$|G| = \sum_{i=1}^{k} \frac{|G|}{|C_G(g_i)|} = |G| \sum_{i=1}^{k} \frac{1}{|C_G(g_i)|}$$

και συνεπώς

$$1 = \sum_{i=1}^{k} \frac{1}{|C_G(g_i)|} \qquad (*)$$

όπου k είναι το πλήθος των κλάσεων συζυγίας. Χρησιμοποιώντας την εξίσωση $(*)$, θα αποδείξουμε τώρα ότι το πλήθος των μη ισόμορφων πεπερασμένων ομάδων που έχουν k ακριβώς κλάσεις συζυγίας είναι πεπερασμένο. Για το λόγο αυτό, θα χρειαστούμε το επόμενο αποτέλεσμα.

5.2.4 Λήμμα (E. Landau 1903). *Έστω $k \in \mathbb{N} - \{0\}$ και $r \in \mathbb{R}$. Τότε το πλήθος των ακολουθιών $(n_1, n_2, \ldots, n_k)$ θετικών ακεραίων αριθμών που είναι λύσεις της*

$$r = \sum_{i=1}^{k} \frac{1}{x_i} \qquad (**)$$

είναι πεπερασμένο.

Απόδειξη. Μπορούμε να υποθέσουμε ότι $r > 0$, διότι διαφορετικά δεν υπάρχει καμιά τέτοια ακολουθία θετικών ακεραίων αριθμών. Επιπλέον, αρκεί να δειχτεί ότι ισχύει το Λήμμα για φθίνουσες ακολουθίες $n_1 \geq n_2 \geq \cdots \geq n_k$. Εφαρμόζουμε επαγωγή στο k. Για $k = 1$ και r της μορφής $\frac{1}{\beta}$ υπάρχει μία μόνο ακολουθία, η (β), ενώ για οποιοδήποτε άλλο r δεν υπάρχει καμία ακολουθία. Έστω ότι η $n_1 \geq n_2 \geq \cdots \geq n_k$ είναι μια ζητούμενη λύση. Τότε $n_k \leq \frac{k}{r}$. Επειδή τώρα οι δυνατές επιλογές θετικών ακέραιων n με $n \leq \frac{k}{r}$ είναι πεπερασμένου πλήθους και (χρησιμοποιώντας την επαγωγική υπόθεση) για κάθε τέτοια επιλογή η εξίσωση

$$r - \frac{1}{n} = \sum_{i=1}^{k-1} \frac{1}{x_i}$$

έχει πεπερασμένο πλήθος ακεραίων θετικών λύσεων $(n_1, n_2, \ldots, n_{k-1})$ με $n_1 \geq n_2 \geq \cdots \geq n_{k-1}$, το Λήμμα ισχύει. ⊤

5.2.5 Θεώρημα. *Για όλες τις πεπερασμένες ομάδες G που έχουν k κλάσεις συζυγίας, για ένα δεδομένο k, υπάρχει ένας θετικός ακέραιος $C(k)$ τέτοιος ώστε $|G| \leq C(k)$.*

Απόδειξη. Έστω G μια πεπερασμένη ομάδα που έχει k κλάσεις συζυγίας. Θεωρούμε ότι $g_1 = 1$, οπότε $C_G(g_1) = G$. Αν στο προηγούμενο Λήμμα θέσουμε $r = 1$ τότε μια λύση της $(**)$ είναι η ακολουθία θετικών ακεραίων

$$(|G|), (|C_G(g_2)|, \ldots, |C_G(g_k)|).$$

Τώρα από όλες τις ακολουθίες θετικών ακεραίων λύσεων $(n_1, n_2, \ldots, n_k)$ με $n_1 \geq n_2 \geq \cdots \geq n_k$ θεωρούμε μια για την οποία το n_1 είναι ο μεγαλύτερος δυνατός ακέραιος, τον οποίο συμβολίζουμε με $C(k)$ (αφού εξαρτάται από το k). Τότε, έχουμε $|G| \leq C(k)$. ⊤

5.2.6 Πόρισμα. *Το πλήθος των πεπερασμένων ομάδων που έχουν k κλάσεις συζυγίας είναι πεπερασμένο.*

Απόδειξη. Κάθε τέτοια ομάδα έχει τάξη μικρότερη ή ίση από $C(k)$. Αλλά για $n \in \mathbb{N}$, υπάρχουν πεπερασμένου πλήθους ομάδες τάξης n (αφού, για παράδειγμα, κάθε μια από αυτές είναι ισόμορφη με μια ομάδα μεταθέσεων βαθμού n, από το θεώρημα του Cayley). ⊺

5.2.7 Παρατήρηση. Είναι φανερό ότι για μια πεπερασμένη ομάδα G το πλήθος των κλάσεων συζυγίας είναι ίσο με την τάξη $|G|$ της G αν και μόνον αν η G είναι Αβελιανή. Αν η G έχει μόνο μία κλάση συζυγίας τότε φυσικά αυτή είναι η τετριμμένη ομάδα. Αν αυτή περιέχει δύο κλάσεις συζυγίας, τότε η μια από αυτές έχει $|G|-1$ στοιχεία και από το Θεώρημα 5.2.1 το $|G|-1$ θα διαιρεί την $|G|$, δηλαδή $|G| = \lambda(|G|-1)$ για κάποιο $\lambda \in \mathbb{Z}$, $\lambda \geq 2$. Άρα $|G| \geq 2(|G|-1)$, οπότε $|G| \leq 2$ και επειδή $|G| \neq 1$, έχουμε $|G| = 2$. Δηλαδή η G είναι η κυκλική ομάδα τάξης 2. Το 1949 οι G. Higman, B.H. Neumann και H. Neumann απέδειξαν ότι υπάρχουν άπειρες το πλήθος ομάδες οι οποίες έχουν μόνο δύο κλάσεις συζυγίας, ενώ κάθε άπειρη ομάδα της οποίας όλα τα στοιχεία εκτός του 1 έχουν άπειρη τάξη μπορεί να εμφυτευτεί σε μία από αυτές.

Μια άλλη σημαντική εφαρμογή του Θεωρήματος 5.2.1 είναι η εξής.

5.2.8 Θεώρημα. *Έστω $|G| = p^n$, όπου p είναι ένας πρώτος αριθμός και $n \geq 1$. Τότε, το κέντρο $Z(G)$ της G δεν είναι τετριμμένο.*

Απόδειξη. Ένα στοιχείο $g \in G$ ανήκει στο κέντρο $Z(G)$ αν και μόνον αν η κλάση συζυγίας του περιέχει μόνο ένα στοιχείο (το ίδιο το g). Αλλά η τάξη $|Z(G)|$ του κέντρου διαιρεί το p^n, και άρα $Z(G) = p^m$. Αν λοιπόν ήταν $m = 0$, δηλαδή $|Z(G)| = 1$, τότε από την εξίσωση κλάσεων και το Θεώρημα 5.2.1, θα είχαμε

$$p^n = 1 + \sum_{i=1}^{k} p^{s_i}, \quad s_i \neq 0$$

όπου p^{s_i} είναι η τάξη της κλάσης συζυγίας $C\ell(g_i)$ με $g_i \neq 1$. Αυτό είναι άτοπο. Άρα πρέπει $m \neq 0$. ⊺

Επιπλέον, ως πόρισμα του Θεωρήματος 5.2.1, μπορούμε να πάρουμε το εξής ήδη γνωστό αποτέλεσμα.

5.2.9 Πόρισμα. *Έστω H, K δύο πεπερασμένες υποομάδες μιας ομάδας G. Τότε*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Απόδειξη. Θεωρούμε την ομάδα H να δρα πάνω στο σύνολο $X = \{xK \mid x \in G\}$ με $h \cdot xK = (hx)K$. Προφανώς έχουμε $HK = \bigcup_{h\in H} hK$. Καθώς $hK = h \cdot K$, βλέπουμε ότι το σύνολο HK είναι η ένωση εκείνων των αριστερών κλάσεων $\bmod K$ στη G που είναι στοιχεία της τροχιάς T_K. Άρα, αφού οι αριστερές κλάσεις $\bmod K$ που περιέχονται στην τροχιά T_K είναι ξένες ανά δύο και κάθε μια περιέχει $|K|$ στοιχεία, πρέπει $|HK| = |K||T_K|$. Αλλά επίσης η σταθεροποιούσα υποομάδα G_K είναι προφανώς η τομή $H \cap K$. Συνεπώς, από το Θεώρημα 5.2.1 έχουμε

$$|T_K| = \frac{|H|}{|H \cap K|} = \frac{|HK|}{|K|}. \quad \square$$

Μια ακόμα χρήσιμη εφαρμογή του Θεωρήματος 5.2.1, προκύπτει αν θεωρήσουμε μια ομάδα G να δρα πάνω στο δυναμοσύνολο της $X = \mathcal{P}(G)$ ως εξής.

$$g \cdot \mathcal{U} = g\mathcal{U}g^{-1}, \quad g \in G,\ u \in X.$$

Η σταθεροποιούσα υποομάδα $G_{\mathcal{U}}$ ενός υποσυνόλου $\mathcal{U}$ της G συμβολίζεται με $N_G(\mathcal{U})$ και ονομάζεται ***κανονικοποιούσα υποομάδα*** του $\mathcal{U}$. Οπότε, από το Θεώρημα 5.2.1, ο δείκτης $|\, G : N_G(\mathcal{U})\,|$ είναι το πλήθος των διακεκριμένων υποσυνόλων της μορφής $g\mathcal{U}g^{-1}$, $g \in G$. Ειδικά, αν $\mathcal{U}$ είναι μια υποομάδα μιας πεπερασμένης ομάδας G και θεωρήσουμε την ένωση $\bigcup\limits_{g\in G} g\mathcal{U}g^{-1}$, τότε έχουμε

$$\left|\bigcup g\mathcal{U}g^{-1}\right| - 1 = \left|\bigcup_{g\in G} (g\mathcal{U}g^{-1} \setminus \{1\})\right| \leq |G : N_G(\mathcal{U})|\,(|\mathcal{U}| - 1),$$

αφού $|g\mathcal{U}g^{-1}| = |\mathcal{U}|$ για κάθε $g \in G$. Αλλά ισχύει $|G : N_G(\mathcal{U})| \leq |G : \mathcal{U}|$. Άρα $|\bigcup g\mathcal{U}g^{-1}| - 1 \leq |G : \mathcal{U}|\,(|\mathcal{U}| - 1) = |G| - |G : \mathcal{U}|$ και τελικά

$$\left|\bigcup g\mathcal{U}g^{-1}\right| \leq 1 + |G| - |G : \mathcal{U}|\,.$$

Αν η $\mathcal{U}$ περιέχει τουλάχιστον ένα στοιχείο από κάθε κλάση συζυγίας της G, τότε η ένωση $\bigcup\limits_{g\in G} g\mathcal{U}g^{-1}$ περιέχει όλα τα στοιχεία της G και άρα αυτή η ένωση θα πρέπει να είναι ίση με τη G. Οπότε, από την προηγούμενη ανισότητα προκύπτει ότι $|G : \mathcal{U}| \leq 1$ και άρα $G = \mathcal{U}$. Από αυτό συμπεραίνουμε ότι:

5.2.10 Πρόταση. *Αν A είναι ένα υποσύνολο της G που περιέχει τουλάχιστον ένα στοιχείο από κάθε κλάση συζυγίας τότε η G παράγεται από το A.*

Απόδειξη. Αρκεί να θεωρήσουμε την υποομάδα $\mathcal{U}$ που παράγεται από το A, οπότε σύμφωνα με τα προηγούμενα, αυτή θα πρέπει να είναι όλη η G. ⊺

Ασκήσεις 5.2

1. Χρησιμοποιήστε την εξίσωση κλάσεων για να βρείτε όλες τις πεπερασμένες ομάδες G για τίς οποίες η κεντροποιούσα υποομάδα $C_G(g)$ κάθε στοιχείου $g \in G \setminus \{1\}$ είναι η $\{1, g, g^{-1}\}$ (με την περίπτωση $g = g^{-1}$ να μην αποκλείεται).

2. Έστω G μια ομάδα με 16 στοιχεία, η οποία δρα σε ένα σύνολο X με 31 στοιχεία. Δείξτε ότι υπάρχει στοιχείο του X που μένει σταθερό κάτω απο τη δράση της G.

3. Έστω G μια ομάδα τάξης p^n και X ένα σύνολο που το πλήθος των στοιχείων του δεν διαιρείται με το p. Υποθέτουμε ότι η G δρα στο X. Δείξτε ότι υπάρχει ένα τουλάχιστον στοιχείο του X που παραμένει σταθερό κάτω από τη δράση της G.

4. Έστω $G = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \mid \alpha \neq 0,\ \alpha, \beta \in \mathbb{R} \right\}$ και $X = \mathbb{R}$. Ορίζουμε $g \cdot x = \alpha x + \beta$, για $g = \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}$ και $x \in \mathbb{R}$. Αφού δειχτεί ότι η G δρα πάνω στο X, να βρεθεί η τροχιά και η σταθεροποιούσα υποομάδα του μηδενός. Ποιος είναι ο πυρήνας της δράσης; Για κάθε δύο πραγματικούς x_1, x_2 υπάρχει $g \in G$ έτσι ώστε $g \cdot x_1 = x_2$;

5. Έστω G_1, G_2 δύο ομάδες. Δείξτε ότι στην $G_1 \times G_2$ τα στοιχεία (a_1, b_1) και (a_2, b_2) είναι συζυγή αν και μόνον αν το a_1 είναι συζυγές του a_2 και το b_1 είναι συζυγές του b_2.

6. Δείξτε ότι δύο συζυγή στοιχεία σε μια ομάδα έχουν την ίδια τάξη. Δώστε ένα παράδειγμα δύο στοιχείων σε μια ομάδα που έχουν την ίδια τάξη αλλά δεν είναι συζυγή.

7. Δείξτε ότι αν X είναι ένα υποσύνολο μιας ομάδας G που περιέχει έναν αντιπρόσωπο από κάθε κλάση συζυγίας και τα στοιχεία του αντιμετατίθενται τότε η G είναι Αβελιανή.

8. Έστω G μια ομάδα και $a, b \in G$ δύο συζυγή στοιχεία. Να δειχτεί ότι οι κεντροποιούσες υποομάδες των a και b είναι ίσες αν (τουλάχιστον) μία από αυτές είναι κανονική.

9. Χρησιμοποιώντας την εξίσωση κλάσεων μιας πεπερασμένης ομάδας αποδείξτε ότι η ομάδα έχει ένα τουλάχιστον στοιχείο g τάξης p όπου p είναι ένας πρώτος διαιρέτης της τάξης της ομάδας (Θεώρημα του Cauchy, βλέπε επόμενη παράγραφο).

10. Πόσες κλάσεις συζυγίας υπάρχουν στις ομάδες S_7 και S_8;

11. Αν $\tau = (1\,3)(2\,4) \in S_n$, για κάποιο $n \geq 4$, υπολογίστε την κεντροποιούσα υποομάδα $C_{S_n}(\tau)$.

12. Έστω G μια πεπερασμένη ομάδα και x, y δύο συζυγή στοιχεία της G. Δείξτε ότι ο αριθμός των στοιχείων $g \in G$ που είναι τέτοια ώστε $g\,x\,g^{-1} = y$ είναι ίσος με $|\,C_G(x)\,|$.

