# Βασική Άλγεβρα

**Τμήμα Μαθηματικών**
**Πανεπιστήμιο Αθηνών**
**Αθήνα – 2013**

# Περιεχόμενα

# Κεφάλαιο 1

# Ακέραιοι

## 1.1 Διαιρετότητα

Θα συμβολίζουμε με

$$\mathbb{N} = \{0, 1, 2, \cdots\}$$

το σύνολο των φυσικών αριθμών, με

$$\mathbb{Z} = \{\cdots, -1, 0, 1, \cdots\}$$

το σύνολο των ακεραίων αριθμών, με

$$\mathbb{Z}_{>0} = \{m \in \mathbb{Z} : m > 0\}$$

το σύνολο των θετικών ακεραίων αριθμών, με

$$\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\}$$

το σύνολο των ρητών αριθμών και με

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$$

το σύνολο των μιγαδικών αριθμών.

**Θεώρημα 1.1.1.** *(Αξίωμα Ελαχίστου) Κάθε μη-κενό υποσύνολο του $\mathbb{N}$ έχει ελάχιστο στοιχείο.*

**Ορισμός 1.1.2.** *Έστω $a, b \in \mathbb{Z}$. Αν υπάρχει $c \in \mathbb{C}$ ώστε $b = ac$, τότε θα λέμε ότι το $a$ διαιρεί το $b$ (ή ότι το $a$ είναι διαιρέτης του $b$). Συμβολισμός: $a|b$.*

**Παρατήρηση 1.1.3.** *$a|0$, για κάθε $a \in \mathbb{Z}$. Ειδικότερα $0|0$.*

**Λήμμα 1.1.4.** (i) *Αν $a|b$ και $b|c$, τότε $a|c$.*

(ii) *Αν $a|b$ και $a|c$, τότε $a|xb+yc$ για κάθε $x, y \in \mathbb{Z}$.*

(iii) *Αν $a|b$ και $b|a$, τότε $a = \pm b$.*

*Απόδειξη.* Ας αποδείξουμε το (iii). Αφού $a|b$ και $b|a$ υπάρχουν $c, d \in \mathbb{Z}$ ώστε $b = ac$ και $a = bd$. Επομένως

$$b = bdc. \tag{1.1.1}$$

Παρατηρήστε ότι αν $b = 0$ τότε από την $b|a$, έπεται $a = 0$. Αν $b \neq 0$ τότε από την (1.1.1) έχουμε $1 = dc$, δηλαδή $d = \pm 1$. Επομένως $a = \pm b$. □

**Ορισμός 1.1.5.** *Ένας ακέραιος $p > 1$ λέγεται πρώτος, αν οι μόνοι διαιρέτες του είναι οι $\pm 1$ και $\pm p$.*

**Παράδειγμα 1.1.6.** *Οι αριθμοί $2, 3, 5, 7 \ldots$ είναι πρώτοι.*

**Πρόταση 1.1.7.** *Κάθε ακέραιος $\alpha > 1$ είναι γινόμενο πρώτων.*
*Σημείωση. Στην παραπάνω πρόταση θεωρούμε και την περίπτωση όπου ο $\alpha$ είναι πρώτος.*

*Απόδειξη.* Υποθέτουμε ότι η πρόταση δεν ισχύει. Έστω $M$ το σύνολο των $\alpha > 1$ που δεν γράφονται ως γινόμενο πρώτων. Τότε $M \neq 0$. Από το Αξίωμα Ελαχίστου υπάρχει ελάχιστο στοιχείο στο $M$, έστω $m$ . Παρατηρήστε ότι αφού ο $m$ δεν είναι πρώτος, υπάρχουν $c, d$ με $1 < c < m$ και $1 < d < m$. Επομένως λόγω του ορισμού του $m$ έπεται ότι οι $c, d$ δεν ανήκουν στο $M$. Όμως $c, d > 1$. Άρα καθένας από τους $c, d$ είναι γινόμενο πρώτων. Δηλαδή $m = cd$ είναι γινόμενο πρώτων. Άτοπο αφού $m \in M$. □

**Θεώρημα 1.1.8.** *(Ευκλείδη) Υπάρχουν άπειροι πρώτοι αριθμοί.*

*Απόδειξη.* Ας υποθέσουμε ότι το σύνολο των πρώτων είναι πεπερασμένο και ίσο με

$$\{p_1, \cdots, p_\kappa\}.$$

Θέτουμε

$$N = p_1 p_2 \cdots p_\kappa + 1.$$

Τότε $N > 1$ και από την πρόταση (1.1.7), έπεται ότι $p_i|N$ για κάποιο $i \in \{1, 2, \cdots, \kappa\}$. Παρατηρήστε ότι $p_i|p_1 p_2 \cdots p_\kappa$, άρα

$$p_i|N - p_1 p_2 \cdots p_\kappa.$$

Επομένως $p_i|1$, άτοπο. □

**Θεώρημα 1.1.9.** *(Αλγόριθμος Ευκλείδη ή Ευκλείδεια διαίρεση). Έστω $a, b \in \mathbb{Z}$ με $a > 0$. Τότε υπάρχουν μοναδικοί $q, r \in \mathbb{Z}$ ώστε*

$$b = qa + r, \qquad 0 \leqslant r < a.$$

**Ορισμός 1.1.10.** *Το $r$ στο παραπάνω θεώρημα λέγεται υπόλοιπο της διαίρεσης του $b$ με το $a$.*

*Για παράδειγμα έχουμε $44 = 7 \cdot 6 + 2$ (το υπόλοιπο είναι 2).*

*Απόδειξη του θεωρήματος 1.1.9.* Έστω

$$M = \{b - ta : t \in \mathbb{Z}\}.$$

Το $M$ είναι μη κενό υποσύνολο του $\mathbb{N}$, επομένως από το Αξίωμα Ελαχίστου έχει ελάχιστο στοιχείο, έστω $r$. Παρατηρήστε ότι $b - aq = r$, $r \in M$. Άρα $r \geqslant 0$. Έστω $r \geqslant a$. Τότε

$$b - aq \geqslant a \qquad \text{ή} \qquad b - (q+1)a \geqslant 0 \qquad \text{ή} \qquad b - (q+1)a \in M.$$

Από τον ορισμό του $r$ έχουμε,

$$b - (q+1)a \geqslant r,$$

δηλαδή

$$r - a \geqslant r.$$

Άτοπο, επομένως $r < a$.

Μοναδικότητα. Έστω

$$b = qa + r, \qquad 0 \leqslant r < a$$

και

$$b_1 = q_1 a + r_1, \qquad 0 \leqslant r_1 < a,$$

όπου $q, r, q_1, r_1 \in \mathbb{Z}$. Τότε,

$$(q - q_1)a = r_1 - r \qquad \text{και} \qquad -a < r_1 - r < a.$$

Επομένως

$$-a < (q - q_1)a < a.$$

Επειδή $a > 0$, έπεται

$$-1 < q_1 - q < 1, \qquad \text{με} \qquad q - q_1 \in \mathbb{Z}.$$

Άρα $q - q_1 = 0$ ή $q = q_1$ και $r = r_1$. □

**Παρατήρηση 1.1.11.** *Έστω $a, b \in \mathbb{Z}$ με $a > 0$. Τότε υπάρχουν μοναδικοί $q, r \in \mathbb{Z}$ ώστε*

$$b = qa + r, \qquad 0 \leqslant r < |a|.$$

**Θεώρημα 1.1.12.** *Έστω $a, b \in \mathbb{Z}$ όχι και οι δύο μηδέν. Τότε υπάρχει μοναδικός μκδ των $a$ και $b$ (συμβολίζουμε $d = \text{μκδ}(a, b)$). Επίσης υπάρχουν $x, y \in \mathbb{Z}$ ώστε $d = ax + by$.*

*Απόδειξη.* Έστω

$$M = \{ax + by > 0 : x, y \in \mathbb{Z}\}.$$

Το $M$ είναι μη κενό ($a^2 + b^2 > 0$) υποσύνολο του $\mathbb{N}$, άρα από το Αξίωμα Ελαχίστου έχει ελάχιστο στοιχείο, έστω $d$. Τότε

$$d = ax + by, \qquad x, y \in \mathbb{Z}.$$

Ισχυρισμός 1. $d|a$ και $d|b$.

Από την ευκλείδεια διαίρεση υπάρχουν $q, r \in \mathbb{Z}$ ώστε

$$a = qd + r, \qquad 0 \leqslant r < d.$$

Παρατηρήστε ότι

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy).$$

Έστω $r \neq 0$, τότε $r \in M$ (ως γραμμικός συνδυασμός των $a$ και $b$) Τότε έχουμε $r \geqslant d$ (γιατί το $d$ ήταν το ελάχιστο). Άτοπο, αφού $0 \leqslant r < d$. Επομένως $r = 0$, άρα $a = qd$, δηλαδή $d|a$. Ομοίως δείχνουμε ότι $d|b$.

Ισχυρισμός 2. Αν $c|a$ και $c|b$, τότε $c|d$.

Πράγματι αφού $c|a$ και $c|b$, έπεται ότι $c|ax+by = d$. Από τους δύο παραπάνω ισχυρισμούς παίρνουμε ότι το $d$ είναι μκδ των $a$ και $b$.

Μοναδικότητα. Έστω $d, d_1$ δύο μκδ των $a$ και $b$. Τότε $d|a$, $d|b$. Αφού $d_1$ είναι μκδ των $a$ και $b$, έπεται ότι $d|d_1$. Ομοίως έχουμε $d_1|d$ (αφού $d_1|a$, $d_1|b$), άρα $d = d_1$ ( αφού $d, d_1 > 0$) □

**Λήμμα 1.1.13.** *(Ευκλείδη.) Έστω $p$ πρώτος και $a, b \in \mathbb{Z}$. Αν $p|ab$, τότε $p|a$ ή $p|b$.*

*Απόδειξη.* Έστω ότι ο $p$ δεν διαιρεί τον $a$. Τότε επειδή ο $p$ είναι πρώτος, έχουμε

$$d = \text{μκδ}(p, a).$$

Από το θεώρημα 1.1.12 υπάρχουν $x, y \in \mathbb{Z}$ ώστε

$$1 = px + ay.$$

Επομένως

$$b = bpx + aby.$$

Επειδή $p|bpx$ και $p|aby$, έπεται $p|b$. □

**Θεώρημα 1.1.14.** *(Θεμελιώδες Θεώρημα Αριθμητικής). Έστω $a \in \mathbb{Z}, a > 1$. Τότε υπάρχουν μοναδικοί πρώτοι $p_1, \cdots p_m$ ώστε*

$$a = p_1 p_2 \cdots p_m$$

*(χωρίς να λαμβάνεται υπόψιν η σειρά).*

*Απόδειξη.* Η ύπαρξη έχει ελεγθεί (πρόταση 1.1.7).

Μοναδικότητα. Έστω $p_1, \ldots, p_m, q_1, \ldots, q_n$ πρώτοι με

$$a = p_1 p_2 \cdots p_m = q_1 \cdots q_n.$$

Υποθέτουμε ότι $m \leqslant n$ και εφαρμόζουμε επαγωγή στο $m$.

Για $m = 1$ έχουμε

$$p_1 = q_1 q_2 \cdots q_n,$$

οπότε ο $p_1$ θα διαιρεί κάποιον από τους $q_j$, έστω τον $q_1$. Επειδή ο $q_1$ είναι πρώτος και $q_1 > 1$, παίρνουμε $p_1 = q_1$. Επομένως

$$1 = q_2 \cdots q_n.$$

Άρα $n = 1$.

Έστω $m > 1$. Από την

$$p_1 \cdots p_m = q_1 \cdots q_n,$$

παίρνουμε όπως πριν

$$p_2 \cdots p_m = q_2 \cdots q_n.$$

Από την επαγωγική υπόθεση έπεται ότι $m - 1 = n - 1$ και τα $q_2, \ldots, q_n$ είναι αναδιάταξη των $p_2, \ldots p_n$. □

**Παρατηρήσεις 1.1.15.** (i) *Το θεώρημα 1.1.14 μας λέει ότι κάθε $a \in \mathbb{Z}, a \neq 0, \pm 1$ γράφεται μοναδικά στην μορφή*

$$a = \pm 1 \cdot p_1^{a_1} \cdots p_m^{a_m},$$

*όπου οι $p_i$ είναι ανά δύο διαφορετικοί πρώτοι αριθμοί και οι $a_i$ είναι θετικοί αριθμοί.*

(ii) *Αν $a, b \in \mathbb{Z}$ $(a, b > 0)$ τότε μπορούμε να γράψουμε*

$$a = \pm p_1^{a_1} \cdots p_m^{a_m}$$

*και*

$$b = \pm p_1^{b_1} \cdots p_m^{b_m},$$

*όπου οι $p_i$ είναι ανά δύο διαφορετικοί πρώτοι αριθμοί και οι $a_i$ είναι θετικοί αριθμοί.*

*Σημείωση.* Με τον Ευκλείδειο αλγόριθμο μπορούμε να

(i) υπολογίσουμε τον μκδ$(a, b)$, με $a, b \in \mathbb{Z}$,

(ii) να υπολογίσουμε $x, y \in \mathbb{Z}$ με μκδ$(a, b) = ax + by$.

**Παρατηρήσεις 1.1.16.** (i) *Αν $b = aq + r$, τότε $\mu\kappa\delta(a, b) = \mu\kappa\delta(r, a)$.*

*Πράγματι, αφού $\mu\kappa\delta(a, b)|a$ και $\mu\kappa\delta(a, b) = b$, παίρνουμε $\mu\kappa\delta(a, b)|r$. Δηλαδή $\mu\kappa\delta(a, b)|a$ και $\mu\kappa\delta(a, b)|r$, άρα $\mu\kappa\delta(a, b)|\mu\kappa\delta(r, a)$. Ομοίως έχουμε $\mu\kappa\delta(r, a)|\mu\kappa\delta(a, b)$. Επομένως $\mu\kappa\delta(a, b) = \mu\kappa\delta(r, a)$.*

(ii) *Έστω $a > 0$. Από τον αλγόριθμο της Ευκλείδειας διαίρεσης παίρνουμε διαδοχικά,*

$$\begin{aligned} b &= aq + r, & 0 \leqslant r < a \\ a &= rq_1 + r_1, & 0 \leqslant r_1 < r \\ r &= r_1q_2 + r_2, & 0 \leqslant r_2 < r_1 \\ &\vdots \\ r_{n-2} &= r_{n-1} \cdot q_n + r_n, & 0 \leqslant r_n < r_{n-1} \\ r_{n-1} &= r_n \cdot q_{n+1} + 0. \end{aligned}$$

*Εφαρμόζοντας το (i) έχουμε ότι*

$$\mu\kappa\delta(a, b) = \mu\kappa\delta(r, a) = \mu\kappa\delta(r, r_1) = \cdots \mu\kappa\delta(r_n, 0) = r_n,$$

*το οποίο είναι το τελευταίο μη μηδενικό υπόλοιπο.*

(iii) *Έχουμε μια γνησίως φθίνουσα ακολουθία φυσικών αριθμών ώστε*

$$a > r > r_1 > r_2 > \cdots$$

*Επομένως μετά από πεπερασμένο πλήθος βημαάτων θα βρούμε $r_{n+1} = 0$.*

**Παράδειγμα 1.1.17.** *Έστω $a = 65$ και $b = 418$. Από τον αλγόριθμο της Ευκλείδειας διαίρεσης έχουμε,*

$$\begin{aligned} 418 &= 2 \cdot 165 + 88 \\ 165 &= 1 \cdot 88 + 77 \\ 88 &= 1 \cdot 77 + 11 \\ 77 &= 7 \cdot 11 + 0. \end{aligned}$$

*Τώρα θα βρούμε $x, y \in \mathbb{Z}$ ώστε*

$$11 = 165x + 418y.$$

*Έχουμε,*

$$\begin{aligned} 11 &= 88 - 1 \cdot 77 = 88 - 1(165 - 1 \cdot 88) \\ &= 2 \cdot 88 - 1 \cdot 165 = 2(418 - 2 \cdot 165) - 1 \cdot 165 \\ &= 165(-5) + 418 \cdot 2. \end{aligned}$$

*Δηλαδή ένα ζεύγος $(x, y)$ είναι το $(-5, 2)$.*

**Παρατήρηση 1.1.18.** *Τα $x, y$ δεν είναι μοναδικά.*

$$d = a(x - tb) + b(y + ta),\ t \in \mathbb{Z}.$$

### Ασκήσεις

**1**. Έστω

$$\alpha = p_1^{\alpha_1} \cdots p_\kappa^{\alpha_\kappa}$$

και

$$\beta = p_1^{\beta_1} \cdots p_\kappa^{\beta_\kappa},$$

όπου $p_i$ πρώτοι με $p_i \neq p_j$ για κάθε $i \neq j$ και $\alpha_i, \beta_i \in \mathbb{N}$. Να δείξετε ότι $\alpha|\beta$ αν και μόνο αν $\alpha_i \leqslant \beta_i$ για κάθε $i$.

*Απόδειξη.* Έστω $\alpha|\beta$. Τότε υπάρχει $\gamma \in \mathbb{Z}$ ώστε $\beta = \alpha\gamma$. Έστω

$$\gamma = p_1^{\gamma_1} \cdots p_\kappa^{\gamma_\kappa} \in \mathbb{N}.$$

Τότε

$$p_1^{\beta_1} \cdots p_\kappa^{\beta_\kappa} = p_1^{\alpha_1+\gamma_1} \cdots p_\kappa^{\alpha_\kappa+\gamma_\kappa}.$$

Από την μοναδικότητα στο θεμελιώδες θεώρημα της Αριθμητικής, έχουμε $\beta_i = \alpha_i + \gamma_i$ για κάθε $i$, άρα $\alpha_i \leqslant \beta_i$.

Αντίστροφα, έστω $\alpha_i \leqslant \beta_i$ για κάθε $i$. Θέτουμε

$$\gamma = p_1^{\gamma_1} \cdots p_\kappa^{\gamma_\kappa},$$

όπου $\gamma_i = \beta_i - \alpha_i \in \mathbb{N}$. Τότε $\beta = \alpha\gamma$ και $\alpha|\beta$. □

**2**. Θεωρούμε τους συμβολισμούς της άσκησης 1. Να δείξετε ότι

$$\text{μκδ}(\alpha, \beta) = p_1^{\delta_1} \cdots p_\kappa^{\delta_\kappa},$$

όπου $\delta_i = \min\{\alpha_i, \beta_i\}$ για κάθε $i$.

*Απόδειξη.* Έπεται άμεσα από την άσκηση 1 και από τον ορισμό του ΜΚΔ. □

**3**. Να δείξετε ότι $\sqrt{2} \notin \mathbb{Q}$.

*Απόδειξη.* Υποθέτουμε ότι $\sqrt{2} \in \mathbb{Q}$ και έστω $\sqrt{2} = \frac{m}{n}$, με $m, n \in \mathbb{Z}, n \neq 0$. Μπορούμε να υποθέσουμε ότι μκδ$(m, n) = 1$ (αν όχι απλοποιούμε το κλάσμα). Έστω ότι υπάρχει $p$ πρώτος με $p|n$. Επειδή $m^2 = 2n^2$ και $p|n$, έχουμε $p|m^2$. Αφού ο $p$ είναι πρώτος, έπεται ότι $p|m$. Δηλαδή $p|m$ και $p|n$, άρα $p|$μκδ$(m, n)$. Επομένως $p|1$, το οποίο είναι άτοπο. Άρα $n = \pm 1$. Τότε $\sqrt{2} = \pm m \in \mathbb{Z}$, που είναι άτοπο. □

**4**. Έστω $a, b, c \in \mathbb{Z}$ με μκδ$(a, b) = 1$. Να δείξετε ότι ισχύουν τα ακόλουθα.

(i) Αν $a|bc$, τότε $a|c$.

(ii) Αν $a|c$ και $b|c$, τότε $ab|c$.

*Απόδειξη.* (i). Αφού μκδ$(a,b)=1$, υπάρχουν $x,y\in\mathbb{Z}$ ώστε

$$1=ax+by,$$

άρα

$$c=acx+bxy.$$

Παρατηρήστε ότι $a|acx$ και $a|bc$. Επομένως,

$$a|acx+bcy=c.$$

(ii). Αφού $a|c$ και $b|c$, έχουμε $ab|acx$ και $ab|bcy$. Επομένως,

$$ab|acx+bcy=c.$$

□

**5**. Έστω $a,b,c\in\mathbb{Z}_{>0}$ με $a^3|b^7$. Να δείξετε ότι $a|b^3$.

*Απόδειξη.* Έστω

$$a=p_1^{a_1}\cdots p_\kappa^{a_\kappa}$$

και

$$b=p_1^{b_1}\cdots p_\kappa^{b_\kappa},$$

όπου $p_i$ πρώτοι με $p_i\neq p_j$ για κάθε $i\neq j$ και $a_i,b_i\in\mathbb{N}$. Άρα

$$a^3=p_1^{3a_1}\cdots p_\kappa^{3a_\kappa}$$

και

$$b^7=p_1^{7b_1}\cdots p_\kappa^{7b_\kappa}.$$

Αφού $a^3|b^7$ από την άσκηση 1, έπεται ότι $3a_i\leqslant 7b_i$. Επομένως

$$a_i\leqslant\frac{7}{3}b_i\leqslant b_i,$$

για κάθε $i$. Πάλι από την άσκηση 1 παίρνουμε ότι $a|b^3$. □

**6**. Να δείξετε ότι αν μκδ$(m,n)=1$, τότε μκδ$(m+n,mn)=1$.

*Απόδειξη.* Υποθέτουμε ότι υπάρχει $p$ πρώτος με $p|$μκδ$(m+n,mn)$. Τότε

$$p|m+n$$

και

$$p|mn. \tag{1.1.2}$$

Επειδή ο $p$ είναι πρώτος από την (1.1.2) έπεται ότι

$$p|m \qquad \text{ή} \qquad p|n.$$

Έστω ότι $p|m$ και $p|m+n$, άρα $p|n$. Επομένως $p|m$ και $p|n$, άρα

$$p|\text{μκδ}(m,n) = 1,$$

το οποίο είναι άτοπο. Ομοίως αν $p|n$ καταλήγουμε σε άτοπο, οπότε $\text{μκδ}(m+n, mn) = 1$. □

**7**. Να δείξετε ότι υπάρχει μοναδική τριάδα της μορφής $(p, p+2, p+4)$, όπου $p, p+2, p+4$ είναι πρώτοι.

*Απόδειξη.* Παρατηρήστε ότι για $p = 3$ έχουμε την τριάδα $(3, 5, 7)$. Έστω $p > 3$, $p$ πρώτος. Από τον αλγόριθμο της Ευκλείδειας διαίρεσης έχουμε $p = 3q$ ή $p = 3q+1$ ή $p = 3q+2$, με $q \in \mathbb{N}$. Όμως $p \neq 3q$, αφού $p \neq 3$ .

Έστω $p = 3q+1$. Τότε

$$p + 2 = 3q + 1 + 2 = 3(q+1),$$

ο οποίος δεν είναι πρώτος.

Έστω $p = 3q+2$. Τότε

$$p + 4 = 3q + 2 + 4 = 3(q+2),$$

ο οποίος δεν είναι πρώτος. □

**8**. Να βρείτε τον $\text{μκδ}(3n+1, 10n+3)$, για κάθε $n \in \mathbb{N}$.

*Λύση.* Έχουμε

$$\begin{aligned} 10n+3 &= 3(3n+1)+n \\ 3n+1 &= 3\cdot n+1 \\ n &= 1\cdot n+0. \end{aligned}$$

Επομένως $\text{μκδ}(3n+1, 10n+3) = 1$. □

**9**. Έστω $a, b, n \in \mathbb{Z}_{>0}$, με $n > 1$. Τότε,

$$\text{μκδ}(n^a - 1, n^b - 1) = n^d - 1,$$

όπου $d = \text{μκδ}(a, b)$.

*Απόδειξη.* Από τον αλγόριθμο της Ευκλειδειας διαίρεσης έχουμε

$$\begin{aligned} b &= aq + r, \qquad 0 \leqslant r < a \\ a &= rq_1 + r_1, \qquad 0 \leqslant r_1 < r \\ r &= r_1q_2 + r_2, \qquad 0 \leqslant r_2 < r_1 \\ &\vdots \\ r_{n-2} &= r_{n-1} \cdot q_n + r_n, \qquad 0 \leqslant r_n < r_{n-1} \\ r_{n-1} &= r_n \cdot q_{n+1} + 0. \end{aligned}$$

Θα χρειαστούμε το εξής. Έστω $b = aq + r$ και

$$Q = n^r \cdot \frac{n^{qa} - 1}{n^a - 1} = n^r(n^{a(q-1)} + \cdots n^a + 1),$$

δηλαδή $Q \in \mathbb{Z}$. Τότε,

$$n^b - 1 = Q \cdot (n^a - 1) + (n^r - 1).$$

Άρα έχουμε,

$$\begin{aligned} n^{b-1} &= Q \cdot (n^a - 1) + n^r - 1 \\ n^a - 1 &= Q_1 \cdot (n^r - 1) + n^{r_1} - 1 \\ n^r - 1 &= Q_2 \cdot (n^{r_1} - 1) + n^{r_2} - 1 \\ &\vdots \\ n^{r_{m-2}} &= Q_m \cdot (n^{r_{m-1}} - 1) + n^{r_m} - 1 \\ n^{r_{m-1}} &= Q_{m+1} \cdot (n^{r_m} - 1) + 0. \end{aligned}$$

Επομένως

$$\text{μκδ}(n^a - 1, n^b - 1) = n^{r_m} - 1,$$

όπου $r_m = \text{μκδ}(a, b)$. □

## 1.2 Ισοτιμίες

**Ορισμός 1.2.1.** *Έστω $a, b, n \in \mathbb{Z}$. Θα λέμε ότι οι $a, b$ είναι ισότιμοι modulo $n$ (ή ισουπόλοιποι modulo $n$), αν $n|a - b$. Στην περίπτωση αυτήν γράφουμε $a \equiv b \text{mod} n$.*

**Παράδειγμα 1.2.2.** (i) $13 \equiv \text{mod}5$, *αφού* $5|13 - 3$.

(ii) $13 \equiv -2\text{mod}5$, *αφού* $5|13 - (-2)$

**Παρατηρήσεις 1.2.3.** (i) *Έχουμε*

$$a \equiv b \bmod n \Leftrightarrow a \equiv b \bmod(-n).$$

*(Συνήθως έχουμε $n \geqslant 0$.)*

(ii) *Αν $n = 0$, τότε*

$$a \equiv b \bmod 0 \Leftrightarrow a = b.$$

**Πρόταση 1.2.4.** *Έστω $a, b, c, n \in \mathbb{Z}$. Τότε ισχύουν τα ακόλουθα.*

(i) $a \equiv a \bmod n$

(ii) *Αν $a \equiv b \bmod n$ τότε $b \equiv a \bmod n$*

(iii) *Αν $a \equiv b \bmod n$ και $b \equiv c \bmod n$, τότε $a \equiv c \bmod n$.*

*Σημείωση. Η ιδιότητα (ii) δικαιολογεί την έλλειψη διάταξης των $a$ και $b$ στον ορισμό.*

**Πρόταση 1.2.5.** *Έστω $a, b, n \in \mathbb{Z}, n \neq 0$. Τότε $a \equiv b \bmod n$ αν και μόνο αν οι $a$ και $b$ αφήνουν το ίδιο υπόλοιπο όταν διαιρεθούν με το $n$.*

*Απόδειξη.* Από τον αλγόριθμο της διαίρεσης υπάρχουν $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, ώστε

$$a = q_1 n + r_1, \qquad 0 \leqslant r_1 < |n|$$

και

$$b = q_2 n + r_2, \qquad 0 \leqslant r_2 < |n|$$

Επομένως

$$a - b = (q_1 - q_2) \cdot n + r_1 - r_2, \qquad \text{με} \qquad 0 \leqslant |r_1 - r_2| < |n|.$$

Άρα

$$a \equiv b \bmod n \Leftrightarrow n | a - b \Leftrightarrow n | r_1 - r_2 \Leftrightarrow r_1 - r_2 = 0 \qquad (\text{αφού } -n < (r_1 - r_2) < n)$$

Δηλαδή

$$a \equiv b \bmod n \Leftrightarrow r_1 = r_2.$$

□

**Πρόταση 1.2.6.** *Έστω $a, b, c, n \in \mathbb{Z}$. Τότε ισχύουν τα ακόλουθα.*

(i) *Αν $a \equiv b \bmod n$ και $c \equiv d \bmod n$, τότε $a + c \equiv (b + d) \bmod n$.*

(ii) *Αν $a \equiv b \bmod n$ και $c \equiv d \bmod n$, τότε $a \cdot c \equiv (b \cdot d) \bmod n$.*

(iii) *Αν $a \equiv b \bmod n$, τότε $a^\kappa \equiv b^\kappa \bmod n$, για κάθε $\kappa \in \mathbb{Z}_{>0}$.*

*Απόδειξη.* (i). Παρατηρήστε ότι

$$a \equiv b \mathrm{mod} n \qquad \Leftrightarrow \qquad n|a-b$$

και

$$c \equiv d \mathrm{mod} n \qquad \Leftrightarrow \qquad n|c-d.$$

Επομένως,

$$n|a-b+c-d \qquad \text{ή} \qquad n|a+c-(b+d).$$

Επομένως,

$$a+c \equiv (b+d) \mathrm{mod} n$$

(ii). Ομοίως έχουμε $n|a-b$ και $n|c-d$. Παρατηρήστε ότι,

$$ac-bd = ac-bc+bc-bd = (a-b)c+b(c-d).$$

Επειδή

$$n|(a-b)c+b(c-d),$$

έπεται ότι

$$n|ac-bd.$$

Επομένως

$$a \cdot c \equiv (b \cdot d) \mathrm{mod} n.$$

(iii). Έπεται άμεσα από το (ii). □

*Σημείωση.* Γενικά δεν ισχύει ότι από την

$$ac \equiv (bd) \mathrm{mod} n, \qquad c \neq 0,$$

έπεται ότι

$$a \equiv b \mathrm{mod} n.$$

Για παράδειγμα, παρατηρήστε ότι

$$5 \cdot 2 \equiv 2 \cdot 2 \mathrm{mod} 6.$$

Αλλά προφανώς δεν ισχύει ότι

$$5 = 2 \mathrm{mod} 6.$$

### Ασκήσεις

**1**. Να δείξετε ότι δεν υπάρχει ακέραιος της μορφής $4n+3, n \in \mathbb{Z}$ που να είναι άθροισμα δύο τετραγώνων ακεραίων.

*Απόδειξη.* Υποθέτουμε ότι υπάρχουν $a, n, b \in \mathbb{N}$ ώστε

$$4n+3 = a^2 + b^2.$$

Τότε

$$3 \equiv (a^2 + b^2) \mathrm{mod} 4. \tag{1.2.1}$$

Παρατηρήστε ότι

$$a = 0, 1, 2, 3 \mathrm{mod} 4 \qquad (\text{αλγόριθμος διαίρεσης}),$$

άρα

$$a^2 = 0^2, 1^2, 2^2, 3^2 \mathrm{mod} 4,$$

δηλαδή

$$a^2 = 0, 1, 0, 1 \mathrm{mod} 4.$$

Τελικά,

$$a^2 \equiv 0, 1 \mathrm{mod} 4, \qquad b^2 \equiv 0, 1 \mathrm{mod} 4.$$

Επομένως

$$a^2 + b^2 \equiv 0, 1, 2 \mathrm{mod} 4.$$

Δηλαδή σε κάθε περίπτωση δεν ισχύει ότι $a^2 + b^2 \equiv 3 \mathrm{mod} 4$, που είναι άτοπο λόγω της (1.2.1). □

**2**. Να δείξετε ότι για κάθε $n \in \mathbb{N}$

$$11 | 3^{3n} - 5^n.$$

*Απόδειξη.* Παρατηρήστε ότι,

$$3^{3n} - 5^n = (3^3)^n - 5^n = 27^n - 5^n \equiv 5^n - 5^n \mathrm{mod} 11.$$

Επομένως

$$3^{3n} - 5^n \equiv 0 \mathrm{mod} 11,$$

δηλαδή

$$11 | 3^{3n} - 5^n.$$

□

**3**. Να δείξετε ότι δεν υπάρχουν $x, y \in \mathbb{Z}$ ώστε

$$x^2 - 5y^2 = 13. \tag{1.2.2}$$

*Απόδειξη.* Δουλεύουμε με mod5 και έστω $x, y \in \mathbb{Z}$ ώστε να ικανοποιείται η (1.2.2). Τότε

$$x^2 \equiv 13 \mathrm{mod} 5,$$

δηλαδή

$$x^2 \equiv 3 \mathrm{mod} 5. \tag{1.2.3}$$

Παρατηρήστε ότι,

$$\begin{aligned} x &= 0, 1, 2, 3, 4 \mathrm{mod} 5 \Rightarrow \\ x^2 &= 0^2, 1^2, 2^2, 3^2, 4^2 \mathrm{mod} 5 \Rightarrow \\ x^2 &= 0, 1, 4, 4, 1 \mathrm{mod} 5. \end{aligned}$$

Επομένως

$$x^2 \equiv 0, 1, 4 \mathrm{mod} 4,$$

δηλαδή σε κάθε περίπτωση δεν ισχύει ότι $x^2 \equiv 3 \mathrm{mod} 5$, το οποίο είναι άτοπο λόγω της (1.2.3). □

**4**. Να δείξετε ότι κανένας ακέραιος της μορφής

$$3^m + 3^n + 1 \ (m, n \in \mathbb{N})$$

δεν είναι τετράγωνο ακεραίου.

*Απόδειξη.* Υποθέτουμε ότι

$$3^m + 3^n + 1 = x^2 \qquad (x \in \mathbb{N}). \tag{1.2.4}$$

Δουλεύουμε με mod8. Ισχυριζόμαστε ότι

$$x^2 = 0, 1, 4 \mathrm{mod} 8. \tag{1.2.5}$$

Πράγματι έχουμε,

$$\begin{aligned} x &= 0, 1, 2, 3, 4, 5, 6, 7 \mathrm{mod} 8 \Rightarrow \\ x^2 &= 0, 1, 4, 9, 16, 25, 36, 49 \mathrm{mod} 8 \Rightarrow \\ x^2 &= 0, 1, 4, 1, 0, 1, 4, 1 \mathrm{mod} 8 \Rightarrow \\ x^2 &= 0, 1, 4 \mathrm{mod} 8. \end{aligned}$$

Θα δείξουμε τώρα ότι

$$3^m \equiv 1, 3 \mathrm{mod} 8.$$

Η απόδειξη θα γίνει με επαγωγή στο $m$. Πράγματι για $m = 1$ έχουμε $3^m \equiv 1, 3 \mathrm{mod} 8$. Έχουμε,

$$3^{m+1} = 3 \cdot 3^m \equiv 3, 9 \mathrm{mod} 8.$$

Επομένως

$$3^{m+1} \equiv 1, 3 \mathrm{mod} 8.$$

Άρα

$$3^m + 3^n + 1 \equiv 1 + 1 + 1, 1 + 3 + 1, 3 + 3 + 1 \mathrm{mod} 8.$$

Δηλαδή

$$3^m + 3^n + 1 \equiv 3, 5, 7 \mathrm{mod} 8,$$

το οποίο δεν μπορεί να συμβαίνει λόγω των (1.2.4) και (1.2.5). □

**5**. Να δείξετε ότι για κάθε $n \in \mathbb{N}$

$$21 | 4^{n+2} + 5^{2n+1}.$$

*Απόδειξη*. Παρατηρήστε ότι,

$$\begin{aligned} 4^{n+2} + 5^{2n+1} &= 4^2 \cdot 4^n + 5(5^2)^n \\ &= 16 \cdot 4^n + 5(25)^n \\ &\equiv 16 \cdot 4^n + 5 \cdot 4^n \mathrm{mod} 21. \end{aligned}$$

Δηλαδή έχουμε

$$16 \cdot 4^n + 5 \cdot 4^n = 21 \cdot 4^n,$$

άρα

$$21 | 4^{n+2} + 5^{2n+1}.$$

□

**6**. Να δείξετε ότι για κάθε $n \in \mathbb{N}$

$$10^n + 3 \cdot 4^{n+2} \equiv 4 \mathrm{mod} 9.$$

*Απόδειξη*. Παρατηρήστε ότι,

$$10^n \equiv 1 \mathrm{mod} 9.$$

Αρκεί να δείξουμε ότι

$$9 | 3 \cdot 4^{n+2} - 3,$$

δηλαδή

$$3 | 4^{n+2} - 1.$$

Αλλά

$$4^{n+2} \equiv 1 \mathrm{mod} 3 \qquad (4 \equiv 1 \mathrm{mod} 3).$$

Επομένως $3 | 4^{n+2} - 1$. □

## 1.3 Οι ακέραιοι modulo $n$

### 1.3α′ Σχέσεις ισοδυναμίας

**Ορισμός 1.3.1.** *Έστω $A$ ένα μη κενό σύνολο. Μια σχέση στο $A$ είναι ένα υποσύνολο του $A \times A$. Αν $X \subset A \times A$, τότε αντί για $(a, a') \in X$ θα γράφουμε $a \sim_x a'$ ή $a \sim a'$ (αν είναι σαφές ποιο είναι το $X$).*

**Ορισμός 1.3.2.** *Έστω $A \neq 0$ και $X \subseteq A \times A$ ($X$ είναι μια σχέση στο $A$). Το $X$ λέγεται σχέση ισοδυναμίας, αν ισχύουν οι ακόλουθες ιδιότητες.*

(i) *$a \sim_x a'$ (ανακλαστική).*

(ii) *Αν $a \sim_x b$, τότε $b \sim_x a$ (συμμετρική).*

(iii) *Αν $a \sim_x b$ και $b \sim_x c$, τότε $a \sim_x c$ (μεταβατική).*

**Ορισμός 1.3.3.** *Έστω $X$ μια σχέση ισοδυναμίας στο $A$. Έστω $a \in A$. Η κλάση ισοδυναμίας του $a$ είναι το σύνολο*

$$[a] = \{x \in A : x \sim a\}.$$

*Παρατηρήστε ότι $a \in [a]$.*

**Παράδειγμα 1.3.4.** (i) *Έστω $A \neq 0$. Ορίζουμε μια σχέση στο $A$ ως εξής.*

$$a \sim b \Leftrightarrow a = b.$$

*Αυτή είναι μια σχέση ισοδυναμίας. Παρατηρήστε ότι $[a] = a$*

(ii) *Έστω $A$ το σύνολο των σημείων του επιπέδου στο $\mathbb{R}^2$. Ορίζουμε την σχέση*

$$P \sim Q \Leftrightarrow |OP| = |OQ|,$$

*όπου $P, Q$ σημεία του επιπέδου και $O$ η αρχή των αξόνων. Η $\sim$ είναι σχέση ισοδυναμίας. Παρατηρήστε ότι $[P]$ = κύκλος με ακτίνα $|OP|$ και κέντρο το $O$.*

(iii) *Έστω $A = \mathbb{Z}$ και $n \in \mathbb{Z}_{>0}$. Ορίζουμε την εξής σχέση στο $\mathbb{Z}$.*

$$a \sim b \Leftrightarrow n|a - b.$$

*Δηλαδή*

$$a \sim b \Leftrightarrow a \equiv b \bmod n.$$

*Παρατηρήστε ότι από την πρόταση 1.2.4 η παραπάνω σχέση είναι σχέση ισοδυναμίας. Για την κλάση ισοδυναμίας του $a$, την οποία συμβολίζουμε με $[a]_n$ ή $[a]$, έχουμε*

$$[a]_n = \{x \in \mathbb{Z} : x = a \bmod n\} = \{a + \kappa n,\ \kappa \in \mathbb{Z}\}.$$

($\alpha$) *Έστω* $n = 2$. *Έχουμε*

$$[0] = \{x \in \mathbb{Z} : x \sim 0\}.$$

*Αλλά*

$$x \sim 0 \Leftrightarrow x \equiv 0 \mathrm{mod} 2 \Leftrightarrow x = 2\kappa,\ \kappa \in \mathbb{Z}.$$

*Επομένως*

$$[0] = \{2\kappa : \kappa \in \mathbb{Z}\} \qquad (\textit{άρτιοι ακέραιοι}).$$

*Ομοίως βλέπουμε ότι,*

$$[1] = \{2\kappa + 1 : \kappa \in \mathbb{Z}\} \qquad (\textit{περιττοί ακέραιοι}).$$

*Επίσης* $[5] = [1]$.

