Εισαγωγη στην Αλγεβρα

Μιχαήλ Χαραλάμπους

ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΑΛΓΕΒΡΑ

Εργαστήριο Ψηφιακής Τυπογραφίας
& Μαθηματικών Εφαρμογών

AT

Περιεχόμενα

1 Προκαταρκτικά **7**

1.1 Στοιχειώδεις συνολοθεωρητικές έννοιες και συμβολισμοί 7
1.2 Ασκήσεις 8
1.3 Συναρτήσεις 9
1.4 Ασκήσεις 10
1.5 Ορισμοί και Αποδείξεις 11
1.6 Ασκήσεις 13
1.7 Σχέσεις ισοδυναμίας 15
1.8 Ασκήσεις 16

2 Οι ακέραιοι **18**

2.1 Διαιρετότητα στο $\mathbb{Z}$ 18
2.2 Ασκήσεις 23
2.3 Ισοτιμία modulo n 25

3 Ομάδες **27**

3.1 Πράξεις 27
3.2 Ασκήσεις 29
3.3 Ομάδες 31
3.4 Ασκήσεις 32
3.5 Η πρόσθεση και ο πολλαπλασιασμός στο $\mathbb{Z}_n$ 35
3.6 Ασκήσεις 37
3.7 Πίνακες ομάδων 39
3.8 Ασκήσεις 40

4 Υποομάδες **42**

4.1 Υποομάδες 42
4.2 Ασκήσεις 43
4.3 Ιδιότητες Δυνάμεων 44
4.4 Ασκήσεις 46
4.5 Κυκλικές υποομάδες 47
4.6 Ασκήσεις 49
4.7 Το θεώρημα Lagrange 52

4.8 Ασκήσεις 54

5 Κι άλλες ομάδες **57**
5.1 Ομάδες μεταθέσεων 57
5.2 Ασκήσεις 59
5.3 Κύκλοι, τροχιές, εναλλάσσουσες ομάδες 60
5.4 Ασκήσεις 64
5.5 Ευθέα Γινόμενα Ομάδων 65
5.6 Ασκήσεις 67

6 Πόσες ομάδες; **68**
6.1 Ομομορφισμοί 68
6.2 Ασκήσεις 71
6.3 Κανονικές υποομάδες και πυρήνες ομομορφισμών 74
6.4 Ασκήσεις 76
6.5 Ομάδες πηλίκα 78
6.6 Ασκήσεις 80
6.7 Ασκήσεις 81

7 Δακτύλιοι **84**
7.1 Βασικές έννοιες και παραδείγματα 84
7.2 Ασκήσεις 87
7.3 Πολυώνυμα 90
7.4 Ασκήσεις 95

8 Ιδεώδη και Ομομορφισμοί Δακτυλίων **98**
8.1 Υποδακτύλιοι 98
8.2 Ασκήσεις 99
8.3 Ομομορφισμοί Δακτυλίων 100
8.4 Ασκήσεις 104

Κεφάλαιο 1

Προκαταρκτικά

Συντομογραφίες. Συχνά χρησιμοποιούμε το $\Leftrightarrow$ αντί του **αν και μόνο αν** και το $\Rightarrow$ αντί του **συνεπάγεται**

1.1 Στοιχειώδεις συνολοθεωρητικές έννοιες και συμβολισμοί

Τα σύνολα συμβολίζονται συνήθως με κεφαλαία λατινικά γράμματα, με ή χωρίς δείκτες. Το κενό σύνολο συμβολίζεται με $\emptyset$. Τα σύνολα των φυσικών αριθμών, των ακεραίων, των ρητών, των πραγματικών και των μιγαδικών αριθμών συμβολίζονται με $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ και $\mathbb{C}$, αντίστοιχα.

Το $\{a_1, a_2, \ldots\}$ παριστάνει το σύνολο που έχει ως μέλη ακριβώς όλα τα στοιχεία $a_1, a_2, \ldots$ Το ίδιο σύνολο γράφεται και ως $\{a_1, a_2, a_3, \ldots\}$ ή και $\{a_1, a_2, \ldots, a_n, \ldots\}$ Π.χ. $\{1, 2, \ldots\} = \{1, 2, 3, \ldots\} = \mathbb{N}$, και $\{1,\ 3,\ 5,\ \ldots\} = \{1,\ 3,\ \ldots, 2n-1,\ \ldots\}$ είναι το σύνολο που αποτελείται από όλους τους περιττούς φυσικούς αριθμούς. Το $\{a_1, a_2, \ldots, a_n\}$ παριστάνει το σύνολο του οποίου μέλη είναι ακριβώς τα στοιχεία $a_1, a_2, \ldots$ μέχρι και το a_n, το πλήθος των οποίων είναι το πολύ n γιατί ενδέχεται να μην είναι όλα διαφορετικά. Π.χ. $\{23, 98, 12\}$, $\{12, 23, 98\}$ και $\{23, 98, 12, 23, 12\}$ παριστάνουν το σύνολο που έχει ως μέλη τους αριθμούς 12, 23 και 98. Το $\{2, 4, 6, \ldots, 100\}$ έχει ως μέλη τους άρτιους αριθμούς από το 2 μέχρι και το 100.

Οι συμβολισμοί $x \in A$ και $y \notin B$ σημαίνουν: το x είναι μέλος ή στοιχείο του A και το y δεν είναι μέλος του B. Λέμε επίσης ότι το x ανήκει στο A και το y δεν ανήκει στο B. Π.χ. $3 \in \mathbb{Z}$, $-3 \notin \mathbb{N}$, $\sqrt{2} \notin \mathbb{Q}$.

Γράφουμε $A \subset B$, και λέμε το A είναι *υποσύνολο* του B, αν κάθε στοιχείο του A είναι στοιχείο και του B. Γράφουμε $A \not\subset B$ αν δεν ισχύει ότι $A \subset B$. Π.χ. $\mathbb{N} \subset \mathbb{Z}$, $\mathbb{Z} \subset \mathbb{Q}$, $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{R} \subset \mathbb{C}$, $\mathbb{Z} \not\subset \mathbb{N}$, $\mathbb{Q} \not\subset \mathbb{Z}$ κ.ο.κ. Δύο σύνολα A, B είναι ίσα αν κάθε μέλος του A είναι μέλος του B και, αντιστρόφως, κάθε μέλος του B είναι μέλος του B. Δηλαδή, $A = B$ αν και μόνον αν $A \subset B$ και $B \subset A$. Διαφορετικά, $A \neq B$

Έστω $P(x)$ μια πρόταση που έχει νόημα για κάθε στοιχείο x ενός συνόλου

A. Το σύνολο όλων των μελών x του A για τα οποία η πρόταση $P(x)$ αληθεύει συμβολίζεται με $\{x \in A : P(x)\}$ ή και με $\{x : x \in A, P(x)\}$. Π.χ. Αν η $P(x)$ είναι η πρόταση «ο x είναι άρτιος», τότε $\{x \in \mathbb{N} : \mathrm{P(x)}\} = \{2, 4, 6, ...\}$. Αν η $P(x)$ είναι πρόταση «ο x είναι περιττός αριθμός και ο x είναι μικρότερος του 1000», τότε $\{x \in \mathbb{N} : \mathrm{P(x)}\} = \{1, 3, 5, ..., 999\}$.

Ακόμη, $\mathbb{Q} = \{x \in \mathbb{R} : P(x)\}$, όπου $P(x)$ είναι η πρόταση «ο x είναι πηλίκο ακεραίων m, n με $n \neq 0$». Συντομογραφικά, $\mathbb{Q} = \{x \in \mathbb{R} : x = m/n, m, n \in \mathbb{Z}, n \neq 0\}$ ή $\mathbb{Q} = \{m/n : m, n \in \mathbb{Z}, n \neq 0\}$.

Έστω ότι για κάθε στοιχείο i κάποιου συνόλου I δίνεται ένα σύνολο A_i. Η ένωση των συνόλων A_i καθώς το i διατρέχει το I, $\bigcup_{i\in I} A_i$, είναι το σύνολο που αποτελείται από όλα τα στοιχεία που ανήκουν σε ένα τουλάχιστον A_i. Η τομή των συνόλων A_i καθώς το i διατρέχει το I, $\bigcap_{i\in I} A_i$, είναι το σύνολο που αποτελείται από τα στοιχεία που ανήκουν σε κάθε A_i. Δηλαδή,

$$\begin{aligned} \bigcup_{i\in I} A_i &= \{x : x \in A_i \text{ για κάποιο } i \in I\}, \\ \bigcap_{i\in I} A_i &= \{x : x \in A_i \text{ για κάθε } i \in I\}. \end{aligned}$$

Διακρίνουμε τρεις ιδιαίτερες περιπτώσεις.

1. Όταν $I = \{1, 2\}$, η ένωση γράφεται $A_1 \cup A_2$ και η τομή $A_1 \cap A_2$.

2. Στην πιο γενική περίπτωση που $I = \{1, 2, \ldots, n\}$, η ένωση γράφεται $A_1 \cup A_2 \cup \ldots \cup A_n$ ή $\bigcup_{i=1}^{n} A_i$ και η τομή $A_1 \cap A_2 \cap \ldots \cap A_n$ ή $\bigcap_{i=1}^{n} A_i$.

3. Όταν $I = \{1, 2, \ldots\}$, η ένωση γράφεται $A_1 \cup A_2 \cup \ldots$ ή $\bigcup_{i=1}^{\infty} A_i$ ή $\bigcup_{i\in\mathbb{N}} A_i$ και η τομή $A_1 \cap A_2 \cap \ldots$ ή $\bigcap_{i=1}^{\infty} A_i$ ή $\bigcap_{i\in\mathbb{N}} A_i$.

Σημειώστε ότι η ένωση δύο αριθμήσιμων συνόλων $\{a_1, a_2, \ldots, \}$, $\{b_1,\ b_2,\ \ldots\}$ γράφεται και στη μορφή $\{\ldots a_2, a_1, b_1, b_2, \ldots, \}$. Έτσι

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

Δοθέντων συνόλων A, B, η συνολοθεωρητική διαφορά $A \setminus B$ είναι το σύνολο που αποτελείται από όλα τα στοιχεία του A που δεν ανήκουν στο B: $A \setminus B = \{x \in A : x \notin B\}$.

1.2 Ασκήσεις

Άσκηση 1.2.1 *Έστω* $A_1 = \{x \in \mathbb{R} : x^2 = 1\}$, $A_2 = \{x \in \mathbb{Z} : x^3 = 1\}$ *και* $A_3 = \{x \in \mathbb{C} : x^4 = 1\}$.

Βρείτε τα σύνολα $A_1 \cup A_2$, $A_2 \cap A_3$, $(A_1 \cap A_2) \cup A_3$, $A_2 \setminus A_3$ *και* $A_3 \setminus A_1$.

Λύση 1.2.2 $A_1 \cup A_2 = A_1 = \{1, -1\}$, $A_2 \cap A_3 = A_2 = \{1\}$, $(A_1 \cap A_2) \cup A_3 = A_3 = \{1, -1, i, -i\}$, $A_2 \setminus A_3 = \emptyset$ *και* $A_3 \setminus A_1 = \{i, -i\}$.

Άσκηση 1.2.3 *Βρείτε την ένωση* $\bigcup_{i\in\mathbb{N}} A_i$ *και την τομή* $\bigcap_{i\in\mathbb{N}} A_i$, *όπου* $A_i = \{x \in \mathbb{R} : 0 \leq x < \frac{1}{i}\}$.

Λύση 1.2.4 $\bigcup_{i\in\mathbb{N}} A_i = \{x \in \mathbb{R} : 0 \leq x < 1\}$, $\bigcap_{i\in\mathbb{N}} A_i = \{0\}$.

Άσκηση 1.2.5 *Βρείτε τα σύνολα* $\bigcup_{x\in\mathbb{R}} A_x, \bigcap_{x\in\mathbb{R}} A_x, \bigcup_{x\in\mathbb{N}} A_x, \bigcap_{x\in\mathbb{N}} A_x, \bigcup_{x\in\mathbb{Z}} A_x, \bigcap_{x\in\mathbb{Z}} A_x$, *όπου* $A_x = \{(x+1)^2, 1, 2\}$.

Λύση 1.2.6 $\bigcup_{x\in\mathbb{R}} A_x = \{x \in \mathbb{R} : x \geq 0\}$, $\bigcap_{x\in\mathbb{R}} A_x = \{1, 2\}$, $\bigcup_{x\in\mathbb{N}} A_x = \{1, 2\} \cup \{4, 9, 16, \ldots\}$, $\bigcap_{x\in\mathbb{N}} A_x = \{1, 2\}$, $\bigcup_{x\in\mathbb{Z}} A_x = \{0, 1, 2\} \cup \{4, 9, 16, \ldots\}$, $\bigcap_{x\in\mathbb{Z}} A_x = \{1, 2\}$.

Άσκηση 1.2.7 *Βρείτε την ένωση* $\bigcup_{x\in X} B_x$ *δεδομένου ότι κάθε* B_x *είναι ένα υποσύνολο του* X *που περιέχει το* x.

Λύση 1.2.8 $\bigcup_{x\in X} B_x = X$.

1.3 Συναρτήσεις

Μια συνάρτηση (ή απεικόνιση) $f : X \to Y$ αποτελείται από δύο σύνολα X, Y μαζί με ένα κανόνα f ο οποίος σε κάθε στοιχείο x του X αντιστοιχίζει μοναδικό στοιχείο $f(x)$ του Y. Το X λέγεται το πεδίο ορισμού και το Y το πεδίο τιμών της συνάρτησης f. Λέμε ότι το x απεικονίζεται από την f στο $f(x)$ ή ότι η f στέλνει το x στο $f(x)$ ή ότι το $f(x)$ είναι η τιμή της f στο x. Για κάθε $A \subset X$ το σύνολο $f(A) = \{f(x) : x \in A\}$ λέγεται ευθεία εικόνα του A μέσω της f.

Δύο συναρτήσεις f, g θεωρούνται ίσες αν έχουν το ίδιο πεδίο ορισμού, το ίδιο πεδίο τιμών και $f(x) = g(x)$ για κάθε x στο πεδίο ορισμού.

Μια συνάρτηση $f : X \to Y$ λέγεται επί (του Y) αν για κάθε $y \in Y$, υπάρχει τουλάχιστον ένα $x \in X$ με $f(x) = y$.

Μια συνάρτηση $f : X \to Y$ λέγεται ένα–προς–ένα (1-1) ή μονοσήμαντη αν για όλα τα στοιχεία $x_1, x_2 \in X$ με $x_1 \neq x_2$, έχουμε $f(x_1) \neq f(x_2)$.

Δεδομένου συνόλου X και υποσυνόλου A του X, ο εγκλεισμός του A στο X είναι η συνάρτηση $i : A \to X$ που ορίζεται με $i(a) = a$ για κάθε $a \in A$. Ο εγκλεισμός του X στο X λέγεται ταυτοτική συνάρτηση πάνω στο X. Κάθε εγκλεισμός είναι 1-1 και κάθε ταυτοτική συνάρτηση είναι 1-1 και επί. Μια συνάρτηση $f : X \to Y$ είναι 1-1 και επί αν και μόνον αν σε κάθε $y \in Y$ αντιστοιχεί μοναδικό $x \in X$ με $f(x) = y$. Για κάθε τέτοια συνάρτηση f, ορίζεται η αντίστροφη συνάρτηση $f^{-1} : Y \to X$ ως εξής. Για $y \in Y$, $f^{-1}(y)$ ορίζεται το μοναδικό $x \in X$ που ικανοποιεί $f(x) = y$. Προφανώς, $f(x) = y \Leftrightarrow f^{-1}(y) = x$. Προκύπτει ότι η και η f^{-1} είναι 1-1 και επί με $(f^{-1})^{-1} = f$.

Έστω σύνολα X, Y. Αν υπάρχει συνάρτηση $f : X \to Y$ που είναι 1-1 και επί, τα X, Y λέγονται ισοδύναμα ή ισοπληθή σύνολα. Ένα σύνολο A είναι ισοδύναμο με το $\{1, 2, \ldots, n\}$, όπου $n \in \mathbb{N}$, αν και μόνον αν το A έχει n ακριβώς μέλη αν και μόνον αν το A γράφεται στη μορφή $\{a_1, a_2, \ldots, a_n\}$ όπου τα στοιχεία a_i είναι διακεκριμένα. Ένα σύνολο λέγεται πεπερασμένο αν είναι κενό ή αν είναι ισοδύναμο με το $\{1, 2, \ldots, n\}$ για κάποιο $n \in \mathbb{N}$, διαφορετικά λέγεται άπειρο. Ένα σύνολο είναι άπειρο αν και μόνον αν περιέχει διακεκριμένα στοιχεία $a_1, a_2, \ldots$

Δεδομένων συναρτήσεων $f : X \to Y$ και $g : Y \to Z$, ορίζεται η σύνθετη συνάρτηση $g \circ f : X \to Z$ με $(g \circ f)(x) = g(f(x))$, για κάθε $x \in X$. Προσέξτε ότι για να έχει νόημα η $g \circ f$ πρέπει το πεδίο τιμών της f να συμπίπτει με το πεδίο ορισμού της g.

1.4 Ασκήσεις

Άσκηση 1.4.1 *Αν οι συναρτήσεις $f : X \to Y$ και $g : Y \to Z$ είναι επί, να δείξετε ότι και η $g \circ f : X \to Z$ είναι επί.*

Λύση 1.4.2 *Έστω $z \in Z$. Αφού η g είναι επί , υπάρχει $y \in Y$ με $g(y) = z$. Τώρα αφού η f είναι επί, υπάρχει $x \in X$ με $f(x) = y$. Μα τότε $(g \circ f)(x) = g(f(x)) = g(y) = z$ και η $g \circ f$ είναι επί.*

Άσκηση 1.4.3 *Αν οι συναρτήσεις $f : X \to Y$ και $g : Y \to Z$ είναι 1-1, να δείξετε ότι και η $g \circ f : X \to Z$ είναι 1-1.*

Λύση 1.4.4 $(g \circ f)(x_1) = (g \circ f)(x_2) \Leftrightarrow g(f(x_1)) = g(f(x_2)) \Rightarrow f(x_1) = f(x_2)$ *γιατί η g είναι 1-1* $\Rightarrow x_1 = x_2$ *γιατί η f είναι 1-1. Άρα η $g \circ f$ είναι 1-1.*

Άσκηση 1.4.5 *Αν οι συναρτήσεις $f : X \to Y$ και $g : Y \to Z$ είναι 1-1 και επί, να δείξετε ότι και η $g \circ f : X \to Z$ είναι 1-1 και επί.*

Λύση 1.4.6 *Έπεται από τις δύο προηγούμενες ασκήσεις.*

Άσκηση 1.4.7 *Έστω $f : \mathbb{R} \to \mathbb{R}$ και $g : \mathbb{R} \to \mathbb{R}$, όπου $f(x) = x^2 + 1$ και $g(x) = 2x$. Βρείτε τους τύπους των συναρτήσεων $f \circ g$ και $g \circ f$. Είναι ίσες;*

Λύση 1.4.8 $(g \circ f)(x) = g(f(x)) = g(x^2 + 1) = 2(x^2 + 1) = 2x^2 + 2$.
$(f \circ g)(x) = f(g(x)) = f(2x) = (2x)^2 + 1 = 4x^2 + 1$.
$g \circ f \neq f \circ g$ *γιατί π.χ.* $(g \circ f)(0) = 2$ *ενώ* $(f \circ g)(0) = 1$.

Άσκηση 1.4.9 *Βρείτε τις ευθείες εικόνες $f(\{-2, -1, 0, 1, 2\})$, $g(\{-2, -1, 0, 1, 2\})$, $f(\mathbb{Z})$, $g(\mathbb{Z})$, $f(\mathbb{R}), g(\mathbb{R})$, όπου f, g είναι οι συναρτήσεις της Άσκησης 1.4.7. Είναι οι συναρτήσεις $f, g, g \circ f, f \circ g$ 1-1 ή επί;*

Λύση 1.4.10 $f(\{-2, -1, 0, 1, 2\}) = \{1, 2, 5\}$,
$g(\{-2, -1, 0, 1, 2\}) = \{-4, -2, 0, 2, 4\}$,
$f(\mathbb{Z}) = \{1, 5, 10, 17, \ldots, n^2 + 1, \ldots\}$,
$g(\mathbb{Z}) = \{\ldots - 4, -2, 0, 2, 4, \ldots\}$,
$f(\mathbb{R}) = \{x \in \mathbb{R} : x \geq 1\}$, $g(\mathbb{R}) = \mathbb{R}$.
$f(-1) = f(1)$. *Άρα η f δεν είναι 1-1. Ομοίως, οι $g \circ f$ και $f \circ g$ δεν είναι 1-1.*
$g(x_1) = g(x_2) \Leftrightarrow 2x_1 = 2x_2 \Leftrightarrow x_1 = x_2$. *Άρα η g είναι 1-1.*
Οι $f, f \circ g$ και $g \circ f$ δεν είναι επί γιατί λαμβάνουν μόνο θετικές τιμές, π.χ. δεν υπάρχει στοιχείο του $\mathbb{R}$ που να απεικονίζεται στο 0.
Για τυχαίο $y \in \mathbb{R}$, υπάρχει το $x = \frac{y}{2} \in \mathbb{R}$ που ικανοποιεί την $g(x) = y$. Άρα η g είναι επί.

Άσκηση 1.4.11 *Δείξτε ότι η $f : \mathbb{R} \to \mathbb{R}$, όπου $f(x) = 3x + 2$ είναι 1-1 και επί και βρείτε την αντίστροφη συνάρτηση.*

Λύση 1.4.12 *Δεδομένου $y \in \mathbb{R}$, για οποιοδήποτε $x \in \mathbb{R}$, $f(x) = y \Leftrightarrow 3x + 2 = y \Leftrightarrow x = \frac{y-2}{3}$. Αυτό δείχνει ότι υπάρχει μοναδικό $x \in \mathbb{R}$ με $f(x) = y$, συγκεκριμένα το $x = \frac{y-2}{3}$. Έπεται ότι η f είναι 1-1 και επί και $f^{-1}(y) = \frac{y-2}{3}$. Ισοδύναμα, $f^{-1}(x) = \frac{x-2}{3}$.*

Άσκηση 1.4.13 *Έστω a, b πραγματικοί αριθμοί με $a \neq 0$. Δείξτε ότι η $f : \mathbb{R} \to \mathbb{R}$, όπου $f(x) = ax + b$ είναι 1-1 και επί και βρείτε την αντίστροφη συνάρτηση.*

Λύση 1.4.14 *Δεδομένου $y \in \mathbb{R}$, για οποιοδήποτε $x \in \mathbb{R}$, $f(x) = y \Leftrightarrow ax + b = y \Leftrightarrow x = \frac{y-b}{a}$. Αυτό δείχνει ότι υπάρχει μοναδικό $x \in \mathbb{R}$ με $f(x) = y$, συγκεκριμένα το $x = \frac{y-b}{a}$. Έπεται ότι η f είναι 1-1 και επί και $f^{-1}(y) = \frac{y-b}{a}$. Ισοδύναμα, $f^{-1}(x) = \frac{x-b}{a}$.*

Άσκηση 1.4.15 *Έστω $A = \{1, 2, 3, 4, 5\}$. Βρείτε την αντίστροφη της συνάρτησης $f : A \to A$ που στέλνει τους $1, 2, 3, 4, 5$, στους $3, 2, 4, 5, 1$, αντίστοιχα.*

Λύση 1.4.16 *Η f^{-1} στέλνει τους $1, 2, 3, 4, 5$, στους $5, 2, 1, 3, 4$, αντίστοιχα.*

Άσκηση 1.4.17 *Βρείτε την αντίστροφη της συνάρτησης $f : \mathbb{R} \to \mathbb{R}$, όπου $f(x) = 5x$ αν ο x είναι ρητός, και $f(x) = -x$ αν ο x είναι άρρητος.*

Λύση 1.4.18 *$f^{-1}(x) = \frac{x}{5}$ αν ο x είναι ρητός, και $f^{-1}(x) = -x$ αν ο x είναι άρρητος.*

1.5 Ορισμοί και Αποδείξεις

Όταν ένας όρος εμφανίζεται για πρώτη φορά σε ένα μαθηματικό κείμενο, γίνεται ένας ακριβής και σαφής ορισμός των χαρακτηριστικών ιδιοτήτων του, συναρτήσει άλλων ήδη γνωστών εννοιών. Π.χ., έχοντας ορίσει την έννοια του διαιρέτη ακεραίων, προτού προχωρήσουμε σε θεωρήματα που αφορούν πρώτους αριθμούς, ορίζουμε την έννοια του *πρώτου* αριθμού:

Ορισμός 1.5.1 *Ένας ακέραιος p λέγεται πρώτος αν $p > 1$ και οι μόνοι θετικοί διαιρέτες του p είναι οι 1 και p.*

Εκτός της επικεφαλίδας, ένας άλλος συνήθης τρόπος ένδειξης ότι πρόκειται για ορισμό κάποιας έννοιας, είναι η χρήση έντονων τυπογραφικών στοιχείων για τον όρο που ορίζεται : «Ένας ακέραιος p λέγεται **πρώτος** αν $p > 1$ και οι μόνοι θετικοί διαιρέτες του p είναι οι 1 και p».

Όλοι οι ορισμοί είναι «αν και μόνο αν» προτάσεις: Ένας ακέραιος p είναι πρώτος αν και μόνο αν $p > 1$ και οι μόνοι θετικοί διαιρέτες του p είναι οι 1 και p. Αν παρουσιαστεί κάποιος πρώτος p, τότε γνωρίζω ότι ο $p > 1$ και οι μόνοι θετικοί διαιρέτες του p είναι οι 1 και p. Αντίστροφα, προκειμένου να δείξω ότι κάποιος

ακέραιος $p > 1$ είναι πρώτος αρκεί να ελέγξω ότι ο μόνος διαιρέτης του που είναι μεγαλύτερος από τον 1 είναι ο p.

Συχνά στα Μαθηματικά απαντούμε προτάσεις της μορφής: Η πρόταση $P(x)$ ισχύει για κάθε x στο X ή, συντομογραφικά,

$$P(x), \forall x \in X \qquad \text{ή} \qquad \forall x \in X, P(x).$$

Για να αποδείξουμε μια τέτοια πρόταση πρέπει να δείξουμε ότι η $P(x)$ ισχύει για κάθε x στο X, όχι μόνο ότι ισχύει για κάποια x στο X. Για να αποδείξουμε ότι μια τέτοια πρόταση δεν ισχύει αρκεί να δείξουμε ότι για κάποιο συγκεκριμένο x_0 στο X η $P(x_0)$ δεν ισχύει. Η άρνηση της $\forall x \in X, P(x)$ είναι προφανώς η $\exists x \in X$ τέτοιο ώστε η $P(x)$ δεν ισχύει ή $P(x)$ δεν ισχύει για κάποιο $x \in X$. Ένα $x_0 \in X$ για το οποίο δεν αληθεύει η $P(x_0)$ λέγεται ένα αντιπαράδειγμα στον ισχυρισμό $P(x), x \in X$. Π.χ. Ο αριθμός $\sqrt{2}$ είναι ένα αντιπαράδειγμα στον ισχυρισμό ότι κάθε πραγματικός αριθμός είναι ρητός, δηλαδή, στη πρόταση $\mathbb{R} \subset \mathbb{Q}$.

Συχνά στα Μαθηματικά προκειμένου να αποδείξουμε μια πρόταση P καταφεύγουμε στη μέθοδο της *εις άτοπον απαγωγής* ή της *έμμεσης* απόδειξης. Δηλαδή, υποθέτουμε κατ΄ αρχάς ότι δεν ισχύει η P και μετά από μια σειρά λογικών επιχειρημάτων καταλήγουμε σε μια πρόταση, η οποία μας είναι απαράδεκτη γιατί έχουμε ήδη αποδείξει ή δεχθεί την άρνησή της. Συνεπώς η P πρέπει να αληθεύει! Π.χ. θέλουμε να δείξουμε ότι ο μιγαδικός αριθμός i δεν είναι πραγματικός. Γνωρίζουμε ότι $x^2 \geq 0$ για κάθε $x \in \mathbb{R}$. Ας υποθέσουμε ότι $i \in \mathbb{R}$. Τότε $i^2 = -1 \geq 0$. Απαράδεκτο (άτοπο) γιατί έχουμε ήδη αποδείξει ότι $-1 < 0$. Συνεπώς $i \notin \mathbb{R}$.

Πρόταση 1.5.2 *(Η αρχή της μαθηματικής επαγωγής). Έστω $P(n)$ μια πρόταση για κάθε $n \in \mathbb{N}$. Έστω ότι (i) η $P(1)$ αληθεύει και (ii) για κάθε $n \in \mathbb{N}$, η $P(n)$ συνεπάγεται την $P(n+1)$, δηλαδή, αν αληθεύει η $P(n)$, αληθεύει και η $P(n+1)$. Τότε η πρόταση $P(n)$ αληθεύει για κάθε $n \in \mathbb{N}$.*

*Απόδειξη:*1.5.1 Έστω A το σύνολο όλων των φυσικών αριθμών n για τους οποίους η $P(n)$ αληθεύει. Από τα δεδομένα (i) $1 \in A$ και (ii) $n \in A \Rightarrow n+1 \in A$. Συνεπώς, $A = \{1, 2, 3, \ldots\} = \mathbb{N}$. Άρα η $P(n)$ αληθεύει για κάθε $n \in \mathbb{N}$. □

Στο πιο κλασικό παράδειγμα $P(n)$ είναι η πρόταση ότι

$$1 + 2 + \ldots + n = \tfrac{1}{2}n(n+1).$$

Εδώ είναι προφανές ότι η $P(1)$ ισχύει και μένει να δείξουμε ότι η $P(n)$ συνεπάγεται την $P(n+1)$. Υποθέτουμε, λοιπόν, ότι η $P(n)$ ισχύει. Κάνουμε, δηλαδή, την *επαγωγική υπόθεση* ότι $1+2+\ldots+n = \frac{1}{2}n(n+1)$. Μένει να δείξουμε ότι ισχύει η $P(n+1)$, δηλαδή, ότι

$$1 + 2 + \ldots + (n+1) = \tfrac{1}{2}(n+1)((n+1)+1).$$

Όμως, $1+2+\ldots+(n+1) = (1+2+\ldots+n)+(n+1)$ και από την επαγωγική υπόθεση $1+2+\ldots+(n+1) = (\frac{1}{2}n(n+1))+(n+1) = \frac{1}{2}(n+1)(n+2) = \frac{1}{2}(n+1)((n+1)+1)$. Αυτό ολοκληρώνει την απόδειξη.

Έστω $A \subset \mathbb{R}$. Ένας πραγματικός αριθμός a_0 τέτοιος ώστε $a_0 \leq a$ για κάθε $a \in A$ λέγεται κάτω φράγμα του A. Ένας πραγματικός αριθμός b_0 τέτοιος ώστε

$a \leq b_0$ για κάθε $a \in A$ λέγεται άνω φράγμα του A. Το A λέγεται κάτω (αντίστοιχα, άνω) φραγμένο αν έχει κάποιο κάτω (αντίστοιχα, άνω) φράγμα. Αν για κάποιο $a_0 \in A$ ισχύει $a_0 \leq a$ για κάθε $a \in A$, το a_0 λέγεται πρώτο ή ελάχιστο στοιχείο του A. Αν για κάποιο $a_0 \in A$ ισχύει $a \leq a_0$ για κάθε $a \in A$, το a_0 λέγεται μέγιστο στοιχείο του A. Προφανώς, τα ελάχιστα και μέγιστα στοιχεία, αν υπάρχουν, είναι μοναδικά. Το $\mathbb{N}$ έχει ελάχιστο στοιχείο, το 0, αλλά δεν έχει μέγιστο στοιχείο. Τα $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ δεν είναι ούτε κάτω ούτε άνω φραγμένα, συνεπώς δεν έχουν ούτε ελάχιστα ούτε μέγιστα στοιχεία.

Πρόταση 1.5.3 *(Η αρχή της καλής διάταξης). Κάθε μη κενό και κάτω φραγμένο υποσύνολο A του $\mathbb{Z}$ έχει ελάχιστο στοιχείο.*

*Απόδειξη:*1.5.2 Έστω k_0 ένας ακέραιος που είναι κάτω φράγμα του A και k_1 ένα στοιχείο του A, οπότε $k_0 \leq k_1$.

Έστω $P(n)$ η πρόταση ότι το $k_0 + n - 1$ είναι κάτω φράγμα του A. Προφανώς, η $P(1)$ αληθεύει, αλλά όχι η $P(k_1 + 2 - k_0)$, η οποία ισχυρίζεται ότι το $k_1 + 1$ είναι κάτω φράγμα του A! Συνεπώς, εφόσον δεν ισχύει η $P(n)$ για κάθε $n \in \mathbb{N}$, από την αρχή της μαθηματικής επαγωγής, για κάποιο $m \in \mathbb{N}$, η $P(m)$ αληθεύει, αλλά όχι η $P(m+1)$. Δηλαδή, το $k_0 + m - 1$ είναι κάτω φράγμα του A, αλλά όχι το $k_0 + m$. Αυτό απλά σημαίνει ότι το κάτω φράγμα $k_0 + m - 1$ είναι στοιχείο του A, συνεπώς είναι το ελάχιστο στοιχείο του A.

□

Η πιο συνήθης μορφή της αρχής καλής διάταξης είναι ή εξής.

Πόρισμα 1.5.4 *(Η αρχή της καλής διάταξης). Κάθε μη κενό υποσύνολο A του $\mathbb{N}$ έχει ελάχιστο στοιχείο.*

*Απόδειξη:*1.5.3 Έπεται από την Πρόταση 1.5.3 αφού το A είναι και κάτω φραγμένο (από το 1). □

Στην Πρόταση 1.5.3, δείξαμε ότι η αρχή της μαθηματικής επαγωγής συνεπάγεται την αρχή της καλής διάταξης. Στην Άσκηση 1.6.3, θα δούμε ότι και το αντίστροφο ισχύει. Έτσι, οι δύο αρχές είναι ισοδύναμες.

1.6 Ασκήσεις

Άσκηση 1.6.1 *(Ακόμη μια μορφή της αρχής της καλής διάταξης). Να δείξετε ότι κάθε μη κενό, άνω φραγμένο υποσύνολο B του $\mathbb{Z}$ έχει μέγιστο στοιχείο.*

Λύση 1.6.2 *Έστω k ένα άνω φράγμα του B. Θέτω $A = \{-x : x \in B\}$. Τότε το A είναι μη κενό υποσύνολο του $\mathbb{Z}$ και $-k$ είναι κάτω φράγμα του A. Από την Πρόταση 1.5.3, το A έχει ελάχιστο στοιχείο. Αν a είναι αυτό το ελάχιστο στοιχείο, εύκολα ελέγχεται ότι το $-a$ είναι μέγιστο στοιχείο του B.*

Άσκηση 1.6.3 *(Μια ισοδύναμη μορφή επαγωγής). Έστω k κάποιος ακέραιος. Για κάθε ακέραιο $n \geq k$, δίνεται μια πρόταση $P(n)$. Έστω ότι (1) η $P(n)$ ισχύει για $n = k$, και (2) αν η $P(n)$ ισχύει για $n = m$, όπου $m \geq k$, τότε η $P(n)$ ισχύει για $n = m + 1$. Να δείξετε ότι οι προτάσεις $P(n)$ αληθεύουν για κάθε $n \geq k$.*

Λύση 1.6.4 *Έστω A το σύνολο όλων των φυσικών αριθμών $n \geq k$ για τους οποίους η $P(n)$ δεν αληθεύει. Αφού η $P(k)$ αληθεύει, το A είναι κάτω φραγμένο από το $k + 1$. Ας υποθέσουμε ότι $A \neq \emptyset$. Από την αρχή καλής διάταξης, κάποιο $l \in A$ είναι ελάχιστο στοιχείο του A. Έτσι, $l \geq k + 1$, $l \in A$ ενώ $l - 1 \notin A$. Δηλαδή, η $P(l)$ δεν αληθεύει παρότι η $P(l - 1)$ αληθεύει. Αυτό αντιφάσκει στη (2) για $m = l - 1$. Συνεπώς, $A = \emptyset$, δηλαδή, οι προτάσεις $P(n)$ αληθεύουν για κάθε $n \geq k$.*

Άσκηση 1.6.5 *Να δείξετε ότι για κάθε φυσικό αριθμό n,*

$$1 + 3 + 5 + \ldots + (2n - 1) = n^2.$$

Λύση 1.6.6 *Η απόδειξη γίνεται με επαγωγή στο n. Θεωρούμε ότι $P(n)$ είναι η πρόταση ότι $1 + 3 + 5 + \ldots + (2n - 1) = n^2$. Προφανώς η $P(n)$ αληθεύει για $n = 1$. Υποθέτουμε ότι η $P(n)$ αληθεύει για $n = m$. Δηλαδή, η επαγωγική μας υπόθεση είναι ότι*

$$1 + 3 + 5 + \ldots + (2m - 1) = m^2.$$

Αρκεί τώρα να δείξουμε ότι ισχύει και η $P(m + 1)$. Επειδή

$$1 + 3 + 5 + \ldots + (2(m + 1) - 1) = (1 + 3 + 5 + \ldots + (2m - 1) + (2(m + 1) - 1),$$

από την επαγωγική υπόθεση,

$$1+3+5+\ldots+(2(m+1)-1) = m^2+(2(m+1)-1) = m^2+2m+1 = (m+1)^2.$$

Συνεπώς, η $P(m + 1)$ ισχύει και η απόδειξη έχει ολοκληρωθεί.

Άσκηση 1.6.7 *Να δείξετε ότι για κάθε φυσικό αριθμό n, το σύνολο $\{1, 2, 3, \ldots, n\}$ έχει 2^n υποσύνολα.*

Λύση 1.6.8 *Η απόδειξη γίνεται με επαγωγή στο n. Το $\{1\}$ έχει $2^1 = 2$ υποσύνολα, τα $\emptyset$ και $\{1\}$. Άρα η πρότασή μας ισχύει για $n = 1$. Υποθέτω ότι η πρόταση ισχύει για $n = m$, δηλαδή, ότι το $\{1, 2, 3, \ldots, m\}$ έχει 2^m υποσύνολα. Τώρα τα υποσύνολα του $\{1, 2, 3, \ldots, m+1\}$ είναι τα υποσύνολα του $\{1, 2, 3, \ldots, m\}$ μαζί με τα σύνολα της μορφής $A \cup \{m + 1\}$, όπου το A είναι υποσύνολο του $\{1, 2, 3, \ldots, m\}$. Από την επαγωγική υπόθεση αυτά ανέρχονται σε $2^m + 2^m = 2^{m+1}$ υποσύνολα. Έτσι ισχύει η πρόταση για $n = m + 1$ και η απόδειξη έχει ολοκληρωθεί.*

Άσκηση 1.6.9 *Να δείξετε ότι για κάθε φυσικό αριθμό $n \geq 10$, $2^n > n^3$.*

Λύση 1.6.10 *Η απόδειξη γίνεται με επαγωγή στο n. Για $n = 10$, η πρόταση ισχύει γιατί $2^{10} = 1024 > 1000 = 10^3$. Ας υποθέσουμε ότι πρόταση ισχύει για $n = m$, δηλαδή, ότι $2^m > m^3$, όπου $m \geq 10$. Μένει να δείξουμε ότι $2^{m+1} = 2^m + 2^m > (m + 1)^3 = m^3 + 3m^2 + 3m + 1$. Εφόσον $2^m > m^3$, αρκεί να δείξουμε ότι $m^3 \geq 3m^2 + 3m + 1$. Όντως, επειδή $m \geq 10$, $3m^2 + 3m + 1 = \frac{1}{3}(9m^2 + 9m + 3) < \frac{1}{3}(m^3 + m^3 + m^3) = m^3$.*

1.7 Σχέσεις ισοδυναμίας

Ένα *διατεταγμένο ζεύγος* (a, b) αποτελείται από δύο στοιχεία a, b μαζί με την συγκεκριμένη διάταξη των δύο στοιχείων, όπου το a εμφανίζεται πρώτο και το b δεύτερο. Έτσι δύο διατεταγμένα ζεύγη (a_1, b_1) και (a_2, b_2) είναι ίσα αν και μόνον αν $a_1 = a_2$ και $b_1 = b_2$. Το σύνολο $A \times B = \{(a, b) : a \in A, b \in B\}$ λέγεται το καρτεσιανό γινόμενο των A, B. Πιο γενικά, για $n \in \mathbb{N}$, μια διατεταγμένη n-άδα $(a_1, a_2, \ldots, a_n)$ αποτελείται από τα στοιχεία $a_1, a_2, \ldots, a_n$ μαζί με την συγκεκριμένη διάταξή τους, δηλαδή, $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ αν και μόνον αν $a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n$. Έχουμε το καρτεσιανό γινόμενο $A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}$, το οποίο όταν $A_1 = A_2 = \ldots = A_n = A$ γράφεται και ως A^n.

Μια *σχέση* S σε ένα σύνολο A είναι τυπικά ένα υποσύνολο S του $A^2 = A \times A$. Γράφουμε aSb όταν το ζεύγος (a, b) είναι μέλος της σχέσης S και λέμε ότι το a *σχετίζεται* με το b, ως προς την S. Προφανώς, μια σχέση S καθορίζεται μονοσήμαντα από τα ζεύγη (a, b) για τα οποία ισχύει ότι aSb. Συνεπώς, προκειμένου να ορίσουμε μια σχέση S, αρκεί να πούμε πότε ισχύει ότι aSb. Συνήθη σύμβολα για σχέσεις είναι: $\sim, <, \leq$ κ.α.

Μια σχέση $\sim$ σε ένα σύνολο A λέγεται

1. **ανακλαστική** αν: $a \sim a$ για κάθε $a \in A$.
2. **συμμετρική** αν: $a \sim b$ συνεπάγεται $b \sim a$, για κάθε $a, b \in A$
3. **μεταβατική** αν: $a \sim b$ και $b \sim c$ συνεπάγονται $a \sim c$, για κάθε $a, b, c \in A$
4. **σχέση ισοδυναμίας** αν είναι ανακλαστική, συμμετρική και μεταβατική.

Σε οποιοδήποτε σύνολο η σχέση της ισότητας $(=)$ είναι σχέση ισοδυναμίας. Σε οποιοδήποτε υποσύνολο του $\mathbb{R}$, η σχέση $\leq$ είναι ανακλαστική και μεταβατική, όχι όμως συμμετρική: παρότι $1 \leq 2$, δεν ισχύει ότι $2 \leq 1$. Η σχέση $<$ είναι μεταβατική αλλά δεν είναι ούτε ανακλαστική ούτε συμμετρική.

Έστω $\sim$ σχέση ισοδυναμίας σε ένα σύνολο A και $x \in A$. Η **κλάση ισοδυναμίας** του x, ως προς την $\sim$, είναι το σύνολο $[x] = \{y \in A : y \sim x\}$. Προφανώς, $[x] = \{y \in A : x \sim y\}$ γιατί $x \sim y$ αν και μόνον αν $y \sim x$. Γράφουμε $x \not\sim y$ όταν δεν ισχύει ότι $x \sim y$.

Πρόταση 1.7.1 *Για μια σχέση ισοδυναμίας $\sim$ σε σύνολο A ισχύουν τα εξής.*

1. $x \in [x]$
2. $[x] = [y] \Leftrightarrow x \sim y$
3. $[x] = [y] \Leftrightarrow x \in [y]$
4. $[x] \cap [y] \neq \emptyset \Leftrightarrow x \sim y$
5. $[x] \cap [y] \neq \emptyset \Leftrightarrow [x] = [y]$
6. $[x] \cap [y] = \emptyset \Leftrightarrow x \not\sim y$

*Απόδειξη:*1.7.1

1. Λόγω ανακλαστικότητας της $\sim$, $x \sim x$. Άρα $x \in [x]$.

2. Έστω ότι $[x] = [y]$. Από την (1), $y \in [y]$, άρα $y \in [x]$. Συνεπώς, $x \sim y$.

   Αντίστροφα, έστω ότι $x \sim y$. Αν $z \in [y]$, τότε $y \sim z$ και, λόγω μεταβατικότητας της $\sim$, $x \sim z$. Άρα $z \in [x]$. Αυτό δείχνει ότι $[y] \subset [x]$. Όμως, λόγω συμμετρικότητας της $\sim$, αφού $x \sim y$, έχουμε $y \sim x$ και συνεπώς $[x] \subset [y]$. Έτσι, $[x] = [y]$.

3. Έπεται από την (2) αφού $x \in [y] \Leftrightarrow x \sim y$.

4. Έστω ότι $[x] \cap [y] \neq \emptyset$. Τότε υπάρχει κάποιο $z \in [x] \cap [y]$. Έτσι $z \in [x]$, άρα $x \sim z$. Επίσης, $z \in [y]$, άρα $z \sim y$. Τώρα λόγω μεταβατικότητας, $x \sim y$.

   Αντίστροφα, ας υποθέσουμε ότι $x \sim y$. Από την (2), $[x] = [y]$ και, από την (1), το σύνολο $[x] \cap [y]$ δεν είναι κενό γιατί περιέχει π.χ. το x.

5. $[x] \cap [y] \neq \emptyset \Leftrightarrow x \sim y$ από την (4) $\Leftrightarrow [x] = [y]$ από την (2).

6. $[x] \cap [y] = \emptyset \Leftrightarrow x \not\sim y$ από την (4).

□

Ενδέχεται δύο στοιχεία $x, y \in A$ να έχουν την ίδια κλάση ισοδυναμίας. Σε τέτοια περίπτωση λέμε ότι ότι τα x, y είναι **αντιπρόσωποι** της ίδιας κλάσης. Αυτό προφανώς συμβαίνει αν και μόνο αν $x \sim y$.