13. Έστω G μια πεπερασμένη ομάδα και $x \in G$. Δείξτε ότι $|\,C_G(x)\,| \geq |\,\overline{G}\,|$, όπου $\overline{G} = G/[G,\,G]$.

14. Έστω V ένας διανυσματικός χώρος επί ενός σώματος $\mathbb{F}$ με διάσταση n. Αν u είναι ένα μη μηδενικό διάνυσμα του V και

$$H = \{A \in GL_n(\mathbb{F}) : \text{το διάνυσμα } u \text{ είναι ιδιοδιάνυσμα του } A\},$$

τότε δείξτε ότι το σύνολο H είναι υποομάδα της $G = GL_n(\mathbb{F})$ και ότι αν $\mathbb{F} = \mathbb{C}$, τότε $GL_n(\mathbb{C}) = \bigcup_{g \in GL_n(\mathbb{C})} gHg^{-1}$.

15. Έστω G μια ομάδα και H μια υποομάδα της. Δείξτε ότι το $C_G(\,H\,) = \{\,g \in G \mid gu = ug,\ \text{για κάθε}\ \ u \in H\,\}$ είναι υποομάδα της G και μάλιστα κανονική υποομάδα της κανονικοποιούσας υποομάδας της H. Επιπλέον δείξτε ότι η ομάδα πηλίκο $N_G(H)/C_G(H)$ είναι ισόμορφη με μια υποομάδα της ομάδας αυτομορφισμών της H.

16. Έστω G μια πεπερασμένη μη κυκλική ομάδα της οποίας κάθε γνήσια υποομάδα είναι Αβελιανή. Δείξτε ότι υπάρχει κανονική υποομάδα N της G με $1 \neq N \neq G$.

17. Έστω G μια ομάδα με τάξη n. Υποθέτουμε ότι ο n είναι σχετικά πρώτος με τον $\varphi(n)$, όπου φ είναι η συνάρτηση του Euler. Δείξτε ότι η ομάδα G είναι Αβελιανή.

5.3 Τα Θεωρήματα του Sylow

Έστω G μια πεπερασμένη ομάδα. Από το θεώρημα του Lagrange, ξέρουμε ότι η τάξη κάθε υποομάδας της G διαιρεί την τάξη της G. Το αντίστροφο αυτού του θεωρήματος δεν ισχύει, δηλαδή αν m είναι ένας διαιρέτης της $|G|$, τότε μπορεί να μην υπάρχει υποομάδα της G που να έχει τάξη m. Για παράδειγμα, η ομάδα A_4 δεν έχει υποομάδα τάξης 6 (βλέπε το Παράδειγμα που ακολουθεί μετά την Παρατήρηση 4.4.27).

Το 1872 ο Νορβηγός μαθηματικός L. Sylow απέδειξε ότι αν η τάξη της G είναι της μορφής $p^\alpha m$, όπου p είναι ένας πρώτος αριθμός, τότε η G έχει μια υποομάδα τάξης p^α. Αυτό το αποτέλεσμα θεωρείται ως το θεμελιώδες θεώρημα της θεωρίας των πεπερασμένων ομάδων. Μια απλή απόδειξη αυτού του θεωρήματος έχει δοθεί από τον Wielandt [31], χρησιμοποιώντας το Θεώρημα 5.2.1.

Δίνουμε μια απόδειξη του επόμενου Λήμματος, το οποίο έχουμε συναντήσει και στην πρώτη Ενότητα (βλέπε Εφαρμογή 1.1.7), χρησιμοποιώντας δράσεις.

5.3.1 Λήμμα. *Έστω B_r το σύνολο όλων των υποσυνόλων του συνόλου $A = \{1, \ldots, n\}$ που το πλήθος των στοιχείων τους είναι ίσο με r. Τότε*

$$|B_r| = \frac{n!}{r!(n-r)!}$$

Απόδειξη. Ορίζουμε μια δράση της συμμετρικής ομάδας $S_A \cong S_n$ στο B_r, θέτοντας $\sigma \cdot \mathcal{U} = \{\sigma(u) \mid u \in \mathcal{U}\}$ για κάθε $\sigma \in S_n$ και $\mathcal{U} \in B_r$. Παρατηρούμε ότι αν $\mathcal{U}_1 = \{u_1, \ldots, u_r\}$ και $\mathcal{U}_2 = \{u'_1, \ldots, u'_r\}$ είναι δύο στοιχεία του B_r, τότε υπάρχει ένα στοιχείο $\sigma \in S_n$, τέτοιο ώστε $\sigma \cdot \mathcal{U}_1 = \mathcal{U}_2$. Αυτό σημαίνει ότι η τροχιά ενός οποιουδήποτε στοιχείου του B_r είναι όλο το B_r, δηλαδή έχουμε μόνο μια τροχιά γι' αυτή τη δράση. Αν θεωρήσουμε το σύνολο $\mathcal{U} = \{1, 2, \ldots, r\}$, τότε η σταθεροποιούσα υποομάδα $G_\mathcal{U}$ του $\mathcal{U}$ είναι το σύνολο όλων των μεταθέσεων

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & r & r+1 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(r) & \sigma(r+1) & \cdots & \sigma(n) \end{pmatrix}$$

έτσι ώστε $\mathcal{U} = \{\sigma(1), \sigma(2), \ldots, \sigma(r)\}$. Άρα η μετάθεση $\sigma(1), \sigma(2), \ldots, \sigma(r)$ μπορεί να είναι μια οποιαδήποτε από τις $r!$ μεταθέσεις των $1, 2, \ldots, r$ και η μετάθεση $\sigma(r+1), \ldots, \sigma(n)$ μπορεί να είναι μια οποιαδήποτε από τις $(n-r)!$ μεταθέσεις των $r+1, \ldots, n$. Συνεπώς $|G_\mathcal{U}| = r!(n-r)!$ και επειδή το B_r είναι η τροχιά του $\mathcal{U}$ έχουμε, με βάση το Θεώρημα 5.2.1,

$$|B_r| = |S_n : G_\mathcal{U}| = \frac{n!}{r!(n-r)!} = \binom{n}{r}. \quad \blacksquare$$

5.3.2 Λήμμα. *Αν p είναι ένας πρώτος αριθμός και p^s είναι η μεγαλύτερη δύναμη του p που διαιρεί το φυσικό αριθμό m τότε ο p^s είναι η μεγαλύτερη δύναμη του p που διαιρεί και τον $\begin{pmatrix} p^\alpha m \\ p^\alpha \end{pmatrix}$.*

Απόδειξη. Έχουμε

$$\begin{pmatrix} p^\alpha m \\ p^\alpha \end{pmatrix} = \frac{p^\alpha m(p^\alpha m-1)\cdots(p^\alpha m-i)\cdots(p^\alpha m-p^\alpha+1)}{p^\alpha(p^\alpha-1)\cdots(p^\alpha-i)\cdots(p^\alpha-p^\alpha+1)}$$

Παρατηρούμε ότι η μέγιστη δύναμη του p που διαιρεί τον $(p^\alpha m-i)$ είναι η ίδια όπως αυτή που διαιρεί και τον $p^\alpha-i$. Συνεπώς όλες οι δυνάμεις του p απαλείφονται εκτός από τη δύναμη που διαιρεί το m . ⊺

5.3.3 1ο Θεώρημα του Sylow. *Αν p^α είναι μια δύναμη ενός πρώτου αριθμού που διαιρεί την τάξη της ομάδας G, τότε η G περιέχει μια υποομάδα τάξης p^α.*

Απόδειξη. Έστω X το σύνολο όλων των υποσυνόλων της G που έχουν τάξη p^α. Τότε η G δρα πάνω στο X με $g\cdot\mathcal{U}=\{\,gu \mid u\in\mathcal{U}\,\}$. Έστω $X_1, X_2, \ldots, X_s$ οι τροχιές αυτής της δράσης. Έχουμε

$$|X|=\sum_{i=1}^{s}|X_i| \quad . \tag{1}$$

Έστω ότι X_i είναι η τροχιά του υποσυνόλου $\mathcal{U}_i$ της G που έχει p^α στοιχεία. Αν H_i είναι η σταθεροποιούσα υποομάδα του $\mathcal{U}_i$, τότε, από το 5.2.1, έχουμε ότι

$$|X_i|=\frac{|G|}{|H_i|}, \quad i=1,2,\ldots,s. \tag{2}$$

Αν $u\in\mathcal{U}_i$ και $x\in H_i$, τότε $xu\in\mathcal{U}_i$ αφού $x\cdot\mathcal{U}_i=\mathcal{U}_i$. Κρατώντας το u σταθερό και θεωρώντας το x να διατρέχει όλα τα στοιχεία της H_i, παίρνουμε $H_iu\subseteq\mathcal{U}_i$. Άρα το $\mathcal{U}_i$ είναι η ένωση όλων των δεξιών κλάσεων H_iu, $u\in\mathcal{U}_i$ (φυσικά όλες αυτές οι κλάσεις μπορεί να μην είναι διάφορες μεταξύ τους). Έστω r_i το πλήθος των διάφορων ανά δύο κλάσεων H_iu, $u\in\mathcal{U}_i$. Τότε $|\mathcal{U}_i|=r_i\,|H_i|$. Αυτό δείχνει ότι η τάξη $|H_i|$ της H_i διαιρεί την τάξη $|\mathcal{U}_i|=p^\alpha$. Συνεπώς έχουμε

$$|H_i|=p^{\alpha_i}, \quad \alpha_i\le\alpha,\ i=1,\ldots,s. \tag{3}$$

Έστω $n=|G|=p^\alpha m$. Από τις (2) και (3) έπεται ότι

$$|X_i|=p^{d_i}m \quad \text{όπου} \quad d_i=\alpha-\alpha_i.$$

Επίσης, από το Λήμμα 5.3.1 έχουμε

$$|X| = \begin{pmatrix} p^\alpha m \\ p^\alpha \end{pmatrix}$$

και αν p^t είναι η μεγαλύτερη δύναμη που διαιρεί τον m τότε, από το 5.3.2, η δύναμη p^{t+1} δεν διαιρεί τον $|X| = m(p^{d_1} + \cdots + p^{d_s})$. Αν ήταν $d_i > 0$, για όλα τα $i = 1, 2, \ldots, s$, τότε η δύναμη p^{t+1} θα διαιρούσε τον $|X|$ που είναι άτοπο. Άρα πρέπει να υπάρχει κάποιο $i = 1, 2, \ldots, s$, έτσι ώστε $d_i = 0$. Γι' αυτό το i θα έχουμε $\alpha_i = \alpha$, δηλαδή $|H_i| = p^\alpha$ που αποδεικνύει το ζητούμενο. ⊤

Ιδιαίτερα αν p^α είναι η μεγαλύτερη δύναμη του p που διαιρεί την τάξη $|G|$, τότε οι υποομάδες της G που έχουν τάξη p^α λέγονται ***p*-υποομάδες του Sylow**.

5.3.4 Πόρισμα (Θεώρημα του Cauchy). *Αν p είναι ένας πρώτος διαιρέτης της τάξης $|G|$ μιας πεπερασμένης ομάδας G, τότε υπάρχει ένα στοιχείο της G που έχει τάξη p.*

5.3.5 Πόρισμα. *Το σύνολο όλων των πρώτων αριθμών που διαιρούν την τάξη μιας πεπερασμένης ομάδας G είναι το σύνολο των πρώτων αριθμών οι οποίοι είναι τάξεις στοιχείων της ομάδας.*

Απόδειξη. Αυτό προκύπτει από το Θεώρημα του Lagrange και το Πόρισμα 5.3.4 . ⊤

5.3.6 Πόρισμα. *Σε μια πεπερασμένη ομάδα G κάθε στοιχείο της, έχει τάξη ίση με μια δύναμη ενός πρώτου p αν και μόνον αν η τάξη της είναι μια δύναμη του p.*

Απόδειξη. Έστω $|G| = p_1^{n_1} \cdots p_s^{n_s}$ η ανάλυση της τάξης της G σε πρώτους παράγοντες. Από το Πόρισμα 5.3.4, έπεται ότι για κάθε $i = 1, \ldots, s$ υπάρχει τουλάχιστον ένα στοιχείο του οποίου η τάξη είναι p_i. Αλλά αν κάθε στοιχείο της G έχει τάξη μια δύναμη του p, τότε πρέπει $p_i = p_2 = \cdots = p_s = p$. ⊤

Μια ομάδα (πεπερασμένη ή άπειρη) λέγεται ***p*-ομάδα** αν κάθε στοιχείο της έχει τάξη μια δύναμη του p, όπου p είναι πρώτος αριθμός. Συνεπώς το Πόρισμα 5.3.6 θα μπορούσε να διατυπωθεί, μ' αυτή την ορολογία ως εξής: "*Μια πεπερασμένη ομάδα είναι μια p-ομάδα αν και μόνον αν η τάξη της είναι μια δύναμη του p.*"

5.3.7 Πρόταση. *Αν P είναι μια p-υποομάδα Sylow και N είναι μια κανονική υποομάδα της πεπερασμένης ομάδας G, τότε*

α) Η υποομάδα PN/N είναι p-υποομάδα του Sylow της G/N.

β) Η τομή $P \cap N$ είναι μια p-υποομάδα του Sylow της N.

Απόδειξη. Από τον ορισμό των p-υποομάδων του Sylow, η P είναι μια p-υποομάδα του Sylow αν και μόνον αν η τάξη της είναι μια δύναμη του p και ο δείκτης της P στην G είναι πρώτος προς τον p.

α) Από το 2ο Θεώρημα των ισομορφισμών έχουμε

$$\frac{PN}{N} \cong \frac{P}{P \cap N}.$$

Άρα η τάξη της PN/N είναι μια δύναμη του p. Από το Πόρισμα 4.4.25, έχουμε

$$|G : P| = |G : PN|\,|PN : P|$$

και άρα ο p δεν διαιρεί το $|G : PN|$. Χρησιμοποιώντας πάλι το Πόρισμα 4.4.25, προκύπτει ότι

$$|G : N| = |G : PN|\,|PN : N|$$

συμπεραίνουμε ότι η PN/N είναι p-υποομάδα του Sylow της G/N.