($\beta$) *Έστω* $n = 3$. *Τότε,*

$$\begin{aligned} \textit{[0]} &= \{3\kappa : \kappa \in \mathbb{Z}\} \\ \textit{[1]} &= \{3\kappa + 1 : \kappa \in \mathbb{Z}\} \\ \textit{[2]} &= \{3\kappa + 2 : \kappa \in \mathbb{Z}\}. \end{aligned}$$

**Πρόταση 1.3.5.** *Έστω $X$ μια σχέση ισοδυναμίας στο $A$ και $a, b \in A$. Τότε ισχύουν τα ακόλουθα.*

(i) $[a] = [b] \Leftrightarrow a \sim b$.

(ii) $[a] \cap [b] = \emptyset \Leftrightarrow a \nsim b$

*Απόδειξη.* (i). Έστω $[a] = [b]$. Τότε $a \in [a] = [b]$, οπότε από τον ορισμό της κλάσης παίρνουμε $a \sim b$.

Αντίστροφα έστω $a \sim b$ και έστω $x \in [a]$. Τότε $x \sim a$ και αφού $a \sim b$, από την μεταβατική ιδιότητα παίρνουμε ότι $x \sim b$. Επομένως $x \in [b]$ και έπεται ότι $[a] \subset [b]$. Ομοίως παίρνουμε ότι $[b] \subset [a]$. Άρα $[a] = [b]$.

(ii) Έστω $[a] \cap [b] = \emptyset$. Ας υποθέσουμε ότι $a \sim b$. Τότε $a \in [a]$ και $a \in [b]$. Άρα $a \in [a] \cap [b]$, άτοπο.

Αντίστροφα έστω $a \nsim b$ και $x \in [a] \cap [b]$. Τότε $x \in [a]$ και $x \in [b]$, δηλαδή $x \sim a$ και $x \sim b$. Τότε $a \sim x$ και $x \sim b$, επομένως $a \sim b$, άτοπο. □

### 1.3β′ Το σύνολο $\mathbb{Z}_n$

**Ορισμός 1.3.6.** *Ορίζουμε με*

$$\mathbb{Z}_n = \{[a]_n : a \in \mathbb{Z}\}$$

*το σύνολο των ακεραίων modulo $n$.*

**Πρόταση 1.3.7.** *Ισχύει*

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \cdots, [n-1]_n\}.$$

**Παρατήρηση 1.3.8.** *Αν* $0 \leqslant i, j \leqslant n-1$ *με* $i \neq j$ *τότε* $[i]_n \neq [j]_n$.

*Απόδειξη της πρότασης 1.3.7.* Προφανώς

$$\{[0]_n, [1]_n, [2]_n, \cdots, [n-1]_n\} \subseteq \mathbb{Z}_n$$

από τον ορισμό του $\mathbb{Z}_n$.

Έστω $[a] \in \mathbb{Z}_n$. Από τον αλγόριθμο της Ευκλείδειας διαίρεσης υπάρχουν $q, r \in \mathbb{Z}$ ώστε

$$a = qn + r, \qquad 0 \leqslant r \leqslant n-1.$$

Τότε $[a]_n = [r]_n$. □

**Παράδειγμα 1.3.9.** *Έχουμε,*

$$\mathbb{Z}_2 = \{[0]_2, [1]_2\},$$

*όπου*

$$[0]_2 = \{2\kappa : \kappa \in \mathbb{Z}\}$$

*και*

$$[1]_2 = \{1 + 2\kappa : \kappa \in \mathbb{Z}\}.$$

*Επίσης*

$$\mathbb{Z}_2 = \{[1]_2, [2]_2\}$$

*και*

$$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}.$$

*Ακόμη,*

$$\mathbb{Z}_3 = \{[1]_3, [6]_3, [8]_3\}.$$

**Παρατήρηση 1.3.10.** *Έστω* $a_0, a_1, \cdots, a_{n-1} \in \mathbb{Z}$ *με* $a_i \equiv i \mathrm{mod} n$. *Τότε*

$$\mathbb{Z}_n = \{[a_0]_n, [a_1]_n, \cdots, [a_{n-1}]_n\}.$$

**Ορισμός 1.3.11.** *Έστω* $[a], [b] \in \mathbb{Z}_n$. *Ορίζουμε δυο πράξεις, δηλαδή δυο απεικονίσεις* $\mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$, *με*

$$+ : ([a], [b]) \to [a + b]$$

*και*

$$\cdot : ([a], [b]) \to [a \cdot b].$$

**Λήμμα 1.3.12.** *Οι απεικονίσεις του προηγούμενου ορισμού είναι καλώς ορισμένες.*

*Απόδειξη.* Έστω $a, a', b, b' \in \mathbb{Z}$ με $[a] = [a']$ και $[b] = [b']$. Θα δείξουμε ότι $[a+b] = [a'+b']$. Πράγματι έχουμε ότι

$$n|a - a' \qquad \text{και} \qquad n|b - b'. \tag{1.3.1}$$

Τότε,

$$n|(a + b) - (a' + b'),$$

δηλαδή

$$a + b = (a' + b')\mathrm{mod}n.$$

Επομένως

$$[a + b] = [a' + b'].$$

Άρα η πρόσθεση που ορίσαμε είναι πράγματι πράξη στο $\mathbb{Z}_n$.

Λόγω της σχέσης (1.3.1) και της πρότασης 1.2.6, έπεται ότι

$$ab = (a'b')\mathrm{mod}n.$$

Επομένως

$$[ab] = [a'b'],$$

δηλαδή η πράξη του πολλαπλασιασμού είναι καλώς ορισμένη. □

**Παράδειγμα 1.3.13.** *Στο $\mathbb{Z}_6$ έχουμε,*

(i) $[8] + [4] = [6] = [0]$.

(ii) $[2] \cdot [4] = [8] = [2]$.

(iii) $[2] + [-7] = [-5] = [1]$.

**Πρόταση 1.3.14.** *Έστω $a, b, c \in \mathbb{Z}$. Στο $\mathbb{Z}_n$ ισχύουν τα ακόλουθα.*

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

*9.* $[a][b] = [b][a]$.

*Απόδειξη.* Εύκολα μπρούμε να ελέγξουμε τις παραπάνω ιδιότητες.
*Σημείωση.* Στο $\mathbb{Z}_6$ έχουμε

$$[2][3] = [6] = [0],$$
$$[2][4] = [2][1].$$

Παρατηρήστε όμως ότι $[4] \neq [1]$. Γενικά ο νόμος της διαγραφής ως προς τον πολλαπλασιασμό δεν ισχύει.

**Ορισμός 1.3.15.** *Ενα στοιχείο* $[a] \in \mathbb{Z}_n$ *λέγεται αντιστρέψιμο, αν υπάρχει* $[a'] \in \mathbb{Z}_n$, *ώστε*

$$[a][a'] = [a'][a] = [1].$$

*Στην περίπτωση αυτήν θα λέμε ότι το στοιχείο* $[a']$ *λέγεται αντίστροφο του* $[a]$ *στο* $\mathbb{Z}_n$.

**Παράδειγμα 1.3.16.** (i) *Στο* $\mathbb{Z}_{10}$ *έχουμε*

$$[3][7] = [7][3] = [21] = 1.$$

*Επομένως το* $[3]$ *και το* $[7]$ *είναι αντιστρέψιμα στοιχεία.*

(ii) *Στο* $\mathbb{Z}_{10}$ *το* $[2]$ *δεν είναι αντιστρέψιμο στοιχείο. Πράγματι, έστω ότι υπάρχει* $[a'] \in \mathbb{Z}_{10}$ *ώστε*

$$[2][a'] = [1].$$

*Τότε*

$$[2a'] = [1],$$

*δηλαδή*

$$2a' \equiv 1 \mathrm{mod} 10.$$

*Έπεται ότι*

$$2a' = 1 + 10\kappa,\ \kappa \in \mathbb{Z}.$$

*Η τελευταία σχέση δεν μπορεί να ισχύει (γιατί ο* $2a'$ *είναι άρτιος, ενώ ο* $1 + 10\kappa$ *είναι περιττός).*

**Πρόταση 1.3.17.** *Το* $[a] \in \mathbb{Z}_n$ *είναι αντιστρέψιμο αν και μόνον αν* $\mu\kappa\delta(a, n) = 1$.

*Απόδειξη.* Έστω $[a]$ αντιστρέψιμο στο $\mathbb{Z}_n$. Τότε υπάρχει $[a'] \in \mathbb{Z}_n$ ώστε

$$[a][a'] = 1.$$

Τότε

$$[aa'] = 1 \qquad \text{ή} \qquad aa' = 1 \mathrm{mod} n.$$

Επομένως,

$$aa' = 1 + \kappa n,\ (\kappa \in \mathbb{Z}).$$

Έπεται

$$\mu\kappa\delta(a,n)|1,$$

άρα

$$\mu\kappa\delta(a,n)=1.$$

Αντίστροφα, έστω ότι $\mu\kappa\delta(a,n)=1$. Τότε υπάρχουν $x,y\in\mathbb{Z}$ ώστε

$$1=ax+ny.$$

Επομένως,

$$[1]=[ax+ny].$$

Τότε,

$$\begin{aligned}[1] &= [a][x]+[n][y]\\ &= [a][x]+[0][y]\\ &= [a][x]+[0]\\ &= [a][x].\end{aligned}$$

Άρα έχουμε,

$$[1]=[a][x],$$

άρα το $[a]$ είναι αντιστρέψιμο. □

**Παρατήρηση 1.3.18.** *Αν το $[a]\in\mathbb{Z}_n$ είναι αντιστρέψιμο, τότε υπάρχει μοναδικό αντίστροφό του.*

*Απόδειξη.* Έστω $[a],[b],[c]\in\mathbb{Z}_n$ ώστε

$$[a][b]=[1] \qquad \text{και} \qquad [a][c]=[1].$$

Τότε,

$$\begin{aligned}[c] &= [c][1]=[c]([a][b])\\ &= ([c][a])[b]=([a][c])[b]\\ &= [1][b]=[b]\end{aligned}$$

□

### Ασκήσεις

1. Να βρείτε το αντίστροφο του $[5]$ στο $\mathbb{Z}_{36}$.

*Λύση.* Επειδή μκδ$(5, 36) = 1$, το $[5]$ έχει αντίστροφο στο $\mathbb{Z}_{36}$. Από τον αλγόριθμο της Ευκλείδειας διαίρεσης έχουμε,

$$\begin{aligned} 36 &= 5 \cdot 7 + 1 \\ 5 &= 5 \cdot 1 + 0. \end{aligned}$$

Άρα

$$1 = 5(-7) + 36,$$

επομένως

$$[1] = 5[-7],$$

δηλαδή το $[5]$ έχει αντίστροφο το $[-7] = [29]$. □

**2**. Να βρείτε όλους τους $x \in \mathbb{Z}$, ώστε

$$8x \equiv 11 \text{mod} 15.$$

*Λύση.* Επειδή μκδ$(8, 15) = 1$, το $[8]$ έχει αντίστροφο στο $\mathbb{Z}_{15}$. Από τον αλγόριθμο της Ευκλείδειας διαίρεσης έχουμε,

$$\begin{aligned} 15 &= 1 \cdot 8 + 7 \\ 8 &= 1 \cdot 7 + 1 \\ 7 &= 7 \cdot 1 + 0. \end{aligned}$$

Επομένως

$$1 = 8 - 1 \cdot 7 = 8 - 1(15 - 1 \cdot 8) = 8(2) + 15(-1).$$

Άρα το αντίστροφο του $[8]$ στο $\mathbb{Z}_{15}$ είναι το $[2]$. Παρατηρήστε ότι,

$$8x \equiv 11 \text{mod} 15 \Leftrightarrow [8][x] = [11].$$

Πολλαπλασιάζοντας με το αντίστροφο του $[8]$ έχουμε

$$[2]([8][x]) = [2][11] \Rightarrow [x] = [22] = [7].$$

Επομένως

$$x = 7 + 15\kappa.$$

□

**3**. Να δείξετε ότι η εξίσωση

$$[a][x] = [b] \tag{1.3.2}$$

έχει λύση στο $\mathbb{Z}_n$ αν και μόνο αν μκδ$(a, n)|b$.

*Απόδειξη.* Έστω ότι υπάρχει $x \in \mathbb{Z}$ ώστε να είναι λύση της (1.3.2). Τότε έχουμε,

$$[ax] = [b] \Rightarrow ax = b + \kappa n \qquad (\kappa \in \mathbb{Z}).$$

Επειδή $\mu\kappa\delta(a,n)|a$ και $\mu\kappa\delta(a,n)|n$, έχουμε $\mu\kappa\delta(a,n)|b$.
Αντίστροφα, έστω ότι $\mu\kappa\delta(a,n)|b$. Τότε υπάρχουν $x, y \in \mathbb{Z}$ ώστε

$$\mu\kappa\delta(a,n) = ay + nz.$$

Πολλαπλασιάζοντας με το $\frac{b}{\mu\kappa\delta(a,n)} \in \mathbb{Z}$, παίρνουμε

$$b = ax + nz_1,$$

για κάποια $x, z_1 \in \mathbb{Z}$. Επομένως

$$[b] = [ax] = [a][x].$$

□

## 1.4 Η συνάρτηση του Euler

**Ορισμός 1.4.1.** *Έστω $\varphi : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ με*

$$\varphi(n) = \textit{πλήθος } \{a \in \mathbb{Z} : 1 \leqslant a \leqslant n, \textit{μκδ}(a,n) = 1\}.$$

*Για παράδειγμα έχουμε $\varphi(10) = 4, \varphi(12) = 4$. Παρατηρήστε ότι*

$$[a] \in \mathbb{Z}_n \qquad \textit{αντιστρέψιμο} \qquad \Leftrightarrow \qquad \textit{μκδ}(a,n) = 1.$$

*Συνεπώς αν*

$$U(\mathbb{Z}_n) = \{[a] \in \mathbb{Z}_n : [a] \textit{ αντιστρέψιμο}\},$$

*τότε*

$$\varphi(n) = |U(\mathbb{Z}_n)| \ (= \textit{πλήθος στοιχείων του } U(\mathbb{Z}_n)).$$

**Πρόταση 1.4.2.** *Η συνάρτηση $\varphi$ του Euler ικανοποιεί τις ακόλουθες ιδιότητες.*

(i) *Αν $p$ πρώτος και $\kappa \in \mathbb{Z}_{>0}$, τότε $\varphi(p) = p^\kappa - p^{\kappa-1}$.*

(ii) *Αν $m, n \in \mathbb{Z}_{>0}$ και $\mu\kappa\delta(m,n) = 1$, τότε $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.*

(iii) *Αν $\alpha \in \mathbb{Z}_{>0}$ και $\alpha = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\kappa^{\alpha_\kappa}$, όπου $p_i$ πρώτοι με $p_i \neq p_j$ για κάθε $i \neq j$, τότε*

$$\varphi(\alpha) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_\kappa^{\alpha_\kappa} - p_\kappa^{\alpha_\kappa - 1}) = \alpha \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_\kappa}\right).$$

**Παράδειγμα 1.4.3.** $\varphi(100) = \varphi(2^2 \cdot 5^2) = (2^2 - 2)(5^2 - 5) = 40.$

**Λήμμα 1.4.4.** *Αν* $a, b, n \in \mathbb{Z}$ *με* $\mu\kappa\delta(a, n) = \mu\kappa\delta(b, n) = 1$, *τότε* $\mu\kappa\delta(ab, n) = 1$.

*Απόδειξη.* Έστω ότι υπάρχει $p$ πρώτος με $p|\mu\kappa\delta(ab, n)$. Τότε $p|ab$ και επειδή ο $p$ είναι πρώτος, έπεται ότι $p|a$ ή $p|b$. Δηλαδή,

$$p|a \text{ και } p|n \qquad \text{ή} \qquad p|b \text{ και } p|n.$$

Έπεται ότι,

$$p|\mu\kappa\delta(a, n) \qquad \text{ή} \qquad p|\mu\kappa\delta(b, n).$$

Επομένως $p|1$, το οποίο είναι άτοπο. □

*Απόδειξη της πρότασης 1.4.2.* (i). Οι ακέραιοι που ικανοποιούν τις $1 \leqslant \alpha \leqslant p^\kappa$ και $\mu\kappa\delta(\alpha, p^\kappa) \neq 1$ είναι ακριβώς τα πολλαπλάσια του $p$ της μορφής $\alpha = p \cdot q$ ,όπου $q = 1, 2, \ldots p^{\kappa-1}$. Επομένως $\varphi(p) = p^\kappa - p^{\kappa-1}$.

(ii). Αρκεί να δείξουμε ότι αν $\mu\kappa\delta(m, n) = 1$, τότε

$$|U(\mathbb{Z}_{mn})| = |U(\mathbb{Z}_n)| \times |U(\mathbb{Z}_m)| = |U(\mathbb{Z}_n| \cdot |U(\mathbb{Z}_m)|.$$

Θεωρούμε την συνάρτηση $\psi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, με

$$\psi([a]_{mn}) = ([a]_m, [a]_n).$$

Η $\psi$ είναι καλά ορισμένη απεικόνιση.

Πράγματι, έστω $[a]_{mn} = [b]_{mn}$. Τότε $mn|a - b$, άρα $m|a - b$ και $n|a - b$. Επομένως $[a]_m = [b]_m$ και $[a]_n = [b]_n$.

Ισχυρισμός. Η $\psi$ είναι $1 - 1$ και επί.

Πράγματι, έστω

$$\psi([a]_{mn}) = \psi([b]_{mn}),$$

άρα

$$([a]_m, [a]_n) = ([b]_m, [b]_n).$$

Έπεται ότι

$$[a]_m = [b]_m \qquad \text{και} \qquad [a]_n = [b]_n,$$

άρα

$$m|a - b \qquad \text{και} \qquad n|a - b.$$

Αφού $\mu\kappa\delta(m, n) = 1$, παίρνουμε ότι $m \cdot n|a - b$, επομένως $[a]_{mn} = [b]_{mn}$, δηλαδή η $\psi$ είναι $1 - 1$.

Επειδή η $\psi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ είναι $1 - 1$ και αφού $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n| (= mn < \infty)$, έπεται ότι η $\psi$ είναι επί.

Θεωρούμε τώρα τον περιορισμό $\bar{\psi}$ της $\psi$ στο υποσύνολο $U(\mathbb{Z}_{mn})$ του $Z_{mn}$. Παρατηρήστε ότι

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

Πράγματι, έστω $[a]_{mn} \in U(\mathbb{Z}_{mn})$, άρα μκδ$(a, mn) = 1$. Επειδή μκδ$(a, m)|$μκδ$(a, mn)$, έπεται ότι μκδ$(a, m) = 1$. Δηλαδή $[a]_m \in U(\mathbb{Z}_m)$. Ομοίως έχουμε $[a]_n \in U(\mathbb{Z}_n)$. Επομένως ορίζεται η συνάρτηση $\bar{\psi} : U(\mathbb{Z}_{mn}) \to U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$ με

$$\bar{\psi}([a]_{mn}) = ([a]_m, [a]_n).$$

Θα δείξουμε τώρα ότι η $\bar{\psi}$ είναι $1-1$ και επί.

Αφού η $\psi$ είναι $1-1$, είναι και η $\bar{\psi}$.

Η $\bar{\psi}$ είναι επί. Πράγματι, έστω $([x]_n, [y]_m) \in U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$. Τότε μκδ$(x, m) =$ μκδ$(y, n) = 1$. Επειδή η $\psi$ είναι επί υπάρχει ένα στοιχείο $[a]_{mn} \in \mathbb{Z}_{mn}$ ώστε

$$([a]_m, [a]_n) = ([x]_m, [y]_n),$$

δηλαδή

$$[a]_m = [x]_m \qquad \text{και} \qquad [a]_n = [y]_n.$$

Τότε $a \equiv x \mathrm{mod} m$ και αφού μκδ$(x, m) = 1$, έπεται μκδ$(a, m) = 1$. Ομοίως παίρνουμε μκδ$(a, n) = 1$. Από το λήμμα 1.4.4 έπεται ότι μκδ$(a, mn) = 1$, δηλαδή $[a]_{mn} \in U(\mathbb{Z}_{mn})$.

(iii). Από τα (ii) και (i) έχουμε διαδοχικά,

$$\begin{aligned} \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\kappa^{\alpha_\kappa}) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_\kappa^{\alpha_\kappa}) \\ &= (p_1^{\alpha_1} - p_1^{\alpha-1})(p_2^{\alpha_2} - p_2^{\alpha-1}) \cdots (p_\kappa^{\alpha_\kappa} - p_\kappa^{\alpha_{\kappa-1}}) \\ &= \alpha \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_\kappa}\right). \end{aligned}$$

□

**Θεώρημα 1.4.5.** *(Euler) Έστω $\alpha \in \mathbb{Z}$ και $n \in \mathbb{Z}_{>0}$ με μκδ$(\alpha, n) = 1$. Τότε*

$$\alpha^{\varphi(n)} = 1 \mathrm{mod} n.$$

(Για παράδειγμα αφού $\varphi(100) = 40$ και μκδ$(17, 100) = 1$, έχουμε $17^{40} \equiv 1 \mathrm{mod} 100$. Δηλαδή τα δύο τελευταία ψηφία του $17^{40}$ στο δεκαδικό σύστημα είναι 0,1.)

**Πόρισμα 1.4.6.** *(Μικρό θεώρημα Fermat) Έστω $\alpha \in \mathbb{Z}$ και $p$ πρώτος.*

*(i) Ισχύει ότι,*

$$\alpha^p \equiv \alpha \mathrm{mod} p.$$

*(ii) Αν $p \nmid \alpha$, τότε*

$$\alpha^{p-1} \equiv 1 \mathrm{mod} p.$$

*(Για παράδειγμα $\alpha^{2011} \equiv \alpha \mathrm{mod} 2011$, για κάθε $\alpha \in \mathbb{Z}$ (2011 πρώτος).)*

*Απόδειξη.*(ii). Έπεται από το θεώρημα του Euler για $n = p$.

(i) Αν $p \nmid \alpha$, τότε μκδ$(\alpha, p) = 1$, οπότε από το θεώρημα του Euler έπεται ότι

$$\alpha^{p-1} \equiv 1 \mathrm{mod} p \Rightarrow \alpha^p \equiv \alpha \mathrm{mod} p$$

*Σημείωση.* Αν $p \mid \alpha$, τότε $\alpha = 0 \mathrm{mod} p$ και $\alpha^p = 0 \mathrm{mod} p$. □

*Απόδειξη του θεωρήματος* Euler. Έστω

$$U((Z_n) = \{[\alpha_1], [\alpha_2], \cdots, [\alpha_\kappa]\},$$

όπου $\kappa = \varphi(n)$. Έστω $[\alpha] \in U(\mathbb{Z}_n)$. Θεωρούμε το σύνολο

$$A = \{[\alpha\alpha_i] : i = 1, 2, \ldots, \kappa\}.$$

Θα δείξουμε ότι $A = U(\mathbb{Z}_n)$. Δείχνουμε πρώτα ότι $A \subseteq U(\mathbb{Z}_n)$.

Γενικά ισχύει ότι αν $[\alpha], [\beta] \in U(\mathbb{Z}_n)$, τότε και $[\alpha\beta] \in U(\mathbb{Z}_n)$. Πράγματι, αν μκδ$(\alpha, n) = 1$ και μκδ$(\beta, n) = 1$, από το λήμμα 1.4.4 ισχύει μκδ$(\alpha\beta, n) = 1$. Επομένως $[\alpha\beta] \in U(\mathbb{Z}_n)$.

Τα σύνολα $A$ και $U(\mathbb{Z}_n)$ είναι πεπερασμένα και έχουν τον ίδιο πλήθος στοιχείων. Αρκεί να δείξουμε ότι $|A| = \kappa$, δηλαδή αν $[\alpha_i] \neq [\alpha_j]$, τότε $[\alpha\alpha_i] \neq [\alpha\alpha_j]$. Έστω ότι $[\alpha\alpha_i] = [\alpha\alpha_j]$. Τότε

$$n|\alpha\alpha_i - \alpha\alpha_j \Rightarrow n|\alpha(\alpha_i - \alpha_j).$$

Επειδή μκδ$(\alpha, n) = 1$, έπεται ότι

$$n|\alpha_i - \alpha_j.$$

Επομένως $[\alpha_i] = [\alpha_j]$, άρα $A = U(\mathbb{Z}_n)$.

Σχηματίζουμε το γινόμενο όλων των στοιχείων του $U(\mathbb{Z}_n)$.

$$[\alpha\alpha_1][\alpha\alpha_2] \cdots [\alpha\alpha_\kappa] = [\alpha_1][\alpha_2] \cdots [\alpha_\kappa].$$

Επομένως

$$[\alpha^\kappa \alpha_1 \alpha_2 \cdots \alpha_\kappa] = [\alpha_1 \alpha_2 \cdots \alpha_\kappa].$$

Πολλαπλασιάζοντας με τον αντίστροφο του $[\alpha_1][\alpha_2] \cdots [\alpha_\kappa]$ (έχουμε δει ότι αν $[x], [y] \in U(\mathbb{Z}_n)$, τότε $[xy] \in U(\mathbb{Z}_n)$), προκύπτει ότι $[\alpha]^\kappa = [1]$, δηλαδή $\alpha^\kappa \equiv 1 \mathrm{mod} n$. Επομένως

$$\alpha^{\varphi(n)} = 1 \mathrm{mod} n.$$

□

## Ασκήσεις

**1**. Να βρείτε το υπόλοιπο της διαίρεσης του $19^{1000}$ με το 14.

*Λύση.* Παρατηρήστε ότι

$$19 \equiv 5 \mathrm{mod} 14 \Rightarrow 19^{1000} \equiv 5^{1000} \mathrm{mod} 14. \tag{1.4.1}$$

Έχουμε

$$\varphi(14) = \varphi(2 \cdot 7) = \varphi(2) \cdot \varphi(7) = 6.$$

Επειδή $1000 = 166 \cdot 6 + 4$, παίρνουμε

$$5^{1000} = (5^6)^{166} \cdot 5^4 \equiv 1^{166} \cdot 5^4 \mathrm{mod} 14,$$

όπου η δεύτερη ισότητα έπεται από το θεώρημα του Euler. Τότε από την 1.4.1 παίρνουμε,

$$19^{1000} \equiv 5^4 \mathrm{mod} 14.$$

Όμως

$$5^4 = (5^2)^2 \equiv 11^2 \mathrm{mod} 14 \equiv (-3)^2 \mathrm{mod} 14 \equiv 9 \mathrm{mod} 14.$$

Επομένως το υπόλοιπο της διαίρεσης του $19^{1000}$ με το 14 είναι το 9. □

**2**. Να δείξετε ότι για κάθε $n \in \mathbb{N}$ ισχύει

$$n^{49} \equiv n \mathrm{mod} 1547.$$

*Σημείωση.* $1547 = 7 \cdot 13 \cdot 17$.

*Απόδειξη.* Επειδή $1547 = 7 \cdot 13 \cdot 17$ αρκεί να δείξουμε ότι

$$n^{49} \equiv n \mathrm{mod} 7,$$

$$n^{49} \equiv n \mathrm{mod} 13,$$

και

$$n^{49} \equiv n \mathrm{mod} 17.$$

Πράματι από το μικρό θεώρημα του Fermat για $p = 7$, έχουμε

$$n^7 = n \mathrm{mod} 7,$$

άρα

$$n^{49} \equiv (n^7)^7 \equiv n \mathrm{mod} 7.$$

Ομοίως από το μικρό θεώρημα του Fermat για $p = 13$, έχουμε

$$n^{13} = n \mathrm{mod} 13.$$

Επειδή $49 = 3 \cdot 13 + 10$ , παίρνουμε

$$n^{49} \equiv (n^{13})^3 \cdot n^{10} \equiv n^3 \cdot n^{10} \equiv n^{13} \equiv n \mathrm{mod} 13.$$

Ομοίως με πριν δείχνουμε ότι

$$n^{49} \equiv n \mathrm{mod} 17.$$

□

**3**. Να δείξετε ότι για κάθε $n \in \mathbb{N}$ ισχύει

$$(n+1)^9 + 4n^5 \equiv 1 \mathrm{mod} 5.$$

*Απόδειξη.* Από το μικρό θεώρημα του Fermat, έχουμε

$$n^5 \equiv n \mathrm{mod} 5 \qquad \text{και} \qquad (n+1)^5 \equiv (n+1) \mathrm{mod} 5.$$

Επομένως,

$$(n+1)^9 = (n+1)^5 \cdot (n+1)^4 \equiv (n+1)(n+1)^4 \equiv (n+1)^5 \equiv (n+1) \mathrm{mod} 5.$$

Από το θεώρημα του Fermat και από το γεγονός ότι $4 \equiv -1 \mathrm{mod} 5$, παίρνουμε ότι

$$4n^5 \equiv 4n \mathrm{mod} 5 \equiv -n \mathrm{mod} 5.$$

Άρα

$$(n+1)^9 + 4n^5 \equiv (n+1) + (-n) \mathrm{mod} 5 \equiv 1 \mathrm{mod} 5.$$

□

**4**. Έστω $n \in \mathbb{N}$. Να δείξετε ότι

$$n^{12} + 12^n \equiv 5 \mathrm{mod} 11 \qquad \Leftrightarrow \qquad n \equiv 2 \mathrm{mod} 11 \qquad \text{ή} \qquad n \equiv 9 \mathrm{mod} 11.$$

*Απόδειξη.* Παρατηρήστε ότι

$$12 \equiv 1 \mathrm{mod} 11 \Rightarrow 12^n \equiv 1 \mathrm{mod} 11.$$

Από το μικρό θεώρημα του Fermat για $p = 11$, παίρνουμε

$$n^{11} \equiv n \mathrm{mod} 11 \Rightarrow n^{12} \equiv n^2 \mathrm{mod} 11,$$

άρα

$$n^{12} + 12^n \equiv (n^2 + 1) \mathrm{mod} 11.$$

Επομένως

$$\begin{aligned} n^{12} + 12^n \equiv 5 \mathrm{mod} 11 \quad &\Leftrightarrow \quad n^2 + 1 \equiv 5 \mathrm{mod} 11 \\ &\Leftrightarrow \quad n^2 - 4 \equiv 0 \mathrm{mod} 11 \\ &\Leftrightarrow \quad 11 | n^2 - 4 \\ &\Leftrightarrow \quad 11 | (n-2)(n+2). \end{aligned}$$

Επειδή ο 11 είναι πρώτος έπεται

$$11 | (n-2) \qquad \text{ή} \qquad 11 | n+2.$$

Επομένως

$$n \equiv 2 \mathrm{mod} 11 \qquad \acute{\eta} \qquad n \equiv -2 \mathrm{mod} 11.$$

Άρα

$$n \equiv 2 \mathrm{mod} 11 \qquad \acute{\eta} \qquad n \equiv 9 \mathrm{mod} 11.$$

□

**5**. Να δείξετε ότι

$$7^n \equiv 1 \mathrm{mod} 20 \Leftrightarrow n = 0 \mathrm{mod} 4.$$

*Απόδειξη.* Από τον αλγόριθμο της Ευκλείδειας διαίρεσης έχουμε

$$n = 4m + r,\ 0 \leqslant r < 4.$$

Επειδή $7^4 = 2401$, έχουμε

$$7^4 = 1 \mathrm{mod} 20,$$

επομένως

$$7^n = (7^4)^m \cdot 7^r \equiv 7^r \mathrm{mod} 20.$$

Επομένως

$$7^n \equiv 1 \mathrm{mod} 20 \Leftrightarrow 7^r \equiv 1 \mathrm{mod} 20. \tag{1.4.2}$$

Για $r = 0$ η (1.4.2) προφανώς ισχύει. Για $r = 1, 2, 3$ κάνοντας πράξεις βλέπουμε ότι η (1.4.2) δεν ισχύει. Επομένως

$$7^n \equiv 1 \mathrm{mod} 20 \Leftrightarrow r = 0 \Leftrightarrow n \equiv 0 \mathrm{mod} 4.$$

□

**Παρατήρηση 1.4.7.** *Έχουμε* $\varphi(20) = \varphi(4 \cdot 5) = \varphi(4) \cdot \varphi(5) = 2 \cdot 4 = 8$. *Επίσης* $\mu\kappa\delta(7, 20) = 1$. *Άρα από το θεώρημα του Euler έχουμε*

$$7^8 \equiv \mathrm{mod} 20.$$

*Στην προηγούμενη άσκηση είδαμε ότι* $7^4 \equiv 1 \mathrm{mod} 20$ . *Άρα γενικά μιλώντας, αν* $\mu\kappa\delta(\alpha, n) = 1$, *τότε ο ακέραιος* $\varphi(n)$ *δεν είναι αναγκαστικά ο μικρότερος θετικός ακέραιος* $\kappa$ *ώστε* $\alpha^\kappa \equiv 1 \mathrm{mod} n$.

**6**. Έστω $p$ πρώτος με $p = 3 \mathrm{mod} 4$. Να δείξετε ότι δεν υπάρχει $\alpha \in \mathbb{Z}$ ώστε

$$\alpha^2 \equiv -1 \mathrm{mod} p. \tag{1.4.3}$$

*Απόδειξη.* Υποθέτουμε ότι υπάρχει $\alpha \in \mathbb{Z}$, ώστε να ικανοποιείται η (1.4.3). Διακρίνουμε τις δύο ακόλουθες περιπτώσεις.