1.8 Ασκήσεις

Άσκηση 1.8.1 *Από τις εξής τρεις σχέσεις στο $A = \{1, 2, 3\}$, ποιες είναι ανακλαστικές, ποιες συμμετρικές και ποιες μεταβατικές;*

1. $S_1 = \{(1,1), (2,2), (3,3), (1,2)\}$
2. $S_2 = \{(1,1), (1,2), (2,1), (2,2)\}$
3. $S_3 = \{(1,1), (1,2), (2,1), (2,2), (2,3), (3,2), (3,3)\}$

Λύση 1.8.2 *Η S_1 δεν είναι συμμετρική γιατί δεν ισχύει ότι $2S_11$ παρότι $1S_12$. Είναι όμως ανακλαστική και μεταβατική.*

Η S_2 δεν είναι ανακλαστική γιατί δεν ισχύει ότι $3S_23$. Είναι όμως συμμετρική και μεταβατική.

Η S_3 δεν είναι μεταβατική γιατί δεν ισχύει ότι $1S_33$ παρότι $1S_32$ και $2S_33$. Είναι όμως ανακλαστική και συμμετρική.

Άσκηση 1.8.3 *Μια σχέση $\sim$ ορίζεται στο $\mathbb{Z}$ με $x \sim y$ αν και μόνον αν ο ακέραιος $x - y$ είναι περιττός. Είναι η $\sim$ ανακλαστική, συμμετρική ή μεταβατική;*

Λύση 1.8.4 *Δεν είναι ανακλαστική γιατί* $x \not\sim x$ *για κάθε* x.

Είναι συμμετρική : $x \sim y \Rightarrow x - y$ *περιττός* $\Rightarrow y - x = -(x - y)$ *περιττός* $\Rightarrow y \sim x$.

Δεν είναι μεταβατική: $1 \not\sim 3$ *παρότι* $1 \sim 2$ *και* $2 \sim 3$.

Άσκηση 1.8.5 *Μια σχέση* $\sim$ *ορίζεται στο* $\mathbb{Z}$ *με* $x \sim y$ *αν και μόνον αν* $x - y \geq 0$. *Είναι η* $\sim$ *ανακλαστική, συμμετρική ή μεταβατική;*

Λύση 1.8.6 *Είναι ανακλαστική γιατί* $x \sim x$ *για κάθε* x *αφού* $x - x = 0 \geq 0$.

Δεν είναι συμμετρική: $3 \not\sim 4$ *παρότι* $4 \sim 3$.

Είναι μεταβατική: $x \sim y, y \sim z \Rightarrow x - y \geq 0, y - z \geq 0 \Rightarrow (x - y) + (y - z) = x - z \geq 0 \Rightarrow x \sim z$.

Άσκηση 1.8.7 *Μια σχέση* $\sim$ *ορίζεται στο* $\mathbb{Z}$ *με* $x \sim y$ *αν και μόνον αν ο* $xy \geq 0$. *Είναι η* $\sim$ *ανακλαστική, συμμετρική ή μεταβατική;*

Λύση 1.8.8 *Είναι προφανώς ανακλαστική και συμμετρική. Δεν είναι μεταβατική:* $-1 \not\sim 1$ *παρότι* $-1 \sim 0$ *και* $0 \sim 1$.

Άσκηση 1.8.9 *Έστω* $\sim$ *σχέση ισοδυναμίας σε σύνολο* A. *Με τι ισούται η ένωση* $\bigcup_{x \in A}[x]$ *όλων των κλάσεων ισοδυναμίας ως προς* $\sim$*;*

Λύση 1.8.10 $\bigcup_{x \in A}[x] = A$.

Άσκηση 1.8.11 *Η σχέση* $\sim$ *που ορίζεται στο* $\mathbb{Z}$ *με* $x \sim y$ *αν και μόνον αν ο* $|x| = |y|$ *είναι σχέση ισοδυναμίας. Με τι ισούται η κλάση ισοδυναμίας* $[x]$ *στοιχείου* x*;*

Λύση 1.8.12 $[x] = \{x, -x\}$.

Άσκηση 1.8.13 *Η σχέση* $\sim$ *ορίζεται στο* $\mathbb{Z}$ *με* $x \sim y$ *αν και μόνον αν ο* $x - y$ *είναι άρτιος. Δείξτε ότι η* $\sim$ *είναι σχέση ισοδυναμίας και βρείτε όλες τις κλάσεις ισοδυναμίας.*

Λύση 1.8.14 *Προφανώς είναι ανακλαστική και συμμετρική. Τώρα* $x \sim y, y \sim z \Rightarrow x - y, y - z$ *άρτιοι* $\Rightarrow x - z = (x - y) + (y - z)$ *άρτιος* $\Rightarrow x \sim z$. *Άρα η* $\sim$ *είναι και μεταβατική. Συνεπώς, είναι σχέση ισοδυναμίας.*

Προφανώς, $[0]$ *αποτελείται από όλους τους ζυγούς αριθμούς και* $[1]$ *αποτελείται από όλους τους μονούς αριθμούς. Από την Πρόταση 1.7.1,* $[x] = [0]$ *αν ο* x *είναι ζυγός και* $[x] = [1]$ *αν ο* x *είναι περιττός. Συνεπώς,* $[0]$ *και* $[1]$ *είναι όλες οι κλάσεις ισοδυναμίας.*

Εδώ προφανώς κάθε άρτιος αριθμός είναι αντιπρόσωπος της $[0]$ *και κάθε περιττός αριθμός είναι αντιπρόσωπος της* $[1]$

Κεφάλαιο 2

Οι ακέραιοι

2.1 Διαιρετότητα στο $\mathbb{Z}$

Θεώρημα 2.1.1 (Αλγόριθμος διαίρεσης) *Έστω $a, b \in \mathbb{Z}$ με $b \neq 0$. Τότε υπάρχουν μοναδικοί $q, r \in \mathbb{Z}$ τέτοιοι ώστε $a = qb + r$ και $0 \leq r < |b|$.*

(Ο q λέγεται το πηλίκο και ο r το υπόλοιπο της διαίρεσης του a με το b).

*Απόδειξη:*2.1.1 Για να δείξουμε την μοναδικότητα των q, r, ας υποθέσουμε ότι υπάρχουν $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ με $a = q_1 b + r_1$, $a = q_2 b + r_2$, $0 \leq r_1 < |b|$ και $0 \leq r_2 < |b|$. Από τις πρώτες δύο εξισώσεις, $|r_1 - r_2| = |q_2 - q_1||b|$ και, από τις τελευταίες δύο εξισώσεις, $|r_1 - r_2| < |b|$. Αυτό συνεπάγεται ότι $|q_2 - q_1| = 0$. Άρα $q_1 = q_2$ και $r_1 = r_2$.

Για να δείξουμε την ύπαρξη των q, r, θεωρούμε πρώτα την περίπτωση που $b > 0$ και ορίζουμε

$$A = \{a - xb : x \in \mathbb{Z}, a - xb \geq 0\}.$$

Αν $a \geq 0$, τότε $a = a - 0b \in A$. Αν $a < 0$, τότε $a - ab = (-a)(b - 1) \geq 0$ και $a - ab \in A$. Έπεται ότι $A \neq \emptyset$. Επιπλέον, το υποσύνολο A του $\mathbb{Z}$ είναι κάτω φραγμένο (από το 0). Από την αρχή της καλής διάταξης, το A έχει ελάχιστο στοιχείο, το οποίο καλούμε r. Από τον ορισμό του A, $r \geq 0$ και $r = a - qb$ για κάποιο ακέραιο q. Έτσι $a = qb + r$ και μένει να δείξουμε ότι $r < b$. Τώρα, αν $r \geq b$, τότε $0 \leq r - b = a - (q+1)b \in A$. Αυτό όμως αντιφάσκει στον ορισμό του r γιατί $r - b < r$. Έτσι $r < b$ και το θεώρημα ισχύει όταν $b > 0$.

Έστω τώρα ότι $b < 0$. Από την προηγούμενη παράγραφο, υπάρχουν $q, r \in \mathbb{Z}$ τέτοια ώστε $a = q(-b) + r$ και $0 \leq r < |-b|$. Αφού $a = (-q)b + r$ και $|b| = |-b|$, το αποτέλεσμα ισχύει και για $b < 0$. □

Έστω $a, b \in \mathbb{Z}$. Αν $a = qb$ για κάποιο $q \in \mathbb{Z}$, τότε λέμε ότι ο b **διαιρεί** τον a ή ότι ο b είναι **παράγοντας** του a ή ότι ο a είναι **πολλαπλάσιος** του b, και γράφουμε $b|a$.

Λήμμα 2.1.2 *Για κάθε $a, b, c, s, t \in \mathbb{Z}$,*

1. $a|0$, $1|a$, $a|a$,
2. $a|b \Rightarrow b = 0$ *ή* $|a| \leq |b|$,
3. $a|b, b|a \Rightarrow a = \pm b$,
4. $a|b \Rightarrow (-a)|b, a|(-b)$,
5. $a|b, b|c \Rightarrow a|c$,
6. $c|a, c|b \Rightarrow c|(sa + tb)$.

*Απόδειξη:*2.1.2

1. $0 = 0a$, $a = a1$, $a = 1a$.
2. $a|b \Leftrightarrow b = qa$ για κάποιο ακέραιο q. Αν $b \neq 0$, $|q| \geq 1$ και $|b| = |q||a| \geq |a|$.
3. $a|b, b|a \Rightarrow |a| = |b|$ από την (2)$\Rightarrow a = \pm b$.
4. $a|b \Rightarrow b = qa$ για κάποιο ακέραιο $q \Rightarrow b = (-q)(-a), -b = (-q)a$.
5. $a|b, b|c \Rightarrow b = qa, c = rb$ για κάποιους $q, r \in \mathbb{Z} \Rightarrow c = (rq)a \Rightarrow a|c$.
6. $c|a, c|b \Rightarrow a = qc, b = rc$ για κάποιους $q, r \in \mathbb{Z} \Rightarrow (sa + tb) = (sq + tr)c \Rightarrow c|(sa + tb)$.

□

Έστω $a, b, d \in \mathbb{Z}$. Ο d λέγεται **κοινός διαιρέτης** των a και b αν $d|a$ και $d|b$. Ο d λέγεται **μέγιστος κοινός διαιρέτης** των a, b, αν (1) $d > 0$, (2) ο d είναι **κοινός διαιρέτης** των a, b και (3) κάθε κοινός διαιρέτης των a, b διαιρεί και τον d. Από το Λήμμα 2.1.2, αν οι d_1, d_2 ικανοποιούν τις δύο τελευταίες ιδιότητες, τότε $d_1 = \pm d_2$. Αν ικανοποιούν και την πρώτη, τότε $d_1 = d_2$. Έπεται ότι ο μέγιστος κοινός διαιρέτης των a, b, αν υπάρχει, είναι μοναδικός. Ο μέγιστος κοινός διαιρέτης των a, b συμβολίζεται με $\mu\kappa\delta(a, b)$.

Θεώρημα 2.1.3 *Έστω $a, b \in \mathbb{Z}$ με a ή $b \neq 0$. Τότε ο $\mu\kappa\delta(a, b)$ υπάρχει. Μάλιστα είναι* ***γραμμικός συνδυασμός*** *των a, b, δηλαδή, γράφεται στη μορφή $sa + tb$ για κάποιους $s, t \in \mathbb{Z}$.*

*Απόδειξη:*2.1.3 Θεωρώ το εξής υποσύνολο του $\mathbb{N}$

$$A = \{xa + yb : x, y \in \mathbb{Z}, xa + yb > 0\}.$$

Το A περιέχει το θετικό αριθμό $a^2 + b^2$. Από την αρχή καλής διάταξης, το A έχει ελάχιστο στοιχείο, το οποίο καλώ d. Θα δείξω ότι $d = \mu\kappa\delta(a, b)$.

Από τον ορισμό του A, $d > 0$ και $d = sa + tb$ για κάποιους $s, t \in \mathbb{Z}$. Από το Λήμμα 2.1.2, κάθε κοινός διαιρέτης των a, b διαιρεί και τον d. Μένει να δείξω $d|a$ και $d|b$. Από τον αλγόριθμο διαίρεσης, υπάρχουν $q, r \in \mathbb{Z}$ με $a = qd + r$ και $0 \leq r < d$. Αν $r > 0$, τότε ο $r = a - qd = (1 - qs)a + (-qt)b$ θα ήταν στοιχείο του A μικρότερο από το d! Έπεται ότι $r = 0$ και $d|a$. Ομοίως, $d|b$. □

Όταν ο $\mu\kappa\delta(a, b) = 1$, οι a, b λέγονται **σχετικά πρώτοι**.

Θεώρημα 2.1.4 *a, b είναι σχετικά πρώτοι αν και μόνον αν $sa + tb = 1$ για κάποιους $s, t \in \mathbb{Z}$.*

*Απόδειξη:*2.1.4 Αν a, b είναι σχετικά πρώτοι, από το Θεώρημα 2.1.3, $\mu\kappa\delta(a, b) = 1 = sa + tb$ για κάποιους $s, t \in \mathbb{Z}$. Αντίστροφα, ας υποθέσουμε ότι $sa + tb = 1$ για κάποιους $s, t \in \mathbb{Z}$. Έστω $d = \mu\kappa\delta(a, b)$. Ο d διαιρεί τους a, b. Από το Λήμμα 2.1.2, ο d διαιρεί και τον $sa + tb = 1$. Μα τότε ο $d = \pm 1$. Αφού όμως, από τον ορισμό ο $\mu\kappa\delta$ είναι πάντα θετικός, $d = 1$. Δηλαδή, $\mu\kappa\delta(a, b) = 1$. □

Ένας ακέραιος p λέγεται **πρώτος** αν $p > 1$ και οι μόνοι θετικοί διαιρέτες του p είναι οι 1 και p. Οι δέκα μικρότεροι πρώτοι είναι οι $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.

Λήμμα 2.1.5 *Κάθε ακέραιος $a > 1$ διαιρείται από ένα τουλάχιστον πρώτο.*

*Απόδειξη:*2.1.5 Το υποσύνολο $A = \{n \in \mathbb{N} : n > 1, n|a\}$ του $\mathbb{N}$ περιέχει τον a. Από την αρχή της καλής διάταξης, μπορούμε να μιλούμε για το ελάχιστο στοιχείο p του A. Προφανώς, $p|a$. Από το Λήμμα 2.1.2, ένας διαιρέτης $n > 1$ του p, διαιρεί και τον a, άρα ανήκει στο A και $n \geq p$. Συνεπώς, $n = p$ και οι μόνοι θετικοί διαιρέτες του p είναι οι $1, p$. Έτσι, ο p είναι ένας πρώτος που διαιρεί τον a. □

Θεώρημα 2.1.6 *(Ευκλείδης). Υπάρχουν άπειροι το πλήθος πρώτοι.*

*Απόδειξη:*2.1.6 Ας υποθέσουμε το αντίθετο, ότι, δηλαδή, για κάποιο $n \in \mathbb{N}$, $p_1, p_2, \ldots, p_n$ είναι όλοι οι πρώτοι. Από το Λήμμα 2.1.5, για κάποιο $i \in \{1, 2, \ldots, n\}$, ο p_i διαιρεί τον $a = 1 + p_1 p_2, \ldots p_n$. Αφού ο p_i διαιρεί και τον $p_1 p_2 \ldots p_n$, προκύπτει ότι ο p_i διαιρεί τον $1 = a - p_1 p_2 \ldots p_n$!
Συνεπώς οι πρώτοι είναι άπειροι το πλήθος. □

Λήμμα 2.1.7 *Έστω p πρώτος και $a \in \mathbb{Z}$. Τότε $p|a$ ή $\mu\kappa\delta(a, p) = 1$.*

*Απόδειξη:*2.1.7 Έστω $d = \mu\kappa\delta(a, p)$. Ο d είναι θετικός και διαιρεί τον πρώτο αριθμό p. Άρα $d = 1$ ή $d = p$. Στη δεύτερη περίπτωση, ο p, ως κοινός διαιρέτης, διαιρεί και τον a. □

Λήμμα 2.1.8 *Έστω ότι $\mu\kappa\delta(a, b) = 1$ και $a|bc$. Τότε $a|c$.*

*Απόδειξη:*2.1.8 Από το Θεώρημα 2.1.4, $sa + tb = 1$ για κάποιους $s, t \in \mathbb{Z}$. Άρα $c = (sc)a + t(bc)$, όπου $a|a$ και $a|bc$. Από το Λήμμα 2.1.2, $a|c$. □

Λήμμα 2.1.9 *Έστω ότι $p|ab$, όπου ο p είναι πρώτος. Τότε $p|a$ ή $p|b$.*

*Απόδειξη:*2.1.9 Έστω ότι p δεν διαιρεί τον a. Από το Λήμμα 2.1.7, $\mu\kappa\delta(a, p) = 1$. Τώρα από το Λήμμα 2.1.8, $p|b$. □

Λήμμα 2.1.10 *Αν ένας πρώτος p διαιρεί το γινόμενο ακεραίων αριθμών $a_1, a_2, \ldots, a_n$, τότε διαιρεί ένα απ΄ αυτούς.*

*Απόδειξη:*2.1.10 Η απόδειξη γίνεται με επαγωγή στο n. Για $n = 1$ ή 2 το αποτέλεσμα ισχύει από το Λήμμα 2.1.9. Υποθέτουμε ότι $n > 2$ και ότι το λήμμα ισχύει για το γινόμενο $n-1$ ακεραίων.

Έστω ότι $p|a_1a_2, \ldots, a_n$. Τότε ο p διαιρεί το γινόμενο του $a_1, a_2, \ldots, a_{n-1}$ με τον a_n. Από το Λήμμα 2.1.9, $p|a_1a_2, \ldots, a_{n-1}$ ή $p|a_n$. Στην πρώτη περίπτωση, από την επαγωγική υπόθεση, ο p διαιρεί ένα από τους $a_1, a_2, \ldots, a_{n-1}$. Σε κάθε περίπτωση, ο p διαιρεί ένα από τους $a_1, a_2, \ldots, a_n$, και η απόδειξη είναι πλήρης. □

Λήμμα 2.1.11 *Αν ένας πρώτος p διαιρεί το γινόμενο πρώτων p_1, p_2, $\ldots, p_n$, τότε ισούται με ένα απ΄ αυτούς.*

*Απόδειξη:*2.1.11 Από το Λήμμα 2.1.10, $p|p_i$, όπου i είναι ένας από τους $1, 2, \ldots, n$. Επειδή ο p είναι πρώτος, $p > 1$, και οι μόνοι θετικοί διαιρέτες του πρώτου p_i είναι οι $1, p_i$. Άρα $p = p_i$. □

Θεώρημα 2.1.12 [Θεμελιώδες θεώρημα της Αριθμητικής ή θεώρημα μοναδικής παραγοντοποίησης για το $\mathbb{Z}$] *Έστω $a \in \mathbb{Z}$ με $a > 1$. Τότε*

1. *ο a είναι γινόμενο πρώτων.*
2. *αν $a = p_1p_2 \ldots p_m$ και $a = q_1q_2 \ldots q_n$ είναι δύο παραστάσεις του a ως γινόμενο πρώτων, τότε $m = n$ και κάθε p_i ισούται με κάποιο q_j.*

*Απόδειξη:*2.1.12 Η απόδειξη γίνεται με επαγωγή στο a. Το αποτέλεσμα είναι προφανές αν $a = 2$ ή πιο γενικά αν ο a είναι πρώτος. Υποθέτουμε, λοιπόν, ότι το αποτέλεσμα ισχύει για όλους τους ακέραιους που είναι $< a$ και ότι ο a δεν είναι πρώτος.

1. Από το Λήμμα 2.1.5, ο a έχει κάποιο πρώτο παράγοντα p. Μα τότε $1 < \frac{a}{p} < a$ και, από την επαγωγική μας υπόθεση, ο $\frac{a}{p}$ είναι γινόμενο πρώτων. Συνεπώς και ο a είναι γινόμενο πρώτων.

2. Έστω ότι $a = p_1p_2 \ldots p_m = q_1q_2 \ldots q_n$, όπου p_i και q_i είναι πρώτοι. Από το Λήμμα 2.1.11, κάθε p_i ισούται με κάποιο q_j. Τότε ο $\frac{a}{p_1}$ έχει μια παράσταση ως γινόμενο $m-1$ πρώτων και μια ως γινόμενο $n-1$ πρώτων. Από την επαγωγική μας υπόθεση, $m - 1 = n - 1$. Συνεπώς, $m = n$.

□

Πόρισμα 2.1.13 *Κάθε ακέραιος $a > 1$ γράφεται με μοναδικό τρόπο ως $a = p_1^{k_1}p_2^{k_2} \ldots p_m^{k_m}$, όπου $p_1, p_2 \ldots, p_n$ είναι πρώτοι με $p_1 < p_2 < \ldots < p_m$ και $k_1, k_2 \ldots, k_m \in \mathbb{N}$.*

*Απόδειξη:*2.1.13 Είναι προφανές από το Θεώρημα 2.1.12 ότι ο a γράφεται στη δοθείσα μορφή. Η απόδειξη της μοναδικότητας γίνεται με επαγωγή στο a. Το αποτέλεσμα είναι προφανές αν $a = 2$ ή πιο γενικά αν ο a είναι πρώτος. Υποθέτουμε, λοιπόν, ότι το αποτέλεσμα ισχύει για όλους τους ακέραιους που είναι $< a$. Έστω ότι $a = p_1^{k_1}p_2^{k_2} \ldots p_m^{k_m} = q_1^{l_1}q_2^{l_2} \ldots q_n^{k_n}$, όπου $p_1, p_2 \ldots, p_m$ είναι πρώτοι με $p_1 <$

$p_2 < \ldots < p_n$, $k_1, k_2 \ldots, k_m \in \mathbb{N}$, $q_1, q_2 \ldots, q_n$ είναι πρώτοι με $q_1 < q_2 < \ldots < q_n$ και $l_1, l_2 \ldots, l_n \in \mathbb{N}$. Εφόσον, από το Θεώρημα 2.1.12, ο p_1 ισούται με κάποιο q_i, τότε $q_1 \leq q_i = p_1$. Ομοίως, $p_1 \leq q_1$. Άρα $p_1 = q_1$. Αν $k_1 < l_1$, εφόσον $\frac{a}{p_1^{k_1}} = p_2^{k_2} \ldots p_m^{k_m} = p_1^{l_1 - k_1} p_2^{l_2} \ldots q_n^{k_n}$, ο p_1 θα διαιρούσε ένα από τους $p_2, p_3, \ldots p_m$! Συνεπώς, $k_1 \geq l_1$ και ομοίως $l_1 \geq k_1$. Συμπεραίνουμε ότι $k_1 = l_1$ και $p_2^{k_2} \ldots p_m^{k_m} = p_2^{l_2} \ldots q_n^{k_n} < a$. Τώρα από την επαγωγική υπόθεση, $m-1 = n-1$ (άρα $m = n$) και $k_2 = l_2, \ldots, k_m = l_m$. □

Το θεώρημα 2.1.3 μας λέει ότι ο μέγιστος κοινός διαιρέτης υπάρχει. Το επόμενο θεώρημα μας λέει πως να τον βρούμε: Έστω a, b ακέραιοι με $b \neq 0$. Έστω r_1 το υπόλοιπο της διαίρεσης του a με το b, r_2 το υπόλοιπο της διαίρεσης του b με το r_1, r_3 το υπόλοιπο της διαίρεσης του r_1 με το r_2, ..., r_i το υπόλοιπο της διαίρεσης του r_{i-2} με το r_{i-1}. Σύμφωνα με το Θεώρημα 2.1.1, $|b| > r_1 > r_2 \ldots$. Άρα, κάποιο r_n είναι το τελευταίο θετικό υπόλοιπο. Τότε $r_n = \mu\kappa\delta(a, b)$.

Θεώρημα 2.1.14 *(Ευκλείδειος αλγόριθμος). Για δεδομένους ακέραιους a, b, έστω ότι υπάρχουν $q_1, q_2, \ldots, q_{n+1}, r_1, r_2, \ldots, r_n \in \mathbb{Z}$ με $r_n > 0$ και*

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\ldots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n + 0. \end{aligned}$$

Τότε $r_n = \mu\kappa\delta(a, b)$.

*Απόδειξη:*2.1.14 Από την τελευταία εξίσωση, έχουμε ότι $r_n | r_{n-1}$. Τώρα, από την προτελευταία εξίσωση και το Λήμμα 2.1.2, έχουμε ότι $r_n | r_{n-2}$. Συνεχίζοντας με τον ίδιο τρόπο, φτάνουμε στην τρίτη εξίσωση, έχοντας αποδείξει ότι $r_n | r_{n-1}$, $r_n | r_{n-2}$,..., $r_n | r_3$, $r_n | r_2$. Τώρα έπεται από την τρίτη εξίσωση ότι $r_n | r_1$, από τη δεύτερη ότι $r_n | b$ και από την πρώτη ότι $r_n | a$. Έτσι ο r_n είναι κοινός διαιρέτης των a, b.

Έστω c ένας κοινός διαιρέτης των a, b. Από την πρώτη εξίσωση και το Λήμμα 2.1.2, έχουμε ότι $c | r_1$, από τη δεύτερη εξίσωση ότι $c | r_2$, ..., και από την προτελευταία ότι $c | r_n$. Με δεδομένο ότι το $r_n > 0$, συμπεραίνουμε ότι $r_n = \mu\kappa\delta(a, b)$. □

Παραδείγματα 1. Προκειμένου να βρω τον $\mu\kappa\delta(365, 15)$, κάνοντας διαδοχικές διαιρέσεις, έχω

$$\begin{aligned} 365 &= 24 \times 15 + 5. \\ 15 &= 3 \times 5 + 0. \end{aligned}$$

Εδώ $n = 1$ και $\mu\kappa\delta(365, 15) = r_1 = 5$

Σημειώστε ότι, ως γραμμικός συνδυασμός των $365, 15$,

$$\mu\kappa\delta(365, 15) = 5 = 365 - 24 \times 15$$

Παραδείγματα 2. Για τον $\mu\kappa\delta(766, 27)$, έχουμε

$$\begin{aligned} 766 &= 28 \times 27 + 10 \\ 27 &= 2 \times 10 + 7 \\ 10 &= 1 \times 7 + 3 \\ 7 &= 2 \times 3 + 1 \\ 3 &= 3 \times 1 + 0 \end{aligned}$$

Άρα ο $\mu\kappa\delta(766, 27) = 1$. Σημειώστε ότι μπορούμε να χρησιμοποιήσουμε τις παραπάνω εξισώσεις προκειμένου να εκφράσουμε τον $\mu\kappa\delta(766, 27)$ ως γραμμικό συνδυασμό των 766 και 27:

$$\begin{aligned} 1 &= 7 - 2 \times 3 \\ &= 7 - 2 \times (10 - 1 \times 7) = 3 \times 7 - 2 \times 10 \\ &= 3 \times (27 - 2 \times 10) - 2 \times 10 = 3 \times 27 - 8 \times 10 \\ &= 3 \times 27 - 8 \times (766 - 28 \times 27) \\ &= -8 \times 766 + 227 \times 27. \end{aligned}$$

2.2 Ασκήσεις

Άσκηση 2.2.1 *Υπάρχει ο $\mu\kappa\delta(0, 0)$;*

Λύση 2.2.2 *Έστω ότι υπάρχει και ισούται με d. Τότε ο διαιρέτης $2d$ του 0 διαιρεί τον θετικό αριθμό d, και από το Λήμμα 2.1.1, $d \geq 2d$! Έπεται ότι δεν υπάρχει ο $\mu\kappa\delta(0, 0)$.*

Άσκηση 2.2.3 *Ποιος είναι ο $\mu\kappa\delta(0, a)$ για $a \neq 0$;*

Λύση 2.2.4 $\mu\kappa\delta(0, a) = |a|$.

Άσκηση 2.2.5 *Οι s, t στα Θεωρήματα 2.1.3 και 2.1.4 είναι μοναδικοί;*

Λύση 2.2.6 *Αντιπαράδειγμα:*
$\mu\kappa\delta(3, 5) = 1 = 2 \times 3 + (-1) \times 5 = (-3) \times 3 + 2 \times 5$.
Εδώ μπορούμε να έχουμε $s = 2, t = -1$ ή $s = -3, t = 2$.

Άσκηση 2.2.7 *Δείξτε ότι ο $\sqrt{2}$ είναι άρρητος.*

Λύση 2.2.8 *Ας υποθέσουμε ότι ο* $\sqrt{2}$ *είναι ρητός. Τότε* $\sqrt{2} = \frac{p}{q}$ *, όπου* p, q *είναι φυσικοί αριθμοί. Μπορούμε να υποθέσουμε ότι* $\mu\kappa\delta(p,q) = 1$*, μετά από απλοποίηση. Τώρα* $2q^2 = p^2$*, και από το Λήμμα 2.1.10, το* 2 *διαιρεί τον* p*. Έτσι* $p = 2r$ *για κάποιο ακέραιο* r*. Έπεται ότι* $2q^2 = 4r^2$*, άρα,* $q^2 = 2r^2$*, και το* 2 *διαιρεί και τον* q*, πράγμα άτοπο αφού* $\mu\kappa\delta(p,q) = 1$*. Αυτό αποδεικνύει ότι ο* $\sqrt{2}$ *είναι άρρητος.*

Άσκηση 2.2.9 *Έστω* $n \in \mathbb{N}$ *με* $\sqrt{n}$ *ρητό. Δείξτε ότι ο* n *είναι τέλειο τετράγωνο, δηλαδή, ισούται με το τετράγωνο κάποιου φυσικού αριθμού ή, ισοδύναμα,* $\sqrt{n} \in \mathbb{N}$*.*

Λύση 2.2.10 *Αυτό αποδεικνύεται με επαγωγή στο* n*. Ισχύει για* $n = 1$*. Έστω ότι ο* $n > 1$ *κι ο* $\sqrt{n}$ *είναι ρητός. Ας υποθέσουμε ότι το αποτέλεσμα ισχύει για όλους τους φυσικούς αριθμούς που είναι* $< n$*. Για κάποιους φυσικούς αριθμούς* p, q *με* $\mu\kappa\delta(p,q) = 1$*,* $\sqrt{n} = \frac{p}{q}$*, άρα* $q^2 n = p^2$*. Από το Λήμμα 2.1.10 κάθε πρώτος διαιρέτης* r *του* n *διαιρεί τον* p*, αλλά όχι και τον* q*. Από την εξίσωση* $q^2 \frac{n}{r} = \frac{p}{r} p$*, ο* r *διαιρεί τον* $q^2 \frac{n}{r}$*, άρα και τον* $\frac{n}{r}$*. Έπεται ότι ο* $\frac{n}{r^2}$ *είναι ακέραιος και ο* $\sqrt{\frac{n}{r^2}} = \frac{\sqrt{n}}{r}$ *είναι ρητός. Από την επαγωγική υπόθεση,* $\frac{\sqrt{n}}{r} \in \mathbb{N}$ *άρα και* $\sqrt{n} \in \mathbb{N}$*.*

Άσκηση 2.2.11 *Έστω* p, q *διακεκριμένοι πρώτοι. Δείξτε ότι οι*

$$\sqrt{p}, \quad \sqrt{q}, \quad \sqrt{pq}, \quad \sqrt{p} + \sqrt{q}$$

δεν είναι ρητοί.

Λύση 2.2.12 *Κανένας από τους* p, q, pq *δεν είναι τέλειο τετράγωνο. Από την Άσκηση 2.2.9, οι* $\sqrt{p}, \sqrt{q}, \sqrt{pq}$ *δεν είναι ρητοί. Τώρα, αν ο* $x = \sqrt{p} + \sqrt{q}$ *ήταν ρητός, τότε και ο* $\sqrt{pq} = \frac{1}{2}(x^2 - p - q)$ *θα ήταν ρητός. Συνεπώς, ούτε ο* $\sqrt{p} + \sqrt{q}$ *είναι ρητός.*

Άσκηση 2.2.13 *Βρείτε τον* $\mu\kappa\delta(365, 25671)$ *και εκφράστε τον ως γραμμικό συνδυασμό των* 365 *και* 25671*.*

Λύση 2.2.14

$$\begin{aligned} 25671 &= 70 \times 365 + 121 \\ 365 &= 3 \times 121 + 2 \\ 121 &= 60 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

Συνεπώς, $\mu\kappa\delta(365, 25671) = 1$*. Από τις παραπάνω εξισώσεις*

$$\begin{aligned} 1 &= 121 - 60 \times 2 \\ &= 121 - 60 \times (365 - 3 \times 121) = -60 \times 365 + 181 \times 121 \\ &= -60 \times 365 + 181 \times (25671 - 70 \times 365) \\ &= 181 \times 25671 - 12730 \times 365 \end{aligned}$$

Άσκηση 2.2.15 *Βρείτε τον* $\mu\kappa\delta(31447, 720685)$

Λύση 2.2.16

$$\begin{aligned} 720685 &= 22 \times 31447 + 28851 \\ 31447 &= 1 \times 28851 + 2596 \\ 28851 &= 11 \times 2596 + 295 \\ 2596 &= 8 \times 295 + 236 \\ 295 &= 1 \times 236 + 59 \\ 236 &= 4 \times 59 + 0 \end{aligned}$$

Συνεπώς, $\mu\kappa\delta(31447, 720685) = 59$.

Άσκηση 2.2.17 *Γράψτε το κλάσμα* $\frac{31447}{720685}$ *σε ανάγωγο μορφή.*

Λύση 2.2.18 *Διαιρώντας αριθμητή και παρονομαστή με τον*

$$\mu\kappa\delta(31447, 720685) = 59,$$

έχουμε $\frac{31447}{720685} = \frac{533}{12215}$.

Άσκηση 2.2.19 *Έστω ότι* $\mu\kappa\delta(a, b) = 1$, $a|c$ *και* $b|c$. *Δείξτε ότι* $ab|c$.

Λύση 2.2.20 *Από τα δεδομένα,* $sa + tb = 1$, $c = \lambda a$ *και* $c = \mu b$ *για κάποιους ακέραιους* s, t, λ, μ. *Έπεται ότι* $c = sac + tbc = (s\mu + t\lambda)ab$. *Άρα,* $ab|c$.

2.3 Ισοτιμία modulo n

Έστω n ένας συγκεκριμένος φυσικός αριθμός. Στο $\mathbb{Z}$ ορίζεται μια σχέση $\sim$ ως εξής:

$$x \sim y \Leftrightarrow n|(x - y).$$

Πρόταση 2.3.1 *Η σχέση* $\sim$ *είναι σχέση ισοδυναμίας.*

*Απόδειξη:*2.3.1 Για όλους τους ακέραιους, x, y, z, χρησιμοποιώντας τον ορισμό της $\sim$ και το Λήμμα 2.1.2,

1. $n|(x - x)$ γιατί $x - x = 0$. Άρα, $x \sim x$ και η $\sim$ είναι ανακλαστική.
2. $x \sim y \Rightarrow n|(x - y) \Rightarrow n|(y - x)$ γιατί $y - x = -(x - y) \Rightarrow y \sim x$. Άρα, η $\sim$ είναι συμμετρική.
3. $x \sim y, y \sim z \Rightarrow n|(x - y), n|(y - z) \Rightarrow n|(x - z)$ αφού $x - z = (x - y) + (y - z) \Rightarrow x \sim z$. Άρα, η $\sim$ είναι μεταβατική.

   Από τα $(1), (2), (3)$, η $\sim$ είναι σχέση ισοδυναμίας.

□

Η $\sim$ λέγεται η σχέση **ισοτιμίας modulo n** και οι κλάσεις ισοδυναμίας ως προς $\sim$ λέγονται κλάσεις **ισοτιμίας modulo n**. Όλοι οι ακέραιοι σχετίζονται modulo 1, ώστε η κλάση ισοτιμίας modulo 1 κάθε ακεραίου είναι το $\mathbb{Z}$. Η σχέση *ισοτιμίας modulo 2* ταυτίζεται με την σχέση της Άσκησης 1.8.13. Έχει δε δύο διακεκριμένες κλάσεις ισοδυναμίας, την $[0]$, που αποτελείται από τους ζυγούς αριθμούς, και την $[1]$, που αποτελείται από τους μονούς αριθμούς.

Πρόταση 2.3.2 *Έστω $[x]$ κλάση ισοτιμίας modulo n ακεραίου x. Τότε*

$$[x] = \{x + kn : k \in \mathbb{Z}\}$$

*Απόδειξη:*2.3.2 Από τον ορισμό της ισοδυναμίας modulo n, $\sim$, και την Πρόταση 1.7.1, $y \in [x] \Leftrightarrow y \sim x \Leftrightarrow n|(y-x) \Leftrightarrow y - x = kn$ για κάποιο $k \in \mathbb{Z} \Leftrightarrow y = x + kn$ για κάποιο $k \in \mathbb{Z}$. □

Αξίζει να σημειωθεί ότι η κλάση $[0]$ περιέχει ακριβώς όλα τα πολλαπλάσια του n. Συνεπώς, $[m] = [0]$ ακριβώς όταν $n|m$.

Πρόταση 2.3.3 *Υπάρχουν ακριβώς n διακεκριμένες κλάσεις ισοτιμίας modulo n, οι $[0], [1], \ldots, [n-1]$.*

*Απόδειξη:*2.3.3 Δεδομένου ακεραίου x, από τον αλγόριθμο διαίρεσης, $x = kn + r$, όπου $k, r \in \mathbb{Z}$ και $0 \leq r < n$. Μα τότε $x \sim r$, και από την Πρόταση 1.7.1, $[x] = [r]$, όπου $r = 0, 1, \ldots,$ ή $n-1$. Αυτό σημαίνει ότι κάθε κλάση ισοτιμίας modulo n ισούται με μια από τις $[0], [1], \ldots, [n-1]$. Μένει να δείξουμε ότι αυτές είναι διακεκριμένες. Όποιες δύο απ' αυτές παριστάνονται ως $[r_1], [r_2]$, όπου $0 \leq r_1 < r_2 < n$. Αν $[r_1] = [r_2]$, από την Πρόταση 1.7.1, $r_1 \sim r_2$. Αυτό συνεπάγεται το άτοπο συμπέρασμα ότι ο n διαιρεί τον ακέραιο $r_2 - r_1$ που ικανοποιεί $0 < r_2 - r_1 < n$. Συνεπώς, οι κλάσεις $[0], [1], \ldots, [n-1]$ είναι διακεκριμένες. □

Το σύνολο όλων των κλάσεων ισοτιμίας modulo n συμβολίζεται με $\mathbb{Z}_n$. Από την Πρόταση 2.3.3

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

Είναι χρήσιμο να σημειωθεί ότι $[x] = [r]$, όπου $0 \leq r \leq n-1$ αν και μόνον αν το υπόλοιπο της διαίρεσης του x με το n είναι ο r.

Κεφάλαιο 3

Ομάδες

3.1 Πράξεις

Ορισμός 3.1.1 *Μια πράξη $*$ σε ένα σύνολο S είναι ένας κανόνας ο οποίος σε κάθε διατεταγμένο ζεύγος (a, b) μελών a, b του S αντιστοιχίζει ένα και μοναδικό στοιχείο του S. Το στοιχείο που η $*$ αντιστοιχίζει στο διατεταγμένο ζεύγος (a, b) συμβολίζεται με $a * b$.*

Οι πιο γνωστές πράξεις είναι οι πράξεις της πρόσθεσης, $+$, και του πολλαπλασιασμού, $\cdot$, στα σύνολα $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ή $\mathbb{C}$. Δεν είναι όμως πράξεις, με την έννοια του Ορισμού 3.1.1, σε κάθε σύνολο αριθμών. Π.χ. η $+$ δεν είναι πράξη, στο σύνολο $S = \{2n + 1 : n \in \mathbb{N}\}$ γιατί π.χ. $3 + 5 \notin \mathbb{S}$ παρότι $3, 5 \in \mathbb{S}$. Ομοίως, ο $\cdot$ δεν είναι πράξη στο σύνολο των αρνητικών αριθμών.

Ορισμός 3.1.2 *Μια πράξη $*$ σε ένα σύνολο S λέγεται*

1. *προσεταιριστική αν $a * (b * c) = (a * b) * c$ για όλα τα μέλη a, b, c του S, και*
2. *μεταθετική αν $a * b = b * a$ για όλα τα μέλη a, b του S.*

Οι $+$ και $\cdot$, στα σύνολα αριθμών όπου είναι πράξεις, είναι προσεταιριστικές και μεταθετικές. Η προσεταιριστικότητα είναι μια πολύ χρήσιμη ιδιότητα. Μας εξασφαλίζει ότι στην πρόσθεση (αντίστοιχα, πολλαπλασιασμό) 3 αριθμών x, y, z δεν έχει σημασία πως τοποθετούνται οι παρενθέσεις και το αποτέλεσμα μπορεί απλά να γραφεί ως $x + y + z$ (αντίστοιχα, xyz). Πράξεις που δεν είναι προσεταιριστικές δεν έχουν αλγεβρικό ενδιαφέρον. Υπάρχουν, όμως, ενδιαφέρουσες πράξεις που δεν είναι μεταθετικές.

Ορισμός 3.1.3 *Έστω $*$ μια πράξη σε ένα σύνολο S. Ένα στοιχείο e του S λέγεται ταυτοτικό (ή ουδέτερο) στοιχείο της $*$ αν $e * a = a$ και $a * e = a$ για κάθε μέλος a του S.*

Είναι προφανές ότι αν η πράξη $*$ στο S είναι μεταθετική, για να δείξουμε ότι το e είναι ταυτοτικό στοιχείο, αρκεί να δείξουμε ότι, για κάθε μέλος $a \in S$, ισχύει

μια από τις ισότητες $e * a = a$, $a * e = a$.

Στα σύνολα $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ή $\mathbb{C}$, η $+$ έχει το 0 ως ταυτοτικό στοιχείο, ο δε $\cdot$ έχει το 1. Το $\mathbb{N}$ έχει ταυτοτικό ως προς $\cdot$, όχι όμως ως προς $+$.

Πρόταση 3.1.4 *Το ταυτοτικό στοιχείο μιας πράξης $*$ σε ένα σύνολο S, αν υπάρχει, είναι μοναδικό.*

*Απόδειξη:*3.1.4 Ας υποθέσουμε ότι το S περιέχει στοιχεία e_1, e_2 που είναι ταυτοτικά, δηλαδή, έχουν τις ιδιότητες που απαιτεί ο Ορισμός 3.1.3. Τότε

1. $e_1 * e_2 = e_2$ γιατί το e_1 είναι ταυτοτικό, και

2. $e_1 * e_2 = e_1$ γιατί το e_2 είναι ταυτοτικό.

Από τις (1) και (2), $e_1 = e_2$. □

Ορισμός 3.1.5 *Έστω $*$ μια πράξη σε ένα σύνολο S με ταυτοτικό στοιχείο e. Έστω $a, b \in S$. Αν $a * b = e$ και $b * a = e$, τότε το b λέγεται (ένα) αντίστροφο στοιχείο του a.*

Προφανώς, σε ένα σύνολο S με ταυτοτικό στοιχείο e, το e έχει ως αντίστροφο στοιχείο το e, και το b είναι αντίστροφο του a αν και μόνον αν το a είναι αντίστροφο του b. Επίσης, αν η πράξη $*$ στο S είναι μεταθετική, για να δείξουμε ότι το b είναι αντίστροφο του a, αρκεί να δείξουμε μια από τις ισότητες $a*b = e$, $b*a = e$.

Στα σύνολα $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ή $\mathbb{C}$, με την έννοια του Ορισμού 3.1.5, αντίστροφο στοιχείου x ως προς την $+$ είναι το $-x$, και ως προς τον $\cdot$ είναι το $\frac{1}{x}$, αν $x \neq 0$. Το 0 δεν έχει αντίστροφο ως προς τον $\cdot$. Το $\mathbb{N}$, ως προς τον $\cdot$ έχει ταυτοτικό στοιχείο το 1, κανένα όμως στοιχείο του $\mathbb{N}$ πλην του 1 δεν έχει αντίστροφο.

Πρόταση 3.1.6 *Έστω S ένα σύνολο εφοδιασμένο με μια προσεταιριστική πράξη $*$ η οποία έχει ταυτοτικό στοιχείο e. Τότε το αντίστροφο ενός στοιχείου a του S, αν υπάρχει, είναι μοναδικό.*

*Απόδειξη:*3.1.6 Ας υποθέσουμε ότι το S περιέχει στοιχεία b_1, b_2 που είναι αντίστροφα του a, δηλαδή, έχουν τις ιδιότητες που απαιτεί ο Ορισμός 3.1.5. Τότε

1. $b_1 * (a * b_2)$
   $= b_1 * e$ γιατί το b_2 είναι αντίστροφο του a
   $= b_1$ γιατί το e είναι ταυτοτικό, και

2. $(b_1 * a) * b_2$
   $= e * b_2$ γιατί το b_1 είναι αντίστροφο του a
   $= b_2$ γιατί το e είναι ταυτοτικό.