β) Από το Πόρισμα 4.4.25, έχουμε

$$|PN : N|\,|N : P \cap N| = |PN : P \cap N| = |PN : P|\,|P : P \cap N| \ .$$

Επειδή όμως $|PN/N| = |P/P \cap N|$, προκύπτει ότι $|N : P \cap N| = |PN : P|$. Αλλά επειδή ο δείκτης $|PN : P|$ διαιρεί το δείκτη $|G : P|$ (που είναι πρώτος προς τον p), έπεται ότι και ο δείκτης $|N : P \cap N|$ είναι πρώτος προς τον p. Συνεπώς, η $P \cap N$ είναι μια p-υποομάδα του Sylow της N. ⊤

5.3.8 Πρόταση. *Μια p-υποομάδα του Sylow της G είναι η μόνη p-υποομάδα του Sylow της κανονικοποιούσας υποομάδας $N_G(P)$.*

Απόδειξη. Η P είναι φυσικά κανονική υποομάδα της $N_G(P)$. Υποθέτουμε ότι P' είναι μια άλλη p-υποομάδα του Sylow της $N_G(P)$. Από το 2ο Θεώρημα ισομορφισμών έχουμε

$$\frac{PP'}{P} \cong \frac{P'}{P \cap P'}.$$

Αυτό δείχνει ότι η τάξη $|PP'|$ της PP' είναι μια δύναμη του p. Αλλά η τάξη $|P|$ της P είναι η μεγαλύτερη δύναμη του p που διαιρεί την τάξη της G. Άρα $|PP'| = |P|$ και συνεπώς $P = P'$. ⊤

5.3.9 Πόρισμα. *Αν η G είναι Αβελιανή ομάδα, τότε αυτή έχει μόνο μια p-υποομάδα του Sylow (αφού $N_G(P) = G$).*

Φυσικά, το αποτέλεσμα αυτό το έχουμε δει και νωρίτερα (βλέπε Πόρισμα 4.8.5).

5.3.10 2ο Θεώρημα του Sylow. *Αν r είναι το πλήθος των p-υποομάδων του Sylow μιας πεπερασμένης ομάδας G, τότε $p \mid r-1$ δηλαδή $r \equiv 1 \mod p$.*

Απόδειξη. Έστω $P_1, P_2, \ldots, P_r$ όλες οι p-υποομάδες του Sylow της G. Η P_1 δρα πάνω στο σύνολο $\{P_1, P_2, \ldots, P_r\}$ με δράση $g \cdot P_i = gP_ig^{-1}$, $g \in P_1$, $i = 1, 2, \ldots, r$ (αφού η gP_ig^{-1} είναι μια p-υποομάδα του Sylow). Κάτω από αυτή τη δράση η μόνη p-υποομάδα που μένει σταθερή είναι η P_1. Πράγματι, αν υπήρχε $i \in \{2, 3, \ldots, r\}$ με $gP_ig^{-1} = P_i$, για κάθε $g \in P_1$, τότε η P_1 θα ήταν υποομάδα της κανονικοποιούσας υποομάδας $N_G(P_i)$ της P_i, αλλά σύμφωνα με την Πρόταση 5.3.8 αυτό είναι άτοπο.

Συνεπώς, γι' αυτή τη δράση, μόνο μια τροχιά περιέχει μόνο ένα στοιχείο και αυτή είναι το μονοσύνολο $\{P_1\}$. Άρα, από το Θεώρημα 5.2.1, το πλήθος των p-υποομάδων του Sylow που περιέχονται σε μια τροχιά διάφορη της $\{P_1\}$ πρέπει να διαιρεί την τάξη $|P_1|$ της P_1, δηλαδή αυτό το πλήθος πρέπει να είναι μια δύναμη του p. Συνεπώς

$$r = 1 + (\text{άθροισμα δυνάμεων του } p)$$

και άρα $p \mid r-1$. ⊤

5.3.11 3ο Θεώρημα του Sylow. *α) Όλες οι p-υποομάδες του Sylow είναι συζυγείς.*

β) Κάθε υποομάδα της G με τάξη μια δύναμη του p είναι υποομάδα μιας p-υποομάδας του Sylow.

Απόδειξη. α) Έστω ότι δεν είναι όλες οι p-υποομάδες του Sylow $P_1, \ldots, P_r$ συζυγείς μεταξύ τους. Με μια κατάλληλη αρίθμηση μπορούμε να υποθέσουμε ότι οι πρώτες $P_1, \ldots, P_s$ με $s < r$, είναι συζυγείς. Η p-υποομάδα του Sylow P_1, όπως και στην απόδειξη του Θεωρήματος 5.3.10, δρα επί του συνόλου $\{P_1, \ldots, P_s\}$ και συνεπώς $s \equiv 1 \mod p$. Έστω t το πλήθος των p-υποομάδων του Sylow που είναι συζυγείς με την P_{s+1}. Με κατάλληλη αρίθμηση μπορούμε να υποθέσουμε ότι αυτές είναι οι $P_{s+1}, P_{s+2}, \ldots, P_{s+t}$. Στο σύνολο $\{P_{s+1}, \ldots, P_{s+t}\}$ δρα τώρα και η P_1 και η P_{s+1}. Άρα, όπως ακριβώς στην απόδειξη του Θεωρήματος 5.3.10, θα έχουμε από τη δράση της P_1, $t \equiv 0 \mod p$ και από τη δράση της P_{s+1}, $t \equiv 1 \mod p$ που είναι άτοπο. Άρα πρέπει να είναι $s = r$.

β) Έστω K μια p-υποομάδα της G. Η K δρα στο σύνολο $\{P_1, \ldots, P_r\}$ με $x \cdot P_i = xP_ix^{-1}$, $x \in K$, $i = 1, \ldots, r$. Επειδή η τάξη της K είναι μια δύναμη του p, από το Θεώρημα 5.2.1, πρέπει κάθε τροχιά αυτής της δράσης να έχει τάξη μια δύναμη του p. Επειδή όμως $r \equiv 1 \mod p$, τουλάχιστον μια τροχιά πρέπει να αποτελείται μόνο από μια p-υποομάδα του Sylow, έστω την P_k. Δηλαδή $xP_kx^{-1} = P_k$, για κάθε $x \in K$, ή $xP_k = P_kx$, για κάθε $x \in K$. Τότε $KP_k = P_kK$ και άρα το σύνολο P_kK είναι υποομάδα. Επιπλέον, η τάξη της P_kK είναι μία δύναμη του p, αφού $|P_kK| = |P_k||K| \,/\, |P_k \cap K|$. Επειδή τώρα $P_k \subseteq P_kK$ και η τάξη $|P_k|$ της P_k είναι η μεγαλύτερη δύναμη του p που διαιρεί την τάξη της G, πρέπει $P_k = P_kK$ και άρα $K \subseteq P_k$. ⊤

Από έδω και στο εξής, θα συμβολίζουμε με $Syl_p(G)$ το σύνολο $\{P_1, \ldots, P_r\}$ όλων των p-υποομάδων του Sylow της ομάδας G, οι οποίες μόλις δείξαμε ότι είναι συζυγείς μεταξύ τους.

5.3.12 Πόρισμα. *Έστω G μια πεπερασμένη ομάδα και έστω $P \in Syl_p(G)$. Τότε*

$$|Syl_p(G)| = |G : N_G(P)| \ .$$

Απόδειξη. Η G δρα με συζυγία πάνω στο σύνολο $Syl_P(G)$. Από το Θεώρημα 5.3.11, έπεται ότι αυτή η δράση έχει μόνο μια τροχιά, η οποία εξαντλεί το σύνολο $Syl_p(G)$. Άρα, το ζητούμενο έπεται από το Θεώρημα 5.2.1. ⊤

5.3.13 Πόρισμα. *Έστω G μια πεπερασμένη ομάδα και $r = |Syl_p(G)|$. Τότε ο r διαιρεί τον δείκτη $|G : P|$.*

Απόδειξη. Από το Πόρισμα 5.3.12 έχουμε $r = |\, G : N_G(P)\,|$ και από το Πόρισμα 4.4.25 παίρνουμε $|G : P| = r\,|N_G(P) : P|$. ⊤

5.3.14 Πόρισμα. *Έστω G μια πεπερασμένη ομάδα και $P \in Syl_p(G)$. Τότε τα εξής είναι ισοδύναμα.*

α) $P \trianglelefteq G$.

β) Η P είναι η μοναδική p-υποομάδα του Sylow.

γ) Κάθε p-υποομάδα της G περιέχεται στην P.

δ) Η P είναι χαρακτηριστική υποομάδα της G, δηλαδή για κάθε αυτομορφισμό ϑ της G ισχύει $\vartheta(P) = P$.

Απόδειξη. α)⇒β) Προφανές από το 5.3.11(α).

β)⇒γ) Προφανές πάλι από το 5.3.11β).

γ)⇒δ) Έστω $\vartheta \in Aut(G)$. Τότε $|\,\vartheta(P)\,| = |\,P\,|$. Καθώς η $\vartheta(P)$ είναι μια p-υποομάδα από την υπόθεση, θα πρέπει $\vartheta(P) \subseteq P$ και άρα $\vartheta(P) = P$.

δ)⇒α) Προφανές. ⊤

5.3.15 Λήμμα. *Αν H είναι μια p-υποομάδα της G, η οποία δεν είναι μια p-υποομάδα του Sylow, τότε $H \lneq N_G(H)$.*

Απόδειξη. Αν ο p δεν διαιρεί το δείκτη $|G : N_G(H)|$, τότε η $N_G(H)$ περιέχει μια p-υποομάδα του Sylow P' που περιέχει την H γνήσια, αφού η H δεν είναι p-υποομάδα του Sylow. Συνεπώς $H \lneq N_G(H)$.

Τώρα υποθέτουμε ότι ο p διαιρεί το δείκτη $|G : N_G(H)|$. Θεωρούμε το σύνολο όλων των υποομάδων που είναι συζυγείς με την H, των οποίων το πλήθος είναι $|G : N_G(H)|$. Θεωρούμε επίσης την H να δρα με συζυγία πάνω σ' αυτό το σύνολο. Μια τροχιά αυτής της δράσης είναι το μονοσύνολο $\{H\}$. Επειδή ο p διαιρεί το δείκτη $|G : N_G(H)|$, ο οποίος ισούται με το άθροισμα των τάξεων των τροχιών, και κάθε τροχιά έχει τάξη μια δύναμη του p, πρέπει να υπάρχουν και άλλες τροχιές που είναι μονοσύνολα. Έστω $\{\mathcal{U}_1\}$, $\mathcal{U}_1 = gHg^{-1}$ μια τέτοια τροχιά, δηλαδή $u\mathcal{U}_1u^{-1} = \mathcal{U}_1$, για κάθε $u \in H$. Αυτό σημαίνει ότι $H \leq N_G(\mathcal{U}_1)$ και επειδή $H \neq \mathcal{U}_1$ πρέπει $\mathcal{U}_1 \lneq N_G(\mathcal{U}_1)$. Άρα $H \lneq N_G(H) = g^{-1}N_G(\mathcal{U}_1)g$. ⊤

5.3.16 Λήμμα. *Έστω $P \in Syl_p(G)$. Τότε όλες οι p-υποομάδες της $N_G(P)$ είναι υποομάδες της P.*

Απόδειξη. Το ζητούμενο προκύπτει από το Πόρισμα 5.3.14. ⊤

Χρησιμοποιώντας το λήμμα μπορούμε να δείξουμε τώρα κάτι ισχυρότερο από το Θεώρημα 5.3.10:

5.3.17 Πόρισμα. *Ισχύει*

$$|Syl_p(G)| \equiv 1 \mod p^e$$

αν $p^e \leq |P : P \cap S|$ για όλες τις $P, S \in Syl_p(G)$ με $P \neq S$.

Απόδειξη. Έστω $P \in Syl_p(G)$. Η P δρα πάνω στο σύνολο $Syl_p(G)$ με συζυγία. Έχουμε δει, στο Θεώρημα 5.3.10, ότι όλες οι τροχιές αυτής της δράσης, εκτός της τροχιάς της P, έχουν τάξη μια θετική δύναμη του p. Έστω $S \neq P$, $S \in Syl_p(G)$. Η τροχιά της S έχει τάξη $|P : N_P(S)|$. Από το Λήμμα 5.3.16 έχουμε ότι $N_P(S) \subseteq S$ και άρα $N_P(S) = P \cap S$. Συνεπώς η τροχιά του S έχει τάξη $|P : P \cap S|$. ⊤

5.3.18 Λήμμα. *Αν μια υποομάδα H της G περιέχει την $N_G(P)$, $P \in Syl_p(G)$, τότε $N_G(H) = H$. Συνεπώς ισχύει $N_G(N_G(P)) = N_G(P)$.*

Απόδειξη. Έστω $g \in N_G(H)$. Επειδή $gHg^{-1} = H$, οι p-υποομάδες του Sylow P και $g^{-1}Pg$ είναι p-υποομάδες του Sylow της H. Από το Θεώρημα 5.3.11, υπάρχει $h \in H$ έτσι ώστε $h^{-1}g^{-1}Pgh = P$. Επομένως $gh \in N_G(P)$ και άρα $gh \in H$ και επειδή $h \in H$ προκύπτει $g \in H$. ⊤

5.3.19 Λήμμα. *Αν μια κανονική υποομάδα H της G περιέχει μια p-υποομάδα του Sylow P, τότε $G = N_G(P)H$.*

Απόδειξη. Οι p-υποομάδες του Sylow της H είναι και p-υποομάδες του Sylow της G. Αν $x \in G$, τότε οι P και $x^{-1}Px$ είναι p-υποομάδες του Sylow της H. Άρα, από το Θεώρημα 5.3.11 έπεται ότι υπάρχει $h \in H$ τέτοιο ώστε $h^{-1}Ph = x^{-1}Px$. Έτσι, έχουμε $xh^{-1}P(xh^{-1})^{-1} = P$, δηλαδή $xh^{-1} \in N_G(P)$. Αυτό σημαίνει ότι $x = nh$ με $h \in H$ και $n \in N(P)$. ⊤

Για να δείξουμε πόσο χρήσιμα είναι τα θεωρήματα του Sylow, μελετούμε τώρα τη δομή ορισμένων ομάδων.

5.3.20 Θεώρημα. *Έστω $|G| = pq$, όπου p, q πρώτοι και $p > q$. Τότε η G έχει μια κανονική p-υποομάδα του Sylow. Αν η G δεν είναι Αβελιανή, τότε $q \mid p-1$ και η G έχει p ακριβώς q-υποομάδες του Sylow. Συνεπώς η G είναι Αβελιανή εκτός αν $q \mid p-1$.*

Απόδειξη. Έστω $r = |Syl_p(G)|$ και $P \in Syl_p(G)$. Από το Πόρισμα 5.3.13, γνωρίζουμε ότι ο r διαιρεί το δείκτη $|G : P| = q$ και άρα $r = 1$ ή q. Από το Θεώρημα 5.3.10, έχουμε ότι $p \mid r-1$ και άρα (καθώς $p > q > 1$) πρέπει $r = 1$. Συνεπώς υπάρχει μόνο μια p-υποομάδα του Sylow, η P, που φυσικά είναι κανονική. Η ομάδα G/P έχει τάξη q και άρα είναι κυκλική. Συνεπώς $[G, G] \subseteq P$. Έστω $s = |Syl_q(G)|$. Τότε, όπως προηγουμένως, πρέπει $s = 1$ ή p. Αν $s = 1$ και Q είναι η q-υποομάδα του Sylow, τότε αυτή είναι κανονική. Όμως η G/Q είναι κυκλική και άρα $[G, G] \subseteq Q$. Συνεπώς $[G, G] \subset P \cap Q = 1$, δηλαδή η G είναι Αβελιανή. Έτσι, αν η G δεν είναι Αβελιανή, θα πρέπει $s = p$ και από το Θεώρημα 5.3.10 έχουμε ότι $q \mid p-1$. ⊤

5.3.21 Παρατήρηση. Μπορεί να δειχτεί ότι για κάθε επιλογή πρώτων αριθμών p και q με $q \mid p-1$ υπάρχει μια μη-Αβελιανή ομάδα τάξης pq, η οποία είναι μοναδική (ως προς ισομορφισμό). Η κατασκευή μιας τέτοιας ομάδας, η οποία μπορεί να γίνει χρησιμοποιώντας την έννοια των ημιευθέων γινομένων, παραλείπεται.