(α′) Έστω ότι $p|\alpha$. Τότε από την (1.4.3) έπεται ότι $p|-1$, το οποίο είναι άτοπο

(β′) Έστω ότι $p \nmid \alpha$. Έστω $p = 4\kappa+3, \kappa \in \mathbb{Z}$ ($p = 3\text{mod}4$). Έστω $N = \frac{p-1}{2} = 2\kappa+1$ (περιττός ακέραιος). Από την (1.4.3) έπεται

$$(\alpha^2)^N \equiv (-1)^N \text{mod} p \Rightarrow \alpha^{2n} \equiv (-1)^N \text{mod} p.$$

Επομένως

$$\alpha^{p-1} \equiv (-1)^N \text{mod} p. \tag{1.4.4}$$

Επειδή ο $N$ είναι περιττός, έχουμε $(-1)^N = -1$, άρα από την (1.4.4) παίρνουμε

$$\alpha^{p-1} \equiv -1 \text{mod} p.$$

Αφού ο $p \nmid \alpha$, από το μικρό θεώρημα του Fermat παίρνουμε

$$\alpha^{p-1} \equiv 1 \text{mod} p.$$

Έπεται ότι

$$1 \equiv -1 \text{mod} p \Rightarrow p = 2,$$

το οποίο είναι άτοπο αφού $p = 3\text{mod}4$. □

**Παρατήρηση 1.4.8.** *Έστω $p = 5$ ($p \equiv 1\text{mod}4$). Τότε*

$$2^2 \equiv -1 \text{mod} 5.$$

**7**. Έστω $\alpha \in \mathbb{Z}$ με μκδ$(\alpha, 72) = 1$. Να δείξετε ότι

$$\alpha^{12} \equiv 1 \text{mod} 72.$$

*Απόδειξη.* Παρατηρήστε ότι $72 = 2^3 \cdot 3^2$. Επειδή μκδ$(2^3, 3^2) = 1$, αρκεί να δείξουμε ότι

$$\alpha^{12} \equiv 1 \text{mod} 8 \qquad \text{και} \qquad \alpha^{12} \equiv 1 \text{mod} 9.$$

Πράγματι αφού μκδ$(\alpha, 72) = 1$, έπεται μκδ$(\alpha, 8) = 1$. Από το θεώρημα του Euler και αφού $\varphi(8) = 2^3 - 2^2 = 4$, έχουμε

$$\alpha^{\varphi(8)} \equiv 1 \text{mod} 8 \Rightarrow \alpha^4 \equiv 1 \text{mod} 8.$$

Επομένως

$$\alpha^{12} = (\alpha^4)^3 \equiv 1^3 \text{mod} 8 \equiv 1 \text{mod} 8.$$

Ομοίως επειδή μκδ$(\alpha, 9) = 1$ και $\varphi(9) = 3^2 - 3 = 6$, από το θεώρημα του Euler παίρνουμε

$$\alpha^{\varphi(9)} \equiv 1 \text{mod} 9 \Rightarrow \alpha^6 = 1 \text{mod} 9.$$

Επομένως

$$\alpha^{12} = 1 \text{mod} 9.$$

□

**8**. Έστω $n \in \mathbb{Z}_{>0}$. Να δείξετε ότι

$$\varphi(2n) = 2\varphi(n) \qquad \Leftrightarrow \qquad n \qquad \text{άρτιος.}$$

*Απόδειξη.* Έστω $\varphi(2n) = 2\varphi(n)$ και ας υποθέσουμε ότι ο $n$ είναι περιττός. Τότε μκδ$(2, n) = 1$ και

$$\varphi(2n) = \varphi(2) \cdot \varphi(n) = \varphi(n).$$

Επομένως

$$\varphi(n) = 2\varphi(n) \Rightarrow \varphi(n) = 0,$$

το οποίο είναι άτοπο.

Αντίστροφα, έστω $n$ άρτιος. Τότε $n = 2^\alpha \cdot m$, όπου $\alpha \in \mathbb{Z}_{>0}$ και $m$ περιττός. Τότε

$$\begin{aligned} \varphi(2n) &= \varphi(2^{\alpha+1} \cdot m) = \varphi(2^{\alpha+1})\varphi(m) \\ &= (2^{\alpha+1} - 2^\alpha) \cdot \varphi(m) = 2^\alpha \varphi(m), \end{aligned}$$

όπου στην δεύτερη ισότητα χρησιμοποιήσαμε το γεγονός ότι μκδ$(2^{\alpha+1}, m) = 1$.

Επίσης έχουμε,

$$\begin{aligned} 2\varphi(n) &= 2\varphi(2^\alpha \cdot m) = 2\varphi(2^\alpha)\varphi(m) \\ &= 2(2^\alpha - 2^{\alpha-1}) \cdot \varphi(m) \\ &= 2 \cdot 2^{\alpha-1}\varphi(m) \\ &= 2^\alpha \varphi(m) \end{aligned}$$

Επομένως $\varphi(2n) = 2\varphi(n)$. □

# Κεφάλαιο 2

# Δακτύλιοι

## 2.1 Ακεραίες περιοχές και σώματα

**Ορισμός 2.1.1.** *Μια πράξη σε ένα μη κενό σύνολο $A$ είναι μια απεικόνιση $A \times A \to A$.*

**Παράδειγμα 2.1.2.** (i) *Η συνήθης πρόσθεση $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, με $(a, b) \mapsto a + b$ και ο συνήθης πολλαπλασιασμός $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, με $(a, b) \mapsto a \cdot b$ είναι πράξεις στο $\mathbb{Z}$.*

(ii) *Στο $\mathbb{Z}_n$ είχαμε ορίσει,*

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, \qquad ([a], [b]) \mapsto [a + b]$$

*και*

$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, \qquad ([a], [b]) \mapsto [a \cdot b].$$

*(Είδαμε ότι οι παραπάνω αντιστοιχίες είναι απεικονίσεις.)*

(iii) *Η αντιστοιχία $\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$, με*

$$([a], [b]) \mapsto [c], \qquad c = \max\{a, b\}.$$

*δεν είναι πράξη (δηλαδή δεν είναι απεικόνιση). Πράγματι,*

$$([0], [1]) \mapsto [1]$$

*και*

$$([2], [1]) \mapsto [2],$$

*αλλά $[1] \neq [2]$.*

(iv) *Συμβολίζουμε με* $M_n(\mathbb{R})$ *το σύνολο των* $n \times n$ *με στοιχεία από το* $\mathbb{R}$ *και ορίζουμε την συνήθη πρόσθεση και τον συνήθη πολλαπλασιασμό με*

$$M_n(\mathbb{R}) \times M_n(\mathbb{R}) \mapsto M_n(\mathbb{R}), \qquad (A, B) \mapsto A + B$$

*και*

$$M_n(\mathbb{R}) \times M_n(\mathbb{R}) \mapsto M_n(\mathbb{R}), \qquad (A, B) \mapsto A \cdot B.$$

*Οι παραπάνω αντιστοιχίες είναι πράξεις.*

**Ορισμός 2.1.3.** *Έστω* $\mathbb{R}$ *ένα σύνολο με τις εξής πράξεις.*

$$R \times R \mapsto R, \qquad (a, b) \mapsto a + b,$$

$$R \times R \mapsto R, \qquad (a, b) \mapsto a \cdot b,$$

*Με τις πράξεις αυτές θα λέμε ότι το* $R$ *είναι ένας δακτύλιος, αν ισχύουν οι παρακάτω ιδιότητες για κάθε* $a, b, c \in R$.

(i) $(a + b) + c = a + (b + c)$ *(προσεταιριστική ιδιότητα)*

(ii) *Υπάρχει ουδέτερο στοιχείο* $0_R \in R$ *ώστε* $a+0_R = 0_R+a = a$ *(ύπαρξη ουδετέρου στοιχείου)*

(iii) *Για κάθε* $a \in R$, *υπάρχει* $a' \in R$ *ώστε* $a+a' = 0_R = a'+a$ *(ύπαρξη αντιθέτου)*

(iv) $a + b = b + a$ *(μεταθετικότητα)*

(v) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(προσεταιριστική του πολλαπλασιασμού)*

(vi) $a(b + c) = a \cdot b + a \cdot c$ *(επιμεριστική)*

(vii) $(a + b) \cdot c = a \cdot c + b \cdot c$ *(επιμεριστική)*

*Σημείωση.* Το στοιχείο $a'$ της ιδιότητας (iii) είναι μοναδικό και συμβολίζεται με $-a$ (ονομάζεται το *αντίθετο* του $a$).

**Παράδειγμα 2.1.4.** *Έστω* $\mathbb{Z}$ *με πράξεις* $a \oplus b = a - b$ *και* $a \cdot b = ab$. *Ως προς τις πράξεις αυτές το* $\mathbb{Z}$ *δεν είναι δακτύλιος. Για παράδειγμα δεν αληθεύει γενικά ότι* $a \oplus b = b \oplus a$, *για κάθε* $a, b \in \mathbb{Z}$.

**Ορισμός 2.1.5.** *Ένας δακτύλιος* $R$ *λέγεται μεταθετικός, αν για κάθε* $a, b \in R$ *ισχύει* $a \cdot b = b \cdot a$.

**Ορισμός 2.1.6.** *Αν* $R$ *δακτύλιος και υπάρχει* $1_R \in R$, *ώστε* $1_R \cdot a = a \cdot 1_R$ *για κάθε* $a \in R$, *θα λέμε ότι ο* $R$ *έχει μοναδιαίο στοιχείο (το* $1_R$*).*

**Παραδείγματα 2.1.7.** (i) *Οι* $\mathbb{Q}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$ *είναι μεταθετικοί δακτύλιοι με μοναδιαίο στοιχείο (ο αριθμός* 1*).*

(ii) *Ο* $\mathbb{Z}_n$ *είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο (το* $[1]$*).*

(iii) *Ο* $M_n(\mathbb{R})$ *είναι δακτύλιος, όχι γενικά μεταθετικός με μοναδιαίο στοιχείο το*

$$1_{M_n(\mathbb{R})} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \in M_n(\mathbb{R}).$$

(iv) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ *είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο (ως προς την πρόσθεση και τον συνήθη πολλαπλασιασμό του* $\mathbb{R}$*).*

*Παρατηρήστε ότι αν* $a, b, c, d \in \mathbb{Q}$*, τότε*

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = a + c + (b + d) \cdot \sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

*και*

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

*(αφού* $ac + 2bd, ad + bc \in \mathbb{Q}$*). Άρα πράγματι έχουμε τις πράξεις στο* $\mathbb{Q}[\sqrt{2}]$ *που λέει το παράδειγμα. Η επαλήθευση των ιδιοτήτων του ορισμού για το παράδειγμα* $\mathbb{Q}[\sqrt{2}]$ *είναι άμεση (αφού ισχύουν στο* $\mathbb{R} \supseteq \mathbb{Q}[\sqrt{2}]$*).*

(v) *Ο* $\mathbb{Z}[\imath] = \{a + b \in \mathbb{C} : a, b \in \mathbb{Z}\}$*, όπου* $\imath^2 = -1$ *είναι μεταθετικός δακτύλιος με μονάδα (το* $1$*). Όπως πριν, αν* $a, b, c, d \in \mathbb{Z}$ *έχουμε*

$$(a + b\imath) + (c + d\imath) = a + c + (b + d)\imath \in \mathbb{Z}[\imath]$$

*και*

$$(a + b\imath) \cdot (c + d\imath) = (ac - bd) + (ad + bc)\imath \in \mathbb{Z}[\imath],$$

*και άρα οι συνήθεις πράξεις της* $+$ *και του* $\cdot$ *του* $\mathbb{C}$ *δίνουν πράξεις στο* $\mathbb{Z}[\imath]$*.*

(vi) *Έστω* $V$ *ένας* $\mathbb{R}$*- διανυσματικός χώρος και ·έστω*

$$\mathcal{L}(V) = \{f : V \to V : f \text{ γραμμική}\}.$$

*Ορίζουμε δύο πράξεις στο* $\mathcal{L}(V)$*,*

$$+ : \mathcal{L}(V) \times \mathcal{L}(V) \to \mathcal{L}(V),$$

$$\cdot : \mathcal{L}(V) \times \mathcal{L}(V) \to \mathcal{L}(V).$$

*Παρατηρήστε ότι αν* $f, g \in \mathcal{L}(V)$ *και για κάθε* $v \in V$*,τότε*

$$(f + g)(v) = f(v) + g(v)$$

*και*

$$(f \circ g)(v) = f(g(v)).$$

*Εύκολα ελέγχουμε ότι ο* $\mathcal{L}(V)$ *είναι ένας δακτύλιος (όχι γενικά μεταθετικός) με μοναδιαίο στοιχείο (το* $1_v : V \to V, v \mapsto v'$*). Θα δείξουμε ότι* $f \circ (g+h) = f \circ g + f \circ h$*. Πράγματι έχουμε,*

$$\begin{aligned} f \circ (g+h)(v) &= f((g+h)(v)) = f(g(v) + h(v)) \\ &= f(g(v)) + f(h(v)) = f \circ g(v) + f \circ h(v) \\ &= (f \circ g + f \circ h)(v), \end{aligned}$$

*για κάθε* $v \in V$*. Επομένως* $f \circ (g+h) = f \circ g + f \circ h$*. Ομοίως ελέγχουμε και τις άλλες ιδιότητες.*

**Παρατήρηση 2.1.8.** *Οι* $+, \circ$ *είναι πράξεις στο* $\mathcal{L}(V)$*, γιατί (από Γραμμική Άλγεβρα) οι* $f+g, f \circ g \in \mathcal{L}(V)$*, για κάθε* $f, g \in (V)$*.*

**Πρόταση 2.1.9.** *Έστω* $R$ *ένας δακτύλιος. Τότε ισχύουν οι επόμενες ιδιότητες.*

(i) *Το* $0_R$ *είναι μοναδικό (ως προς την ιδιότητα (ii) του ορισμού 2.1.3.).*

(ii) *Για κάθε* $a \in R$*, το* $a'$ *είναι μοναδικό (ως προς την ιδιότητα (iii) του ορισμού 2.1.3.).*

(iii) *Αν* $a, b, c \in R$ *και* $a + b = a + c$*, τότε* $b = c$*.*

(iv) *Για κάθε* $a \in R$*,* $-(-a) = a$*.*

(v) $0_R \cdot a = a \cdot 0_R = 0_R$*, για κάθε* $a \in R$*.*

(vi) $-(a+b) = (-a) + (-b)$*, για κάθε* $a, b \in R$*.*

(vii) $-(a) \cdot b = a(-b) = -(ab)$*, για κάθε* $a, b \in R$*.*

(viii) $(-a)(-b) = ab$*, για κάθε* $a, b \in R$*.*

*Απόδειξη.* (i). Έστω $0_R, 0'_R$ ώστε

$$0_R + a = a + 0_R = a = 0'_R + a = a + 0'_R,$$

για κάθε $a \in R$. Για $a = 0'_R$, παίρνουμε

$$0_R + 0'_R = 0'_R \Rightarrow 0_R = 0'_R.$$

(ii). Έστω ότι υπάρχουν $a', a''$ ώστε

$$a + a' = 0_R = a + a''.$$

Τότε,

$$a'' = a'' + 0_R = a'' + (a + a') = (a'' + a) + a' = 0_R + a' = a'.$$

(iii). Έστω $a, b, c \in R$ με $a + b = a + c$. Τότε (αφού η + είναι πράξη) έχουμε

$$a' + (a + b) = a' + (a + c),$$

επομένως

$$(a' + a) + b = (a' + a) + c \Rightarrow 0_R + b = 0_R + c \Rightarrow b = c.$$

(iv). Έπεται άμεσα από την ιδιότητα (iii) του ορισμού 1.2.1.,

$$a + (-a) = (-a) + a = 0_R$$

(λόγω συμμετρίας) και την μοναδικότητα του $-(-a)$.

(v). Επειδή $0_R + 0_R = 0_R$ και ο πολλαπλασιασμός είναι πράξη, παίρνουμε

$$(0_R + 0_R) \cdot a = 0_R \cdot a \Rightarrow 0_R \cdot a + 0_R \cdot a = 0_R \cdot a + 0_R \Rightarrow 0_R a = 0_R.$$

(vi). Παρατηρήστε ότι,

$$\begin{aligned}(a + b) + ((-a) + (-b)) &= (a + b) + ((-b) + (-a)) \\ &= ((a + b) + (-b)) + (-a) \\ &= (a + (b + (-b))) + (-a) \\ &= (a + 0_R) + (-a) \\ &= a + (-a) = 0_R.\end{aligned}$$

Επομένως $-(a + b) = (-a) + (-b)$.

(v). Έχουμε,

$$\begin{aligned}a + (-a) = 0_R &\Rightarrow (a + (-a)) \cdot b = 0_R \cdot b \\ &\Rightarrow ab + (-a)b = 0_R \\ &\Rightarrow (-a)b = -(ab).\end{aligned}$$

Ομοίως δείχνουμε $a(-b) = -(ab)$.

(vi). Βάζουμε στην (v) όπου $b$ το -$b$ και χρησιμοποιούμε την ιδιότητα (iv). □

**Ορισμός 2.1.10.** *Έστω $R$ ένας δακτύλιος με μοναδιαίο στοιχείο $(1_R)$. Ένα στοιχείο $r \in R$ λέγεται αντιστρέψιμο, αν υπάρχει $r' \in R$ ώστε*

$$rr' = r'r = 1_R.$$

*Θα λέμε ότι το $r'$ είναι το αντίστροφο του $r$ (συμβολίζουμε με $r' = r^{-1}$). Το σύνολο των αντιστρέψιμων στοιχείων του $R$ συμβολίζεται με $U(R)$.*

**Παρατήρηση 2.1.11.** *Αν το $r \in R$ είναι αντιστρέψιμο, τότε το $r' \in R$ του προηγούμενου ορισμού είναι μοναδικό.*

*Πράγματι, έστω*

$$r \cdot r' = r' \cdot r = 1_R \qquad \text{και} \qquad r \cdot r'' = r'' \cdot r = 1_R \qquad (r, r', r'' \in R).$$

*Τότε έχουμε,*

$$r'' = 1_R \cdot r'' = (r'r) \cdot r'' = r'(rr'') = r'(1_R) = r'.$$

□

**Παραδείγματα 2.1.12.** (i) $U(\mathbb{Z}) = \{1, -1\}$, $U(\mathbb{R}) = \mathbb{R} \setminus \{0\}$.

(ii) $U(\mathbb{Z}_n) = \{[a] \in \mathbb{Z}_n : \mu\kappa\delta(a, n) = 1\}$. *Για παράδειγμα,* $U(\mathbb{Z}_{10}) = \{[1], [3], [7], [9]\}$.

**Παράδειγμα 2.1.13.** *Ισχύει ότι*

$$U(\mathbb{Z}[\imath]) = \{1, -1, \imath - \imath\},$$

*όπου*

$$\mathbb{Z}[\imath] = \{a + b\imath : a, b \in \mathbb{Z}\}.$$

*Πράγματι, προφανώς*

$$\{1, -1, \imath - \imath\} \subseteq U(\mathbb{Z}[\imath]).$$

*(Για παράδειγμα $\imath(-\imath) = 1$, δηλαδή το $\pm\imath$ είναι αντιστρέψιμο.) Έστω $a + b\imath \in U(\mathbb{Z}[\imath])$, όπου $a, b \in \mathbb{Z}$. Τότε υπάρχουν $c, d \in \mathbb{Z}$ ώστε $(a + b\imath)(c + d\imath) = 1$. Παίρνοντας μέτρα μιγαδικών έχουμε,*

$$\begin{aligned} |(a + b\imath)| \cdot |(c + d\imath| &= 1 \Rightarrow \\ |(a + b\imath)|^2 \cdot |(c + d\imath|^2 &= 1 \Rightarrow \\ (a^2 + b^2)(c^2 + d^2) &= 1. \end{aligned}$$

*Επομένως $a^2 + b^2 = 1$ (αφού $a^2 + b^2, c^2 + d^2 \in \mathbb{Z}_{>0}$). Αφού $a^2 + b^2 = 1$ και $a, b \in \mathbb{Z}$ έχουμε*

$$a = \pm 1 \qquad \text{και} \qquad b = 0$$

*ή*

$$a = 0 \qquad \text{και} \qquad b = \pm 1.$$

*Άρα $a + b\imath = \pm 1, \pm\imath$.* □

**Παράδειγμα 2.1.14.** *Ισχύει ότι*

$$U(\mathbb{Q}[\sqrt{2}]) = \mathbb{Q}[\sqrt{2}] \setminus \{0\},$$

*όπου*

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

*Παρατηρήστε πρώτα ότι αν* $a, b \in \mathbb{Q}$ *τότε* $a + b\sqrt{2} = 0$ *αν και μόνο αν* $a = b = 0$. *Πράγματι, αν* $a + b\sqrt{2} = 0$, *με* $b \neq 0$, *τότε* $\sqrt{2} = -\frac{a}{b} \in \mathbb{Q}$, *το οποίο είναι άτοπο* ($\sqrt{2} \notin \mathbb{Q}$).

*Έστω* $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ *με* $a + b\sqrt{2} \neq 0$. *Αρκεί να δείξουμε ότι το* $a + b\sqrt{2}$ *είναι αντιστρέψιμο. Πράγματι έχουμε,*

$$\begin{aligned} \frac{1}{a+b\sqrt{2}} &= \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2} \\ &= \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}], \end{aligned}$$

*αφού* $a^2 - 2b^2 \neq 0$ *(αν* $a^2 - 2b^2 = 0$ *το* $\sqrt{2}$ *θα ήταν ρητός, το οποίο είναι άτοπο) και* $a, b, a^2 - 2b^2 \in \mathbb{Q}$. □

**Ορισμός 2.1.15.** *Έστω* $R$ *ένας δακτύλιος. Ο* $R$ *λέγεται περιοχή (ή ακεραία περιοχή) αν,*

(i) *ο* $R$ *είναι μεταθετικός,*

(ii) *ο* $R$ *έχει μοναδιαίο στοιχείο* $1_R \neq 0_R$ *και*

(iii) *αν για κάθε* $a, b \in 0_R$, *με* $ab = 0_R$, *ισχύει* $a = 0_R$ *ή* $b = 0_R$.

**Παραδείγματα 2.1.16.** (i) *Οι* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *είναι ακεραίες περιοχές.*

(ii) *Οι* $\mathbb{Z}[i]$ *και* $\mathbb{Q}[\sqrt{2}]$ *(από πριν) είναι ακεραίες περιοχές.*

(iii) *Ο* $\mathbb{Z}_{[6]}$ *δεν είναι ακεραία περιοχή. Πράγματι στο* $\mathbb{Z}_6$ *έχουμε* $[2][3] = [6] = [0]$, *ενώ* $[2] \neq 0$ *και* $[3] \neq 0$.

(iv) *Έστω* $F(\mathbb{R}, \mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \ \ \textit{συνάρτηση}\}$. *Ορίζουμε,*

$$+ : F(\mathbb{R}, \mathbb{R}) \times F(\mathbb{R}, \mathbb{R}) \to F(\mathbb{R}, \mathbb{R}),$$

*με*

$$(f, g) \mapsto f + g, \ (f + g)(x) = f(x) + g(x)$$

*και*

$$+ : F(\mathbb{R}, \mathbb{R}) \times F(\mathbb{R}, \mathbb{R}) \to F(\mathbb{R}, \mathbb{R}),$$

*με*

$$(f, g) \mapsto f \times g, \ (fg)(x) = f(x)g(x).$$

*Ο* $F(\mathbb{R}, \mathbb{R})$ *είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο το* $1 : \mathbb{R} \to \mathbb{R}, \ x \mapsto 1$. *Όμως ο* $F(\mathbb{R}, \mathbb{R})$ *δεν είναι ακεραία περιοχή, αφού μπορούμε να βρούμε* $f, g : \mathbb{R} \to \mathbb{R}$ *συνεχείς με* $f, g \neq 0$ *και* $f \cdot g = 0$.

**Πρόταση 2.1.17.** *Έστω* $n \in \mathbb{N}$. *Τότε* $\mathbb{Z}_n$ *είναι ακεραία περιοχή αν και μόνο αν ο* $n$ *είναι πρώτος ή* $n = 0$.

*Απόδειξη.* Έστω ότι $\mathbb{Z}_n$ είναι ακεραία περιοχή. Τότε $n \neq 1$ (γιατί $\mathbb{Z}_1 = \{[0]\}$ δεν είναι ακεραία περιοχή). Έστω λοιπόν $n > 1$ και έστω $n = ab$, $a, b \in \mathbb{N}$. Τότε, $[n] = [ab]$, δηλαδή $[0] = [a][b]$. Επειδή $\mathbb{Z}_n$ ακεραία περιοχή, έχουμε $[a] = [0]$ ή $[b] = [0]$, δηλαδή $n|a$ ή $n|b$. Άρα $n = a$ ή $n = b$, οπότε ο $n$ είναι πρώτος.

Αντίστροφα, έστω $n = [0]$. Τότε $\mathbb{Z}_0 = \mathbb{Z}$ που είναι ακεραία περιοχή. Υποθέτουμε τώρα ότι ο $n$ είναι πρώτος. Τότε $n > 1$, άρα $[1] \neq [0]$. Ο $\mathbb{Z}_n$ είναι μεταθετικός δακτύλιος και έστω $[a][b] = [0]$, $(a, b \in \mathbb{Z})$. Τότε,

$$[ab] = [0] \Rightarrow n|ab$$

και αφού ο $n$ είναι πρώτος έπεται ότι $n|a$ ή $n|b$, δηλαδή $[a] = [0]$ ή $[b] = [0]$. □

**Ορισμός 2.1.18.** *Ένας δακτύλιος $R$ λέγεται σώμα αν,*

(i) *ο $R$ είναι μεταθετικός,*

(ii) *υπάρχει μοναδιαίο στοιχείο $1_R \neq 0_R$,*

(iii) *κάθε $r \in R$, $r \neq 0$ είναι αντιστρέψιμο.*

**Πρόταση 2.1.19.** *Κάθε σώμα είναι ακεραία περιοχή.*

*Απόδειξη.* Πράγματι, έστω $ab = 0_R$ $(a, b \in R)$ και $a \neq 0$. Τότε υπάρχει το $a^{-1} \in R$ (αντίστροφο του $a$). Παρατηρήστε ότι,

$$a^{-1}(ab) = 0_R \Rightarrow (a^{-1} \cdot a) \cdot b = 0_R \Rightarrow 1_R b = 0_r \Rightarrow b = 0_R.$$

□

**Παραδείγματα 2.1.20.** (i) *Τα $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ είναι σώματα, ενώ το $\mathbb{Z}$ δεν είναι σώμα.*

(ii) *$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \in R : a, b \in \mathbb{Q}\}$ είναι σώμα. (Από το παράδειγμα 2.1.14. έχουμε $U(\mathbb{Q}[\sqrt{2}]) = \mathbb{Q}[\sqrt{2}] \setminus \{0\}$.)*

**Πρόταση 2.1.21.** *Έστω $n \in \mathbb{N}$. Τότε $\mathbb{Z}_n$ είναι σώμα αν και μόνο αν ο $n$ είναι πρώτος.*

*Απόδειξη.* Έστω $\mathbb{Z}_n$ σώμα. Τότε $n \neq 0$ ($\mathbb{Z}_0 = \mathbb{Z}$ δεν είναι σώμα) και $n \neq 1$ ($\mathbb{Z}_1 = \{[0]\}$ δεν είναι σώμα). Από την παρατήρηση 2.1.19. $\mathbb{Z}_n$ είναι ακεραία περιοχή, άρα ο $n$ είναι πρώτος ή $n = 0$. Επομένως ο $n$ είναι πρώτος.

Αντίστροφα, έστω ότι ο $n$ είναι πρώτος. Τότε $n > 1$ και άρα $[1] \neq [0]$. Ο $\mathbb{Z}_n$ είναι μεταθετικός για κάθε $n$ και επειδή ο $n$ είναι πρώτος έχουμε μκδ$(\alpha, n) = 1$, για κάθε $\alpha = 1, 2, \ldots, n-1$. Επομένως τα $U(\mathbb{Z}_n) = \mathbb{Z}_n \setminus \{[0]\}$, δηλαδή $\mathbb{Z}_n$ είναι σώμα. □

**Παραδείγματα 2.1.22.** (i) *$M_n(\mathbb{R})$ δεν είναι σώμα, αν $n \geqslant 2$. Για $n = 1$, $M_n(\mathbb{R}) = \mathbb{R}$, σώμα.*

(ii) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ *είναι ακεραία περιοχή, αλλά όχι σώμα, αφού για παράδειγμα το* $1/2 \notin \mathbb{Z}[\sqrt{2}]$. *Πράγματι, αν* $a, b \in \mathbb{Z}[\sqrt{2}]$ *τότε* $a + b\sqrt{2} = 0 \Leftrightarrow a = b = 0$. *Αν* $1/2 \in \mathbb{Z}[\sqrt{2}]$, *τότε*

$$\frac{1}{2} = a + b\sqrt{2} \qquad (a, b \in \mathbb{Z}),$$

*δηλαδή*

$$2a - 1 + 2b\sqrt{2} = 0 \Rightarrow 2a - 1 = 2b = 0 \Rightarrow a = \frac{1}{2},$$

*άτοπο*

□

*Σημείωση.* Έστω $a, b, c, d \in R$. Τότε,

$$a + \big(b + (c + d)\big) = (a + c) + (c + d) = \big((a + b) + c\big) + d$$

κλπ. Το στοιχείο το συμβολίζουμε με $a + b + c + d$. Ειδικότερα, αν $a = b = c = d$ τότε θα το συμβολίζουμε με $4a$.

**Ορισμός 2.1.23.** *Έστω* $R$ *ένας δακτύλιος,* $r \in R$ *και* $m \in \mathbb{Z}$. *Ορίζουμε,*

$$mr = \begin{cases} r + r + \cdots + r \qquad (m\text{φορές}) & \text{αν } m > 0 \\ 0_R & \text{αν } m = 0 \\ (-r) + (-r) + \cdots + (-r) \qquad (-m\text{φορές}) & \text{αν } m < 0 \end{cases}$$

*Για κάθε* $r, s \in R$ *και* $m, n \in \mathbb{Z}$ *ισχύουν οι ακόλουθες ιδιότητες.*

(i) $(m + n)r = mr + nr$.

(ii) $m(nr) = (mn)r$.

(iii) $(-m)r = m(-r) = -(mr)$.

(iv) $m(r + s) = mr + ms$.

**Ορισμός 2.1.24.** *Έστω* $R$ *δακτύλιος,* $r \in R$ *και* $m \in \mathbb{Z}_{>0}$. *Ορίζουμε,*

$$r^m = r \cdot r \cdots r \ (m - \text{φορές}).$$

*Για κάθε* $r \in R$ *και* $m \in \mathbb{Z}_{>0}$ *ισχύουν οι ακόλουθες ιδιότητες.*

(i) $r^{m+n} = r^m r^n \qquad (r^0 = 1_R)$.

(ii) $(r^m)^n = r^{mn}$.

*Σημείωση.* Έστω $a, b, c, d \in R$. Τότε,

$$a + \big(b(cd)\big) = (ab)(cd) = \big((ab)c\big)d$$

κλπ. Το στοιχείο το συμβολίζουμε με $abcd$. Ειδικότερα, αν $a = b = c = d$ τότε θα το συμβολίζουμε με $a^4$.

**Παράδειγμα 2.1.25.** *Έστω $R$ δακτύλιος. Τότε ο $R$ είναι μεταθετικός αν και μόνο αν*

$$(a + b)^2 = a^2 + 2ab + b^2,$$

*για κάθε $a, b \in \mathbb{R}$.*

*Απόδειξη.* Παρατηρήστε ότι

$$(a + b)^2 = (a + b)(a + b) = a(a + b) + b(a + b) = a^2 + ab = ba + b^2.$$

Έχουμε,

$$\begin{aligned} (a + b)^2 &= a^2 + 2ab + b^2 \Leftrightarrow a^2 + ab + ab + b^2 = a^2 + 2ab + b^2 \Leftrightarrow \\ ab + ab &= 2ab \Leftrightarrow ba = ba \qquad (\text{για κάθε } a, b \in R) \end{aligned}$$

Επομένως ο $R$ είναι μεταθετικός αν και μόνο αν $(a+b)^2 = a^2+2ab+b^2$, για κάθε $a, b \in \mathbb{R}$. □

**Παράδειγμα 2.1.26.** *Έστω $R$ δακτύλιος, $a, b \in R$ και $n \in \mathbb{N}$, $n \geqslant 2$. Αν $ab = ba$, τότε*

$$(a + b)^n = a^n + \sum_{i=1}^{n-i} \binom{n}{i} a^{n-i} b^i + b^n, \tag{2.1.1}$$

*όπου*

$$\binom{n}{i} = \frac{n!}{(n-i)!i!} \qquad (\kappa! = 1 \cdot 2 \cdots (\kappa - 1) \cdot \kappa).$$

*Σημείωση.*

$$\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i} \qquad (i = 2, \ldots n-1).$$

*Απόδειξη.* Η απόδειξη θα γίνει με επαγωγή στο $n$. Πράγματι για $n = 2$, έχουμε

$$\begin{aligned} (a + b)^2 &= (a + b)(a + b) = a(a + b) + b(a + b) \\ &= a^2 + ab + ba + b^2 = a^2 + 2ab + b^2, \end{aligned}$$

όπου στην τελευταία ισότητα χρησιμοποιήσαμε το γεγονός ότι $ab = ba$, για κάθε $a, b \in R$. Έστω ότι ισχύει η (2.1.1.). Θα δείξουμε ότι ισχύει και για $n + 1$. Πράγματι από την επαγωγική υπόθεση έχουμε,

$$\begin{aligned} (a + b)^{n+1} &= (a + b)(a + b)^n \\ &= a^{n+1} + \sum_{i=1}^{n-1} \binom{n}{i} a^{n+1-i} b^i + ab^n + ba^n + \sum_{i=1}^{n-1} \binom{n}{i} a^{n-i} b^{i+1} + b^{n+1}. \end{aligned}$$

Παρατηρήστε ότι στην τελευταία σχέση, ο συντελεστής του $a^{n+1}$ είναι 1, ο συντελεστής του $a^{n+1-i}b^i$ είναι

$$\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i} \qquad (1 < i < n),$$

ο συντελεστής του $ab^n$ είναι

$$1 + \binom{n}{n-1} = 1 + n = \binom{n+1}{n},$$

ο συντελεστής του $ba^n$ είναι

$$1 + \binom{n}{1} = n + 1 = \binom{n+1}{1}$$

και ο συντελεστής του $b^{n+1}$ είναι 1. Επομένως η (2.1.1.) ισχύει για $n+1$ στην θέση του $n$. □

**Παράδειγμα 2.1.27.** *Έστω $R$ μεταθετικός δακτύλιος ώστε $3r = 0$, για κάθε $r \in R$. Τότε*

$$(r+s)^3 = r^3 + s^3,$$

*για κάθε $r, s \in R$.*

*Απόδειξη.* Πράγματι ο $R$ είναι μεταθετικός δακτύλιος και

$$\begin{aligned}(r+s)^3 &= r^3 + \binom{3}{1}r^2s + \binom{3}{2}rs^2 + s^3 \\ &= r^3 + 3r^2s + 3rs + s^3 \\ &= r^3 + s^3.\end{aligned}$$

□

### 2.1α′ Υποδακτύλιοι

**Ορισμός 2.1.28.** *Έστω $\oplus : A \times A \to A$ μια πράξη στο $A$ και έστω $B \subseteq A$. Θα λέμε ότι το $B$ είναι κλειστό ως προς την πράξη $\oplus$, αν για κάθε $b_1, b_2 \in B$ έχουμε ότι $b_1 \oplus b_2 \in B$.*

**Παρατήρηση 2.1.29.** *Αν $\oplus : A \times A \to A$ και $B \subseteq A$ κλειστό ως προς την $\oplus$ και $B \neq \emptyset$, τότε ορίζεται η πράξη $\oplus : B \times B \to B : b_1 \oplus' b_2 = b_1 \oplus b_2$. (Μπορούμε να πούμε ότι, $\oplus' =$ ο περιορισμός της $\oplus$.)*

**Παραδείγματα 2.1.30.** (i) *Ως προς την πρόσθεση και τον πολλαπλασιασμό του $\mathbb{Z}$, το σύνολο*

$$2\mathbb{Z} = \{2m : m \in \mathbb{Z}\}$$

*είναι κλειστό.*

(ii) *Ως προς τις ίδιες πράξεις το σύνολο*

$$2\mathbb{Z}+1=\{2m+1 : m\in\mathbb{Z}\}$$

*δεν είναι κλειστό ως προς την πρόσθεση, αλλά είναι κλειστό ως προς τον πολλαπλασιασμό.*

**Ορισμός 2.1.31.** *Έστω $R$ ένας δακτύλιος και $S\subseteq R$ ένα κλειστό σύνολο ως προς τις πράξεις του $R$. Αν ο $S$ είναι δακτύλιος ως προς τους περιορισμούς των πράξεων του $R$, θα λέμε ότι ο $S$ είναι ένας υποδακτύλιος του $R$.*

**Παραδείγματα 2.1.32.** (i) *Το $\mathbb{Z}$ είναι υποδακτύλιος των $\mathbb{Q},\mathbb{R},\mathbb{C}$.*

(ii) *Το $2\mathbb{Z}$ είναι υποδακτύλιος του $\mathbb{Z}$.*

(iii) *Το $\mathbb{N}$ είναι κλειστό στο $\mathbb{Z}$, αλλά δεν είναι υποδακτύλιος (δεν έχει αντίθετο).*

**Πρόταση 2.1.33.** *Έστω $S$ ένας δακτύλιος και $R\subseteq S$, $R\neq\emptyset$. Ο $R$ είναι υποδακτύλιος του $S$ αν και μόνο αν ισχύουν τα ακόλουθα.*

(i) *$a+b\in R$ για κάθε $a,b\in R$.*

(ii) *$ab\in R$ για κάθε $a,b\in R$.*

(iii) *$-a\in R$ για κάθε $a\in R$.*

*Απόδειξη.* Έστω ότι ο $R$ είναι υποδακτύλιος του $S$. Τότε οι (i) και (ii) ισχύουν από τον ορισμό. Παρατηρήστε ότι $0_R=0_S$. Πράγματι, αν $a\in R$, τότε

$$a+0_R=a \qquad \text{και} \qquad a+0_S=a.$$

Επομένως

$$a+0_s=a+0_R\Rightarrow 0_s=0_R,$$

όπου το τελευταίο βήμα έπεται από τον νόμο της διαγραφής. Τώρα για κάθε $a\in R$ έχουμε,

$$(a)+(-a)=0_S\Rightarrow (a)+(-a)=0_R,$$

άρα $(-a)\in R$.