Επειδή όμως η $*$ είναι προσεταιριστική, $b_1 * (a * b_2) = (b_1 * a) * b_2$. Έπεται από τις (1) και (2), ότι $b_1 = b_2$. □

Έστω S ένα σύνολο εφοδιασμένο με μια πράξη $*$. Το στοιχείο $a_1 * a_2$, όπου $a_1, a_2 \in S$, συνήθως καλείται το γινόμενο των a_1, a_2, ως προς την $*$. Σε τρία στοιχεία a_1, a_2, a_3 του S, με την συγκεκριμένη διάταξη, αντιστοιχούν τα γινόμενα $a_1 * (a_2 * a_3)$ και $(a_1 * a_2) * a_3$, τα οποία είναι ίσα όταν η $*$ είναι προσεταιριστική. Σε περισσότερα στοιχεία αντιστοιχούν διάφορα γινόμενα, ανάλογα με τον τρόπο που τοποθετούνται οι παρενθέσεις. Κάθε γινόμενο στοιχείων $a_1, a_2, \ldots, a_n \in S$ ισούται με ένα γινόμενο $A * B$, όπου για κάποιο $1 \leq i < n$, το A είναι ένα γινόμενο των $a_1, a_2, \ldots, a_i$ και το B είναι ένα γινόμενο των $a_{i+1}, a_{i+2}, \ldots, a_n$.

Πρόταση 3.1.7 *Έστω S ένα σύνολο εφοδιασμένο με μια προσεταιριστική πράξη $*$ και $a_1, a_2, \ldots, a_n \in S$. Τότε όλα τα γινόμενα των $a_1, a_2, \ldots, a_n$ είναι ίσα.*

*Απόδειξη:*3.1.7 Η απόδειξη είναι με επαγωγή στο n. Το αποτέλεσμα ισχύει για γινόμενα ≤ 3 στοιχείων. Ας υποθέσουμε $n \geq 3$ και ότι όλα τα γινόμενα $n-1$ στοιχείων είναι ίσα. Ένα γινόμενο Γ των $a_1, a_2, \ldots, a_n$ ισούται με $A * B$, όπου για κάποιο $1 \leq i < n$, το A είναι ένα γινόμενο των $a_1, a_2, \ldots, a_i$ και το B είναι ένα γινόμενο των $a_{i+1}, a_{i+2}, \ldots, a_n$. Θα δείξω ότι $\Gamma = D * a_n$, όπου το D είναι ένα γινόμενο των $a_1, a_2, \ldots, a_{n-1}$. Αυτό είναι προφανές όταν $i = n-1$. Αν $i < n-1$, από την επαγωγική υπόθεση, $B = C * a_n$, όπου το C είναι ένα γινόμενο των $a_{i+1}, a_{i+2}, \ldots, a_{n-1}$. Από την προσεταιριστικότητα της $*$, $\Gamma = A * B = A * (C * a_n) = (A * C) * a_n$, και μπορώ να θέσω $D = A * C$.

Θεωρώ τώρα δύο γινόμενα Γ_1, Γ_2 των $a_1, a_2, \ldots, a_n$. Από την προηγούμενη παράγραφο, $\Gamma_1 = D_1 * a_n$ και $\Gamma_2 = D_2 * a_n$, όπου τα D_1, D_2 είναι γινόμενα των $a_1, a_2, \ldots, a_{n-1}$. Από την επαγωγική υπόθεση, $D_1 = D_2$. Άρα και $\Gamma_1 = \Gamma_2$. □

Έστω S ένα σύνολο εφοδιασμένο με μια προσεταιριστική πράξη $*$. Από την Πρόταση 3.1.7, δεν έχει καμία σημασία πως τοποθετούνται οι παρενθέσεις στα γινόμενα πεπερασμένων το πλήθος στοιχείων. Έτσι, το γινόμενο στοιχείων $a_1, a_2, \ldots, a_n$ του S είναι μονοσήμαντα ορισμένο και συνήθως συμβολίζεται απλά με $a_1 * a_2 * \ldots * a_n$.

Για παιδαγωγικούς λόγους αποφεύγουμε την χρήση της Πρότασης 3.1.7 στις αμέσως επόμενες ενότητες.

3.2 Ασκήσεις

Άσκηση 3.2.1 *Η πράξη $*$ στο $\mathbb{Q}$ ορίζεται με $x * y = x - y$*
Είναι η $*$ προσεταιριστική ή μεταθετική; Έχει ταυτοτικό στοιχείο;

Λύση 3.2.2 $1 * (1 * 1) = 1 * 0 = 1 \neq -1 = 0 * 1 = (1 * 1) * 1$. *Άρα η $*$ δεν είναι προσεταιριστική.*
$1 * 2 = -1 \neq 1 = 2 * 1$. *Άρα η $*$ δεν είναι μεταθετική.*
Έστω ότι υπάρχει ταυτοτικό στοιχείο e στο $\mathbb{Q}$. Τότε

1. $1 = 1 * e = 1 - e \Rightarrow e = 0$

2. $1 = e * 1 = e - 1 \Rightarrow e = 2$!

Συνεπώς, η $*$ δεν έχει ταυτοτικό στοιχείο.

Άσκηση 3.2.3 *Η πράξη $*$ στο $\mathbb{Z}$ ορίζεται με $x * y = 2x + 3y$.*
Είναι η $*$ προσεταιριστική ή μεταθετική; Έχει ταυτοτικό στοιχείο;

Λύση 3.2.4 $0 * (1 * 1) = 0 * 5 = 15$ *ενώ* $(0 * 1) * 1 = 3 * 1 = 9$. *Άρα η $*$ δεν είναι προσεταιριστική.*
$0 * 1 = 3 \neq 2 = 1 * 0$. *Άρα η $*$ δεν είναι μεταθετική.*

Αν e είναι ταυτοτικό στοιχείο, τότε $1 = 1 * e = 2 + 3e \Rightarrow 3e = -1$, αδύνατο για $e \in \mathbb{Z}$. Άρα η $*$ δεν έχει ταυτοτικό στοιχείο.

Άσκηση 3.2.5 *Η πράξη $*$ στο $\mathbb{Q}$ ορίζεται με $x * y = 3xy$.*
Είναι η $*$ προσεταιριστική ή μεταθετική; Έχει ταυτοτικό στοιχείο; Ποια στοιχεία έχουν αντίστροφο;

Λύση 3.2.6 *Είναι προφανές ότι η $*$ είναι μεταθετική γιατί ο πολλαπλασιασμός αριθμών είναι μεταθετική πράξη.*
$x * (y * z) = x * (3yz) = 9xyz = (3xy) * z = (x * y) * z$. *Άρα η $*$ είναι και προσεταιριστική.*
Αν ένας ρητός e είναι ταυτοτικό στοιχείο, τότε $1 = 1 * e = 3e \Rightarrow e = \frac{1}{3}$. Όντως, $\frac{1}{3} \in \mathbb{Q}$ και για κάθε $x \in \mathbb{Q}$, $x * \frac{1}{3} = x = \frac{1}{3} * x$.
Συνεπώς, η $*$ έχει το $\frac{1}{3}$ ως ταυτοτικό στοιχείο.
Εύκολα προκύπτει ότι το 0 δεν έχει αντίστροφο, αλλά κάθε ρητός $x \neq 0$ έχει τον $\frac{1}{9x} \in \mathbb{Q}$ ως αντίστροφο.

Άσκηση 3.2.7 *Έστω $*$ μια προσεταιριστική πράξη σε ένα σύνολο S και a, b, c, d στοιχεία του S.*
Πόσα γινόμενα αντιστοιχούν στα στοιχεία a, b, c, d, με την συγκεκριμένη διάταξη; Δείξτε ότι όλα αυτά τα γινόμενα είναι ίσα, χωρίς να χρησιμοποιήσετε την Πρόταση 3.1.7.

Λύση 3.2.8 *Γράφοντας το γινόμενο στην μορφή $A * B$, υπάρχουν οι εξής περιπτώσεις για το A.*

1. *$A = a$, οπότε προκύπτουν τα γινόμενα $a * ((b * c) * d)$ και $a * (b * (c * d))$, που είναι ίσα λόγω προσεταιριστικότητας.*

2. *$A = a * b$, οπότε προκύπτει μόνο το $(a * b) * (c * d)$, το οποίο λόγω προσεταιριστικότητας ισούται με $a * (b * (c * d))$ και με $((a * b) * c) * d$.*

3. *Το A είναι γινόμενο των a, b, c, οπότε προκύπτουν τα γινόμενα $((a * b) * c) * d$ και $(a * (b * c)) * d$, που είναι ίσα λόγω προσεταιριστικότητας.*

Από τα παραπάνω,τα 5 γινόμενα είναι ίσα.

3.3 Ομάδες

Ορισμός 3.3.1 *Μια ομάδα $(G, *)$ αποτελείται από ένα σύνολο G εφοδιασμένο με μια πράξη $*$ η οποία ικανοποιεί τα τρία αξιώματα:*

1. *η $*$ είναι προσεταιριστική στο G*
2. *το G περιέχει ένα στοιχείο που είναι ταυτοτικό στοιχείο ως προς την $*$, και*
3. *για κάθε $a \in G$, το G περιέχει ένα στοιχείο που είναι αντίστροφο του a ως προς την $*$.*

Από την Προτάση 3.1.4, το ταυτοτικό στοιχείο μιας ομάδας είναι μοναδικό. Συνήθως αυτό συμβολίζεται με e.
Από την Προτάση 3.1.6, το αντίστροφο δοθέντος στοιχείου a μιας ομάδας είναι μοναδικό. Συνήθως αυτό συμβολίζεται με a'. Είναι προφανές από τον Ορισμό 3.1.5 ότι $(a')' = a$.

Παρατήρηση 3.3.2 *Λέμε «το $(G, *)$ είναι ομάδα » ή «το G είναι ομάδα ως προς την $*$» ή απλά, όταν δεν χρειάζεται να αναφερθεί η πράξη, «το G είναι ομάδα».*

Παραδείγματα 1. Κάθε ένα από τα σύνολα $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ εφοδιασμένο με την πρόσθεση $(+)$ είναι ομάδα. Ταυτοτικό είναι το 0 και το αντίστροφο του x είναι το $-x$.

Το $(\mathbb{N}, +)$ δεν είναι ομάδα γιατί δεν ικανοποιείται το τρίτο αξίωμα του ορισμού. Το $(\mathbb{R}, .)$ δεν είναι ομάδα γιατί το 0 δεν έχει αντίστροφο, γίνεται όμως ομάδα αν αφαιρέσουμε το 0.

Συμβολισμοί. Αν A είναι ένα σύνολο αριθμών, το σύνολο $A \setminus \{0\}$ θα συμβολίζεται με A^*.
Αν A είναι πραγματικών αριθμών A, το σύνολο $\{x \in A : x > 0\}$ θα συμβολίζεται με A^+.

Παραδείγματα 2. Τα σύνολα $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*, \mathbb{Q}^+, \mathbb{R}^+$ αποτελούν ομάδα ως προς το πολλαπλασιασμό $(\cdot)$. Ταυτοτικό είναι το 1 και το αντίστροφο του x το $\frac{1}{x}$.

Ορισμός 3.3.3 *Μια ομάδα λέγεται αβελιανή αν η πράξη της είναι μεταθετική.*

Στα Παραδείγματα 1 και 2 όλες οι ομάδες είναι αβελιανές.

Θεώρημα 3.3.4 *Σε μια ομάδα $(G, *)$, ισχύουν :*

1. *$a * b = a * c \Rightarrow b = c$. (Αριστερός νόμος διαγραφής ή απλοποίησης).*
2. *$b * a = c * a \Rightarrow b = c$. (Δεξιός νόμος διαγραφής ή απλοποίησης).*

*Απόδειξη:*3.3.4

1. $a * b = a * c \Rightarrow$
   $a' * (a * b) = a' * (a * c) \Rightarrow$ (λόγω προσεταιριστικότητας της $*$)
   $(a' * a) * b = (a' * a) * c \Rightarrow$(επειδή το a' είναι το αντίστροφο του a)
   $e * b = e * c \Rightarrow$ (επειδή το e είναι ταυτοτικό στοιχείο)
   $b = c$.

2. $b * a = c * a \Rightarrow$
   $(b * a) * a' = (c * a) * a' \Rightarrow$ (λόγω προσεταιριστικότητας της $*$)
   $b * (a * a') = c * (a * a') \Rightarrow$ (επειδή το a' είναι το αντίστροφο του a)
   $b * e = c * e \Rightarrow$ (επειδή το e είναι ταυτοτικό στοιχείο)
   $b = c$.

□

Πόρισμα 3.3.5 *Σε κάθε ομάδα, $a * b = e \Rightarrow b = a', a = b'$.*

*Απόδειξη:*3.3.5 Έστω ότι $a * b = e$. Τότε $a * b = a * a'$ και, από τον αριστερό νόμο διαγραφής, $b = a'$. Συνεπώς, $b' = (a')' = a$. □

Πόρισμα 3.3.6 *Για όλα τα μέλη a, b μιας ομάδας $(G, *)$, $(a * b)' = b' * a'$.*

*Απόδειξη:*3.3.6 Χρησιμοποιώντας δύο φορές την προσεταιριστικότητα της $*$

$$(a * b) * (b' * a') = ((a * b) * b') * a' = (a * (b * b')) * a' = (a * e) * a' = a * a' = e$$

Έπεται από το Πόρισμα 3.3.5 ότι το $b' * a'$ είναι το αντίστροφο του $a * b$. □

Θεώρημα 3.3.7 *Σε μια ομάδα $(G, *)$, για κάθε $a, b \in G$, κάθε μια από τις γραμμικές εξισώσεις $a * x = b$ και $x * a = b$ έχει μοναδική λύση.*

*Απόδειξη:*3.3.7 Το $a' * b$ είναι μια λύση της $a * x = b$ γιατι, λόγω προσεταιριστικότητας της $*$,

$$a * (a' * b) = (a * a') * b = e * b = b.$$

Αντίστροφα, αν x είναι οποιαδήποτε λύση της $a * x = b$, τότε $a * x = a * (a' * b)$.
Τώρα από τον αριστερό κανόνα απαλοιφής, $x = a' * b$.
Έτσι το $a' * b$ αποτελεί μοναδική λύση της $a * x = b$ στην G.
Με παρόμοιο τρόπο αποδεικνύεται ότι η $x * a = b$ έχει μοναδική λύση το στοιχείο $b * a'$ της G. □

3.4 Ασκήσεις

Άσκηση 3.4.1 *Στο $\mathbb{R}^+$ η $*$ ορίζεται μέσω της $x * y = 5xy$.*
Δείξτε ότι το ζεύγος $(\mathbb{R}^+, *)$ είναι ομάδα.
Βρείτε ολες τις λύσεις των

1. $4 * x = 100$,
2. $4 * (x * 1) = 100$,
3. $(x * 5) * x = 500$.

Λύση 3.4.2 *Εύκολα αποδεικνύεται ότι το* $(\mathbb{R}^+, *)$ *είναι αβελιανή ομάδα με ταυτοτικό στοιχείο το* $\frac{1}{5}$ *και αντίστροφο του* $x \in \mathbb{R}^+$ *το* $\frac{1}{25x}$ *(βλέπε Άσκηση 3.2.5).*

1. $4 * x = 100 \Leftrightarrow 20x = 100 \Leftrightarrow x = 5$.
   Διαφορετικά, από το Θεώρημα 3.3.7, $x = 4' * 100 = \frac{1}{100} * 100 = 5$.
2. $4 * (x * 1) = 100 \Leftrightarrow 4 * (x * 1) = 4 * 5x = 100x = 100 \Leftrightarrow x = 1$
3. $(x * 5) * x = 500 \Leftrightarrow 125x^2 = 500 \Leftrightarrow x^2 = 4 \Leftrightarrow x = 2$.

Άσκηση 3.4.3 *Δείξτε ότι στο* $\mathbb{R} \setminus \{1\}$ *ορίζεται μια πράξη* $*$ *μέσω της* $x * y = xy - x - y + 2$.
Στη συνέχεια δείξτε ότι το $(\mathbb{R} \setminus \{1\}, *)$ *είναι αβελιανή ομάδα.*
Λύστε την εξίσωση $4 * (5 * x) = 13$.

Λύση 3.4.4 *Παρατηρώ ότι* $x * y = (x-1)(y-1)+1$. *Έτσι* $x * y \neq 1$ *όταν* $x \neq 1$ *και* $y \neq 1$, *και η* $*$ *όντως είναι πράξη στο* $\mathbb{R} \setminus \{1\}$.
$H *$ *είναι προφανώς μεταθετική.*
Προσεταιριστικότητα: $(x*y)*z = ((x-1)(y-1)+1)*z = (x-1)(y-1)(z-1)+1 = x * ((y-1)(z-1)+1) = x * (y * z)$.
Το 2 *είναι ταυτοτικό στοιχείο:* $2 * x = x * 2 = (x-1)(2-1)+1 = x$.
Αντίστροφο του $x \in \mathbb{R} \setminus \{1\}$*:* $x * y = (x-1)(y-1)+1 = 2 \Leftrightarrow y = \frac{x}{x-1} \in \mathbb{R} \setminus \{1\}$.
Έτσι στο $\in \mathbb{R} \setminus \{1\}$, *κάθε στοιχείο* x *έχει αντίστροφο το* $\frac{x}{x-1}$.
Συνεπώς, το $(\mathbb{R} \setminus \{1\}, *)$ *είναι αβελιανή ομάδα.*

$$4 * (5 * x) = 13 \Leftrightarrow (4-1)(5-1)(x-1)+1 = 13 \Leftrightarrow x - 1 = 1 \Leftrightarrow x = 2.$$

Άσκηση 3.4.5 *Έστω* $*$ *μια προσεταιριστική πράξη σε ένα σύνολο* G *τέτοια ώστε*

- *το* G *περιέχει ένα στοιχείο* e *που ικανοποιεί* $e * x = x$ *για κάθε* $x \in G$
  (ένα τέτοιο e *λέγεται αριστερό ταυτοτικό στοιχείο)*
- *για κάθε* $x \in G$, *υπάρχει* $x' \in G$ *τέτοιο ώστε* $x' * x = e$
  (ένα τέτοιο x' *λέγεται αριστερό αντίστροφο του* x*).*

Να δείξετε ότι για κάθε $a, b, c \in G$,

1. $a * b = a * c \Rightarrow b = c$,
2. $a * e = a$,
3. $a * a' = e$.

Συνεπώς, το $(G,*)$ αποτελεί ομάδα.

Λύση 3.4.6 *Χρησιμοποιώντας την προσεταιριστικότητα της $*$ και τις ιδιότητες του αριστερού αντιστρόφου και του αριστερού ταυτοτικού στοιχείου,*

1. $a*b=a*c \Rightarrow a'*(a*b)=a'*(a*c) \Rightarrow$
   $(a'*a)*b=(a'*a)*c \Rightarrow e*b=e*c \Rightarrow b=c.$
2. $a'*(a*e)=(a'*a)*e=e*e=e.$
   Έτσι $a'*(a*e)=a'*a$, και η (1) συνεπάγεται ότι $a*e=a$.
3. $a'*(a*a')=(a'*a)*a'=e*a'=a'.$
   Από την (2), $a'=a'*e$. Άρα $a'*(a*a')=a'*e$ και η (1) συνεπάγεται ότι $a*a'=e$.

Άσκηση 3.4.7 *Διατυπώστε μια πρόταση για δεξιό ταυτοτικό και δεξιό αντίστροφο ανάλογη της Άσκησης 3.4.5.*

Λύση 3.4.8 *Έστω G ένα σύνολο εφοδιασμένο με μια προσεταιριστική πράξη $*$ τέτοια ώστε*

1. *$x*e=e$ για κάποιο $e\in G$ και για κάθε $x\in G$,*
2. *για κάθε $x\in G$, υπάρχει $x'\in G$ με $x*x'=e$.*

   Τότε το $(G,*)$ είναι ομάδα.

Άσκηση 3.4.9 *Στο $\mathbb{R}^*$ η $*$ ορίζεται μέσω της $a*b=a|b|$.*
Εξετάστε αν η $*$ είναι μεταθετική ή προσεταιριστική.
Έχει δεξιό ή αριστερό ταυτοτικό στοιχείο;
Έχει ταυτοτικό στοιχείο;
Είναι η $(\mathbb{R}^*,*)$ ομάδα;

Λύση 3.4.10 *Η $*$ είναι προσεταιριστική:*
$(a*b)*c=(a|b|)*c=(a|b|)|c|=a(|b||c|)=a(|(b|c|)|)=a*(b*c)$.
Η $*$ δεν είναι μεταθετική: $(-1)*1=-1\neq 1=1*(-1)$.
Ταυτοτικό στοιχείο: Αν το e είναι ταυτοτικό στοιχείο, τότε $e*1=1$, δηλ. $e=1$.
Όμως, το 1 δεν είναι ταυτοτικό στοιχείο γιατί δεν είναι αριστερό ταυτοτικό στοιχείο ($1*(-1)=1\neq -1$) παρότι το 1 είναι δεξιό ταυτοτικό στοιχείο ($a*1=a$). Άρα η $(\mathbb{R}^*,*)$ δεν είναι ομάδα.
Σημειώστε ότι τα αρνητικά μέλη a δεν έχουν δεξιό αντίστροφο: $a*b=a|b|\neq 1$ για κάθε b παρότι $\frac{1}{|a|}*a=1$.

Άσκηση 3.4.11 *Βρείτε όλες τις λύσεις τις $x*x=x$ σε μια ομάδα $(G,*)$.*

Λύση 3.4.12 *Από το δεξιό νόμο διαγραφής σε ομάδα,*
$x*x=x \Leftrightarrow x*x=e*x \Leftrightarrow x=e$.

Άσκηση 3.4.13 *Αν για όλα τα μέλη a,b μιας ομάδας $(G,*)$ ισχύει ότι $(a*b)'=a'*b'$, δείξτε ότι η G είναι αβελιανή.*

Λύση 3.4.14 *Έστω ότι* $(a*b)' = a'*b'$. *Τότε* $e = (a*b)*(a'*b')$ *και χρησιμοποιώντας επανειλημμένα την προσεταιριστικότητα της* $*$
$b*a = e*(b*a) = ((a*b)*(a'*b'))*(b*a) = (((a*b)*(a'*b'))*b)*a =$
$((a*b)*((a'*b')*b))*a = ((a*b)*(a'*(b'*b)))*a = ((a*b)*(a'*e))*a =$
$((a*b)*a')*a = (a*b)*(a'*a) = (a*b)*e = a*b.$

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

Θυμίζουμε ότι, για κάθε $n \in \mathbb{N}$, $\mathbb{Z}_n = \{[x] : x \in \mathbb{Z}\}$, όπου $[x]$ είναι η κλάση ισοτιμίας modulo n του ακεραίου x.
Στο $\mathbb{Z}_n$ ορίζουμε την πράξη της πρόσθεσης $\oplus$ ως εξής:

$$[x] \oplus [y] = [x+y],$$

όπου $+$ συμβολίζει την πρόσθεση ακεραίων.

Προκύπτει το ερώτημα κατά πόσον η $\oplus$ όπως ορίστηκε παραπάνω είναι καλά ορισμένη: Η κλάση $[x+y]$ εξαρτάται μόνο από τις κλάσεις $[x]$ και $[y]$ ή παίζουν κάποιο ρόλο οι συγκεκριμένοι αντιπρόσωποι x και y των δύο κλάσεων; Ας υποθέσουμε ότι $[x_1] = [x_2]$ και $[y_1] = [y_2]$. Αυτό σημαίνει ότι ο n διαιρεί τους $x_1 - x_2$ και $y_1 - y_2$. Άρα, ο n διαιρεί και τον $(x_1+y_1)-(x_2+y_2) = (x_1-x_2)+(y_1-y_2)$. Συνεπώς, $[x_1+y_1] = [x_2+y_2]$, και η $\oplus$ είναι καλά ορισμένη.

Θεώρημα 3.5.1 *Το* $(\mathbb{Z}_n, \oplus)$ *είναι αβελιανή ομάδα.*

*Απόδειξη:*3.5.1 Κάθε ιδιότητα της $\oplus$ προκύπτει από την αντίστοιχη ιδιότητα της $+$ στο $\mathbb{Z}$ (και, βέβαια, από τον ορισμό της $\oplus$). Π.χ. η $\oplus$ είναι μεταθετική γιατί από τον ορισμό της $\oplus$,

$$[x] \oplus [y] = [x+y] = [y+x] = [y] \oplus [x],$$

όπου στη δεύτερη ισότητα χρησιμοποιήσαμε το γεγονός ότι $x+y = y+x$ στο $\mathbb{Z}$. Οι άλλες ισότητες είναι απλά ο ορισμός της $\oplus$. Για τις λοιπές ιδιότητες της $\oplus$ που πρέπει να επαληθεύσουμε,

1. $([x] \oplus [y]) \oplus [z] = [x+y] \oplus [z] = [(x+y)+z]$
   το οποίο λόγω προσεταιριστικότητας της $+$ ισούται με
   $[x+(y+z)] = [x] \oplus [y+z] = [x] \oplus ([y] \oplus [z])$.
   Έτσι η $\oplus$ είναι προσεταιριστική.

2. $[x] \oplus [0] = [x+0] = [x]$ γιατί στο $\mathbb{Z}$, $x+0 = x$.
   Άρα το $[0]$ είναι ταυτοτικό στοιχείο της μεταθετικής $\oplus$.

3. $[x] \oplus [-x] = [x+(-x)] = [0]$ γιατί στο $\mathbb{Z}$, $x+(-x) = 0$.
   Άρα το $[-x]$ είναι αντίστροφο του $[x]$, δηλαδή, στο $\mathbb{Z}_n$, κάθε στοιχείο έχει αντίστροφο.

□

Ο πολλαπλασιασμός $\odot$ στο $\mathbb{Z}_n$ ορίζεται ως εξής:

$$[x] \odot [y] = [x \cdot y]$$

όπου $x \cdot y$ είναι το γινόμενο των ακεραίων x, y στο $\mathbb{Z}$, το οποίο συνήθως γράφεται απλά ως xy. Ο $\odot$ είναι καλά ορισμένος: Ας υποθέσουμε ότι $[x_1] = [x_2]$ και $[y_1] = [y_2]$. Αυτό σημαίνει ότι ο n διαιρεί τους $x_1 - x_2$ και $y_1 - y_2$. Άρα, ο n διαιρεί και τον $y_1 \cdot (x_1 - x_2) + x_2 \cdot (y_1 - y_2) = x_1 \cdot y_1 - x_2 \cdot y_2$. Συνεπώς, $[x_1 \cdot y_1] = [x_2 \cdot y_2]$.

Όπως με την $\oplus$, εύκολα αποδεικνύεται ότι ο $\odot$ είναι μεταθετικός, προσεταιριστικός και έχει ταυτοτικό στοιχείο το $[1]$. Το $[0]$ δεν έχει πολλαπλασιαστικό αντίστροφο όταν $n > 1$: Για οποιοδήποτε $[x] \in \mathbb{Z}_n$, $[x] \odot [0] = [x \cdot 0] = [0] \neq [1]$.

Λήμμα 3.5.2 *Στο $(\mathbb{Z}_n, \odot)$, ένα στοιχείο $[m]$ έχει αντίστροφο αν και μόνον αν $\mu\kappa\delta(m, n) = 1$.*

*Απόδειξη:*3.5.2 Έστω ότι το $[m]$ έχει αντίστροφο $[k] \in \mathbb{Z}_n$. Τότε $[k] \odot [m] = [1]$, δηλαδή, $[km] = [1]$. Αυτό σημαίνει ότι ο n διαιρεί τον $km - 1$, δηλαδή, για κάποιο ακέραιο λ, $km - 1 = \lambda n$, οπότε, $km + (-\lambda)n = 1$. Από το Θεώρημα 2.1.4, $\mu\kappa\delta(m, n) = 1$.
Αντίστροφα, αν $\mu\kappa\delta(m, n) = 1$, από το Θεώρημα 2.1.4, για κάποιους ακέραιους s, t, έχουμε $sm + tn = 1$. Τότε $[1] = [sm + tn] = [sm] \oplus [tn] = ([s] \odot [m]) \oplus ([t] \odot [n]) = ([s] \odot [m]) \oplus ([t] \odot [0]) = ([s] \odot [m]) \oplus ([t \cdot 0]) = ([s] \odot [m]) \oplus [0]] = [s] \odot [m]$. Αφού ο $\odot$ είναι μεταθετικός, από την εξίσωση $[s] \odot [m] = 1$, συμπεραίνουμε ότι το $[s]$ είναι αντίστροφο του $[m]$ στο $\mathbb{Z}_n$, ως προς τον $\odot$. □

Ο πολλαπλασιασμός ακεραίων, $\cdot$, είναι πράξη και πάνω στο σύνολο $\mathbb{Z}^*$ των μη μηδενικών ακεραίων γιατί $x, y \neq 0 \Rightarrow x \cdot y \neq 0$. Η αντίστοιχη ιδιότητα για τον $\odot$ στο $\mathbb{Z}_n$ ισχύει μόνο όταν ο n είναι πρώτος. Για παράδειγμα, στο $\mathbb{Z}_6$, $[2] \odot [3] = [6] = [0]$ παρότι $[2], [3] \neq [0]$.

Λήμμα 3.5.3 *Έστω $[m], [n] \in \mathbb{Z}_p$ με $[m] \odot [n] = [0]$, όπου ο p είναι πρώτος. Τότε $[m] = 0$ ή $[n] = 0$.*

*Απόδειξη:*3.5.3 Αφού $[mn] = [m] \odot [n] = [0]$ στο $\mathbb{Z}_p$, ο πρώτος p διαιρεί τον mn. Από το Λήμμα 2.1.9, ο p διαιρεί έναν από τους m, n. Συνεπώς, ένας από τους $[m]$, $[n]$ ισούται με το $[0]$. □

Στο εξής, $\mathbb{Z}_n^*$ θα συμβολίζει το σύνολο $\mathbb{Z}_n \setminus \{[0]\} = \{[1], [2], \ldots, [n-1]\}$. Από το Λήμμα 3.5.3, ο πολλαπλασιασμός $\odot$ είναι πράξη και πάνω στο $\mathbb{Z}_p^*$ όταν ο p είναι πρώτος.

Θεώρημα 3.5.4 *Το $\mathbb{Z}_p^*$, όταν ο p είναι πρώτος, είναι αβελιανή ομάδα ως προς τον πολλαπλασιασμό.*

*Απόδειξη:*3.5.4 Γνωρίζουμε ήδη ότι ο πολλαπλασιασμός είναι μεταθετικός, προσεταιριστικός και έχει ταυτοτικό στοιχείο το [1]. Μένει να δείξουμε την ύπαρξη αντιστρόφου κάθε στοιχείου $[m] \in \mathbb{Z}_p^*$. Αφού $[m] \neq [0]$, ο p δεν διαιρεί τον m. Από το Λήμμα 2.1.7, $\mu\kappa\delta(m,p) = 1$. Τέλος, από το Λήμμα 3.5.2, για κάποιο ακέραιο s, $[s] \odot [m] = [1]$. Προφανώς, $[s] \neq [0]$ και το $[s] \in \mathbb{Z}_p^*$ είναι αντίστροφο του $[m]$. □

Συμβολισμοί. Στο εξής θα χρησιμοποιούμε το σύμβολο $+$ για την πρόσθεση στο $\mathbb{Z}_n$ και το σύμβολο $\cdot$ για τον πολλαπλασιασμό στο $\mathbb{Z}_n$. Επίσης, με την εξαίρεση περιπτώσεων όπου είναι ανάγκη να γίνει διάκριση μεταξύ ενός ακεραίου και της κλάσης ισοτιμίας του modulo n, το μέλος $[m]$ του $\mathbb{Z}_n$ θα γράφεται απλά ως m. Τέλος, όταν μιλάμε για αντίστροφο κάποιου στοιχείου του $\mathbb{Z}_n$, θα εννοούμε αντίστροφο ως προς τον πολλαπλασιασμό. Το αντίστροφο ως προς την πρόσθεση λέγεται το **αντίθετο** στοιχείο. Τα **αντιστρέψιμα** στοιχεία είναι εκείνα που έχουν αντίστροφο (ως προς τον πολλαπλασιασμό).

3.6 Ασκήσεις

Άσκηση 3.6.1 *Στο $\mathbb{Z}_3$, ποιο είναι το αντίστροφο (ως προς τον πολλαπλασιασμό) του 2;*

Λύση 3.6.2 *Το 2 γιατί στο $\mathbb{Z}_3$, $2 \cdot 2 = 4 = 3 + 1 = 0 + 1 = 1$.*

Άσκηση 3.6.3 *Στο $\mathbb{Z}_5$, βρείτε τα αντίστροφα των $1, 2, 3, 4$.*

Λύση 3.6.4 $1, 3, 2, 4$, *αντίστοιχα.*

Άσκηση 3.6.5 *Στο $\mathbb{Z}_8$, ποια από τα $1, 2, \ldots, 7$ είναι αντιστρέψιμα; Βρείτε το αντίστροφό τους.*

Λύση 3.6.6 *Σχετικά πρώτα με το 8 είναι μόνο τα $1, 3, 5, 7$. Σύμφωνα με το Λήμμα 3.5.2 αυτά είναι τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_8$.*
Τα αντίστροφά τους είναι τα $1, 3, 5, 7$, αντίστοιχα, γιατί
$1 \cdot 1 = 1 = 3 \cdot 3 = 5 \cdot 5 = 7 \cdot 7$.

Άσκηση 3.6.7 *Στο $\mathbb{Z}_{12}$, ποια από τα $1, 2, \ldots, 11$ είναι αντιστρέψιμα; Βρείτε το αντίστροφό τους.*

Λύση 3.6.8 *Σχετικά πρώτα με το 12 είναι μόνο τα $1, 5, 7, 11$. Σύμφωνα με το Λήμμα 3.5.2 αυτά είναι τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_{12}$.*
Τα αντίστροφά τους είναι τα $1, 5, 7, 11$, αντίστοιχα, γιατί
$1 \cdot 1 = 1 = 5 \cdot 5 = 7 \cdot 7 = 11 \cdot 11$.

Άσκηση 3.6.9 *Στο $\mathbb{Z}_n$, αν το a είναι αντιστρέψιμο, δείξτε ότι η εξίσωση $a \cdot x = b$ έχει μοναδική λύση.*

Λύση 3.6.10 *Αν υπάρχει το a', τότε το $a' \cdot b$ έχει νόημα.*
Το $a' \cdot b$ είναι λύση: $a \cdot (a' \cdot b) = (a \cdot a') \cdot b = 1 \cdot b = b$.
Μόνο το $a' \cdot b$ είναι λύση: $a \cdot x = b \Rightarrow a' \cdot (a \cdot x) = a' \cdot b \Rightarrow (a' \cdot a) \cdot x = a' \cdot b \Rightarrow 1 \cdot x = a' \cdot b \Rightarrow x = a' \cdot b$.

Άσκηση 3.6.11 *Βρείτε όλες τις λύσεις της $5 \cdot x + 7 = 3 \ mod\ 12$, δηλαδή, στο $\mathbb{Z}_{12}$.*

Σημείωση Το $5 \cdot x + 7$ σημαίνει $(5 \cdot x) + 7$ και όχι $5 \cdot (x + 7)$.

Λύση 3.6.12 *Στο $\mathbb{Z}_{12}$, το 5 έχει αντίστροφο το 5. Τώρα*
$5 \cdot x + 7 = 3 \Leftrightarrow 5 \cdot x = 3 - 7 = -4 = 8$.
Από την Άσκηση 3.6.7, η εξίσωση έχει μοναδική λύση το $x = 5 \cdot 8 = 40 = 4$.

Άσκηση 3.6.13 *Βρείτε όλες τις λύσεις της $3 \cdot x + 15 = 3 \ mod\ 6$.*

Λύση 3.6.14 *Στο $\mathbb{Z}_6$,* $3 \cdot x + 15 = 3 \Leftrightarrow 3 \cdot x = 3 - 15 = 0$.
Εξετάζοντας ένα προς ένα τα στοιχεία του $\mathbb{Z}_6$, βλέπουμε ότι $x = 0, 2$ ή 4.

Άσκηση 3.6.15 *Βρείτε όλες τις λύσεις της $2 \cdot x + 7 = 16 \ mod\ 8$.*

Λύση 3.6.16 *Στο $\mathbb{Z}_8$,* $2 \cdot x + 7 = 16 \Leftrightarrow 2 \cdot x = 1$.
Εξετάζοντας ένα προς ένα τα στοιχεία του $\mathbb{Z}_8$, βλέπουμε ότι η εξίσωση δεν έχει λύση στο $\mathbb{Z}_8$.
Η έλλειψη λύσης οφείλεται στο γεγονός ότι το 8 δεν διαιρεί ένα περιττό αριθμό!

Άσκηση 3.6.17 *Έστω $a = a_k 10^k + \ldots + a_2 10^2 + a_1 10 + a_0$, όπου $a_0, a_1, \ldots, a_k$ είναι ακέραιοι. Να δείξετε ότι*

1. $3|a \Leftrightarrow 3|(a_k + \ldots + a_2 + a_1 + a_0)$
2. $9|a \Leftrightarrow 9|(a_k + \ldots + a_2 + a_1 + a_0)$
3. $11|a \Leftrightarrow 11|(a_0 - a_1 + a_2 - a_3 \ldots + (-1)^k a_k)$.

Λύση 3.6.18 1. *Στο $\mathbb{Z}_3$,*
$[10] = [9] + [1] = [0] + [1] = [1]$,
$[10^2] = [10] \cdot [10] = [1] \cdot [1] = [1]$,
$[10^3] = [10^2.10] = [10^2] \cdot [10] = [1] \cdot [1] = [1]$
$\ldots$
Άρα,
$[a] = [a_k 10^k + \ldots + a_2 10^2 + a_1 10 + a_0] =$
$[a_k 10^k] + \ldots + [a_2 10^2] + [a_1 10] + [a_0] =$
$[a_k] \cdot [10^k] + \ldots + [a_2] \cdot [10^2] + [a_1] \cdot [10] + [a_0] =$
$[a_k] \cdot [1] + \ldots + [a_2] \cdot [1] + [a_1] \cdot [1] + [a_0] =$
$[a_k] + \ldots + [a_2] + [a_1] + [a_0] =$
$[a_k + \ldots + a_2 + a_1 + a_0]$.
Συνεπώς,
$3|a \Leftrightarrow [a] = [0] \Leftrightarrow [a_k + \ldots + a_2 + a_1 + a_0] = [0] \Leftrightarrow 3|(a_k + \ldots + a_2 + a_1 + a_0)$.

2. *Γίνεται με τον ίδιο τρόπο δουλεύοντας στο* $\mathbb{Z}_9$, *όπου επίσης έχουμε* $[1] = [10] = [10^2] = \ldots$.

3. *Γίνεται με τον ίδιο τρόπο δουλεύοντας στο* $\mathbb{Z}_{11}$, *όπου έχουμε* $[10] = [-1], [10^2] = [1], [10^3] = [-1] \ldots [10^k] = [(-1)^k]$.

Άσκηση 3.6.19 *Βρείτε το αντίστροφο του* 26 *στο* $\mathbb{Z}_{139}$.

Λύση 3.6.20 *Κάνοντας διαδοχικές διαιρέσεις,*

$$\begin{aligned} 139 &= 5 \times 26 + 9 \\ 26 &= 2 \times 9 + 8 \\ 9 &= 1 \times 8 + 1 \\ 8 &= 8 \times 1 + 0 \end{aligned}$$

Άρα,

$$\begin{aligned} 1 &= 9 - (26 - 2 \times 9) \\ &= 3 \times 9 - 26 \\ &= 3 \times (139 - 5 \times 26) - 26 \\ &= 3 \times 139 - 16 \times 26 \end{aligned}$$

Έπεται ότι στο $\mathbb{Z}_{139}$, $1 = 3 \cdot 0 - 16 \cdot 26 = -16 \cdot 26$ *και το αντίστροφο του* 26 *είναι το* $-16 = 123$.

3.7 Πίνακες ομάδων

Ο πίνακας μιας πράξης $*$ σε ένα σύνολο που αποτελείται από n στοιχεία $a_1, a_2, \ldots, a_n$ είναι:

$*$	a_1	a_2	$\ldots$	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	$\ldots$	$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	$\ldots$	$a_2 * a_n$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
a_n	$a_n * a_1$	$a_n * a_2$	$\ldots$	$a_n * a_n$

όπου στην τομή της γραμμής του a_i με την στήλη του a_j τοποθετείται το στοιχείο $a_i * a_j$. Όταν πρόκειται για πράξη με ταυτοτικό στοιχείο, τη θέση του πρώτου στοιχείου παίρνει το ταυτοτικό.

Ο πίνακας της ομάδας $(\mathbb{Z}_4, +)$ είναι:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Έστω $V = \{1, \alpha, \beta, \gamma\}$, όπου α, β, γ είναι τα στοιχεία $3, 5, 7$ του $\mathbb{Z}_8$, αντίστοιχα. Προκύπτει ο πίνακας πολλαπλασιασμού

$\cdot$	1	α	β	γ
1	1	α	β	γ
α	α	1	γ	β
β	β	γ	1	α
γ	γ	β	α	1

Γνωρίζουμε ήδη ότι ο $\cdot$ είναι προσεταιριστικός και μεταθετικός με ταυτοτικό το 1 και κάθε στοιχείο του V έχει τον εαυτό του ως αντίστροφο. Ο πίνακας δείχνει ότι ο $\cdot$ είναι πράξη και στο V, γιατί το γινόμενο δύο στοιχείων του V είναι στοιχείο του V. Συνεπώς το $(V, \cdot)$ είναι αβελιανή ομάδα.
Η V λέγεται η 4–**ομάδα του Klein**.

3.8 Ασκήσεις

Άσκηση 3.8.1 *Κάνετε το πίνακα πολλαπλασιασμού της* $\mathbb{Z}_5^*$.

Λύση 3.8.2

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Άσκηση 3.8.3 *Έστω* $U = \{1, a, b, c\}$, *όπου* a, b, c *είναι τα στοιχεία* $5, 7, 11$ *του* $\mathbb{Z}_{12}$, *αντίστοιχα. Κάνετε τον πίνακα του* U *ως προς τον πολλαπλασιασμό του* $\mathbb{Z}_{12}$. *Να συμπεράνετε ότι το* $(U, \cdot)$ *αποτελεί ομάδα.*

Λύση 3.8.4

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Όπως ακριβώς στην περίπτωση της $(V, \cdot)$, *έτσι και το* $(U, \cdot)$ *αποτελεί ομάδα.*

Άσκηση 3.8.5 *Ο πίνακας της $(U, \cdot)$ προκύπτει από τον πίνακα της $(V, \cdot)$ όταν αντικαταστήσουμε τα α, β, γ με τα a, b, c, αντίστοιχα.*
Μπορούμε να βρούμε μια $1-1$ και επί συνάρτηση $f : V \to \mathbb{Z}_5^*$ έτσι ώστε όταν στον πίνακα της $(V, \cdot)$ αντικαταστήσουμε τα $1, \alpha, \beta, \gamma$ με τα $f(1), f(\alpha), f(\beta), f(\gamma)$, αντίστοιχα, να προκύπτει ο πίνακας της $\mathbb{Z}_5^*$;

Λύση 3.8.6 *Όχι, γιατί αν κάτι τέτοιο ήταν δυνατό, τότε θα είχαμε $f(1) = x \cdot x$ για κάθε $x \in \mathbb{Z}_5^*$ και συνεπώς $1 \cdot 1 = 2 \cdot 2$!*

Κεφάλαιο 4

Υποομάδες

4.1 Υποομάδες

Ορισμός 4.1.1 *Έστω S ένα σύνολο όπου ορίζεται μια πράξη $*$. Ένα υποσύνολο T του S λέγεται κλειστό ως προς την $*$ αν $a, b \in T \Rightarrow a * b \in T$.*

Προφανώς το T είναι κλειστό ως προς την $*$ αν και μόνον αν η $*$ είναι πράξη και στο T.

Ορισμός 4.1.2 *Έστω $(G, *)$ μια ομάδα. Ένα υποσύνολο H του G λέγεται υποομάδα της G αν το H είναι κλειστό ως προς την $*$ και το $(H, *)$ αποτελεί ομάδα.*

Παραδείγματα
Τα $\mathbb{N}$, $\mathbb{Z}$ είναι κλειστά ως προς την πρόσθεση και τον πολλαπλασιασμό αριθμών, το $\{2, 3\}$ δεν είναι κλειστό ούτε ως προς την πρόσθεση ούτε ως προς τον πολλαπλασιασμό.
Η $(\mathbb{Z}, +)$ είναι υποομάδα της $(\mathbb{Q}, +)$, που είναι υποομάδα της $(\mathbb{R}, +)$, που είναι υποομάδα της $(\mathbb{C}, +)$. Οι $(\mathbb{Q}^+, \cdot)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^+, \cdot)$ και $(\mathbb{R}^*, \cdot)$ είναι υποομάδες της $(\mathbb{R}^*, \cdot)$.

Κάθε ομάδα G έχει ως υποομάδες το G και το μονοσύνολο που αποτελείται από το ταυτοτικό στοιχείο της G. Αν υπάρχουν κι άλλες υποομάδες της G, αυτές λέγονται **γνήσιες** υποομάδες.

Θεώρημα 4.1.3 *Έστω $(G, *)$ μια ομάδα και H μια υποομάδα της G. Τότε*

1. *το ταυτοτικό στοιχείο της H ισούται με το ταυτοτικό στοιχείο e της G,*
2. *για κάθε $a \in H$, το αντίστροφο του a στην H ισούται με το αντίστροφο a' του a στην G.*

*Απόδειξη:*4.1.3

1. Έστω u το ταυτοτικό στοιχείο της H. Τότε $u * u = u$. Επειδή όμως το u είναι στοιχείο και της G, $u * e = u$. Άρα $u * u = u * e$. Τώρα από τον αριστερό νόμο διαγραφής για την ομάδα G, $u = e$.

2. Έστω b το αντίστροφο του a στην H. Τότε $a*b = e$ και $a*a' = e$. Συνεπώς, $a * b = a * a'$ και, από τον αριστερό νόμο διαγραφής για την G, $b = a'$.