5.3.22 Θεώρημα. *Έστω $|G| = p^2q$, όπου p και q πρώτοι αριθμοί. Τότε η G έχει μια κανονική p-υποομάδα του Sylow ή μια κανονική q-υποομάδα του Sylow.*

Απόδειξη. Αν $|Syl_q(G)| = 1$, τότε η μοναδική q-υποομάδα του Sylow είναι κανονική. Έστω ότι $|Syl_q(G)| > 1$. Γνωρίζουμε ότι $|Syl_q(G)| = |G : N(Q)| = r$, όπου Q είναι μια q-υποομάδα του Sylow. Γνωρίζουμε επίσης ότι ο r διαιρεί το δείκτη $|G : Q| = p^2$. Επειδή $q \mid r-1$, έπεται ότι $q \neq p$ και άρα ο $r = p$ ή p^2.

Έστω ότι $r = p$. Τότε $p \equiv 1 \mod q$ και άρα $p > q$. Άρα $q \not\equiv 1 \mod p$ και έτσι δεν μπορούμε να έχουμε $|Syl_p(G)| = q$. Άρα $|Syl_p(G)| = 1$.

Έστω ότι $r = p^2$. Τότε υπάρχουν $(q-1)p^2$ στοιχεία με τάξη q. Πράγματι, αν $Q_1, Q_2 \in Syl_q(G)$ με $Q_1 \neq Q_2$, τότε $Q_1 \cap Q_2 = 1$, αφού κάθε μια από αυτές έχει τάξη q. Επειδή υπάρχουν p^2 q-υποομάδες του Sylow που η κάθε μια έχει $q-1$ στοιχεία τάξης q, η ομάδα G έχει $(q-1)p^2$ στοιχεία τάξης q. Έστω X το σύνολο των στοιχείων της G που δεν έχουν τάξη q. Τότε $|X| = |G| - (q-1)p^2 = p^2$. Έστω $P \in Syl_p(G)$. Τότε $P \subseteq X$, $|P| = p^2$ και άρα $P = X$. Συνεπώς η P είναι η μοναδική p-υποομάδα του Sylow και άρα αυτή είναι κανονική. ⊤

5.3.23 Θεώρημα. *Έστω $|G| = p^3q$, όπου p, q πρώτοι αριθμοί. Τότε είτε η G έχει μια κανονική p ή q-υποομάδα του Sylow ή $p = 2$, $q = 3$ και $|G| = 24$.*

Απόδειξη. Αν $|Syl_q(G)| = 1$, τότε η μοναδική q-υποομάδα του Sylow είναι κανονική. Έστω ότι $|Syl_q(G)| = r > 1$ και άρα $p \neq q$ και $r = p$ ή p^2 ή p^3. Επίσης μπορούμε να υποθέσουμε ότι $|Syl_p(G)| > 1$ και άρα $|Syl_p(G)| = q$ και $q \equiv 1 \mod p$, αφού ο αριθμός $|Syl_p(G)|$ διαιρεί το δείκτη $|G : P| = q$, όπου P είναι μια p-υποομάδα του Sylow. Συνεπώς $q > p$ και δεν μπορεί να ισχύει $p \equiv 1 \mod q$. Άρα $r = p^2$ ή p^3.

Τώρα έστω $r = p^3$. Μετράμε τα στοιχεία της G που έχουν τάξη q. Όπως και προηγουμένως, αν Q_1, Q_2 είναι δύο q-υποομάδες του Sylow με $Q_1 \neq Q_2$ τότε $Q_1 \cap Q_2 = 1$. Επειδή υπάρχουν p^3 q-υποομάδες του Sylow, όλα τα στοιχεία τάξης q είναι $p^3(q-1)$, αφού κάθε q-υποομάδα του Sylow περιέχει $q-1$ τέτοια στοιχεία. Άρα το σύνολο X όλων των στοιχείων της G που δεν έχουν τάξη q είναι $|X| = |G| - p^3(q-1) = p^3$. Άρα μια p-υποομάδα του Sylow είναι όλο το X, δηλαδή υπάρχει μόνο μια τέτοια υποομάδα που πρέπει να είναι κανονική. Αυτό όμως είναι άτοπο αφού η υπόθεση είναι $|Syl_p(G)| > 1$.

Τέλος, έστω $r = p^2$. Τότε $p^2 \equiv 1 \mod q$, δηλαδή $q \mid p^2 - 1$. Άρα το $q \mid p+1$ ή $q \mid p-1$. Επειδή όμως $q > p$ το $q \nmid p-1$ και άρα $q \mid p+1$. Συνεπώς έχουμε $p < q \leq p+1$. Επομένως πρέπει $q = p+1$. Δηλαδή πρέπει $p = 2$ και $q = 3$ (αφού το 2 και το 3 είναι οι μόνοι διαδοχικοί πρώτοι αριθμοί), δηλαδή $|G| = 24$. ⊤

5.3.24 Παρατήρηση. Το παραπάνω θεώρημα δε μας εξασφαλίζει την ύπαρξη μιας ομάδας τάξης 24, για την οποία καμιά 2- ή 3-υποομάδα του Sylow δεν είναι κανονική. Πράγματι όμως η S_4 δεν έχει καμιά υποομάδα κανονική τάξης 8 ή 3 (γιατί;). Σημειώνουμε εδώ ότι όλες οι ομάδες τάξης $p^\alpha q^\beta$, όπου p, q πρώτοι, δεν είναι απλές, δηλαδή περιέχουν κάποια μη-τετριμμένη γνήσια κανονική υποομάδα εκτός αν $\alpha = 1$ και $\beta = 0$ ή $\alpha = 0$ και $\beta = 1$. Αυτό το αποτέλεσμα είναι ένα από τα βασικά θεωρήματα του Burnside, το οποίο όμως δε θα αποδείξουμε σε αυτό το βιβλίο.

5.3.25 Θεώρημα. *Έστω* $|G| = pqr$, *όπου* $p > q > r$ *πρώτοι αριθμοί. Τότε η* G *έχει μια κανονική υποομάδα τάξης* p. *Αν επιπλέον* $p \not\equiv 1 \mod q$ *τότε η* G *έχει και μια κανονική υποομάδα τάξης* q.

Απόδειξη. Έστω ότι για τον πρώτο p έχουμε περισσότερες από μια υποομάδες του Sylow. Τότε έχουμε $1 + kp$ p-υποομάδες του Sylow με $k \neq 0$. Από το Πόρισμα 5.3.13 προκύπτει ότι $1 + kp \mid pqr$. Άρα $1 + kp \mid qr$ και συνεπώς $1 + kp = qr$. Επομένως υπάρχουν $qr(p-1)$ στοιχεία τάξης p. Αν το πλήθος $1 + \lambda q$ και $1 + tr$ των υποομάδων τάξης q και r αντίστοιχα είναι μεγαλύτερο του 1, τότε $1 + \lambda q = p$, ή pr και $1 + tr \geq q$. Από αυτό προκύπτει ότι υπάρχουν $p(q-1)$ στοιχεία τάξης q και $q(r-1)$ στοιχεία τάξης r. Έτσι έχουμε $|G| \geq qr(p-1) + p(q-1) + q(r-1) + 1 = pqr - qr + pq - p + qr - q + 1 = pqr + (p-1)(q-1) > pqr$ που είναι άτοπο. Συνεπώς ένας από τους αριθμούς $1 + \lambda q$, $1 + tr$ είναι ίσος με 1.

Έστω P, Q, R Sylow υποομάδες τάξης p, q και r αντίστοιχα και S μια από τις υποομάδες Q και R που είναι κανονική. Αν το στοιχείο g είναι γεννήτορας της S, έστω m η τάξη του. Έστω επίσης $P =< h >$. Τότε, $hgh^{-1} = g^i$ και συνεπώς $g = h^p g h^{-p} = g^{i^p}$. Άρα $i^p \equiv 1 \mod m$. Αλλά ο μ.κ.δ.$(p, m-1) = 1$ και $i^{m-1} \equiv 1 \mod m$, άρα $i \equiv 1 \mod m$. Συνεπώς $hgh^{-1} = g$ ή $g^{-1}hg = h$, δηλαδή $g \in N_G(P)$. Αλλά $|N_G(P)| = \dfrac{|G|}{1+kp} = p$ και το g έχει τάξη q ή r που είναι άτοπο. Άρα $1 + kp = 1$, δηλαδή $P \lhd G$. Τώρα έχουμε $|G : PQ| = r$ και σύμφωνα με το Πόρισμα 4.9.7 θα πρέπει $PQ \lhd G$. Αν $p \not\equiv 1 \mod q$ τότε η PQ είναι κυκλική σύμφωνα με το Θεώρημα 5.3.20 και άρα $Q \lhd G$ (γιατί;). ⊤

Τελειώνουμε αυτή την παράγραφο εφαρμόζοντας τα Θεωρήματα του Sylow για να αποδείξουμε ένα θεώρημα το οποίο αναφέρεται στις απλές ομάδες.

5.3.26 Θεώρημα. *Υποθέτουμε ότι* $|G| = p^\alpha m$, *όπου* $\alpha > 0$, $m > 1$ *και* $p \nmid m$. *Αν η* G *είναι απλή, τότε το πλήθος* $r = |Syl_p(G)|$ *ικανοποιεί τις εξής συνθήκες:*

α) Ο r *διαιρεί τον* m.

β) $r \equiv 1 \mod p$.

γ) Η τάξη $|G|$ *της* G *διαιρεί το* $r!$.

Απόδειξη. Τα α) και β) είναι τα Θεωρήματα 5.3.13 και 5.3.10 αντίστοιχα. Για το γ) έστω $P \in Syl_p(G)$. Τότε, από το Πόρισμα 5.3.12 έχουμε $r = |G : N_G(P)|$. Καθώς η G είναι απλή, από το Θεώρημα 4.9.6 συμπεραίνουμε ότι η τάξη $|G|$ διαιρεί το $r!$. ⊤

5.3.27 Παραδείγματα.

1. Έστω G μια ομάδα με τάξη $|G| = 1.000.000 = 2^6 \cdot 5^6$. Τότε η G δεν είναι απλή. Πράγματι, αν η G ήταν απλή θα έπρεπε κάποιος αριθμός $1 + 5k$ να

διαιρούσε τον 2^6. Τέτοιος είναι ο 1 και ο $1+3\cdot 5$ μόνο. Αλλά κανείς από αυτούς δεν είναι τέτοιος ώστε $2^6\cdot 5^6 \mid 1!$ ή $16!$

2. Έστω ότι $|G| = 8000 = 2^6\cdot 5^3$. Τότε η G δεν είναι απλή. Πράγματι, έστω ότι η G ήταν απλή. Για $p=5$ παίρνουμε $r=16$, γιατί αν $r=1$ τότε η συνθήκη γ) του Θεωρήματος 5.3.26 δεν ισχύει. Αλλά $16 \not\equiv 1 \mod 5^2$. Άρα από το Πόρισμα 5.3.17 υπάρχουν $P_1, P_2 \in Syl_5(G)$ με $P_1 \neq P_2$ και $5^2 > |P_1 : P_1\cap P_2|$. Άρα $|P_1 : P_1\cap P_2| = 5$ και επομένως από το Θεώρημα 4.9.6 έπεται ότι $P_1\cap P_2 \lhd P_1$ και όμοια $P_1\cap P_2 \lhd P_2$. Έστω $H = N_G(P_1\cap P_2)$. Επειδή η G είναι απλή και $P_1\cap P_2 > \{e\}$, έχουμε $H \lneq G$. Τώρα έχουμε $P_1 \leq H$ και $P_2 \leq H$. Άρα από το Θεώρημα του Lagrange προκύπτει ότι $P_1, P_2 \in Syl_5(H)$. Άρα $r_H = |Syl_5(H)| > 1$. Επειδή ο r_H διαιρεί τον $|H : P_1|$ θα πρέπει να διαιρεί τον 2^6. Αλλά πρέπει $r_H \equiv 1 \mod 5$ και άρα $r_H = 2^4$. Συνεπώς ο 2^4 διαιρεί την τάξη $|H|$. Άρα ο $2^4\cdot 5^3$ διαιρεί την τάξη $|H|$ της H και συνεπώς $|G : H| \leq 2^2$. Αυτό είναι άτοπο σύμφωνα με το Θεώρημα 4.9.6.

3. Αν ο p είναι ένας πρώτος αριθμός, τότε η συμμετρική ομάδα S_p έχει $(p-2)!$ p-υποομάδες του Sylow. Πράγματι, γνωρίζουμε ότι η κλάση συζυγίας του στοιχείου $\sigma = (1\ 2\ \cdots\ p)$ έχει $(p-1)!$ στοιχεία. Κάθε ένα στοιχείο από αυτά παράγει μια κυκλική ομάδα τάξης p. Επίσης, δεν υπάρχει στοιχείο τάξης p που δεν είναι συζυγές με το σ. (Με άλλα λόγια δύο στοιχεία τάξης p στην S_p είναι πάντα συζυγή).

Συνεπώς, από το Θεώρημα 5.3.10 έπεται ότι $(p-2)! - 1 \equiv 0 \mod p$ και άρα $(p-1)! + 1 \equiv 0 \mod p$. Αυτό είναι το γνωστό Θεώρημα του Wilson της Θεωρίας Αριθμών (βλ. Εφαρμογή 2.4.6 3)).

4. Έστω ότι $|G| = 45 = 5\cdot 3^2$. Τότε η ομάδα G πρέπει να είναι Αβελιανή. Πράγματι, έστω K και H μια 5-υποομάδα και 3-υποομάδα του Sylow αντίστοιχα. Καθώς κανένας αριθμός της μορφής $1+5k$ και $1+3k$ με $k>0$ δεν είναι ένας από τους διαιρέτες $1, 3, 5, 9, 15$ και 45 του 45, συμπεραίνουμε ότι η K και η H είναι κανονικές υποομάδες. Επίσης αυτές είναι Αβελιανές και $G = HK$ αφού $H\cap K = \{e\}$. Τώρα έχουμε $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K$ και $h(kh^{-1}k^{-1}) \in H$ και άρα $hkh^{-1}k^{-1} = 1$ για $h\in H$ και $k\in K$. Συνεπώς, $G = H\times K$.

5. **Η ταξινόμηση των ομάδων τάξης 12:** Έχουμε δει (Θεώρημα 5.3.22) ότι αυτές οι ομάδες έχουν ή μια κανονική υποομάδα τάξης 4 ή μια κανονική υποομάδα τάξης 3. Έχουμε λοιπόν τρεις δυνατές περιπτωσεις:

1η Περίπτωση. Υπάρχει μόνο μια κανονική υποομάδα K_2 τάξης 4 και μόνο μια κανονική υποομάδα K_3 τάξης 3. Σ' αυτή την περίπτωση όμως $K_2\cap K_3 = \{1\}$, καθώς η υποομάδα $K_2\cap K_3$ έχει τάξη που πρέπει να διαιρεί την τάξη της K_2 και της K_3. Άρα $G = K_2K_3$. Αλλά αν $\kappa_2\in K_2$ και $\kappa_3\in K_3$, τότε $\kappa_2(\kappa_3\kappa_2^{-1}\kappa_3^{-1}) =$

$(\kappa_2\kappa_3\kappa_2^{-1})\kappa_3 \in K_2 \cap K_3 = \{1\}$ αφού οι K_2 και K_3 είναι κανονικές. Αυτό σημαίνει ότι η G είναι Αβελιανή.