Αντίστροφα έστω ότι ισχύουν οι (i),(ii) και (iii). Τότε από τις (i) και (ii) ο $R$ είναι κλειστός ως προς τις πράξεις του $S$. Ας δούμε την ύπαρξη του $0_R$. Αφού $R\neq\emptyset$ υπάρχει $a\in R$, οπότε από την (iii) -$a\in R$. Επομένως από την (i) $a+(-a)\in R$. Άρα $0_S\in R$. Θέτουμε $0_R=0_S$. Τότε για κάθε $a\in R$ έχουμε,

$$a+(-a)=(-a)+a=0_R.$$

Η ύπαρξη του $(-a)$ στο $R$ έπεται άμεσα από την (iii). Οι υπόλοιπες ιδιότητες του ορισμού του δακτυλίου ισχύουν στον $R$, αφού ισχύουν στον $S$ και $R\subseteq S$. □

**Πρόταση 2.1.34.** *Έστω $S$ ένας δακτύλιος και $R \subseteq S$, $R \neq \emptyset$. Ο $R$ είναι υποδακτύλιος του $S$ αν και μόνο αν για κάθε $a, b \in R$ ισχύουν ότι $a - b \in R$ και $ab \in R$.*

*Απόδειξη.* Έστω $a \in R$. Τότε $a - a \in R$, άρα $0 \in R$. Τότε $0 - a \in R$, άρα $-a \in R$. Επίσης αν $a, b \in R$, τότε

$$a - b \in R \Rightarrow a - (-b) \in R \Rightarrow a + b \in R.$$

Από την πρόταση (2.1.33.), ο $R$ είναι υποδακτύλιος του $S$. □

### Ασκήσεις

**1**. Το

$$\mathbb{Z}[\imath] = \{a + b\imath : a, b \in \mathbb{Z}\}$$

(ακέραιοι του Gauss) είναι υποδακτύλιος του $\mathbb{C}$.

*Απόδειξη.* Έστω $a, b, c, d \in \mathbb{Z}$. Τότε έχουμε,

$$(a + b\imath) - (c + d\imath) = (a - c) + (b - d)\imath \in \mathbb{Z}[\imath]$$

και

$$(a + b\imath)(c + d\imath) = (ac - bd) + (ab + bc)\imath \in \mathbb{Z}[\imath].$$

Επίσης $\mathbb{Z}[\imath] \neq \emptyset$, συνεπώς $\mathbb{Z}[\imath]$ είναι υποδακτύλιος του $\mathbb{C}$. □

**2**. Το

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$$

είναι υποδακτύλιος του $\mathbb{R}$.

*Απόδειξη.* Πράγματι, $\mathbb{Z}[\sqrt{2}] \neq \emptyset$. Έστω $a, b, c, d \in \mathbb{Z}$. Τότε έχουμε,

$$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

και

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ab + bc)\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

Επομένως $\mathbb{Z}[\sqrt{2}]$ είναι υποδακτύλιος του $\mathbb{R}$. □

**3**. Το

$$R = \{a + b^3\sqrt{2} : a, b \in \mathbb{Z}\}$$

δεν είναι υποδακτύλιος του $\mathbb{R}$.

*Απόδειξη.* Πράγματι, δεν είναι υποδακτύλιος του $\mathbb{R}$, διότι δεν είναι κλειστό ως προς τον πολλαπλασιασμό. Ειδικότερα, $\sqrt[3]{2} \in R$, αλλά $(\sqrt[3]{2})(\sqrt[3]{2}) = \sqrt[3]{4} \notin R$. □

**4**. Εξετάστε αν το $S = \{[0], [4], [8]\}$ είναι υποδακτύλιος του $\mathbb{Z}_{12}$.

*Απόδειξη.* Εύκολα επαληθεύουμε με πράξεις ότι $[a] - [b] \in S$ και $[a][b] \in S$ για κάθε $[a], [b] \in S$. Επίσης έχει μοναδιαίο στοιχείο το $[4]$ ($1_S = [4]$). □

**Παρατηρήσεις 2.1.35.** *Έστω $S$ υποδακτύλιος του $R$.*

*(i)* $0_S = 0_R$ *(το είδαμε στην απόδειξη της πρότασης 2.1.33.).*

*(ii) Αν οι $S$ και $R$ έχουν μοναδιαία στοιχεία, δεν είναι απαραίτητο ότι* $1_R = 1_S$ *(για παράδειγμα στην άσκηση 4,* $1_S \neq 1_{\mathbb{Z}_{12}}$*).*

*(iii) Αν το $a \in S$ είναι αντιστρέψιμο στο $S$, δεν είναι απαραίτητα ότι το $a \in R$ είναι αντιστρέψιμο (για παράδειγμα στην άσκηση 4, $a = [4] \in S$).*

*(iv) Είναι δυνατόν ο $R$ να έχει μοναδιαίο στοιχείο και ο $S$ να μην έχει μοναδιαίο στοιχείο. Για παράδειγμα, $R = \mathbb{Z}$ και $S = 2\mathbb{Z}$.*

*(v) Έστω ότι οι $R$ και $S$ έχουν μοναδιαία στοιχεία και ότι $1_R = 1_S$. Αν το $S$ είναι αντιστρέψιμο στον $S$, τότε το $s \in R$ είναι αντιστρέψιμο και τα δύο αντίστροφα στοιχεία ταυτίζονται.*

**5**. Έστω $R = M_2(R)$ και

$$S = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & \alpha \end{pmatrix} : \alpha \in \mathbb{R} \right\}.$$

Εξετάστε αν ο $S$ είναι υποδακτύλιος του $R$.

*Απόδειξη.* $S \neq \emptyset$. Παρατηρήστε ότι,

$$\begin{pmatrix} 0 & 0 \\ 0 & \alpha \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & \beta \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & \alpha - \beta \end{pmatrix} \in S$$

και

$$\begin{pmatrix} 0 & 0 \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & \beta \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & \alpha\beta \end{pmatrix} \in S.$$

Επομένως ο $S$ είναι υποδακτύλιος του $M_2(\mathbb{R})$. Ο $S$ είναι μεταθετικός με μοναδιαίο στοιχείο το

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

Παρατηρήστε ότι,

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \notin U(M_2(\mathbb{R}))$$

αλλά

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in U(S).$$

**6**. Έστω

$$R = \left\{ \frac{m}{2^a 3^b} \in \mathbb{Q} : m \in \mathbb{Z}, a, b \in \mathbb{N} \right\}.$$

(i) Να δείξετε ότι ο $R$ είναι υποδακτύλιος του $\mathbb{Q}$.

(ii) Να δείξετε ότι ο $R$ περιέχεται σε κάθε υποδακτύλιο του $\mathbb{Q}$ που περιέχει τα $\frac{1}{2}$ και $\frac{1}{3}$.

(iii) Αληθεύει ότι ο $R$ είναι σώμα;

*Απόδειξη.* (i). Παρατηρήστε ότι το $0 \in R$, άρα $R \neq \emptyset$. Έστω $m \in \mathbb{Z}, a, b, c, d \in \mathbb{N}$. Τότε,

$$\frac{m}{2^a \cdot 3^b} - \frac{n}{2^c \cdot 3^b} = \frac{m2^c 3^d - n2^a 3^b}{2^{a+c} 3^{b+d}} \in R$$

και

$$\frac{m}{2^a \cdot 3^b} \cdot \frac{n}{2^c \cdot 3^b} = \frac{mn}{2^{a+c} 3^{b+d}} \in R.$$

Άρα ο $R$ είναι υποδακτύλιος του $\mathbb{Q}$.

(ii). Έστω $S$ υποδακτύλιος του $\mathbb{Q}$ ώστε $\frac{1}{2}, \frac{1}{3} \in S$. Τότε αφού ο $S$ είναι υποδακτύλιος και επειδή $1 = \frac{1}{2} + \frac{1}{2}$, έπεται ότι το $1 \in S$, άρα και $-1 \in S$. Επομένως κάθε στοιχείο της μορφής

$$\pm 1 \pm 1 \cdots \pm 1 \in S.$$

Άρα $\mathbb{Z} \subseteq S$. Επίσης επειδή ο $S$ είναι κλειστός ως προς τον πολλαπλασιασμό έχουμε

$$\frac{1}{2^a} = \left(\frac{1}{2}\right)^a \in S \qquad \text{και} \qquad \frac{1}{3^b} = \left(\frac{1}{3}\right)^b \in S$$

για κάθε $(a, b) \in \mathbb{N}$. (Αν $a = 0$, $\left(\frac{1}{2}\right)^0 = 1 \in S$.) Επομένως,

$$m = \frac{1}{2^a} \frac{1}{3^b} \in S$$

(από την κλειστότητα του πολλαπλασιασμού του $S$). Δηλαδή $R \subseteq S$.

(iii). Θα δείξουμε ότι ο $R$ δεν είναι σώμα. Παρατηρήστε ότι το $5 \in R$ ($m = 5, a = b = 0$). Αρκεί να δείξουμε ότι το 5 δεν είναι αντιστρέψιμο στον $R$. Πράγματι, ας υποθέσουμε ότι είναι αντιστρέψιμο. Τότε το αντίστροφό του στον $R$ είναι ίσο με $\frac{1}{5}$ (γιατί το 5 είναι αντιστρέψιμο και στο $\mathbb{Q}$). Ο $R$ είναι υποδακτύλιος του $\mathbb{Q}$ και $1_R = 1_{\mathbb{Q}} = 1$. Επομένως,

$$\frac{1}{5} = \frac{m}{2^a 3^b} \qquad (m \in \mathbb{Z}, a, b \in \mathbb{N}).$$

Τότε έχουμε,

$$5m = 2^m \cdot 3^b \overset{(5 \text{ πρώτος})}{\Longrightarrow} 5|2^a \qquad \text{ή} \qquad 5|3^b,$$

άτοπο. □

**7**. Έστω $n \in \mathbb{Z}_{>0}$ και

$$T_2(\mathbb{Z}_n) = \left\{ A \in M_2(\mathbb{Z}_n) : A = \begin{pmatrix} [a] & [b] \\ [0] & [c] \end{pmatrix} \right\}.$$

(i) Να δείξετε ότι ο $T_2(\mathbb{Z}_n)$ είναι υποδακτύλιος του $M_2(\mathbb{Z}_n)$.

(ii) Αληθεύει ότι ο $T_2(\mathbb{Z}_n)$ είναι μεταθετικός;

(iii) Να δείξετε ότι

$$|U(T_2(\mathbb{Z}_n)| = n \cdot \varphi(n)^2,$$

όπου $\varphi$ η συνάρτηση του Euler.

*Απόδειξη.* (i). Όπως και στις προηγούμενες ασκήσεις, λόγω της πρότασης 2.1.34.,εύκολα δείχνουμε ότι ο $T_2(\mathbb{Z}_n)$ είναι υποδακτύλιος του $M_2(\mathbb{Z}_n)$.

(ii). Παρατηρήστε ότι,

$$\begin{pmatrix} [2] & [3] \\ [0] & [4] \end{pmatrix} \begin{pmatrix} [1] & [2] \\ [0] & [3] \end{pmatrix} = \begin{pmatrix} [2] & [13] \\ [0] & [12] \end{pmatrix}$$

και

$$\begin{pmatrix} [1] & [2] \\ [0] & [3] \end{pmatrix} \begin{pmatrix} [2] & [3] \\ [0] & [4] \end{pmatrix} = \begin{pmatrix} [2] & [11] \\ [0] & [12] \end{pmatrix}.$$

Προφανώς,

$$\begin{pmatrix} [2] & [13] \\ [0] & [12] \end{pmatrix} \neq \begin{pmatrix} [2] & [11] \\ [0] & [12] \end{pmatrix},$$

άρα ο $T_2(\mathbb{Z}_n)$ δεν είναι μεταθετικός.

(iii). Έστω

$$A = \begin{pmatrix} [a] & [b] \\ [0] & [c] \end{pmatrix} \in M_2(\mathbb{Z}_n).$$

Τότε $A \in U\left(M_2(\mathbb{Z}_n)\right)$ αν και μόνο αν υπάρχει $B \in U\left(M_2(\mathbb{Z}_n)\right)$, ώστε

$$AB = BA = \begin{pmatrix} [1] & [0] \\ [0] & [1] \end{pmatrix}.$$

Δηλαδή υπάρχουν $x, y, z \in \mathbb{Z}$ ώστε

$$\begin{pmatrix} [a] & [b] \\ [0] & [c] \end{pmatrix} \begin{pmatrix} [x] & [y] \\ [0] & [z] \end{pmatrix} = \begin{pmatrix} [1] & [0] \\ [0] & [1] \end{pmatrix}.$$

Επομένως

$$\begin{pmatrix} [ax] & [ay+bz] \\ [0] & [cz] \end{pmatrix} = \begin{pmatrix} [1] & [0] \\ [0] & [1] \end{pmatrix}.$$

Έπεται ότι,

$$[ax] = [cz] = [1],$$

δηλαδή

$$[a][x] = [c][z] = 1.$$

Επομένως $[a], [c] \in U(\mathbb{Z}_n)$. Παρατηρήστε ότι αν $[a], [c] \in U(\mathbb{Z}_n)$, τότε επιλέγοντας

$$B = \begin{pmatrix} [a'] & [y] \\ [0] & [c'] \end{pmatrix},$$

όπου $[y] = -[a'][c'][b]$, $[a']$ το αντίστροφο του $[a]$ και $[c']$ το αντίστροφο του $[c]$ στο $\mathbb{Z}_n$, εύκολα ελέγχουμε με πράξεις ότι

$$AB = BA = \begin{pmatrix} [1] & [0] \\ [0] & [1] \end{pmatrix}.$$

Επομένως,

$$A = \begin{pmatrix} [a] & [b] \\ [0] & [c] \end{pmatrix} \in U(M_2(\mathbb{Z}_n)) \qquad \Leftrightarrow \qquad [a], [c] \in U(\mathbb{Z}_n) \qquad \text{και} \qquad [b] \qquad \text{τυχαίο.}$$

Επομένως,

$$|U(M_2(\mathbb{Z}_n)| = |U(\mathbb{Z}_n)|^2 \cdot |\mathbb{Z}_n| = \varphi(n)^2 \cdot n.$$

□

**8**. Έστω $R$ ένας δακτύλιος και έστω $r \in R$. Το $r$ λέγεται *μηδενοδύναμο*, αν $r^m = 0$ για κάποιο $m \in \mathbb{Z}_{>0}$.

(i) Να βρείτε τα μηδενοδύναμα στοιχεία του $\mathbb{Z}_{30}$ και του $\mathbb{Z}_{60}$.

(ii) Να δείξετε ότι ο $\mathbb{Z}_n$, $n > 1$ δεν έχει μη μηδενικό μηδενοδύναμο στοιχείο αν και μόνο αν το $n$ δεν διαιρείται με το τετράγωνο πρώτου.

(ii) Έστω $R$ ένας μεταθετικός δακτύλιος. Τότε το σύνολο των μηδενοδύναμων στοιχείων του $R$ είναι υποδακτύλιος του $\mathbb{R}$.

*Απόδειξη.* (i). Έστω $[a] \in \mathbb{Z}_{30}$ με $[a]^m = 0$, για κάποιο $m \in \mathbb{Z}_{>0}$. Τότε $[a^m] = [0]$, δηλαδή $30|a^m$. Αφού $30 = 2 \cdot 3 \cdot 5$, έχουμε

$$2|a^m,\ 3|a^m,\ 5|a^m.$$

Αφού $2, 3, 5$ είναι πρώτοι, έχουμε

$$2|a,\ 3|a,\ 5|a.$$

Έπεται ότι $30|a$ (αφού $2, 3, 5$ είναι σχετικά πρώτοι). Τότε $[a] = [0]$, άρα στο $\mathbb{Z}_{30}$ υπάρχει μοναδικό μηδενοδύναμο στοιχείο, το $[0]$.

Έστω τώρα $[a] \in \mathbb{Z}_{60}$ με $[a]^m = 0$, για κάποιο $m \in \mathbb{Z}_{>0}$. Τότε $[a^m] = [0]$, δηλαδή $60|a^m$. Αφού $60 = 2^2 \cdot 3 \cdot 5$, έχουμε

$$2|a^m,\ 3|a^m,\ 5|a^m.$$

Αφού $2, 3, 5$ είναι πρώτοι, έχουμε

$$2|a,\ 3|a,\ 5|a.$$

Έπεται ότι $30|a$ (αφού $2, 3, 5$ είναι σχετικά πρώτοι). Άρα $[a] = [0]$ ή $[a] = [30]$ (στο $\mathbb{Z}_{60}$). Παρατηρήστε ότι το $[30]$ είναι μηδενοδύναμο ($[30]^2 = [900] = [0]$). Άρα υπάρχουν ακριβώς δύο μηδενοδύναμα στοιχεία στο $\mathbb{Z}_{60}$, το $[0]$ και το $[30]$.

(ii). Έστω ότι ο $\mathbb{Z}_n$, $n > 1$ δεν έχει μη μηδενικό μηδενοδύναμο στοιχείο. Έστω

$$n = p_1^{n_1} \cdots p_\kappa^{n_\kappa},$$

η ανάλυση του $n$ σε γινόμενο πρώτων παραγόντων και έστω

$$\alpha = p_1 p_2 \cdots p_\kappa$$

και

$$N = \max\{n_1, \cdots n_\kappa\}.$$

Παρατηρήστε ότι

$$[\alpha]^N = [\alpha^N] = [0],$$

αφού $n|\alpha^N$. Από την υπόθεση έχουμε $[\alpha] = [0]$, δηλαδή $n|\alpha$. Άρα

$$n = \alpha = p_1^{n_1} \cdots p_\kappa^{n_\kappa}.$$

Αντίστροφα, έστω ότι δεν υπάρχει πρώτος $p$ ώστε $p^2|n$. Τότε η ανάλυση του $n$ σε γινόμενο πρώτων είναι $n = p_1 p_2 \cdots p_\kappa$ ($p_i$ διακεκριμμένοι πρώτοι). Έστω $[\alpha] \in \mathbb{Z}_n$ ώστε $[\alpha]^m = [0]$. Τότε

$$[\alpha^m] = [0] \Rightarrow n|\alpha^m \Rightarrow p_i|\alpha,$$

για κάθε $i$. Επειδή οι $p_1, p_2, \ldots, p_n$ είναι ανά δύο σχετικά πρώτοι, έπεται ότι

$$p_1 p_2 \cdots p_n|\alpha.$$

Άρα $[n]|\alpha$, δηλαδή $[\alpha] = [0]$.

(iii). Έστω $r, s \in R$ με $r^m = s^n = 0$ για κάποια $m, n \in \mathbb{Z}_{>0}$. Έστω

$$N(R) = \{x \in R : x^\kappa = 0,\ \text{για κάποιο}\ \kappa \in \mathbb{Z}_{>0}\}.$$

Προφανώς $N(R) \neq \emptyset$, αφού $0_R \in N(R)$. Θα δείξουμε ότι $rs \in N(R)$. Πράγματι έχουμε,

$$(rs)^m = r^m s^m = 0_R \cdot s^m = 0_R,$$

όπου στην πρώτη ισότητα χρησιμοποιήσαμε το γεγονός ότι ο $R$ είναι μεταθετικός. Επίσης $-r \in N(R)$. Πράγματι,

$$(-r)^m = (-1)^m \cdot r^m = 0_R.$$

Τέλος θα δείξουμε ότι $r+s \in N(R)$. Επειδή ο $R$ είναι μεταθετικός, έχουμε

$$(r+s)^{m+n} = r^{m+n} + \sum_{i=1}^{m+n-1} \binom{m+n}{i} r^{m+n-i} \cdot s^i + s^{m+n}. \tag{2.1.2}$$

Παρατηρήστε ότι,

$$r^{m+n} = r^m \cdot r^n = 0 \cdot r^n = 0$$

και

$$s^{m+n} = s^m \cdot s^n = s^m \cdot 0 = 0.$$

Επίσης αν $i \geqslant n$, τότε

$$r^{m+n-i} \cdot s^i = r^{m+n-i} \cdot 0 = 0.$$

Αν $i \leqslant n$, τότε $m+n-i \geqslant m$ και

$$r^{m+n-i} \cdot s^i = 0 \cdot s^i = 0.$$

Επομένως από την (2.1.2) έπεται ότι $(r+s)^{m+n} = 0$, οπότε $r+s \in N(R)$. Η απόδειξη είναι πλήρης. □

## 2.2 Πολυώνυμα και πολυωνυμικές συναρτήσεις

**Πρόταση 2.2.1.** *Έστω $R$ δακτύλιος με $1_R$. Τότε υπάρχει δακτύλιος $\overline{R}$ με $1_{\overline{R}} = 1_R$, ώστε*

(i) *Ο $R$ είναι υποδακτύλιος του $\overline{R}$.*

(ii) *Υπάρχει $x \in \overline{R}$ ώστε $rx = xr$, για κάθε $r \in R$.*

(iii) *Κάθε στοιχείο του $\overline{R}$ έχει μια παράσταση της μορφής*

$$r_0 + r_1 x + r_2 x^2 + \cdots + r_m x^m \ \ (r_i \in R).$$

(iv) *Αν*

$$r_0 + r_1 x + r_2 x^2 + \cdots + r_m x^m = s_0 + s_1 x + r_2 x^2 + \cdots + s_n x^n \ \ (r_i, s_i \in R), m \leqslant n,$$

*τότε*

$$r_0 = s_0, r_1 = s_1, \ldots, r_m = s_m, \ldots, s_{m+1} = \cdots = s_n = 0_R.$$

*Συμβολίζουμε με $\overline{R} = R[x]$.*

*(Η απόδειξη παραλείπεται.)*

**Παρατηρήσεις 2.2.2.** (i) $0_{R[x]} = 0_R$ *(αφού* $R$ *υποδακτύλιος του* $R[x]$*).*

(ii) $0_R x^\kappa = 0_R$*, για κάθε* $\kappa \in \mathbb{Z}_{>0}$*.*

(iii) *Αν* $f(x), g(x) \in R[x]$*, μπορούμε να γράψουμε*

$$f(x) = f_0 + f_1 x + \cdots + f_m x^m \ \ (f_i \in R),$$

$$g(x) = g_0 + g_1 x + \cdots + g_m x^m \ \ (g_i \in R)$$

*(όπου το* $m$ *είναι το ίδιο).*

(iv) *Οι πράξεις στον δακτύλιο* $R[x]$ *ορίζονται ως εξής. Αν* $f(x), g(x)$ *όπως πριν, τότε*

$$f(x) + g(x) = f_0 + g_0 + (f_1 + g_1)x + \cdots + (f_m + g_m)x^m.$$

*Αν* $f(x) = f_0 + f_1 x + \cdots + f_m x_m$ *και* $g(x) = g_0 + g_1 x + \cdots + g_n x^n$*, τότε*

$$f(x) \cdot g(x) = c_1 x + c_2 x^2 + \cdots c_{m+n} x^{m+n},$$

*όπου*

$$c_\kappa = \sum_{i=0}^{\kappa} f_i \cdot g_{\kappa - i}.$$

*Το γεγονός ότι οι πράξεις είναι αυτές έπεται από την προταση 2.2.1.*

(v) *Έστω* $R$ *ένας μεταθετικός δακτύλιος με μονάδα* $(1_R)$*. Τότε και ο* $R[x]$ *είναι μεταθετικός (σαφές από το (iv) ).*

**Λήμμα 2.2.3.** *Αν* $p$ *πρώτος, τότε* $p | \binom{p}{i}$*, για κάθε* $i = 1, 2, \ldots, p-1$*.*

*Απόδειξη.* Έστω $\alpha = \binom{p}{i}$, $\alpha \in \mathbb{Z}$. Παρατηρήστε ότι

$$p! = \alpha i!(p-1)!.$$

Αφού $p | p!$, έπεται

$$p | \alpha i!(p-1)!.$$

Ο $p$ είναι πρώτος, $p \nmid i!$, $p \nmid (p-i)!$, για κάθε $i = 1, 2, \ldots, p-1$. Άρα, $p | \alpha$. □

**Λήμμα 2.2.4.** *Έστω* $p$ *πρώτος. Αν* $R$ *είναι μεταθετικός δακτύλιος ώστε* $pr = 0_R$ *για κάθε* $r \in R$*. Τότε*

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

*για κάθε* $r, s \in R$*.*

*Απόδειξη.* Αφού ο $R$ είναι μεταθετικός, παίρνουμε

$$\begin{aligned}(r+s)^p &= r^p + \sum_{i=1}^{p-1} \binom{p}{i} r^{p-i} \cdot s^i + s^p \\ &= r^p \cdot r^s,\end{aligned}$$

όπου η τελευταία ισότητα έπεται από το λήμμα 2.2.3. □

**Παράδειγμα 2.2.5.** *Έστω $p$ πρώτος. Τότε για κάθε $f(x) \in \mathbb{Z}_p[x]$ ισχύει*

$$(f(x))^p = f(x^p),$$

*δηλαδή*

$$(f_0 + f_1 x + \cdots + f_m x_m)^p = f_0 + f_1 x^p + \cdots + f_m (x^p)^m.$$

*(Στο $\mathbb{Z}_3[x]$, έχουμε $([1] + [1]x + [2]x^5)^3 = [1] + [1]x^3 + [2]x^{15}$).*

*Απόδειξη.* Από την προφανή επέκταση επέκταση του λήμματος 2.2.4, έχουμε

$$\begin{aligned}(f_0 + f_1 x + \cdots + f_m x^m)^p &= (f_0)^p + (f_1 x)^p + \cdots + (f_m x^m)^p \\ &= f_0^p + f_1^p x^p + \cdots + f_m^p (x^m)^p.\end{aligned}$$

Παρατηρήστε όμως ότι για κάθε $i$, έχουμε $f_i^p = f_i$ ($f_i \in \mathbb{Z}_p$, έπεται από το μικρό θεώρημα του Fermat). □

**Ορισμός 2.2.6.** *Έστω $R$ δακτύλιος με $1_R$. Ο δακτύλιος $R[x]$ έχει μοναδιαίο στοιχείο $1_{R[x]} = 1_R$. Δεχόμαστε ότι $x^0 = 1$. Κάθε $f(x) \in R[x]$ με $f(x) \neq 0$ γράφεται μοναδικά στην μορφή*

$$f(x) = f_0 x^0 + f_1 x^+ \cdots + f_m x^m, \;\; f_i \in R, \;\; f_m \neq 0.$$

*Αν $f(x) \neq 0$, τότε το $f_m \neq 0$ λέγεται ο μεγιστοβάθμιος συντελεστής του $f(x)$ και το $m$ λέγεται ο βαθμός του $f(x)$ (συμβολίζουμε με $m = \deg f(x)$). Αν $f(x) \neq 0$ (μηδενικό στοιχείο του $R[x]$), δεχόμαστε ότι $\deg f(x) = -\infty$, $-\infty < n$ για κάθε $n \in \mathbb{N}$ και $-\infty + n = -\infty$ για κάθε $n \in \mathbb{N}$. Για παράδειγμα, όταν λέμε $f(x) \in R[x]$, $\deg f(x) \leqslant 2$, εννοούμε ότι $f(x) = 0$ ή $f(x) \neq 0$ και $\deg f(x) = 0, 1, 2, \ldots$.*

**Πρόταση 2.2.7.** *Έστω $R$ δακτύλιος με μοναδιαίο στοιχείο και $f(x), g(x) \in R[x]$. Τότε ισχύουν τα ακόλουθα.*

(i)
$$\deg(f(x) + g(x)) \leqslant \max\{\deg f(x), \deg g(x)\}.$$

*Ειδικότερα, αν για τους μεγιστοβάθμιους όρους $f_m$ και $g_n$ των $f(x)$, $g(x)$ αντίστοιχα έχουμε $f_m x^m + g_n x^n \neq 0$, τότε ισχύει η ισότητα.*

(ii)
$$\deg(f(x)g(x)) \leqslant \deg f(x) + \deg g(x).$$
*Ειδικότερα, αν για τους μεγιστοβάθμιους όρους $f_m$ και $g_n$ των $f(x)$, $g(x)$ αντίστοιχα έχουμε $f_m \cdot g_n \neq 0$, τότε ισχύει η ισότητα.*

*Απόδειξη.* Άμεση από τον ορισμό 2.2.6. □

**Παράδειγμα 2.2.8.** *Πόσα πολυώνυμα στο $\mathbb{Z}_2[x]$ έχουν βαθμό $\leqslant 3$;*

*Λύση.* Παρατηρήστε ότι, $f(x) \in \mathbb{Z}_2[x]$, με $\deg f(x) \leqslant 3$ αν και μόνο αν
$$f(x) = f_0 + f_1 x + f_2 x^2 + f_3 x^3 \ \ (f_i \in \mathbb{Z}_2).$$
Όμως τα $f_i$ είναι μοναδικά, άρα έχουμε συνολικά $2^4$ περιπτώσεις. □

**Πρόταση 2.2.9.** *Έστω $R$ μια ακεραία περιοχή. Τότε ισχύουν τα επόμενα.*

(i) *$R[x]$ είναι ακεραία περιοχή.*

(ii) *Αν $f(x), g(x) \in R[x]$, τότε*
$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x).$$

(iii) $U(R[x]) = U(R)$.

*Απόδειξη.* (i). Γνωρίζουμε ότι ο $R[x]$ είναι δακτύλιος με $1_{R[x]} = 1_R$. Επειδή $R$ είναι ακεραία περιοχή, $1_R \neq 0_R$. Επομένως, $1_{R[x]} \neq 0_{R[x]}$. Αφού ο $R$ είναι μεταθετικός, είναι και ο $R[x]$. Έστω $f(x), g(x) \in R[x]$ με $f(x), g(x) \neq 0 (= 0_R)$. Έστω $f_m, g_m$ οι μεγιστοβάθμιοι συντελεστές των $f(x), g(x)$ αντίστοιχα. Τότε $f_m, g_n \neq 0$ και επειδή $R$ ακεραία περιοχή, έπεται $f_m \cdot g_n \neq 0$. Δηλαδή ο μεγιστοβάθμιος συντελεστής των $f(x), g(x)$ δεν είναι μηδέν. Άρα, $f(x) \cdot g(x) \neq 0$, δηλαδή $R[x]$ είναι ακεραία περιοχή.

(ii). Το είδαμε στην πρόταση (2.2.7).

(ii). Ο εγκλεισμός $U(R) \subseteq U(R[x])$ είναι προφανής, αφού ο $R$ είναι υποδακτύλιος του $R[x]$ και $1_R = 1_{R[x]}$.

Αντίστροφα, έστω $f(x) \in U(R[x])$. Τότε υπάρχει $g(x) \in U(R[x])$ ώστε,
$$\begin{aligned} f(x) \cdot g(x) &= 1 \Rightarrow \\ \deg(f(x)g(x)) &= \deg 1 \Rightarrow \\ \deg f(x) + \deg g(x) &= 0 \Rightarrow \\ \deg f(x) = \deg g(x) &= 0. \end{aligned}$$
Επομένως $f(x), g(x) \in R$ και επειδή $f(x) \cdot g(x) = 1$, έχουμε ότι $f(x) \in U(R)$. □

**Παράδειγμα 2.2.10.** *Στο $\mathbb{Z}_4[x]$ (που δεν είναι ακεραία περιοχή), έχουμε*

$$([2]x + [1])(2[x] + [1]) = [4]x^2 + [4]x + [1] = [1].$$

*Δηλαδή βρήκαμε πολυώνυμο πρώτου βαθμού, το $[2]x + [1] \in U(\mathbb{Z}_4[x])$ (που είναι αντιστρέψιμο).* □

**Παρατηρήσεις 2.2.11.** (i) *Για καθένα από τα τρία συμπεράσματα της πρότασης 2.2.9, η υπόθεση ότι $R$ είναι ακεραία περιοχή δεν μπορεί να παραληφθεί.*

*Για παράδειγμα στο $\mathbb{Z}_4[x]$, έχουμε*

$$([2]x + [1])([2]x + [1]) = [1],$$

*δηλαδή $[2][x] + [1] \in U(\mathbb{Z}_4[x])$ και $[2][x] + [1] \notin \mathbb{Z}_4$.* □

(ii) *Έστω $R$ περιοχή. Τότε δεν υπάρχει $f(x) \in R[x]$ ώστε,*

$$(x + 1)^{2011} + (x^2 + 1)^{40} = f(x)^{30}.$$

*Πράγματι,* $\deg(x + 1)^{2011} = 2011$, $\deg(x^2 + 1)^{40} = 80$. *Επομένως,*

$$\deg((x + 1)^{2011} + (x^2 + 1)^{40}) = 2011.$$

*Δηλαδή,*

$$\deg f(x)^{30} = 2011 \Rightarrow 30\deg f(x) = 2011,$$

*που είναι άτοπο (χρησιμοποιήσαμε την δεύτερη ιδιότητα της πρότασης 2.2.9).*

□

### 2.2α′ Πολυωνυμικές συναρτήσεις

**Ορισμός 2.2.12.** *Έστω $R$ δακτύλιος με $1_R$ και $f(x) \in R[x]$,*

$$f(x) = f_0 + f_1 r + \cdots f_m r^m \in R.$$

*Έτσι ορίζεται μια συνάρτηση $\bar{f} : R \to R$ με $\bar{f}(r) = f(r)$. Η $\bar{f}$ λέγεται πολυωνυμική συνάρτηση που επάγεται από το $f(x)$. Έστω $F(R, R) = \{g : R \to R\}$ (όλες οι συναρτήσεις $g : R \to R$). Συνεπώς έχουμε μια συνάρτηση $\psi : R[x] \to F(R, R)$, με $\psi(f(x)) = \bar{f}$.*

**Παρατήρηση 2.2.13.** *Η $\psi$ γενικά δεν είναι $1 - 1$.*

*Πράγματι,έστω $p$ πρώτος και $R = \mathbb{Z}_p$. Έστω $f_1(x) = x^p - x \in \mathbb{Z}_p[x]$ και $f_2(x) = 0$. Τότε για κάθε $r \in \mathbb{Z}_p$, $\bar{f}_1(r) = r^p - r = 0$ (Μικρό θεώρημα Fermat). Δηλαδή,*

$$\psi(f_1(x)) = \psi(f_2(x)), \qquad \text{αλλά} \qquad f_1(x) \neq f_2(x).$$

*Σημείωση.* Θα δούμε στην συνέχεια ότι αν το $R$ είναι άπειρο σώμα (για παράδειγμα $R = \mathbb{R}$ ή $R = \mathbb{C}$), τότε η $\psi$ είναι $1 - 1$.

## 2.3 Διαιρετότητα πολυωνύμων

**Ορισμός 2.3.1.** *Έστω $R$ δακτύλιος με $1_R$. Έστω $a(x), b(x) \in R[x]$. Θα λέμε ότι το $a(x)$ διαιρεί το $b(x)$ στο $R[x]$, αν υπάρχει $c(x) \in R[x]$ ώστε $b(x) = a(x)c(x)$. (Συμβολίζουμε με $a(x)|b(x)$.)*

**Πρόταση 2.3.2.** *Έστω $R$ μεταθετικός δακτύλιος με $1_R$. Τότε ισχύουν τα ακόλουθα.*

(i) *Αν $f(x), a(x), b(x) \in R[x]$, με $f(x)|a(x)$ και $f(x)|b(x)$, τότε*

$$f(x)|a(x)g(x) + b(x)h(x),$$

*για κάθε $g(x), h(x) \in R[x]$.*

(ii) *Αν $a(x), b(x), c(x) \in R[x]$ και $a(x)|b(x)$, $b(x)|c(x)$, τότε $a(x)|c(x)$.*

(iii) *Αν $R$ ακεραία περιοχή και $a(x), b(x) \in R[x]$ με $a(x)|b(x)$, τότε $\deg a(x) \leqslant \deg b(x)$.*

(iv) *Αν $R$ ακεραία περιοχή και $a(x), b(x) \in R[x]$ με $a(x)|b(x)$ και $b(x)|a(x)$, τότε υπάρχει $u \in U(R)$ ώστε $b(x) = ua(x)$.*

*Απόδειξη.* Τα (i),(ii) και (iii) έπονται άμεσα (το (iii) έπεται από την ιδιότητα (ii) της πρότασης 2.2.9).