□

Το επόμενο αποτέλεσμα είναι το σημαντικότερο κριτήριο προκειμένου να αποφασίσουμε αν κάποιο υποσύνολο μιας ομάδας αποτελεί υποομάδα.

Θεώρημα 4.1.4 *Έστω $(G, *)$ μια ομάδα. Ένα υποσύνολο H του G αποτελεί υποομάδα της G αν και μόνον αν*

1. *το H είναι κλειστό ως προς την $*$,*
2. *$e \in H$, όπου e είναι το ταυτοτικό της G, και*
3. *$a \in H \Rightarrow a' \in H$, όπου a' παριστάνει το αντίστροφο του a στην G.*

*Απόδειξη:*4.1.4 Αν η H είναι υποομάδα της G, τότε το (1) ισχύει από τον Ορισμό 4.1.2 και οι $(2), (3)$ ισχύουν από το Θεώρημα 4.1.3.
Αντίστροφα, αν ισχύει η (1), τότε η $*$ είναι πράξη στο H. Μάλιστα είναι προσεταιριστική στο H γιατί είναι προσεταιριστική στο πιο μεγάλο σύνολο G. Αν ισχύει η (2), τότε το e είναι ταυτοτικό στοιχείο του H. Αν ισχύει και η (3), τότε στο H κάθε στοιχείο a έχει το a' ως αντίστροφο. Συνεπώς, αν ισχύουν, οι $(1), (2), (3)$, από τον Ορισμό 3.3.1, η $(H, *)$ είναι ομάδα, και το H αποτελεί υποομάδα της G.
□

4.2 Ασκήσεις

Άσκηση 4.2.1 *Για κάθε ακέραιο n, το σύνολο $\{mn : m \in \mathbb{Z}\}$ όλων των πολλαπλασίων του n συμβολίζεται με $n\mathbb{Z}$.*
Να επαληθεύσετε ότι το $n\mathbb{Z}$ αποτελεί υποομάδα της $(\mathbb{Z}, +)$.

Λύση 4.2.2
1. *$a, b \in n\mathbb{Z} \Rightarrow a = sn, b = tn$ για κάποια $s, t \in \mathbb{Z} \Rightarrow a + b = (s + t)n \in n\mathbb{Z}$*
2. *$0 = 0n \in n\mathbb{Z}$*
3. *$a \in n\mathbb{Z} \Rightarrow a = sn$ για κάποιο $s \in \mathbb{Z} \Rightarrow -a = (-s)n \in n\mathbb{Z}$*

Έπεται από το Θεώρημα 4.1.4 ότι το $n\mathbb{Z}$ αποτελεί υποομάδα της $(\mathbb{Z}, +)$.

Άσκηση 4.2.3 *Ποια από τα $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{Q}^*, \mathbb{Q}^+, n\mathbb{Z}$ είναι υποομάδες της $(\mathbb{R}, +)$.*

Λύση 4.2.4 *Μόνο τα $\mathbb{Z}, \mathbb{Q}, n\mathbb{Z}$. Τα λοιπά δεν ικανοποιούν π.χ. τη συνθήκη (2) του Θεωρήματος 4.1.4.*

Άσκηση 4.2.5 *Ποια από τα $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{Q}^*, \mathbb{Q}^+, n\mathbb{Z}$ είναι υποομάδες της $(\mathbb{R}^*, \cdot)$.*

Λύση 4.2.6 *Μόνο τα $\mathbb{Q}^*, \mathbb{Q}^+$ είναι υποομάδες της $(\mathbb{R}^*, \cdot)$.*
Στο $\mathbb{N}$, μόνο το 1 έχει αντίστροφο. Τα λοιπά δεν είναι καν υποσύνολα του $\mathbb{R}^*$, γιατί περιέχουν το 0.

Άσκηση 4.2.7 *Έστω $U_n = \{z \in \mathbb{C} : z^n = 1\}$, όπου $n \in \mathbb{N}$.*
Να δείξετε ότι το U_n αποτελεί υποομάδα της $(\mathbb{C}^*, \cdot)$.

Λύση 4.2.8 *1.* $1 \in U_n$

2. $z_1, z_2 \in U_n \Rightarrow z_1^n = z_2^n = 1 \Rightarrow (z_1 z_2)^n = z_1^n z_2^n = 1 \cdot 1 = 1 \Rightarrow z_1 z_2 \in U_n$

3. $z \in U_n \Rightarrow z^n = 1 \Rightarrow (z^{-1})^n = (z^n)^{-1} = 1^{-1} = 1 \Rightarrow z^{-1} \in U_n$.
Έπεται από το Θεώρημα 4.1.4 ότι το U_n αποτελεί υποομάδα της $(\mathbb{R}^*, \cdot)$.

Άσκηση 4.2.9 *Βρείτε όλα τα στοιχεία της ομάδας U_4 της Άσκησης 4.2.5 και κάνετε τον πίνακα πολλαπλασιασμού της.*
Ποια ιδιότητα έχει η ομάδα του Klein V που δεν έχουν οι $U_4, \mathbb{Z}_4$;

Λύση 4.2.10 $U_4 = \{1, -1, i, -i\}$.

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Το αντίστροφο κάθε στοιχείου της V είναι το ίδιο το στοιχείο.

Άσκηση 4.2.11 *Έστω $(G, *)$ μια ομάδα, και H ένα μη κενό υποσύνολο του G με την ιδιότητα ότι*

$$a, b \in H \Rightarrow a * b' \in H. \qquad (\#) \tag{4.1}$$

Να δείξετε ότι η H είναι υποομάδα της G.

Λύση 4.2.12 *1. Το H περιέχει ένα τουλάχιστον στοιχείο a_0 και η $(\#) \Rightarrow a_0 * (a_0)' = e \in H$.*

2. Τώρα από την $(\#)$, $a \in H \Rightarrow e * a' = a' \in H$.

3. Έστω $a, b \in H$. Από την (2), $b' \in H$ και, από την $(\#)$, $a * (b')' = a * b \in H$.
Τώρα έπεται από το Θεώρημα 4.1.4 ότι το H αποτελεί υποομάδα της G.

4.3 Ιδιότητες Δυνάμεων

Έστω G ένα σύνολο εφοδιασμένο με μια προσεταιριστική πράξη. Το γινόμενο δύο στοιχείων x, y του G, όταν δεν χρειάζεται να αναφερθεί ρητά η πράξη του G, γράφεται απλά ως xy. Ομοίως, το γινόμενο n στοιχείων $x_1, x_2, \ldots, x_n$, $n \geq 1$, όπως ορίστηκε αμέσως μετά την Πρόταση 3.1.7, γράφεται ως $x_1 x_2 \ldots x_n$. Αν όλα τα $x_1, x_2, \ldots, x_n$ είναι ίσα με συγκεκριμένο στοιχείο x, το γινόμενό τους λέγεται η **n–οστή δύναμη** του x και συμβολίζεται με x^n. Αν το G διαθέτει ταυτοτικό στοιχείο e, ορίζουμε $x^0 = e$. Τέλος, αν το G είναι ομάδα, για αρνητικό ακέραιο n, η **n–οστή δύναμη** του x ορίζεται με $x^n = (x^{-n})'$. Έτσι, $x^1 = x$,

$x^2 = xx$, $x^3 = xxx$, ..., και αν το G είναι ομάδα, $x^{-1} = x'$, το αντίστροφο του x, $x^{-2} = (xx)'$, $x^{-3} = (xxx)'$, ...

Σημειώστε ότι $(x^n)' = x^{-n}$ για κάθε $n \in \mathbb{Z}$.

Λήμμα 4.3.1 *Έστω G ένα σύνολο εφοδιασμένο με μια προσεταιριστική πράξη, $x \in G$ και $m, n \in \mathbb{N}$. Τότε*

1. $x^m x^n = x^{m+n}$,
2. $(x^m)^n = x^{mn}$.

*Απόδειξη:*4.3.1

1. Αν $A = x_1 x_2 \dots x_{m+n}$, $B = x_1 x_2 \dots x_m$ και $C = x_{m+1} x_{m+2} \dots x_{m+n}$ από την Πρόταση 3.1.7, $A = BC$. Θέτοντας $x_1 = x_2 = \ldots = x_{m+n} = x$, έχουμε ότι $A = x^{m+n}, B = x^m$ και $C = x^n$, οπότε $x^{m+n} = x^m x^n$.

2. Γίνεται με επαγωγή στο n:

   (α′) Προφανώς, ισχύει για $n = 1$ και, χρησιμοποιώντας την (1),

   (β′) $(x^m)^n = x^{mn} \Rightarrow (x^m)^{n+1} = (x^m)^n x^m = x^{mn} x^m = x^{mn+m} = x^{m(n+1)}$.

□

Πρόταση 4.3.2 *Έστω x ένα στοιχείο μιας ομάδας G και $m, n \in \mathbb{Z}$. Τότε*

1. $x^m x^n = x^{m+n}$,
2. $(x^m)^n = x^{mn}$.

*Απόδειξη:*4.3.2

1. Το αποτέλεσμα ισχύει για $m = 0$ ή $n = 0$ και, αν το αποτέλεσμα ισχύει για ένα ζεύγος ακεραίων (m, n), τότε ισχύει και για το $(-n, -m)$:

   $$x^{-n} x^{-m} = (x^n)'(x^m)' = (x^m x^n)' = (x^{m+n})' = x^{-(m+n)}.$$

   Έτσι, από το Λήμμα 4.3.1, το αποτέλεσμα ισχύει όταν $m \geq 0, n \geq 0$ και όταν $m \leq 0, n \leq 0$. Μένει, προφανώς, να το δείξουμε όταν $m > 0, n < 0$. Οπότε, από ό,τι έχουμε ήδη δειξει,

   (α′) αν $m + n \geq 0$,
   $x^m x^n = x^{(m+n)-n} x^n = (x^{m+n} x^{-n}) x^n = x^{m+n}(x^{-n} x^n) = x^{m+n}$

   (β′) και αν $m + n < 0$,
   $x^m x^n = x^m x^{-m+(m+n)} = x^m (x^{-m} x^{m+n}) = (x^m x^{-m}) x^{m+n} = x^{m+n}$.

2. Υποθέτοντας $(x^m)^{n-1} = x^{m(n-1)}$, από την (1),

$$(x^m)^n = (x^m)^{n-1}x^m = x^{m(n-1)}x^m = x^{m(n-1)+m} = x^{mn}.$$

Συνεπώς, για $n \geq 0$, το αποτέλεσμα προκύπτει με επαγωγή στο n. Οπότε, για $n < 0$,

$$(x^m)^n = ((x^m)^{-n})' = (x^{-mn})' = x^{mn}.$$

□

4.4 Ασκήσεις

Στις ασκήσεις που ακολουθούν, εφαρμόζεται το Λήμμα 4.3.1 στο $\mathbb{Z}_n$ εφοδιασμένο με την πράξη του πολλαπλασιασμού.

Άσκηση 4.4.1 *Βρείτε το υπόλοιπο της διαίρεσης* $3^{614} : 5$.

(: Στο $\mathbb{Z}_5$, $3^2 = -1$)

Λύση 4.4.2 *Στο* $\mathbb{Z}_5$, $3^{614} = (3^2)^{307} = (-1)^{307} = -1 = 4$. *Έτσι το υπόλοιπο της διαίρεσης* $3^{614} : 5$ *είναι το* 4.

Άσκηση 4.4.3 *Βρείτε το τελευταίο ψηφίο του* 3^{614}.

(: Το ζητούμενο είναι το υπόλοιπο της διαίρεσης $3^{614} : 10$.)

Λύση 4.4.4 *Στο* $\mathbb{Z}_{10}$, $3^2 = -1$, *άρα* $3^{614} = (3^2)^{307} = (-1)^{307} = -1 = 9$ *και το τελευταίο ψηφείο του* 3^{614} *είναι το* 9.

Άσκηση 4.4.5 *Βρείτε το υπόλοιπο της διαίρεσης* $3^{6014} : 7$.

Λύση 4.4.6 *Στο* $\mathbb{Z}_7$, $3^3 = -1$, *άρα* $3^{6014} = 3^{(3\times 2004)+2} = (3^3)^{2004} \times 3^2 = -1^{2004} \times 9 = 1 \times 2 = 2$. *Άρα το υπόλοιπο της διαίρεσης* $3^{6014} : 7$ *είναι το* 2.

Άσκηση 4.4.7 *Βρείτε το υπόλοιπο της διαίρεσης* $7^{2007} : 25$.

Λύση 4.4.8 *Στο* $\mathbb{Z}_{25}$, $7^2 = -1$, *άρα* $7^{2007} = 7^{(2\times 1003)+1} = (7^2)^{1003} \times 7 = (-1)^{1003} \times 7 = -1 \times 7 = -7 = 18$, *και το υπόλοιπο της διαίρεσης* $7^{2007} : 25$ *είναι* 18.

Άσκηση 4.4.9 *Σε ένα σύνολο εφοδιασμένο με μια προσεταιριστική πράξη, έστω* a, b *δύο στοιχεία που* ***μετατίθενται****, δηλαδή, ισχύει ότι* $ab = ba$.

Δείξτε ότι για κάθε $m, n \in \mathbb{N}$,

1. $ab^n = b^n a$
2. $a^m b^n = b^n a^m$
3. $(ab)^n = a^n b^n$

Λύση 4.4.10 *1. Προκύπτει από την αρχή της επαγωγής αφού ισχύει για* $n = 1$ *και*
$ab^n = b^n a \Rightarrow ab^{n+1} = a(bb^n) = (ab)b^n = (ba)b^n = b(ab^n) = b(b^n a) = (bb^n)a = b^{n+1}a.$

2. Από την (1), a^m *και* b *μετατίθενται, άρα* $a^m b^n = b^n a^m$.

3. Προκύπτει από την αρχή της επαγωγής αφού ισχύει για $n = 1$ *και*
$(ab)^n = a^n b^n \Rightarrow (ab)^{n+1} = (ab)^n ab = a^n b^n ab = a^n(b^n a)b$, *και από την* (1),
$= a^n(ab^n)b = (a^n a)(b^n b) = a^{n+1}b^{n+1}$.

4.5 Κυκλικές υποομάδες

Θεώρημα 4.5.1 *Για κάθε στοιχείο* a *μιας ομάδας* G, *το σύνολο* $\langle a\rangle = \{a^n : n \in \mathbb{Z}\}$ *όλων των δυνάμεων του* a *αποτελεί αβελιανή υποομάδα της* G.

*Απόδειξη:*4.5.1 Από την Πρόταση 4.3.2,

1. $x, y \in \langle a\rangle \Rightarrow x = a^m, y = a^n$, όπου $m, n \in \mathbb{Z}$,
   $\Rightarrow xy = a^{m+n} = a^{n+m} = yx \in \langle a\rangle$.
2. $e = a^0 \in \langle a\rangle$.
3. $x \in \langle a\rangle \Rightarrow x = a^m$, όπου $m \in \mathbb{Z}$, $\Rightarrow x' = a^{-m} \in \langle a\rangle$.

Τώρα, από το Θεώρημα 4.1.4, το $\langle a\rangle$ αποτελεί υποομάδα της G. Μάλιστα, από το (1), η $\langle a\rangle$ είναι αβελιανή. □

Η ομάδα $\langle a\rangle$ συνήθως αναφέρεται ως η (κυκλική) υποομάδα της G που **παράγεται** από το a. Μια ομάδα G λέγεται **κυκλική** αν $G = \langle a\rangle$ για κάποιο στοιχείο a της G. Ένα τέτοιο a καλείται (ένας) **γεννήτορας** της G. Προφανώς, κάθε κυκλική ομάδα είναι αβελιανή.

Το πλήθος των μελών ενός πεπερασμένου συνόλου X συμβολίζεται με $|X|$ και, όταν το X είναι ένα άπειρο σύνολο, θέτουμε $|X| = \infty$. Η **τάξη** μιας ομάδας G είναι το πλήθος των μελών της, δηλαδή, το $|G|$. Η **τάξη** ενός στοιχείου a μιας ομάδας G, είναι η τάξη της υποομάδας $\langle a\rangle$, συμβολίζεται δε με $o(a)$. Προφανώς, $o(a) \leq |G|$, κάθε στοιχείο πεπερασμένης ομάδας έχει πεπερασμένη τάξη, και το μόνο στοιχείο με τάξη 1 είναι το ταυτοτικό.

Παρατήρηση 4.5.2 *Όταν μιλάμε για τις ομάδες* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$, *εννοείται ότι η πράξη τους είναι η πρόσθεση, γιατί δεν είναι ομάδες ως προς τον πολλαπλασιασμό. Για τον ίδιο λόγο, όταν μιλάμε για τις ομάδες* $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*, {\mathbb{Z}_p}^*$, *όπου ο* p *είναι πρώτος, ή τις ομάδες* $\mathbb{Q}^+, \mathbb{R}^+, \mathbb{C}^+$, *εννοείται ότι η πράξη τους είναι ο πολλαπλασιασμός. Στις ομάδες* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, *λοιπόν, η* n*–οστή δύναμη στοιχείου* m *είναι προφανώς ο αριθμός* nm *και* $\langle m\rangle = \{nm : n \in \mathbb{Z}\} = m\mathbb{Z}$, *το σύνολο των πολλαπλασίων του* m. *Συνεπώς,* $\langle 1\rangle = \langle -1\rangle = \mathbb{Z}$, *η* $\mathbb{Z}$ *είναι κυκλική, τα* $1, -1$ *είναι γεννήτορές της και έχουν τάξη* ∞. *Ομοίως, η* $\mathbb{Z}_n$ *είναι κυκλική, τα* $1, -1$ *είναι γεννήτορές της και έχουν τάξη* n.

Θεώρημα 4.5.3 *Κάθε υποομάδα H μιας κυκλικής ομάδας G είναι κυκλική.*

*Απόδειξη:*4.5.3 Προφανώς, $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ για κάποιο $a \in G$.
Αν $H = \{e\}$, τότε η H είναι κυκλική γιατί ισούται με $\langle e \rangle$. Διαφορετικά η υποομάδα H της G, για κάποιο $m \in \mathbb{Z} \setminus \{0\}$, περιέχει το a^m, καθώς και το αντίστροφό του a^{-m}. Συνεπώς, $A = \{i \in \mathbb{N} : a^i \in H\} \neq \emptyset$. Από την αρχή της καλής διάταξης, το A έχει ελάχιστο στοιχείο, το οποίο καλούμε k.

Θεωρώ τώρα τυχαίο $x \in H \subset G$. Προφανώς, $x = a^n$ για κάποιο $n \in \mathbb{Z}$. Από τον αλγόριθμο διαίρεσης,

$$n = qk + r, \text{ όπου } q, r \in \mathbb{Z} \text{ και } 0 \leq r < k.$$

Από την Πρόταση 4.3.2,

$$a^r = a^{n-qk} = a^n a^{-qk} = x(a^k)^{-q}.$$

Προφανώς, η υποομάδα H περιέχει τα x, a^k, $(a^k)^{-q}$ και, συνεπώς, το $a^r = x(a^k)^{-q}$. Αν $r > 0$, τότε $r \in A$ και $r < k$. Αυτό αντιφάσκει στον ορισμό του k. Άρα $r = 0$ και $x = a^{qk} = (a^k)^q$.
Συμπεραίνουμε ότι η H είναι κυκλική με ένα γεννήτορα το a^k. □

Λήμμα 4.5.4 *Έστω a ένα στοιχείο μιας ομάδας G και m ένας φυσικός αριθμός τέτοιος ώστε $a^m = e$. Τότε*

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{m-1}\}.$$

*Απόδειξη:*4.5.4 Ένα τυχαίο στοιχείο του $\langle a \rangle$ γράφεται ως a^n, όπου $n \in \mathbb{Z}$. Από τον αλγόριθμο διαίρεσης,

$$n = qm + r, \text{ όπου } q, r \in \mathbb{Z} \text{ και } 0 \leq r < m.$$

Έτσι, από την Πρόταση 4.3.2, $a^n = a^{qm}a^r = (a^m)^q a^r = e^q a^r = a^r$. Αυτό σημαίνει ότι οποιοδήποτε στοιχείο του $\langle a \rangle$ ισούται με ένα από τα $e, a, a^2, \ldots, a^{m-1}$, όλα από τα οποία είναι μέλη του $\langle a \rangle$. Έτσι $\langle a \rangle = \{e, a, a^2, \ldots, a^{m-1}\}$. □

Θεώρημα 4.5.5 *Για ένα στοιχείο a μιας ομάδας G, τα εξής είναι ισοδύναμα.*

1. *$o(a) < \infty$,*
2. *$a^m = e$ για κάποιο $m \in \mathbb{N}$.*

*Απόδειξη:*4.5.5 Ας υποθέσουμε ότι ισχύει το (1). Τότε το $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ είναι πεπερασμένο. Αυτό συνεπάγεται ότι $a^i = a^j$ για κάποιους ακέραιους i, j με $i < j$. Μα τότε, $m = j - i \in \mathbb{N}$ και, από την Πρόταση 4.3.2, $a^m = a^j a^{-i} = a^i(a^i)' = e$.

Αντίστροφα, έστω ότι $a^m = e$ για κάποιο $m \in \mathbb{N}$. Από το Λήμμα 4.5.4, $\langle a \rangle = \{e, a, a^2, \ldots, a^{m-1}\}$. Συνεπώς, $o(a) = |\langle a \rangle| \leq m < \infty$. □

Η αρχή της καλής διάταξης και το Θεώρημα 4.5.5 μας εξασφαλίζουν την ύπαρξη του ακεραίου m στο επόμενο αποτέλεσμα.

Θεώρημα 4.5.6 *Έστω a ένα στοιχείο μιας ομάδας με $o(a) < \infty$. Έστω m ο ελάχιστος φυσικός αριθμός με $a^m = e$. Τότε*

1. $\langle a \rangle = \{e, a, a^2, \ldots, a^{m-1}\}$,
2. $o(a) = m$,
3. $a^n = e, n \in \mathbb{Z} \Rightarrow m|n$.

*Απόδειξη:*4.5.6

1. Από το Λήμμα 4.5.4, $\langle a \rangle = \{e, a, a^2, \ldots, a^{m-1}\}$.
2. Ας υποθέσουμε ότι $0 \leq r_1 < r_2 < m$. Τότε $0 < k = r_2 - r_1 < m$ και, από τον ορισμό του m, $a^k = a^{r_2}a^{-r_1} = a^{r_2}(a^{r_1})' \neq e$. Άρα, $a^{r_1} \neq a^{r_2}$. Συνεπώς, τα στοιχεία $e, a, a^2, \ldots, a^{m-1}$ είναι διακεκριμένα και, από την (1), $o(a) = |\langle a \rangle| = m$.
3. Έστω ότι $a^n = e$. Από τον αλγόριθμο διαίρεσης,

$$n = qm + r, \text{ όπου } q, r \in \mathbb{Z} \text{ και } 0 \leq r < m.$$

Συνεπώς, $a^r = a^{n-qm} = a^n a^{-qm} = e(a^m)^{-q} = e^{-q} = e$. Από τον ορισμό του m, $r = 0$. Συνεπώς, $n = qm$ και $m|n$.

□

Παρατήρηση 4.5.7 *Σε περιπτώσεις που η $+$ χρησιμοποιείται για την πράξη μιας ομάδας, η ομάδα είναι πάντοτε αβελιανή, το ταυτοτικό της συμβολίζεται με 0 και το αντίστροφο στοιχείου a λέγεται το **αντίθετο** του a και συμβολίζεται με $-a$. Επίσης, η n–οστή δύναμη του a συμβολίζεται με na, οπότε οι κανόνες της Πρότασης 4.3.2 παίρνουν τη μορφή: $mx + nx = (m + n)x$ και $n(mx) = (nm)x$, για κάθε $m, n \in \mathbb{Z}$.*

4.6 Ασκήσεις

Άσκηση 4.6.1 *Βρείτε τις υποομάδες $\langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle$ της $\mathbb{Z}_5^*$.*
Βρείτε την τάξη των $1, 2, 3, 4$. Είναι η $\mathbb{Z}_5^*$ κυκλική;

Λύση 4.6.2 $\langle 1 \rangle = \{1\}$, $\langle 2 \rangle = \mathbb{Z}_5^*$ *γιατί* $2^2 = 4, 2^3 = 8 = 3, 2^4 = 16 = 1$,
$\langle 3 \rangle = \{3, 4, 2, 1\} = \mathbb{Z}_5^*$, $\langle 4 \rangle = \{4, 1\}$.
$o(1) = 1, o(2) = 4 = o(3), o(4) = 2$.
Η $\mathbb{Z}_5^*$ είναι κυκλική και τα $2, 3$ είναι γεννήτορές της.

Άσκηση 4.6.3 *Βρείτε όλες τις κυκλικές υποομάδες της $\mathbb{Z}_8$, την τάξη κάθε στοιχείου της και όλους τους γεννήτορές της.*

Λύση 4.6.4 *Εδώ,* $7 = -1$*, συνεπώς* $\langle 1\rangle = \langle 7\rangle = \mathbb{Z}_8$*,* $\langle 2\rangle = \{2, 4, 6, 0\}$*,*
$\langle 3\rangle = \{3, 6, 1, 4, 7, 2, 5, 0\} = \mathbb{Z}_8$*,* $\langle 4\rangle = \{4, 0\}$*,*
$\langle 5\rangle = \{5, 2, 7, 4, 1, 6, 3, 0\} = \mathbb{Z}_8$*,* $\langle 6\rangle = \{6, 4, 2, 0\}$*.*
$o(0) = 1, o(1) = 8 = o(3) = (5) = o(7), o(2) = 4 = o(6), o(4) = 2$
Γεννήτορες είναι τα $1, 3, 5, 7$*.*

Άσκηση 4.6.5 *Βρείτε τις υποομάδες* $\langle 1\rangle, \langle -1\rangle$ *και* $\langle 2\rangle$ *της* $\mathbb{R}^*$*.*

Λύση 4.6.6 $\langle 1\rangle = \{1\}, \langle -1\rangle = \{1, -1\}, \langle 2\rangle = \{1, 2^1, 2^2 \ldots\} \cup \{2^{-1}, 2^{-2} \ldots\}$*.*

Άσκηση 4.6.7 *Ποιες από τις ομάδες* $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ *είναι κυκλικές;*

Λύση 4.6.8 *Καμία από αυτές τις ομάδες δεν είναι κυκλική γιατί για οποιοδήποτε μη μηδενικό στοιχείο* x*, το* $\langle x\rangle = \{nx : n \in \mathbb{Z}\}$ *δεν περιέχει π.χ. το στοιχείο* $\frac{x}{2}$ *της ομάδας.*

Άσκηση 4.6.9 *Βρείτε όλες της υποομάδες της* $\mathbb{Z}$*.*

Λύση 4.6.10 *Από το Θεώρημα 4.5.3, κάθε τέτοια ομάδα είναι κυκλική. Συνεπώς, οι υποομάδες της* $\mathbb{Z}$ *είναι:* $\{0\}$*,* $\mathbb{Z}$*,* $\langle 2\rangle = 2\mathbb{Z}$*,* $\langle 3\rangle = 3\mathbb{Z}$*, ..., δηλ. οι ομάδες* $n\mathbb{Z}, n \in \mathbb{Z}$*.*

Άσκηση 4.6.11 *Δείξτε ότι η* U_n *είναι κυκλική ομάδα.*

Λύση 4.6.12 $U_n = \{1, x, x^2, \ldots, x^{n-1}\}$*, όπου* $x = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$*.*

Άσκηση 4.6.13 *Δείξτε ότι κάθε πεπερασμένη κυκλική υποομάδα της* $\mathbb{C}^*$ *είναι της μορφής* U_n*.*

Λύση 4.6.14 *Έστω* a *ένας γεννήτορας μιας τέτοιας υποομάδας* H*. Τότε από το Θεώρημα 4.5.6,* $H = \langle a\rangle = \{1, a, a^2, \ldots, a^{n-1}\}$ *όπου* n *είναι ο ελάχιστος φυσικός αριθμός με* $a^n = 1$*, μάλιστα* $o(a) = |H| = n$*. Συνεπώς, κάθε ένα από τα* n *μέλη της* H *είναι μια από τις* n *ρίζες τις* $z^n = 1$*, δηλαδή,* $H = U_n$*.*

Άσκηση 4.6.15 *Ποιες από τις ομάδες* $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*, \mathbb{Q}^+, \mathbb{R}^+$ *είναι κυκλικές;*

Λύση 4.6.16 *Κάθε κυκλική ομάδα είναι αριθμήσιμη. Συνεπώς, οι* $\mathbb{R}^*, \mathbb{C}^*, \mathbb{R}^+$ *δεν είναι κυκλικές.*
Έστω a *ένας υποψήφιος γεννήτορας της* $\mathbb{Q}^+$*. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι* $a > 1$*. Τότε*

$$\ldots a^{-3} < a^{-2} < a^{-1} < 1 < a < a^2 < a^3 \ldots.$$

Είναι προφανές ότι π.χ. ο $\frac{1+a}{2}$ *δεν είναι δύναμη του* a*. Συμπεραίνουμε ότι η* $\mathbb{Q}^+$ *δεν είναι κυκλική.*
Τώρα μόνο ένας αρνητικός αριθμός a *θα μπορούσε να ήταν γεννήτορας της* $\mathbb{Q}^*$*, και τότε ο* a^2 *θα ήταν γεννήτορας της* $\mathbb{Q}^+$*, η οποία όμως δεν είναι κυκλική! Συνεπώς, ούτε η* $\mathbb{Q}^*$ *δεν είναι κυκλική.*

Άσκηση 4.6.17 *Εξετάστε αν η 4–ομάδα Klein V είναι κυκλική.*

Λύση 4.6.18 *Όχι, γιατί τα μη ταυτοτικά στοιχεία έχουν τάξη $2 \neq 4 = |V|$.*

Άσκηση 4.6.19 *Δείξτε ότι $\langle a \rangle = \langle a^{-1} \rangle$ για κάθε μέλος a μιας ομάδας. Συνεπώς, $o(a) = o(a^{-1})$.*

Λύση 4.6.20 *Κάθε μέλος $x \in \langle a \rangle$ γράφεται ως $x = a^n$ για κάποιο ακέραιο n. Από την Πρόταση 4.3.2, $x = (a^{-1})^{-n}$. Άρα $x \in \langle a^{-1} \rangle$. Έτσι, $\langle a \rangle \subset \langle a^{-1} \rangle$, άρα και $\langle a^{-1} \rangle \subset \langle (a^{-1})^{-1} \rangle = \langle a \rangle$. Συνεπώς, $\langle a \rangle = \langle a^{-1} \rangle$.*

Άσκηση 4.6.21 *Έστω a ένα στοιχείο μιας ομάδας, $b = a^n$ και $m = o(a) < \infty$. Δείξτε ότι $\langle a \rangle = \langle b \rangle$ αν και μόνον αν $\mu\kappa\delta(m, n) = 1$.*

Λύση 4.6.22 *Από την $b = a^n$ έπεται ότι $\langle b \rangle \subset \langle a \rangle$. Προφανώς, $\langle a \rangle = \langle b \rangle$ αν και μόνον αν το a είναι δύναμη του b.*
Ας υποθέσουμε ότι $\mu\kappa\delta(m, n) = 1$. Τότε $sm + tn = 1$ για κάποιους ακέραιους s, t. Άρα, από την Πρόταση 4.3.2, $a = a^{sm+tn} = (a^m)^s (a^n)^t = e^s b^t = b^t$. Συνεπώς, $\langle a \rangle = \langle b \rangle$.
Αντιστρόφως, ας υποθέσουμε ότι $\langle a \rangle = \langle b \rangle$, οπότε $a = b^k$ για κάποιο ακέραιο k. Τότε $e = aa^{-1} = b^k a^{-1} = ((a^n)^k)a^{-1} = a^{kn} a^{-1} = a^{kn-1}$. Από το Θεώρημα 4.5.6, $m|(kn-1)$. Δηλαδή, για κάποιο ακέραιο l, $kn-1 = lm$. Άρα $(-l)m + kn = 1$, δηλαδή, $\mu\kappa\delta(m, n) = 1$.

Άσκηση 4.6.23 *Βρείτε όλους τους γεννήτορες της $\mathbb{Z}_{24}$.*

Λύση 4.6.24 *Επειδή, $\langle 1 \rangle = \mathbb{Z}_{24}$, $o(1) = 24 = 2^3 \times 3$ και, από την Άσκηση 4.6.21, ο n είναι γεννήτορας της $\mathbb{Z}_{24}$ αν και μόνον αν $\mu\kappa\delta(24, n) = 1$. Συνεπώς, γεννήτορες είναι οι $1, 5, 7, 11, 13, 17, 19, 23$.*

Άσκηση 4.6.25 *Έστω a, b στοιχεία μιας ομάδας που μετατίθενται, δηλαδή, $ab = ba$. Δείξτε ότι για κάθε $m, n \in \mathbb{Z}$,*

1. *$ab^n = b^n a$*
2. *$a^m b^n = b^n a^m$*
3. *$(ab)^n = a^n b^n$*

Λύση 4.6.26

1. *Προφανώς ισχύει για $n = 0$. Από την Άσκηση 4.4.9, ισχύει για $n > 0$. Από το Πόρισμα 3.3.6,*
   $ab^n = b^n a \Rightarrow b^{-n} a' = a' b^{-n} \Rightarrow b^{-n} = (a' b^{-n})a = a'(b^{-n} a) \Rightarrow ab^{-n} = b^{-n} a$. Συνεπώς, το αποτέλεσμα ισχύει και για $n < 0$.
2. *Εφαρμόζοντας την (1) δύο φορες έχω $ab^n = b^n a$, άρα και $a^m b^n = b^n a^m$.*
3. *Προφανώς ισχύει για $n = 0$. Από την Άσκηση 4.4.9, ισχύει για $n > 0$. Από το Πόρισμα 3.3.6,*
   $(ba)^n = b^n a^n \Rightarrow (ab)^{-n} = (ba)^{-n} = ((ba)^n)' = (b^n a^n)' = (a^n)'(b^n)' = a^{-n} b^{-n}$.
   Συνεπώς, το αποτέλεσμα ισχύει και για $n < 0$.

Άσκηση 4.6.27 *Έστω a, b στοιχεία μιας ομάδας με $μκδ(o(a), o(b)) = 1$ και $ab = ba$.*
Δείξτε ότι $o(ab) = o(a)o(b)$.

Λύση 4.6.28 *Έστω $k = o(a), m = o(b), n = o(ab)$ οι τάξεις των a, b, ab, αντίστοιχα. Τότε από την Άσκηση 4.6.23 και την Πρόταση 4.3.2*

$$(ab)^{km} = a^{km}b^{km} = (a^k)^m(b^m)^k = e.e = e.$$

Από το Θεώρημα 4.5.6, $n|km$. Αρκεί τώρα να δείξω $km|n$. Τώρα

$$e = ((ab)^n)^k = (ab)^{kn} = a^{kn}b^{kn} = (a^k)^n b^{kn} = e^n b^{kn} = b^{kn}.$$

Έπεται ότι το $m|kn$. Αφού $μκδ(k, m) = 1$, συμπεραίνουμε ότι $m|n$. Ομοίως, $k|n$. Τώρα από την Άσκηση 2.2.19, $km|n$. Συνεπώς, $km = n$.

Άσκηση 4.6.29 *Δώστε παραδείγματα δύο στοιχείων a, b μιας ομάδας με $o(ab) \neq o(a)o(b)$ παρότι $ab = ba$.*

Λύση 4.6.30 *Σε κάθε ομάδα, για $a \neq e$ και $b = a'$, $ab = ba$ ενώ $o(ab) = 1 \neq o(a)o(b)$.*
Στην ομάδα Klein, $o(\alpha) = 2 = o(\beta) = o(\alpha\beta)$.
Στην $\mathbb{Z}_{12}$, $o(2) = 6, o(4) = 3$ ενώ $o(2 + 4) = 2$.

Άσκηση 4.6.31 *Για όλα τα μέλη a, b μιας ομάδας G ισχύει $(ab)^2 = a^2b^2$.*
Δείξτε ότι η G είναι αβελιανή.

Λύση 4.6.32 *Έχουμε $abab = aabb$.*
Από αριστερή απαλοιφή, προκύπτει ότι $bab = abb$.
Από δεξιά απαλοιφή, προκύπτει ότι $ba = ab$.

4.7 Το θεώρημα Lagrange

Έστω G μια ομάδα και H μια υποομάδα της G. Στο σύνολο G ορίζουμε μια σχέση $\sim$ με

$$a \sim b \text{ αν και μόνον αν } a'b \in H.$$

Λήμμα 4.7.1 *$H \sim$ είναι σχέση ισοδυναμίας.*

*Απόδειξη:*4.7.1 Για καθε $a, b, c \in G$, έχοντας υπόψη ότι η H είναι υποομάδα της G,

1. $a'a = e \in H$. Άρα $a \sim a$.
2. $a \sim b \Rightarrow a'b \in H \Rightarrow (a'b)' = b'a \in H \Rightarrow b \sim a$.
3. $a \sim b, b \sim c \Rightarrow a'b \in H, b'c \in H \Rightarrow (a'b)(b'c) = a'c \in H \Rightarrow a \sim c$.

□

Το **αριστερό σύμπλοκο** της H στην G που καθορίζει ένα στοιχείο a της G είναι το σύνολο $\{ah : h \in H\}$, το οποίο συμβολίζεται με aH. Προφανώς, $eH = H$. Το πλήθος όλων αυτών των (διακεκριμένων) αριστερών συμπλόκων λέγεται ο **δείκτης** της H στην G και συμβολίζεται με $|G : H|$.

Λήμμα 4.7.2 *Κάθε αριστερό σύμπλοκο aH ισούται με την κλάση ισοδυναμίας $[a]$ του a ως προς την σχέση $\sim$.*

*Απόδειξη:*4.7.2 $b \in [a] \Leftrightarrow a \sim b \Leftrightarrow h = a'b \in H \Leftrightarrow b = ah$ για κάποιο $h \in H \Leftrightarrow b \in aH$. □

Πρόταση 4.7.3 *Για κάθε $a, b \in G$,*

1. $a \in aH$
2. $aH = bH \Leftrightarrow aH \cap bH \neq \emptyset$
3. $aH = bH \Leftrightarrow a \in bH$
4. $aH \neq bH \Leftrightarrow aH \cap bH = \emptyset$
5. $aH = H \Leftrightarrow a \in H$

*Απόδειξη:*4.7.3 Οι (1), (2), (3), (4) έπονται από την Πρόταση 1.7.1 εφόσον τα αριστερά σύμπλοκα είναι κλάσεις ισοδυναμίας. Η (5) προκύπτει θέτοντας $b = e$ στην (3). □

Λήμμα 4.7.4 $|H| = |aH|$ *για κάθε στοιχείο a της G.*

*Απόδειξη:*4.7.4 Για να δείξουμε ότι τα δύο σύνολα είναι ισοπληθή, αρκεί να δείξουμε ότι υπάρχει μια $f : H \to aH$ η οποία είναι $1-1$ και επί. Μια τέτοια συνάρτηση ορίζεται θέτοντας $f(h) = ah$ για κάθε $h \in H$.
Πράγματι, η f είναι επί γιατί για κάθε μέλος y της aH, $y = ah_0$, όπου $h_0 \in H$, και συνεπώς $y = f(h_0)$.
Η f είναι $1-1$ γιατί από τον αριστερό κανόνα διαγραφής,

$$f(h_1) = f(h_2) \Rightarrow ah_1 = ah_2 \Rightarrow h_1 = h_2.$$

□

Θεώρημα 4.7.5 *(Lagrange). Για κάθε υποομάδα H μιας πεπερασμένης ομάδας G,*

$$|G| = |G : H||H|.$$

Συνεπώς, η τάξη της H διαιρεί την τάξη της G.

*Απόδειξη:*4.7.5 Από την Πρόταση 4.7.3, το σύνολο G είναι η ένωση $|G : H|$ τον αριθμό αριστερών συμπλόκων της H στην G, και κάθε δύο από αυτά είναι ξένα μεταξύ τους. Από δε το Λήμμα 4.7.4, κάθε ένα από αυτά τα σύμπλοκα περιέχει $|H|$ στοιχεία. Συνεπώς, η G περιέχει $|G : H||H|$ στοιχεία. □

Πόρισμα 4.7.6 *Η τάξη $o(a)$ ενός στοιχείου a μιας πεπερασμένης ομάδας G διαιρεί την τάξη της G.*

*Απόδειξη:*4.7.6 Στο Θεώρημα Lagrange, θέτουμε $H = \langle a \rangle$. □

Πόρισμα 4.7.7 *Αν η τάξη μιας ομάδας G είναι πρώτος αριθμός, τότε η G είναι κυκλική και κάθε μη ταυτοτικό στοιχείο της G είναι γεννήτοράς της.*

*Απόδειξη:*4.7.7 Έστω ότι ο αριθμός $|G|$ είναι πρώτος. Τότε υπάρχει $a \in G$ με $a \neq e$. Προφανώς, $o(a) > 1$ και, από το Πόρισμα 4.7.6, ο φυσικός αριθμός $o(a)$ διαιρεί τον πρώτο αριθμό $|G|$. Έπεται ότι $o(a) = |\langle a \rangle| = |G|$. Επειδή το $\langle a \rangle$ είναι υποσύνολο του πεπερασμένου συνόλου G, συμπεραίνουμε ότι $G = \langle a \rangle$.

Συνεπώς, η G είναι κυκλική με γεννήτορα κάθε $a \in G$ με $a \neq e$. □

Παρατήρηση 4.7.8 *Όταν η πράξη της ομάδας G είναι η $+$, το αριστερό σύμπλοκο μιας υποομάδας H στην G που καθορίζει ένα στοιχείο a της G συμβολίζεται με $a+H$, δηλαδή, $a+H = \{a+h : h \in H\}$. Συνεπώς, η Πρόταση 4.7.3 μεταφράζεται σε*

1. $a \in (a + H)$
2. $a + H = b + H \Leftrightarrow (a + H) \cap (b + H) \neq \emptyset$
3. $a + H = b + H \Leftrightarrow a \in (b + H)$
4. $a + H \neq b + H \Leftrightarrow (a + H) \cap (b + H) = \emptyset$
5. $a + H = H \Leftrightarrow a \in H$.

4.8 Ασκήσεις

Άσκηση 4.8.1 *Βρείτε όλα τα αριστερά σύμπλοκα της $H = \langle 3 \rangle$ στην $\mathbb{Z}_6$.*

Λύση 4.8.2 $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}, H = \{0, 3\}$.
Αριστερά σύμπλοκα:
$0 + H = H = 3 + H$
$1 + H = \{1, 4\} = 4 + H$
$2 + H = \{2, 5\} = 5 + H$.

Άσκηση 4.8.3 *Βρείτε όλα τα αριστερά σύμπλοκα της $H = \langle 2 \rangle$ στην $\mathbb{Z}_6$.*

Λύση 4.8.4 $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}, H = \{0, 2, 4\}$.
Αριστερά σύμπλοκα:
$0 + H = H = 2 + H = 4 + H$
$1 + H = \{1, 3, 5\} = 3 + H = 5 + H$.

Άσκηση 4.8.5 *Βρείτε όλα τα αριστερά σύμπλοκα της $H = \langle 6 \rangle$ στην $\mathbb{Z}_7^*$.*

Λύση 4.8.6 $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}, H = \langle 6\rangle = \{1,6\}$.
Αριστερά σύμπλοκα:
$1H = H = 6H$
$2H = \{2,5\} = 5H$
$3H = \{3,4\} = 4H$.

Άσκηση 4.8.7 *Βρείτε όλα τα αριστερά σύμπλοκα της $H = 8\mathbb{Z}$ στην $2\mathbb{Z}$.*

Λύση 4.8.8 $2\mathbb{Z} = \{\ldots 0,2,4,6,8,10,\ldots\}, H = \{\ldots 0,8,16,24,32,\ldots\}$.
Αριστερά σύμπλοκα:
$\ldots = 0+H = H = 8+H = 16+H = \ldots$
$\ldots = 2+H = \{\ldots,2,10,18,26,34,\ldots\} = 10+H = 18+H = \ldots$
$\ldots = 4+H = \{\ldots,4,12,20,28,36,\ldots\} = 12+H = 20+H = \ldots$
$\ldots = 6+H = \{\ldots,6,14,22,30,38,\ldots\} = 14+H = 22+H = \ldots$.

Άσκηση 4.8.9 *Έστω G μια ομάδα και H μια υποομάδα της. Στο G ορίζεται μια σχέση $\smile$ με $a \smile b$ αν και μόνον αν $ab' \in H$.*
Δείξτε ότι η $\smile$ είναι σχέση ισοδυναμίας.
Στη συνέχεια, δείξτε ότι η κλάση ισοδυναμίας του a ως προς την $\smile$ ισούται με $Ha = \{ha : a \in H\}$.
*Το Ha λέγεται το **δεξιό σύμπλοκο** της H στην G που καθορίζει το a.*

Λύση 4.8.10 *Για $a,b,c \in G$, χρησιμοποιώντας σε κάθε περίπτωση ότι το H είναι υποομάδα της G,*

1. *$aa' = e \in H$, άρα $a \smile a$.*
2. *$a \smile b \Rightarrow ab' \in H \Rightarrow ba' = (ab')' \in H \Rightarrow b \smile a$.*
3. *$a \smile b, b \smile c \Rightarrow ab' \in H, bc' \in H \Rightarrow ac' = (ab')(bc') \in H \Rightarrow a \smile c$.*

Έτσι η $\smile$ είναι σχέση ισοδυναμίας.
Προφανώς, $b \smile a \Leftrightarrow ba' \in H \Leftrightarrow b = ha$ για κάποιο $h \in H$. Συνεπώς, η κλάση ισοδυναμίας του a, δηλαδή το σύνολο $\{b \in G : b \smile a\}$ ισούται με Ha.