2η Περίπτωση. Έστω ότι υπάρχει μόνο μια υποομάδα τάξης 4 (που είναι κανονική) και $1+3t$ με $t \neq 0$ υποομάδες τάξης 3. Επειδή το $1+3t$ διαιρεί το 12 πρέπει $t = 1$. Άρα υπάρχουν 4 υποομάδες τάξης 3. Έστω K_2 η μοναδική 2-υποομάδα του Sylow. Αυτή είναι τάξης 4 και συνεπώς είναι ισόμορφη με την κυκλική ομάδα C_4 τάξης 4 ή με την ομάδα του Klein $C_2 \times C_2$. Αν η K_2 ήταν κυκλική έστω $K_2 =< x >$, $x^4 = 1$, τότε $Aut(K_2) \cong C_2$, αφού κάθε αυτομορφισμός της K_2 θα στέλνει το x ή στον εαυτό του ή στο $x^3 = x^{-1}$. Αλλά αν ένα $y \in G$ έχει τάξη 3 (δηλαδή είναι γεννήτορας μιας 3-υποομάδας του Sylow) τότε $y \notin K_2$ και το y ορίζει έναν αυτομορφισμό (μέσω συζυγίας) της K_2. Αυτός ο αυτομορφισμός πρέπει να είναι ο ταυτοτικός, αφού διαφορετικά θα ήταν τάξης 3, ενώ η K_2 δεν έχει τέτοιο αυτομορφισμό. Συνεπώς θα πρέπει $y\,x\,y^{-1} = x$. Άρα το xy έχει τάξη 12 και η G θα ήταν κυκλική. Συνεπώς σ' αυτή την περίπτωση πρέπει $K_2 \cong C_2 \times C_2$. Έστω K_3 μια οποιαδήποτε 3-υποομάδα του Sylow. Αν $\beta \in K_3$, $\beta \neq 1$, επειδή $K_2 \cap K_3 = \{1\}$, έχουμε

$$G = K_2 \cup \beta K_2 \cup \beta^2 K_2, \quad \text{με} \quad G/K_2 \cong C_3.$$

Άρα

$$G = \{1, \alpha, \gamma, \alpha\gamma, \beta, \beta\alpha, \beta\gamma, \beta\alpha\gamma, \beta^2, \beta^2\alpha, \beta^2\gamma, \beta^2\alpha\gamma\}.$$

Καθώς $\beta^{-1}K_2\beta = K_2$ και η G δεν είναι Αβελιανή, υπάρχει ένα $x \in K_2$, με $\beta^{-1}x\beta \neq x$. Θέτουμε $\beta^{-1}x\beta = y \in K_2$. Επειδή δύο οποιαδήποτε στοιχεία της K_2 διάφορα του 1 καθορίζουν πλήρως την K_2, μπορούμε να υποθέσουμε ότι $x = \alpha$ και $y = \gamma$. Έτσι, έχουμε $\beta^{-1}\alpha\beta = \gamma$, δηλαδή $\beta\gamma = \alpha\beta$. Επίσης το $\beta^{-1}\gamma\beta \in K_2$ και άρα το $\beta^{-1}\gamma\beta = \alpha\gamma$. Δηλαδή $\gamma\beta = \beta\alpha\gamma$ και συνεπώς $\alpha\gamma\beta = \beta\alpha$. Συνεπώς αν υπάρχει μια ομάδα G με 12 στοιχεία που έχει τέσσερες 3-υποομάδες του Sylow και μια 2-υποομάδα του Sylow αυτή πρέπει να περιέχει τα στοιχεία $\{1, \alpha, \gamma, \alpha\gamma, \beta, \beta\alpha, \beta\gamma, \beta\alpha\gamma, \beta^2, \beta^2\alpha, \beta^2\gamma, \beta^2\alpha\gamma\}$, τα οποία πολλαπλασιάζονται κάτω από τους περιορισμούς $\alpha^2 = \gamma^2 = \beta^3 = 1$, $\alpha\gamma = \gamma\alpha$, $\alpha\beta = \beta\gamma$, $\gamma\beta = \beta\alpha\gamma$ και $\alpha\gamma\beta = \beta\alpha$.

Μια τέτοια ομάδα πράγματι υπάρχει και είναι η A_4. Τα στοιχεία της A_4 μπορούν να γραφούν:

$i = (1)$, $\alpha = (1\,2)(3\,4)$, $\gamma = (1\,3)(2\,4)$, $\alpha\gamma = (1\,4)(2\,3)$
$\beta = (1\,2\,3)$, $\beta\alpha = (1\,3\,4)$, $\beta\gamma = (2\,4\,3)$, $\beta\alpha\gamma = (1\,4\,2)$
$\beta^2 = (1\,3\,2)$, $\beta^2\alpha = (2\,3\,4)$, $\beta^2\gamma = (1\,2\,4)$, $\beta^2\alpha\gamma = (1\,4\,3)$.

Κλάσεις συζυγίας

$\{(1)\}, \{(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$
$\{(1\,2\,3), (1\,4\,2), (1\,3\,4), (2\,4\,3)\}, \{(1\,3\,2), (1\,2\,4), (1\,4\,3), (2\,3\,4)\}$

Κέντρο της A_4 $Z(A_4) = \{(1)\}$.
Υποομάδα μεταθετών: $A_4' = K_2 = \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$.
Διάγραμμα Υποομάδων

A_4

A_4'

H_1 H_2 H_3 H_4 H_5 H_6 H_7

$Z(A_4) = \{(1)\}$

$H_1 =< \alpha >, H_2 =< \gamma >, H_3 =< \alpha\gamma >, H_4 =< \beta >, H_5 =< \beta\gamma >,$
$H_6 =< \beta\gamma >, H_7 =< \beta\alpha\gamma > .$

3η Περίπτωση. Υποθέτουμε ότι υπάρχει μόνο μια (κανονική) υποομάδα K_3 τάξης 3 και περισσότερες από μια υποομάδες τάξης 4. Επειδή το πλήθος των υποομάδων τάξης 4 είναι $1 + 2k$, $k \neq 0$, το k πρέπει να είναι ίσο με 1. Έστω K_2 μια οποιαδήποτε από αυτές.

Έστω ότι $K_2 =< \alpha >$, $\alpha^4 = 1$. Καθώς $K_2 \cap K_3 = \{1\}$, πρέπει $\alpha^i \notin K_3$, $i = 1, 2, 3$. Επειδή $| G/K_3 | = 4$ έχουμε ότι $G = K_3 \cup \alpha K_3 \cup \alpha^2 K_3 \cup \alpha^3 K_3$. Άρα $G = \{1, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2, \alpha^2, \alpha^2\beta, \alpha^2\beta^2, \alpha^3, \alpha^3\beta, \alpha^3\beta^2\}$, όπου $K_3 =< \beta >$. Θεωρούμε το $\beta\alpha$. Έχουμε $\beta\alpha \in K_3\alpha = \alpha K_3$. Άρα $\beta\alpha \in \{\alpha, \alpha\beta, \alpha\beta^2\}$ και άρα $\beta\alpha = \alpha\beta^2$ (οι σχέσεις $\beta\alpha = \alpha$ και $\beta\alpha = \alpha\beta$ δεν μπορούν να ισχύουν). Άρα ο πίνακας πολλαπλασιασμού θα υπόκειται στις σχέσεις $\alpha^4 = \beta^3$ και $\beta\alpha = \alpha\beta^2$. Αν θεωρήσουμε τους πίνακες

$$A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \text{ και } B = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$$

με $i^2 = -1$ και $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ τότε εύκολα μπορούμε να διαπιστώσουμε ότι η ομάδα που παράγεται από τους πίνακες A και B είναι ένα παράδειγμα μιας τέτοιας ομάδας.

Κλάσεις συζυγίας

$\{1\}, \{\alpha^2\}, \{\beta, \beta^2\}, \{\alpha^2\beta, \alpha^2\beta^2\}, \{\alpha, \alpha\beta, \alpha\beta^2\}, \{\alpha^3, \alpha^3\beta, \alpha^3\beta^2\}$.

Κέντρο της G: $Z(G) = \{1, \alpha^2\}$.

Υποομάδα μεταθετών: $G' = K_3$, αφού $|G/K_3| = 4$, $K_3 \supset G'$ άρα $|G'| = 3$.

Υπάρχουν τρεις κυκλικές υποομάδες τάξης 4, $K_2' =< \alpha >$, $K_2^2 =< \alpha\beta >$, $K_2^3 =< \alpha\beta^2 >$.

Κάθε υποομάδα τάξης 6 είναι κανονική (δείκτου 2). Άρα είναι η ένωση συζυγών κλάσεων και κανένα στοιχείο τάξης 4 δεν ανήκει σε μια τέτοια. Άρα υπάρχει μόνο μια, η $<\alpha^2\beta>$.

Διάγραμμα Υποομάδων

$$G$$

$$< \alpha > \qquad < \alpha\beta > \qquad\qquad < \alpha\beta^2 > \qquad < \alpha^2\beta >$$

$$Z(G) \qquad\qquad G'$$

$$\{1\}$$

Τώρα υποθέτουμε ότι η K_2 είναι ισόμορφη με την $C_2 \times C_2$, δηλαδή ότι

$$K_2 =< \alpha, \gamma \mid \alpha^2 = \gamma^2 = (\alpha\gamma)^2 = 1 >= \{1, \alpha, \gamma, \alpha\gamma\}.$$

Όπως πριν, $K_3 =< \beta >$ και $K_2 \cap K_3 = \{1\}$. Εύκολα προκύπτει ότι $G = K_3 \cup \alpha K_3 \cup \gamma K_3 \cup \alpha\gamma K_3$. Άρα $G = \{1, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2, \gamma, \gamma\beta, \gamma\beta^2, \alpha\gamma, \alpha\gamma\beta, \alpha\gamma\beta^2\}$. Επειδή $K_3 \lhd G$, για κάθε $x \in K_2$ έχουμε $x^{-1}\beta x \in K_3$. Η περίπτωση $x^{-1}\beta x = \beta$ δεν μπορεί να ισχύει γιατί η G θα ήταν Αβελιανή. Άρα για κάποιο $x \in K_2$ πρέπει $x^{-1}\beta x \neq \beta$. Μπορούμε να υποθέσουμε ότι $\alpha^{-1}\beta\alpha \neq \beta$. Άρα $\alpha^{-1}\beta\alpha = \beta^2$.

Συνεπώς $\beta\alpha = \alpha\beta^2$. Εύκολα επίσης προκύπτει ότι $\gamma^{-1}\beta\gamma = \beta$ ή β^2. Αν είναι β τότε $(\alpha\gamma)^{-1}\beta\alpha\gamma = \beta^2$ και αντίστροφα. Όποιο και αν ισχύει παίρνουμε ισόμορφες ομάδες G. Έστω λοιπόν ότι $\gamma^{-1}\beta\gamma = \beta$ και $(\alpha\gamma)^{-1}\beta\alpha\gamma = \beta^2$. Έτσι έχουμε ότι

$$G = \{1, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2, \gamma, \gamma\beta, \gamma\beta^2, \alpha\gamma, \alpha\gamma\beta, \alpha\gamma\beta\}$$

με τον πολλαπλασιασμό να υπόκειται στις σχέσεις $\alpha^2 = \gamma^2 = 1$, $\beta^3 = 1$, $\alpha\gamma = \gamma\alpha$, $\beta\gamma = \gamma\beta$ και $\beta\alpha = \alpha\beta^2$. Μια τέτοια ομάδα είναι η διεδρική D_6.

5.3.28 Παρατήρηση. Το πρόβλημα της ταξινόμησης των μη-ισόμορφων μη-Αβελιανών ομάδων τάξης μεγαλύτερης του 15 γίνεται αρκετά πιο δύσκολο και αυτό μπορεί να φανεί από τον πιο κάτω πίνακα στον οποίο δίνουμε το πλήθος των ομάδων τάξης μικρότερης ή ίσης του 100. (Βλέπε A.D. Thomas and G.V. Wood [29]).

Τ	Π	Τ	Π	Τ	Π	Τ	Π	Τ	Π
1	0	21	1	41	0	61	0	81	10
2	0	22	1	42	5	62	1	82	1
3	0	23	0	43	0	63	2	83	0
4	0	24	12	44	2	64	256	84	13
5	0	25	0	45	0	65	0	85	0
6	1	26	1	46	1	66	3	86	1
7	0	27	2	47	0	67	0	87	0
8	2	28	2	48	47	68	3	88	9
9	0	29	0	49	0	69	0	89	0
10	1	30	3	50	3	70	3	90	8
11	0	31	0	51	0	71	0	91	0
12	3	32	44	52	3	72	44	92	2
13	0	33	0	53	0	73	0	93	1
14	1	34	1	54	12	74	1	94	1
15	0	35	0	55	1	75	1	95	0
16	9	36	10	56	10	76	0	96	223
17	0	37	0	57	1	77	0	97	0
18	3	38	1	58	2	78	5	98	3
19	0	39	1	59	0	79	0	99	0
20	3	40	11	60	11	80	47	100	10

Εδώ Τ είναι η τάξη μιας ομάδας και Π το πλήθος των μη-ισόμορφων μη-Αβελιανών ομάδων με τάξη Τ.

Σημειώνουμε ότι μεταξύ των ομάδων τάξης μικρότερης ή ίσης του 1000 υπάρχουν μόνο 5 απλές μη Αβελιανές ομάδες που η τάξη τους είναι 60, 168,

360, 504 και 600 και οι δύο από αυτές είναι η A_5 και η A_6. Για τις ομάδες τάξης 2^n, $n \leq 6$, βλέπε M. Hall και J.K. Senior [12]. Πρόσφατα έχει βρεθεί το πλήθος των ομάδων τάξης μικρότερης ή ίσης του 2000.

Ασκήσεις 5.3

1. Έστω ότι μια πεπερασμένη ομάδα G έχει n το πλήθος p-υποομάδες του Sylow $P_1, P_2, \ldots, P_n$. Να δειχθεί ότι υπάρχει ένας ομομορφισμός

   $$\phi : G \longrightarrow S_n$$

   όπου S_n είναι η συμμετρική ομάδα βαθμού n.

   Να βρεθεί ο πυρήνας $\ker \phi$ συναρτήσει των κανονικοποιουσών υποομάδων $N_G(P_i)$ των P_i:

   α) Γενικά

   β) Αν μια από τις Sylow p-υποομάδες είναι κανονική στην G.

   γ) Αν $G = A_4$ και $p = 3$.

2. Δείξτε ότι το κέντρο $Z(G)$ μιας μη-Αβελιανής ομάδας τάξης p^3, όπου p πρώτος, συμπίπτει με την υποομάδα $[G, G]$ των μεταθετών και έχει τάξη p.