(iv) Αφού $a(x)|b(x)$ και $b(x)|a(x)$ υπάρχουν $c(x), d(x) \in R[x]$, ώστε

$$b(x) = c(x)a(x) \qquad \text{και} \qquad a(x) = d(x)b(x).$$

Τότε

$$b(x) = c(x)d(x)b(x).$$

Έστω $b(x) \neq 0$. Επειδή ο $R$ είναι ακεραία περιοχή, ο $R[x]$ είναι ακεραία περιοχή, άρα $1 = c(x)d(x)$, δηλαδή $c(x) \in U(R[x])$. Τότε από την ιδιότητα (iii) της πρότασης 2.2.9 έπεται $c(x) = u \in U(R)$. Αν $b(x) = 0$, αφου $b(x)|a(x)$, έπεται $a(x) = 0$ και το ζητούμενο έπεται. □

*Σημείωση.* Αντί να γράφουμε

$$[3]x^2 - [4]x + [5] \in \mathbb{Z}_7[x],$$

θα γράφουμε απλά

$$3x^2 - 4x + 5 \in \mathbb{Z}_7[x].$$

(Δηλαδή εδώ έχουμε $3 = [3]$.)

**Ορισμός 2.3.3.** *Έστω $R$ μεταθετικός δακτύλιος με $1_R$. Ένα $p(x) \in R[x]$ θα λέγεται ανάγωγο αν $\deg p(x) \geqslant 1$ και δεν υπάρχουν $a(x), b(x) \in R[x]$ ώστε*

$$p(x) = a(x)b(x) \qquad \text{με} \qquad \deg a(x) \geqslant 1,\ \deg b(x) \geqslant 1.$$

**Παραδείγματα 2.3.4.** (i) *Αν $R$ ακεραία περιοχή, τότε κάθε $p(x) \in R[x]$ με $\deg p(x) = 1$ είναι ανάγωγο στον $R[x]$ (έπεται από τον ορισμό και από την ιδιότητα (ii) της πρότασης 2.2.9).*

(ii) *Στο $\mathbb{Z}_4[x]$ το $2x+1 \in \mathbb{Z}_4[x]$ δεν είναι ανάγωγο, γιατί*

$$2x+1 = 1 \cdot (2x+1) = (2x+1)(2x+1)(2x+1)$$

*(παράδειγμα 2.2.10).*

(iii) *Το $5x+1 \in \mathbb{Z}_6[x]$ δεν είναι ανάγωγο στο $\mathbb{Z}_6[x]$, αφού*

$$5x+1 = (2x+1)(3x+1).$$

(iv) *Το $x^2+1 \in \mathbb{R}[x]$ είναι ανάγωγο στο $\mathbb{R}[x]$, αλλά το $x^2+1 \in \mathbb{C}[x]$ δεν είναι ανάγωγο στο $\mathbb{C}[x]$, αφού*

$$x^2+1 = (x=\imath)(x-\imath).$$

(v) *Το $x^4+x^2+1 \in \mathbb{Z}_2[x]$ δεν είναι ανάγωγο στο $\mathbb{Z}_2[x]$, αφού*

$$(x^2+x+1)^2 = x^4+x^2+1.$$

(vi) *Αν $p$ πρώτος το $x^p+a \in \mathbb{Z}_p[x]$ δεν είναι ανάγωγο, αφού*

$$x^p+a = x^p+a^p = (x+a)^p,$$

*όπου στην πρώτη ισότητα χρησιμοποιήσαμε το μικρό θεώρημα του Fermat και στην δεύτερη ισότητα το λήμμα 2.2.4 για $R = \mathbb{Z}_p[x]$.*

**Θεώρημα 2.3.5.** *(Ευκλείδειος αλγόριθμος για πολυώνυμα.) Έστω $F$ σώμα και $f(x), g(x) \in F(x)$ με $g(x) \neq 0$. Τότε υπάρχουν μοναδικά $q(x), r(x) \in F(x)$ ώστε*

$$f(x) = q(x) \cdot g(x) + r(x), \quad \deg r(x) < \deg g(x).$$

*Απόδειξη.* Ύπαρξη. Έστω $\deg f(x) < \deg g(x)$. Τότε $f(x) = 0 \cdot f(x) + f(x)$.
Έστω $\deg f(x) \geqslant \deg g(x)$. Έστω

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n$$

και

$$g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_n x^n, \quad g_m \neq 0.$$

Η απόδειξη θα γίνει με επαγωγή στο $\deg f(x)$. Αν $\deg f(x) = 0$, τότε

$$f(x) = f_0 = (f_0 g_0^{-1}) g_0 + 0.$$

($g(x) = g_0$ αφού $\deg g(x) \leqslant \deg f(x)$.) Έστω ότι ισχύει η ύπαρξη για κάθε $f(x)$ με βαθμό $< n$. Έστω

$$h(x) = f(x) - x^{n-m} f_n g_m^{-1} g(x) \in F[x].$$

Στο $h(x)$ ο συντελεστής του $x^n$ είναι

$$f_n - f_n \cdot g_m^{-1} \cdot g_m = f_n - f_n = 0.$$

Άρα $\deg h(x) < n$. Από την επαγωγική υπόθεση υπαρχουν $q_1(x), r_1(x) \in F[x]$ ώστε

$$h(x) = q_1(x) \cdot g(x) + r(x), \;\; \deg r(x) < \deg g(x).$$

Άρα

$$f(x) = (x^{n-m} f_n \cdot g_m^{-1}) g(x) + r(x).$$

Μοναδικότητα. Έστω

$$f(x) = q(x)g(x) + r(x), \;\; \deg r(x) < \deg g(x)$$

και

$$f(x) = q_1(x)g(x) + r_1(x), \;\; \deg r_1(x) < \deg g(x).$$

Τότε

$$(q(x) - q_1(x))g(x) = r_1(x) - r(x).$$

Αν $q(x) - q_1(x) \neq 0$, τότε

$$\deg(r_1(x) - r(x)) = \deg(q(x) - q_1(x)) + \deg g(x) \geqslant \deg g(x),$$

το οποίο είναι άτοπο γιατί $\deg r(x) < \deg g(x)$ και $\deg r_1(x) < \deg g(x)$. □

**Παράδειγμα 2.3.6.** *Εστω $f(x), g(x) \in \mathbb{Z}_5[x]$ με $f(x) = x^4 + 4x^2 + x + 1$ και $g(x) = 2x^2 + 1$. Παρατηρήστε ότι στο $\mathbb{Z}_5$ έχουμε $2^{-1} = 3$, αφού $2 \cdot 3 = 6$ στο $\mathbb{Z}_5$ (εδώ έχουμε $2 = [2] \in \mathbb{Z}_5$). Τότε από την Ευκλείδεια διαίρεση παίρνουμε*

$$f(x) = (3x^2 + 3)g(x) + x - 2.$$

**Ορισμός 2.3.7.** (i) *Ένα πολυώνυμο $f(x) \in R[x]$ ονομάζεται μονικό αν ο μεγιστοβάθμιος συντελεστής του είναι το 1. Παρατηρήστε ότι αν το $F$ είναι σώμα και $f(x) \in F[x]$ είναι μη μηδενικό με μεγιστοβάθμιο συντελεστή $c \in F$, τότε το $c^{-1}f(x)$ είναι μονικό.*

(ii) *Έστω $F$ σώμα και $f(x), g(x) \in F[x]$, όχι και τα δύο μηδέν. Ένα μονικό πολυώνυμο $d(x) \in F[x]$ ονομάζεται μέγιστος κοινός διαιρέτης των $f(x)$ και $g(x)$ αν ικανοποιεί τις επόμενες ιδιότητες.*

*(α) $d(x)|f(x)$ και $d(x)|g(x)$ στο $F(x)$ και*

*(β) αν $c(x) \in F[x]$ με $c(x)|f(x)$ και $c(x)|g(x)$, τότε $c(x)|d(x)$.*

**Θεώρημα 2.3.8.** *Έστω $f(x), g(x) \in F(x)$ όχι και τα δύο μηδέν. Τότε υπάρχει μοναδικός μκδ των $f(x), g(x)$. Επιπλέον υπάρχουν $a(x), b(x) \in F[x]$ ώστε*

$$\mu\kappa\delta(f(x), g(x)) = a(x)f(x) + b(x)g(x).$$

*Απόδειξη.* Έστω

$$I = \{a(x)f(x) + b(x)g(x) : a(x), b(x) \in F[x]\}.$$

Τότε το $I$ περιέχει πολυώνυμα βαθμού $\geqslant 0$ (αφού $f(x) \neq 0$ ή $g(x) \neq 0$). Έστω $d(x) \in I$ με ελάχιστο βαθμό και $d(x) \neq 0$. Τότε

$$d(x) = a(x)f(x) + b(x)g(x), \tag{2.3.1}$$

όπου $a(x), b(x) \in F[x]$.

Ισχυρισμός 1. $d(x)|f(x)$ και $d(x)|g(x)$. Πράγματι από τον αλγόριθμο της Ευκλείδειας διαίρεσης υπάρχουν $q(x), r(x) \in F[x]$ ώστε

$$f(x) = q(x)d(x) + r(x), \ \ \deg r(x) < \deg d(x).$$

Επομένως

$$\begin{aligned} r(x) &= f(x) - q(x)(a(x)f(x) + b(x)g(x)) \\ &= (1 - q(x)a(x))f(x) + (-q(x)b(x))g(x). \end{aligned}$$

Αν $r(x) \neq 0$, τότε αφού $r(x) \in I$ και $\deg r(x) < \deg d(x)$ έχουμε άτοπο. Επομένως $r(x) = 0$ και άρα $d(x)|f(x)$. Ομοίως δείχνουμε ότι $d(x)|g(x)$.

Ισχυρισμός 2. Έστω $c(x)|f(x)$ και $c(x)|g(x)$. Τότε $c(x)|d(x)$. Πράγματι αφού $c(x)|f(x)$ και $c(x)|g(x)$ από την (2.3.1) έπεται ότι $c(x)|d(x)$.

Αφού $d(x) \neq 0$ για τον μεγιστοβάθμιο συντελεστή του $d_n$ έχουμε $d_n \neq 0$. Επειδή το $F$ είναι σώμα, το $d_n$ είναι αντιστρέψιμο. Αντικαθιστούμε το $d(x)$ με το $d_n^{-1}d(x)$. Παρατηρήστε ότι το $d_n^{-1}d(x)$ είναι μονικό και ικανοποιεί τους δύο ισχυρισμούς που δείξαμε παραπάνω. Επομένως το $d_n^{-1}d(x)$ ικανοποιεί τις ιδιότητες $(\alpha)$ και $(\beta)$ του ορισμού 2.3.7(ii). Επίσης

$$d_n^{-1}d(x) = (d_n^{-1}a(x)) \cdot f(x) + (d_n^{-1}b(x)) \cdot g(x).$$

Θα δείξουμε τώρα την μοναδικότητα. Έστω $d_1(x)$ και $d_2(x)$ δύο μονικά πολυώνυμα που ικανοποιούν τις ιδιότητες $(\alpha)$ και $(\beta)$ του ορισμού 2.3.7(ii). Τότε επειδή $d_1(x)|a(x)$, $d_1(x)|b(x)$ και το $d_2(x)$ είναι μέγιστος κοινός διαιρέτης, από την ιδιότητα $(\beta)$ του ορισμού 2.3.7(ii) έπεται ότι $d_1(x)|d_2(x)$. Ομοίως παίρνουμε ότι $d_2(x)|d_1(x)$. Επειδή $F$ ακεραία περιοχή υπάρχει $u \in F$, $u \neq 0$ ώστε $d_2(x) = ud_1(x)$. Αφού τα $d_1(x), d_2(x)$ είναι μονικά πολυώνυμα, έχουμε $u = 1$. Έπεται $d_2(x) = d_1(x)$. □

**Λήμμα 2.3.9.** *Έστω $F$ σώμα, $p(x), a(x), b(x) \in F[x]$ και $p(x)$ ανάγωγο. Αν $p(x)|a(x)b(x)$, τότε $p(x)|a(x)$ ή $p(x)|b(x)$.*

*Απόδειξη.* Έστω ότι $p(x) \nmid a(x)$. Επειδή ότι το $p(x)$ είναι ανάγωγο, έχουμε μκδ$(p(x), a(x)) = 1$. Από το θεώρημα 2.3.8 υπάρχουν $f(x), g(x) \in F[x]$ ώστε

$$1 = f(x)p(x) + g(x)a(x).$$

Έπεται ότι,

$$b(x) = b(x)f(x)p(x) + g(x)a(x)b(x).$$

Επειδή $p(x)|a(x)b(x)g(x)$ και $p(x)|b(x)f(x)p(x)$, έπεται ότι $p(x)|b(x)$. □

**Θεώρημα 2.3.10.** *Έστω $F$ σώμα και $f(x) \in F[x]$ θετικού βαθμού. Τότε υπάρχουν ανάγωγα πολυώνυμα $p_1(x), p_2(x), \ldots, p_n(x) \in F[x]$ ώστε*

$$f(x) = p_1(x)p_2(x)\cdots p_n(x).$$

*Έστω ότι έχουμε και την παραγοντοποίηση*

$$f(x) = q_1(x)q_2(x)\cdots q_m(x),$$

*όπου $q_i$ ανάγωγο πολυώνυμο. Τότε $m = n$ και μετά ενδεχομένως από αναδιάταξη υπάρχουν $c_i \in F \setminus \{0\}$ ώστε $q_i(x) = c_i p_i(x)$.*

*Απόδειξη.* Έστω

$$M = \{f(x) \in F[x] : \deg f(x) \geqslant 1 \text{ και το } f(x) \text{ δεν γράφεται ως γινόμενο αναγώγων}\}.$$

Έστω $M \neq \emptyset$ και έστω $f(x) \in M$ ελαχίστου βαθμού. Παρατηρήστε ότι το $f(x)$ δεν είναι ανάγωγο (αν ήταν, θα ήταν γινόμενο αναγώγων κατά τετριμμένο τρόπο), άρα

$$f(x) = a(x)b(x), \ \deg a(x) \geqslant 1, \ \deg b(x) \geqslant 1.$$

Επειδή $F$ ακεραία περιοχή,

$$\deg f(x) = \deg a(x) + \deg b(x).$$

Επομένως, $\deg a(x), \deg b(x) < \deg f(x)$, οπότε $a(x), b(x) \notin M$ . Επειδή τα $a(x), b(x)$ είναι θετικού βαθμού και $a(x), b(x) \notin M$, έπεται ότι και τα $a(x)$ και $b(x)$ είναι γινόμενο αναγώγων. Άρα το ίδιο συμβαίνει και με το $f(x) = a(x)b(x)$, που είναι άτοπο.

Ας δείξουμε τώρα την μοναδικότητα. Με τον συμβολισμό της εκφώνησης εχουμε,

$$p_1(x)p_2(x)\cdots p_n(x) = q_1(x)q_2(x)\cdots q_m(x). \tag{2.3.2}$$

Υποθέτουμε ότι $n \geqslant m$ και εφαρμόζουμε επαγωγή στο $n$. Τότε από την (2.3.2) και από το λήμμα 2.3.9, έπεται ότι $p_j(x)|q_j(x)$ για κάποιο $j$ (αφού $p_j(x)$ ανάγωγο). Έστω $p_1(x)|q_1(x)$. Αφού το $q_1(x)$ είναι ανάγωγο και $\deg p_1(x) \geqslant 1$, υπάρχει $c_i \in F \setminus \{0\}$ ώστε $q_1(x) = c_1 \cdot p_1(x)$. Επομένως

$$p_1(x)p_2(x)\cdots p_n(x) = c_1 p_1(x)q_2(x)\cdots q_m(x).$$

Άρα

$$p_2(x)\cdots p_n(x) = c_1 q_2(x)\cdots q_m(x). \tag{2.3.3}$$

Εφαρμόζοντας στην (2.3.2) την επαγωγική υπόθεση το ζητούμενο προκύπτει. □

**Ασκήσεις**

**1**. Έστω $F$ σώμα και $a(x), b(x) \in F[x]$ με μκδ$(a(x), b(x)) = 1$.

($\alpha$) Αν $a(x)|f(x)$ και $b(x)|f(x)$,τότε $a(x)b(x)|f(x)$ .

($\beta$) Αν $a(x)|b(x)f(x)$, τότε $a(x)|f(x)$.

($\gamma$)
$$\text{μκδ}(a(x)b(x), f(x)) = \text{μκδ}(a(x), f(x))\text{μκδ}(b(x), f(x)).$$

*Απόδειξη.* ($\alpha$). Αφού μκδ$(a(x), b(x)) = 1$ υπάρχουν $g(x), h(x) \in F[x]$ ώστε
$$1 = g(x)a(x) + h(x)b(x).$$

Τότε,

$$f(x) = f(x)g(x)a(x) + f(x)h(x)b(x). \tag{2.3.4}$$

Παρατηρήστε ότι $a(x)|f(x)$, $a(x)|a(x)$, $b(x)|f(x)$ και $b(x)|b(x)$. Επομένως $a(x)b(x)|f(x)$.
($\beta$). Λόγω της (2.3.4) και επειδή $a(x)|b(x)f(x)$, έπεται ότι $a(x)|f(x)$.
($\gamma$). Παρατηρήστε ότι

$$\text{μκδ}(b(x), f(x))|a(x) \qquad \text{και} \qquad \text{μκδ}(a(x), f(x))|f(x).$$

Επομένως
$$\text{μκδ}(a(x), f(x))|\text{μκδ}(a(x)b(x), f(x)).$$

Ομοίως παίρνουμε,
$$\text{μκδ}(b(x), f(x))|\text{μκδ}(a(x)b(x), f(x)).$$

Επειδή μκδ$(a(x), b(x)) = 1$, μκδ$(a(x), f(x))|a(x)$ και μκδ$(b(x), f(x))|b(x)$, έπεται ότι

$$\text{μκδ}(\text{μκδ}(a(x), f(x)), \text{μκδ}(b(x), f(x))) = 1.$$

Επομένως από το ερώτημα ($\alpha$) παίρνουμε ότι

$$\text{μκδ}(a(x), f(x)) \cdot \text{μκδ}(b(x), f(x))|\text{μκδ}(a(x)b(x), f(x)).$$

Επειδή
$$\text{μκδ}(a(x)b(x), f(x))|a(x)b(x)$$
και $a(x), b(x)$ σχετικά πρώτοι, έχουμε

$$\text{μκδ}(a(x)b(x), f(x)) = d_1(x) \cdot d_2(x),$$

όπου $d_1(x)|a(x)$ και $d_2(x)|b(x)$. Τότε, $d_1(x)|a(x)$ και $d_2(x)|f(x)$, οπότε

$$d_1(x)|\text{μκδ}(a(x), f(x)).$$

Ομοίως έχουμε

$$d_2(x)|\mu\kappa\delta(b(x), f(x)).$$

Άρα

$$d_1(x)d_2(x)|\mu\kappa\delta(a(x), f(x)) \cdot \mu\kappa\delta(b(x), f(x)).$$

□

**2**. Έστω $F$ σώμα.

($\alpha$) Να δείξετε ότι υπάρχουν άπειρα το πλήθος ανάγωγα πολυώνυμα στο $F[x]$.

($\beta$) Έστω ότι το $F$ είναι πεπερασμένο σώμα. Τότε για κάθε $n \in \mathbb{N}$ υπάρχει ανάγωγο πολυώνυμο του $F[x]$ βαθμού $\geqslant n$.

*Απόδειξη.* ($\alpha$). Η απόδειξη είναι παρόμοια με αυτήν της ύπαρξης άπειρων πρώτων στους ακεραίους (θεώρημα 1.1.8) και αφήνεται ως άσκηση.

($\beta$). Υποθέτουμε ότι υπάρχει $n \in \mathbb{N}$ ώστε κάθε ανάγωγο πολυώνυμο του $F[x]$ να έχει βαθμό μικρότερο του $n$. Επειδή το $F$ είναι πεπερασμένο σύνολο, το σύνολο

$$\{f(x) \in F[x] : \deg f(x) < n\}$$

είναι πεπερασμένο, άρα το

$$\{f(x) \in F[x] : f(x) \text{ ανάγωγο}\}$$

είναι πεπερασμένο και ας υποθέσουμε ότι είναι το

$$\{p_1(x), p_2(x), \ldots, p_m(x)\}.$$

Θέτουμε

$$P(x) = p_1(x)p_2(x)\cdots p_m(x) + 1.$$

Τότε $\deg P(x) \geqslant 1$, οπότε από το θεώρημα 2.3.10 το $P(x)$ έχει έναν ανάγωγο διαιρέτη, δηλαδή $P_i(x)|P(x)$ για κάποιο $i$. Επομένως $p_i(x)|1$, το οποίο είναι άτοπο. □

**3**. Έστω $p$ πρώτος. Ποια απεικόνιση $\mathbb{Z}_p \to \mathbb{Z}_p$ επάγει το $x^{p^n} - x \in \mathbb{Z}_p[x]$ , $n \in \mathbb{N}$;

*Λύση.* Από το μικρό θεώρημα του Fermat έχουμε $\alpha^p = \alpha$, για κάθε $\alpha \in \mathbb{Z}_p$. Επαγωγικά παίρνουμε,

$$\alpha^{p^n} = \left(\alpha^{p^{n-1}}\right)^p = \alpha^p = \alpha.$$

□

**4**. Να βρείτε όλα τα μονικά πολυώνυμα $f(x) \in \mathbb{R}[x]$ βαθμού 3 ώστε

$$\mu\kappa\delta(f(x), x^2 + 1) \neq 1 \qquad \text{και} \qquad \mu\kappa\delta(f(x), x^2 - 3x + 2) \neq 1.$$

*Λύση.* Το $x^2+1 \in \mathbb{R}[x]$ είναι ανάγωγο στο $R[x]$, άρα κάθε διαιρέτης στο $R[x]$ είναι της μορφής $c$ ή $c(x^2+1)$, όπου $c \in \mathbb{R} \setminus \{0\}$. Επομένως αφού $\mu\kappa\delta(f(x), x^2+1) \neq 1$, έπεται ότι $\mu\kappa\delta(f(x), x^2+1) = x^2+1$. Δηλαδή

$$x^2+1 | f(x) \qquad (\text{στο } \mathbb{R}[x]). \tag{2.3.5}$$

Παρατηρήστε ότι $x^2-3x+2 = (x-1)(x-2)$, επομένως

$$\mu\kappa\delta(f(x), x^2-3x+2) = \begin{cases} 1 & \text{ή} \\ x-1 & \text{ή} \\ x-2 & \text{ή} \\ (x-1)(x-2) = x^2-3x+2 \end{cases}$$

Παρατηρήστε ότι αν $\mu\kappa\delta(f(x), x^2-3x+2) = x^2-3x+2$, τότε

$$x^2-3x+2 | f(x). \tag{2.3.6}$$

Από τις (2.3.5), (2.3.6) και από το γεγονός ότι $\mu\kappa\delta(x^2+1, x^2-3x+2) = 1$, έπεται ότι $(x^2+1)(x^2-3x+2) | f(x)$, δηλαδή $\deg f(x) \geqslant 4$, το οποίο είναι άτοπο. Συνεπώς

$$\mu\kappa\delta(f(x), x^2-3x+2) = \begin{cases} x-1 & \text{ή} \\ x-2 \end{cases}$$

Έστω ότι $\mu\kappa\delta(f(x), x^2-3x+2) = x-1$. Τότε $x-1 | f(x)$, $x^2+1 | f(x)$ και επειδή $\mu\kappa\delta(x-1, x^2+1) = 1$, έπεται ότι

$$(x-1)(x^2+1) | f(x).$$

Αλλά επειδή $\deg f(x) = 3$ και το $f(x)$ είναι μονικό, έπεται ότι

$$f(x) = (x-1)(x^2+1).$$

Αν $\mu\kappa\delta(f(x), x^2-3x+2) = x-2$, ομοίως παίρνουμε ότι

$$f(x) = (x-2)(x^2+1).$$

□

**5**. Έστω $p$ πρώτος και έστω $f(x) = x^p - x + 1 \in \mathbb{Z}_p[x]$.

($\alpha$) Να δείξετε ότι το $f(x)$ δεν έχει ρίζα στο $\mathbb{Z}_p$.

($\beta$) Έστω $F$ σώμα που περιέχει τον $\mathbb{Z}_p$ ως υποδακτύλιο.

(i) Να δείξετε ότι $1_F = 1_{\mathbb{Z}_p}$ και $pr = 0$ για κάθε $r \in F$.

(ii) Να δείξετε ότι αν το $F$ περιέχει μια ρίζα του $f(x)$, τότε περιέχει $p$ διακεκριμμένες ρίζες του $f(x)$

*Απόδειξη.* $(\alpha)$. Από το μικρό θεώρημα του Fermat έχουμε $\alpha^p = \alpha$, για κάθε $\alpha \in \mathbb{Z}_p$. Επομένως

$$f(\alpha) = \alpha^p - \alpha + 1 = \alpha - \alpha + 1 = 1 \neq 0$$

$(1 = [1] \in \mathbb{Z}_p$ και $1 \neq 0$ αφού είναι ακεραία περιοχή).

$(\beta)$.(i). Έχουμε ότι $\mathbb{Z}_p$ και $F$ είναι σώματα και $\mathbb{Z}_p \subseteq F$ ($\mathbb{Z}_p$ υποδακτύλιος του $F$). Συμβολίζουμε με $R = \mathbb{Z}_p$ και με $S = F$, δηλαδή $R \subseteq S$. Παρατηρήστε ότι,

$$1_S \cdot s = s \cdot 1_S = s,$$

για κάθε $s \in S$. Επομένως

$$1_S \cdot 1_R = 1_R = 1_R \cdot 1_R \Rightarrow (1_S - 1_R) \cdot 1_R = 0_S = 0_R.$$

Αν $1_S - 1_R \neq 0_R$, τότε $1_R = 0_R$, το οποίο είναι άτοπο, αφού $R$ ακεραία περιοχή. Άρα $1_R = 1_S$.

*Σημείωση.* Δείξαμε ότι αν $S$ ακεραία περιοχή που περιέχει ως υποδακτύλιο ακεραία περιοχή $R$, τότε $1_R = 1_S$.

Παρατηρήστε ότι για κάθε $r \in F$ έχουμε,

$$\begin{aligned} pr &= r + r + \cdots + r \\ &= 1_F \cdot r + 1_F \cdot r + \cdots + 1_F \cdot r \\ &= (1_F + 1_F + \cdots + 1_F) \cdot r \\ &= (1_{\mathbb{Z}_p} + 1_{\mathbb{Z}_p} \cdot + 1_{\mathbb{Z}_p}) \cdot r \\ &= 0_{\mathbb{Z}_p} \cdot r = 0_F \cdot r = 0_F. \end{aligned}$$

(ii). Θα χρησιμοποήσουμε το λήμμα 2.2.4, το οποίο υπενθυμίζουμε.

Έστω $R$ μεταθετικός δακτύλιος ώστε $pr = 0$ για κάθε $r \in R$ (όπου $p$ πρώτος). Τότε $(r + s)^p = r^p + s^p$ για κάθε $r, s \in R$.

Έστω $\alpha$ ρίζα του $f(x)$, δηλαδή

$$f(\alpha) = \alpha^p - \alpha + 1 = 0. \tag{2.3.7}$$

Θα δείξουμε ότι το $\alpha + 1_F$ είναι ρίζα του $f(x)$. Παρατηρήστε ότι,

$$\begin{aligned} f(\alpha + 1_F) &= (\alpha + 1_F)^p - (\alpha + 1_F) + 1 \\ &= (\alpha + 1_F)^p - \alpha \\ &= \alpha^p + 1_F^p - \alpha \\ &= \alpha^p + 1_F - \alpha = 0, \end{aligned}$$

όπου στην τρίτη ισότητα χρησιμοποιήσαμε το λήμμα 2.2.4, ενώ η τελευταία ισότητα έπεται από την (2.3.7). Επομένως τα στοιχεία

$$\alpha, \alpha+1, \ldots, \alpha+(p-1)$$

είναι διακεκριμμένες, αφού αν $\alpha+i=\alpha+j$, όπου $i,j\in\{0,1,\ldots,p-1\}$ τότε $i=j$. □

**6**. Έστω $f(x), g(x)\in\mathbb{Z}_7[x]$, με

$$f(x)=4x^4+2x^3+6x^2+4x+5 \qquad \text{και} \qquad g(x)=3x^3+5x^2+6x.$$

Να βρείτε τον μκδ$(f(x),g(x))$ και $a(x),b(x)\in\mathbb{Z}_7[x]$ ώστε

$$\text{μκδ}(f(x),g(x))=a(x)f(x)+b(x)g(x).$$

*Απόδειξη.* Από τον Ευκλείδειο αλγόριθμο έχουμε,

$$\begin{aligned} f(x) &= (6x)g(x)+5x^2+4x+5\\ g(x) &= (2x+5)(5x^2+4x+5)+4x+3\\ 5x^2+4x+5 &= (3x+4)(4x+3)+0. \end{aligned}$$

Άρα μκδ$(f(x),g(x))=4^{-1}(4x+3)$, όπου το $4^{-1}$ είναι το αντίστροφο της κλάσης 4 στο $\mathbb{Z}_7$, εδώ $4^{-1}=2$. Επομένως μκδ$(f(x),g(x))=x+6$.

Πάλι από τον Ευκλείδειο αλγόριθμο έχουμε,

$$\begin{aligned} 4x+3 &= g(x)-(2x+5)(5x^2+4x+5)\\ &= g(x)-(2x+5)(f(x)-(6x)g(x))\\ &= (-2x-5)\cdot f(x)+(1+(2x+5)6x)\cdot g(x). \end{aligned}$$

Πολλαπλασιάζοντας με $4^{-1}=2$ παίρνουμε,

$$x+6=2(-2x-5)f(x)+2[1+(2x+5)6x]g(x),$$

δηλαδή $a(x)=2(-2x-5)$ και $b(x)=2[1+(2x+5)6x]$. □

**7**. Έστω $p$ πρώτος και $f(x),g(x)\in\mathbb{Z}_p[x]$, με

$$f(x)=x^4+2x^3+4x^2+8x+9 \qquad \text{και} \qquad g(x)=x^2+2x+3.$$

Να βρείτε για ποιους $p$, ισχύει μκδ$(f(x),g(x))=2$.

*Λύση.* Γνωρίζουμε ότι μκδ$(f(x),g(x))|g(x)$. Έχουμε ότι $\deg g(x)=2$ και το $g(x)$ είναι μονικό. Επειδή δυο μονικά πολυώνυμα ίδιου βαθμού διαιρούνται μεταξύ τους αν και μόνο αν είναι ίσα, παίρνουμε

$$\text{μκδ}(f(x),g(x))=2 \Leftrightarrow \text{μκδ}(f(x),g(x))=g(x) \Leftrightarrow g(x)|f(x).$$

Από τον αλγόριθμο της Ευκλείδειας διαίρεσης παίρνουμε,

$$f(x) = (x^2+1)g(x) + 6x + 6.$$

Άρα

$$g(x)|f(x) \Leftrightarrow 6x+6 = 0 \ \ (\text{στο} \ \ \mathbb{Z}_p[x]) \Leftrightarrow p = 2 \ \ \acute{\eta} \ \ p = 3$$

□

**8**. Έστω $f(x), g(x) \in \mathbb{C}[x]$, με

$$f(x) = x(x^4-1) \qquad \text{και} \qquad g(x) = x^9 - 1.$$

Να βρείτε τον μκδ$(g(x), f(x))$ και $\alpha(x), \beta(x)$ ώστε

$$x^{2011} - 1 = \alpha(x) \cdot f(x) + \beta(x) \cdot g(x).$$

*Λύση.* Από τον Ευκλείδειο αλγόριθμο παίρνουμε,

$$\begin{aligned} x^9 - 1 &= (x^5 - x)(x^4+1) + x - 1 \\ x^5 - x &= (x-1)(x^4 + x^3 + x^2 + x) + 0. \end{aligned}$$

Άρα

$$\text{μκδ}(x^5 - x, x^9 - 1) = x - 1.$$

Επομένως,

$$x - 1 = x^9 - 1 + (-x^4 - 1)(x^5 - x).$$

Πολλαπλασιάζοντας με $x^{2010} + x^{2009} + \cdots + x + 1$,βρίσκουμε τα $\alpha(x)$ και $\beta(x)$. □

## 2.4 Ρίζες πολυωνύμων

**Ορισμός 2.4.1.** *Έστω $R$ μεταθετικός δακτύλιος με $1_R$ και έστω $f(x) \in R[x]$. Ένα $r \in R$ λέγεται ρίζα του $f(x)$, αν $f(r) = 0$.*

**Πρόταση 2.4.2.** *Έστω $F$ σώμα. Το υπόλοιπο της διαίρεσης του $f(x) \in F[x]$ με το $x - \alpha$ είναι ίσο με $f(\alpha)$ . Επομένως,*

$$x - \alpha | f(x) \Leftrightarrow f(\alpha) = 0.$$

*Απόδειξη.* Από την Ευκλείδεια διαίρεση έχουμε,

$$f(x) = q(x)(x-\alpha) + r(x), \ \ \text{deg}r(x) < \deg(x-\alpha).$$

Άρα, $r(x) = c \in F$. Για $x = \alpha$ παίρνουμε,

$$f(\alpha) = q(\alpha) \cdot 0 + r(\alpha).$$

Επομένως το υπόλοιπο είναι $r(x) = f(\alpha)$. □

**Πρόταση 2.4.3.** *Έστω $F$ σώμα και $f(x) \in F[x]$ βαθμού 2 ή 3. Τότε το $f(x) \in F[x]$ είναι ανάγωγο αν και μόνο αν δεν έχει ρίζα στο $F$.*

*Απόδειξη.* Έστω $f(x) \in F[x]$ με $\deg f(x) = 2$ ή 3. Αν το $f(x)$ είναι ανάγωγο, τότε από την πρόταση 2.4.2 δεν έχει ρίζα στο $F$.

Αντίστροφα, έστω $\deg f(x) = 2$ ή 3 και έστω ότι το $f(x)$ δεν έχει ρίζα στο $F$. Αν το $f(x)$ δεν είναι ανάγωγο τότε υπάρχουν $\alpha(x)$, $\beta(x) \in F[x]$ θετικού βαθμού ώστε

$$f(x) = \alpha(x)\beta(x).$$

Επειδή

$$\deg\alpha(x) + \deg\beta(x) = \deg f(x) = 2 \text{ ή } 3,$$

έχουμε

$$\deg\alpha(x) = 1 \qquad \text{ή} \qquad \deg\beta(x) = 1.$$

Δηλαδή το $f(x)$ έχει ρίζα, το οποίο είναι άτοπο. □

**Πρόταση 2.4.4.** *Έστω $F$ σώμα και $f(x) \in F[x]$ με $\deg f(x) = n \geqslant 1$. Τότε το $f(x)$ έχει το πολύ $n$ ρίζες στο $F$.*

*Απόδειξη.* Με επαγωγή στο $n$. □

**Παραδείγματα 2.4.5.** (i) *Το $x^3 - x \in \mathbb{Z}_6[x]$ έχει 6 ρίζες στο $\mathbb{Z}_6$. Άρα το συμπέρασμα της πρότασης 2.4.4 δεν αληθεύει για τυχαίο $R$ στην θέση του σώματος $F$.*

(ii) *Να βρείτε την παραγοντοποίηση του $f(x) = x^3 + x + 1 \in \mathbb{Z}_3[x]$ σε γινόμενο αναγώγων.*

*Παρατηρήστε ότι,*

$$f(1) = 1 + 1 + 1 = 3 = 0$$

*στο $\mathbb{Z}_3[x]$. Τότε από την πρόταση 2.4.2 στο $\mathbb{Z}_3[x]$ έχουμε, $x - 1 | f(x)$. Από την Ευκλείδεια διαίρεση έχουμε,*

$$x^3 + x + 1 = (x - 1)(x^2 + x + 2),$$

*όπου το $x - 1$ είναι ανάγωγο. Το $x^2 + x + 2 \in \mathbb{Z}_3[x]$ είναι βαθμού 2 και δεν έχει ρίζα στο $\mathbb{Z}_3$, οπότε από την πρόταση 2.4.3 έπεται ότι και το $x^2 + x + 2$ είναι ανάγωγο στο $\mathbb{Z}_3[x]$.*

(iii) *Να βρείτε την ανάλυση του $x^p + \alpha \in \mathbb{Z}_p[x]$ σε γινόμενο αναγώγων.*

*Από το μικρό θεώρημα Fermat έχουμε $\alpha^p = \alpha$. Επομένως*

$$x^p + \alpha = x^p + \alpha^p = (x + \alpha)^p.$$

□

### 2.4α′ Τα ανάγωγα πολυώνυμα στο $\mathbb{C}[x]$ και στο $\mathbb{R}[x]$

**Θεώρημα 2.4.6.** *(Θεμελιώδες θεώρημα της Άλγεβρας.) Κάθε $f(x) \in \mathbb{C}[x]$ θετικού βαθμού έχει τουλάχιστον μια ρίζα στο $\mathbb{C}$.*

**Πόρισμα 2.4.7.** *Έστω $f(x) \in \mathbb{C}[x]$ θετικού βαθμού. Τότε υπάρχουν $c, z_1, z_2, \ldots, z_n$ ($n = \deg f(x)$) ώστε*

$$f(x) = c(x - z_1)(x - z_2)\cdots(x - z_n).$$

*($z_i$ όχι αναγκαστικά διακεκριμένοι.)*

*Απόδειξη.* Με επαγωγή στο $\deg f(x)$. □

**Πρόταση 2.4.8.** *Τα ανάγωγα πολυώνυμα στο $\mathbb{C}[x]$ είναι ακριβώς τα πρωτοβάθμια πολυώνυμα.*

Για την συνέχεια χρειαζόμαστε κάποια ορολογία. Αν $z = a + bi \in \mathbb{C}$ $(a, b \in \mathbb{R})$ με $\overline{z}$ συμβολίζουμε το $\overline{z} = a - bi$ $\overline{z}$ ο συζυγής του $z$. Τότε αν $z_1, z_2 \in \mathbb{C}$ ισχύουν τα ακόλουθα.