Άσκηση 4.8.11 *Έστω G μια ομάδα και H μια υποομάδα της.*
Δείξτε ότι $aH = bH \Leftrightarrow Ha' = Hb'$ για κάθε και $a,b \in G$.

Λύση 4.8.12 *Από την Πρόταση 1.7.1,*

$$aH = bH \Leftrightarrow a \sim b \Leftrightarrow a'b = a'(b')' \in H \Leftrightarrow a' \smile b' \Leftrightarrow Ha' = Hb'.$$

Άσκηση 4.8.13 *Έστω G μια πεπερασμένη ομάδα και H μια υποομάδα της.*
Δείξτε ότι το πλήθος των δεξιών συμπλόκων της H ισούται με το πλήθος των αριστερών συμπλόκων της H.

Λύση 4.8.14 *Από την Άσκηση 4.8.11, αν τα διακεκριμένα αριστερά σύμπλοκα είναι τα $a_1H, a_2H, \ldots, a_mH$, τότε τα διακεκριμένα δεξιά σύμπλοκα είναι τα $Ha_1', Ha_2', \ldots, Ha_m'$.*

Άσκηση 4.8.15 *Έστω H μια υποομάδα κάποιας ομάδας G με $|G : H| = 2$.*
Δείξτε ότι $aH = Ha$ για κάθε στοιχείο a της G.

Λύση 4.8.16 *Αν $a \in H$, τότε $aH = H = Ha$. Μπορώ λοιπόν να υποθέσω ότι $a \notin H$, οπότε $eH = H \neq aH$ και $He = H \neq Ha$. Τώρα η G έχει μόνο δύο αριστερά σύμπλοκα, τα H και aH. Εφόσον αυτά είναι ξένα μεταξύ τους, $aH = G \setminus H$. Από την Άσκηση 4.8.13, η G έχει δύο δεξιά σύμπλοκα, τα H και Ha. Επειδή δύο διακεκριμένα δεξιά σύμπλοκα είναι ξένα μεταξύ τους, $Ha = G \setminus H = aH$.*

Άσκηση 4.8.17 *Έστω G μια ομάδα και H μια υποομάδα της.*
Δείξτε ότι $|aH| = |Ha|$ για κάθε στοιχείο a της G.

Λύση 4.8.18 *Η συνάρτηση $g : aH = Ha$, που στέλνει το ah στο ha είναι προφανώς επί. Είναι και $1 - 1$:*

$$g(ah_1) = g(ah_2) \Rightarrow h_1a = h_2a \Rightarrow h_1 = h_2 \Rightarrow ah_1 = ah_2.$$

Άσκηση 4.8.19 *Έστω G μια ομάδα με $|G| = pq$, όπου p, q είναι (όχι απαραίτητα διακεκριμένοι) πρώτοι.*
Δείξτε ότι κάθε γνήσια υποομάδα H της G είναι κυκλική.

Λύση 4.8.20 *Από το Θεώρημα Lagrange, ο αριθμός $|H|$, όντας διαιρέτης του pq, είναι ένας από τους $1, p, q, pq$. Εφόσον η H είναι γνήσια υποομάδα, ο $|H|$ ισούται με p ή q, δηλ. είναι πρώτος. Από το Πόρισμα 4.7.7, η H είναι κυκλική.*

Κεφάλαιο 5

Κι άλλες ομάδες

5.1 Ομάδες μεταθέσεων

Έστω A ένα συγκεκριμένο σύνολο. Μια συνάρτηση $f : A \to A$ η οποία είναι $1-1$ και επί λέγεται **μετάθεση** του A. Το σύνολο όλων των μεταθέσεων του A συμβολίζεται με S_A. Η σύνθεση $g \circ f$ δύο συναρτήσεων $f, g \in S_A$ είναι μια $1-1$ και επί συνάρτηση από το A στο A. Συνεπώς, $g \circ f \in S_A$ και η $\circ$ είναι πράξη στο S_A.

Θεώρημα 5.1.1 *Το $(S_A, \circ)$ αποτελεί ομάδα.*

*Απόδειξη:*5.1.1

1. Έστω $f, g, h \in S_A$. Για κάθε $x \in A$,
   $(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = ((f \circ g) \circ h)(x)$.
   Συνεπώς, $f \circ (g \circ h) = (f \circ g) \circ h$ και η $\circ$ είναι προσεταιριστική.

2. Η συνάρτηση $e = e_A : A \to A$, όπου $e(x) = x$, δρα ως το ταυτοτικό στοιχείο της S_A γιατί προφανώς $f \circ e = e \circ f = f$ για κάθε $f \in S_A$.

3. Κάθε $f : A \to A$ που ανήκει στο S_A είναι $1-1$ και επί. Συνεπώς, σε κάθε $x \in A$ αντιστοιχεί μοναδικό $y \in A$ με $x = f(y)$. Ορίζεται, επομένως, μια $1-1$ και επί συνάρτηση $f^{-1} : A \to A$ με $f^{-1}(x) = y \Leftrightarrow x = f(y)$.
   Για κάθε $a \in A$, $(f \circ f^{-1})(a) = f(f^{-1}(a)) = a$, γιατί $b = f^{-1}(a) \Rightarrow f(b) = a$. Ομοίως, $(f^{-1} \circ f)(a) = f^{-1}(f(a)) = a$. Συνεπώς, $f \circ f^{-1} = e = f^{-1} \circ f$ και το μέλος f^{-1} της S_A δρα ως το αντίστροφο του στοιχείου f.

□

Στην ειδική περίπτωση που $A = \{1, 2, \ldots, n\}$, $n \in \mathbb{N}$, η ομάδα S_A συμβολίζεται με S_n και λέγεται η **συμμετρική ομάδα σε n στοιχεία**. Τα μέλη της, εκτός του ταυτοτικού e, συνήθως συμβολίζονται με μικρά ελληνικά γράμματα και γράφουμε $\sigma\tau$ αντί $\sigma \circ \tau$. Επίσης,

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ m_1 & m_2 & \ldots & m_n \end{pmatrix}$$

συμβολίζει τη μετάθεση σ με $\sigma(1) = m_1, \sigma(2) = m_2, \ldots, \sigma(n) = m_n$. Προφανώς, υπάρχουν n επιλογές για το m_1, $n-1$ επιλογές για το m_2, ... Προκύπτει ότι $|S_n| = n!$.

Η S_1 περιέχει μόνο το e. Τα δύο στοιχεία της S_2 είναι το e και το $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. Τα στοιχεία της S_3 είναι τα

$$\rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \rho^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \rho^3 = e$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Εύκολα υπολογίζεται ότι $\mu_1\rho = \mu_2$ ενώ $\rho\mu_1 = \mu_3$. Συνεπώς, η S_3 δεν είναι αβελιανή.

Έστω Π_n το κανονικό πολύγωνο με n κορυφές $P_1, P_2, \ldots, P_n$, όπου $P_i, P_{i+1}, 1 \leq i < n$, και Pn, P_1 είναι γειτονικές κορυφές. Κάθε $\sigma \in S_n$ τέτοια ώστε οι κορυφές $P_{\sigma(i)}, P_{\sigma(i+1)}, 1 \leq i < n$, και $P_{\sigma(n)}, P_{\sigma(1)}$ γειτνιάζουν λέγεται μια **συμμετρία** του Π_n και αντιστοιχεί σε μια απεικόνιση του Π_n στο Π_n που διατηρεί την απόσταση μεταξύ σημείων. Το σύνολο των συμμετριών του Π_n αποτελεί μια υποομάδα της S_n, την **διεδρική** ομάδα D_n. Προφανώς, μια συμμετρία σ καθορίζεται από τις τιμές $\sigma(1)$ και $\sigma(2)$. Υπάρχουν, όμως, n επιλογές για το $\sigma(1)$ και δύο για το $\sigma(2)$. Έτσι, η D_n περιέχει $2n$ στοιχεία.

Για $n = 3$, Π_3 είναι το ισόπλευρο τρίγωνο και $D_3 = S_3$. Μάλιστα, η ρ αντιστοιχεί σε στροφή 120° γύρω από το κέντρο του τριγώνου, και κάθε μ_i αντιστοιχεί σε ανάκλαση ως προς τη διχοτόμο της γωνίας P_i.

Για $n = 4$, Π_4 είναι το τετράγωνο και

$$D_4 = \{\rho, \rho^2, \rho^3, \rho^4 = e, \mu_1, \mu_2, \delta_1, \delta_2\},$$

όπου

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

$$\delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

Η ρ αντιστοιχεί σε στροφή 90° γύρω από το κέντρο του τετραγώνου, οι μ_1, μ_2 αντιστοιχούν σε ανακλάσεις ως προς τις δύο μεσοκαθέτους και οι δ_1, δ_2 αντιστοιχούν σε ανακλάσεις ως προς τις δύο διαγωνίους.

5.2 Ασκήσεις

Άσκηση 5.2.1 *Να κάνετε τον πίνακα πολλαπλασιασμού της S_3.*

Λύση 5.2.2

$\circ$	e	ρ	ρ^2	μ_1	μ_2	μ_3
e	e	ρ	ρ^2	μ_1	μ_2	μ_3
ρ	ρ	ρ^2	e	μ_3	μ_1	μ_2
ρ^2	ρ^2	e	ρ	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	e	ρ	ρ^2
μ_2	μ_2	μ_3	μ_1	ρ^2	e	ρ
μ_3	μ_3	μ_1	μ_2	ρ	ρ^2	e

Άσκηση 5.2.3 *Βρείτε την τάξη όλων των στοιχείων της S_3.*

Λύση 5.2.4 $o(\rho) = o(\rho^2) = 3, o(\mu_1) = o(\mu_2) = o(\mu_3) = 2, o(e) = 1.$

Άσκηση 5.2.5 *Δείξτε ότι η D_4 δεν είναι αβελιανή.*
(: Υπολογίστε τα $\mu_1\delta_1$ και $\delta_1\mu_1$.)

Λύση 5.2.6 $\mu_1\delta_1 = \rho^3 \neq \rho = \delta_1\mu_1.$

Άσκηση 5.2.7 *Βρείτε την τάξη όλων των στοιχείων της D_4.*
Υπολογίστε το ρ^{27}.

Λύση 5.2.8 $o(\rho) = o(\rho^2) = o(\rho^3) = 4, o(\mu_1) = o(\mu_2) = o(\delta_1) = o(\delta_2) = 2, o(e) = 1.$
$\rho^{27} = \rho^{4\times 6+3} = (\rho^4)^6\rho^3 = e^6\rho^3 = \rho^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$

Άσκηση 5.2.9 *Βρείτε όλα τα αριστερά και όλα τα δεξιά σύμπλοκα της υποομάδας $H = \langle \mu_1 \rangle$ της S_3.*

Λύση 5.2.10 $H = \{e, \mu_1\}$.
Αριστερά σύμπλοκα: $eH = H = \mu_1 H$,
$\rho H = \{\rho, \rho\mu_1\} = \{\rho, \mu_3\} = \mu_3 H$,
$\rho^2 H = \{\rho^2, \rho^2\mu_1\} = \{\rho^2, \mu_2\} = \mu_2 H$.
Δεξιά σύμπλοκα:
$He = H = H\mu_1$,
$H\rho = \{\rho, \mu_1\rho\} = \{\rho, \mu_2\} = H\mu_2$,
$H\rho^2 = \{\rho^2, \mu_1\rho^2\} = \{\rho^2, \mu_3\} = H\mu_3$.

Άσκηση 5.2.11 *Δώστε ένα παράδειγμα υποομάδας H μιας ομάδας G όπου ισχύει $aH = Ha$ για όλα τα στοιχεία a της G και ένα παράδειγμα όπου δεν ισχύει.*

Λύση 5.2.12 *Ισχύει όταν η G είναι αβελιανή ομάδα.*
Δεν ισχύει για $G = S_3$ και $H = \{e, \mu_1\}$: π.χ. $\rho H \neq H\rho$.

Άσκηση 5.2.13 *Δώστε ένα παράδειγμα δύο στοιχείων a, b μιας ομάδας με $o(ab) \neq o(a)o(b)$ παρότι $\mu\kappa\delta(o(a), o(b)) = 1$. Δείτε Άσκηση 4.6.27.*

Λύση 5.2.14 *Στην S_3, αν $a = \rho, b = \mu_1$, τότε $o(a) = 3, o(b) = 2$ ενώ $o(ab) = 2 \neq 6 = o(a)o(b)$.*

5.3 Κύκλοι, τροχιές, εναλλάσσουσες ομάδες

Στο κεφάλαιο αυτό το n θα παριστάνει ένα συγκεκριμένο φυσικό αριθμό ≥ 2. Έστω $a_1, a_2, \ldots, a_m$ διακεκριμένα μέλη του $\{1, 2, \ldots, n\}$. Τότε με $(a_1\ a_2\ \ldots\ a_m)$ θα συμβολίζεται η μετάθεση που στέλνει το a_1 στο a_2, το a_2 στο a_3, ..., το a_{m-1} στο a_m, το a_m στο a_1 και αφήνει τα υπόλοιπα στοιχεία αμετάβλητα. Το $(a_1\ a_2\ \ldots\ a_m)$ είναι προφανώς μέλος της S_n τάξης m. Λέγεται **κύκλος μήκους** m. Αν $m = 1$, ο κύκλος (a_1) είναι εξ ορισμού το ταυτοτικό στοιχείο της S_n. Οι κύκλοι μήκους 2 λέγονται και **αντιμεταθέσεις**.

Παράδειγμα Στην S_5, $(1\ \ 2)$ και $(5\ \ 2)$ είναι αντιμεταθέσεις, $(3\ \ 5\ \ 4)$, $(4\ \ 3\ \ 5\ \ 1)$, $(3\ \ 2\ \ 4\ \ 5\ \ 1)$ είναι κύκλοι μήκους $3, 4, 5$, αντίστοιχα. Σημειώστε ότι σύμφωνα με τον τρόπο γραφής που υιοθετήθηκε στην Ενότητα 5.1, στην S_5,

$$\begin{aligned}(3\ \ 5\ \ 4) &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix}, \\ (3\ \ 2\ \ 4\ \ 5\ \ 1) &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}.\end{aligned}$$

Σημειώστε επίσης ότι, π.χ., στην S_6,

$$\begin{aligned}(3\ \ 5\ \ 4) &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 3 & 4 & 6 \end{pmatrix}, \\ (3\ \ 2\ \ 4\ \ 5\ \ 1) &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 5 & 1 & 6 \end{pmatrix}.\end{aligned}$$

Λήμμα 5.3.1 *Οι εξής κύκλοι είναι όλοι ίσοι:*

$$(a_1\ \ a_2\ \ \ldots\ \ a_m),\ (a_2\ \ a_3\ \ \ldots\ \ a_m\ \ a_1),\ \ldots,\ (a_m\ \ a_1\ \ \ldots\ \ a_{m-1}).$$

*Απόδειξη:*5.3.1 Εφαρμοζόμενοι σε οποιοδήποτε στοιχείο του $\{1, 2, \ldots, n\}$, οι πιο πάνω κύκλοι οδηγούν στο ίδιο αποτέλεσμα. □

Λήμμα 5.3.2 *Κάθε κύκλος $(a_1\ \ a_2\ \ \ldots\ \ a_m)$ είναι γινόμενο αντιμεταθέσεων.*

*Απόδειξη:*5.3.2 Εύκολα ελέγχεται ότι

$$(a_1\ \ a_2\ \ \ldots\ \ a_m) = (a_1\ \ a_m)(a_1\ \ a_{m-1})\ldots(a_1\ \ a_2).$$

□

Δύοι μεταθέσεις σ, τ λέγονται **ξένες** όταν

$$\{m : \sigma(m) \neq m\} \cap \{m : \tau(m) \neq m\} = \emptyset.$$

Οι $(1\ \ 3\ \ 4)$, $(2\ \ 5\ \ 6)$ είναι ξένοι κύκλοι της S_8. Οι $(1\ \ 3)(7\ \ 9)$, $(2\ \ 5\ \ 4\ \ 6)(2\ \ 6\ \ 5)$ είναι ξένες μεταθέσεις στην S_{23}.

Προφανώς, δύο κύκλοι

$$(a_1 \;\; a_2 \;\; \ldots \;\; a_k), (b_1 \;\; b_2 \;\; \ldots \;\; b_l)$$

είναι ξένοι αν και μόνο αν

$$\{a_1, a_2, \ldots, a_k\} \cap \{b_1 \;\; b_2 \;\; \ldots \;\; b_l\} = \emptyset.$$

Λήμμα 5.3.3 *Δύο ξένες μεταθέσεις σ, τ μετατίθενται, δηλαδή, $\sigma\tau = \tau\sigma$.*

*Απόδειξη:*5.3.3 Προφανώς, $\sigma\tau(m) = m = \tau\sigma(m)$ αν $\sigma(m) = m$ και $\tau(m) = m$. Διαφορετικά, μπορούμε χωρίς βλάβη της γενικότητας να υποθέσουμε ότι $\sigma(m) = m$ και $\tau(m) \neq m$, άρα $\tau\sigma(m) = \tau(m)$. Επίσης, επειδή η τ είναι $1-1$, $\tau(\tau(m)) \neq \tau(m)$. Και επειδή οι σ, τ είναι ξένες, $\sigma\tau(m) = \tau(m)$. Άρα, $\sigma\tau(m) = \tau\sigma(m)$. Συμπεραίνουμε ότι $\sigma\tau = \tau\sigma$. □

Λήμμα 5.3.4 *Έστω $\sigma \in S_n$. Στο $\{1, 2, \ldots, n\}$, η $\sim$ ορίζεται με $i \sim j \Leftrightarrow j = \sigma^m(i)$ για κάποιο $m \in \mathbb{N}$. Τότε η $\sim$ είναι σχέση ισοδυναμίας.*

*Απόδειξη:*5.3.4 Έστω $k = o(\sigma)$. Προφανώς, $1 \leq k \leq n!$ και $\sigma^k = e$. Για $1 \leq i, j, l \leq n$,

1. $\sigma^k(i) = e(i) = i \Rightarrow i \sim i$,
2. $i \sim j \Rightarrow j = \sigma^m(i)$ για κάποιο $m \in \mathbb{N} \Rightarrow i = \sigma^{-m}(j) = \sigma^{k(m+1)-m}(j)$ και $k(m+1) - m \in \mathbb{N} \Rightarrow j \sim i$,
3. $i \sim j, j \sim l \Rightarrow j = \sigma^{m_1}(i)$, $l = \sigma^{m_2}(j)$ για κάποια $m_1, m_2 \in \mathbb{N}$ $\Rightarrow l = \sigma^{m_2+m_1}(i) \Rightarrow i \sim l$.

□

Η κλάση ισοδυναμίας ενός στοιχείου i ως προς την $\sim$ λέγεται η **τροχιά** του i (ως προς την σ) και θα συμβολίζεται με $O_{\sigma,i}$. Αν m είναι ο πρώτος φυσικός αριθμός με $\sigma^m(i) = i$, τότε τα $\sigma(i)$, $\sigma^2(i)$, $\ldots, \sigma^m(i)$ είναι όλα τα στοιχεία του $O_{\sigma,i}$. Μάλιστα, αυτά είναι διακεκριμένα γιατί $\sigma^k(i) = \sigma^l(i), 1 \leq k < l \leq m$ συνεπάγεται $\sigma^{l-k}(i) = i$ παρότι $1 \leq l - k < m$. Ο κύκλος

$$(\sigma(i) \;\; \sigma^2(i) \;\; \ldots \;\; \sigma^m(i)) = (i \;\; \sigma(i) \;\; \sigma^2(i) \;\; \ldots \;\; \sigma^{m-1}(i))$$

θα συμβολίζεται με $\kappa_{\sigma,i}$.

Λήμμα 5.3.5 *Για $1 \leq i, j \leq n$ και $\sigma \in S_n$,*

1. *$\kappa_{\sigma,i}(j) = \sigma(j)$ για $j \in O_{\sigma,i}$,*
2. *$\kappa_{\sigma,i}(j) = j$ για $j \notin O_{\sigma,i}$,*
3. *$\kappa_{\sigma,i}, \kappa_{\sigma,j}$ είναι ξένοι κύκλοι για $j \notin O_{\sigma,i}$.*

*Απόδειξη:*5.3.5 Οι (1), (2) προκύπτουν άμεσα από τον ορισμό του $\kappa_{\sigma,i}$ και το Λήμμα 5.3.1, και η (3) από το γεγονός ότι οι τροχιές των i και j είναι ξένα σύνολα. □

Θεώρημα 5.3.6 *Κάθε $\sigma \in S_n$ είναι γινόμενο ξένων κύκλων.*

*Απόδειξη:*5.3.6 Έστω $O_{\sigma,i_1}, O_{\sigma,i_2}, \ldots, O_{\sigma,i_l}$ οι διακεκριμένες τροχιές των μελών του $\{1, 2, \ldots, n\}$. Τότε

$$\sigma = \kappa_{\sigma,i_1}\kappa_{\sigma,i_2}\ldots\kappa_{\sigma,i_l}.$$

Όντως, για δεδομένο στοιχείο j του $\{1, 2, \ldots, n\}$ έστω $O_{\sigma,i}$ η μοναδική από τις τροχιές $O_{\sigma,i_1}, O_{\sigma,i_2}, \ldots, O_{\sigma,i_l}$ στην οποία ανήκει. Από το Λήμμα 5.3.5, $\kappa_{\sigma,i}(j) = \sigma(j)$ και οι υπόλοιποι από τους κύκλους $\kappa_{\sigma,i_1}, \kappa_{\sigma,i_2}, \ldots, \kappa_{\sigma,i_l}$ αφήνουν το j και το $\sigma(j)$ αμετάβλητα, οπότε

$$\sigma(j) = (\kappa_{\sigma,i_1}\kappa_{\sigma,i_2}\ldots\kappa_{\sigma,i_l})(j).$$

□

Θεώρημα 5.3.7 *Κάθε $\sigma \in S_n$ είναι γινόμενο αντιμεταθέσεων.*

*Απόδειξη:*5.3.7 Αυτό έπεται από το Θεώρημα 5.3.6 και το Λήμμα 5.3.2. □

Μια μετάθεση αν γράφεται ως γινόμενο άρτιου αριθμού αντιμεταθέσεων λέγεται **άρτια**, αν γράφεται ως γινόμενο περιττού αριθμού αντιμεταθέσεων λέγεται **περιττή**. Αναμένουμε ότι μια μετάθεση δεν μπορεί να είναι ταυτόχρονα άρτια και περιττή. Αυτό όμως χρειάζεται απόδειξη.

Μέχρι και το τέλος των Ασκήσεων 5.4, το πλήθος των τροχιών μιας μετάθεσης σ θα συμβολίζεται με $T(\sigma)$.

Λήμμα 5.3.8 *Έστω σ μια μετάθεση και $\tau = (i, j)$ μια αντιμετάθεση της S_n. Τότε $T(\tau\sigma) - T(\sigma) = \pm 1$.*

*Απόδειξη:*5.3.8 Παρατηρούμε ότι η $\tau\sigma(m) = \sigma(m)$ αν το m δεν ανήκει στις τροχιές των i, j ως προς την σ, οπότε $O_{\tau\sigma,m} = O_{\sigma,m}$. Μένει να εξετάσουμε τι γίνεται με τις τροχιές $O_{\sigma,i}$ και $O_{\sigma,j}$. Διακρίνουμε δύο περιπτώσεις.

1. Αν $O_{\sigma,i} = O_{\sigma,j}$, ο κύκλος $\kappa_{\sigma,i}$ ισούται με τον $\kappa_{\sigma,j}$ και γράφεται ως

$$\kappa_{\sigma,i} = (\sigma(i) \;\; \sigma^2(i) \;\; \ldots \;\; \sigma^k(i) = j \;\; \ldots \;\; \sigma^m(i) = i).$$

   Προκύπτει ότι

$$O_{\tau\sigma,i} = \{\sigma(i), \sigma^2(i), \ldots, \sigma^{k-1}(i), \tau\sigma^k(i) = \tau(j) = i\} \text{ και}$$
$$O_{\tau\sigma,j} = \{\tau\sigma(j) = \sigma^{k+1}(i), \ldots, \sigma^{m-1}(i), \tau\sigma^m(i) = \tau(i) = j\}.$$

   Συνεπώς, $T(\tau\sigma) - T(\sigma) = 1$.

2. Αν $O_{\sigma,i} \neq O_{\sigma,j}$, οι κύκλοι $\kappa_{\sigma,i}, \kappa_{\sigma,j}$ είναι ξένοι και γράφονται ως

$$\kappa_{\sigma,i} = (\sigma(i) \;\; \sigma^2(i) \;\; \ldots \;\; \sigma^k(i) = i),\ \kappa_{\sigma,j} = (\sigma(j) \;\; \sigma^2(j) \;\; \ldots \;\; \sigma^m(j) = j).$$

Προκύπτει ότι η τροχιά $O_{\tau\sigma,i}$ ισούται με το σύνολο

$$\{\sigma(i), \sigma^2(i), \ldots, \tau\sigma^k(i) = \tau(i) = j, \sigma(j), \sigma^2(j), \ldots, \tau\sigma^m(j) = \tau(j) = i).$$

Συνεπώς, $T(\tau\sigma) - T(\sigma) = -1$.

□

Λήμμα 5.3.9 *Έστω σ μια μετάθεση και τ_1, τ_2 δύο αντιμεταθέσεις της S_n. Τότε ο αριθμός $T(\tau_1\tau_2\sigma) - T(\sigma)$ είναι άρτιος.*

*Απόδειξη:*5.3.9 Από το Λήμμα 5.3.8, ο $T(\tau_1\tau_2\sigma) - T(\sigma)$, ως το άθροισμα των δύο μονών αριθμών $T(\tau_1\tau_2\sigma) - T(\tau_2\sigma)$ και $T(\tau_2\sigma) - T(\sigma)$, είναι άρτιος. □

Πρόταση 5.3.10 *Έστω σ μια μετάθεση και $\tau_1, \tau_2, \ldots$ αντιμεταθέσεις της S_n. Τότε για κάθε $m \in \mathbb{N}$,*

1. *ο αριθμός $T(\tau_1\tau_2 \ldots \tau_{2m-1}\sigma) - T(\sigma)$ είναι περιττός και*
2. *ο $T(\tau_1\tau_2 \ldots \tau_{2m}\sigma) - T(\sigma)$ είναι άρτιος.*

*Απόδειξη:*5.3.10

1. Γίνεται με επαγωγή στο m. Από το Λήμμα 5.3.8, ισχύει για $m = 1$. Αν ισχύει για $m = k$, ο $T(\tau_3\tau_4 \ldots \tau_{2k+1}\sigma) - T(\sigma)$ είναι περιττός ενώ, από το Λήμμα 5.3.9, ο $T(\tau_1\tau_2 \ldots \tau_{2k+1}\sigma) - T(\tau_3\tau_2 \ldots \tau_{2k+1}\sigma)$ είναι άρτιος. Συνεπώς, το άθροισμά τους, δηλαδή, ο $T(\tau_1\tau_2 \ldots \tau_{2(k+1)-1}\sigma) - T(\sigma)$ είναι περιττός.

2. Από την (1), οι

$$T(\tau_1\tau_2 \ldots \tau_{2m}\sigma) - T(\tau_2\tau_3 \ldots \tau_{2m}\sigma)$$

και

$$T(\tau_2\tau_3 \ldots \tau_{2m}\sigma) - T(\sigma)$$

είναι περιττοί. Συνεπώς, το άθροισμά τους $T(\tau_1\tau_2 \ldots \tau_{2m}\sigma) - T(\sigma)$ είναι άρτιος.

□

Πρόταση 5.3.11 *Μια μετάθεση σ της S_n δεν μπορεί να είναι και περιττή και άρτια.*

*Απόδειξη:*5.3.11 Ας υποθέσουμε ότι η σ είναι περιττή. Τότε υπάρχουν αντιμεταθέσεις $\tau_1, \tau_2, \ldots, \tau_{2m-1}$ τέτοιες ώστε $\sigma = \tau_1\tau_2 \ldots \tau_{2m-1}$. Έτσι, $\sigma = \tau_1\tau_2 \ldots \tau_{2m-1}e$ και από την Πρόταση 5.3.10, ο $T(\sigma) - T(e)$ είναι περιττός. Ομοίως, αν η σ είναι άρτια, ο $T(\sigma) - T(e)$ είναι άρτιος. Συνεπώς, η σ είναι περιττή ή άρτια, όχι όμως και τα δύο. □

Η **εναλλάσσουσα ομάδα** A_n αποτελείται από όλες τις άρτιες μεταθέσεις της S_n. Είναι όντως ομάδα :

Θεώρημα 5.3.12 *Η A_n είναι υποομάδα της S_n.*

*Απόδειξη:*5.3.12

1. Είναι προφανές ότι το γινόμενο δύο άρτιων μεταθέσεων είναι μια άρτια μετάθεση.
2. $(1\ \ 2)(1\ \ 2) = e \Rightarrow e \in A_n$.
3. $\sigma \in A_n \Rightarrow \sigma = \tau_1\tau_2 \dots \tau_{2m}$, όπου οι $\tau_1, \tau_2, \dots, \tau_{2m}$ είναι αντιμεταθέσεις, $\Rightarrow \sigma^{-1} = \tau_{2m}\tau_{2m-1} \dots \tau_1 \Rightarrow \sigma^{-1} \in A_n$.

□

Θεώρημα 5.3.13 *Η A_n αποτελείται από $\frac{1}{2}n!$ στοιχεία.*

*Απόδειξη:*5.3.13 Κάθε περιττή μετάθεση τ είναι το γινόμενο της $(1\ \ 2)$ με μια $\sigma \in A_n$, όπου $\sigma = (1\ \ 2)\tau$. Συνεπώς, η A_n έχει μόνο δύο αριστερά σύμπλοκα, το $eA_n = A_n$, που αποτελείται από τις άρτιες μεταθέσεις, και το $(1,2)A_n$, που αποτελείται από τις περιττές μεταθέσεις. Άρα, $|S_n : A_n| = 2$ και, από το Θεώρημα Lagrange, $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$. □

5.4 Ασκήσεις

Άσκηση 5.4.1 *Πότε είναι άρτιος ένας κύκλος μήκους m;*

Λύση 5.4.2 *Αν και μόνον αν το μήκος του είναι περιττός αριθμός. Βλέπε απόδειξη του Λήμματος 5.3.2.*

Άσκηση 5.4.3 *Βρείτε όλες τις τροχιές της σ, γράψτε την ως γινόμενο ξένων κύκλων, γράψτε την ως γινόμενο αντιμεταθέσεων, και προσδιορίστε αν είναι άρτια ή περιττή όταν*

1. *σ είναι το μέλος της S_3 που στέλνει τους $1, 2, 3$ στους $3, 1, 2$, αντίστοιχα.*
2. *σ είναι το μέλος της S_4 που στέλνει τους $1, 2, 3, 4$ στους $4, 3, 2, 1$, αντίστοιχα*
3. *σ είναι το μέλος της S_8 που στέλνει τους $1, 2, \dots, 8$ στους $4, 3, 8, 5, 1, 7, 6, 2$, αντίστοιχα.*
4. *σ είναι το μέλος της S_9 που στέλνει τους $1, 2, \dots, 9$ στους $3, 4, 5, 6, 7, 8, 1, 2, 9$, αντίστοιχα.*

Λύση 5.4.4

1. $\sigma = (1\ \ 3\ \ 2) = (1\ \ 2)(1\ \ 3)$. *Άρτια με 1 τροχιά.*
2. $\sigma = (1\ \ 4)(2\ \ 3)$. *Άρτια με 2 τροχιές.*
3. $\sigma = (1\ \ 4\ \ 5)(2\ \ 3\ \ 8)(6\ \ 7) = (1\ \ 5)(1\ \ 4)(2\ \ 8)(2\ \ 3)(6\ \ 7)$.
   Περιττή με 3 τροχιές.

4. $\sigma = (1\ \ 3\ \ 5\ \ 7)(2\ \ 4\ \ 6\ \ 8)(9) = (1\ \ 7)(1\ \ 5)(1\ \ 3)(2\ \ 8)(2\ \ 6)(2\ \ 4)$.
Άρτια με 3 *τροχιές.*

Άσκηση 5.4.5 *Στην* S_9*, να εκφράσετε την*

$$(1\ \ 2\ \ 3\ \ 6)(1\ \ 5\ \ 4)(3\ \ 4\ \ 7\ \ 8)(8\ \ 9\ \ 2\ \ 3)$$

ως γινόμενο ξένων κύκλων.

Λύση 5.4.6 $(1\ \ 5\ \ 4\ \ 7\ \ 8\ \ 9\ \ 3\ \ 6)(2)$.

Άσκηση 5.4.7 *Γράψτε την* $(1\ \ 2\ \ 3\ \ \ldots\ \ 2m+1)^2$ *ως γινόμενο ξένων κύκλων.*

Λύση 5.4.8 $(1\ \ 3\ \ 5\ \ \ldots\ \ 2m+1\ \ 2\ \ 4\ \ 6\ \ \ldots\ \ 2m)$.

Άσκηση 5.4.9 *Δώστε όλα τα στοιχεία της* A_3.

Λύση 5.4.10 $e, (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)$.

Άσκηση 5.4.11 *Δώστε όλα τα στοιχεία της* A_4*. Είναι αβελιανή;*

Λύση 5.4.12 e, $(1,2)(3,4)$, $(1,3)(2,4)$, $(1,4)(2,3)$,
$(1\ \ 2\ \ 3)$, $(1\ \ 3\ \ 2)$, $(1\ \ 2\ \ 4)$, $(1\ \ 4\ \ 2)$, $(1\ \ 3\ \ 4)$, $(1\ \ 4\ \ 3)$, $(2\ \ 3\ \ 4)$, $(2\ \ 4\ \ 3)$.
Δεν είναι αβελιανή:

$$(1\ \ 2\ \ 3)(2\ \ 3\ \ 4) = (1\ \ 2)(3\ \ 4)$$

ενώ

$$(2\ \ 3\ \ 4)(1\ \ 2\ \ 3) = (1\ \ 3)(2\ \ 4).$$

Άσκηση 5.4.13 *Βρείτε την τάξη των στοιχείων της* A_4.

Λύση 5.4.14 $o(e) = 1$ *ενώ τα* $(1,2)(3,4)$, $(1,3)(2,4)$, $(1,4)(2,3)$ *έχουν τάξη* 2. *Τα λοιπά στοιχεία έχουν τάξη* 3.

Άσκηση 5.4.15 *Έχει η* A_4 *κυκλικές υποομάδες τάξης* 4*; Βρείτε όλες τις υποομάδες της* A_4 *τάξης* 4.

Λύση 5.4.16 *Δεν έχει κυκλικές υποομάδες τάξης* 4 *γιατί δεν έχει στοιχεία τάξης* 4. *Έτσι, από το Θεώρημα Lagrange, μια υποομάδα* H *τάξης* 4 *περιέχει μόνο στοιχεία τάξης* 2 *και το* e. *Συνεπώς,* $H = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, *που εύκολα ελέγχεται ότι είναι υποομάδα.*

5.5 Ευθέα Γινόμενα Ομάδων

Το **ευθύ γινόμενο** ομάδων G_1, G_2 είναι το καρτεσιανό γινόμενο $G_1 \times G_2$ εφοδιασμένο με την πράξη που ορίζεται με

$$(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2).$$

Στην παραπάνω φόρμουλα, προφανώς $(x_1, x_2)(y_1, y_2)$ είναι το γινόμενο των $(x_1, x_2), (y_1, y_2)$ στην $G_1 \times G_2$, x_1y_1 είναι το γινόμενο των x_1, y_1 στην G_1 και x_2y_2 είναι το γινόμενο των x_2, y_2 στην G_2.

Πιο γενικά το **ευθύ γινόμενο** ομάδων $G_1, G_2 \dots G_n$ είναι το καρτεσιανό γινόμενο $G_1 \times G_2 \times \ldots \times G_n$ εφοδιασμένο με την πράξη που ορίζεται με

$$(x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n) = (x_1y_1, x_2y_2, \ldots, x_ny_n).$$

Θεώρημα 5.5.1 *Το ευθύ γινόμενο $G_1 \times G_2 \times \ldots \times G_n$ ομάδων $G_1, G_2 \dots G_n$ είναι ομάδα. Και αν κάθε G_i είναι αβελιανή ομάδα, το ίδιο ισχύει για το ευθύ γινόμενο.*

*Απόδειξη:*5.5.1

1. $(x_1, x_2, \ldots, x_n)\big((y_1, y_2, \ldots, y_n)(z_1, z_2, \ldots, z_n)\big) =$
   $(x_1, x_2, \ldots, x_n)(y_1z_1, y_2z_2, \ldots, y_nz_n) = (x_1(y_1z_1), x_2(y_2z_2), \ldots, x_n(y_nz_n))$
   $= ((x_1y_1)z_1, (x_2y_2)z_2, \ldots, (x_ny_n)z_n) = (x_1y_1, x_2y_2, \ldots, x_ny_n)(z_1, z_2, \ldots, z_n)$
   $\big((x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n)\big)(z_1, z_2, \ldots, z_n)$,
   όπου η τρίτη ισότητα οφείλεται στο ότι η πράξη της κάθε G_i είναι προσεταιριστική. Έτσι η πράξη του γινομένου είναι προσεταιριστική. Με ανάλογο τρόπο αποδεικνύεται ότι

2. το $e = (e_1, e_2, \ldots, e_n)$ είναι το ταυτοτικό του γινομένου, όπου e_i είναι το ταυτοτικό της G_i.

3. το $(x_1', x_2', \ldots, x_n')$ είναι το αντίστροφο του $(x_1, x_2, \ldots, x_n)$, όπου x_i' είναι το αντίστροφο του x_i στην G_i.

4. αν κάθε G_i είναι αβελιανή ομάδα, το ίδιο ισχύει για το γινόμενο.

□

Σημείωση. Όταν η πράξη της κάθε μίας από της G_i είναι η $+$, τότε και η πράξη του γινομένου τους συμβολίζεται με $+$ και το ταυτοτικό της με 0.
Η ομάδα $\mathbb{R}^n$, ως προς την πρόσθεση, είναι το ευθύ γινόμενο n αντιτύπων της ομάδας $\mathbb{R}$. Ομοίως, το ευθύ γινόμενο n αντιτύπων ομάδας G συμβολίζεται με G^n.

Θεώρημα 5.5.2 *Αν $\mu\kappa\delta(m, n) = 1$, τότε η $\mathbb{Z}_m \times \mathbb{Z}_n$ είναι κυκλική τάξης mn.*

*Απόδειξη:*5.5.2 Επειδή στην $\mathbb{Z}_m \times \mathbb{Z}_n$, $k(1, 1) = (k, k)$, και $0 = (0, 0)$, έχουμε
$k(1, 1) = 0$ στην $\mathbb{Z}_m \times \mathbb{Z}_n \Leftrightarrow k = 0$ στην $\mathbb{Z}_m$ και $k = 0$ στην $\mathbb{Z}_n \Leftrightarrow$ (από το Θεώρημα 4.5.6) $m|k$ και $n|k \Leftrightarrow$ (από την Άσκηση 2.2.19) $mn|k$.
Προκύπτει ότι το στοιχείο $(1, 1)$ της $\mathbb{Z}_m \times \mathbb{Z}_n$ έχει τάξη mn και, αφού $|\mathbb{Z}_m \times \mathbb{Z}_n| = mn$, $\mathbb{Z}_m \times \mathbb{Z}_n = \langle(1, 1)\rangle$. Συνεπώς , η $\mathbb{Z}_m \times \mathbb{Z}_n$ είναι κυκλική με ένα γεννήτορα το $(1, 1)$. □

5.6 Ασκήσεις

Άσκηση 5.6.1 *Βρείτε την τάξη του στοιχείου $g = (\alpha, 2)$ της $V \times \mathbb{Z}_5^*$.*
Σημείωση: V είναι η ομάδα του Klein της ενότητας 3.7.

Λύση 5.6.2 *Έχουμε*
$g^2 = (1, 4), g^3 = (\alpha, 3), g^4 = (1, 1) = e$.

Συνεπώς, $o(g) = 4$.

Άσκηση 5.6.3 *Βρείτε την τάξη του στοιχείου $g = (2, 3, 6)$ της $\mathbb{Z}_3^* \times \mathbb{Z}_5^* \times \mathbb{Z}_7^*$.*

Λύση 5.6.4 *Έχουμε*
$g^2 = (1, 4, 1), g^3 = (2, 2, 6), g^4 = (1, 1, 1) = e$.

Συνεπώς, $o(g) = 4$.

Άσκηση 5.6.5 *Βρείτε την τάξη κάθε στοιχείου της $\mathbb{Z}_2 \times \mathbb{Z}_2$.*
Είναι η $\mathbb{Z}_2 \times \mathbb{Z}_2$ κυκλική;

Λύση 5.6.6 *Πλην του 0, τα λοιπά στοιχεία έχουν τάξη $2 < 4 = |\mathbb{Z}_2 \times \mathbb{Z}_2|$. Άρα η $\mathbb{Z}_2 \times \mathbb{Z}_2$ δεν είναι κυκλική.*

Άσκηση 5.6.7 *Βρείτε την τάξη κάθε στοιχείου της $\mathbb{Z}_2 \times \mathbb{Z}_4$.*
Είναι η $\mathbb{Z}_2 \times \mathbb{Z}_4$ κυκλική;

Λύση 5.6.8 *Το 0 έχει τάξη 1.*
Το $(0, 1)$ έχει τάξη 4, όπως και τα $(1, 1), (0, 3), (1, 3)$.
Τα $(0, 2), (1, 0), (1, 2)$ έχουν τάξη 2.
Άρα η $\mathbb{Z}_2 \times \mathbb{Z}_4$, που έχει 8 στοιχεία, δεν είναι κυκλική.

Άσκηση 5.6.9 *Βρείτε την τάξη κάθε στοιχείου της $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.*
Είναι η $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ κυκλική;

Λύση 5.6.10 *Πλην του 0, τα λοιπά 7 στοιχεία έχουν τάξη 2. Άρα η $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ δεν είναι κυκλική.*

Άσκηση 5.6.11 *Αν $\mu\kappa\delta(m, n) \neq 1$, να δείξετε ότι η $\mathbb{Z}_m \times \mathbb{Z}_n$ δεν είναι κυκλική.*

Λύση 5.6.12 *Ο ακέραιος $k = \frac{mn}{d}$, όπου $d = \mu\kappa\delta(m, n)$, είναι μικρότερος του $mn = |\mathbb{Z}_m \times \mathbb{Z}_n|$. Για κάθε στοιχείο (i, j) της $\mathbb{Z}_m \times \mathbb{Z}_n$, $k(i, j) = (ki, kj) = (\frac{n}{d}m, \frac{m}{d}n) = (0, 0) = 0$. Συνεπώς, $o(i, j) \leq k < mn$ και η $\mathbb{Z}_m \times \mathbb{Z}_n$ δεν είναι κυκλική.*

Κεφάλαιο 6

Πόσες ομάδες;

6.1 Ομομορφισμοί

Έχουμε ήδη συναντήσει ένα αρκετά μεγάλο αριθμό ομάδων τάξης 4. Το ερώτημα πού τίθεται είναι ποιες από αυτές είναι ουσιαστικά διαφορετικές, δηλαδή, ποιες έχουν διαφορετικές αλγεβρικές ιδιότητες. Πιο γενικά, πότε θα θεωρούμε ότι δύο ομάδες είναι αλγεβρικά ισοδύναμες; Η απάντηση είναι: όταν οι δύο ομάδες είναι **ισόμορφες**. Ακολουθούν οι σχετικοί ορισμοί.

Ορισμός 6.1.1 *Έστω G_1, G_2 δύο ομάδες. Μια συνάρτηση $\phi : G_1 \to G_2$ λέγεται ομομορφισμός (ομάδων) αν για κάθε $x, y \in G_1$,*

$$\phi(xy) = \phi(x)\phi(y).$$

Παρατήρηση. Στον παραπάνω ορισμό, το xy παριστάνει το γινόμενο στην G_1 των δύο στοιχείων της x, y, ενώ το $\phi(x)\phi(y)$ παριστάνει το γινόμενο στην G_2 των δύο στοιχείων της $\phi(x), \phi(y)$.

Παραδείγματα. Η συνάρτηση $\phi : \mathbb{R} \to \mathbb{R}$ που ορίζεται με $\phi(x) = 3x$ είναι ομομορφισμός γιατί $\phi(x + y) = 3(x + y) = 3x + 3y = \phi(x) + \phi(y)$. Όμως, η $\phi : \mathbb{R}^* \to \mathbb{R}$ που ορίζεται με τον ίδιο τύπο, $\phi(x) = 3x$, δεν είναι ομομορφισμός, γιατί εδώ πρέπει να ισχύει $\phi(x \cdot y) = 3(x \cdot y) = \phi(x) + \phi(y) = 3x + 3y$, για κάθε $x, y \in \mathbb{R}^*$. Αυτό δεν ισχύει π.χ. για $x = y = 1$.

Έστω $\phi : G_1 \to G_2$ ένας ομομορφισμός ομάδων. Ο ϕ λέγεται **μονομορφισμός** (ομάδων) αν η ϕ (ως συνάρτηση) είναι $1 - 1$. Ο ϕ λέγεται **επιμορφισμός** αν η ϕ είναι επί. Ο ϕ λέγεται **ισομορφισμός** αν η ϕ είναι $1 - 1$ και επί.
Δύο ομάδες G_1, G_2 λέγονται **ισόμορφες** (κατ' άλλους **ισομορφικές**) αν υπάρχει κάποιος ισομορφισμός $\phi : G_1 \to G_2$.