3. Δείξτε ότι υπάρχει μόνο μια ομάδα τάξης 33.

4. Δείξτε ότι μια ομάδα τάξης 30 δεν είναι απλή.

5. Δείξτε ότι αν $|G| = 56$ τότε η G δεν είναι απλή. Όμοια, μια ομάδα τάξης 312 δεν είναι απλή.

6. Να βρεθούν οι Sylow p-υποομάδες της $GL_2(\mathbb{Z}_p)$ και γενικά της $GL_n(\mathbb{Z}_p)$.

7. Πόσα στοιχεία τάξης 7 υπάρχουν σε μια απλή ομάδα τάξης 168;

8. Έστω G μια πεπερασμένη μη Αβελιανή $p-$ομάδα. Δείξτε ότι η τάξη της ομάδας $G/[G, G]$ είναι μεγαλύτερη ή ίση του p^2.

9. Να κατασκευάσετε μια μη Αβελιανή ομάδα τάξης 39 .

5.4 Η Απαρίθμηση των Τροχιών

Μια βασική μέθοδος της Συνδυαστικής είναι να απαριθμήσουμε τα στοιχεία ενός πεπερασμένου συνόλου με δύο διαφορετικούς τρόπους και μετά να εξισώσουμε τα αποτελέσματα που βρίσκουμε. Ακριβέστερα, έστω $\mathcal{U}$ και V δύο πεπερασμένα σύνολα και $S \subseteq \mathcal{U} \times V$. Ορίζουμε

$$S(\alpha, \cdot) = \{\, (u, v) \in S \mid u = \alpha \,\}$$
$$S(\cdot, \beta) = \{\, (u, v) \in S \mid v = \beta \,\}.$$

Τότε έχουμε τις ξένες ενώσεις

$$S = \dot{\bigcup_{\alpha \in \mathcal{U}}} S(\alpha, \cdot) = \dot{\bigcup_{\beta \in V}} S(\cdot, \beta)$$

οπότε

$$|S| = \sum_{\alpha \in \mathcal{U}} |S(\alpha, \cdot)| = \sum_{\beta \in V} |S(\cdot, \beta)| \,.$$

Σε πολλές περιπτώσεις συμβαίνει να έχουμε $|S(\alpha, \cdot)| = r$ για κάθε $\alpha \in \mathcal{U}$ και $|S(\cdot, \beta)| = s$, για κάθε $\beta \in V$, οπότε παίρνουμε σαν αποτέλεσμα

$$r \ |\mathcal{U}| = s \ |V| \,.$$

Εδώ θα εφαρμόσουμε αυτή τη μέθοδο για να απαριθμήσουμε το πλήθος των τροχιών ενός πεπερασμένου συνόλου X κάτω από τη δράση μιας πεπερασμένης ομάδας. Το επόμενο αποτέλεσμα οφείλεται στους Cauchy και Frobenius αλλά έχει επικρατήσει να ονομάζεται Λήμμα του Burnside. Ο τελευταίος το χρησιμοποίησε σε προβλήματα της θεωρίας ομάδων.

5.4.1 Θεώρημα. *Έστω N το πλήθος των τροχιών της δράσης της ομάδας G πάνω στο X. Τότε*

$$N = \frac{1}{|G|} \sum_{g \in G} |F(g)|$$

όπου $F(g) = \{\, x \in X \mid g \cdot x = x \,\}$.

Απόδειξη. Θεωρούμε το υποσύνολο

$$S = \{\, (g, x) \in G \times X \mid g \cdot x = x, \ g \in G, x \in X \,\}$$

του $G \times X$. Τότε έχουμε $|S(g, \cdot)| = |F(g)|$ και $|S(\cdot, x)| = |G_x|$ και άρα

$$|S| = \sum_{g \in G} |F(g)| = \sum_{x \in X} |G_x| \,.$$

Αν $x_1, x_2, \ldots, x_N \in X$ αντιπροσωπεύουν τις N τροχιές, τότε

$$\sum_{g\in G} |F(g)| = \sum_{i=1}^{N} \sum_{x\in T_{x_i}} |G_x| .$$

Αλλά αν $x \in T_{x_i}$, έστω $g \cdot x_i = x$, τότε για $g' \in G_x$ έχουμε $(g'g)\cdot x_i = x$. Οπότε $g^{-1}\cdot((g'g)\cdot x_i) = x_i$. Άρα $g^{-1}g'g \in G_{x_i}$ που σημαίνει ότι $g' \in gG_{x_i}g^{-1}$, για κάθε $g' \in G_x$, δηλαδή $G_x \subseteq gG_{x_i}g^{-1}$. Με τον ίδιο τρόπο προκύπτει ότι $gG_{x_i}g^{-1} \subseteq G_x$ και άρα $G_x = gG_{x_i}g^{-1}$. Συνεπώς για κάθε $x \in T_{x_i}$ έχουμε $|G_x| = |gG_{x_i}g^{-1}| = |G_{x_i}|$ και άρα

$$|F(g)| = \sum_{i=1}^{N} |T_{x_i}| \cdot |G_{x_i}| = \sum_{i=1}^{N} |G| = N\,|G| ,$$

δηλαδή

$$N = \frac{1}{|G|} \sum |F(g)| \cdot \mathsf{T}$$

5.4.2 Παρατήρηση. Ένας κατάλληλος τρόπος για να κατανοήσουμε την ισότητα $\sum_{g\in G} |F(g)| = \sum_{x\in X} |G_x|$ είναι ο εξής. Θεωρούμε ένα πίνακα με $|G|$ γραμμές και $|X|$ στήλες. Σε κάθε γραμμή αντιστοιχούμε ένα στοιχείο g της G και σε κάθε στήλη ένα στοιχείο x του X. Τα στοιχεία του X τα τοποθετούμε κατά μήκος στην επάνω γραμμή του πίνακα και αυτά της G τα τοποθετούμε στην αριστερή κάθετη στήλη του πίνακα. Το στοιχείο του πίνακα που αντιστοιχεί στην (g, x) θέση είναι 1 ή 0 αν $g \in G_x$ (ή ισοδύναμα αν $x \in F(g)$) ή $g \notin G_x$ αντίστοιχα. Αν προσθέσουμε τις μονάδες σε κάθε γραμμή τότε το άθροισμα των αριθμών που θα βρούμε είναι ακριβώς το $\sum\limits_{g\in G} |F(g)|$. Κάνοντας το ίδιο για τις στήλες παίρνουμε το αντίστοιχο άθροισμα $\sum\limits_{x\in X} |G_x|$ που είναι ίσο με το προηγούμενο άθροισμα.

Για παράδειγμα, έχουμε τον παρακάτω πίνακα για την περίπτωση της ομάδας S_3, η οποία δρα στο σύνολο $X = \{1, 2, 3\}$:

	1	2	3	
i	1	1	1	3
(12)	0	0	1	1
(13)	0	1	0	1
(23)	1	0	0	1
(123)	0	0	0	0
(132)	0	0	0	0
	2	2	2	6

$= \sum |G_x| = \sum |F(g)|$

Στο προηγούμενο θεώρημα ο τύπος που μας δίνει το πλήθος N των τροχιών μπορεί να βελτιωθεί από την παρατήρηση ότι αν g_1 και g_2 είναι δύο συζυγή στοιχεία της G τότε $|F(g_1)| = |F(g_2)|$. Έτσι έχουμε

$$N = \frac{1}{|G|} \sum_{i=1}^{s} k_i \, |F(g_i)|$$

όπου $\{g_1, g_2, \ldots, g_s\}$ είναι ένα πλήρες σύστημα αντιπροσώπων των κλάσεων συζυγίας της G και $|C\ell(g_i)| = k_i$.

5.4.3 Παραδείγματα.

1. Θεωρούμε ένα ισόπλευρο τρίγωνο με κορυφές 1, 2, 3. Ας βρούμε το πλήθος N όλων των δυνατών τρόπων τοποθέτησης των πέντε γραμμάτων του συνόλου $S = \{\, \text{A}, \text{B}, \Gamma, \Delta, \text{E} \,\}$ στις κορυφές 1, 2, 3 του τριγώνου έτσι ώστε τουλάχιστον δύο γράμματα σε κάθε κορυφή να είναι διαφορετικά.

   Θεωρούμε την ομάδα συμμετρίας S_3 του τριγώνου να δρα πάνω στο σύνολο X όλων των τριάδων (α, β, γ) όπου $\alpha, \beta, \gamma \in S$ και δύο τουλάχιστον από αυτά είναι διακεκριμένα. Το πλήθος των στοιχείων του X είναι $\dfrac{10!}{3!7!} = 120$ (γιατί;). Επίσης η S_3 έχει τις κλάσεις $C\ell(i) = \{\, i \,\}$, $C\ell((12)) = \{\, (12), (13), (23) \,\}$ και $C\ell((123)) = \{(123), (132)\,\}$. Είναι φανερό ότι είναι $|F(i)| = 120$, $|F((12))| = 20$ (αφού η (12) αφήνει σταθερά όλα τα στοιχεία (α, α, β)) και $|F(123)| = 0$. Άρα $N = \frac{1}{6}(120 + 60 + 0) = 30$.

2. Έστω G μια πεπερασμένη ομάδα που δρα πάνω σε ένα πεπερασμένο σύνολο X. Αν t είναι ένας θετικός ακέραιος, θεωρούμε το σύνολο $X_t = \{1, 2, \ldots, t\}$ και έστω F το σύνολο των απεικονίσεων $f : X \longrightarrow X_t$. Τότε η G δρα πάνω στο F με

   $$(gf)(x) = f(g^{-1} \cdot x), \;\; g \in G, \;\; f \in F, \;\; x \in X.$$

   Από το θεώρημα του Burnside (Θεώρημα 5.4.1), έπεται ότι το πλήθος των τροχιών αυτής της δράσης είναι ο ακέραιος αριθμός

   $$\frac{1}{|G|} \sum_{g \in G} |F(g)|$$

   όπου $F(g) = \{\, f \in F \mid g \cdot f = f \,\}$. Αλλά $g \cdot f = f$ σημαίνει ότι $f(g^{-1} \cdot x) = f(x)$, για κάθε $x \in X$. Δηλαδή $f(g^k \cdot x) = f(x)$, για κάθε $x \in X$ και κάθε $k \in \mathbb{Z}$. Με άλλα λόγια, $f \in F(g)$ αν και μόνον αν η f είναι σταθερή

απεικόνιση επί των τροχιών της κυκλικής ομάδας $< g >$ πάνω στο X. Συνεπώς το πλήθος $\mid F(g) \mid$ είναι ίσο με το πλήθος των απεικονίσεων $f : X \longrightarrow X_t$ που είναι σταθερές στις τροχιές της $\langle g \rangle$ πάνω στο X. Αυτό το πλήθος των απεικονίσεων είναι $t^{\alpha(g)}$ όπου $\alpha(g)$ είναι το πλήθος των τροχιών της $\langle g \rangle$ πάνω στο X. Αυτό μας λέει ότι ο αριθμός

$$\frac{1}{|G|}\sum t^{\alpha(g)}$$

είναι ακέραιος για κάθε θετικό ακέραιο αριθμό t.

Για παράδειγμα, ας θεωρήσουμε μια κυκλική ομάδα G τάξης p, όπου p πρώτος αριθμός. Θεωρούμε επίσης τη δράση της G στο σύνολο $X = G$, η οποία ορίζεται από τον πολλαπλασιασμό της G. Τότε, για κάθε ακέραιο t ο αριθμός

$$\frac{1}{|G|}\sum_{g\in G} t^{\alpha(g)} = \frac{1}{p}\sum_{k=0}^{p-1} t^{\alpha(g^k)} = \frac{1}{p}(t^p + (p-1)t) = \frac{1}{p}(t^p - t + pt)$$

είναι επίσης ακέραιος και άρα $\dfrac{1}{p}(t^p - t) \in \mathbb{Z}$. Αυτό είναι το μικρό Θεώρημα του Fermat.

Ασκήσεις 5.4

1. Έστω V ένας διανυσματικός χώρος διάστασης n επί του σώματος $\mathbb{Z}_p$ και G μια υποομάδα της $GL_n(\mathbb{Z}_p)$ που έχει τάξη μια δύναμη του p. Δείξτε ότι υπάρχει ένα μη μηδενικό διάνυσμα u του V τέτοιο ώστε $g\,u = u$, για κάθε $g \in G$.

2. Αν G είναι μια πεπερασμένη ομάδα και $k(G)$ το πλήθος των κλάσεων συζυγίας της, δείξτε ότι

$$k(G) = \frac{1}{|G|}\sum_{g\in G} |C_G(g)| \ .$$

3. Έστω G πεπερασμένη ομάδα και p ο μικρότερος πρώτος διαιρέτης της τάξης της $|G|$. Αν $k(G) \geq |G|/p$, τότε $Z(G) \neq 1$.

4. Αν G είναι μια μη Αβελιανή πεπερασμένη ομάδα, τότε $k(G) > |Z(G)| + 1$.

5. Δείξτε ότι αν η τάξη μιας μη-Αβελιανής ομάδας G είναι p^3 για κάποιον πρώτο αριθμό p, τότε $k(G) = p^2 + p - 1$.

Παραρτήματα

6.1 Σχέσεις Ισοδυναμίας

Ορισμός *Έστω X ένα μη κενό σύνολο. Μία* ***σχέση*** *στο σύνολο X είναι ένα μη κενό υποσύνολο του $X \times X$.*

Αν $R \subseteq X \times X$ είναι μία σχέση θα χρησιμοποιούμε τον συμβολισμό $x\,R\,y$ για να δηλώσουμε ότι το ζεύγος (x, y) ανήκει στο R και διαβάζουμε: *"Το x σχετίζεται με το y μέσω της σχέσης R".*

Μια σχέση σε ένα σύνολο X λέγεται σχέση ***ισοδυναμίας*** και συμβολίζεται (συνηθώς) με $\sim$ αν ικανοποιεί τις ακόλουθες ιδιότητες:

α) Είναι ***αυτοπαθής***, δηλαδή $x \sim x$ για κάθε $x \in X$.

β) Είναι ***συμμετρική***, δηλαδή αν για $x, y \in X$ ισχύει $x \sim y$, τότε $y \sim x$.

γ) Είναι ***μεταβατική***, δηλαδή αν για $x, y, z \in X$ ισχύει $x \sim y$ και $y \sim z$, τότε $x \sim z$.

Παραδείγματα

1. Έστω X το σύνολο όλου του πληθυσμού της γης. Στο σύνολο αυτό ορίζεται μια σχέση ως εξής $x \sim y$ αν και μόνο αν ο x και ο y έχουν γεννηθεί κατά τη διάρκεια του ιδίου έτους.

2. Έστω X το σύνολο όλων των σημείων ενός επιπέδου. Στο σύνολο αυτό ορίζεται μια σχέση ως εξής $x \sim y$ αν και μόνο αν το σημείο x και το σημείο y ισαπέχουν από την αρχή των αξόνων.

3. Έστω $\varphi : X \longrightarrow Y$ μια απεικόνιση που είναι επί. Στο σύνολο X ορίζεται μια σχέση ως εξής $x_1 \sim x_2$ αν και μόνο αν $\varphi(x_1) = \varphi(x_2)$.