(i) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$.

(ii) $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$.

Αν $f(x) = f_n x^n + \cdots + f_1 x + f_0 \in \mathbb{C}[x]$ θέτουμε $\overline{f(x)} = \overline{f_n} x^n + \cdots + \overline{f_1} x + \overline{f_0}$. Τότε αν $f(x), g(x) \in \mathbb{C}[x]$ ισχύουν τα ακόλουθα.

(i) $\overline{f(x) + g(x)} = \overline{f(x)} + \overline{g(x)}$.

(ii) $\overline{f(x)g(x)} = \overline{f(x)}\,\overline{g(x)}$.

**Λήμμα 2.4.9.** *Έστω $f(x), g(x) \in \mathbb{R}[x]$. Τότε αν $f(x)|g(x)$ στο $\mathbb{C}[x]$ ισχύει $f(x)|g(x)$ στο $\mathbb{R}[x]$.*

*Απόδειξη.* Έστω $f(x)|g(x)$ στο $\mathbb{C}[x]$. Τότε υπάρχει $h(x) \in \mathbb{C}[x]$ ώστε

$$g(x) = h(x)f(x). \tag{2.4.1}$$

Τότε,

$$\overline{g(x)} = \overline{h(x)f(x)} \Rightarrow \overline{g(x)} = \overline{h(x)} \cdot \overline{f(x)}.$$

Επομένως,

$$g(x) = \overline{h(x)} \cdot f(x). \tag{2.4.2}$$

Από τις (2.4.1) και (2.4.2) έπεται $h(x) = \overline{h(x)}$ (από την μοναδικότητα στην ευκλείδεια διαίρεση). Άρα $h(x) \in \mathbb{R}[x]$. □

**Λήμμα 2.4.10.** *Έστω $f(x) \in \mathbb{R}[x]$. Αν το $z \in \mathbb{C}$ είναι ρίζα του $f(x)$ τότε το $\overline{z} \in \mathbb{C}$ είναι ρίζα του $f(x)$.*

*Απόδειξη.* Έστω $f(z) = 0$. Τότε $\overline{f(z)} = \overline{0} = 0$. Αλλά $\overline{f(z)} = f(\overline{z}) = 0$, αφού $f(x) \in \mathbb{R}[x]$. Άρα το $\overline{z}$ είναι ρίζα του $f(x)$. □

**Θεώρημα 2.4.11.** *Ένα $f(x) \in \mathbb{R}[x]$ είναι ανάγωγο στο $\mathbb{R}[x]$ αν και μόνο αν*

(i) $\deg f(x) = 1$

(ii) $f(x) = ax^2 + bx + c$, *με* $\Delta = d^2 - 4ac < 0$.

*Απόδειξη.* Έστω $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$. Από την πρόταση 2.4.3, το $f(x)$ είναι ανάγωγο στο $\mathbb{R}[x]$ αν και μόνο αν δεν έχει καμιά πραγματική ρίζα, δηλαδή αν και μόνο αν $\Delta = d^2 - 4ac < 0$.

Έστω τώρα $f(x) \in \mathbb{R}[x]$ με $\deg f(x) \geqslant 3$. Θα δείξουμε ότι το $f(x)$ δεν είναι ανάγωγο. Από το λήμμα 2.4.10 και από το θεμελιώδες θεώρημα της Άλγεβρας έχουμε,

$$f(x) = c(x - \varrho_1) \cdots (x - \varrho_\kappa)(x - z_1) \cdots (x - z_m)(x - \overline{z}_1) \cdots (x - \overline{z}_m),$$

όπου $\varrho_1, \ldots, \varrho_\kappa \in \mathbb{R}$, $z_1, \ldots, z_m \in \mathbb{C} \setminus \mathbb{R}$, $c \in \mathbb{C}$. Παρατηρήστε ότι,

$$(x - z_\iota)(x - \overline{z}_\iota) = x^2 - (z_\iota + \overline{z}_\iota)x + z_\iota \overline{z}_\iota \in \mathbb{R}[x],$$

όπου $z_\iota + \overline{z}_\iota \in \mathbb{R}$ και $z_\iota \overline{z}_\iota \in \mathbb{R}$. Επομένως,

$$x^2 - (z_\iota + \overline{z}_\iota) + z_\iota \overline{z}_\iota | f(x),$$

στο $\mathbb{C}[x]$, όπου $x^2 - (z_\iota + \overline{z}_\iota) + z_\iota \overline{z}_\iota \in \mathbb{R}[x]$ και $f(x) \in \mathbb{R}[x]$. Από το λήμμα 2.4.9 έπεται ότι

$$x^2 - (z_\iota + \overline{z}_\iota) + z_\iota \overline{z}_\iota | f(x)$$

στο $\mathbb{R}[x]$. □

**Παρατήρηση 2.4.12.** *Κάθε $f(x) \in \mathbb{R}[x]$ περιττού βαθμού έχει τουλάχιστον μια πραγματική ρίζα.*

**Παράδειγμα 2.4.13.** *Έστω $n \in \mathbb{Z}_{>0}$. Να δείξετε ότι*

$$x^2 + x + 1 | (x + 1)^n + x^n + 1 \ \text{στο} \ \mathbb{R}[x] \ \Leftrightarrow \ n = 2 \ \text{ή} \ 4 \bmod 6. \tag{2.4.3}$$

*Απόδειξη.* Θα δείξουμε πρώτα τον εξής ισχυρισμό.

$$x^2 + x + 1 | (x + 1)^n + x^n + 1 \ \text{στο} \ \mathbb{R}[x] \ \Leftrightarrow \ f(a) = 0,$$

όπου $f(x) = (x + 1)^n + x^n + 1$ και το $a$ είναι ριζα του $x^2 + x + 1$.

Πράγματι, έστω $f(a) = 0$. Οι ρίζες του $x^2 + x + 1$ στο $\mathbb{C}$ είναι το $a$ και το $\overline{a}$. Τότε

$$f(a) = 0 \Rightarrow \overline{f(a)} = 0 \Rightarrow f(\overline{a}) = 0.$$

Επομένως

$$x - a | f(x) \qquad \text{και} \qquad x - \overline{a} | f(x)$$

στο $\mathbb{C}[x]$. Επειδή $a \neq \overline{a}$, έπεται

$$(x - a)(x - \overline{a}) | f(x),$$

άρα

$$x^2 + x + 1 | f(x)$$

στο $\mathbb{C}[x]$. Από το λήμμα 2.4.9 έπεται ότι

$$x^2 + x + 1 | f(x)$$

στο $\mathbb{R}[x]$. Το αντίστροφο είναι σαφές.

Θα δείξουμε τώρα την (2.4.3). Υπολογίζουμε πότε ισχύει $f(a) = 0$. Από την

$$a^2 + a + 1 \Rightarrow a + 1 = -a^2$$

παίρνουμε

$$f(a) = (a + 1)^n + a^n + 1 = (-1)^n a^{2n} + 1.$$

Από την $a^2 + a + 1 = 0$, έπεται $a^3 = 1$ ($x^3 - 1 = (x - 1)(x^2 + x + 1)$). Διακρίνουμε τις ακόλουθες περιπτώσεις.

(i) Έστω $n = 6\kappa,\ \kappa \in \mathbb{Z}_{>0}$. Τότε,

$$f(a) = (a^3)^{4\kappa} + (a^3)^{2\kappa} + 1 = 1 + 1 + 1 = 3 \neq 0.$$

(ii) Έστω $n = 6\kappa + 1,\ \kappa \in \mathbb{Z}_{>0}$. Τότε,

$$f(a) = -(a^3)^4 \cdot a^2 + (a^3)^{2\kappa} \cdot a + 1 = -a^2 + a + 1 = 2a + 1 \neq 0.$$

(iii) Έστω $n = 6\kappa + 2,\ \kappa \in \mathbb{Z}_{>0}$. Τότε,

$$f(a) = (a^3)^{4\kappa+1} \cdot a + (a^3)^{2\kappa} \cdot a^2 + 1 = a = a^2 + 1 = 0.$$

$$\vdots$$

$$\vdots$$

Τελικά $f(a) = 0$ αν και μόνο αν $n = 2$ ή $4 \bmod 6$. □

**Ορισμός 2.4.14.** *Έστω $(R, +, \cdot)$ και $(S, \oplus, \odot)$ δύο δακτύλιοι. Θεωρούμε το καρτεσιανό γινόμενο*

$$R \times S = \{(r, s) : r \in R, s \in S\}$$

*με τις εξής πράξεις.*

$$(r, \cdot) \boxplus (r', s') = (r + r', s \oplus s')$$

$$(r, \cdot) \boxdot (r', s') = (r \cdot r', s \odot s')$$

*Τότε εύκολα ελέγχουμε ότι το $R \times S$ με τις παραπάνω πράξεις είναι δακτύλιος και ονομάζεται το ευθύ γινόμενο των $R$ και $S$.*

**Παράδειγμα 2.4.15.** *Στο $\mathbb{Z}_4 \times \mathbb{Z}_3$, έχουμε*

$$([2]_4, [1]_3) \boxplus ([2]_4, [2]_3) = ([4]_4, [3]_3) = ([0]_4, [0]_3).$$

*Σημείωση.* Οι πράξεις στον $R \times S$ θα συμβολίζονται ως εξής.

$$(r, s) + (r', s') = (r + r', s + s')$$

όπου η πρόσθεση στο πρώτο μέλος είναι η πρόσθεση στο γινόμενο, ενώ η πρώτη πρόσθεση στο δεύτερο μέλος είναι στον $R$ και η δεύτερη είναι στον $S$.

$$(r, s) \cdot (r', s') = (rr', ss').$$

### Ασκήσεις

1. Να δείξετε ότι δεν υπάρχει $f(x) \in \mathbb{Z}[x]$ θετικού βαθμού ώστε για κάθε $m \in \mathbb{Z}$, το $f(m)$ να είναι πρώτος.

   *Απόδειξη.* Έστω ότι υπάρχει $f(x) \in \mathbb{Z}[x]$ θετικού βαθμού και $m \in \mathbb{Z}$ ώστε $f(m) = p$ πρώτος. Παρατηρήστε ότι για κάθε $\kappa \in \mathbb{Z}$,

   $$m + \kappa p \equiv m \mathrm{mod} p.$$

   Επομένως για κάθε $n \in \mathbb{Z}_{>0}$ έχουμε,

   $$(m + \kappa p)^n \equiv m^n \mathrm{mod} p,$$

   οπότε

   $$f(m + \kappa p) \equiv f(m) \mathrm{mod} p.$$

   Άρα

   $$f(m + \kappa p) \equiv 0 \mathrm{mod} p$$

   για κάθε $\kappa$, άρα το $m + \kappa p$ διαιρεί το $p$. Αλλά $f(m + \kappa p)$ είναι πρώτος από υπόθεση, οπότε $f(m + \kappa p) = p$ για κάθε $\kappa \in \mathbb{Z}$. Τότε το $f(x) - p \in \mathbb{Z}[x]$ έχει άπειρες ρίζες, άρα $f(x) = p$ που είναι άτοπο, αφού $\deg f(x) > 0$. □

**2**. Έστω $p$ πρώτος.

($\alpha$) Να δείξετε ότι,

$$x^p - x \equiv x(x-1)\cdots(x-(p-1)). \tag{2.4.4}$$

($\beta$) Να δείξετε ότι, $(p-1)! \equiv -1 \mathrm{mod} p$ (θεώρημα Wilson).

($\gamma$) Να βρείτε το υπόλοιπο της διαίρεσης του 98! με το 101.

*Απόδειξη.*($\alpha$). Από το μικρό θεώρημα του Fermat έχουμε $\alpha^p = \alpha$ για κάθε $\alpha \in \mathbb{Z}_p$. Δηλαδή κάθε $\alpha \in \mathbb{Z}_p$ είναι ρίζα του $f(x) = x^p - x$, οπότε $x - \alpha | x^p - x$ για κάθε $\alpha \in \mathbb{Z}_p$. Επειδή τα $x, x-1, x-2, \ldots, x-(p-1) \in \mathbb{Z}_p[x]$ είναι ανά δύο σχετικά πρώτα, έχουμε

$$x(x-1)(x-2)\cdots(x-(p-1)) | x^p - x.$$

Επειδή

$$\mathrm{deg} x(x-1)\cdots(x-(p-1)) = \mathrm{deg}(x^p - x),$$

υπάρχει $c \in \mathbb{Z}_p[x]$ ώστε

$$x^p - x = c \cdot x(x-1)\cdots(x-(p-1)).$$

Αφού τα πολυώνυμα είναι μονικά, έχουμε $c = 1$.

($\beta$). Προφανώς για $p = 2$ το ζητούμενο ισχύει, αφού $1 \equiv -1 \mathrm{mod} 2$. Παρατηρήστε ότι ο συντελεστής του αριστερού μέλους της (2.4.4) είναι $-1 \in \mathbb{Z}_p$, ενώ ο συντελεστής του $x$ στο δεξιό μέλος της (2.4.4) είναι

$$(-1)(-2)\cdots(-(p-1)) = (-1)^{p-1} \cdot 1 \cdot 2 \cdots (p-1) \in \mathbb{Z}_p.$$

Επομένως έχουμε,

$$-1 = (-1)^{p-1} \cdot 1 \cdot 2 \cdots (p-1).$$

Επειδή ο $p$ είναι περιττός, έχουμε $(-1)^{p-1} = 1$, άρα

$$-1 = 1 \cdot 2 \cdots (p-1)$$

στο $\mathbb{Z}_p$. Τελικά στο $\mathbb{Z}$ έχουμε $-1 = (p-1)!$.

($\gamma$). Το 101 είναι πρώτος, οπότε από το θεώρημα Wilson έχουμε

$$100! \equiv -1 \mathrm{mod} 101,$$

δηλαδή

$$[1 \cdot 2 \cdots 98 \cdot 99 \cdot 100] = [-1]$$

στο $\mathbb{Z}_{101}$. Έπεται

$$[1][2]\cdots[98][99][100] = [-1] \tag{2.4.5}$$

στο $\mathbb{Z}_{101}$. Παρατηρήστε ότι $[1][2]\cdots[98] = [98!]$. Από τον Ευκλείδειο αλγόριθμο βρίσκουμε ότι το αντίστροφο του $[99][100]$ είναι το $[-50]$. Πολλαπλασιάζοντας κατά μέλη με $[-50]$ την (2.4.5) παίρνουμε, $[98!] = [50]$ . Επομένως το ζητούμενο υπόλοιπο είναι 50. □

**3**. Έστω $p$ πρώτος. Να βρείτε την ανάλυση του $x^{p^2} - x^p \in \mathbb{Z}_p[x]$.

*Λύση.* Από το παράδειγμα 2.2.5 γνωρίζουμε ότι αν $g(x) \in \mathbb{Z}_p[x]$, τότε $(g(x))^p = g(x^p)$. Επομένως

$$(x^p - x)^p = (x^p)^p - x^p = x^{p^2} - x^p = f(x).$$

Αλλά από την (2.4.4) έχουμε

$$x^p - x \equiv x(x-1)\cdots(x-(p-1)).$$

Επομένως η ζητούμενη ανάλυση είναι

$$f(x) = x^p(x-1)^p\cdots(x-(p-1))^p \qquad \text{(ανάλυση σε γινόμενο αναγώγων)}.$$

□

**4**. Έστω $p$ πρώτος και έστω

$$f(x) = (x^2+x+1)^p - (x^2+x+1) \in \mathbb{Z}_p[x].$$

($\alpha$) Να δείξετε ότι $x^p - x | f(x)$ στο $\mathbb{Z}_p[x]$.

($\beta$) Να βρείτε την ανάλυση του $f(x) \in \mathbb{Z}_p[x]$ για $p = 2$ και $p = 3$.

*Απόδειξη.* ($\alpha$). Πρώτος τρόπος. Αφού $f(x) \in \mathbb{Z}_p[x]$ από το παράδειγμα 2.2.5 παίρνουμε ότι,

$$\begin{aligned} f(x) &= x^{2p} + x^p + 1 - x^2 - x - 1 \\ &= x^{2p} + x^p - x^2 - x \\ &= (x^p - x)(x^p + x) + x^p - x \\ &= (x^p - x)(x^p + x + 1). \end{aligned}$$

Δηλαδή $x^p - x | f(x)$ στο $\mathbb{Z}_p[x]$.

Δεύτερος τρόπος. Υπόδειξη. Για κάθε $\alpha \in \mathbb{Z}_p$, $f(\alpha) = 0$. (Αν το $f(\alpha) = 0$ για κάθε $\alpha$, τότε διαιρείται με το δεξί μέλος, άρα και με το αριστερό.)

($\beta$). Έστω $p = 2$. Τότε $f(x) = x(x-1)(x^2+x+1)$. Το $x^2+x+1 \in \mathbb{Z}_2[x]$ είναι δευτέρου βαθμού και δεν έχει ρίζες στο $\mathbb{Z}_2$ ($0^2+0+1 = 1 \neq 2$, $1^2+1+1 = 3 \neq 2$). Τότε από την πρόταση 2.4.3 το $x^2+x+1$ είναι ανάγωγο. Επομένως η ζητούμενη ανάλυση είναι $f(x) = x(x-1)(x^2+x+1)$.

Έστω $p = 3$. Τότε $f(x) = x(x-1)(x+1)(x^3+x+1)$. Παρατηρήστε ότι $1^3+1+1 = 3 = 0$, άρα το $x^3+x+1 \in \mathbb{Z}_3[x]$ διαιρείται με το $x-1$ στο $\mathbb{Z}_3[x]$. Από την ευκλείδεια διαίρεση παίρνουμε,

$$x^3 + x + 1 = (x-1)(x^2+x+2).$$

Το $x^2+x+2 \in \mathbb{Z}_3[x]$ είναι δευτέρου βαθμού και δεν έχει ρίζες στο $\mathbb{Z}_3[x]$, επομένως είναι ανάγωγο στο $\mathbb{Z}_3[x]$. Άρα η ζητούμενη ανάλυση είναι

$$f(x) = x(x-1)^2(x+1)(x^2+x+2)$$

στο $\mathbb{Z}_3[x]$. □

## 2.5 Ομομορφισμοί και ιδεώδη

**Ορισμός 2.5.1.** *Έστω $R$ και $S$ δύο δακτύλιοι. Μια απεικόνιση $\varphi \to S$ λέγεται ομορφισμός δακτυλίων αν*

(i) $\varphi(r+r') = \varphi(r) + \varphi(r')$ *για κάθε $r, r' \in R$*

(ii) $\varphi(rr') = \varphi(r)\varphi(r')$ *για κάθε $r, r' \in R$, όπου ο πολλαπλασιασμός στο πρώτο μέλος είναι πολλαπλασιασμός στον $R$ ενώ στο δεύτερο μέλος είναι πολλαπλασιασμός στον $S$.*

*Ένας ομομορφισμός δακτυλίων λέγεται*

(i) *μονομορφισμός αν είναι 1-1,*

(ii) *επιμορφισμός αν είναι επί,*

(iii) *ισομορφισμός αν είναι 1-1 και επί.*

*Αν υπάρχει ισομορφισμός $R \to S$ θα λέμε ότι ο $R$ είναι ισόμορφος με τον $S$ (ή οι $R, S$ είναι ισόμορφοι).*

**Παραδείγματα 2.5.2.** (i) *Έστω*

$$R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right\}$$

*και $S = \mathbb{C}$. Τότε η απεικόνιση $\varphi : R \to S$ με*

$$\varphi \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a + bi$$

*είναι ισομορφισμός.*

*Πράγματι έχουμε,*

$$\begin{aligned}\varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}+\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}\right) &= \varphi\left(\begin{pmatrix} a+a' & b+b' \\ -(b+b') & a+a' \end{pmatrix}\right)\\ &= a+a'+(b+b')\imath\\ &= (a+b\imath)+(a'+b'\imath)\\ &= \varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right)+\varphi\left(\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}\right)\end{aligned}$$

*και*

$$\begin{aligned}\varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}\right) &= \varphi\left(\begin{pmatrix} aa'-bb' & ab'+ba' \\ -(ab'+ba') & aa'-bb' \end{pmatrix}\right)\\ &= aa'-bb'+(ab'+ba')\imath\\ &= (a+b\imath)(a'+b'\imath)\\ &= \varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right)\varphi\left(\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}\right).\end{aligned}$$

*Προφανώς η $\varphi$ είναι επί (αφού έχουμε την εικόνα τυχαίου μιγαδικού) και 1-1, γιατί αν*

$$\varphi\begin{pmatrix} a & b \\ -b & a \end{pmatrix}=\varphi\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}$$

*τότε*

$$a+b\imath=a'+b'\imath \Rightarrow a=a' \qquad \text{και} \qquad b=b'$$

*δηλαδή*

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}=\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}.$$

(ii) *Η απεικόνιση $\varphi:\mathbb{C}\to\mathbb{C}$ με $\varphi(a+b\imath)=a-b\imath$ $(a,b\in\mathbb{R})$ είναι ισομορφισμός δακτυλίων.*

*Πράγματι γνωρίζουμε ότι*

$$\varphi(a+b\imath+a'+b'\imath)=\varphi(a+b\imath)+\varphi(a'+b'\imath)$$

*και*

$$\varphi\left((a+b\imath)(a'+b'\imath)\right)=\varphi(a+b\imath)\varphi(a'+b'\imath).$$

*Επίσης η $\varphi$ είναι 1-1 και επί.*

(iii) *Έστω*

$$\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}:a,b\in\mathbb{Z}\}.$$

*Η απεικόνιση $\varphi:\mathbb{Z}[\sqrt{2}]\to\mathbb{Z}[\sqrt{2}]$ με $\varphi(a+b\sqrt{2})=a-b\sqrt{2}$ είναι ισομορφισμός.*

*Παρατηρήστε πρώτα ότι η $\varphi$ είναι καλώς ορισμένη. Πράγματι, έστω $a+b\sqrt{2} = a'+b'\sqrt{2}$. Αρκεί να δείξουμε ότι $\varphi(a+b\sqrt{2}) = \varphi(a'+b'\sqrt{2})$. Έχουμε,*

$$a-b\sqrt{2} = a'-b'\sqrt{2} \Rightarrow a-a' = (b-b')\sqrt{2},$$

*οπότε αν $b'-b \neq 0$, τότε*

$$\sqrt{2} = \frac{a-a'}{b-b'} \in \mathbb{Q},$$

*που είναι άτοπο. Επομένως $b'-b=0$, άρα $a-a'=0$. Επίσης έχουμε,*

$$\begin{aligned}\varphi\Big((a+b\sqrt{2})+(a'+b'\sqrt{2})\Big) &= \varphi\Big(a+a'+(b+b')\sqrt{2}\Big)\\ &= a+a'-(b+b')\sqrt{2}\\ &= a-b\sqrt{2}+a'-b'\sqrt{2}\\ &= \varphi(a+b\sqrt{2})+\varphi(a'+b'\sqrt{2})\end{aligned}$$

*και*

$$\begin{aligned}\varphi\Big((a+b\sqrt{2})(a'+b'\sqrt{2})\Big) &= \varphi\Big(aa'+2bb'+(ab'+ba')\sqrt{2}\Big)\\ &= aa'+2bb'-(ab'+ba')\sqrt{2}\\ &= (a-b\sqrt{2})(a'-b'\sqrt{2})\\ &= \varphi(a+b\sqrt{2})\varphi(a'+b'\sqrt{2})\end{aligned}$$

*Τέλος είναι σαφές ότι η $\varphi$ είναι 1-1 και επί.*

(iv) *Αν $\mu\kappa\delta(m,n)=1$, τότε υπάρχει ισομορφισμός δακτυλίων $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$. Ορίζουμε $\varphi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, με*

$$\varphi([a]_{mn}) = ([a]_m, [a]_n).$$

*Παρατηρήστε πρώτα ότι η $\varphi$ είναι καλώς ορισμένη απεικόνιση. Πράγματι, αν $[a]_{mn} = [b]_{mn}$, τότε $mn|a-b$, οπότε $m|a-b$ και $n|a-b$, δηλαδή $[a]_m = [b]_m$ και $[a]_n = [b]_n$. Άρα,*

$$([a]_m, [a]_n) = ([b]_m, [b]_n),$$

*δηλαδή*

$$\varphi([a]_{mn}) = \varphi([b]_{mn}).$$

*Έχουμε,*

$$\begin{aligned}\varphi([a]_{mn}+[a']_{mn}) &= \varphi([a+a']_{mn}) = ([a+a']_m, [a+a']_n)\\ &= ([a]_m+[a']_m, [a]_n+[a']_n)\\ &= ([a]_m, [a]_n)+([a']_m, [a']_n)\\ &= \varphi([a]_{mn})+\varphi([a']_{mn}).\end{aligned}$$

*Ομοίως δείχνουμε ότι,*

$$\varphi([a]_{mn}[a']_{mn}) = \varphi([a]_{mn})\varphi([a']_{mn}).$$

*Η $\varphi$ είναι 1-1. Πράγματι, έστω $\varphi([a]_{mn}) = \varphi([a']_{mn})$. Τότε,*

$$([a]_m, [a]_n) = ([a']_m, [a']_n).$$

*Επομένως, $[a]_m = [a']_m$ και $[a]_n = [a']_n$. Άρα $m|a - a'$ και $n|a - a'$. Επειδή όμως $\mu\kappa\delta(m, n) = 1$, έχουμε $mn|a - a'$. Άρα, $[a]_{mn} = [b]_{mn}$.*

*Η $\varphi$ είναι επί. Πράγματι η $\varphi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ είναι 1-1 και*

$$|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n| = m \cdot n < \infty.$$

*Επομένως η $\varphi$ είναι επί.*

(v) *Η απεικόνιση $\varphi : \mathbb{Z} \to \mathbb{Z}_m$, με $\varphi(a) = [a]$ είναι επιμορφισμός.*

*Πράγματι είναι σαφές ότι η $\varphi$ είναι ομομορφισμός, αφού*

$$[a + a'] = [a] + [a']$$

*και*

$$[aa'] = [a][a'].$$

*Επίσης είναι σαφές ότι η $\varphi$ είναι επί.*

(vi) *Έστω $R$ μεταθετικός δακτύλιος ώστε $pr = 0$ για κάθε $r \in R$ και για κάποιο πρώτο $p$. Τότε η απεικόνιση $\varphi : R \to R$, $\varphi(r) = r^p$ είναι ομομορφισμός.*

*Πράγματι από το λήμμα 2.2.4 αν $r, s \in R$ τότε $(r + s)^p = r^p + s^p$. Δηλαδή,*

$$\varphi(r + s) = \varphi(r) + \varphi(s).$$

*Επίσης,*

$$\varphi(rs) = (rs)^p = r^p \cdot s^p$$

*αφού ο $R$ είναι μεταθετικός. Για παράδειγμα η απεικόνιση*

$$\mathbb{Z}_p[x] \to \mathbb{Z}_p[x],\ f(x) \mapsto f(x)^p,$$

*όπου $p$ πρώτος είναι ομομορφισμός δακτυλίων.*

□

**Πρόταση 2.5.3.** *Έστω $\varphi : R \to S$ ομομορφισμός δακτυλίων. Τότε ισχύουν τα ακόλουθα.*

(i) *Για κάθε* $r_1, \ldots, r_n \in R$

$$\varphi(r_1 + \cdots + r_n) = \varphi(r_1) + \cdots + \varphi(r_n) \qquad \text{και} \qquad \varphi(r_1 \cdots r_n) = \varphi(r_1) \cdots \varphi(r_n).$$

*Ειδικότερα,*

$$\varphi(nr) = n\varphi(r)$$

*για κάθε* $n \in \mathbb{Z}$, *για κάθε* $r \in R$ *και*

$$\varphi(r^n) = \varphi(r)^n$$

*για κάθε* $n \in \mathbb{Z}_{>0}$ *και για κάθε* $r \in R$

(ii) $\varphi(0_R) = 0_S$.

(iii) $\varphi(-r) = -\varphi(r)$ *για κάθε* $r \in R$.

(iv) *Αν η* $\varphi$ *είναι επί και ο* $R$ *έχει μοναδιαίο στοιχείο* $1_R$, *τότε ο* $S$ *έχει μοναδιαίο στοιχείο το* $1_S = \varphi(1_R)$.

*Απόδειξη.* (i). Έπεται άμεσα με επαγωγή.
(ii). Παρατηρήστε ότι,

$$\begin{aligned} 0_R + 0_R &= 0_R \Rightarrow \\ \varphi(0_R + 0_R) &= \varphi(0_R) \Rightarrow \\ \varphi(0_R) + \varphi(0_R) &= \varphi(0_R) \Rightarrow \\ \varphi(0_R) &= 0_S \end{aligned}$$

(νόμος διαγραφής πρόσθεσης στον $S$)
(iii). Παρατηρήστε ότι,

$$\begin{aligned} a + (-a) &= 0_R \Rightarrow \\ \varphi(a + (-a)) &= \varphi(0_R) \Rightarrow \\ \varphi(a) + \varphi(-a) &= \varphi(0_R) = 0_S \Rightarrow \\ \varphi(-a) &= -\varphi(a). \end{aligned}$$

(iv). Έστω $\varphi : R \to S$ επιμορφισμός και έστω $s \in S$. Επειδή η $\varphi$ είναι επί, υπάρχει $r \in R$ ώστε $\varphi(r) = s$. Επομένως,

$$\varphi(1_R) \cdot s = \varphi(1_R) \cdot \varphi(r) = \varphi(1_R \cdot r) = \varphi(r) = s.$$

Ομοίως παίρνουμε ότι, $s\varphi(1_R) = s$. Επομένως ο $S$ έχει μοναδιαίο στοιχείο το $\varphi(1_R)$. □

**Παραδείγματα 2.5.4.** (i) *Οι δακτύλιοι $2\mathbb{Z}$ και $3\mathbb{Z}$ δεν είναι ισόμορφοι.*

*Πράγματι, έστω $\varphi : 2\mathbb{Z} \to 3\mathbb{Z}$ ομομορφισμός. Τότε το $\varphi(2)$ είναι κάποιο πολλαπλάσιο του 3, άρα $\varphi(2) = 3m$, για κάποιο $m \in \mathbb{Z}$. Παρατηρήστε ότι,*

$$\varphi(4) = \varphi(2+2) = \varphi(2) + \varphi(2) = 3m + 3m = 6m$$

*και*

$$\varphi(4) = \varphi(2^2) = \varphi(2)^2 = (3m)^2 = 9m^2.$$

*Άρα,*

$$6m = 9m^2 \Rightarrow m(3m-2) = 0 \Rightarrow m = 0,$$

*αφού $\frac{2}{3} \notin \mathbb{Z}$. Δηλαδή $\varphi(z) = 0$, αλλά $\varphi(0) = 0$. Άρα η $\varphi$ δεν είναι 1-1, επομένως δεν είναι ισομορφισμός.*

(ii) *Οι δακτύλιοι $\mathbb{C}$ και $\mathbb{R}$ δεν είναι ισόμορφοι.*

*Εστω $\varphi : \mathbb{C} \to \mathbb{R}$ ισομορφισμός. Αφού έχουμε $\imath^2 = -1$ στο $\mathbb{C}$, παίρνουμε*

$$\varphi(\imath^2) = \varphi(-1) \Rightarrow \varphi(\imath)^2 = -\varphi(1) = -1.$$

*($\varphi(1) = 1$, η $\varphi$ είναι 1-1 και έχει μονάδα στο $\mathbb{C}$ άρα θα έχει και στο $\mathbb{R}$.) Άρα $\varphi(\imath) \in \mathbb{R}$, άτοπο.*

□

**Ορισμός 2.5.5.** *Έστω $\varphi : R \to S$ ομομορφισμός δακτυλίων. Ο πυρήνας της $\varphi$ είναι το σύνολο*

$$\mathrm{Ker}\varphi = \{r \in R : \varphi(r) = 0_S\}.$$

**Παραδείγματα 2.5.6.** (i) *Αν $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ με $\varphi(m) = [m]$, τότε $\varphi$ είναι ομομορφισμός δακτυλίων και*

$$\mathrm{Ker}\varphi = \{m \in \mathbb{Z} : [m] = [0]\} = \{m \in \mathbb{Z} : n|m\} = n\mathbb{Z}.$$

(ii) *Έστω $F$ σώμα και $\alpha \in F$. Η απεικόνιση $\varphi : F[x] \to F$ με $\varphi(f(x)) = f(\alpha)$ είναι ομομορφισμός δακτυλίων και*

$$\mathrm{Ker}\varphi = \{f(x) \in F[x] : f(\alpha) = 0\} = \{(x-\alpha)g(x) : g(x) \in F[x]\}.$$

(iii) *Έστω $F$ σώμα. Η απεικόνιση $\varphi : F[x] \to F \times F$ με $\varphi(f(x)) = (f(0), f(1))$ είναι ομομορφισμός δακτυλίων και*

$$\mathrm{Ker}\varphi = \{f(x) \in F[x] : f(0) = f(1) = 0\} = \{x(x-1)g(x) : g(x) \in F[x]\},$$

*όπου η δεύτερη ισότητα προκύπτει ως εξής.*

$$\begin{aligned} f(0) = f(1) = 0 &\Leftrightarrow x|f(x) \quad \text{και} \quad x-1|f(x) \\ &\Leftrightarrow x(x-1)|f(x) \quad (\text{αφού} \quad \mu\kappa\delta(x, x-1) = 1) \\ &\Leftrightarrow f(x) = x(x-1)g(x),\ \ g(x) \in F[x]. \end{aligned}$$

(iv) *Έστω*

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{Z}) : a, b, c \in \mathbb{Z} \right\}.$$

*Η απεικόνιση*

$$\varphi : R \to \mathbb{Z},\ \varphi \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = c$$

*είναι ομομορφισμός δακτυλίων και*

$$\mathrm{Ker}\varphi = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) : a, b \in \mathbb{Z} \right\}.$$

**Πρόταση 2.5.7.** *Έστω $\varphi : R \to S$ ομομορφισμός δακτυλίων. Τότε η $\varphi$ είναι 1-1 αν και μόνο αν $\ker \varphi = \{0_R\}$.*

*Απόδειξη.* Έστω $\varphi$ 1-1 και έστω $\alpha \in \mathrm{Ker}\varphi$. Τότε,

$$\varphi(\alpha) = 0_S = \varphi(0_R) \Rightarrow \alpha = 0_R,$$

αφού η $\varphi$ είναι 1-1. Επομένως $\ker \varphi = \{0_R\}$.

Αντίστροφα, έστω $\ker \varphi = \{0_R\}$ και έστω ότι $\varphi(\alpha) = \varphi(\beta),\ \alpha, \beta \in R$. Τότε,

$$\varphi(\alpha) - \varphi(\beta) = 0_S \Rightarrow \varphi(\alpha - \beta) = 0_S \overset{\ker \varphi = \{0_R\}}{\Longrightarrow} \alpha - \beta = 0_R \Rightarrow \alpha = \beta.$$

□

**Πρόταση 2.5.8.** *Έστω $\varphi : R \to S$ ομομορφισμός δακτυλίων. Τότε ισχύουν οι ακόλουθες ιδιότητες.*

(i) $\ker \varphi \neq \emptyset$.

(ii) *Αν $a, b \in \mathrm{Ker}\varphi$ τότε $a - b \in \ker \varphi$.*

(iii) *Αν $a \in \mathrm{Ker}\varphi$ και $r \in R$, τότε $ra \in \mathrm{Ker}\varphi$ και $ar \in \mathrm{Ker}\varphi$.*

*Σημείωση.* Από τις παραπάνω ιδιότητες έπεται ότι ο $\mathrm{Ker}\varphi$ είναι υποδακτύλιος του $R$.

*Απόδειξη.* (i). Παρατηρήστε ότι $\varphi(0_R) = 0_S$, άρα το $0_R \in \ker \varphi$.

(ii). Έστω $\varphi(a) = \varphi(b) = 0_S$. Τότε,

$$\varphi(a - b) = \varphi(a) - \varphi(b) = 0_S \Rightarrow a - b \in \mathrm{Ker}\varphi.$$

(iii). Έστω $\varphi(a) = 0_S$. Τότε

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0_S = 0_S \Rightarrow ra \in \mathrm{Ker}\varphi.$$

Ομοίως δείχνουμε ότι $ar \in \mathrm{Ker}\varphi$. □

**Ορισμός 2.5.9.** *Έστω $R$ δακτύλιος και $I \subseteq R$. Το $I$ λέγεται ιδεώδες του $R$ αν ισχύουν τα ακόλουθα.*

(i) $I \neq \emptyset$.