Παρατήρηση. Έστω G_1 μια ομάδα η οποία αποτελείται από διακεκριμένα στοιχεία $x_1, x_2, \ldots$. Έστω G_2 μια δεύτερη ομάδα και $\phi : G_1 \to G_2$ μια συνάρτηση

που είναι $1-1$ και επί. Αυτό σημαίνει ότι τα $\phi(x_1), \phi(x_2), \ldots$ είναι διακεκριμένα και μάλιστα είναι όλα τα στοιχεία της G_2. Τώρα, η ϕ είναι ισομομορφισμός αν και μόνον αν, για κάθε $x_i, x_j \in G_1$, $\phi(x_i)\phi(x_j) = \phi(x_i x_j)$. Δηλαδή, η ϕ είναι ισομομορφισμός αν και μόνον αν αντικαθιστώντας στον πίνακα της G_1 κάθε $x \in G_1$ με το αντίστοιχο $\phi(x) \in G_2$ εκείνο το οποίο προκύπτει είναι ο πίνακας της G_2.

Ακολουθούν οι βασικές ιδιότητες ομομορφισμών.

Θεώρημα 6.1.2 *Έστω $\phi : G_1 \to G_2$ ένας ομομορφισμός ομάδων. Τότε*

1. $\phi(e) = e$,
2. $\phi(x') = \phi(x)'$ *για κάθε* $x \in G_1$ *και*
3. $\phi(x^n) = \phi(x)^n$ *για κάθε* $x \in G_1$ *και* $n \in \mathbb{Z}$.

*Απόδειξη:*6.1.2

1. Για να είμαστε πιο ακριβείς, στην (1) θέλουμε να δείξουμε ότι $\phi(e_1) = e_2$, όπου e_1, e_2 είναι τα ταυτοτικά των G_1, G_2, αντίστοιχα. Προφανώς, $\phi(e_1) = \phi(e_1 e_1) = \phi(e_1)\phi(e_1)$ επειδή ο ϕ είναι ομομορφισμός. Έτσι, $\phi(e_1)\phi(e_1) = \phi(e_1)e_2$ και, από τον αριστερό νόμο διαγραφής στην G_2, $\phi(e_1) = e_2$.

2. Από την (1), $\phi(x)\phi(x') = \phi(xx') = \phi(e_1) = e_2 = \phi(x)\phi(x)'$ και, από τον αριστερό νόμο διαγραφής στην G_2, $\phi(x') = \phi(x)'$.

3. Το αποτέλεσμα ισχύει για $n = 1$ και από την (1) για $n = 0$. Έστω ότι ισχύει για κάποιο $n \in \mathbb{N}$, δηλαδή, $\phi(x^n) = \phi(x)^n$. Τότε,

   (α′) $\phi(x^{n+1}) = \phi(x^n x) = \phi(x^n)\phi(x) = \phi(x)^n\phi(x) = \phi(x)^{n+1}$, δηλαδή, το αποτέλεσμα ισχύει για τον $n+1$. Από την αρχή της επαγωγής το αποτέλεσμα ισχύει για κάθε $n \in \mathbb{N}$.

   (β′) από την (2), $\phi((x^n)') = (\phi(x)^n)'$, δηλαδή, $\phi(x^{-n}) = \phi(x)^{-n}$ και το αποτέλεσμα ισχύει για τον $-n$. Έτσι, το αποτέλεσμα ισχύει για κάθε $n \in \mathbb{Z}$.

□

Θεώρημα 6.1.3 *Έστω $\phi : G_1 \to G_2$ ένας μονομορφισμός ομάδων και $a \in G_1$. Τότε $o(a) = o(\phi(a))$.*

*Απόδειξη:*6.1.3 Από το Θεώρημα 6.1.2, $\phi(a^n) = \phi(a)^n$ και $\phi(e) = e$. Μάλιστα, επειδή η συνάρτηση ϕ είναι $1-1$, $\phi(x) = e$ αν και μόνον αν $x = e$.

1. Για κάθε k με $1 \le k < o(a)$, από το Θεώρημα 4.5.6, $a^k \neq e$. Άρα, $\phi(a)^k = \phi(a^k) \neq e$. Συνεπώς, $o(a) \le o(\phi(a))$.

2. Για κάθε k με $1 \le k < o(\phi(a))$, από το Θεώρημα 4.5.6, $\phi(a^k) = \phi(a)^k \neq e$. Άρα, $a^k \neq e$. Συνεπώς, $o(\phi(a)) \le o(a)$.

Από τις (1) και (2) συμπεραίνουμε ότι $o(a) = o(\phi(a))$. □

Θεώρημα 6.1.4 *Έστω $\phi : G_1 \to G_2$ ένας επιμορφισμός ομάδων. Αν η G_1 είναι αβελιανή, τότε και η G_2 είναι αβελιανή. Αν η G_1 είναι κυκλική, τότε και η G_2είναι κυκλική.*

*Απόδειξη:*6.1.4 Έστω ότι η G_1 είναι αβελιανή. Για κάθε $y_1, y_2 \in G_2$, επειδή η ϕ είναι επί, $y_1 = \phi(x_1), y_2 = \phi(x_2)$ για κάποια $x_1, x_2 \in G_1$. Επειδή η G_1 είναι αβελιανή, $x_1x_2 = x_2x_1$ και επειδή η ϕ είναι ομομορφισμός, $y_1y_2 = \phi(x_1)\phi(x_2) = \phi(x_1x_2) = \phi(x_2x_1) = \phi(x_2)\phi(x_1) = y_2y_1$. Συνεπώς, η G_2 είναι αβελιανή.
Έστω τώρα ότι η G_1 είναι κυκλική. Τότε $G_1 = \langle a\rangle = \{a^n : n \in \mathbb{Z}\}$ για κάποιο a. Για κάθε $y \in G_2$, επειδή η ϕ είναι επί, $y = \phi(x)$ για κάποιο $x \in G_1$. Όμως, $x = a^n$ για κάποιο $n \in \mathbb{Z}$, οπότε, από το Θεώρημα 6.1.2, $y = \phi(a^n) = \phi(a)^n$. Συνεπώς, η G_2 είναι κυκλική με ένα γεννήτορα το $\phi(a)$. □

Θεώρημα 6.1.5 *Έστω $\phi : G_1 \to G_2$ και $\psi : G_2 \to G_3$ ομομορφισμοί ομάδων. Τότε η σύνθετη συνάρτηση $\psi \circ \phi : G_1 \to G_3$ είναι ομομορφισμός. Αν οι ϕ και ψ είναι μονομορφισμοί, επιμορφισμοί ή ίσομορφισμοί, τότε την ίδια ιδιότητα έχει και η $\psi \circ \phi$.*

*Απόδειξη:*6.1.5 Για κάθε $x, y \in G_1$,

$$(\psi \circ \phi)(xy) = \psi(\phi(xy)) = \psi(\phi(x)\phi(y)) = \psi(\phi(x))\psi(\phi(y)) = (\psi \circ \phi)(x)(\psi \circ \phi)(y)$$

όπου η δεύτερη ισότητα ισχύει γιατί ο ϕ είναι ομομορφισμός και η τρίτη γιατί ο ψ είναι ομομορφισμός. Έπεται ότι η $\psi \circ \phi$ είναι ομομορφισμός.
Αν τώρα οι συναρτήσεις ϕ και ψ είναι και οι δύο $1-1$ (αντίστοιχα, επί), τότε ως γνωστόν και η $\psi \circ \phi$ είναι $1-1$ (αντίστοιχα, επί). Έπεται ότι, αν οι ϕ και ψ είναι μονομορφισμοί, επιμορφισμοί ή ίσομορφισμοί, τότε την ίδια ιδιότητα έχει και η $\psi \circ \phi$. □

Θεώρημα 6.1.6 *Έστω $\phi : G_1 \to G_2$ ένας ισομορφισμός ομάδων. Τότε και η αντίστροφη συνάρτηση $\phi^{-1} : G_2 \to G_1$ είναι ισομορφισμός.*

*Απόδειξη:*6.1.6 Για κάθε $x, y \in G_2$, επειδή ο ϕ είναι ομομορφισμός,

$$\phi(\phi^{-1}(x)\phi^{-1}(y)) = \phi(\phi^{-1}(x))\phi(\phi^{-1}(y)) = xy.$$

Συνεπώς, $\phi^{-1}(xy) = \phi^{-1}(x)\phi^{-1}(y)$ και η ϕ^{-1} είναι ομομορφισμός. Άρα, επειδή ως γνωστόν η αντίστροφη συνάρτηση όταν ορίζεται είναι $1-1$ και επί, η ϕ^{-1} είναι ισομορφισμός. □

Γράφουμε $G_1 \cong G_2$ αν οι δύο ομάδες G_1, G_2 είναι **ισόμορφες**, δηλαδή, αν υπάρχει κάποιος ισομορφισμός $\phi : G_1 \to G_2$. Προφανώς, $G \cong G$ για κάθε ομάδα γιατί η ταυτοτική απεικόνιση $G \to G$ είναι ισομορφισμός. Από τα τελευταία δύο θεωρήματα, η $\cong$ είναι σχέση ισοδυναμίας. Δύο ισόμορφες ομάδες έχουν τις ίδιες αλγεβρικές ιδιότητες. Π.χ.(1) έχουν το ίδιο πλήθος στοιχείων, (2) αν η μια περιέχει ένα στοιχείο τάξης m, τότε και η άλλη περιέχει ένα στοιχείο τάξης m (βλέπε Θεώρημα 6.1.3), (3) αν η μια είναι αβελιανή, τότε και η άλλη είναι αβελιανή, (4) αν η μια είναι κυκλική, τότε και η άλλη είναι κυκλική (βλέπε Θεώρημα 6.1.4). Στην Άλγεβρα, δύο ισόμορφες ομάδες θεωρούνται ίδιες.

Θεώρημα 6.1.7 *Η μόνη άπειρη κυκλική ομάδα είναι η $\mathbb{Z}$.*

*Απόδειξη:*6.1.7 Έστω G μια άπειρη κυκλική ομάδα με γεννήτορα το a. Τότε $a^k = e$ μόνο για $k = 0$.
Ορίζουμε μια συνάρτηση $\phi : \mathbb{Z} \to G$ με $\phi(n) = a^n$. Από ιδιότητες δυνάμεων, $\phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n)$ και η ϕ είναι ομομορφισμός. Η ϕ είναι επί γιατί κάθε μέλος της G είναι δύναμη του a. Η ϕ είναι $1-1$ γιατί

$$\phi(m) = \phi(n) \Rightarrow a^m = a^n \Rightarrow a^{m-n} = e \Rightarrow m - n = 0 \Rightarrow m = n.$$

Συνεπώς, ο ϕ είναι ισομορφισμός και η G είναι ισόμορφη με την $\mathbb{Z}$. □

Πόρισμα 6.1.8 *Δύο άπειρες κυκλικές ομάδες είναι ισόμορφες.*

Θεώρημα 6.1.9 *Δύο πεπερασμένες κυκλικές ομάδες της ίδιας τάξης είναι ισόμορφες.*

*Απόδειξη:*6.1.9 Έστω G, H δύο κυκλικές ομάδες τάξης $k < \infty$. Έστω a ένας γεννήτορας της G και b ένας γεννήτορας της H. Ορίζουμε μια συνάρτηση $\phi : G \to H$ με $\phi(a^n) = b^n$. Η ϕ είναι καλά ορισμένη: $a^m = a^n \Rightarrow a^{m-n} = e \Rightarrow k = o(a) = o(b) | m - n \Rightarrow b^{m-n} = e \Rightarrow b^m = b^n \Rightarrow \phi(a^m) = \phi(a^n)$.
Από ιδιότητες δυνάμεων, $\phi(a^{m+n}) = b^{m+n} = b^m b^n = \phi(a^m)\phi(a^n)$, και η ϕ είναι ομομορφισμός.
Η ϕ είναι επί γιατί κάθε μέλος της H είναι δύναμη του b.
Η ϕ είναι $1-1$ γιατί $\phi(a^m) = \phi(a^n) \Rightarrow b^m = b^n \Rightarrow$
$b^{m-n} = e \Rightarrow k = o(a) = o(b) | m - n \Rightarrow a^{m-n} = e \Rightarrow a^m = a^n$.
Συνεπώς, ο ϕ είναι ισομορφισμός και οι G, H είναι ισόμορφες. □

Πόρισμα 6.1.10 *Η μόνη κυκλική ομάδα ταξης n είναι η $\mathbb{Z}_n$.*

6.2 Ασκήσεις

Άσκηση 6.2.1 *Δείξτε ότι η $\phi : \mathbb{R} \to \mathbb{R}^+$, όπου $\phi(x) = e^x$, είναι ομομορφισμός. Είναι η ϕ ισομομορφισμός;*

Λύση 6.2.2 *Η ϕ είναι ομομορφισμός γιατί, από ιδιότητες δυνάμεων, $\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$.*
Η ϕ είναι $1-1$ και επί γιατί, ως γνωστόν, σε κάθε στοιχείο y του $\mathbb{R}^+$ αντιστοιχεί ένα και μοναδικό $x = log(y) \in \mathbb{R}$ με $\phi(x) = y$. Συνεπώς, η ϕ ισομομορφισμός.

Άσκηση 6.2.3 *Δείξτε ότι η $f : \mathbb{R} \to \mathbb{R}^*$, όπου $f(x) = 2^x$, είναι ομομορφισμός. Είναι η f μονομορφισμός, επιμορφισμός ή ισομορφισμός;*

Λύση 6.2.4 *Η f είναι ομομορφισμός για τον ίδιο λόγο που η ϕ της Άσκησης 6.2.1 είναι ομομορφισμός.*
Είναι μονομορφισμός γιατί $f(x) = f(y) \Rightarrow 2^x = 2^y \Rightarrow 2^{x-y} = 0 \Rightarrow x = y$.
Δεν είναι επιμορφισμός γιατί κάθε $f(x)$ είναι θετικό. Έτσι, π.χ., δεν υπάρχει $x \in \mathbb{R}$ με $f(x) = -1$. Συνεπώς, η f δεν είναι ούτε ισομορφισμός.

Άσκηση 6.2.5 *Είναι η $f : \mathbb{R}^* \to \mathbb{R}^*$, όπου $f(x) = |x|$, ομομορφισμός, μονομορφισμός, επιμορφισμός ή ισομορφισμός;*

Λύση 6.2.6 *Ως γνωστόν, $|xy| = |x||y|$, δηλ. $f(xy) = f(x)f(y)$. Άρα η f είναι ομομορφισμός.*
Δεν είναι μονομορφισμός, άρα ούτε ισομορφισμός, γιατί π.χ. $f(1) = f(-1)$.
Δεν είναι επιμορφισμός γιατί π.χ. $-1 \neq f(x)$ για κάθε $x \in \mathbb{R}^*$.

Άσκηση 6.2.7 *Είναι η $g : \mathbb{R} \to \mathbb{R}$, όπου $g(x) = |x|$, ομομορφισμός;*

Λύση 6.2.8 *Όχι: $g(3 + (-3)) = g(0) = 0 \neq 6 = |3| + |-3| = g(3) + g(-3)$.*

Άσκηση 6.2.9 *Να εξετάσετε κατά πόσον οι συναρτήσεις $f, g, h : \mathbb{R} \to \mathbb{R}$, οι οποίες ορίζονται με $f(x) = 2x + 3, g(x) = 5x, h(x) = x^5$, είναι ισομορφισμοί;*

Λύση 6.2.10 *$f(0 + 3) = f(3) = 3 \neq 3 + 9 = f(0) + f(3)$. Συνεπώς, η f δεν είναι ούτε καν ομομορφισμός.*
$g(x + y) = 5(x + y) = 5x + 5y = g(x) + g(y)$. Άρα η g είναι ομομορφισμός. Μάλιστα, είναι ισομορφισμός γιατί εύκολα δείχνεται ότι η g είναι $1 - 1$ και επί.
$h(1 + 1) = 2^5 \neq 1 + 1 = h(1) + h(1)$. Συνεπώς, η h δεν είναι ούτε καν ομομορφισμός.

Άσκηση 6.2.11 *Υπάρχουν δύο από τις ομάδες $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_6$, S_3, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ που να είναι ισόμορφες;*

Λύση 6.2.12 *Όχι. Δύο ισόμορφες ομάδες έχουν την ίδια τάξη. Συνεπώς,*
(1) Η $\mathbb{Z}_4$ μόνο με την $\mathbb{Z}_2 \times \mathbb{Z}_2$ θα μπορούσε να είναι ισόμορφη. Δεν είναι όμως ισόμορφες γιατί η πρώτη ομάδα είναι κυκλική, όχι όμως και η δεύτερη.
(2) Η $\mathbb{Z}_6$ μόνο με την S_3 θα μπορούσε να είναι ισόμορφη. Δεν είναι όμως ισόμορφες γιατί η πρώτη ομάδα είναι αβελιανή, όχι όμως και η δεύτερη.
(3) Η $\mathbb{Z}_8$ μόνο με τις $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ θα μπορούσε να είναι ισόμορφη. Δεν είναι όμως ισόμορφη με αυτές γιατί η $\mathbb{Z}_8$ είναι κυκλική, όχι όμως και οι άλλες δύο.
(4) Τέλος, η $\mathbb{Z}_2 \times \mathbb{Z}_4$ έχει στοιχείο τάξης 4, π.χ. το $(0, 1)$, ενώ κάθε στοιχείο της $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ έχει τάξη ≤ 2. Άρα, οι $\mathbb{Z}_2 \times \mathbb{Z}_4$ και $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ δεν είναι ισόμορφες.

Άσκηση 6.2.13 *Έστω p ένας πρώτος αριθμός. Πόσες ομάδες τάξης p υπάρχουν;*

Λύση 6.2.14 *Μία, γιατί από το Πόρισμα 4.7.7 μια τέτοια ομάδα είναι κυκλική τάξης p και, από το Πόρισμα 6.1.10, είναι ισόμορφη με την $\mathbb{Z}_p$.*

Άσκηση 6.2.15 *Έστω G μια μη κυκλική ομάδα τάξης 4. Να δείξετε ότι*

1. *$x^2 = e$, άρα $x = x'$, για κάθε $x \in G$,*
2. *$xy = z$, αν x, y, z είναι τα διακεκριμένα μη ταυτοτικά στοιχεία της G,*
3. *η G είναι αβελιανή.*

Λύση 6.2.16 *1. Επειδή, η τάξη του x, $o(x)$, διαιρεί την τάξη της G, δηλ το 4, $o(x) = 1, 2$ ή 4. Επειδή η G δεν είναι κυκλική, $o(x) \neq 4$. Συνεπώς, $o(x) = 1$ ή 2. Σε κάθε περίπτωση $x^2 = e$.*

2. *(α′) Από την (1), $xy = e \Rightarrow x = y' = y$!*

   (β′) Από το δεξιό νόμο διαγραφής, $xy = y = ey \Rightarrow x = e$!

   (γ′) Από τον αριστερό νόμο διαγραφής, $xy = x = xe \Rightarrow y = e$!
   Μένει η επιλογή $xy = z$.

3. *Θέλω να δείξω ότι $xy = yx$, για κάθε $x, y \in G$. Αυτό είναι προφανές όταν $x = e$ ή $y = e$ και, από την (1), όταν $x = y$. Συνεπώς, μπορούμε να υποθέσουμε ότι x, y είναι δύο από τα τρία μη ταυτοτικά στοιχεία της G. Τώρα, από την (2), xy και yx ισούνται με το τρίτο μη ταυτοτικό στοιχείο της G. Άρα, $xy = yx$.*

Άσκηση 6.2.17 *Έστω G_1, G_2 δύο μη κυκλικές ομάδες τάξης 4, και $f : G_1 \to G_2$ μία $1-1$ και επί συνάρτηση με $f(e) = e$. Να δείξετε ότι η f είναι ισομορφισμός.*

Λύση 6.2.18 *Αρκεί να δείξουμε ότι $f(xy) = f(x)f(y)$ για κάθε $x, y \in G$. Αυτό προφανώς ισχύει όταν $x = e$ ή $y = e$ και, από την Άσκηση 6.2.15, όταν $x = y$. Μένει η περίπτωση που x, y είναι δύο από τα τρία μη ταυτοτικά στοιχεία της G_1, οπότε $xy = z$ είναι το τρίτο. Επειδή, η f είναι $1-1$ και επί και $f(e) = e$, τα $f(x), f(y), f(z)$ είναι τα τρία μη ταυτοτικά στοιχεία της G_2. Από την Άσκηση 6.2.15, $f(x)f(y) = f(z)$. Συνεπώς, $f(xy) = f(z) = f(x)f(y)$.*

Άσκηση 6.2.19 *Πόσες ομάδες τάξης 4 υπάρχουν;*

Λύση 6.2.20 *Αν μια ομάδα τάξης 4 είναι κυκλική τότε είναι ισόμορφη με την $\mathbb{Z}_4$. Αν δεν είναι κυκλική, από την Άσκηση 6.2.17, τότε είναι ισόμορφη με την 4-ομάδα V του Klein. Συνεπώς, οι $\mathbb{Z}_4$ και V είναι οι μόνες ομάδες τάξης 4.*

Άσκηση 6.2.21 *Πόσοι ισομορφισμοί $f : V \to V$ υπάρχουν;*

Λύση 6.2.22 *Από την Άσκηση 6.2.17, μια συνάρτηση $f : V \to V$ είναι ισομορφισμός αν και μόνο αν $f(e) = e$ και η f είναι $1-1$ και επί. Υπάρχουν 3 επιλογές για το $f(\alpha)$, 2 για το $f(\beta)$ και 1 για το $f(\gamma)$. Συνεπώς, υπάρχουν 6 τέτοιες συναρτήσεις.*

Άσκηση 6.2.23 *Έστω G, H δύο ομάδες πεπερασμένης τάξης, $\phi : G \to H$ ένας ομομορφισμός, $a \in G$, $m = o(a)$ και $n = o(\phi(a))$. Να δείξετε ότι*

1. *$n|m$, και*

2. *$m = n$ όταν ο ϕ είναι μονομορφισμός.*

Ισχύει πάντοτε ότι $m = n$, ακόμη και όταν ο ϕ είναι απλά ένας ομομορφισμός;

Λύση 6.2.24 *1. $a^m = e$ και από το Θεώρημα 6.1.2, $\phi(a)^m = \phi(a^m) = \phi(e) = e$. Συνεπώς, από το Θεώρημα 4.5.6, $n|m$.*

2. *όταν ο ϕ είναι μονομορφισμός, η $\phi(a^n) = \phi(a)^n = e = \phi(e)$ συνεπάγεται $a^n = e$. Άρα, από το Θεώρημα 4.5.6, $m|n$. Από την (1), $m = n$.*

Δεν ισχύει ότι $m = n$, π.χ., όταν η $\phi : G \to H$ ορίζεται με $\phi(x) = e$, για κάθε $x \in G$, και $a \neq e$.

Άσκηση 6.2.25 *Πόσοι ομομορφισμοί $f : \mathbb{Z}_4 \to \mathbb{Z}_7$ υπάρχουν;*

Λύση 6.2.26 *Από την Άσκηση 6.2.23, για το 1 του $\mathbb{Z}_4$, η $o(f(1))$ διαιρεί την $o(1) = 4$. Από το Πόρισμα 4.7.6, η $o(f(1))$ διαιρεί την $|\mathbb{Z}_7| = 7$. Συνεπώς, $o(f(1)) = 1$ και $f(1) = 0$. Έπεται ότι ο μόνος ομομορφισμός $f : \mathbb{Z}_7 \to \mathbb{Z}_4$ είναι ο τετριμμένος ομομορφισμός που ορίζεται με $f(x) = 0$.*

Άσκηση 6.2.27 *Έστω G μια ομάδα. Η $f : G \to G$ ορίζεται με $f(x) = x'$. Αν η f είναι ομομορφισμός, να δείξετε ότι η G είναι αβελιανή.*

Λύση 6.2.28 *Για κάθε $x, y \in G$, $f(xy) = f(x)f(y)$. Δηλαδή, $(xy)' = x'y'$. Από το Πόρισμα 3.3.6, $(xy)' = y'x'$. Συνεπώς, $x'y' = y'x'$, άρα και $x''y'' = y''x''$, δηλαδή $xy = yx$.*

Άσκηση 6.2.29 *Έστω G μια ομάδα. Η $f : G \to G$ ορίζεται με $f(x) = x^2$. Αν η f είναι ομομορφισμός, να δείξετε ότι η G είναι αβελιανή.*

Λύση 6.2.30 *Για κάθε $x, y \in G$, $f(xy) = f(x)f(y)$. Δηλαδή, $xyxy = xxyy$. Εφαρμόζοντας τον κανόνα διαγραφής δύο φορές, έχουμε ότι $yxy = xyy$ και $yx = xy$.*

Άσκηση 6.2.31 *Έστω G μια αβελιανή ομάδα και $n \in \mathbb{Z}$. Η $f : G \to G$ ορίζεται με $f(x) = x^n$. Να δείξετε ότι η f είναι ομομορφισμός.*

Λύση 6.2.32 *Από την Άσκηση 4.6.25, $f(xy) = (xy)^n = x^n y^n = f(x)f(y)$.*

6.3 Κανονικές υποομάδες και πυρήνες ομομορφισμών

Μια υποομάδα H μιας ομάδας G λέγεται **κανονική υποομάδα** αν

$$g \in G, h \in H \Rightarrow ghg' \in H.$$

Πρόταση 6.3.1 *Κάθε υποομάδα H μιας αβελιανής ομάδας G είναι κανονική.*

*Απόδειξη:*6.3.1 Για κάθε $g \in G$ και $h \in H$, έχουμε ότι $ghg' = gg'h = h$, άρα $ghg' \in H$. □

Πρόταση 6.3.2 *Η A_n είναι κανονική υποομάδα της S_n.*

*Απόδειξη:*6.3.2 Έστω $\sigma \in S_n$ και $\tau \in A_n$. Η σ γράφεται ως γινόμενο $2k$ αντιμεταθέσεων και η τ ως γινόμενο m αντιμεταθέσεων. Άρα η $\tau\sigma\tau'$ γράφεται ως γινόμενο $m + 2k + m = 2(k + m)$ αντιμεταθέσεων. Συνεπώς, $\tau\sigma\tau' \in A_n$. □

Ο **πυρήνας** ενός ομομορφισμού $\phi : G \to H$ είναι το σύνολο

$$\{g \in G : \phi(g) = e\},$$

συμβολίζεται δε με $Ker\phi$. Προφανώς, $e \in Ker\phi$. Αυτό έπεται από το Θεώρημα 6.1.2, στο οποίο βασίζονται και τα επόμενα τρία αποτελέσματα.

Πρόταση 6.3.3 *Ένας ομομορφισμός $\phi : G \to H$ είναι μονομορφισμός αν και μόνον αν $Ker\phi = \{e\}$.*

*Απόδειξη:*6.3.3 Έστω ότι ο ϕ είναι μονομορφισμός. Αν $x \in Ker\phi$, τότε $\phi(x) = e = \phi(e)$, άρα $x = e$. Συνεπώς, $Ker\phi = \{e\}$.
Αντιστρόφως, έστω ότι $Ker\phi = \{e\}$. Αν $\phi(x) = \phi(y)$, τότε $\phi(xy') = \phi(x)\phi(y') = \phi(x)\phi(y)' = \phi(x)\phi(x)' = e$. Άρα, $xy' \in Ker\phi = \{e\}$ και $xy' = e$. Συνεπώς, $x = y$ και ο ϕ είναι μονομορφισμός. □

Θεώρημα 6.3.4 *Ο πυρήνας $Ker\phi$ ενός ομομορφισμού $\phi : G \to H$ είναι κανονική υποομάδα της G.*

*Απόδειξη:*6.3.4

1. $e \in Ker\phi$.
2. $x, y \in Ker\phi \Rightarrow \phi(x) = \phi(y) = e \Rightarrow \phi(xy) = \phi(x)\phi(y) = ee = e \Rightarrow xy \in Ker\phi$.
3. $x \in Ker\phi \Rightarrow \phi(x) = e \Rightarrow \phi(x') = \phi(x)' = e \Rightarrow x' \in Ker\phi$.
4. $x \in Ker\phi, y \in G \Rightarrow \phi(x) = e \Rightarrow \phi(yxy') = \phi(y)e\phi(y') = \phi(y)\phi(y)' = e \Rightarrow yxy' \in Ker\phi$.

Από τις $(1), (2), (3)$, ο πυρήνας $Ker\phi$ είναι υποομάδα της G. Η (4) συνεπάγεται ότι είναι κανονική υποομάδα. □

Πρόταση 6.3.5 *Έστω $\phi : G_1 \to G_2$ ένας ομομορφισμός ομάδων και H μια υποομάδα της G_1. Τότε η **ευθεία εικόνα** της H μέσω της ϕ*

$$\phi(H) = \{\phi(x) : x \in H\}$$

είναι μια υποομάδα της G_2.

*Απόδειξη:*6.3.5

1. $y_1, y_2 \in \phi(H) \Rightarrow y_1 = \phi(x_1), y_2 = \phi(x_2)$ για κάποια $x_1, x_2 \in H \Rightarrow$ το x_1x_2 ανήκει στην υποομάδα H της G_1 και το $y_1y_2 = \phi(x_1)\phi(x_2) = \phi(x_1x_2) \in \phi(H)$,
2. $e = \phi(e) \in \phi(H)$ αφού το e ανήκει στην υποομάδα H της G_1,
3. $y \in \phi(H) \Rightarrow y = \phi(x)$ για κάποιο $x \in H \Rightarrow$ το x' ανήκει στην υποομάδα H της G_1 και το $y' = \phi(x)' = \phi(x') \in \phi(H)$.

□

Δεδομένου ομομορφισμού ομάδων $\phi : G \to H$, η εικόνα

$$\phi(G) = \{\phi(x) : x \in G\}$$

συμβολίζεται με $Im\phi$. Προφανώς, η ϕ είναι επί αν και μόνον αν $Im\phi = H$.

Πρόταση 6.3.6 *Έστω H μια κανονική υποομάδα μιας ομάδας G. Τότε για κάθε $g \in G$ και $h \in H$,*

1. *υπάρχει $h_1 \in H$ με $gh = h_1 g$,*
2. *υπάρχει $h_2 \in H$ με $hg = gh_2$.*

*Απόδειξη:*6.3.6

1. Προφανώς, $h_1 = ghg' \in H$ και $gh = h_1 g$.
2. Προφανώς, $h_2 = g'hg = g'h(g')' \in H$ και $gh_2 = hg$.

□

6.4 Ασκήσεις

Άσκηση 6.4.1 *Δείξτε ότι η υποομάδα $H = \langle(1\ \ 2)\rangle$ της S_3 δεν είναι κανονική.*

Λύση 6.4.2 $(2\ \ 3)(1\ \ 2)(2\ \ 3)' = (2\ \ 3)(1\ \ 2)(2\ \ 3) = (3\ \ 1) \notin H = \{(1\ \ 2), e\}$.

Άσκηση 6.4.3 *Δείξτε ότι η υποομάδα $H = \langle(1\ \ 2\ \ 3)\rangle$ της S_3 είναι κανονική.*

Λύση 6.4.4 *Αρκεί να δείξουμε $ghg' \in H = \{(1\ \ 2\ \ 3), (1\ \ 3\ \ 2), e\}$ για $g = (1\ \ 2), (2\ \ 3)$ ή $(1\ \ 3)$ και $h = (1\ \ 2\ \ 3)$ ή $(1\ \ 3\ \ 2)$. Πράγματι,*
$(1\ \ 2)(1\ \ 2\ \ 3)(1\ \ 2) = (1\ \ 3\ \ 2) \in H$
$(1\ \ 3)(1\ \ 2\ \ 3)(1\ \ 3) = (1\ \ 3\ \ 2) \in H$
$(2\ \ 3)(1\ \ 2\ \ 3)(2\ \ 3) = (1\ \ 3\ \ 2) \in H$
$(1\ \ 2)(1\ \ 3\ \ 2)(1\ \ 2) = (1\ \ 2\ \ 3) \in H$
$(1\ \ 3)(1\ \ 3\ \ 2)(1\ \ 3) = (1\ \ 2\ \ 3) \in H$
$(2\ \ 3)(1\ \ 3\ \ 2)(2\ \ 3) = (1\ \ 2\ \ 3) \in H$
.

Άσκηση 6.4.5 *Δείξτε ότι κάθε υποομάδα H ομάδας G με $|G : H| = 2$ είναι κανονική.*

Λύση 6.4.6 *Έστω $g \in G, h \in H$. Θέλω να δείξω ότι $ghg' \in H$. Μπορώ να υποθέσω ότι $g \notin H$. Τότε τα δύο αριστερά σύμπλοκα της G είναι τα H και gH. Αν $ghg' \in gH$, τότε $ghg' = gh_1$, όπου $h_1 \in H$, άρα $hg' = h_1$. Συνεπώς, $g' = h'h_1$ και $g = h'_1 h \in G$! Έπεται ότι $ghg' \in H$ και η H είναι κανονική υποομάδα.*

Άσκηση 6.4.7 *Δείξτε ότι η $f : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ που ορίζεται με $f(x) = 3x$ είναι ομομορφισμός.*
Βρείτε τα σύνολα $Kerf$ και Imf. Είναι ο f μονομορφισμός ή επιμορφισμός;

Λύση 6.4.8 *Είναι ομομορφισμός από την Άσκηση 6.2.31.*
$Kerf = \{0, 4, 8\} \neq \{0\}$, άρα ο f δεν είναι μονομορφισμός.
$Imf = \{0, 3, 6, 9\} \neq \mathbb{Z}_{12}$, άρα ο f δεν είναι επιμορφισμός.

Άσκηση 6.4.9 *Ο ομομορφισμός $f : \mathbb{R}^* \to \mathbb{R}^*$ ορίζεται με $f(x) = |x|$.*
Βρείτε τα σύνολα $Kerf$ και Imf. Είναι ο f μονομορφισμός ή επιμορφισμός;

Λύση 6.4.10 *$Kerf = \{1, -1\}$, άρα ο f δεν είναι μονομορφισμός.*
$Imf = \mathbb{R}^+$, άρα ο f δεν είναι επιμορφισμός.

Άσκηση 6.4.11 *Η $f : S_n \to \mathbb{Z}_2$ στέλνει τις άρτιες μεταθέσεις στο 0 και τις περιττές στο 1.*
Δείξτε ότι η f είναι ομομορφισμός και βρείτε τα σύνολα $Kerf$ και Imf.

Λύση 6.4.12 *Θέλω να δείξω ότι $f(xy) = f(x) + f(y)$ για κάθε $x, y \in S_n$. Έχουμε τις εξής 4 περιπτώσεις.*

1. *x και y άρτιες $\Rightarrow xy$ άρτια, οπότε $f(xy) = 0 = 0 + 0 = f(x) + f(y)$.*
2. *x και y περιττές $\Rightarrow xy$ άρτια, οπότε $f(xy) = 0 = 1 + 1 = f(x) + f(y)$.*
3. *x άρτια, y περιττή $\Rightarrow xy$ περιττή, οπότε $f(xy) = 1 = 0 + 1 = f(x) + f(y)$.*
4. *x περιττή, y άρτια $\Rightarrow xy$ περιττή, οπότε $f(xy) = 1 = 1 + 0 = f(x) + f(y)$.*

$Kerf = A_n$, $Imf = \mathbb{Z}_2$.

Άσκηση 6.4.13 *Έστω H_1, H_2 υποομάδες μιας ομάδας G. Δείξτε ότι και η τομή τους $H_1 \cap H_2$ είναι υποομάδα της G.*

Λύση 6.4.14 *Επειδή οι H_1, H_2 είναι υποομάδες της G, έχουμε ότι*

1. *$e \in H_1, e \in H_2$. Άρα, $e \in H_1 \cap H_2$,*
2. *$x, y \in H_1 \cap H_2 \Rightarrow x, y \in H_1$ και $x, y \in H_2 \Rightarrow xy \in H_1$ και $xy \in H_2 \Rightarrow xy \in H_1 \cap H_2$,*
3. *$x \in H_1 \cap H_2 \Rightarrow x \in H_1$ και $x \in H_2 \Rightarrow x' \in H_1$ και $x' \in H_2 \Rightarrow x' \in H_1 \cap H_2$.*

Από τις $(1), (2), (3)$, η $H_1 \cap H_2$ είναι υποομάδα της G.

Άσκηση 6.4.15 *Έστω H_1, H_2 κανονικές υποομάδες μιας ομάδας G. Δείξτε ότι και η τομή τους $H_1 \cap H_2$ είναι κανονική υποομάδα της G.*

Λύση 6.4.16 *Η $H_1 \cap H_2$ είναι υποομάδα της G από την Άσκηση 6.4.13. Έστω τώρα $g \in G$ και $h \in H_1 \cap H_2$. Τότε το h είναι στοιχείο των κανονικών υποομάδων H_1, H_2. Συνεπώς, το ghg' ανήκει σε κάθε μία από τις H_1, H_2. Άρα ανήκει και στην $H_1 \cap H_2$, η οποία είναι επομένως κανονική υποομάδα της G.*

Άσκηση 6.4.17 *Έστω G μία ομάδα και $a \in G$. Δείξτε ότι η $f : G \to G$ που ορίζεται με $f(x) = axa'$ είναι ισομορφισμός ομάδων.*

Λύση 6.4.18 *1. Η f είναι ομομορφισμός: $f(xy) = axya' = axeya' = ax(a'a)ya' = (axa')(aya') = f(x)f(y)$.*

2. Η f είναι $1-1$: $f(x) = f(y) \Rightarrow axa' = aya' \Rightarrow a'axa'a = a'aya'a \Rightarrow x = y$.

3. Η f είναι επί: $y \in G \Rightarrow y = f(a'ya)$.

Άσκηση 6.4.19 *Έστω G μία ομάδα. Έστω ότι η H είναι η μόνη υποομάδα της G τάξης m. Δείξτε ότι η H είναι κανονική υποομάδα της G.*

Λύση 6.4.20 *Έστω $g \in G$. Από την Άσκηση 6.4.17, η $f : G \to G$ που ορίζεται με $f(x) = gxg'$ είναι (1) ομομορφισμός, και (2) $1-1$ και επί. Από την (1) και την Πρόταση 6.3.5, η $f(H)$ είναι υποομάδα της G, και από την (2), έχουμε $|f(H)| = |H| = m$. Από τα δεδομένα προκύπτει ότι $f(H) = H$. Έτσι, για κάθε $h \in H$, $ghg' = f(h) \in f(H) = H$. Συνεπώς, η H είναι κανονική υποομάδα της G.*

6.5 Ομάδες πηλίκα

Στο κεφάλαιο αυτό το H παριστάνει μια κανονική υποομάδα μιας ομάδας G και το G/H συμβολίζει το σύνολο των αριστερών συμπλόκων της H στην G. Αξίζει να υπενθυμίσουμε ότι τα αριστερά σύμπλοκα είναι κλάσεις ισοδυναμίας ως προς τη σχέση ισοδυναμίας $\sim$ που ορίζεται με

$$x \sim y \Leftrightarrow x'y \in H.$$

Συνεπώς, $xH = yH \Leftrightarrow y \in xH \Leftrightarrow y = xh$ για κάποιο $h \in H$. Επίσης, $xH = H \Leftrightarrow x \in H$.

Σκοπός μας είναι να μετατρέψουμε το G/H σε ομάδα. Ορίζουμε, λοιπόν, μια πράξη $*$ στο G/H με $xH * yH = xyH$, όπου, ως συνήθως το xy συμβολίζει το γινόμενο των x, y στην G. Προκύπτει αμέσως το ερώτημα κατά πόσο η $*$ είναι καλά ορισμένη: Έστω ότι $x_1H = x_2H$ και $y_1H = y_2H$, οπότε $x_2 = x_1h_1$ και $y_2 = y_1h_2$ για κάποια $h_1, h_2 \in H$. Θέλουμε να δείξουμε ότι $x_1x_2H = y_1y_2H$. Έχουμε $x_2y_2 = x_1h_1y_1h_2$ και, επειδή η H είναι κανονική υποομάδα, από την Πρόταση 6.3.6, $h_1y_1 = y_1h_3$ για κάποιο $h_3 \in H$. Συνεπώς, έχουμε $h_3h_2 \in H$ και $x_2y_2 = x_1(y_1h_3)h_2 = (x_1y_1)(h_3h_2)$. Άρα, $x_1x_2H = y_1y_2H$.

Θεώρημα 6.5.1 *Το $(G/H, *)$ αποτελεί ομάδα με ταυτοτικό το $H = eH$ και αντίστροφο του xH το $x'H$. Επιπλέον, ισχύουν και τα εξής.*

1. *Η $\pi : G \to G/H$ που στέλνει το x στο xH είναι επιμορφισμός με $Ker\pi = H$.*
2. *Αν η G είναι αβελιανή, τότε και η H είναι αβελιανή.*
3. *Αν η G είναι κυκλική, τότε και η H είναι κυκλική.*

4. Αν η G είναι πεπερασμένη, τότε $|G/H| = \frac{|G|}{|H|}$.

*Απόδειξη:*6.5.1 Οι ιδιότητες της $*$ προκύπτουν από τις αντίστοιχες ιδιότητες της πράξης της G (και τον ορισμό της $*$).
Προσεταιριστικότητα:
$xH*(yH*zH) = xH*yzH = x(yz)H = (xy)zH = xyH*zH = (xH*yH)*zH$.
Ταυτοτικό: $xH * eH = xeH = xH = exH = eH * xH$.
Αντίστροφο του xH: $xH * x'H = xx'H = eH = x'xH = x'H * xH$.
Συνεπώς, το $(G/H, *)$ αποτελεί ομάδα.
Ο π είναι ομομορφισμός: $\pi(xy) = xyH = xH * yH = \pi(x) * \pi(y)$.
Η συνάρτηση π είναι προφανώς επί, άρα ο π είναι επιμορφισμός.
Τώρα, $\pi(x) = xH = H$ αν και μόνον αν $x \in H$. Άρα, $Ker\pi = H$.
Οι (2) και (3) έπονται τώρα από το Θεώρημα 6.1.4.
Τέλος, η (4), έπεται από το Θεώρημα Lagrange αφού προφανώς $|G/H| = |G : H|$.
□

Η G/H με την παραπάνω πράξη λέγεται η ομάδα **πηλίκο** της G δια H ή η ομάδα **πηλίκο** της G **modulo** H. Ο επιμορφισμός $\pi : G \to G/H$ λέγεται η **φυσική** απεικόνιση της G στην G/H.

Θεώρημα 6.5.2 *(Το Θεμελιώδες θεώρημα ομομορφισμού). Έστω $\phi : G \to K$ ένας ομομορφισμός. Τότε $G/Ker\phi \cong Im\phi$.*

*Απόδειξη:*6.5.2 Θέτουμε $H = Ker\phi$ και ορίζουμε μια συνάρτηση $\psi : G/H \to Im\phi$ με $\psi(xH) = \phi(x)$. Η ψ είναι καλά ορισμένη γιατί
$yH = xH \Rightarrow y = xh$ για κάποιο $h \in H \Rightarrow \phi(y) = \phi(x)\phi(h) = \phi(x)e = \phi(x) \Rightarrow \psi(yH) = \psi(xH)$.
Επειδή ο ϕ είναι ομομορφισμός,
$\psi(xH * yH) = \psi(xyH) = \phi(xy) = \phi(x)\phi(y) = \psi(xH)\psi(yH)$.
Άρα, η ψ είναι ομομορφισμός.
Η ψ είναι επί γιατί κάθε μέλος της $Im\phi$ γράφεται ως $\phi(x) = \psi(xH)$ για κάποιο $x \in G$.
Η ψ είναι και $1-1$ γιατί
$\psi(xH) = \psi(yH) \Rightarrow \phi(x) = \phi(y) \Rightarrow \phi(x'y) = \phi(x')\phi(y) = \phi(x)'\phi(y) = e \Rightarrow h = x'y \in H = Ker\phi \Rightarrow y = xh$, όπου $h \in H$, $\Rightarrow xH = yH$.
Συνεπώς, η $\psi : G/H \to Im\phi$ είναι ισομορφισμός και $G/Ker\phi \cong Im\phi$. □

Πόρισμα 6.5.3 *Έστω $\phi : G \to K$ ένας επιμορφισμός. Τότε $G/Ker\phi \cong K$.*

*Απόδειξη:*6.5.3 Εφόσον ο $\phi : G \to K$ είναι επιμορφισμός, έχουμε $Im\phi = K$. □

Σημείωση. Από τώρα και στο εξής, επανερχόμαστε στη συνήθη πρακτική όπου το γινόμενο δύο στοιχείων xH, yH της G/H γράφεται ως $xHyH$. Μόνη εξαίρεση αποτελεί η περίπτωση που η πράξη της G ειναι η $+$ οπότε υιοθετούμε το ίδιο συμβολο για την πράξη της ομάδας πηλίκο, γράφοντας $(x+H)+(y+H)$ για το «γινόμενο» δύο μελών $(x+H)$ και $(y+H)$ της G/H.