Δεν είναι δύσκολο να επαληθεύσουμε ότι οι σχέσεις, που έχουν ορισθεί στα προηγούμενα παραδείγματα, είναι σχέσεις ισοδυναμίας.

Ορισμός *Έστω $\sim$ μια σχέση ισοδυναμίας σε ένα σύνολο X. Για κάθε $x \in X$ ορίζεται το σύνολο $\{\, y \in X \mid x \sim y \,\}$, το οποίο ονομάζεται* ***κλάση ισοδυναμίας*** *του x. Μια κλάση ισοδυναμίας (συνήθως) συμβολίζεται με $[x]$ (ή C_x) και το x ονομάζεται* ***αντιπρόσωπος*** *της κλάσης $[x]$.*

Όπως εύκολα μπορούμε να επαληθεύσουμε, για τις κλάσεις ισοδυναμίας ισχύουν οι εξής ιδιότητες.

α) Κάθε κλάση ισοδυναμίας είναι ένα μη κενό υποσύνολο του X.
Πράγματι, για κάθε $x \in X$ έχουμε $x \in [x]$, αφού $x \sim x$.

β) Το σύνολο X είναι ίσο με την ένωση των κλάσεων ισοδύναμίας του, αφού για κάθε $x \in X$ υπάρχει η κλάση ισοδυναμίας $[x]$ έτσι ώστε $x \in [x]$.

γ) Για δύο στοιχεία $x, y \in X$ ισχύει $x \sim y$ αν και μόνο αν $[x] = [y]$.

Η τελευταία ιδιότητα είναι ισοδύναμη με την

γ') Δύο κλάσεις ισοδυναμίας είτε ταυτίζονται ή είναι ξένες μεταξύ τους. Πράγματι, αν $y \in [x] \cap [z]$, τότε $x \sim y$ και $z \sim y$, οπότε από τη συμμετρική και τη μεταβατική ιδιότητα έχουμε $x \sim z$. Από από την γ) έχουμε τότε $[x] = [z]$.

Από την τελευταία ιδιότητα έχουμε ότι το σύνολο X είναι η διακεκριμένη (ξένη) ένωση των κλάσεων ισοδυναμίας του. Αν από κάθε κλάση ισοδυναμίας πάρουμε έναν αντιπρόσωπο, τότε σχηματίζουμε ένα σύνολο, έστω T, ***αντιπροσώπων***. Οπότε, από τα προηγούμενα έχουμε ότι $X = \dot{\bigcup}_{x \in T}[x]$.

Το σύνολο όλων των κλάσεων ισοδυναμίας ενός συνόλου X λέγεται ***σύνολο πηλίκο*** και συμβολίζεται $X/\sim$. Η αντιστοιχία $\pi : X \longrightarrow X/\sim$ με $\pi(x) = [x]$ προφανώς ορίζει μια απεικόνιση, η οποία είναι επί. Η απεικόνιση αυτή ονομάζεται ***"φυσική"*** απεικόνιση από το X στο $X/\sim$.

Όπως είδαμε, μια σχέση ισοδυναμίας σε ένα σύνολο ***διαμερίζει*** το σύνολο σε κλάσεις ισοδυναμίας οι οποίες ικανοποιούν τις παραπάνω ιδιότητες α)–γ). Θα δούμε ότι ισχύει και το αντίστροφο. Μια ***διαμέριση*** ενός συνόλου X είναι μια οικογένεια μη κενών υποσυνόλων του, ανά δύο ξένων μεταξύ τους, των οποίων η ένωση είναι όλο το σύνολο X.

Έστω $(A_i),\ i \in I$ μια διαμέριση ενός συνόλου X. Στο σύνολο X ορίζουμε μία σχέση $\sim$ ως εξής $x \sim y$ αν και μόνο αν υπάρχει $i \in I$ έτσι ώστε $x, y \in A_i$.

Προφανώς $x \sim x$ και αν $x \sim y$, τότε $y \sim x$. Επίσης αν $x \sim y$ και $y \sim z$, δηλαδή υπάρχουν $i, j \in I$ έτσι ώστε $x, y \in A_i$ και $y, z \in A_j$, τότε $y \in A_i \cap A_j$ και επειδή το (A_i), $i \in I$ αποτελεί διαμέριση του X, έχουμε $i = j$, δηλαδή $x \sim z$. Δηλαδή η σχέση $\sim$ είναι σχέση ισοδυναμίας. Επιπλέον ισχύει $[x] = A_i$ (γιατί ;). Επομένως αποδείξαμε ότι μια διαμέριση ορίζει μια σχέση ισοδυναμίας, της οποίας οι κλάσεις ισοδυναμίας είναι τα μέλη της διαμέρισης.

Δεν είναι δύσκολο να δούμε ότι ξεκινώντας από μια σχέση ισοδυναμίας σε ένα σύνολο λαμβάνουμε μια διαμέρισή του, η οποία με τη σειρά της ορίζει την αρχική σχέση ισοδυναμίας. Όπως επίσης ξεκινώντας από μια διαμέριση ενός συνόλου λαμβάνουμε μια σχέση ισοδυναμίας, η οποία με τη σειρά της ορίζει την αρχική διαμέριση.

Στο παράδειγμα 3 είχαμε θεωρήσει μια απεικόνιση $\varphi : X \longrightarrow Y$ που ήταν επί και στο σύνολο X είχαμε ορίσει μια σχέση ισοδυναμίας $x_1 \sim x_2$ αν και μόνο αν $\varphi(x_1) = \varphi(x_2)$. Παρατηρούμε ότι οι αντίστροφες εικόνες $\varphi^{-1}(y)$ των στοιχείων του συνόλου Y είναι οι κλάσεις ισοδυναμίας. Δηλαδή το σύνολο πηλίκο είναι το $X/\sim = \{\, \varphi^{-1}(y) \mid y \in Y \,\}$. Η αντιστοιχία $\bar{\varphi} : X/\sim \longrightarrow Y$ με $\bar{\varphi}(\varphi^{-1}(y)) = y$ ορίζει μια 1 - 1 και επί απεικόνιση μεταξύ του συνόλου πηλίκο $X/\sim$ και του συνόλου Y. Επιπλέον, η $\bar{\varphi}$ είναι η μοναδική απεικόνιση με $\bar{\varphi} \circ \pi = \varphi$.

Συνεπώς, με την έννοια που περιγράψαμε παραπάνω, υπάρχει μια ένα προς ένα αντιστοιχία μεταξύ των σχέσεων ισοδυναμίας που ορίζονται σε ένα σύνολο X, των διαμερίσεων τις οποίες δέχεται το X και των απεικονίσεων από το X επί ενός (τυχαίου) συνόλου Y.

6.2 Γενικευμένη Προσεταιριστική Ιδιότητα

Ορισμός *Έστω A, B δύο μη κενά σύνολα. Μία* **αντιστοιχία** *από το A στο B είναι ένα μη κενό υποσύνολο του $A \times B$.*

Αν $X \subseteq A \times B$ είναι μία αντιστοιχία θα χρησιμοποιούμε τον συμβολισμό $a \overset{X}{\mapsto} b$ για να δηλώσουμε ότι το ζεύγος (a, b) ανήκει στο X. Αν δεν υπάρχει περίπτωση σύγχυσης, θα γράφουμε $a \mapsto b$ στη θέση του $a \overset{X}{\mapsto} b$.

Ορισμός *Έστω A, B δύο μη κενά σύνολα. Μια αντιστοιχία X από το A στο B θα λέγεται* **απεικόνιση** *(ή συνάρτηση) αν για κάθε $a \in A$ υπάρχει μοναδικό $b \in B$ τέτοιο ώστε $a \mapsto b$.*

Παραδείγματα

1) Έστω $A = \{a, b, c\}$ και $B = \{1, 2\}$. Τα παρακάτω σύνολα είναι αντιστοιχίες από το A στο B

$$X = \{(a, 1), (a, 2), (b, 2), (c, 2)\}$$
$$Y = \{(b, 1), (c, 1)\}$$
$$Z = \{(a, 1), (b, 1), (c, 2)\}$$

Η αντιστοιχία X δεν είναι απεικόνιση από το A στο B γιατί για το στοιχείο $a \in A$ έχουμε δύο ζεύγη $(a, 1), (a, 2) \in X$ δηλαδή $a \overset{X}{\mapsto} 1$, $a \overset{X}{\mapsto} 2$. Η αντιστοιχία Y δεν είναι απεικόνιση από το A στο B αφού δεν υπάρχει ζεύγος της μορφής (a, i) που να ανήκει στο Y. Δηλαδή δεν υπάρχει i τέτοιο ώστε $a \overset{Y}{\mapsto} i$. Η αντιστοιχία Z είναι μια απεικόνιση από το A στο B.

2) Το σύνολο $X = \{(x^2, x) \in \mathbb{R}_{\geq 0} \times \mathbb{R} | x \in \mathbb{R}\}$ είναι μία αντιστοιχία από το σύνολο $\mathbb{R}_{\geq 0}$ των μη αρνητικών πραγματικών αριθμών στο σύνολο $\mathbb{R}$ των πραγματικών αριθμών. Η αντιστοιχία αυτή δεν είναι απεικόνιση αφού, για παράδειγμα, $1 \mapsto 1$ και $1 \mapsto -1$.

Μια αντιστοιχία X από το A στο B θα συμβολίζεται συχνά με $X : A \to B$.

Ορισμός *Μια* **πράξη** *σε ένα μη κενό σύνολο A είναι μια απεικόνιση από το $A \times A$ στο A.*

Συνεπώς, αν $X : A \times A \to A$ είναι μία πράξη στο A, τότε **για κάθε** ζεύγος $(a, b) \in A \times A$ υπάρχει **μοναδικό** $c \in A$ τέτοιο ώστε $(a, b) \mapsto c$.

Ορισμός *Ένα* **αλγεβρικό σύστημα** *είναι ένα μη κενό σύνολο εφοδιασμένο με μία ή περισσότερες πράξεις.*

Έστω $A \times A \to A$, $(a,b) \mapsto ab$ μία πράξη στο σύνολο A τέτοια ώστε $(ab)c = a(bc)$ για κάθε $a,b,c \in A$. Μια τέτοια πράξη ονομάζεται ***προσεταιριστική***. Έστω $a_1, a_2, \ldots, a_n$ μια διατεταγμένη n-άδα στοιχείων του A. Κάθε στοιχείο του A που μπορεί να σχηματιστεί από τα $a_1, \ldots, a_n$ (με τη συγκεκριμένη σειρά) με την παρεμβολή παρενθέσεων θα λέμε ότι **αντιστοιχεί** στη διατεταγμένη n-άδα $a_1, \ldots, a_n$. Για παράδειγμα, αν $n = 4$ τότε στην τετράδα a_1, a_2, a_3, a_4 αντιστοιχούν τα εξής στοιχεία

$$a_1(a_2(a_3a_4)),\ (a_1a_2)(a_3a_4),\ ((a_1a_2)a_3)a_4,\ a_1((a_2a_3)a_4),\ (a_1(a_2a_3))a_4.$$

Θα δείξουμε ότι όλα τα στοιχεία που αντιστοιχούν στη διατεταγμένη n-άδα $a_1, \ldots, a_n$ είναι ίσα.

Λήμμα *Έστω A ένα σύνολο και $A \times A \to A$, $(a,b) \mapsto ab$, μια προσεταιριστική πράξη. Αν $a_1, \ldots, a_n$ είναι στοιχεία του A, ορίζουμε το στοιχείο $\prod_{i=1}^{n} a_i \in A$ με επαγωγή στο πλήθος n των παραγόντων, ως εξής: Για $n = 1$ είναι $\prod_{i=1}^{n} a_i = a_1$, ενώ για $n \geq 1$ ορίζουμε $\prod_{i=1}^{n+1} a_i = \left(\prod_{i=1}^{n} a_i\right) a_{n+1}$. Τότε, για κάθε $n, m \geq 1$ ισχύει $\left(\prod_{i=1}^{n} a_i\right)\left(\prod_{j=1}^{m} a_{n+j}\right) = \prod_{k=1}^{n+m} a_k$.*

Απόδειξη. Χρησιμοποιούμε επαγωγή στον m. Η περίπτωση $m = 1$ είναι προφανής, ενώ για το επαγωγικό βήμα έχουμε

$$\begin{aligned}
\left(\prod_{i=1}^{n} a_i\right)\left(\prod_{j=1}^{m+1} a_{n+j}\right) &= \left(\prod_{i=1}^{n} a_i\right)\left(\left(\prod_{j=1}^{m} a_{n_j}\right) a_{n+m+1}\right) \\
&= \left(\left(\prod_{i=1}^{n} a_i\right)\left(\prod_{j=1}^{m} a_{n+j}\right)\right) a_{n+m+1} \\
&= \left(\prod_{k=1}^{n+m} a_k\right) a_{n+m+1} \\
&= \prod_{k=1}^{n+m+1} a_k.
\end{aligned}$$

∎

Θεώρημα (*Γενικευμένη Προσεταιριστική Ιδιότητα*). *Έστω A ένα σύνολο εφοδιασμένο με μια προσεταιριστική πράξη $A \times A \to A$, $(a,b) \mapsto ab$. Έστω*

$a_1, \ldots, a_n$ *μια διατεταγμένη* n*-άδα στοιχείων του* A*,* $n \geq 3$*. Τότε κάθε στοιχείο του* A *που αντιστοιχεί στην παραπάνω διατεταγμένη* n*-άδα είναι ίσο με το* $\prod_{i=1}^{n} a_i$*.*

Απόδειξη. Χρησιμοποιούμε επαγωγή στον n. Για $n = 3$, τα στοιχεία που αντιστοιχούν στην τριάδα a_1, a_2, a_3 είναι τα $(a_1a_2)a_3$, $a_1(a_2a_3)$. Αυτά είναι ίσα. Επιπλέον $\prod_{i=1}^{3} a_i = (a_1a_2)a_3$. Έστω τώρα $n \geq 4$ και έστω ότι το θεώρημα ισχύει για κάθε m-άδα με $m < n$. Κάθε στοιχείο του A που αντιστοιχεί στην n-άδα $a_1, \ldots, a_n$ είναι της μορφής cd, όπου το c (αντίστοιχα, το d) είναι ένα στοιχείο του A που αντιστοιχεί σε μία m-άδα $a_1, \ldots, a_m$ (αντίστοιχα, σε μία $n-m$-άδα $a_{m+1}, \ldots, a_n$), όπου $1 < m < n$. Από την υπόθεση της επαγωγής έχουμε

$$c = \prod_{i=1}^{m} a_i \quad \text{και} \quad d = \prod_{j=1}^{n-m} a_{m+j}.$$

Από τη σχέση (1) έχουμε ότι $cd = \prod_{i=1}^{n} a_i$. ⊤

6.3 Πολυώνυμα

Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο και $R^{\mathbb{N}}$ το σύνολο των ακολουθιών $(a_0, a_1, a_2, \ldots)$, όπου $a_i \in R$ για κάθε $i \in \mathbb{N}$. Αν $(a_0, a_1, a_2, \ldots,)$, $(b_0, b_1, b_2, \ldots) \in R^{\mathbb{N}}$ ορίζουμε

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots)$$

και

$$(a_0, a_1, \ldots)(b_0, b_1, \ldots) = (c_0, c_1, \ldots)$$

με $c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0$ για κάθε $n \in \mathbb{N}$.