(ii) *Για κάθε* $a, b \in I$, $a - b \in I$.

(iii) *Για κάθε* $r \in R$ *και για κάθε* $a \in I$, $ra \in I$ *και* $ar \in I$.

**Παρατήρηση 2.5.10.** *Αν $\varphi : R \to S$ είναι ομομορφισμός δακτυλίων τότε* $\ker \varphi$ *είναι ιδεώδες του $R$.*

**Παραδείγματα 2.5.11.** *1. Από την προηγούμενη παρατήρηση και από τα παραδείγματα 2.5.6 ισχύουν τα ακόλουθα.*

*(α′)* $n\mathbb{Z}$ *ιδεώδες του* $\mathbb{Z}$.

*(β′)* $\{f(x) \in F[x] : f(a) = 0\}$ *ιδεώδες του* $F(x)$.

*(γ′)* $\left\{f(x) \in F[x] : f(0) = f(1) = 0\right\}$ *ιδεώδες του* $F(x)$.

*(δ′)* $\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) : a, b \in \mathbb{Z} \right\}$ *είναι ιδεώδες.*

*(ε′)* $\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{Z}) : a, b, c \in \mathbb{Z} \right\}$ *είναι ιδεώδες.*

*2. Αν $R$ δακτύλιος, τότε τα $I = R$ και $J = \{0_R\}$ (το μηδενικό ή τετριμμένο ιδεώδες) είναι ιδεώδη.*

(i) *Έστω*

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{Z}) : a, b, c \in \mathbb{Z} \right\} \quad \text{και} \quad I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) : b \in \mathbb{Z} \right\}.$$

*Τότε το $I$ είναι ιδεώδες του $R$.*

*Πράγματι, το $I \neq \emptyset$, αφού για παράδειγμα* $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in I$.

*Έστω* $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} \in I$. *Τότε,*

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b - b' \\ 0 & 0 \end{pmatrix} \in I.$$

*Τέλος έστω* $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in R$ *και* $\begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} \in I$. *Τότε,*

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ab' \\ 0 & 0 \end{pmatrix} \in I$$

*και*

$$\begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & b'c \\ 0 & 0 \end{pmatrix} \in I.$$

*Εναλλακτικά για να δείξουμε ότι το $I$ είναι ιδεώδες του $R$ θεωρούμε*

$$\varphi : R \to \mathbb{Z}\times\mathbb{Z}, \ \ \mu\epsilon \ \varphi\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = (a,c).$$

*Τότε,*

$$\begin{aligned} \varphi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}\right) &= \varphi\begin{pmatrix} a+a' & b+b' \\ 0 & c+c' \end{pmatrix} \\ &= (a+a', c+c') \\ &= (a,c)+(a',c') \\ &= \varphi\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \end{aligned}$$

*και*

$$\begin{aligned} \varphi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}\right) &= \varphi\begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix} \\ &= (aa', cc') \\ &= (a,c)(a',c') \\ &= \varphi\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}. \end{aligned}$$

*Επομένως ο $\varphi$ είναι ομομορφισμός δακτυλίων. Επίσης,*

$$\begin{aligned} \mathrm{Ker}\varphi &= \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{Z}) : (a,c) = 0\right\} \\ &= \left\{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z})\right\} = I. \end{aligned}$$

*Όμως το $I$ ως πυρήνας είναι ιδεώδες του $R$.*

**Ορισμός 2.5.12.** *Έστω $R$ μεταθετικός δακτύλιος με μονάδα $1_R$ και έστω $\alpha \in R$. Το σύνολο $\{r\alpha : r \in R\}$ είναι ένα ιδεώδες του $R$ που λέγεται κύριο ιδεώδες που παράγεται από το $\alpha$ και συμβολίζεται με $< \alpha >$.*

**Παρατηρήσεις 2.5.13.** *1. Το $\alpha \in < \alpha >$, αφού $\alpha = 1_R\alpha$.*

*2 Το γεγονός ότι το $< \alpha >$ είναι ιδεώδες είναι σαφές. Πράγματι έχουμε,*

*(α′)* $< \alpha > \neq \emptyset$ *(για παράδειγμα* $0_R = 0_R\alpha \in < \alpha >$*).*

*(β′) Αν* $r\alpha, s\alpha \in < \alpha >$ $(r, s \in R)$*, τότε*

$$r\alpha - s\alpha = (r - s)\alpha \in < \alpha > .$$

*(γ′) Αν* $r\alpha \in < \alpha >$ *και* $r' \in R$*, τότε*

$$r'(r\alpha) = (r'r)\alpha \in < \alpha >$$

*και*

$$(r\alpha)r' = r'(r\alpha) = (r'r)\alpha \in < \alpha >$$

*(ο* $R$ *είναι μεταθετικός).*

**Παραδείγματα 2.5.14.** (i) *Έστω* $R = \mathbb{Z}$ *και* $m \in \mathbb{Z}$*. Τότε,* $< m >= m\mathbb{Z}$*.*

(ii) *Έστω* $F$ *σώμα και* $f(x) \in F[x]$*. Τότε,*

$$< f(x) >= \{g(x)f(x) : g(x) \in F[x]\}.$$

(iii) *Έστω* $F$ *σώμα και* $\alpha \in F$*. Τότε στον δακτύλιο* $F[x]$ *έχουμε,*

$$< x - \alpha >= \{g(x)(x - \alpha) : g(x) \in F[x]\} = \{f(x) \in F[x] : f(\alpha) = 0\}.$$

**Θεώρημα 2.5.15.** *Κάθε ιδεώδες του* $\mathbb{Z}$ *και κάθε ιδεώδες του* $F[x]$*, όπου* $F$ *σώμα είναι κύριο.*

*Απόδειξη.* Έστω $I$ ιδεώδες του $F[x]$. Αν $I = \{0\}$, τότε $I =< 0 >$. Έστω $I \neq \{0\}$. Τότε υπάρχει $f(x) \in I$, ώστε $f(x) \neq 0$. Έστω $f(x) \in F[x]$ με $f(x) \in I$ και $\deg f(x)$ ελάχιστο $(f(x) \neq 0)$. Θα δείξουμε ότι $I =< f(x) >$.

Πράγματι ο εγκλεισμός $< f(x) > \subseteq I$ είναι σαφής, αφού $g(x)f(x) \in I$ και $I$ ιδεώδες.

Έστω $g(x) \in I$. Από τον ευκλείδειο αλγόριθμο υπάρχουν $q(x), r(x) \in F[x]$ ώστε

$$g(x) = q(x)f(x) + r(x), \ \ \deg r(x) < \deg f(x).$$

Τότε,

$$r(x) = g(x) - q(x)f(x) \in I,$$

αφού $g(x), f(x) \in I$ και $I$ ιδεώδες. Αν $r(x) \neq 0$ τότε αφού $\deg r(x) < \deg f(x)$ και $r(x) \in I$ έχουμε άτοπο, αφού $\deg f(x)$ ελάχιστο. Επομένως $r(x) = 0$, δηλαδή

$$g(x) = q(x) \cdot f(x) \in < f(x) > .$$

Άρα $I \subseteq < f(x) >$. □

Έστω τώρα $I$ ιδεώδες του $\mathbb{Z}$. Αν $I = \{0\}$, τότε $I =< 0 >= 0\mathbb{Z}$ κύριο ιδεώδες. Έστω $I \neq \{0\}$ και $\alpha \neq 0$, $\alpha \in I$. Παρατηρήστε ότι,

$$0 - \alpha = -\alpha \in I \ \ (0, \alpha \in I).$$

Επομένως $\alpha, -\alpha \in I$ , άρα το $I$ περιέχει κάποιον θετικό ακέραιο. Έστω $b$ ο ελάχιστος θετικός ακέραιος στο $I$. Θα δείξουμε ότι $I =< b >= b\mathbb{Z}$

Έστω $c \in I$. Από τον ευκλείδειο αλγόριθμο υπάρχουν $q, r \in \mathbb{Z}$ ώστε

$$c = bq + r,\ o \leqslant r < b.$$

Επειδή $b \in I \Rightarrow bq \in I$ και αφού $c \in I$, έπεται $c - bq \in I$. Επομένως $r \in I$. Επειδή όμως $r < b$ και ο $b$ είναι ο ελάχιστος θετικός ακέραιος στο $I$, έπεται $r = 0$. Άρα $c = bq$, δηλαδή $I =< b >$. □

**Παρατήρηση 2.5.16.** *Κάθε ιδεώδες $I$ του $R$ είναι υποδακτύλιος του $R$. Το αντίστροφο όμως δεν ισχύει. Πράγματι, ο $\mathbb{Z}$ είναι υποδακτύλιος του $\mathbb{Q}$, αλλά δεν είναι ιδεώδες, αφού $\frac{1}{2} \cdot 1 = \frac{1}{2} \notin \mathbb{Q}$.*

**Ορισμός 2.5.17.** *Έστω $I, J$ ιδεώδη ενός δακτυλίου $R$. Θέτουμε,*

$$I + J = \{a + b \in R : a \in I, b \in J\}.$$

*Το $I + J$ λέγεται το άθροισμα των $I$ και $J$.*

**Πρόταση 2.5.18.** *Έστω $R$ δακτύλιος και $I, J$ ιδεώδη του $R$. Τότε το σύνολο $I + J$ του παραπάνω ορισμού είναι ιδεώδες.*

*Απόδειξη.* Παρατηρήστε πρώτα ότι $I + J \neq \emptyset$. Πράγματι, $0_R = 0_R + 0_R \in I + J$. Έστω $a, a' \in I$ και $b, b' \in I$. Τότε,

$$a + b - (a' + b') = (a - a') + (b - b') \in I + J,$$

αφού $I, J$ ιδεώδη και $a - a' \in I,\ b - b' \in J$. Έστω $r \in R, a \in I$ και $b \in I$. Επειδή $I, J$ ιδεώδη έχουμε $ra \in I$ και $rb \in J$. Τότε,

$$r(a + b) = ra + rb \in I + J.$$

Ομοίως δείχνουμε ότι $(a + b)r \in I + J$. □

**Παρατήρηση 2.5.19.** *$I \subseteq I + J$ και $J \subseteq I + J$.*

*Πράγματι, έστω $a \in I$. Το $0 \in J$, άρα*

$$a = a + 0 \in I + J.$$

*Ομοίως αν $b \in J$, αφού $0 \in I$ έπεται*

$$b = 0 + b \in I + J.$$

*Δηλαδή, $I, J \subseteq I + J$.* □

**Πρόταση 2.5.20.** *Έστω $R$ δακτύλιος και $I, J$ ιδεώδη του $R$. Τότε $I \cap J$ είναι ιδεώδες του $R$.*

*Απόδειξη.* Πράγματι, έστω $a, b \in I \cap J$. Τότε $a - b \in I$ και $a - b \in J$. Επομένως $a - b \in I \cap J$. Έστω τώρα $a \in I \cap J$ και $r \in R$. Τότε αφού $I, J$ ιδεώδη του $R$, $ar$ και $ra \in I \cap J$. □

**Ασκήσεις**

**1**. Έστω $R, S, T$ δακτύλιοι.

(i) Αν $\varphi : R \to S$ ισομορφισμός τότε υπάρχει $\varphi^{-1} : S \to R$ ισομορφισμός.

(ii) Αν $\varphi : R \to S$ και $\psi : S \to T$ ομομορφισμοί τότε $\psi \circ \varphi : R \to T$ είναι ομομορφισμός.

*Απόδειξη.* (i). Η $\varphi : R \to S$ είναι ομομορφισμός, 1-1 και επί. Ορίζεται $\varphi^{-1} = h : S \to R$ η οποία είναι 1-1 και επί ($h(s) = r \Leftrightarrow s = \varphi(r)$). Θα δείξουμε ότι $\varphi^{-1} = h$ είναι ομομορφισμός. Πράγματι, έστω $s_1, s_2 \in S$. Αφού η $\varphi$ είναι επί υπάρχουν $r_1, r_2 \in R$ ώστε

$$\varphi(r_1) = s_1 \qquad \text{και} \qquad \varphi(r_2) = s_2.$$

Τότε,

$$h(s_1 + s_2) = h(\varphi(r_1) + \varphi(r_2)) = h(\varphi(r_1 + r_2)) = r_1 + r_2 = h(s_1) + h(s_2)$$

και

$$h(s_1 \cdot s_2) = h(\varphi(r_1) \cdot \varphi(r_2)) = h(\varphi(r_1 \cdot r_2)) = r_1 \cdot r_2 = h(s_1) \cdot (s_2).$$

(ii). Έστω $r_1, r_2 \in R$. Τότε,

$$\begin{aligned} (\psi \circ \varphi)(r_1 + r_2) &= \psi(\varphi(r_1 + r_2)) \\ &= \psi(\varphi(r_1) + \varphi(r_2)) \\ &= \psi(\varphi(r_1) + \psi(\varphi(r_2) \\ &= (\psi \circ \varphi)(r_1) + (\psi \circ \varphi)(r_2) \end{aligned}$$

και

$$\begin{aligned} (\psi \circ \varphi)(r_1 r_2) &= \psi(\varphi(r_1 r_2)) \\ &= \psi(\varphi(r_1)\varphi(r_2)) \\ &= \psi(\varphi(r_1)\psi(\varphi(r_2) \\ &= (\psi \circ \varphi)(r_1)(\psi \circ \varphi)(r_2). \end{aligned}$$

□

*Σημείωση.* Αν $\varphi : R \to S$ και $\psi : S \to T$ ισομορφισμοί, τότε $\psi \circ \varphi : R \to T$ είναι επίσης ισομορφισμός. Πράγματι, έστω $\varphi, \psi$ 1-1. Θα δείξουμε ότι και η $\psi \circ \varphi$ είναι 1-1. Έχουμε,

$$\begin{aligned} (\psi \circ \varphi)(r_1) &= (\psi \circ \varphi)(r_2) \Rightarrow \\ \psi(\varphi(r_1)) &= \psi(\varphi(r_2)) \Rightarrow \\ \varphi(r_1) &= \varphi(r_2) \Rightarrow \\ r_1 &= r_2, \end{aligned}$$

όπου στην δεύτερη συνεπαγωγή χρησιμοποίήσαμε το γεγονός ότι η $\psi$ είναι 1-1, ενώ στην τρίτη συνεπαγωγή χρησιμοποίήσαμε το γεγονός ότι η $\varphi$ είναι 1-1.

Έστω τώρα $\varphi, \psi$ επί. Θα δείξουμε ότι και η $\psi \circ \varphi$ είναι επί. Έστω $t \in T$. Αφού η $\psi$ είναι επί υπάρχει $s \in S$ με $\psi(s) = t$. Επειδή η $\varphi$ είναι επί υπάρχει $r \in R$ ώστε $\varphi(r) = s$. Τότε,

$$(\psi \circ \varphi)(r) = \psi(\varphi(r)) = \psi(s) = t.$$

**2**. Έστω

$$R = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \in M_2(\mathbb{Z}) : \alpha, \beta \in \mathbb{Z} \right\}.$$

Να δείξετε ότι $R \backsimeq \mathbb{Z} \times \mathbb{Z}$.

*Απόδειξη.* Ορίζουμε $\varphi : R \to \mathbb{Z} \times \mathbb{Z}$ με

$$\varphi \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} = (\alpha, \beta).$$

Θα δείξουμε ότι η $\varphi$ είναι ομομορφισμός. Πράγματι, έστω

$$A_1 = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \beta_1 \end{pmatrix} \in R \qquad \text{και} \qquad A_2 = \begin{pmatrix} \alpha_2 & 0 \\ 0 & \beta_2 \end{pmatrix} \in R.$$

Τότε παίρνουμε,

$$\begin{aligned} \varphi(A_1 + A_2) &= \varphi\left( \begin{pmatrix} \alpha_1 & 0 \\ 0 & \beta_1 \end{pmatrix} + \begin{pmatrix} \alpha_2 & 0 \\ 0 & \beta_2 \end{pmatrix} \right) \\ &= \varphi \begin{pmatrix} \alpha_1 + \alpha_2 & 0 \\ 0 & \beta_1 + \beta_2 \end{pmatrix} \\ &= (\alpha_1 + \alpha_2, \beta_1 + \beta_2) \\ &= (\alpha, \beta_1) + (\alpha_2, \beta_2) \\ &= \varphi \begin{pmatrix} \alpha_1 & 0 \\ 0 & \beta_1 \end{pmatrix} + \varphi \begin{pmatrix} \alpha_2 & 0 \\ 0 & \beta_2 \end{pmatrix} \\ &= \varphi(A_1) + \varphi(A_2) \end{aligned}$$

και

$$\begin{aligned} \varphi(A_1 A_2) &= \varphi\left( \begin{pmatrix} \alpha_1 & 0 \\ 0 & \beta_1 \end{pmatrix} \begin{pmatrix} \alpha_2 & 0 \\ 0 & \beta_2 \end{pmatrix} \right) \\ &= \varphi \begin{pmatrix} \alpha_1 \alpha_2 & 0 \\ 0 & \beta_1 \beta_2 \end{pmatrix} \\ &= (\alpha_1 \alpha_2, \beta_1 \beta_2) \\ &= (\alpha, \beta_1)(\alpha_2, \beta_2) \\ &= \varphi \begin{pmatrix} \alpha_1 & 0 \\ 0 & \beta_1 \end{pmatrix} \varphi \begin{pmatrix} \alpha_2 & 0 \\ 0 & \beta_2 \end{pmatrix} \\ &= \varphi(A_1)\varphi(A_2). \end{aligned}$$

Θα δείξουμε τώρα ότι η $\varphi$ είναι 1-1. Γνωρίζουμε ότι

$$\varphi \ 1-1 \Leftrightarrow \mathrm{Ker}\varphi = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}.$$

Έχουμε,

$$\begin{aligned} \mathrm{Ker}\varphi &= \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \in R : \varphi \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} = (0,0) \right\} \\ &= \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \in R : (\alpha, \beta) = (0,0) \right\} \\ &= \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \in R : \alpha = 0, \ \beta = 0 \right\} \\ &= \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}. \end{aligned}$$

Τέλος θα δείξουμε ότι η $\varphi$ είναι επί. Πράγματι, έστω $(y_1, y_2) \in \mathbb{Z} \times \mathbb{Z}$. Αναζητούμε $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \in R$ ώστε

$$\varphi \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} = (y_1, y_2).$$

Ισοδύναμα αναζητούμε $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \in R$ ώστε $(\alpha, \beta) = (y_1, y_2)$. Για

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} = \begin{pmatrix} y_1 & 0 \\ 0 & y_2 \end{pmatrix}$$

το συμπέρασμα έπεται. Επομένως η $\varphi$ είναι επί. Τελικά $R \backsimeq \mathbb{Z} \times \mathbb{Z}$. □

**3**. Έστω $\varphi : R \to S$ επιμορφισμός.

(i) Να δείξετε ότι αν ο $R$ έχει μοναδιαίο στοιχείο $1_R$, τότε και ο $S$ έχει.

(ii) Να δείξετε ότι αν ο $R$ είναι μεταθετικός, τότε και ο $S$ είναι.

*Απόδειξη.* (i). Έστω $s \in S$. Αφού η $\varphi$ είναι επί υπάρχει $r \in R$ ώστε $\varphi(r) = s$. Τότε,

$$s\varphi(r) = \varphi(r)\varphi(1_R) = \varphi(r1_R) = \varphi(r) = s.$$

Ομοίως,

$$\varphi(1_R)s = \varphi(1_R)\varphi(r) = \varphi(1_R r) = \varphi(r) = s.$$

Επομένως $1_S = \varphi(1_R)$.

(ii). Έστω $s_1, s_2 \in S$. Θα δείξουμε ότι $s_1 s_2 = s_2 s_1$. Επειδή η $\varphi$ είναι επί υπάρχουν $r_1, r_2 \in R$ ώστε

$$\varphi(r_1) = s_1 \qquad \text{και} \qquad \varphi(r_2) = s_2.$$

Τότε,

$$s_1 s_2 = \varphi(r_1)\varphi(r_2) = \varphi(r_1 r_2) = \varphi(r_2 r_1) = \varphi(r_2)\varphi(r_1) = s_2 s_1,$$

όπου στη τρίτη ισότητα χρησιμοποιήσαμε το γεγονός ότι ο $R$ είναι μεταθετικός. □

**4**. Έστω $R, S$ ισόμορφοι δακτύλιοι.

(i) Να δείξετε ότι αν $R$ είναι ακεραία περιοχή, τότε $S$ είναι ακεραία περιοχή.

(ii) Να δείξετε ότι αν $R$ είναι σώμα, τότε $S$ είναι σώμα.

*Απόδειξη.* (i). Έστω $\varphi : R \to S$ ισομορφισμός και έστω $R$ είναι ακεραία περιοχή. Θα δείξουμε ότι $S$ είναι ακεραία περιοχή. Λόγω της άσκησης 3, ο $S$ έχει μονάδα και είναι μεταθετικός. Έστω $s_1, s_2 \in S$ με $s_1 s_2 = 0$. Θα δείξουμε $s_1 = 0$ ή $s_2 = 0$. Αφού η $\varphi$ είναι επί υπάρχουν $r_1, r_2 \in R$ με $\varphi(r_1) = s_1$ και $\varphi(r_2) = s_2$. Παρατηρήστε ότι,

$$s_1 s_2 = 0 \Rightarrow \varphi(r_1)\varphi(r_2) = 0 \Rightarrow \varphi(r_1 r_2) = 0.$$

Όμως οι ομομορφισμοί απεικονίζουν το μηδενικό στοιχείο στο μηδενικό, άρα

$$\varphi(r_1 r_2) = \varphi(0) \Rightarrow r_1 r_2 = 0 \Rightarrow r_1 = 0 \qquad \text{ή} \qquad r_2 = 0,$$

όπου στο προτελευταίο βήμα χρησιμοποιήσαμε το γεγονός ότι η $\varphi$ είναι 1-1, ενώ στο τελευταίο βήμα χρησιμοποιήσαμε το γεγονός ότι $R$ είναι ακεραία περιοχή.

(ii). Έστω $s \in S$ με $s \neq 0$. Θα δείξουμε ότι το $s$ είναι αντιστρέψιμο. Αφού η $\varphi$ είναι επί υπάρχει $r \in R$ ώστε $\varphi(r) = s$. Παρατηρήστε ότι αν $r = 0$, τότε $s = \varphi(r) = \varphi(0) = 0$, άτοπο, επομένως $r \neq 0$. Επειδή το $R$ είναι σώμα υπάρχει $r' \in R$ ώστε $rr' = 1_R$ και $r'r = 1_R$. Τότε,

$$s\varphi(r') = \varphi(r)\varphi(r') = \varphi(rr') = \varphi(1_R) = 1_S$$

και

$$\varphi(r')s = \varphi(r')\varphi(r) = \varphi(r'r) = \varphi(1_R) = 1_S,$$

όπου οι τελευταίες ισότητες στις δύο προηγούμενες σχέσεις έπονται από την άσκηση 3(i). □

**5**. Να εξετάσετε αν για τα ακόλουθα ζεύγη οι δακτύλιοι είναι ισόμορφοι.

(i) $2\mathbb{Z}$ και $\mathbb{Z}$.

(ii) $\mathbb{C}$ και $\mathbb{R} \times \mathbb{R}$.

(iii) $R = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) : \alpha \in \mathbb{Z} \right\}$ και $\mathbb{Z}$.

(iv) $R = \left\{ \begin{pmatrix} 0 & \beta \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) : \beta \in \mathbb{Z} \right\}$ και $\mathbb{Z}$.

(v) $R = \left\{ \begin{pmatrix} \alpha & \beta \\ 2\beta & \alpha \end{pmatrix} \in M_2(\mathbb{Z}) : \alpha, \beta \in \mathbb{Z} \right\}$ και
$S = \left\{ \begin{pmatrix} \alpha & \beta \\ 2\beta & \alpha \end{pmatrix} \in M_2(\mathbb{Z}) : \alpha, \beta \in \mathbb{Z} \right\}$.

*Λύση*. (i). Έστω $\varphi : \mathbb{Z} \to 2\mathbb{Z}$ ισομορφισμός. Αφού ο $\mathbb{Z}$ έχει μονάδα και ο $\varphi$ είναι επιμορφισμός, τότε και ο $2\mathbb{Z}$ έχει μονάδα, άτοπο. Επομένως $\mathbb{Z} \ncong 2\mathbb{Z}$.
(ii). Το $\mathbb{C}$ είναι ακεραία περιοχή, ενώ το $\mathbb{R} \times \mathbb{R}$ δεν είναι. Πράγματι,

$$(1,0)(0,1) = (0,0),$$

όπου $(1,0) \neq (0,0)$ και $(0,1) \neq (0,0)$. Άρα $\mathbb{C} \ncong \mathbb{R} \times \mathbb{R}$.
(iii). Θα δείξουμε ότι

$$R = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) : \alpha \in \mathbb{Z} \right\} \cong \mathbb{Z}.$$

Ορίζουμε

$$\varphi : R \to \mathbb{Z} \qquad \text{με} \qquad \varphi \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} = \alpha.$$

Παρατηρήστε ότι,

$$\varphi\left( \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} \beta & 0 \\ 0 & 0 \end{pmatrix} \right) = \varphi \begin{pmatrix} \alpha+\beta & 0 \\ 0 & 0 \end{pmatrix} = \alpha+\beta = \varphi \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} + \varphi \begin{pmatrix} \beta & 0 \\ 0 & 0 \end{pmatrix}$$

και

$$\varphi\left( \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \beta & 0 \\ 0 & 0 \end{pmatrix} \right) = \varphi \begin{pmatrix} \alpha\beta & 0 \\ 0 & 0 \end{pmatrix} = \alpha\beta = \varphi \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} \varphi \begin{pmatrix} \beta & 0 \\ 0 & 0 \end{pmatrix}.$$

Επίσης έχουμε,

$$\begin{aligned}\mathrm{Ker}\varphi &= \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) : \varphi \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} = 0 \right\} \\ &= \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) : \alpha = 0 \right\} \\ &= \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}.\end{aligned}$$

Επομένως η $\varphi$ είναι 1-1. Έστω $y \in \mathbb{Z}$. Αναζητούμε $\begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} \in R$ με $\varphi \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} = y$. Ισοδύναμα αναζητούμε $\begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} \in R$ με $\alpha = y$. Παρατηρήστε ότι για

$$\begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} y & 0 \\ 0 & 0 \end{pmatrix}$$

το ζητούμενο έπεται.

(iv). Το $\mathbb{Z}$ είναι ακεραία περιοχή, ενώ το $\begin{pmatrix} 0 & \beta \\ 0 & 0 \end{pmatrix}$ δεν είναι. Πράγματι έχουμε,

$$\begin{pmatrix} 0 & \beta_1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & \beta_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

όπου $\beta_1 \neq \beta_2,\ \beta_1, \beta_2 \neq 0$. Επομένως $R = \left\{ \begin{pmatrix} 0 & \beta \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) : \beta \in \mathbb{Z} \right\} \ncong \mathbb{Z}$.

(v). Θα δείξουμε ότι οι δακτύλιοι $R$ και $S$ δεν είναι ισόμορφοι. Θα δείξουμε πρώτα ότι $R \cong \mathbb{Z}[\sqrt{2}] = \{\alpha + \beta\sqrt{2} : \alpha, \beta \in \mathbb{Z}\}$. Ορίζουμε

$$\varphi : \mathbb{Z}[\sqrt{2}] \to R \qquad \text{με} \qquad \varphi(\alpha + \beta\sqrt{2}) = \begin{pmatrix} \alpha & \beta \\ 2\beta & \alpha \end{pmatrix}.$$

Έστω $\alpha + \beta\sqrt{2}, \gamma + \delta\sqrt{2} \in \mathbb{Z}\sqrt{2}$. Τότε έχουμε,

$$\begin{aligned}\varphi\Big((\alpha + \beta\sqrt{2}) + (\gamma + \delta\sqrt{2})\Big) &= \varphi\Big((\alpha + \gamma) + (\beta + \delta\sqrt{2})\Big) \\ &= \begin{pmatrix} \alpha + \gamma & \beta + \delta \\ 2(\beta + \delta) & \alpha + \gamma \end{pmatrix} \\ &= \begin{pmatrix} \alpha & \beta \\ 2\beta & \alpha \end{pmatrix} + \begin{pmatrix} \gamma & \delta \\ 2\delta & \gamma \end{pmatrix} \\ &= \varphi(\alpha + \beta\sqrt{2}) + \varphi(\gamma + \delta\sqrt{2}).\end{aligned}$$

Επίσης,

$$\begin{aligned}\varphi\left((\alpha+\beta\sqrt{2})(\gamma+\delta\sqrt{2})\right) &= \varphi\left(\alpha\gamma+\alpha\delta\sqrt{2}+\beta\gamma\sqrt{2}+2\beta\delta\right)\\ &= \varphi\left((\alpha\gamma+2\beta\delta)+(\alpha\delta+\beta\gamma)\sqrt{2}\right)\\ &= \begin{pmatrix}\alpha\gamma+2\beta\delta & \alpha\delta+\beta\gamma\\ 2(\alpha\delta+\beta\gamma) & \alpha\gamma+2\beta\delta\end{pmatrix}\end{aligned}$$

και

$$\begin{aligned}\varphi(\alpha+\beta\sqrt{2})\varphi(\gamma+\delta\sqrt{2}) &= \begin{pmatrix}\alpha & \beta\\ 2\beta & \alpha\end{pmatrix}\begin{pmatrix}\gamma & \delta\\ 2\delta & \gamma\end{pmatrix}\\ &= \begin{pmatrix}\alpha\gamma+2\beta\delta & \alpha\delta+\beta\gamma\\ 2(\alpha\delta+\beta\gamma) & \alpha\gamma+2\beta\delta\end{pmatrix}.\end{aligned}$$

Επομένως

$$\varphi\left((\alpha+\beta\sqrt{2})(\gamma+\delta\sqrt{2})\right)=\varphi(\alpha+\beta\sqrt{2})\varphi(\gamma+\delta\sqrt{2}).$$

Παρατηρήστε ότι

$$\begin{aligned}\mathrm{Ker}\varphi &= \left\{\alpha+\beta\sqrt{2}\in\mathbb{Z}[\sqrt{2}]:\varphi(\alpha+\beta\sqrt{2})=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}\right\}\\ &= \left\{\alpha+\beta\sqrt{2}\in\mathbb{Z}[\sqrt{2}]:\begin{pmatrix}\alpha & \beta\\ 2\beta & \alpha\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}\right\}\\ &= \left\{\alpha+\beta\sqrt{2}\in\mathbb{Z}[\sqrt{2}]:\alpha=0,\ \beta=0\right\}\\ &= \{0+\sqrt{2}\}.\end{aligned}$$

Επομένως η $\varphi$ είναι 1-1. Τέλος θα δείξουμε ότι η $\varphi$ είναι επί. Πράγματι έστω $\begin{pmatrix}x & y\\ 2y & x\end{pmatrix}\in R$. Αναζητούμε $\alpha+\beta\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$ με

$$\varphi(\alpha+\beta\sqrt{2})=\begin{pmatrix}x & y\\ 2y & x\end{pmatrix}.$$

Ισοδύναμα αναζητούμε $\alpha+\beta\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$ με

$$\begin{pmatrix}\alpha & \beta\\ 2\beta & \alpha\end{pmatrix}=\begin{pmatrix}x & y\\ 2y & x\end{pmatrix}.$$

Ισοδύναμα αναζητούμε $\alpha+\beta\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$ με

$$\alpha=x \qquad \text{και} \qquad \beta=y.$$

Το ζητούμενο έπεται αν $\alpha+\beta\sqrt{2}=x+y\sqrt{2}$. Πράγματι,

$$\varphi(x+y\sqrt{2})=\begin{pmatrix} x & y \\ 2y & x \end{pmatrix}.$$

Επομένως $R\cong\mathbb{Z}[\sqrt{2}]$. Για να δείξουμε ότι $R\ncong S$, αρκεί να δείξουμε ότι $\mathbb{Z}[\sqrt{2}]\ncong S$. Πράγματι ο $\mathbb{Z}[\sqrt{2}]$ είναι ακεραία περιοχή, αφού ανήκει μέσα σε μια $\mathbb{R}$- ακεραία περιοχή (δηλαδή είναι πραγματικός) και $\mathbb{R}$ είναι ακεραία περιοχή. (*Σημείωση*. Το αντίστοιχο για σώματα δεν ισχύει.)
Αλλά ο $S$ δεν είναι ακεραία περριοχή. Πράγματι

$$\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}\begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

με $\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}\neq\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ και $\begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix}\neq\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. □

**6**. Να βρείτε όλα τα ιδεώδη $I$ του $\mathbb{Z}$ ώστε $20\mathbb{Z}\subseteq I\subseteq 2\mathbb{Z}$.

*Λύση*. Από το θεώρημα 2.5.15, έχουμε $I=<m>$. Επομένως,

$$\begin{aligned} 20\mathbb{Z}\subseteq I\subseteq 2\mathbb{Z} &\Leftrightarrow <20>\subseteq<m>\subseteq<2> \\ &\Leftrightarrow <20>\subseteq<m> \quad \text{και} \quad <m>\subseteq<2> \\ &\Leftrightarrow m|20 \quad \text{και} \quad 2|m. \end{aligned}$$

Επομένως ζητάμε τους ακεραίους που είναι άρτιοι και διαιρούν το 20. Άρα $m=\pm2,\pm4,\pm10,\pm20$. Τότε $<2>=<-2>$, $<4>=<-4>$, $<10>=<-10>$, $<20>=<-20>$. Άρα $I=<2>,<4>,<10>,<20>$. □

**7**. Να βρείτε ένα $f(x)\in\mathbb{R}[x]$ ώστε

$$<f(x)>=\{g(x)\in\mathbb{R}[x]: g(0)=g(3-4i)=0\}.$$

*Λύση*. Έστω $g(x)\in\mathbb{R}[x]$. Τότε,

$$g(0)=0\Leftrightarrow x|g(x)$$

και

$$\begin{aligned} g(3-4i)=0 &\Leftrightarrow g(3+4i)=0 \quad \text{(αφού έχουμε πραγματικούς συντελεστές)} \\ &\Leftrightarrow x-(3-4i)|g(x) \quad \text{και} \quad x-(3+4i)|g(x) \text{ στο } \mathbb{C}[x]. \end{aligned}$$

Όμως επειδή μκδ$(x-3+4i,x-3-4i)=1$, έπεται ότι

$$(x-(3-4i))(x-(3+4i))|g(x) \text{ στο } \mathbb{C}[x]\Leftrightarrow x^2-6x+25|g(x) \text{ στο } \mathbb{C}[x].$$

Αλλά $x^2-6x+25, g(x) \in \mathbb{R}[x]$, οπότε από το λήμμα 2.4.9 έπεται ότι

$$x^2-6x+25|g(x) \text{ στο } \mathbb{R}[x].$$

Άρα

$$x(x^2-6x+25)|g(x) \text{ στο } \mathbb{R}[x] \Leftrightarrow g(x) \in \{f(x) \in \mathbb{R}[x] : f(0) = f(3-4i) = 0\}.$$

Επομένως

$$\{f(x) \in \mathbb{R}[x] : f(0) = f(3-4i) = 0\} =< x(x^2-6x+25) > .$$

□

**8**. Έστω $m, n \in \mathbb{Z}_{>0}$. Τότε στο $\mathbb{Z}$ έχουμε,

$$< m > + < n > =< d >, \ \ d = \text{μκδ}(m,n).$$

*Απόδειξη.* Γνωρίζουμε ότι υπάρχουν $a, b \in \mathbb{Z}$ ώστε

$$d = am + bn.$$

Άρα $d \in < m > + < n >$. Επομένως $< d > \subseteq < m > + < n >$ (αφού $< m > + < n >$ ιδεώδη). Αντίστροφα, αφού $d|m$ έχουμε $< m > \subseteq < d >$. Ομοίως $< n > \subseteq < d >$. Επομένως $< m > + < n > \subseteq < d >$ (γιατί το $< d >$ είναι ιδεώδες). □

## 2.6 Δακτύλιος πηλίκο

Έστω $R$ δακτύλιος και $I$ ιδεώδες του $R$. Ο σκοπός μας είναι να κατασκευάσουμε τον *δακτύλιο πηλίκο* $R/I$.

**Ορισμός 2.6.1.** *Έστω $R$ δακτύλιος και $I$ ιδεώδες του $R$. Ορίζουμε στο $R$ την εξής σχέση ισοδυναμίας.*

$$a \equiv b \text{mod} I \Leftrightarrow a - b \in I.$$

**Παρατήρηση 2.6.2.** *Η παραπάνω σχέση είναι πράγματι σχέση ισοδυναμίας.*
*Παρατηρήστε ότι,*

(i) $a \equiv a \text{mod} I$, *για κάθε* $a \in R$ *αφού* $a - a = 0_R \in I$.