6.6 Ασκήσεις

Άσκηση 6.6.1 *Να αναγνωρίσετε την ομάδα πηλίκο S_n/A_n.*

Λύση 6.6.2 *Επειδή έχει τάξη δύο, η $S_n/A_n \cong \mathbb{Z}_2$.*

***Διαφορετικά**: Από την Άσκηση 6.4.11, υπάρχει ένας επιμορφισμός $f : S_n \to \mathbb{Z}_2$ με $Kerf = A_n$. Τώρα έπεται από το Πόρισμα 6.5.3 ότι $S_n/A_n \cong \mathbb{Z}_2$.*

Άσκηση 6.6.3 *Να κάνετε τον πίνακα και στη συνέχεια να αναγνωρίσετε την ομάδα πηλίκο $\mathbb{Z}/4\mathbb{Z}$.*

Λύση 6.6.4 *Θέτοντας $H = 4\mathbb{Z} = \{\ldots, 0, 4, 8, 12, \ldots\}$, τα στοιχεία της ομάδας $\mathbb{Z}/4\mathbb{Z}$ είναι:*
$\ldots = H = 0 + H = 4 + H = 8 + H = 12 + H = \ldots$
$\ldots = 1 + H = 5 + H = 9 + H = 13 + H = \ldots$
$\ldots = 2 + H = 6 + H = 10 + H = 14 + H = \ldots$ *και*
$\ldots = 3 + H = 7 + H = 11 + H = 15 + H = \ldots$
Από τον πίνακα, το $1 + H$ έχει τάξη 4.
Άρα, $\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$.

***Βλέπε** και Άσκηση 6.6.11.*

Άσκηση 6.6.5 *Να κάνετε τον πίνακα και στη συνέχεια να αναγνωρίσετε την ομάδα πηλίκο $\mathbb{Z}_4 \times \mathbb{Z}_2/\langle(2,0)\rangle$.*

Λύση 6.6.6 *Θέτοντας $H = \langle(2,0)\rangle = \{(2,0),(0,0)\}$, τα στοιχεία της ομάδας $\mathbb{Z}_4 \times \mathbb{Z}_2/\langle(2,0)\rangle$ είναι:*
$H = (0,0) + H = (2,0) + H$
$(1,0) + H = \{(3,0),(1,0)\} = (3,0) + H$
$(1,1) + H = \{(3,1),(1,1)\} = (3,1) + H$ *και*
$(2,1) + H = \{(0,1),(2,1)\} = (0,1) + H$
Από τον πίνακα, όλα τα μη μηδενικά στοιχεία έχουν τάξη 2.
Άρα η $\mathbb{Z}_4 \times \mathbb{Z}_2/\langle(2,0)\rangle$ είναι η 4-ομάδα Klein.

Άσκηση 6.6.7 *Να κάνετε τον πίνακα και στη συνέχεια να αναγνωρίσετε την ομάδα πηλίκο $\mathbb{Z}_4 \times \mathbb{Z}_2/\langle 2,1\rangle$.*

Λύση 6.6.8 *Θέτοντας $H = \langle(2,1)\rangle = \{(2,1),(0,0)\}$, τα στοιχεία της ομάδας $\mathbb{Z}_4 \times \mathbb{Z}_2/\langle(2,1)\rangle$ είναι:*
$H = (0,0) + H = (2,1) + H$
$(1,0) + H = \{(3,1),(1,0)\} = (3,1) + H$
$(2,0) + H = \{(0,1),(2,0)\} = (0,1) + H$ *και*
$(3,0) + H = \{(1,1),(3,0)\} = (1,1) + H$
Από τον πίνακα, το $(1,0) + H$ έχει τάξη 4. Άρα, $\mathbb{Z}_4 \times \mathbb{Z}_2/\langle(2,1)\rangle \cong \mathbb{Z}_4$.

Άσκηση 6.6.9 *Έστω a ένα στοιχείο μιας ομάδας G. Να δείξετε ότι η $\phi : \mathbb{Z} \to G$ που ορίζεται με $\phi(n) = a^n$ είναι ομομορφισμός. Ποιος είναι ο πυρήνας του;*

Λύση 6.6.10 *Ο ϕ είναι ομομορφισμός γιατί, από τις ιδιότητες δυνάμεων,*

$$\phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n).$$

Αν $o(a) = m < \infty$, τότε $\phi(n) = a^n = e \Leftrightarrow m|n$. Συνεπώς, $Ker\phi = m\mathbb{Z}$.
Αν $o(a) = \infty$, τότε $\phi(n) = a^n = e \Leftrightarrow n = 0$. Συνεπώς, $Ker\phi = \{0\}$.

Άσκηση 6.6.11 *Να δείξετε ότι $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, για κάθε $m \in \mathbb{Z}$.*

Λύση 6.6.12 *Στην Άσκηση 6.6.9 θέτουμε $G = \mathbb{Z}_m$ και $a = 1$. Προκύπτει ότι η $\phi : \mathbb{Z} \to \mathbb{Z}_m$ που ορίζεται με $\phi(n) = n$ είναι ομομορφισμός με $Ker\phi = m\mathbb{Z}$. Επειδή η ϕ είναι προφανώς επί, από το Πόρισμα 6.5.3, $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$.*

Άσκηση 6.6.13 *Αναγνωρίστε την ομάδα $\mathbb{Z}_m \times \mathbb{Z}_n/\langle(1,0)\rangle$.*

Λύση 6.6.14 *Θέτοντας $H = \langle(1,0)\rangle = \{(1,0),(2,0),\ldots,(m-1,0),(0,0)\}$, βλέπουμε ότι το στοιχείο $(0,1)+H$ της ομάδας πηλίκο έχει τάξη n, όπως και η ομάδα πηλίκο.*

Συνεπώς, η $\mathbb{Z}_m \times \mathbb{Z}_n/\langle(1,0)\rangle$ είναι κυκλική, μάλιστα $\mathbb{Z}_m \times \mathbb{Z}_n/\langle(1,0)\rangle \cong \mathbb{Z}_n$.

Άσκηση 6.6.15 *Δείξτε ότι η $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ που ορίζεται με $f(x,y) = x - y$ είναι ένας επιμορφισμός.*
Αναγνωρίστε την ομάδα $\mathbb{Z} \times \mathbb{Z}/\langle(1,1)\rangle$.

Λύση 6.6.16 *$f\big((x_1,y_1)+(x_2,y_2)\big) = f(x_1+x_2, y_1+y_2) = (x_1+x_2)-(y_1+y_2) = (x_1-y_1)+(x_2-y_2) = f(x_1,y_1)+f(x_2,y_2)$. Άρα η f ειναι ομομορφισμός. Είναι επιμορφισμός γιατί $x = f(x,0)$.*
Προφανώς, $Kerf = \langle(1,1)\rangle$ και, από τό Πόρισμα 6.5.3, $\mathbb{Z} \times \mathbb{Z}/\langle(1,1)\rangle \cong \mathbb{Z}$.

6.7 Ασκήσεις

Άσκηση 6.7.1 *Δείξτε ότι μια ομάδα G της οποίας η τάξη είναι άρτιος αριθμός περιέχει στοιχείο τάξης 2.*

Λύση 6.7.2 *Για κάθε $x \in G$, ορίζουμε $A_x = \{x, x'\}$. Προφανώς, $A_x \cap A_y \neq \emptyset \Leftrightarrow x = y$ ή $x = y' \Leftrightarrow A_x = A_y$. Επίσης, $A_e = \{e\}$. Έστω $A_e, A_{x_1}, A_{x_2}, \ldots A_{x_n}$ μια απαρίθμηση των διακεκριμένων συνόλων της μορφής A_x. Τότε, $|G| = 1 + |A_{x_1}| + |A_{x_2}| + \ldots + |A_{x_n}|$. Με δεδομένο ότι ο αριθμός $|G|$ είναι άρτιος, πρέπει για κάποιο i το A_{x_i} να περιέχει ένα μόνο στοιχείο. Συνεπώς, $x_i = x_i'$, οπότε $o(x_i) = 2$.*

Άσκηση 6.7.3 *Έστω G μια ομάδα τέτοια ώστε $x^2 = e$ για κάθε $x \in G$. Δείξτε ότι*

1. *η G είναι αβελιανή.*
2. *αν $|G| \geq 4$, τότε η G περιέχει την ομάδα του Klein V ως υποομάδα.*

Λύση 6.7.4 *1. Για κάθε $x, y \in G$, $xyxy = e = ee = xxyy$. Από το νόμο διαγραφής, παίρνουμε $yxy = xxy$ και $yx = xy$.*

2. Αν $|G| \geq 4$, το $G \setminus \{e\}$ περιέχει διακεκριμένα στοιχεία a, b, ab, όλα τάξης 2. Εύκολα ελέγχεται ότι το $H = \{e, a, b, ab\}$ αποτελεί μη κυκλική υποομάδα της G. Άρα, από την Άσκηση 6.2.19, $H \cong V$.

Άσκηση 6.7.5 *Έστω G μια μη κυκλική ομάδα τάξης 6. Δείξτε ότι*

1. η G περιέχει ένα στοιχείο a τάξης 2 και ένα στοιχείο b τάξης 3, μάλιστα

2. $G = \{e, b, b^2, a, ab, ab^2\}$.

Να κάνετε τον πίνακα πολλαπλασιασμού της G.

Λύση 6.7.6 *1. Η τάξη τυχαίου στοιχείου της G διαιρεί την $|G| = 6$, συνεπώς είναι ένας από τους $1, 2, 3, 6$. Αν η G είχε στοιχείο τάξης 6, τότε θα ήταν κυκλική. Η ύπαρξη στοιχείου a τάξης 2 προκύπτει από την Άσκηση 6.7.1. Αν όλα τα στοιχεία του $G \setminus \{e\}$ είχαν τάξη 2, από την Άσκηση 6.7.3, η G θα είχε κάποια υποομάδα τάξης 4, πράγμα που αποκλείεται από το Θεώρημα Lagrange, εφόσον $4 \nmid 6$. Συνεπώς, η G περιέχει ένα στοιχείο b τάξης 3.*

2. Προφανώς, τα b, b^2 έχουν τάξη 3 ενώ το a έχει τάξη 2. Άρα, τα e, b, b^2, a είναι 4 διακεκριμένα στοιχεία της G. Μάλιστα, από τον κανόνα απαλοιφής, εύκολα προκύπτει ότι τα e, b, b^2, a, ab, ab^2 είναι όλα διακεκριμένα και, αφού $|G| = 6$, $G = \{e, b, b^2, a, ab, ab^2\}$.

Ο πίνακας πολλαπλασιασμού της G, συνάγεται εύκολα από τον κανόνα απαλοιφής: Π.χ. το ba δεν μπορεί να είναι ένα από τα e, b, b^2, a. Αν $ba = ab$, τότε $(ab)^2 = abab = aabb = b^2 \neq e$, $(ab)^3 = abb^2 = a \neq e$ και συνεπώς $o(ab) = 6$! Η μόνη επιλογή, επομένως, είναι $ba = ab^2$. Από αυτό προκύπτουν $b^2a = bab^2 = ab^2b^2 = ab$, $aba = aab^2 = b^2, \ldots$.

$\circ$	e	b	b^2	a	ab	ab^2
e	e	b	b^2	a	ab	ab^2
b	b	b^2	e	ab^2	a	ab
b^2	b^2	e	b	ab	ab^2	a
a	a	ab	ab^2	e	b	b^2
ab	ab	ab^2	a	b^2	e	b
ab^2	ab^2	a	ab	b	b^2	e

Άσκηση 6.7.7 *Πόσες μη κυκλικές ομάδες τάξης 6 υπάρχουν;*

Λύση 6.7.8 *Στην Άσκηση 6.7.5, από την πληροφορία ότι μια ομάδα G τάξης 6 δεν είναι κυκλική οδηγηθήκαμε στο συμπέρασμα ότι η G περιέχει ένα στοιχείο a τάξης 2 και ένα στοιχείο b τάξης 3 και ότι $G = \{e, b, b^2, a, ab, ab^2\}$. Στη συνέχεια καταλήξαμε μονοσήμαντα στο πίνακα της G. Αν τώρα μια άλλη μη κυκλική ομάδα H έχει τάξη 6, τότε και η H περιέχει ένα στοιχείο α τάξης 2 και ένα στοιχείο β τάξης 3 και μάλιστα $H = \{e, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2\}$. Συνεπώς, ο πίνακας της H είναι*

εκείνος που προκύπτει όταν στο πίνακα της G αντικαταστήσουμε το a με το α και το b με το β. Αυτό σημαίνει ότι η $f : G \to H$ που στέλνει τα e, b, b^2, a, ab, ab^2 στα $e, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2$, αντίστοιχα, είναι ισομορφισμός. Άρα, $G \cong H$.
Έπεται ότι η μόνη μη κυκλική ομάδα τάξης 6 είναι η S_3.

Άσκηση 6.7.9 *Δείξτε ότι υπάρχουν μόνο δύο ομάδες τάξης 6.*

Λύση 6.7.10 *Έστω ότι η G είναι ομάδα τάξης 6. Υπάρχουν οι εξής δύο περιπτώσεις.*

1. *Η G είναι κυκλική, οπότε $G \cong \mathbb{Z}_6$.*
2. *Η G δεν είναι κυκλική, οπότε, από την Άσκηση 6.7.7, $G \cong S_3$.*

Κεφάλαιο 7

Δακτύλιοι

7.1 Βασικές έννοιες και παραδείγματα

Ένας **δακτύλιος** $(S, +, \cdot)$ αποτελείται από ένα σύνολο S και δύο πράξεις, την πρόσθεση $+$ και τον πολλαπλασιασμό $\cdot$, οι οποίες ικανοποιούν τα εξής τρία αξιώματα.

1. Το $(S, +)$ αποτελεί αβελιανή ομάδα.
2. Ο πολλαπλασιασμός $\cdot$ είναι προσεταιριστικός.
3. Για όλα τα στοιχεία a, b, c του S, έχουμε

   (α') $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (αριστερός επιμεριστικός νόμος), και

   (β') $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ (δεξιός επιμεριστικός νόμος).

Ένας δακτύλιος $(S, +, .)$ λέγεται **μεταθετικός** αν η πράξη $\cdot$ είναι μεταθετική. Να σημειωθεί ότι όταν ο πολλαπλασιασμός είναι μεταθετικός, τότε ο αριστερός επιμεριστικός νόμος συνεπάγεται το δεξιό, και αντιστρόφως.

Παραδείγματα. Τα $(\mathbb{C}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$, $(n\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$ είναι όλα μεταθετικοί δακτύλιοι. Για $n \geq 2$, το σύνολο των $n \times n$ πινάκων, εφοδιασμένο με τις γνωστές πράξεις πρόσθεσης και πολλαπλασιασμού πινάκων, αποτελεί μη μεταθετικό δακτύλιο.

Έστω $(S, +, .)$ ένας δακτύλιος. Το ουδέτερο στοιχείο του S ως προς την $+$, ως συνήθως, συμβολίζεται με 0, το $-a$ παριστάνει το αντίθετο του a και το $a + (-b)$ απλοποιείται σε $a - b$. Όλοι οι παραπάνω δακτύλιοι, με εξαίρεση τον $(n\mathbb{Z}, +, \cdot)$ για $n \geq 2$, έχουν ταυτοτικό στοιχείο ως προς τον πολλαπλασιασμό. Σημειώστε ότι το ταυτοτικό στοιχείο ως προς τον πολλαπλασιασμό του $\mathbb{Z}_1$ είναι το 0. Αν ο S έχει ταυτοτικό στοιχείο ως προς τον πολλαπλασιασμό το οποίο είναι διάφορο του 0, το μοναδικό αυτό στοιχείο συμβολίζεται με 1 και λέγεται το **μοναδιαίο** στοιχείο του S.
Σε ένα δακτύλιο S, το γινόμενο $a \cdot b$ απλοποιείται σε ab, δηλαδή, παραλείπεται το

σύμβολο του πολλαπλασιασμού. Επίσης, υιοθετείται η σύμβαση ότι σε εκφράσεις που περιέχουν τα σύμβολα $\cdot$ και $+$ (ή $-$), ο πολλαπλασιασμός εκτελείται πρώτα. Η σύμβαση αυτή μας επιτρέπει να παραλείπουμε κάποιες παρενθέσεις. Έτσι το $-(a \cdot b)$ απλοποιείται σε $-ab$ και οι επιμεριστικοί νόμοι γράφονται

$$a(b+c) = ab + ac \quad \text{και} \quad (b+c)a = ba + ca.$$

Επαγωγικά δε οι επιμεριστικοί νόμοι γενικεύονται σε

$$a(b_1 + b_2 + ... + b_n) = ab_1 + ab_2 + ... + ab_n \quad \text{και}$$
$$(b_1 + b_2 + ... + b_n)a = b_1a + b_2a + ... + b_na.$$

Πρόταση 7.1.1 *Για όλα τα στοιχεία a, b, c ενός δακτυλίου S,*

1. *$a0 = 0$ και $0a = 0$,*
2. *$a(-b) = (-a)b = -ab$,*
3. *$(-a)(-b) = ab$,*
4. *$(a-b)c = ac - bc$ και $c(a-b) = ca - cb$,*
5. *αν ο S έχει μοναδιαίο στοιχείο 1, τότε $a(-1) = (-1)a = -a$.*

*Απόδειξη:*7.1.1

1. Από το γεγονός ότι το $(S, +)$ αποτελεί ομάδα και το δεξιό επιμεριστικό νόμο, $a0 + 0 = a0 = a(0 + 0) = a0 + a0$. Εφαρμόζοντας τον αριστερό νόμο διαγραφής για την ομάδα $(S, +)$ στην εξίσωση $a0 + a0 = a0 + 0$, παίρνουμε $a0 = 0$. Ομοίως, $0a = 0$.
2. Από την (1) και το δεξιό επιμεριστικό νόμο, $0 = a(b + (-b)) = ab + a(-b)$. Άρα $ab + a(-b) = ab + (-ab)$ και από τον αριστερό νόμο διαγραφής για την ομάδα $(S, +)$, έχουμε $a(-b) = -ab$. Ομοίως, $(-a)b = -ab$.
3. Από την (2), $(-a)(-b) = -(a(-b)) = -(-ab) = ab$.
4. Από το δεξιό επιμεριστικό νόμο και την (2), $(a-b)c = (a + (-b))c = ac + (-b)c = ac + (-bc) = ac - bc$. Ομοίως, $c(a-b) = ca - cb$.
5. Από την (2), $a(-1) = -a1 = -a$ και $(-1)a = -1a = -a$.

□

Έστω S ένας δακτύλιος με 1. Τα αντιστρέψιμα (ως προς τον πολλαπλασιασμό) στοιχεία του S λέγονται και **μονάδες** του S. Το σύνολο όλων των μονάδων του S, θα συμβολίζεται με $U(S)$. Σημειώστε ότι το 0 δεν είναι αντιστρέψιμο γιατί $x0 = 0 \neq 1$, για κάθε $x \in S$.

Πρόταση 7.1.2 *Έστω S ένας δακτύλιος με 1. Τότε το $U(S)$ αποτελεί ομάδα ως προς τον πολλαπλασιασμό.*

*Απόδειξη:*7.1.2 Για κάθε $x, y \in U(S)$, υπάρχουν $x', y' \in S$ με $xx' = 1 = x'x$ και $yy' = 1 = y'y$. Τότε, λόγω προσεταιριστικότητας του πολλαπλασιασμού, $xy(y'x') = x(yy')x' = x1x' = xx' = 1$ και ομοίως $(y'x')xy = 1$. Προκύπτει ότι το $xy \in U(S)$ και ο πολλαπλασιασμός είναι πράξη και στο $U(S)$, το οποίο προφανώς αποτελεί ομάδα με ταυτοτικό το 1. □

Σημειώστε ότι σε δακτύλιο S με 1 το γινόμενο δύο αντιστρέψιμων στοιχείων είναι διάφορο του 0 αφού ανήκει στο $U(S)$.
Ένας μεταθετικός δακτύλιος S με 1 όπου

$$a \neq 0, b \neq 0 \Rightarrow ab \neq 0$$

ονομάζεται **ακέραια περιοχή**. Η παραπάνω ιδιότητα γράφεται ισοδύναμα στην μορφή

$$ab = 0 \Rightarrow a = 0 \text{ ή } b = 0.$$

Ένας μεταθετικός δακτύλιος S με 1 ονομάζεται **σώμα** αν κάθε μη μηδενικό στοιχείο του S είναι αντιστρέψιμο, δηλαδή, αν $U(S) = S \setminus \{0\}$. Κάθε σώμα είναι και ακέραια περιοχή, αφού τα μη μηδενικά στοιχεία καθώς και τα γινόμενά τους είναι προφανώς αντιστρέψιμα.

Παραδείγματα. Τα $(\mathbb{C}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ είναι σώματα, όχι όμως τα $(\mathbb{Z}, +, \cdot)$, $(n\mathbb{Z}, +, \cdot)$. Το $(\mathbb{Z}_n, +, \cdot)$ είναι σώμα αν και μόνον αν ο αριθμός n είναι πρώτος (βλέπε Θεώρημα 3.5.4 και Άσκηση 7.2.13).
Το $\mathbb{Z}$ είναι μια ακέραια περιοχή, όχι όμως τα $\mathbb{Z}_4, \mathbb{Z}_6, \mathbb{Z}_8, \mathbb{Z}_9 \ldots$.

Πρόταση 7.1.3 *Ένας δακτύλιος S που έχει μοναδιαίο στοιχείο είναι σώμα αν και μόνον αν το σύνολο $S \setminus \{0\}$ αποτελεί αβελιανή ομάδα ως προς τον πολλαπλασιασμό.*

*Απόδειξη:*7.1.3 Αν ο S είναι σώμα, τότε ο S είναι μεταθετικός και, από την Πρόταση 7.1.2, το σύνολο $S \setminus \{0\}$ αποτελεί αβελιανή ομάδα ως προς τον πολλαπλασιασμό. Αντιστρόφως, αν το $S \setminus \{0\}$ αποτελεί αβελιανή ομάδα ως προς τον πολλαπλασιασμό, τότε $ab = ba$ για $a, b \neq 0$. Όμως, από την Πρόταση 7.1.1, $ab = ba$ ακόμη και όταν $a = 0$ ή $b = 0$. Συνεπώς, ο πολλαπλασιασμός του S αναι μεταθετικός και ο S είναι σώμα. □

Έστω S ένας δακτύλιος και $a, b \in S$. Αν για κάποιο $q \in S$, $b = qa$, τότε λέμε ότι το a **διαιρεί** το b ή ότι το a είναι **παράγοντας** του b ή ότι το b είναι **πολλαπλάσιο** του a, και γράφουμε $a|b$.

Πρόταση 7.1.4 *Για κάθε $a, b, c, s, t \in S$,*

1. $a|0$,
2. $a|b \Rightarrow (-a)|b, a|(-b)$,
3. $a|b, b|c \Rightarrow a|c$,
4. $c|a, c|b \Rightarrow c|(sa + tb)$.

*Απόδειξη:*7.1.4

1. $0 = 0a$.
2. $a|b \Rightarrow b = qa$ για κάποιο $q \in S \Rightarrow b = (-q)(-a), -b = (-q)a$.
3. $a|b, b|c \Rightarrow b = qa, c = rb$ για κάποια $q, r \in S \Rightarrow c = r(qa) = (rq)a \Rightarrow a|c$.
4. $c|a, c|b \Rightarrow a = qc, b = rc$ για κάποια $q, r \in S \Rightarrow (sa + tb) = sqc + trc = (sq + tr)c \Rightarrow c|(sa + tb)$.

□

Σε δακτύλιο S, αν $c|a$ και $c|b$, τότε το c λέγεται **κοινός διαιρέτης** των a, b. Το d λέγεται (ένας) **μέγιστος κοινός διαιρέτης** των a, b αν (1) το d είναι κοινός διαιρέτης των a, b και (2) κάθε κοινός διαιρέτης των a, b διαιρεί και τον d. Δεν αποκλείεται το ενδεχόμενο να υπάρχουν περισσότεροι από ένα μέγιστοι κοινοί διαιρέτες δύο στοιχείων σε κάποιους δακτυλίους S. Στην περίπτωση του δακτυλίου $\mathbb{Z}$, η μοναδικότητα του μεγίστου κοινού διαιρέτη ήταν αποτέλεσμα της πρόσθετης απαίτησης να είναι ένας θετικός αριθμός.

Θεώρημα 7.1.5 *(Ευκλείδειος αλγόριθμος). Για δεδομένα στοιχεία a, b ενός δακτυλίου S, έστω ότι υπάρχουν $q_1, q_2, \ldots, q_{n+1}, r_1, r_2, \ldots, r_n \in S$ τέτοια ώστε*

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\ldots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n + 0. \end{aligned}$$

Τότε το r_n είναι ένας μέγιστος κοινός διαιρέτης των a, b.

*Απόδειξη:*7.1.5 Από την τελευταία εξίσωση, έχουμε ότι $r_n|r_{n-1}$. Από την προτελευταία εξίσωση και την Πρόταση 7.1.4, παίρνουμε ότι $r_n|r_{n-2}$. Επαναλαμβάνοντας το ίδιο επιχείρημα, φτάνουμε στην τρίτη εξίσωση, έχοντας αποδείξει ότι $r_n|r_{n-1}$, $r_n|r_{n-2}, \ldots$, $r_n|r_3$, $r_n|r_2$. Τώρα έπεται από την τρίτη εξίσωση ότι $r_n|r_1$, από τη δεύτερη ότι $r_n|b$ και από την πρώτη ότι $r_n|a$. Έτσι το r_n είναι κοινός διαιρέτης των a, b.
Έστω c ένας κοινός διαιρέτης των a, b. Από την πρώτη εξίσωση και την Πρόταση 7.1.4, παίρνουμε ότι $c|r_1$, από τη δεύτερη εξίσωση, $c|r_2$, $\ldots$, και από την προτελευταία, $c|r_n$. Άρα, το r_n είναι ένας μέγιστος κοινός διαιρέτης των a, b. □

7.2 Ασκήσεις

Άσκηση 7.2.1 *Ισχύει στον $\mathbb{Z}_6$ η εξής συνεπαγωγή;*

$$a \cdot b = 0 \Rightarrow a = 0 \text{ ή } b = 0.$$

Λύση 7.2.2 *Όχι:* $2 \cdot 3 = 6 = 0$ *παρότι* $2 \neq 0$ *και* $3 \neq 0$.

Άσκηση 7.2.3 *Είναι ο πολλαπλασιασμός πράξη στο* $\mathbb{Z}_9^*$*;*

Λύση 7.2.4 *Όχι:* $3, 6 \in \mathbb{Z}_9^*$ *ενώ* $3 \cdot 6 = 18 = 0 \notin \mathbb{Z}_9^*$.

Άσκηση 7.2.5 *Αναγνωρίστε την ομάδα* $U(\mathbb{Z}_9)$.

Λύση 7.2.6 *Από το Λήμμα 3.5.2,* $U(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$. *Η* $U(\mathbb{Z}_9)$*, ως αβελιανή ομάδα τάξης* 6*, είναι ισόμορφη με την* $\mathbb{Z}_6$.

Άσκηση 7.2.7 *Αναγνωρίστε την ομάδα* $U(\mathbb{Z}_{18})$.

Λύση 7.2.8 *Από το Λήμμα 3.5.2,* $U(\mathbb{Z}_{18}) = \{1, 5, 7, 11, 13, 17\}$. *Η* $U(\mathbb{Z}_{18})$*, ως αβελιανή ομάδα τάξης* 6*, είναι ισόμορφη με την* $\mathbb{Z}_6$.

Άσκηση 7.2.9 *Είναι η ομάδα* $U(\mathbb{Z}_{24})$ *κυκλική;*.

Λύση 7.2.10 *Όχι, γιατί κάθε μη ταυτοτικό στοιχείο της* $U(\mathbb{Z}_{24}) = \{1, 5, 7, 11, 13, 17, 19, 23\}$ *έχει τάξη* 2.

Άσκηση 7.2.11 *Έστω* a *ένα αντιστρέψιμο στοιχείο δακτυλίου* S *με 1. Να αποδείξετε τους κανόνες απαλοιφής*

1. $ab = ac \Rightarrow b = c$,
2. $ba = ca \Rightarrow b = c$.

Λύση 7.2.12

1. $ab = ac \Rightarrow a'ab = a'ac \Rightarrow (a'a)b = (a'a)c \Rightarrow 1b = 1c \Rightarrow b = c$,
2. $ba = ca \Rightarrow baa' = baa' \Rightarrow b(aa') = b(aa') \Rightarrow b1 = c1 \Rightarrow b = c$.

Άσκηση 7.2.13 *Αν ένας ακέραιος* $n > 1$ *δεν είναι πρώτος, να δείξετε ότι ο δακτύλιος* $\mathbb{Z}_n$ *δεν είναι σώμα.*

Λύση 7.2.14 *Αν ο* $n > 1$ *δεν είναι πρώτος, τότε* $n = n_1 n_2$ *όπου* $n_1, n_2 \in \mathbb{Z}$ *με* $1 < n_1, n_2 < n$. *Στον* $\mathbb{Z}_n$, $n_1 n_2 = 0$ *ενώ* $n_1, n_2 \neq 0$. *Συνεπώς, ο δακτύλιος* $\mathbb{Z}_n$ *δεν είναι ούτε καν ακέραια περιοχή.*
Διαφορετικά, από το Λήμμα 3.5.2, τα n_1, n_2 *του* $\mathbb{Z}_n$ *δεν είναι αντιστρέψιμα γιατί* $\mu\kappa\delta(n_1, n) = n_1 \neq 1, \mu\kappa\delta(n_2, n) = n_2 \neq 1$.

Άσκηση 7.2.15 *Έστω* S *ένας μεταθετικός δακτύλιος με 1 και* $u \in U(S)$. *Να δείξετε ότι για κάθε* $a, b \in S$,

1. $u|a$,
2. $a|u \Rightarrow a \in U(S)$,

3. $a|b \Leftrightarrow ua|b$.

Λύση 7.2.16 1. $a = (au')u$.

2. $a|u \Rightarrow u = qa$ *για κάποιο* $q \in S \Rightarrow 1 = (u'q)a \Rightarrow a \in U(S)$ *με αντίστροφο το* $u'q$.

3. $a|b \Rightarrow b = qa$ *για κάποιο* $q \in S \Rightarrow b = (qu')ua \Rightarrow ua|b$.
Άρα, επειδή το $u' \in U(S)$, *από ό,τι έχουμε ήδη δείξει,*
$ua|b \Rightarrow u'(ua)|b \Rightarrow a|b$.

Άσκηση 7.2.17 *Στο* Z_6 *βρείτε*

1. *τους κοινούς διαιρέτες των* $2, 4$,

2. *τους μέγιστους κοινούς διαιρέτες των* $2, 4$,

3. *τους κοινούς διαιρέτες των* $2, 3$,

4. *τους μέγιστους κοινούς διαιρέτες των* $2, 3$.

Λύση 7.2.18 *Μονάδες είναι τα* $1, 5$. *Λαμβάνοντας υπόψη την Άσκηση 7.2.15,*

1. *κοινοί διαιρέτες των* $2, 4$*:* $1, 5, 2, 4$.

2. *μέγιστοι κοινοί διαιρέτες των* $2, 4$*:* $2, 4$.

3. *κοινοί διαιρέτες των* $2, 3$*:* $1, 5$.

4. *μέγιστοι κοινοί διαιρέτες των* $2, 3$*:* $1, 5$.

Άσκηση 7.2.19 *Σε ακέραια περιοχή* D, *να δείξετε ότι*

1. $ab = ac, a \neq 0 \Rightarrow b = c$,

2. $a|b, b|a \Leftrightarrow b = ua$ *για κάποιο* $u \in U(D)$.

Λύση 7.2.20 1. $ab = ac, a \neq 0 \Rightarrow a(b - c) = ab - ac = 0, a \neq 0 \Rightarrow b - c = 0 \Rightarrow b = c$.

2. *Έστω ότι* $a|b, b|a$. *Τότε* $b = ua, a = vb$ *για κάποια* $u, v \in D$. *Άρα*

$$a1 = a = vua = a(uv).$$

Τώρα αν $a \neq 0$, *από την* (1), $uv = 1$ *και* $u \in U(D)$.
Αν $a = 0$, *εφόσον* $a|b$, *θα έχουμε* $b = 0$ *και* $b = 1a$.
Αντιστρόφως, αν $b = ua$ *κάποιο* $u \in U(D)$ *τότε* $a = u'b$ *και είναι προφανές ότι* $a|b$ *και* $b|a$.

Άσκηση 7.2.21 *Έστω ότι* e, d *είναι μκδ δύο στοιχείων μιας ακέραιας περιοχής* D. *Να δείξετε ότι* $e = ud$ *για κάποιο* $u \in U(D)$.

Λύση 7.2.22 *Από τα δεδομένα* $d|e$ *και* $e|d$. *Από την Άσκηση 7.2.19,* $e = ud$ *για κάποιο* $u \in U(D)$.

7.3 Πολυώνυμα

Ένα **πολυώνυμο** $p(x)$ με συντελεστές σε ένα δακτύλιο S είναι μια τυπική έκφραση της μορφής

$$p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots,$$

όπου $a_0, a_1, a_2, a_3, \ldots \in S$ και για κάποιο ακέραιο $m \geq 0$, $a_{m+1} = a_{m+2} = a_{m+3} \ldots = 0$. Τα $a_0, a_1, a_2, a_3, \ldots$ λέγονται οι **συντελεστές** του $p(x)$. Το a_0 καλείται ο σταθερός συντελεστής του $p(x)$, και το a_n ο συντελεστής βαθμού n.

Σημείωση: Ο προσδιορισμός *τυπική έκφραση* στον παραπάνω ορισμό σημαίνει ακριβώς ότι δύο πολυώνυμα με συντελεστές $a_0, a_1, a_2, a_3, \ldots$ και $b_0, b_1, b_2, b_3, \ldots$, αντίστοιχα, θα θεωρούνται ίσα αν και μόνον αν για κάθε $n \geq 0$, έχουμε $a_n = b_n$.

Συνήθως, στη γραφή του $p(x)$ παραλείπονται οι όροι με μηδενικό συντελεστή. Έτσι, το $p(x) = a_kx^k$ είναι το πολυώνυμο του οποίου όλοι οι συντελεστές είναι μηδενικοί, εκτός ενδεχομένως του συντελεστή βαθμού k. Και το

$$p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_mx^m,$$

είναι το πολυώνυμο του οποίου όλοι οι συντελεστές βαθμού $> m$ είναι μηδενικοί, χωρίς να προεξοφλείται ότι $a_0, a_1, \ldots, a_m \neq 0$.
Ένα πολυώνυμο της μορφής $p(x) = a_0$ λέγεται **σταθερό** πολυώνυμο ή πολυώνυμο **βαθμού** 0. Ο μεγαλύτερος ακέραιος για τον οποίον ο αντίστοιχος συντελεστής ενός μη σταθερού πολυωνύμου $p(x)$ δεν είναι μηδενικός λέγεται ο **βαθμός** του $p(x)$ και συμβολίζεται με $deg(p(x))$.

Το $S[x]$ θα συμβολίζει το σύνολο όλων των πολυωνύμων με συντελεστές σε ένα δακτύλιο S. Στο $S[x]$ ορίζονται οι πράξεις $+, \cdot$ ως εξής.
Έστω $p(x)$ και $q(x)$ δύο μέλη του $S[x]$ με συντελεστές $a_0, a_1, a_2, a_3, \ldots$ και $b_0, b_1, b_2, b_3, \ldots$, αντίστοιχα. Τοτε

1. το $p(x) + q(x)$ είναι το πολυώνυμο με συντελεστή βαθμού n το $a_n + b_n$,
2. το $p(x).q(x)$ είναι το πολυώνυμο με συντελεστή βαθμού n το $a_0b_n + a_1b_{n-1} + \ldots + a_nb_0 = \sum_{i=0}^{n} a_ib_{n-i} = \sum_{i+j=n} a_ib_j$.

Πρόταση 7.3.1 *Το $(S[x], +, \cdot)$ είναι δακτύλιος για κάθε δακτύλιο S. Επιπλέον,*

1. *αν ο S είναι μεταθετικός, τότε και ο $S[x]$ είναι μεταθετικός,*
2. *αν ο S έχει 1, τότε και ο $S[x]$ έχει 1,*
3. *$deg(p(x) + q(x)) \leq \max\{deg(p(x)), deg(q(x))\}$ για κάθε $p(x), q(x) \in S[x]$,*
4. *$deg(p(x)q(x)) \leq deg(p(x)) + deg(q(x))$ για κάθε $p(x), q(x) \in S[x]$,*
5. *αν ο S είναι μια ακέραια περιοχή, τότε και ο $S[x]$ είναι ακέραια περιοχή και $deg(p(x)q(x)) = deg(p(x)) + deg(q(x))$ για κάθε $p(x), q(x) \in S[x] \setminus \{0\}$.*

*Απόδειξη:*7.3.1 Από τον ορισμό των πράξεων του, προκύπτει άμεσα ότι το $(S[x],+)$ αποτελεί αβελιανή ομάδα με το $p(x)=0$ ως το μηδενικό στοιχείο. Προφανώς, το αντίθετο πολυωνύμου με συντελεστές τους $a_0,a_1,a_2,a_3,\ldots$ είναι το πολυώνυμο με συντελεστές τους $-a_0,-a_1,-a_2,-a_3,\ldots$, και αν ο S είναι μεταθετικός, το ίδιο ισχύει για το $S[x]$.
Προκειμένου να δείξουμε ότι ο πολλαπλασιασμός είναι προσεταιριστικός, έστω $p(x),q(x),r(x)\in S[x]$ με συντελεστές $a_0,a_1,a_2,a_3,\ldots$, $b_0,b_1,b_2,b_3,\ldots$, $c_0,c_1,c_2,c_3,\ldots$, αντίστοιχα. Τότε ο συντελεστής βαθμού n του $p(x)(q(x)r(x))$ λόγω του αριστερού επιμεριστικού νόμου του S ισούται με

$$\sum_{k+m=n} a_k(\sum_{i+j=m} b_ic_j)=\sum_{k+i+j=n} a_k(b_ic_j)=\sum_{i+j+k=n} a_i(b_jc_k),$$

και ο συντελεστής βαθμού n του $(p(x)q(x))r(x)$ λόγω του δεξιού επιμεριστικού νόμου του S ισούται με

$$\sum_{m+k=n}(\sum_{i+j=m} a_ib_j)c_k=\sum_{i+j+k=n}(a_ib_j)c_k.$$

Οι δύο συντελεστές είναι ίσοι λόγω προσεταιριστικότητας του πολλαπλασιασμού του S. Άρα, $p(x)(q(x)r(x))=(p(x)q(x))r(x)$ και ο ο πολλαπλασιασμός του $S[x]$ είναι προσεταιριστικός. Οι επιμεριστικοί νόμοι εύκολα επαληθεύονται. Συνεπώς, ο $S[x]$ είναι ένας δακτύλιος.

Αν ο S έχει ως μοναδιαίο στοιχείο το 1, τότε το $p(x)=1$ είναι μοναδιαίο στοιχείο για τον $S[x]$.
Το (3) είναι προφανές. Προκειμένου να δείξουμε τα (4) και (5), θεωρούμε $p(x)\neq 0, q(x)\neq 0$ με $deg(p(x))=m, deg(q(x))=n$ και συντελεστές $a_0,a_1,a_2,a_3,\ldots$, $b_0,b_1,b_2,b_3,\ldots$, αντίστοιχα. Έστω $c_0,c_1,c_2,c_3,\ldots$ οι συντελεστές του γινομένου $p(x)q(x)$. Τότε $a_i=0$ για $i>m$, $a_m\neq 0$, $b_j=0$ για $j>n$, και $b_n\neq 0$. Συνεπώς, ένας από τους a_i,b_j ισούται με 0 για $i+j>m+n$. Άρα, $c_k=0$ για $k>m+n$ και $deg(p(x)q(x))\leq m+n$. Επίσης, $c_{m+n}=a_mb_n$. Όταν ο S είναι μια ακέραια περιοχή, τότε $a_mb_n\neq 0$, οπότε $p(x)q(x)\neq 0$. Άρα, ο $S[x]$ είναι ακέραια περιοχή και $deg(p(x)q(x))=m+n=deg(p(x))+deg(q(x))$. □

Να σημειωθεί ότι, στον $\mathbb{Z}_6[x]$, τα $p(x)=2x^3$ και $q(x)=3x^3$ έχουν βαθμό 3, ενώ $p(x)q(x)=0$.

Θεώρημα 7.3.2 *(Αλγόριθμος διαίρεσης). Έστω F ένα σώμα και $f(x),g(x)\in F[x]$ με $g(x)\neq 0$. Τότε υπάρχουν $q(x),r(x)\in F[x]$ τέτοια ώστε*

$$f(x)=q(x)g(x)+r(x) \text{ και } r(x)=0 \text{ ή } deg(r(x))<deg(g(x)).$$

*Απόδειξη:*7.3.2 Με επαγωγή στο βαθμό του διαιρετέου.
Αν το $g(x)$ είναι σταθερό, $g(x)=b_0\neq 0$, τότε μπορούμε να θέσουμε $q(x)=b_0'f(x)$ και $r(x)=0$. Έτσι μπορούμε να υποθέσουμε ότι $deg(g(x))>0$.
Αν $deg(f(x))<deg(g(x))$, τότε μπορούμε να θέσουμε $q(x)=0$ και $r(x)=f(x)$. Μπορούμε, λοιπόν, να υποθέσουμε ότι

$$f(x)=a_0+a_1x+a_2x^2+a_3x^3+\ldots+a_nx^n,$$
$$g(x)=b_0+b_1x+b_2x^2+b_3x^3+\ldots+b_mx^m,$$

όπου $0 < m \leq n, a_n \neq 0, b_m \neq 0$. Τώρα το

$$h(x) = f(x) - a_n b'_m x^{n-m} g(x)$$

έχει βαθμό $\leq n-1$ και από την επαγωγική υπόθεση, υπάρχουν $q_1(x), r_1(x) \in F[x]$ τέτοια ώστε

$$h(x) = q_1(x)g(x) + r_1(x) \text{ και } r_1(x) = 0 \text{ ή } deg(r_1(x)) < deg(g(x)).$$

Αρκεί τώρα να θέσουμε $q(x) = a_n b'_m x^{n-m} + q_1(x)$ και $r(x) = r_1(x)$.

□

Σημείωση: Το $q(x)$ στο Θεώρημα 7.3.2 καλείται το **πηλίκο** της διαίρεσης του $f(x)$ με το $g(x)$, και το $r(x)$ το **υπόλοιπο**.

Όπως και στον δακτύλιο $\mathbb{Z}$, με δεδομένο τον Ευκλείδειο αλγόριθμο, ο αλγόριθμος διαίρεσης μας εξασφαλίζει μια διαδικασία εύρεσης ενός μέγιστου κοινού διαιρέτη δύο πολυωνύμων $f(x), g(x)$ στον $F[x]$, η οποία, μάλιστα, μας επιτρέπει να τον εκφράσουμε ως γραμμικό συνδυασμό των $f(x), g(x)$.

Παράδειγμα 1. Έστω ότι θέλουμε ένα $\mu\kappa\delta(f(x), g(x))$ στο $\mathbb{Q}[x]$, όπου $f(x) = x^4 + x^2 + x + 1, g(x) = x^2 + 1$.
Κάνοντας, με το γνωστό τρόπο, διαδοχικές διαιρέσεις, έχουμε

$$\begin{aligned} f(x) = x^4 + x^2 + x + 1 &= x^2(x^2+1) + (x+1), \quad r_1(x) = x+1 \\ g(x) = x^2 + 1 &= (x-1)(x+1) + 2, \qquad r_2(x) = 2 \\ r_1(x) = x + 1 &= \frac{1}{2}(x+1)2 + 0 \end{aligned}$$

Από τον Ευκλείδειο αλγόριθμο, το $r_2(x) = 2$ είναι ένας $\mu\kappa\delta(f(x), g(x)))$. Από τις παραπάνω εξισώσεις,

$$\begin{aligned} 2 &= g(x) - (x-1)(x+1) \\ &= g(x) - (x-1)(f(x) - x^2 g(x) \\ &= (1-x)f(x) + (x^3 - x^2 + 1)g(x). \end{aligned}$$

Παράδειγμα 2. Για να βρούμε στο $\mathbb{Z}_2[x]$ ένα $\mu\kappa\delta(f(x), g(x))$, όπου $f(x) =$

$x^4 + x^2 + x + 1, g(x) = x^2 + 1$, κάνοντας διαδοχικές διαιρέσεις, έχουμε

$$\begin{aligned} f(x) = x^4 + x^2 + x + 1 &= x^2(x^2+1) + (x+1), \\ g(x) = x^2 + 1 &= (x+1)(x+1) + 0 \end{aligned}$$

Άρα το $x+1$ είναι ένας $\mu\kappa\delta(f(x),g(x))$.
Προφανώς, $x+1 = f(x) - x^2 g(x)$.