Πρόταση *Το $R^{\mathbb{N}}$ με τις παραπάνω πράξεις είναι ένας δακτύλιος με μοναδιαίο στοιχείο το $(1_R, 0_R, 0_R, \ldots)$.*

Απόδειξη. Οι επαληθεύσεις των ιδιοτήτων στον ορισμό του δακτυλίου είναι εύκολες και αφήνονται σαν άσκηση. ⊺

Ορισμός *Ένα στοιχείο $(a_0, a_1, a_2, \ldots)$ του $R^{\mathbb{N}}$ ονομάζεται* ***πολυώνυμο*** *αν υπάρχει $m \in \mathbb{N}$ με $a_k = 0$ για κάθε $k > m$.*

Έστω $\Re$ το σύνολο των πολυωνύμων του $R^{\mathbb{N}}$. Είναι φανερό ότι το $\Re$ είναι ένας υποδακτύλιος του $R^{\mathbb{N}}$. Επιπλέον, η απεικόνιση

$$f : R \to \Re, \quad a \mapsto (a, 0_R, 0_R, \ldots)$$

είναι ένας μονομορφισμός δακτυλίων. Πράγματι, η f είναι $1-1$, ενώ ισχύει $f(a+b) = f(a) + f(b)$ και $f(ab) = f(a)f(b)$ για κάθε $a, b \in R$. Θα ταυτίζουμε ένα $a \in R$ με το αντίστοιχο πολυώνυμο $(a, 0_R, 0_R, \ldots)$. Κάτω από αυτήν την ταύτιση, το μηδενικό στοιχείο του $\Re$, δηλαδή το $(0_R, 0_R, \ldots)$, ταυτίζεται με το 0_R και το μοναδιαίο στοιχείο του $\Re$ ταυτίζεται με το 1_R. Έτσι ο R μπορεί να θεωρηθεί σαν υποδακτύλιος του $\Re$. Αν θέσουμε $x = (0_R, 1_R, 0_R, \ldots)$, τότε με επαγωγή στο n αποδεικνύεται εύκολα ότι $x^n = (0_R, 0_R, \ldots, 1_R, 0_R, \ldots)$ για κάθε $n \in \mathbb{N}$, όπου το 1_R ευρίσκεται στη θέση $n+1$. Από τον ορισμό, κάθε στοιχείο του $\Re$ είναι της μορφής $(a_0, a_1, \ldots, a_m, 0_R, 0_R, \ldots)$. Παρατηρούμε ότι

$$\begin{aligned}
(a_0, a_1, \ldots, a_m, 0_R, 0_R, \ldots) =& (a_0, 0_R, \ldots) + (0_R, a_1, 0_R, \ldots) + \cdots \\
&+ (0_R, \ldots, 0_R, a_m, 0_R, \ldots) \\
=& (a_0, 0_R, \ldots)(1_R, 0_R, \ldots) \\
&+ (a_1, 0_R, \ldots)(0_R, 1_R, 0_R, \ldots) \\
&+ \cdots + (a_m, 0_R, \ldots)(0_R, \ldots, 0_R, 1_R, 0_R, \ldots) \\
=& (a_0, 0_R, \ldots)x^0 + (a_1, 0_R, \ldots)x + \cdots \\
&+ (a_m, 0_R, \ldots)x^m.
\end{aligned}$$

Άρα, το στοιχείο $(a_0, a_1, \ldots, a_m, 0_R, \ldots)$, κάτω από την ταύτιση που αναφέραμε πριν, έχει μια παράσταση της μορφής

$$a_0 + a_1 x + \cdots + a_m x^m.$$

Επιπλέον είναι φανερό ότι $ax = xa$ για κάθε $a \in R$. Τέλος είναι προφανές ότι αν $a_0+a_1x+\cdots+a_mx^m = b_0+b_1x+\cdots b_nx^n$ με $m \geq n$, τότε $a_i = b_i$ για κάθε $i \leq n$ και $a_j = 0$ για κάθε $j = n+1, \ldots, m$. Ιδιαίτερα αν $a_0+a_1x+\cdots+a_mx^m = 0_R$, τότε $a_i = 0_R$ για κάθε $i = 0, 1, \ldots, m$.

Συνοψίζοντας, έχουμε αποδείξει το εξής αποτέλεσμα (το οποίο διατυπώσαμε στην Παράγραφο 2.2).

Θεώρημα *Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Τότε υπάρχει δακτύλιος $\Re$ με μοναδιαίο στοιχείο το 1_R που περιέχει τον R ως υποδακτύλιο και έχει τις εξής ιδιότητες:*

- *Υπάρχει στοιχείο $x \in \Re$ τέτοιο ώστε $ax = xa$ για κάθε $a \in R$.*
- *Κάθε στοιχείο του $\Re$ έχει μια παράσταση της μορφής*

  $$a_0 + a_1 x + \cdots + a_m x^m,$$

  όπου $m \in \mathbb{N}$ και $a_i \in R$, $i = 0, 1, \ldots, m$.
- *Αν $a_0+a_1x+\cdots+a_mx^m = b_0+b_1x+\cdots+b_nx^n$ με $m, n \in \mathbb{N}$, $m \geq n$ και $a_0, \ldots, a_m$, $b_0, \ldots, b_n \in R$ τότε για κάθε $i = 0, 1, \ldots, n$ έχουμε $a_i = b_i$ και για κάθε $j = n+1, \ldots, m$ έχουμε $a_j = 0_R$.*

Ο δακτύλιος $\Re$ συμβολίζεται με $R[x]$. Τα στοιχεία του $R[x]$ συμβολίζονται συνήθως με $f(x), g(x), \ldots$ ή $f, g, \ldots$.

Αναφορές και Βιβλιογραφία

7.1 Αναφορές

1. A. F. Archer, A Modern Treatment of the 15 Puzzle, Monthly 106, November 1999.

2. M. Artin, Algebra, Prentice Hall, 1991.

3. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wislon, ATLAS of finite groups, Clarendon Press, London, 1985.

4. Δ. Βάρσος, Δ Δεριζιώτης, Μ. Μαλιάκας, Σ.Γ Παπασταυρίδης, Ε, Ράπτης, Ο. Ταλέλλη, Εισαγωγή στη Γραμμική Άλγεβρα, Τόμος Α, Εκδόσεις Σοφία, 2003.

5. O. Campoli, A principal ideal domain that is not Euclidean, Amer. Math. Monthly, 95 (1988), 868-871.

6. D. Cox, J. Little and D.O'Shea, Ideals, Varieties and Algorithms, Springer, 1992.

7. H. S. M. Coxeter, Introduction to Geometry, 2nd Edition, Wiley Classical Library, John Wiley, 1989.

8. H.S.M. Coxeter, Regular Polytopes, Dover Publications, Inc., New York, 1973.

9. W. Feit and J. G. Thompson, Solvability of groups of odd order, Pacific J. Math. 13(1963) 775-1029.

10. H. Goldstein, Classical Mechanics, Addison-Wesley Publishing Company, 1950.

11. E. Grosswald, Representations of Integers as Sums of Squares, Springer, 1985.

12. M. Hall and J. K. Senior, The Groups of order $2^n (n \leq 6)$ The Macmillan N.Y., 1964.

13. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Claredon press, 1979.

14. I. N. Herstein, Topics in Algebra, Second Edition, Wiley, 1975.

15. D. L, Johnson, Presentations of Groups, Cambridge University Press 1976. lecture Note Series 22 London Mathematical Society.

16. A.Kurosh, The Theory of Groups Vols. I, II, Chelsea Publicashing Company, New York, 1960.

17. Μ. Μαλιάκας, Μεταθετική Άλγεβρα και Εφαρμογές: Εισαγωγικές Σημειώσεις, Πανεπιστήμιο Αθηνών, 1999.

18. N. H. McCoy and G. Janusz, Introduction to Modern Algebra, Allyn & Bacon (4th edition) 1987.

19. Ι. Μοσχοβάκης, Σημειώσεις στη Συνολοθεωρία, Εκδόσεις Νεφέλη, 1993.

20. M. Reid, Undergraduate Algebraic Geometry, Cambridge University Press, 1988.

21. M. Reid, Undergraduate Commutative Algebra, Cambridge University Press, 1990.

22. F. S. Roberts, Applied Combinatorics, Prentice Hall, 1984.

23. D. F. Robinson, Permutation in a group table, Math. Gazette (1969), 293.

24. K. Rosen, Elementary Number Theory and its Applications, Third Edition, Addison-Wesley, 1993.

25. J. J. Rotman, An Introduction to the Theory of Groups, 4th Edition, Graduate Texts in Mathematics, Springer-Verlag, N.Y., 1995.

26. H. Ryser, Combinatorial Mathematics, MAA, 1963.

27. C. Small, A simple proof of the four squares theorem, Amer. Math. Monthly 89 (1982), 59-61.

28. I. Stewart, Galois Theory, Second Edition, Chapman, 1989.

29. A. D. Thomas and G. V. Wood, Group tables, Shiva Publishing Limited, 1980.

30. H. Weyl, Symmetry, Princeton University Press, Princeton, New Jersey, First Princeton Paperbank printing, 1982.

31. H. Wielandt, Finite Permutation Groups, Academic Press, 1964.

32. H. Wussing, The Genesis of the Abstract Group Concept, The MIT Press, Cambridge, Massachusetts, 1984.

33. P. Yale, Geometry and Symmetry, Dover Publications, 1988.

7.2 Βιβλιογραφία

Για μια περαιτέρω μελέτη στην Άλγεβρα, συναφή θέματα και εφαρμογές προτείνουμε μεταξύ των άλλων τα παρακάτω εισαγωγικά βιβλία:

Γενική Άλγεβρα

R. B. J .T Allenby, Rings, Fields and Groups, Edward Arnold, 1983.

M. Artin, Algebra Prentice Hall 1991,

G. Birkoff and S. Machane, A Survey of Modern Algebra, Macmillan (4th edition), 1977.

A. M. Cohen, H. Cuypers, H. Sterk, Algebra Interactive, Springer, 1999.

M. Cohn, Algebra 2 Vols, J. Wiley, 1974, 1977.

J. B. Fraleigh, A First Course in Abstract Algebra, Addison-Wesley (4th edition), 1989. (Έχει μεταφρασθεί στα Ελληνικά από τις Πανεπιστημιακές Εκδόσεις Κρήτης).

J. A. Gallian, Contemporary Abstract Algebra, (3rd edition) D. C. Heath and Company 1994,

R. Godement, Cours d' Algebre, Hermann, 1963.

I. N. Herstein, Topics in Algebra, (2nd edition) Wiley, N.Y., 1975.

I. N. Herstein, Abstract Algebra, Prentice Hall, 1990.

T. W. Hungerford, Algebra, Holt, Rinehart and Winston, Inc. 1974.

I.M. Isaacs, Algebra (a Graduate Course), Brooks/Cole Publishing Company, 1994.

A. Papantonopoulou, Algebra Pure and Applied, Prentice Hall, N.J. 2002.

J. J. Rotman, A First Course in Abstract Algebra 2nd ed. Prentice Hall, 2000.

B. L. Van der Waerden, Modern Algebra, Ungar, New York, 1970.

Θεωρία Δακτυλίων

W. Adams and P. Loustaunau, An Introduction to Grobner Bases, AMS, 1994.

D. Burton, A First Course in Rings and Ideals, Addison Wesley, 1970.

A. Chatters and C.R. Hajarvanis, An Introductory Course in Commutative Algebra, Oxford University Press, 1998.

I. Kaplansky, Fields and Rings, Univ. Chicago, 1974.

N. McCoy, The Theory of Rings, Macmillan, 1964.

M. Reid, Undergraduate Commutative Algebra, Cambridge University Press, 1990.

R. Sharp, Steps in Commutative Algebra, Cambridge University Press, 1990.

Θεωρία Ομάδων

W. Burnside, Theory of groups of finite order, 2nd ed. Cambridge 1911 (Rover reprint 1955).

R. Carmichael, An Introduction to the Theory of Groups, Ginn, 1937.

M. Hall Jr. The Theory of Groups, Macmillan, 1959.

A. G. Kurosh, The Theory of Groups, (2 Vols) 2nd English ed. Chelsea, 1960.

W. Ledermann, Introduction to Group Theory, Oliver and Boyd, 1973.

J. S. Rose, A Course on Group Theory, Dover Publications, N.Y., 1994.

J. J. Rotman, An Introduction to the Theory of Groups 4th ed. Springer, N.Y., 1995.

E. Schenkman, Group Theory, Van Nostrand, 1965.

O. J. Schmidt, Abstract Theory of Groups, 2nd ed. Freeman, 1966.

W. R. Scott, Group Theory, Prentice-Hall, 1964.

M. Suzuki, Group Theory, I and II, Springer, 1982 and 1986.

H. Zassenhaus, The Theory of Groups, 2nd English ed. Chelsea, 1958.

Συμμετρία και Ομάδες

M. A. Armstrong, Groups and Symmetry, N.Y., Springer, 1988 (Έχει μεταφρασθεί στα Ελληνικά από τις Εκδόσεις Leader Books).

H. M. S. Coxeter, Introduction to Geometry, Wiley, 1989.

E. Rees, Notes on Geometry, Springer, 1988.

H. Weyl, Symmetry, Princeton University Press, 1952.

P. B. Yale, Geometry and Symmetry, Dover Publications, 1988.

Θεωρία του Galois

J. J. Rotman, Galois Theory, 2nd ed. New York, Springer, 1998.(Έχει μεταφρασθεί στα Ελληνικά από τις ΕκδόσειςLeader Books)

J. Stewart,Galois Theory, 2nd ed., London, Chapman and Hall, 1989.

Θεωρία Αριθμών

L. E. Dickson, Introduction to the Theory of Numbers, Dover Publications, N.Y., 1957.

G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Claredon press, 1979.

F. Richman, Number Theory: An Introduction to Algebra, Brooks/Cole, 1971.

K. H. Rosen, Elementary Number Theory and its applications, 2nd ed., Addison-Wesley, 1988.

J. Silverman, A Friendly Introduction to Number Theory, Prentice hall, 2001.

J. E. Shockley, Introduction to Number Theory, Holt, Rinehart and Winston, 1967.

Εφαρμογές της Άλγεβρας

N. J. Bloch, Abstract Algebra with Applications, Wiley 1987.

W. J. Gilbert, Modern Algebra with Applications, Wiley, 1976.

K. H. Kim and F. W. Roush, Applied Abstract Algebra, Wiley, 1983.

N. Koblitz, A Course in Number Theory and Cryptography, Springer, 1994.

R. Lidl and G. Pilz, Applied Abstract Algebra, Springer, 1984.

Ιστορικές Πηγές

B. L. Van der Waerden, A History of Algebra, Springer, 1985.

"Οι μαθηματικοί δεν μελετούν αντικείμενα, αλλά σχέσεις μεταξύ αντικειμένων. Επομένως, διαθέτουν την ελευθερία να αντικαταστήσουν κάποια αντικείμενα με άλλα εφόσον οι σχέσεις παραμένουν αμετάβλητες."

Jules Henri Poincaré (1854-1912)