Παράδειγμα 3. Για να βρούμε στο $\mathbb{Z}_{11}[x]$ ένα $\mu\kappa\delta(f(x),g(x))$, όπου $f(x) = x^4+x^2+x+1, g(x) = x^2+1$, κάνοντας διαδοχικές διαιρέσεις, έχουμε

$$\begin{aligned} f(x) = x^4+x^2+x+1 &= x^2(x^2+1)+(x+1), \\ g(x) = x^2+1 &= (x-1)(x+1)+2, \\ x+1 &= 6(x+1)2+0. \end{aligned}$$

Από τον Ευκλείδειο αλγόριθμο, το 2 είναι ένας $\mu\kappa\delta(f(x),g(x))$. Από τις παραπάνω εξισώσεις,

$$\begin{aligned} 2 &= g(x)-(x-1)(x+1) \\ &= g(x)-(x-1)(f(x)-x^2g(x) \\ &= (1-x)f(x)+(x^3-x^2+1)g(x). \end{aligned}$$

Σημείωση: Έστω F ένα σώμα. Είναι προφανές ότι οι μονάδες του $F[x]$ είναι ακριβώς όλα τα μη μηδενικά σταθερά πολυώνυμα. Ένα πολυώνυμο θα λέγεται **μονικό** αν ο συντελεστής μεγίστου βαθμού είναι το 1. Έστω $d(x)$ ένας μέγιστος κοινός διαιρέτης δύο πολυωνύμων $f(x), g(x) \in F[x]$, εκ των οποίων τουλάχιστον το ένα δεν είναι μηδενικό. Τότε οι λοιποί μέγιστοι κοινοί διαιρέτες είναι της μορφής $\lambda d(x)$, λ μια μονάδα του $F[x]$. Το μοναδικό μονικό πολυώνυμο εξ αυτών θεωρείται *ο μεγιστος κοινός διαιρέτης* των $f(x), g(x)$.
Στα παραπάνω παραδείγματα, οι μέγιστοι κοινοί διαιρέτες είναι: 1, $x+1$ και 1, αντίστοιχα.

Έστω S ένας δακτύλιος. Για κάθε $a \in S$ και κάθε πολυώνυμο

$$p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_mx^m$$

με συντελεστές στον S, $p(a)$ συμβολίζει το στοιχείο του S πού προκύπτει όταν στο $p(x)$ αντικαταστήσουμε το x με το a. Δηλαδή,

$$p(a) = a_0 + a_1a + a_2a^2 + a_3a^3 + \ldots + a_mx^m.$$

Αν $p(a) = 0$, το a λέγεται **ρίζα** του $p(x)$. Αν $f(x) = p(x)+q(x)$ και $g(x) = p(x)q(x)$, εύκολα επαληθεύεται ότι $f(a) = p(a)+q(a)$ και $g(a) = p(a)q(a)$.

Πρόταση 7.3.3 *Έστω F ένα σώμα, $a \in F$ και $f(x) \in F[x]$. Τότε το $x-a$ διαιρεί το $f(x)$ αν και μόνον αν το a είναι ρίζα του $f(x)$.*

*Απόδειξη:*7.3.3 Από τον αλγόριθμο διαίρεσης για τον $F[x]$,

$$f(x) = q(x)(x-a) + r(x) \text{ με } deg(r(x)) < deg(x-a) = 1.$$

Έτσι, το $r(x)$ είναι ένα σταθερό πολυώνυμο, και μπορούμε να θέσουμε $r(x) = b$. Οπότε, αν το a είναι ρίζα του $f(x)$, τότε $0 = q(a)(a-a) + b = b = r(x)$ και, επομένως, το $x-a$ διαιρεί το $f(x)$.
Αντιστρόφως, αν το $x-a$ διαιρεί το $f(x)$, τότε $f(x) = g(x)(x-a)$ για κάποιο $g(x) \in F[x]$, οπότε $f(a) = g(a)(a-a) = 0$. □

Πρόταση 7.3.4 *Έστω F ένα σώμα και $f(x) \in F[x]$ με $deg(f(x)) = n > 0$. Τότε στο F το $f(x)$ έχει $\leq n$ ρίζες.*

*Απόδειξη:*7.3.4 Με επαγωγή στο βαθμό του πολυωνύμου. Βέβαια, ένα πολυώνυμο πρώτου βαθμού, $ax + b \in F[x]$, έχει μοναδική ρίζα το $-ba' \in F$. Μπορούμε, λοιπόν, να υποθέσουμε ότι $deg(f(x)) = n > 1$ και ότι το $f(x)$ έχει μια τουλάχιστον ρίζα $a \in F$. Από την Πρόταση 7.3.3, έχουμε $f(x) = g(x)(x-a)$ για κάποιο $g(x) \in F[x]$. Επομένως, κάθε ρίζα του $f(x)$ διαφορετική από την a θα είναι ρίζα και του $g(x)$. Από την Πρόταση 7.3.1, $deg(g(x)) = n-1 > 0$ και, από την προφανή επαγωγική υπόθεση, το $g(x)$ έχει $\leq n-1$ ρίζες στο F. Συνεπώς, το $f(x)$ έχει $\leq (n-1)+1 = n$ ρίζες. □

Έστω S ένας δακτύλιος και $f(x) \in S[x]$ με $degf(x) = n > 0$. Το $f(x)$ λέγεται **αναγώγιμο** πάνω από τον S αν είναι γινόμενο δύο πολυωνύμων $g(x), h(x) \in S[x]$ με $deg(g(x)) < n, deg(h(x)) < n$. Διαφορετικά το $f(x)$ λέγεται **ανάγωγο** πάνω από το S. Προφανώς, όλα τα πολυώνυμα βαθμού 1 είναι ανάγωγα.

Πρόταση 7.3.5 *Έστω F ένα σώμα και $f(x) \in F[x]$ με $degf(x) = n > 1$. Αν το $f(x)$ έχει κάποια ρίζα $a \in F$, τότε το $f(x)$ είναι αναγώγιμο πάνω από το F.*

*Απόδειξη:*7.3.5 Από την Πρόταση 7.3.3, έχουμε $f(x) = g(x)(x-a)$ για κάποιο $g(x) \in F[x]$. Από την Πρόταση 7.3.1, $deg(g(x)) = n-1$. Αφού και $deg(x-a) = 1 < n = degf(x)$, το $f(x)$ είναι αναγώγιμο. □

Σημειώστε ότι το γεγονός ότι το $f(x) = (x^2+1)(x^2+1)$ δεν έχει ρίζες στο $\mathbb{R}$ δεν εξασφαλίζει ότι το $f(x)$ είναι ανάγωγο πάνω από το $\mathbb{R}$.

Πρόταση 7.3.6 *Έστω F ένα σώμα και $f(x) \in F[x]$ με $deg(f(x)) = 2$ ή 3. Τότε το $f(x)$ είναι αναγώγιμο πάνω από το F αν και μόνον αν το $f(x)$ έχει τουλάχιστον μια ρίζα στο F.*

*Απόδειξη:*7.3.6 Έστω ότι το $f(x)$ είναι αναγώγιμο, οπότε γράφεται ως $f(x) = g(x)h(x)$ με $g(x), h(x) \in F[x]$ και $deg(g(x)), deg(h(x)) < deg(f(x))$. Τότε, επειδή $deg(f(x)) = 2$ ή 3, αναγκαστικά τουλάχιστον ένα από τα $g(x), h(x)$ θα είναι πρώτου βαθμού, επομένως θα έχει μια ρίζα στο F, η οποία θα είναι προφανώς ρίζα και του $f(x)$. Το αντίστροφο είναι συνέπεια της Πρότασης 7.3.5. □

7.4 Ασκήσεις

Άσκηση 7.4.1 *Να δείξετε ότι τα $q(x)$ και $r(x)$ στο Θεώρημα 7.3.2 είναι μοναδικά.*

Λύση 7.4.2 *Έστω ότι*

$$f(x) = q_1(x)g(x) + r_1(x), \text{ όπου } r_1(x) = 0 \text{ ή } deg(r_1(x)) < deg(g(x)) \text{ και}$$

$$f(x) = q_2(x)g(x) + r_2(x), \text{ όπου } r_2(x) = 0 \text{ ή } deg(r_2(x)) < deg(g(x)).$$

Τότε $r_2(x) - r_1(x) = (q_1(x) - q_2(x))g(x)$. Αν $q_1(x) - q_2(x) \neq 0$, από την Πρόταση 7.3.1, $deg(r_2(x) - r_1(x)) \geq deg(g(x))$. Αυτό συνεπάγεται ότι $r_1(x) = 0$ και $r_2(x) = 0$, οπότε $(q_1(x) - q_2(x))g(x) = 0$, πράγμα που αντιφάσκει στο γεγονός ότι ο $F[x]$ είναι ακέραια περιοχή. Συνεπώς, $q_1(x) - q_2(x) = 0$, $q_1(x) = q_2(x)$ και $r_1(x) = r_2(x)$.

Άσκηση 7.4.3 *Βρείτε ένα μκδ των $2x^3 + 2x^2 + 1$ και $3x^2 + 2$ στο $\mathbb{Z}_5[x]$.*

Λύση 7.4.4 *Στο $\mathbb{Z}_5[x]$,*

$$\begin{aligned} 2x^3 + 2x^2 + 1 &= (4x + 4)(3x^2 + 2) + (2x + 3) \\ 3x^2 + 2 &= (4x + 4)(2x + 3) + 0. \end{aligned}$$

Άρα, ένας μκδ είναι το $2x + 3$. Ο μκδ είναι το $3(2x + 3) = x + 4$.

Άσκηση 7.4.5 *Βρείτε ένα μκδ των $f(x) = x^5 + 2$ και $g(x) = 3x^3 + 1$ στο $\mathbb{Z}_{11}[x]$.*

Λύση 7.4.6 *Στο $Z_{11}[x]$,*

$$\begin{aligned} x^5 + 2 &= 4x^2(3x^3 + 1) + (7x^2 + 2) \\ 3x^3 + 1 &= 2x(7x^2 + 2) + (7x + 1) \\ 7x^2 + 2 &= (x + 3)(7x + 1) - 1 \\ 7x + 1 &= (-7x - 1)(-1) + 0 \end{aligned}$$

Άρα, ένας μκδ είναι το $-1 = 10$. Ο μκδ είναι το 1.

Άσκηση 7.4.7 *Βρείτε ένα μκδ των $f(x) = x^7 + 2x^6 + 3x^5 + x^4 + 2x + 5$ και $g(x) = 3x^4 + 4$ στο $\mathbb{Z}_7[x]$.*

Λύση 7.4.8 *Στο $Z_7[x]$,*

$$\begin{aligned} x^7 + 2x^6 + 3x^5 + x^4 + 2x + 5 &= (5x^3 + 3x^2 + x + 5)(3x^4 + 4) + (x^3 + 2x^2 + 5x + 6) \\ 3x^4 + 4 &= (3x + 1)(x^3 + 2x^2 + 5x + 6) + (4x^2 + 5x + 5) \\ x^3 + 2x^2 + 5x + 6 &= (2x + 5)(4x^2 + 5x + 5) + (5x + 2) \\ 4x^2 + 5x + 5 &= (5x + 6)(5x + 2) + 0. \end{aligned}$$

Ένας μκδ είναι το $5x + 2$. Ο μκδ είναι το $3(5x + 2) = x + 6$.

Άσκηση 7.4.9 *Είναι το $f(x) = x^4 + 4x^2 + 3$ αναγώγιμο πάνω από το $\mathbb{R}$; Έχει ρίζες στο $\mathbb{R}$;*

Λύση 7.4.10 $f(x) = x^4 + 4x^2 + 3 = (x^2 + 1)(x^2 + 3)$
Είναι μεν αναγώγιμο πάνω από το $\mathbb{R}$, αλλά δεν έχει ρίζες στο $\mathbb{R}$ γιατί και οι 4 ρίζες του είναι φανταστικές.

Άσκηση 7.4.11 *Είναι το $f(x) = x^3 + 3x + 2$ ανάγωγο πάνω από το $\mathbb{Z}_2$;*
Αναλύστε το $f(x)$ σε γραμμικούς παράγοντες πάνω από το $\mathbb{Z}_2$.

Λύση 7.4.12 *Προφανώς, $f(0) = f(1) = 0$ και το $f(x)$ είναι αναγώγιμο. Μάλιστα*

$$f(x) = x^3 + x = x(x^2 + 1) = x(x + 1)^2 = x(x + 1)(x + 1).$$

Άσκηση 7.4.13 *Αναλύστε το $f(x) = x^3 + 3x + 2$ σε γραμμικούς παράγοντες πάνω από το $\mathbb{Z}_3$.*

Λύση 7.4.14 *Το 1 είναι η μόνη ρίζα, και $f(x) = x^3 - 1 = (x - 1)^3$.*

Άσκηση 7.4.15 *Εξετάστε αν το $f(x) = x^4 + 4$ αναλύεται σε γραμμικούς παράγοντες πάνω από το Z_5.*

Λύση 7.4.16 *Το $f(x) = x^4 + 4 = x^4 - 1 = (x^2 - 1)(x^2 + 1)$ έχει ρίζες τα $1, -1, 2, -2$.*
Προφανώς, $f(x) = (x - 1)(x + 1)(x - 2)(x + 2)$.

Άσκηση 7.4.17 *Εξετάστε αν το $f(x) = x^3 + 3x + 2$ είναι ανάγωγο πάνω από το Z_5.*

Λύση 7.4.18 *$f(0) = 2, f(1) = 1, f(-1) = 3, f(2) = 1, f(-2) = 3$. Από την Πρόταση 7.3.6, το τριτοβάθμιο πολυώνυμο $f(x)$ είναι ανάγωγο πάνω από το Z_5 γιατί δεν έχει ρίζες στο Z_5.*

Άσκηση 7.4.19 *Εξετάστε αν το $f(x) = x^3 + x + 1$ είναι ανάγωγο πάνω από το Z_7.*

Λύση 7.4.20 *Στο $\mathbb{Z}_7$, $f(0) = 1, f(1) = 3, f(2) = 4, f(3) = 3, f(4) = f(-3) = -1, f(5) = f(-2) = -2$, $f(6) = f(-1) = -1$. Αφού είναι τρίτου βαθμού και δεν έχει ρίζες στο Z_7, από την Πρόταση 7.3.6,το $f(x)$ είναι ανάγωγο πάνω από το Z_7.*

Άσκηση 7.4.21 *Εξετάστε αν το $f(x) = x^3 + x + 1$ είναι ανάγωγο πάνω από το Z_{11}.*

Λύση 7.4.22 *Στο Z_{11}, το 2 είναι μια ρίζα του $f(x)$ και $deg(f(x)) > 1$. Έτσι το $f(x)$ είναι αναγώγιμο πάνω από το Z_{11}.*

Άσκηση 7.4.23 *Για ποιους πρώτους αριθμούς p, είναι το $x + 4$ παράγοντας του $f(x) = x^3 + x + 2$ στο $Z_p[x]$;*

Λύση 7.4.24 *Στο $Z_p[x]$, από την Πρόταση 7.3.3, το $x+4$ είναι παράγοντας του $f(x) = x^3 + x + 2$ αν και μόνον αν $f(-4) = -66 = 0$. Οι ζητούμενοι πρώτοι είναι οι διαιρέτες του $66 = 2 \times 3 \times 11$, δηλαδή, οι $2, 3, 11$.*

Άσκηση 7.4.25 *Δείξτε ότι το $f(x) = x^4 + x^3 + x + 1$ είναι αναγώγιμο πάνω από οποιοδήποτε σώμα F.*

Λύση 7.4.26 *Το $f(x)$ έχει μια τουλάχιστον ρίζα, το $-1 \in F$, και συνεπώς είναι αναγώγιμο.*

Άσκηση 7.4.27 *Βρείτε όλες τις ρίζες του $x^2 - 1$ στον Z_8.*

Λύση 7.4.28 *Ρίζες του $x^2 - 1$ είναι ακριβώς όλες οι μονάδες του Z_8, δηλαδή, τα $1, 3, 5, 7$.*

Άσκηση 7.4.29 *Έστω ότι κάποια διακεκριμένα στοιχεία $a_1, a_2, \ldots, a_k$ ενός σώματος F είναι ρίζες ενός πολυωνύμου $f(x) \in F[x]$.*
Να δείξετε ότι το πολυώνυμο $(x - a_1)(x - a_2) \ldots (x - a_k)$ διαιρεί το $f(x)$.

Λύση 7.4.30 *Η απόδειξη γίνεται με επαγωγή στο k. Από την Πρόταση 7.3.3, το αποτέλεσμα ισχύει για $k = 1$. Υποθέτουμε, λοιπόν, ότι $k > 1$ και το αποτέλεσμα ισχύει για $k - 1$ ρίζες οποιουδήποτε πολυωνύμου. Τότε το $x - a_k$ διαιρεί το $f(x)$ και, συνεπώς, για κάποιο $g(x) \in F[x]$, έχουμε ότι $f(x) = g(x)(x - a_k)$. Έτσι, για $1 \leq i < k$, έχουμε ότι $a_i - a_k \neq 0$ και $f(a_i) = 0 = (a_i - a_k)g(a_i)$. Συνεπώς, τα $a_1, a_2, \ldots, a_{k-1}$ αποτελούν ρίζες του $g(x)$. Τώρα, από την επαγωγική υπόθεση, για κάποιο $h(x) \in F[x]$, έχουμε ότι*

$$g(x) = h(x)(x - a_1)(x - a_2) \ldots (x - a_{k-1})$$

Συνεπώς,

$$f(x) = g(x)(x - a_k) = h(x)(x - a_1)(x - a_2) \ldots (x - a_k),$$

και το $(x - a_1)(x - a_2) \ldots (x - a_k)$ διαιρεί το $f(x)$.

Κεφάλαιο 8

Ιδεώδη και Ομομορφισμοί Δακτυλίων

8.1 Υποδακτύλιοι

Στη θεωρία ομάδων οι έννοιες της υποομάδας και της κανονικής υποομάδας είναι πολύ σημαντικές. Οι αντίστοιχες έννοιες στη θεωρία δακτυλίων είναι εκείνες του υποδακτυλίου και του ιδεώδους.

Έστω $(S, +, \cdot)$ ένας δακτύλιος. Ένα υποσύνολο H του S λέγεται **υποδακτύλιος** του S αν είναι κλειστό ως προς τις πράξεις $+$ και $\cdot$ και το $(H, +, \cdot)$ αποτελεί δακτύλιο. Προφανώς, το H είναι υποδακτύλιος του S αν και μόνον αν το H είναι κλειστό ως προς τις πράξεις $+$ και $\cdot$ και το $(H, +)$ αποτελεί υποομάδα της $(S, +)$. Ένα υποσύνολο H ενός δακτυλίου S λέγεται **ιδεώδες** του S αν

(i) το $(H, +)$ είναι υποομάδα της $(S, +)$ και

(ii) για κάθε $h \in H$ και κάθε $s \in S$, τα στοιχεία hs και sh ανήκουν στο H.

Προφανώς, κάθε ιδεώδες του S είναι και υποδακτύλιος του S.

Παραδείγματα. Για κάθε $n \in \mathbb{N}$, το $n\mathbb{Z}$ είναι ένα ιδεώδες του $\mathbb{Z}$.
Το $\mathbb{Z}$ είναι ένας υποδακτύλιος του $\mathbb{Q}$, δεν είναι όμως ένα ιδεώδες του $\mathbb{Q}$.

Πρόταση 8.1.1 *Έστω H ένα μη κενό υποσύνολο ενός μεταθετικού δακτυλίου S με 1. Τότε το H είναι ιδεώδες του S αν και μόνον αν $sa + tb \in H$ για κάθε $a, b \in H$ και $s, t \in S$.*

*Απόδειξη:*8.1.1 Αν το H είναι ιδεώδες του S, είναι προφανές ότι $sa, tb \in H$, άρα και $sa + tb \in H$, για κάθε $a, b \in H$ και $s, t \in S$.

Αντιστρόφως, ας υποθέσουμε ότι $sa + tb \in H$ για κάθε $a, b \in H$ και $s, t \in S$. Τότε, αφού ο S είναι μεταθετικός, για κάθε $h \in H$ και $s \in S$, $hs = sh = sh + 0h \in H$. Προφανώς, για να δείξουμε ότι το το H είναι ιδεώδες του S, αρκεί τώρα να

δείξουμε ότι είναι υποομάδα ως προς την $+$. Αυτό προκύπτει από το γεγονός ότι ισχύουν οι εξής τρεις συνθήκες.

1. Για κάθε $a, b \in H$, $a + b = 1a + 1b \in H$.
2. Έστω h_0 ένα μέλος του μη κενού H. Τότε $0 = 0h_0 + 0h_0 \in H$.
3. $h \in H \Rightarrow -h = 0h + (-1)h \in H$.

□

Από την Πρόταση 8.1.1, για κάθε μέλος a ενός μεταθετικού δακτυλίου S με 1, το σύνολο

$$\langle a \rangle = \{sa : s \in S\},$$

δηλαδή, το σύνολο όλων των πολλαπλασίων του a, αποτελεί ένα ιδεώδες του S. Το $\langle a \rangle$ λέγεται το **κύριο ιδεώδες** με **γεννήτορα** το a ή το κύριο ιδεώδες που **παράγεται** από το a.

8.2 Ασκήσεις

Άσκηση 8.2.1 *Δείξτε ότι το σύνολο $\mathbb{Z}(i) = \{m + ni : m, n \in \mathbb{Z}\}$ είναι υποδακτύλιος του $\mathbb{C}$.*

Λύση 8.2.2 *Εύκολα ελέγχεται ότι το $\mathbb{Z}(i)$, ως προς την $+$, είναι υποομάδα της $\mathbb{C}$. Επίσης, είναι κλειστό ως προς τον $\cdot$ γιατί για κάθε $m_1, n_1, m_2, n_2 \in \mathbb{Z}$,*

$$(m_1 + n_1 i)(m_2 + n_2 i) = (m_1 m_2 - n_1 n_2) + (m_1 n_2 + m_2 n_1)i \in \mathbb{Z}(i).$$

Συνεπώς, το $\mathbb{Z}(i)$ είναι υποδακτύλιος του $\mathbb{C}$.

Άσκηση 8.2.3 *Δείξτε ότι, για κάθε $k \in \mathbb{N}$, το σύνολο*

$$\mathbb{Z}(\sqrt{k}) = \{m + n\sqrt{k} : m, n \in \mathbb{Z}\}$$

είναι υποδακτύλιος του $\mathbb{R}$.

Λύση 8.2.4 *Εύκολα ελέγχεται ότι το $\mathbb{Z}(\sqrt{k})$, ως προς την $+$, είναι υποομάδα της $\mathbb{R}$. Επίσης, είναι κλειστό ως προς τον $\cdot$ γιατί για κάθε $m_1, n_1, m_2, n_2 \in \mathbb{Z}$,*

$$(m_1 + n_1\sqrt{k})(m_2 + n_2\sqrt{k}) = (m_1 m_2 + n_1 n_2 k) + (m_1 n_2 + m_2 n_1)\sqrt{k} \in \mathbb{Z}(i).$$

Συνεπώς, το $\mathbb{Z}(\sqrt{k})$ είναι υποδακτύλιος του $\mathbb{R}$.

Άσκηση 8.2.5 *Δείξτε ότι, για κάθε $k \in \mathbb{N}$ το σύνολο*

$$\mathbb{Q}(\sqrt{k}) = \{p + q\sqrt{k} : p, q \in \mathbb{Q}\}$$

είναι υπόσωμα του $\mathbb{R}$.

Σημείωση Ένα υποσύνολο T ενός σώματος S λέγεται **υπόσωμα** του S αν το T αποτελεί σώμα ως προς τις πράξεις της πρόσθεσης και του πολλαπλασιασμού του S.

Λύση 8.2.6 *Ότι το $\mathbb{Q}(\sqrt{k})$ είναι ένας υποδακτύλιος του $\mathbb{R}$ αποδεικνύεται όπως και η Άσκηση 8.2.3. Προφανώς, το $\mathbb{Q}(\sqrt{k})$ είναι μεταθετικός δακτύλιος με 1. Αν η $\sqrt{k}$ είναι ένας ρητός αριθμός, τότε $\mathbb{Q}(\sqrt{k}) = \mathbb{Q}$. Αν $\sqrt{k} \notin \mathbb{Q}$, ένα μη μηδενικό στοιχείο $p + q\sqrt{k}$ του $\mathbb{Q}(\sqrt{k})$ έχει αντίστροφο το $\frac{p-q\sqrt{k}}{p^2-q^2k} \in \mathbb{Q}(\sqrt{k})$. Οπότε σε κάθε περίπτωση το $\mathbb{Q}(\sqrt{k})$ είναι ένα σώμα, ένα υπόσωμα του $\mathbb{R}$.*

Άσκηση 8.2.7 *Να δείξετε ότι ένα σώμα F έχει μόνο 2 ιδεώδη.*

Λύση 8.2.8 *Έστω H ένα ιδεώδες του F. Ας υποθέσουμε ότι $H \neq \{0\}$. Τότε υπάρχει $h_0 \in H$ με $h_0 \neq 0$. Βέβαια το μη μηδενικό στοιχείο h_0 του σώματος F έχει αντίστροφο $h_0' \in F$. Τώρα, για κάθε $x \in F$, $xh_0' \in F$. Επειδή το H είναι ιδεώδες, $x = (xh_0')h_0 \in H$. Άρα, $H = F$.*
Συνεπώς, το F έχει μόνο 2 ιδεώδη, το $\{0\}$ και το F.

8.3 Ομομορφισμοί Δακτυλίων

Έστω S και T δύο δακτύλιοι. Μια συνάρτηση $\phi : S \to T$ λέγεται **ομομορφισμός δακτυλίων** αν για κάθε $a, b \in S$,

1. $\phi(a + b) = \phi(a) + \phi(b)$, και
2. $\phi(ab) = \phi(a)\phi(b)$.

Η (1) μας εξασφαλίζει ότι η $\phi : (S, +) \to (T, +)$ είναι ομομορφισμός ομάδων.

Πρόταση 8.3.1 *Έστω $\phi : S \to T$ ένας ομομορφισμός δακτυλίων. Τότε*

1. $\phi(0) = 0$,
2. $\phi(-x) = -\phi(x)$ *για κάθε* $x \in S$,
3. $\phi(nx) = n\phi(x)$ *για κάθε* $x \in S$ *και* $n \in \mathbb{Z}$,
4. $\phi(x - y) = \phi(x) - \phi(y)$ *για κάθε* $x, y \in S$.

Απόδειξη:8.3.1 Τα σύνολα S και T είναι ομάδες ως προς την $+$ και ο $\phi : S \to T$ είναι ομομορφισμός ομάδων. Συνεπώς, τα (1), (2) και (3) δεν είναι παρά μια ειδική περίπτωση του Θεωρήματος 6.1.2. Το (4) έπεται από το (2):

$$\phi(x - y) = \phi(x + (-y)) = \phi(x) + \phi(-y) = \phi(x) + (-\phi(y)) = \phi(x) - \phi(y).$$

□

Ένας ομομορφισμός δακτυλίων $\phi : S \to T$ λέγεται **μονομορφισμός**, **επιμορφισμός**, ή **ισομορφισμός** αν η συνάρτηση ϕ είναι $1 - 1$, επί, ή $1 - 1$ και επί, αντίστοιχα.

Πρόταση 8.3.2 *Έστω $\phi : S \to T$ ένας επιμορφισμός δακτυλίων. Τότε,*

1. *αν ο S είναι μεταθετικός, τότε και ο T είναι μεταθετικός,*
2. *αν ο S έχει το 1 ως μοναδιαίο στοιχείο, τότε ο T έχει το $\phi(1)$ ως μοναδιαίο στοιχείο.*

*Απόδειξη:*8.3.2

1. Έστω $t_1, t_2 \in T$. Επειδή ο ϕ είναι επί, υπάρχουν $s_1, s_2 \in S$ τέτοια ώστε $\phi(s_1) = t_1, \phi(s_2) = t_2$. Επειδή ο ϕ είναι ομομορφισμός και ο S είναι μεταθετικός,

$$t_1 t_2 = \phi(s_1)\phi(s_2) = \phi(s_1 s_2) = \phi(s_2 s_1) = \phi(s_2)\phi(s_1) = t_2 t_1.$$

   Άρα και ο T είναι μεταθετικός.

2. Έστω ότι ο S έχει το 1 ως μοναδιαίο στοιχείο. Κάθε $t \in T$ γράφεται ως $t = \phi(s)$ για κάποιο $s \in S$, οπότε

$$t\phi(1) = \phi(s)\phi(1) = \phi(s1) = \phi(s) = t \text{ και}$$
$$\phi(1)t = \phi(1)\phi(s) = \phi(1s) = \phi(s) = t.$$

   Συνεπώς, το $\phi(1)$ είναι μοναδιαίο στοιχείο για τον T.

□

Έστω $\phi : S \to T$ ένας ομομορφισμός δακτυλίων. Το υποσύνολο

$$\{s \in S : \phi(s) = 0\}$$

του S ονομάζεται ο **πυρήνας** του ϕ και συμβολίζεται με $Ker\phi$.

Πρόταση 8.3.3 *Ο πυρήνας $Ker\phi$ ομομορφισμού δακτυλίων $\phi : S \to T$ είναι ένα ιδεώδες του S.*

*Απόδειξη:*8.3.3 Τα σύνολα S και T είναι ομάδες ως προς την $+$, ο $\phi : S \to T$ είναι ομομορφισμός ομάδων και $Ker\phi$ είναι ο πυρήνας αυτού του ομομορφισμού. Από το Θεώρημα 6.3.4, το σύνολο $Ker\phi$ είναι υποομάδα της S. Τώρα, για κάθε $s \in S$ και $h \in H$, έχουμε ότι $\phi(h) = 0$ και, από την ιδιότητα (2) του ορισμού του ομομορφισμού δακτυλίων,

$$\phi(sh) = \phi(s)\phi(h) = \phi(s)0 = 0 \text{ και } \phi(hs) = \phi(h)\phi(s) = 0\phi(s) = 0.$$

Συνεπώς, $sh, hs \in Ker\phi$ και ο $Ker\phi$ είναι ένα ιδεώδες του S. □

Αντιστρόφως, όπως θα δείξουμε στο επόμενο Θεώρημα, κάθε ιδεώδες ενός δακτυλίου S είναι ο πυρήνας ενός ομομορφισμού με πεδίο όρισμού το S.

Έστω H ένα ιδεώδες ενός δακτυλίου S. Στο σύνολο $S/H = \{a + H : a \in S\}$, το οποίο αποτελείται από όλα τα αριστερά σύμπλοκα της υποομάδας H της $(S, +)$, στη Θεωρία Ομάδων, ορίσαμε την πράξη $+$ με

$$(a+H)+(b+H)=(a+b)+H.$$

Τώρα που το S είναι εφοδιασμένο και με την πράξη του πολλαπλασιασμού, ορίζουμε τον **πολλαπλασιασμό** $\cdot$ στο S/H με

$$(a+H)\cdot(b+H)=ab+H.$$

Αν $a_1+H=a_2+H$ και $b_1+H=b_2+H$, τότε $a_1-a_2, b_1-b_2\in H$. Επειδή το H είναι ιδεώδες,

$$(a_1-a_2)b_1, a_2(b_1-b_2)\in H, \text{ άρα και}$$
$$a_1b_1-a_2b_2=(a_1-a_2)b_1+a_2(b_1-b_2)\in H.$$

Συνεπώς, $a_1b_1+H=a_2b_2+H$ και ο πολλαπλασιασμός στο S/H είναι καλά ορισμένος.

Θεώρημα 8.3.4 *Για κάθε ιδεώδες H ενός δακτυλίου S, το $(S/H,+,.)$ είναι δακτύλιος με ουδέτερο στοιχείο το $0+H=H$. Επιπλέον, ισχύουν και τα εξής.*

1. *Η φυσική απεικόνιση $\pi: S\to S/H$ που στέλνει το a στο $a+H$ είναι επιμορφισμός δακτυλίων με $Ker\pi=H$.*
2. *Αν ο S είναι μεταθετικός, το ίδιο ισχύει και για τον S/H.*
3. *Αν ο S έχει μοναδιαίο στοιχείο 1, τότε ο S/H έχει το $1+H$ ως μοναδιαίο στοιχείο.*
4. *Αν ο S είναι πεπερασμένος, τότε $|S|=|S/H||H|$.*

*Απόδειξη:*8.3.4 Γνωρίζουμε ήδη από το Θεώρημα 6.5.1 ότι το S/H ως προς την $+$ αποτελεί αβελιανή ομάδα με ουδέτερο στοιχείο το $0+H=H$. Η προσεταιριστικότητα του πολλαπλασιασμού του S/H και οι επιμεριστικοί νόμοι έπονται με τετριμμένο τρόπο από τις αντίστοιχες ιδιότητες του S. Συνεπώς, το $(S/H,+,.)$ αποτελεί δακτύλιο.

1. Προφανώς, $\pi(xy)=xy+H=(x+H)\cdot(y+H)=\pi(x)\cdot\pi(y)$.
   Τα υπόλοιπα μας τα εξασφαλίζει το Θεώρημα 6.5.1.
2. Έπεται από την Πρόταση 8.3.2.
3. Έπεται από την Πρόταση 8.3.2.
4. Μας το εξασφαλίζει το Θεώρημα 6.5.1.

□

Ο δακτύλιος S/H λέγεται ο **δακτύλιος πηλίκο** του S **modulo** H.

Θεώρημα 8.3.5 *Έστω F ένα σώμα και $f(x)$ ένα πολυώνυμο του $F[x]$ με $deg(f(x))=n>0$. Τότε*

1. *κάθε μέλος του* $F[x]/\langle f(x)\rangle$ *γράφεται με μοναδικό τρόπο στη μορφή* $r(x)+\langle f(x)\rangle$, *όπου* $r(x)\in F[x]$ *με* $degr(x)<n$, *και*

2. *όταν το* $f(x)$ *ένα ανάγωγο, ο δακτύλιος πηλίκο* $F[x]/\langle f(x)\rangle$ *είναι σώμα.*

*Απόδειξη:*8.3.5 Θέτουμε $H=\langle f(x)\rangle$.

1. Θεωρούμε τυχαίο στοιχείο $g(x)+H$ του $F[x]/H$. Από τον αλγόριθμο διαίρεσης, δηλαδή, το Θεώρημα 7.3.2, υπάρχουν $q(x), r(x)\in F[x]$ τέτοια ώστε

$$g(x)=q(x)f(x)+r(x) \text{ και } deg(r(x))<deg(f(x))=n.$$

   Συνεπώς,

$$g(x)+H=(q(x)f(x)+H)+(r(x)+H)=(0+H)+(r(x)+H)=r(x)+H.$$

   Τώρα, αν $g(x)+H=r_1(x)+H=r_2(x)+H$ με $degr_1(x)<n$ και $degr_2(x)<n$, τότε το $r_1(x)-r_2(x)$ είναι ένα πολλαπλάσιο του $f(x)$ με $deg<n$. Αυτό συνεπάγεται ότι $r_1(x)-r_2(x)=0$, άρα $r_1(x)=r_2(x)$.

2. Έστω ότι το $f(x)$ ένα ανάγωγο. Θεωρούμε μη μηδενικό στοιχείο $g(x)+H$ του $F[x]/H$. Από το (1), $g(x)+H=r(x)+H$, όπου $degr(x)<n$ και, βέβαια, $r(x)\neq 0$. Οι μόνοι διαιρέτες του $f(x)$ που έχουν βαθμό $<n$ είναι τα σταθερά πολυώνυμα. Έπεται ότι το 1 είναι ένας μέγιστος κοινός διαιρέτης των $r(x)$ και $f(x)$. Από τον Ευκλείδειο αλγόριθμο, για κάποια $s(x), t(x)\in F[x]$, $1=s(x)r(x)+t(x)f(x)$. Έτσι

$$1+H=(s(x)r(x)+H)+0=(s(x)+H)(r(x)+H)=(s(x)+H)(g(x)+H).$$

   Γνωρίζοντας ήδη από το Θεώρημα 8.3.4 ότι ο $F[x]/H$ είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο το $1+H$, συμπεραίνουμε ότι το $s(x)+H$ αποτελεί αντίστροφο για το $g(x)+H$. Συνεπώς, το $F[x]/H$ είναι σώμα.

□

Πόρισμα 8.3.6 *Έστω* p *ένας πρώτος αριθμός και* $f(x)$ *ένα ανάγωγο πολυώνυμο του* $\mathbb{Z}_p[x]$ *με* $deg(f(x))=n>0$. *Τότε ο δακτύλιος πηλίκο* $F[x]/\langle f(x)\rangle$ *είναι ένα σώμα που περιέχει* p^n *στοιχεία.*

*Απόδειξη:*8.3.6 Υπάρχουν p^n πολυώνυμα της μορφής

$$r(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1},$$

όπου $a_0, a_1, \ldots, a_{n-1}\in\mathbb{Z}_p$, και κάθε στοιχείο του $F[x]/\langle f(x)\rangle$ αντιστοιχεί σε ακριβώς ένα τέτοιο πολυώνυμο. □

8.4 Ασκήσεις

Άσκηση 8.4.1 *Έστω $f(x) = x^3 + x^2 + x + 1$ και F ένα σώμα. Εξετάστε αν το πηλίκο $F[x]/\langle f(x)\rangle$ είναι σώμα.*

Λύση 8.4.2 *Επειδή $f(x) = (x+1)(x^2+1)$, στο $F[x]/\langle f(x)\rangle$, έχουμε ότι $(x+1) + \langle f(x)\rangle \neq 0$ και $(x^2+1) + \langle f(x)\rangle \neq 0$, ενώ το γινόμενο τους*
$((x+1) + \langle f(x)\rangle)((x^2+1) + \langle f(x)\rangle) = f(x) + \langle f(x)\rangle = 0$.
Άρα, το $F[x]/\langle f(x)\rangle$ δεν είναι σώμα.

Άσκηση 8.4.3 *Κάνετε τους πίνακες πρόσθεσης και πολλαπλασιασμού για τον δακτύλιο $\mathbb{Z}_2[x]/\langle f(x)\rangle$, όπου $f(x) = x^2 + x + 1$.*

1. *Αναγνωρίστε την ομάδα $(Z_2[x]/\langle f(x)\rangle, +)$.*
2. *Δείξτε ότι ο $Z_2[x]/\langle f(x)\rangle$ είναι σώμα, χωρίς τη βοήθεια του Θεωρήματος 8.3.5.*
3. *Βρείτε όλες τις ρίζες του $x^2 + x + 1$ στο $Z_2[x]/\langle f(x)\rangle$.*

Λύση 8.4.4 *Τα στοιχεία του $\mathbb{Z}_2[x]/\langle f(x)\rangle$ είναι τα εξής:*
0, $1 = 1 + \langle f(x)\rangle$, $\alpha = x + \langle f(x)\rangle$ και $\beta = (1+x) + \langle f(x)\rangle$.
Για τον πίνακα πρόσθεσης, προσέξτε ότι $s + s = 0$ για κάθε στοιχείο s.
Για τον πίνακα πολλαπλασιασμού, απλά προσέξτε ότι $\alpha\beta = -1 = 1$.

1. *Η ομάδα $(Z_2[x]/\langle f(x)\rangle, +)$ είναι ισόμορφη με την 4-ομάδα του Klein.*
2. *Κάθε μη μηδενικό στοιχείο είναι προφανώς αντιστρέψιμο, και ο μεταθετικός δακτύλιος $Z_2[x]/\langle f(x)\rangle$ είναι σώμα.*
3. *Εύκολα επαληθεύεται ότι οι ρίζες του $x^2 + x + 1$ στο $Z_2[x]/\langle f(x)\rangle$ είναι οι α και β.*

Άσκηση 8.4.5
1. *Δείξτε ότι ο δακτύλιος $\mathbb{Z}_2[x]/\langle f(x)\rangle$, όπου $f(x) = x^3 + x^2 + 1$, είναι σώμα. Δώστε όλα τα στοιχεία του και αναγνωρίστε την ομάδα των μονάδων του.*
2. *Βρείτε την τιμή του f στα σημεία $\alpha = x + \langle f(x)\rangle, \beta = (1+x) + \langle f(x)\rangle$ και $\gamma = x^2 + \langle f(x)\rangle$ του $\mathbb{Z}_2[x]/\langle f(x)\rangle$.*
3. *Βρείτε όλες τις ρίζες του $f(x)$ στο $\mathbb{Z}_2[x]/\langle f(x)\rangle$.*

Λύση 8.4.6
1. *Επειδή $f(0) = 1 = f(1)$, το τρίτου βαθμού πολυώνυμο $f(x) = x^3 + x^2 + 1$ δεν έχει ρίζες στο $\mathbb{Z}_2$. Άρα είναι ανάγωγο. Από το Θεώρημα 8.3.5, το $\mathbb{Z}_2[x]/\langle f(x)\rangle$ είναι σώμα, και τα στοιχεία του είναι τα εξής:*
$0 = 0 + \langle f(x)\rangle$, $1 = 1 + \langle f(x)\rangle$, $\alpha = x + \langle f(x)\rangle$,
$\beta = (1+x) + \langle f(x)\rangle$, $\gamma = x^2 + \langle f(x)\rangle$, $\delta = 1 + x^2 + \langle f(x)\rangle$, $\epsilon = x + x^2 + \langle f(x)\rangle$,
και $\zeta = 1 + x + x^2 + \langle f(x)\rangle$.
Η ομάδα των μονάδων του αποτελείται από 7 στοιχεία και είναι, συνεπώς, ισόμορφη με την $\mathbb{Z}_7$.

2. $f(\alpha) = (x^3 + x^2 + 1) + \langle f(x)\rangle = 0$,
$f(\beta) = f(\alpha + 1) = (\alpha^3 + 3\alpha^2 + 3\alpha + 1) + (\alpha^2 + 2\alpha + 1) + 1 =$
$(\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^2 + 1) + 1 = (\alpha^3 + \alpha^2 + 1) + (\alpha^2 + \alpha) = \epsilon$.
$f(\gamma) = f(\alpha^2) = \alpha^6 + \alpha^4 + 1 = (\alpha^3 + \alpha^2 + 1)^2 = 0$.

3. *Δύο λύσεις είναι οι* α *και* γ. *Αν* s *είναι η τρίτη λύση, τότε*

$$x^3 + x^2 + 1 = (x - \alpha)(x - \gamma)(x - s).$$

Έπεται ότι ο συντελεστής δευτέρου βαθμού του $x^3 + x^2 + 1$, *δηλαδή, το* 1 *ισούται με* $-\alpha - \gamma - s$. *Άρα,*

$$s = -s = 1 + \alpha + \gamma = (1 + x + x^2) + \langle f(x)\rangle = \zeta.$$

Άσκηση 8.4.7 1. *Δείξτε ότι ο δακτύλιος* $\mathbb{Z}_3[x]/\langle f(x)\rangle$, *όπου* $f(x) = x^2 + 1$, *είναι σώμα.*

2. *Αναγνωρίστε την ομάδα των μονάδων του* $\mathbb{Z}_3[x]/\langle f(x)\rangle$.

3. *Βρείτε το αντίστροφο κάθε μη μηδενικού στοιχείου του* $\mathbb{Z}_3[x]/\langle f(x)\rangle$.

4. *Βρείτε όλες τις ρίζες του* $g(x) = x^4 + 2$ *στο* $\mathbb{Z}_3[x]/\langle f(x)\rangle$.

Λύση 8.4.8 1. *Το βαθμού δύο πολυώνυμο* $f(x) = x^2 + 1$ *είναι ανάγωγο πάνω από το* $\mathbb{Z}_3$ *γιατί δεν έχει ρίζες στο* $\mathbb{Z}_3$.
Από το Θεώρημα 8.3.5, ο δακτύλιος $\mathbb{Z}_3[x]/\langle f(x)\rangle$ *είναι σώμα και τα στοιχεία του είναι τα* 0, 1, $2 = 2 + \langle f(x)\rangle$, $\alpha = x + \langle f(x)\rangle, 2\alpha = 2x + \langle f(x)\rangle$, $\alpha + 1 = (1 + x) + \langle f(x)\rangle$, $\alpha + 2 = (2 + x) + \langle f(x)\rangle$, $2\alpha + 1 = (1 + 2x) + \langle f(x)\rangle$ *και* $2\alpha + 2 = (2 + 2x) + \langle f(x)\rangle$.

2. *Η ομάδα των μονάδων του* $\mathbb{Z}_3[x]/\langle f(x)\rangle$ *έχει τάξη* 8. *Το* $\alpha + 2$ *είναι ένας γεννήτοράς της γιατί* $(\alpha + 2)^2 = \alpha$ *και το* α *έχει τάξη* 4. *Άρα, είναι ισόμορφη με την* $\mathbb{Z}_8$.

3. *Προφανώς,* $1' = 1$ *και* $2' = 2$. *Από την παρατήρηση ότι* $\alpha\alpha = -1$, *έπεται ότι* $\alpha 2\alpha = -2 = 1$ *και, επομένως,* $\alpha' = 2\alpha$. *Ομοίως,* $(\alpha + 1)' = \alpha + 2$ *και* $(2\alpha + 1)' = 2\alpha + 2$.

4. *Επειδή* $g(x) = x^4 + 2 = x^4 - 1 = (x^2 - 1)(x^2 + 1)$, *οι ρίζες της είναι οι* $1, 2 = -1, \alpha$ *και* $-\alpha = 2\alpha$.

Άσκηση 8.4.9 *Βρείτε ένα σώμα με* 27 *στοιχεία.*

Λύση 8.4.10 *Το* $f(x) = x^3 + 2x + 1$ *είναι ανάγωγο πάνω από το* $\mathbb{Z}_3$, *γιατί είναι τρίτου βαθμού και δεν έχει ρίζες στο* $\mathbb{Z}_3$. *Από το Πόρισμα 8.3.6, το* $\mathbb{Z}_3[x]/\langle f(x)\rangle$ *είναι ένα σώμα με* $3^3 = 27$ *στοιχεία.*

Άσκηση 8.4.11 *Βρείτε ένα σώμα με* 125 *στοιχεία.*

Λύση 8.4.12 *Το* $f(x) = x^3 + 2x + 1$ *είναι ανάγωγο πάνω από το* $\mathbb{Z}_5$, *γιατί είναι τρίτου βαθμού και δεν έχει ρίζες στο* $\mathbb{Z}_5$. *Από το Πόρισμα 8.3.6, το* $\mathbb{Z}_5[x]/\langle f(x)\rangle$ *είναι ένα σώμα με* $5^3 = 125$ *στοιχεία.*