(ii) *Αν* $a \equiv b \text{mod} I$, *τότε* $a - b \in I$ *και επειδή το* $I$ *είναι ιδεώδες έπεται* $-(a-b) \in I$ . *Επομένως,*

$$b - a \in I \Rightarrow b \equiv a \text{mod} I.$$

(iii) *Αν* $a \equiv b \text{mod} I$ *και* $b \equiv c \text{mod} I$, *τότε* $a - b \in I$ *και* $b - c \in I$. *Επειδή το* $I$ *είναι ιδεώδες, έπεται*

$$(a-b) + (b-c) = a - c \in I.$$

**Παρατήρηση 2.6.3.** *Η κλάση ισοδυναμίας του $a \in R$ είναι*

$$\begin{aligned}[a] &= \{b \in R : b \equiv a \mathrm{mod} I\} \\ &= \{b \in R : b - a \in I\}.\end{aligned}$$

Παρατηρήστε ότι,

$$b \equiv a \mathrm{mod} I \Leftrightarrow b - a = c \in I.$$

Άρα,

$$b = a + c, \;\; c \in I.$$

Δηλαδή,

$$[a] = \{a + c \in R : c \in I\}.$$

Συμβολικά γράφουμε,

$$[a] = a + I.$$

**Ορισμός 2.6.4.** $R/I = \{a + I : a \in R\}$. *Ο δακτύλιος $R/I$ λέγεται ο δακτύλιος πηλίκο του $R$ moduloI.*

**Παρατήρηση 2.6.5.** *Αν $R = \mathbb{Z}$ και $I =< n >$, τότε $R/I = \mathbb{Z}_n$.*

**Θεώρημα 2.6.6.** *Το $R/I$ είναι δακτύλιος με τις ακόλουθες πράξεις.*

$$+ : R/I \times R/I \to R/I$$

*με*

$$(a + I) + (b + I) = (a + b) + I.$$

*και*

$$\cdot : R/I \times R/I \to R/I$$

*με*

$$(a + I)(b + I) = ab + I.$$

*Επιπλέον αν ο $R$ είναι μεταθετικός, τότε ο $R/I$ είναι μεταθετικός. Επίσης αν ο $R$ έχει μοναδιαίο στοιχείο, τότε και ο $R/I$ έχει μοναδιαίο στοιχείο.*

*Απόδειξη.* Πρώτα θα δείξουμε ότι οι παραπάνω πράξεις είναι καλώς ορισμένες. Πράγματι, έστω $a + I = a' + I$ και $b + I = b' + I$. Τότε $a - a' \in I$ και $b - b' \in I$. Επομένως,

$$(a - a') + (b - b') \in I \qquad \text{ή} \qquad (a + b) - (a' + b') \in I.$$

Επομένως,

$$a + b \equiv a' + b' \mathrm{mod} I \Rightarrow a + b + I = a' + b' + I.$$

Άρα η πρόσθεση είναι καλώς ορισμένη. Θα δείξουμε το ίδιο και για τον πολλαπλασιασμό. Πράγματι, έστω $a+I=a'+I$ και $b+I=b'+I$. Τότε ομοίως με πριν παίρνουμε $a-a'\in I$ και $b-b'\in I$. Παρατηρήστε ότι,

$$ab-a'b'=ab-ab'+ab'-a'b'=a(b-b')+(a-a')b'\in I,$$

αφού το $I$ είναι ιδεώδες. Επομένως,

$$ab\equiv a'b'\mathrm{mod}I\Rightarrow ab+I=a'b'+I.$$

Ας δείξουμε την προσεταιριστικότητα του πολλαπλασιασμού (οι άλλες ιδιότητες είναι εξίσου άμεσες). Πράγματι έχουμε,

$$\begin{aligned}((a+I)(b+I))\,(c+I) &= (ab+I)(c+I)\\ &= (ab)c+I\\ &= a(bc)+I\\ &= (a+I)\,((b+I)(c+I))\,,\end{aligned}$$

όπου η τρίτη ισότητα έπεται από την προσεταιριστικότητα του πολλαπλασιασμού στο $\mathbb{R}$. Επομένως ο $R/I$ με τις δοσμένες πράξεις είναι δακτύλιος.

Έστω τώρα $a,b\in R$ με $ab=ba$. Τότε,

$$(a+I)(b+I)=(b+I)(a+I)$$

στο $R/I$. Άρα, αν

$$R\ \text{μεταθετικός}\ \Rightarrow\ R/I\ \text{μεταθετικός}.$$

Τέλος αν $1_R\in R$, τότε ο $R/I$ έχει μοναδιαίο στοιχείο το $1_R+I$. □

**Παράδειγμα 2.6.7.** *Έστω $R=\mathbb{Z}_2[x]$ και*

$$I=<x^3+1>=\{g(x)(x^3+1):g(x)\in\mathbb{Z}_2[x]\}.$$

*Τότε,*

$$(x^4+x^3)+I=x+1+I.$$

*Πράγματι έχουμε,*

$$x^4+x^3-(x+1)=(x+1)(x^3+1)\in I.$$

*(Ευκλείδειος αλγόριθμος για $x^4+x^3-(x+1)$ και $x^3+1$.)*

**Θεώρημα 2.6.8.** *Έστω $F$ σώμα, $p(x)\in F[x]$ και $I=<p(x)>$. Τότε ο δακτύλιος $F[x]/I$ είναι σώμα αν και μόνο αν το $p(x)\in F[x]$ είναι ανάγωγο.*

*Απόδειξη.* Έστω ότι ο δακτύλιος $F[x]/I$ είναι σώμα. Θα δείξουμε ότι το $p(x) \in F[x]$ είναι ανάγωγο. Έστω ότι

$$p(x) = a(x)b(x), \quad a(x), b(x) \in F[x]. \tag{2.6.1}$$

Άρα

$$\deg p(x) = \deg a(x) + \deg b(x). \tag{2.6.2}$$

Λόγω της (2.6.1) παίρνουμε $a(x)b(x) + I = I$ (αφού $a(x)b(x) = p(x) \in I$). Επομένως,

$$(a(x) + I)(b(x) + I) = I = 0_{R/I}.$$

Επειδή ο $R/I$ είναι σώμα, ο $R/I$ είναι ακεραία περιοχή, άρα

$$a(x) + I = I \qquad \text{ή} \qquad b(x) + I = I.$$

Δηλαδή,

$$a(x) \in I =< p(x) > \qquad \text{ή} \qquad b(x) \in I =< p(x) > .$$

Επομένως,

$$p(x)|a(x) \qquad \text{ή} \qquad p(x)|b(x).$$

Άρα,

$$\deg p(x) \leqslant \deg a(x) \qquad \text{ή} \qquad \deg p(x) \leqslant \deg b(x).$$

Λόγω της (2.6.2) έπεται ότι,

$$\deg a(x) = 0 \qquad \text{ή} \qquad \deg b(x) = 0.$$

Επειδή $p(x) = a(x)b(x)$, έχουμε $a(x) \neq 0$ και $b(x) \neq 0$.

Αντίστροφα, έστω $p(x) \in F[x]$ ανάγωγο. Ο $F[x]/I$ είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο το $1_R + I$. Παρατηρήστε ότι

$$1_R + I \neq 0_R + I \ \ (\text{δηλαδή } \ 1_{F[x]/I} \neq 0_{F[x]/I}).$$

Πράγματι, αλλιώς θα είχαμε $1_R \in I = p(x)$. Δηλαδή,

$$p(x)|1_R \Rightarrow \deg p(x) = 0,$$

άτοπο αφού $\deg p(x) > 0$ και $p(x)$ ανάγωγο. Έστω $f(x) + I \in F[x]/I$ με $f(x) + I \neq 0_{F[x]/I}$. Τότε $f(x) \notin I$, δηλαδή $p(x) \nmid f(x)$. Επειδή το $p(x)$ είναι ανάγωγο, έχουμε μκδ$(f(x), p(x)) = 1_{F[x]}$. Τότε υπάρχουν $a(x), b(x) \in F[x]$ ώστε

$$1 = a(x)f(x) + b(x)p(x).$$

Επειδή το $b(x)p(x) \in I$, έχουμε $b(x)p(x) + I = I$. Επομένως

$$\begin{aligned} 1 + I &= (a(x)f(x) + I) + (b(x)p(x) + I) \\ &= a(x)f(x) + I \\ &= (a(x) + I)(f(x) + I). \end{aligned}$$

Επομένως το $f(x) + I$ είναι αντιστρέψιμο. □

**Παρατηρήσεις 2.6.9.** (i) *Έστω $F$ σώμα και $p(x) \in F[x]$ ανάγωγο. Η απόδειξη του ($\Leftarrow$) του θεωρήματος 2.6.8 δίνει έναν τρόπο υπολογισμού του αντιστρόφου του $f(x)+ < p(x) >$ αν $f(x)+ < p(x) > \neq < p(x) >$, με βάση τον ευκλείδειο αλγόριθμο.*

(ii) *Έστω $f(x) \in F[x]$. Τότε τα εξής είναι ισοδύναμα.*

*(α΄)* $p(x) \nmid f(x)$.

*(β΄)* $\mu\kappa\delta(p(x), f(x)) = 1$.

*(γ΄) Το* $f(x) + I = f(x)+ < p(x) >$ *είναι αντιστρέψιμο στο σώμα* $F[x]/ < p(x) >$.

**Παρατήρηση 2.6.10.** *Έστω $\varphi : R \to S$ ομομορφισμός δακτυλίων. Τότε ο* $\mathrm{Ker}\varphi$ *είναι ιδεώδες του $R$. Άρα ο* $R/\mathrm{Ker}\varphi$ *είναι δακτύλιος. Ποια είναι η σχέση του* $R/\mathrm{Ker}\varphi$ *με τον $S$; Σύμφωνα με το επόμενο θεώρημα οι δακτύλιοι* $R/\mathrm{Ker}\varphi$ *και $S$ είναι ισόμορφοι.*

**Θεώρημα 2.6.11.** *(Πρώτο Θεώρημα Ισομορφισμών Δακτυλίων) Έστω $\varphi : R \to S$ ομομορφισμός δακτυλίων. Τότε οι δακτύλιοι* $R/\mathrm{Ker}\varphi$ *και $S$ είναι ισόμορφοι.*

*Απόδειξη.* Ορίζουμε την αντιστοιχία

$$\psi : R/\mathrm{Ker}\varphi \to \mathrm{Im}\varphi, \;\; \psi(r + \mathrm{Ker}\varphi) = \varphi(r).$$

Θα δείξουμε πρώτα ότι η αντιστοιχία αυτή είναι μια καλώς ορισμένη απεικόνιση. Πράγματι, έστω $r + \mathrm{Ker}\varphi = r' + \mathrm{Ker}\varphi$. Τότε, $r - r' \in \mathrm{Ker}\varphi$, άρα

$$\begin{aligned} \varphi(r - r') &= 0_S \Rightarrow \\ \varphi(r) - \varphi(r') &= 0_S \Rightarrow \\ \varphi(r) &= \varphi(r') \Rightarrow \\ \psi(r + \mathrm{Ker}\varphi) &= \psi(r' + \mathrm{Ker}\varphi). \end{aligned}$$

Τώρα θα δείξουμε ότι η $\psi$ είναι ομομορφισμός. Πράγματι, έστω $r_1 + \mathrm{Ker}\varphi,\ r_2 + \mathrm{Ker}\varphi \in R/\mathrm{Ker}\varphi$. Τότε,

$$\begin{aligned} \psi\left((r_1 + \mathrm{Ker}\varphi) + (r_2 + \mathrm{Ker}\varphi)\right) &= \psi(r_1 + r_2 + \mathrm{Ker}\varphi) \\ &= \varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) \\ &= \psi(r_1 + \mathrm{Ker}\varphi) + \psi(r_2 + \mathrm{Ker}\varphi). \end{aligned}$$

Ομοίως δείχνουμε ότι,

$$\psi\left((r_1 + \mathrm{Ker}\varphi) \cdot (r_2 + \mathrm{Ker}\varphi)\right) = \psi(r_1 + \mathrm{Ker}\varphi) \cdot \psi(r_2 + \mathrm{Ker}\varphi).$$

Τέλος θα δείξουμε ότι η $\psi$ είναι ισομορφισμός. Πράγματι, έστω $r + \mathrm{Ker}\varphi \in \mathrm{Ker}\psi$. Τότε,

$$\psi(r + \mathrm{Ker}\varphi) = 0_S \Leftrightarrow \varphi(r) = 0_S \Leftrightarrow r \in \mathrm{Ker}\varphi \Leftrightarrow r + \mathrm{Ker}\varphi = 0_{R/\mathrm{Ker}\varphi}.$$

Άρα

$$\mathrm{Ker}\psi = \{0_{R/\mathrm{Ker}\varphi}\},$$

δηλαδή η $\psi$ είναι 1-1. Είναι προφανές από τον ορισμό ότι η $\psi$ είναι επί. Η απόδειξη είναι πλήρης. □

### Ασκήσεις

**1**. Έστω $R$ δακτύλιος και $I$ ιδεώδες του $R$. Να δείξετε ότι ο $R/I$ είναι μεταθετικός αν και μόνο αν ισχύει $ab - ba \in I$.

*Απόδειξη.* Παρατηρήστε ότι,

$$(a+I)(b+I) = (b+I)(a+I) \Leftrightarrow ab + I = ba + I \Leftrightarrow ab - ba \in I.$$

Επομένως ο $R/I$ είναι μεταθετικός αν και μόνο αν $ab - ba \in I$. □

**2**. Έστω $R = \mathbb{Z}_2[x]$ και $I =< x^2 + 1 >$. Να δείξετε ότι ο $R/I$ δεν είναι σώμα.

*Απόδειξη.* Ο $\mathbb{Z}_2[x]/ < x^2+1 >$ είναι μεταθετικός με μοναδιαίο στοιχείο. Θα δείξουμε ότι ο $\mathbb{Z}_2[x]/ < x^2 + 1 >$ δεν είναι ακεραία περιοχή, οπότε δεν θα είναι και σώμα. Παρατηρήστε ότι στο $\mathbb{Z}_2[x]$, ισχύει $x^2 + 1 = (x + 1)^2$. Επομένως,

$$\begin{aligned}(x+1+ < x^2+1)(x+1+ < x^2+1 >) &= (x+1)^2+ < x^2+1 > \\ &= x^2+1+ < x^2+1 > \\ &= < x^2+1 > \quad (x^2+1 \in < x^2+1 >) \\ &= 0_{\mathbb{Z}_2[x]/<x^2+1>}.\end{aligned}$$

Έστω

$$x + 1 + < x^2 + 1 > \neq 0_{\mathbb{Z}_2[x]/<x^2+1>},$$

δηλαδή

$$x + 1 + < x^2 + 1 > \neq < x^2 + 1 >,$$

γιατί $x+1 \notin < x^2+1 >$. Πράγματι, αν $x+1 \in < x^2+1 >$ τότε υπάρχει $g(x) \in \mathbb{Z}_2[x]$ ώστε

$$x + 1 = g(x)(x^2 + 1).$$

Τότε αφού $\mathbb{Z}_2[x]$ είναι ακεραία περιοχή, έπεται

$$1 = \deg g(x) + 2,$$

άτοπο. Επομένως

$$x+1+ < x^2+1 >= 0_{\mathbb{Z}_2[x]/<x^2+1>} \qquad \text{και} \qquad (x+1+ < x^2+1)(x+1+ < x^2+1 >) = 0_{\mathbb{Z}_2[x]/<x^2+1>}.$$

Άρα ο $\mathbb{Z}_2[x]/ < x^2 + 1 >$ δεν είναι ακεραία περιοχή. □

**3**. Έστω $p(x) = x^2 + 1 \in \mathbb{Z}_3[x]$ και $I =< p(x) >$.

(i) Να δείξετε ότι ο δακτύλιος $\mathbb{Z}_3[x]/I$ είναι σώμα με 9 στοιχεία.

(ii) Να εξετάσετε αν τα στοιχεία $x^4 + x + 1 + I$ και $x^4 + 2 + I$ είναι αντιστρέψιμα και να βρείτε τα αντίστροφά τους αν υπάρχουν.

*Απόδειξη.* (i) Στο $\mathbb{Z}_3$ έχουμε,

$$\begin{aligned} [0]^2+[1] &= [1]\neq[0] \\ [1]^2+[1] &= [2]\neq[0] \\ [2]^2+[1] &= [5]\neq[0] \end{aligned}$$

Άρα το $p(x)$ δεν έχει ρίζα στο $\mathbb{Z}_3$. Επειδή $\deg p(x)=2$, το $p(x)\in\mathbb{Z}_3[x]$ είναι ανάγωγο, επομένως από το θεώρημα 2.6.8, ο δακτύλιος $\mathbb{Z}_3[x]/<p(x)>$ είναι σώμα. Έστω $f(x)+I\in\mathbb{Z}_3[x]/I$. Από τον ευκλείδειο αλγόριθμο υπάρχουν $q(x),r(x)\in\mathbb{Z}_3[x]$ ώστε

$$f(x)=q(x)p(x)+r(x),\ \ \deg r(x)<\deg p(x).$$

Έχουμε $p(x)=x^2+1$, άρα $\deg r(x)<2$. Επομένως $f(x)-r(x)\in I$, άρα

$$f(x)+I=r(x)+I.$$

Επειδή $r(x)=ax+b\ \ (a,b\in\mathbb{Z}_3)$, έπεται

$$\left|\mathbb{Z}_3[x]/I\right|\leqslant 3\cdot 3=9.$$

Για να δείξουμε την ισότητα, αρκεί να δείξουμε ότι δεδομένου ότι $f(x)\in\mathbb{Z}_3[x]$ υπάρχει μοναδικό $r(x)\in\mathbb{Z}_3[x]$ με $\deg r(x)<2$ ώστε $f(x)+I=r(x)+I$. Έστω

$$f(x)+I=r(x)+I,\ \ \deg r(x)<2$$

και

$$f(x)+I=r_1(x)+I,\ \ \deg r_1(x)<2$$

Τότε,

$$r(x)+I=r_1(x)+I\Rightarrow r(x)-r_1(x)\in I(=<x^2+1>).$$

Επειδή $\deg(r(x)-r_1(x))<2$, έπεται $r(x)-r_1(x)=0$.

(ii). Από τον αλγόριθμο της ευκλειδειας διαίρεσης παίρνουμε,

$$\begin{aligned} x^4+x+1 &= (x^2-1)(x^2+1)+x+2 \\ x^2+1 &= (x+1)(x+2)-1 \\ x+2 &= (-(x+2))(-1)+0. \end{aligned}$$

Επομένως $\mu\kappa\delta(x^4+x+1,x^2+1)=1$. Τότε από την παρατήρηση 2.6.9(ii) το $x^4+x+1+I$ είναι αντιστρέψιμο. Θα υπολογίσουμε τώρα το αντίστροφό του. Συνεχίζοντας την διαδικασία στον ευκλείδειο αλγόριθμο βρίσκουμε μετά από πράξεις ότι

$$1=(x+1)(x^4+x+1)+(-(x+1)(x^2-1)-1)(x^2+1).$$

Άρα

$$1 + I = (x + 1)(x^4 + x + 1) + I$$

στο $\mathbb{Z}_3[x]$ (αφού $I =< x^2 + 1 >$). Επομένως

$$1 + I = ((x + 1) + I)(x^4 + x + 1 + I),$$

δηλαδή το αντίστροφο του $x^4 + x + 1 + I$ είναι το $x + 1 + I$.

Με χρήση του ευκλειδείου αλγορίθμου βρίσκουμε ότι $x^4 + 2 = (x^2 - 1)(x^2 + 1)$. Άρα στο $\mathbb{Z}_3[x]/ < x^2 + 1 >$ έχουμε

$$x^4 + 2 + < x^2 + 1 >=< x^2 + 1 >= 0_{\mathbb{Z}_3[x]/<x^2+1>}.$$

Επομένως το $x^4 + 2 + < x^2 + 1 >$ δεν είναι αντιστρέψιμο. □

**4**. Έστω $F$ σώμα και $a \in F$. Να δείξετε ότι υπάρχει ισομορφισμός δακτυλίων

$$F[x]/ < x - a >\cong F.$$

*Απόδειξη.* Θεωρούμε την

$$\varphi : F[x] \to F, \;\; \varphi(f(x)) = f(a).$$

Εύκολα ελέγχουμε ότι η $\varphi$ είναι καλώς ορισμένη απεικόνιση και ομομορφισμός δακτυλίων. Θα δείξουμε ότι $\mathrm{Ker}\varphi =< x - a >$. Πράγματι ο εγκλεισμός $\mathrm{Ker}\varphi \subseteq < x - a >$ είναι σαφής. Έστω $\varphi(f(x)) = 0$. Τότε $f(a) = 0$, άρα $x - a | f(x)$ στο $F[x]$. Επομένως $f(x) \in < x - a >$. Δηλαδή, $\mathrm{Ker}\varphi =< x - a >$. Είναι σαφές ότι η $\varphi$ είναι επί. Τότε από το πρώτο θεώρημα ισομορφισμών δακτυλίων παίρνουμε ότι

$$F[x]/ < x - a >\cong F.$$

□

**5**. Έστω ο δακτύλιος

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in M_2(\mathbb{Z}) : a, b \in \mathbb{Z} \right\}.$$

Να δείξετε ότι το

$$I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) : b \in \mathbb{Z} \right\}.$$

είναι ιδεώδες του $R$ και $R/I \cong \mathbb{Z}$.

*Απόδειξη.* Έστω

$$\varphi : R \to \mathbb{Z}, \;\; \varphi \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = a.$$

Εύκολα ελέγχουμε ότι η $\varphi$ είναι ομομορφισμός δακτυλίων. Τότε ο Ker$\varphi$ είναι ιδεώδες του $R$. Αλλά,

$$\text{Ker}\varphi = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{Z} \right\},$$

άρα το $I$ είναι ιδεώδες του $R$. Προφανώς η $\varphi$ είναι επί, άρα από το πρώτο θεώρημα ισομορφισμών δακτυλίων παίρνουμε $R/I \cong \mathbb{Z}$ (Ker$\varphi = I$ και Im$\varphi = \mathbb{Z}$). □

**6**. Έστω $f(x) \in F[x]$ μονικό. Να δείξετε ότι

$$\mathbb{R}[x]/ < f(x) > \cong \mathbb{C} \qquad \Leftrightarrow \qquad f(x) = x^2 + ax + b, \ \text{με} \ a^2 - 4b < 0.$$

*Απόδειξη.* Έστω $\mathbb{R}[x]/ < f(x) > \cong \mathbb{C}$. Σύμφωνα με το θεώρημα 2.6.8 έχουμε ότι το $\mathbb{R}[x]/ < f(x) >$ είναι σώμα αν και μόνο αν το $f(x) \in \mathbb{R}[x]$ είναι ανάγωγο. Αλλά τα ανάγωγα πολυώνυμα $f(x) \in \mathbb{R}[x]$ είναι τα

$$f(x) = \begin{cases} x - a, & a \in \mathbb{R} \\ x^2 + ax + b, & a, b \in \mathbb{R}, \ a^2 - 4b < 0 \end{cases}$$

Έστω $f(x) = x - a, \ a \in \mathbb{R}$. Τότε σύμφωνα με την άσκηση 4, έχουμε

$$\mathbb{R}[x]/ < x - a > \cong \mathbb{R}.$$

Επομένως $f(x) = x^2 + ax + b$, με $a^2 - 4b < 0$.

Θα δείξουμε τώρα ότι αν $a^2 - 4b < 0$, τότε $\mathbb{R}[x]/ < x^2 + ax + b > \cong \mathbb{C}$. Έστω $z \in \mathbb{C}$ ρίζα του $x^2 + ax + b$. Τότε $\overline{z}$ ρίζα του $x^2 + ax + b$ (γιατί $a, b \in \mathbb{R}$) και $z \neq \overline{z}$ γιατί $a^2 - 4b < 0$. Θεωρούμε τον ομομορφισμό δακτυλίων

$$\psi : \mathbb{R}[x] \to \mathbb{C}, \ \ \psi(f(x)) = f(z).$$

Προφανώς η $\psi$ είναι επί. Θα δείξουμε ότι Ker$\psi =< x^2 + ax + b >$. Έστω $f(x) \in F[x]$. Τότε,

$$f(x) \in \text{Ker}\psi \Leftrightarrow f(z) = 0 \Leftrightarrow f(z) = f(\overline{z}) = 0.$$

Επομένως

$$x - z | f(x) \ \ \text{στο} \ \ \mathbb{C}[x] \qquad \text{και} \qquad x - \overline{z} | f(x) \ \ \text{στο} \ \ \mathbb{C}[x].$$

Επειδή $z \neq \overline{z}$ παίρνουμε,

$$\begin{array}{rcl} (x - z)(x - \overline{z}) & | & f(x) \ \ \text{στο} \ \ \mathbb{C}[x] \Leftrightarrow \\ x^2 + ax + b & | & f(x) \text{στο} \ \ \mathbb{C}[x] \Leftrightarrow \\ x^2 + ax + b & | & f(x) \text{στο} \ \ \mathbb{R}[x] \ \ (\text{αφού} \ \ x^2 + ax + b, f(x) \in \mathbb{R}[x]). \end{array}$$

Άρα $\mathrm{Ker}\psi =< x^2+ax+b >$. Τότε από το πρώτο θεώρημα ισομορφισμών δακτυλίων έπεται ότι,

$$\mathbb{R}[x]/ < x^2+ax+b > \cong \mathbb{C}.$$

*Σημείωση.*

$$\mathbb{R}[x]/ < x^2+1 > \cong \mathbb{R}[x]/ < x^2+x+1 > \cong \mathbb{C}.$$

□

**7**. Να βρείτε ένα $f(x) \in \mathbb{R}[x]$ ώστε

$$I = \{g(x) \in \mathbb{R}[x] : g(2+5i) = g(0) = 0\} =< f(x) > .$$

Αληθεύει ότι $\mathbb{R}[x]/ < f(x) >$ είναι ακεραία περιοχή;

*Απόδειξη.* Έστω $g(x) \in I$. Τότε,

$$g(0) = 0 \Leftrightarrow x | g(x) \text{ στο } \mathbb{R}[x].$$

Επίσης,

$$g(2+5i) = 0 \Leftrightarrow g(2-5i) = 0 \Leftrightarrow x-(2+5i) | g(x) \text{ στο } \mathbb{C}[x] \quad \text{και} \quad x-(2-5i) | g(x) \text{ στο } \mathbb{C}[x].$$

Επειδή $\mu\kappa\delta(x-(2-5i), x-(2+5i)) = 1$, έπεται

$$x^2-4x+29 | g(x) \text{ στο } \mathbb{C}[x].$$

Αλλά $x^2-4x+29,\ g(x) \in \mathbb{R}[x]$, οπότε από το λήμμα 2.4.9 έπεται ότι $x^2-4x+29 | g(x)$ στο $\mathbb{R}[x]$. Δηλαδή,

$$g(x) \in I \Leftrightarrow x^2-4x+29 | g(x) \text{ στο } \mathbb{R}[x] \quad \text{και} \quad x | g(x) \text{ στο } \mathbb{R}[x].$$

Συνεπώς μπορούμε να θέσουμε $f(x) = x^3-4x^2+29x$. Τότε θα έχουμε $I =< f(x) >$.

Έχουμε $I =< f(x) >,\ f(x) = x^3-4x^2+29x = x(x^2-4x+29)$. Θέτουμε,

$$a = x+ < f(x) >,\ b = x^2-4x+29+ < f(x) > \in \mathbb{R}[x]/ < f(x) > .$$

Παρατηρήστε ότι,

$$a \cdot b = f(x)+ < f(x) > =< f(x) > = 0_{\mathbb{R}[x]/<f(x)>},$$

$a \neq 0$, αφού $f(x) \nmid x$ και $b \neq 0$, αφού $f(x) \nmid x^2-4x+29$. Επομένως $\mathbb{R}[x]/ < f(x) >$ δεν είναι ακεραία περιοχή. □

**8**. Έστω $f(x) = x^2+x+1 \in \mathbb{Z}_5[x]$ και $I =< f(x) >$.

(i) Να δείξετε ότι το $\mathbb{Z}_5[x]/ < f(x) >$ είναι σώμα με 25 στοιχεία.

(ii) Να βρείτε (αν υπάρχει) το αντίστροφο του $x^3+x+1+<f(x)>\in \mathbb{Z}_5[x]/<f(x)>$

*Απόδειξη.* (i). Παρατηρήστε ότι για κάθε $a(x)\in\mathbb{Z}_5,\ a^2+a+1\neq 0$ (για παράδειγμα, για $a=3,\ a^2+a+1=9+3+1=13=3\neq 0$ στο $\mathbb{Z}_5$). Επειδή $\deg(x^2+x+1)=2$ και το $\mathbb{Z}_5$ είναι σώμα (5 πρώτος), το $f(x)\in\mathbb{Z}_5[x]$ είναι ανάγωγο. Από το θεώρημα 2.6.8 έπεται ότι το $\mathbb{Z}_5[x]/<f(x)>$ είναι σώμα (αφού το $\mathbb{Z}_5$ είναι σώμα).

Έστω $g(x)\in<f(x)>$. Θα δείξουμε ότι υπάρχει μοναδικό $h(x)\in\mathbb{Z}_5[x]$ με $\deg h(x)\leqslant 1$, ώστε

$$h(x)+<f(x)>=g(x)+<f(x)>.$$

Τότε, επειδή $h(x)=ax+b\in\mathbb{Z}_5[x]$, παίρνουμε $\left|\frac{\mathbb{Z}_5[x]}{f(x)}\right|=5^2=25$.

Ύπαρξη. Από τον αλγόριθμο της ευκλειδειας διαίρεσης έχουμε,

$$g(x)=q(x)f(x)+r(x),\ \ \deg r(x)<\deg f(x)=2.$$

Τότε,

$$g(x)+<f(x)>=r(x)+<f(x)>,$$

αφού $g(x)r(x)=q(x)f(x)\in<f(x)>$.

Μοναδικότητα. Έστω $h_1(x),h_2(x)\in\mathbb{Z}_5[x]$ με $\deg h_1(x),\ \deg h_2(x)\leqslant 1$ και

$$h_1(x)+<f(x)>=h_2(x)+<f(x)>.$$

Τότε,

$$f(x)\mid h_1(x)-h_2(x)\overset{(\mathbb{Z}_5\ \text{σώμα})}{\Longrightarrow} h_1(x)-h_2(x)=0,$$

αφού $\deg(h_1(x)-h_2(x))<2$.

(ii). Από τον αλγόριθμο της ευκλειδειας διαίρεσης έχουμε,

$$\begin{aligned}
x^3+x+1 &= (x^2+x+1)(x-1)+x+2\\
x^2+x+1 &= (x+2)(x-1)+3\\
3 &= x^2+x+1-(x+2)(x-1)\\
&= x^2+x+1-\left[(x^3+x+1)-(x^2+x+1)(x-1)\right](x-1)\\
&= (x^2+x+1)(1+(x-1)^2)+(x^3+x+1)(-x+1).
\end{aligned}$$

Πολλαπλασιάζοντας με το αντίστροφο του 3 στο $\mathbb{Z}_5$, δηλαδή με το 2 παίρνουμε,

$$1=2(x^2+x+1)(1+(x-1)^2)+(x^3+x+1)(-2x+2). \tag{2.6.3}$$

Τότε στο $\mathbb{Z}_5/<f(x)>$ από την (2.6.3) παίρνουμε,

$$1+<f(x)>=\left((x^3+x+1)+<f(x)>\right)\left((-2x+2)+<f(x)>\right).$$

Επειδή ο $\mathbb{Z}_5/<f(x)>$ είναι μεταθετικός, το $x^3+x+1+<f(x)>$ είναι αντιστρέψιμο και το αντίστροφό του είναι το $-2x+2+<f(x)>$. □

**9**. Έστω $f(x) \in \mathbb{Q}[x]$ που έχει ρίζα το $a + b\sqrt{2}$, όπου $a, b \in \mathbb{Q}$.

(i) Να δείξετε ότι έχει ρίζα το $a - b\sqrt{2}$.

(ii) Να δείξετε ότι υπάρχει ισομορφισμός δακτυλίων $\mathbb{Q}[x]/ < x^2 - 2 > \backsimeq \mathbb{Q}[\sqrt{2}]$.

*Απόδειξη*. (i). Θεωρούμε τον δακτύλιο $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{C} : a, b \in \mathbb{Q}\}$ (έχουμε δει ότι είναι υποδακτύλιος του $\mathbb{C}$ και την απεικόνιση

$$\varphi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}], \;\; a + b\sqrt{2} \mapsto a - b\sqrt{2}.$$

Θα δείξουμε ότι η $\varphi$ είναι ομομορφισμός δακτυλίων. Πράγματι, εύκολα ελέγχουμε ότι η $\varphi$ είναι καλώς ορισμένη. Παρατηρήστε ότι,

$$\begin{aligned} \varphi\Big((a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})\Big) &= \varphi(a_1 + a_2 + (b_1 + b_2)\sqrt{2}) \\ &= a_1 + a_2 - (b_1 + b_2)\sqrt{2} \\ &= a_1 - b_1\sqrt{2} + a_2 - b_2\sqrt{2} \\ &= \varphi(a_1 + b_1\sqrt{2}) + \varphi(a_2 + b_2\sqrt{2}) \end{aligned}$$

και

$$\begin{aligned} \varphi\Big((a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})\Big) &= \varphi(a_1a_2 + 2b_1b_2 + (a_1b_2 + a_2b_1)\sqrt{2}) \\ &= a_1a_2 + 2b_1b_2 - (a_1b_2 + a_2b_1)\sqrt{2} \\ &= (a_1 - b_1\sqrt{2})(a_2 - b_2\sqrt{2}) \\ &= \varphi(a_1 + b_1\sqrt{2})\varphi(a_2 + b_2\sqrt{2}). \end{aligned}$$

Έστω τώρα

$$f(x) = f_nx^n + \cdots + f_1x + f_0 \in \mathbb{Q}[x] \qquad \text{και} \qquad f(a + b\sqrt{2}) = 0,$$

όπου $a, b \in \mathbb{Q}$. Τότε,

$$f_n(a + b\sqrt{2})^n + \cdots + f_1(a + b\sqrt{2}) + f_0 = 0.$$

Επομένως,

$$\begin{aligned} \varphi(f_n)\Big(\varphi(a + b\sqrt{2})\Big)^n + \cdots + \varphi(f_1)\varphi(a + b\sqrt{2}) + \varphi(f_0) &= \varphi(0) \Rightarrow \\ f_n(a - b\sqrt{2})^n + \cdots + f_1(a - b\sqrt{2}) + f_0 &= 0 \Rightarrow \\ f(a - b\sqrt{2}) &= 0. \end{aligned}$$

(ii). Ορίζουμε

$$\psi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}], \;\; f(x) \mapsto f(\sqrt{2}).$$

Εύκολα ελέγχουμε ότι η $\psi$ είναι καλώς ορισμένη, ομομορφισμός δακτυλίων. Προφανώς η $\psi$ είναι επί. Πράγματι, έστω $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Τότε $a+b\sqrt{x} \in \mathbb{Q}[x]$ και $f(a+b\sqrt{x}) = a+b\sqrt{2}$.

Έχουμε,

$$\text{Ker}\psi = \{f(x) \in Q[x] : f(\sqrt{2}) = 0\}.$$

Παρατηρήστε ότι,

$$\begin{aligned} f(\sqrt{2}) = 0 &\Leftrightarrow f(-\sqrt{2}) = f(\sqrt{2}) = 0 \\ &\Leftrightarrow x-(-\sqrt{2}) \mid f(x) \text{ στο } \mathbb{Q}[\sqrt{2}][x] \quad \text{και} \quad x-\sqrt{2} \mid f(x) \text{ στο } \mathbb{Q}[\sqrt{2}][x] \\ &\Leftrightarrow (x-(-\sqrt{2}))(x-\sqrt{2}) \mid f(x) \text{ στο } \mathbb{Q}[\sqrt{2}][x] \\ &\Leftrightarrow x^2-2 \mid f(x) \text{ στο } \mathbb{Q}[\sqrt{2}][x] \\ &\Leftrightarrow x^2-2 \mid f(x) \text{ στο } \mathbb{Q}[x], \end{aligned}$$

όπου στη τελευταία συνεπαγωγή χρησιμοποιήσαμε το ανάλογο του λήμματος 2.4.9. Αν $a(x), b(x) \in \mathbb{Q}[x]$, τότε $a(x) \mid b(x)$ στο $\mathbb{Q}[x]$ αν και μόνο αν $a(x) \mid b(x)$ στο $\mathbb{Q}[\sqrt{2}][x]$. Επομένως,

$$f(x) \in \text{Ker}\psi \Leftrightarrow x^2-2 \mid f(x) \text{ στο } \mathbb{Q}[x],$$

δηλαδή $\text{Ker}\psi =< x^2-2 >$. Από το πρώτο θεώρημα ισομορφισμών δακτυλίων έπεται, $\mathbb{Q}[x]/ < x^2-2 > \backsimeq \mathbb{Q}[\sqrt{2}]$. □

**10**. Έστω $F$ πεπερασμένο σώμα. Υπολογίστε το $c = \sum_{a \in F} a$.

*Απόδειξη.* Αν $|F| = 2$, τότε $F = \{0_F, 1_F\}$ και $c = 1_F$. Έστω $|F| > 2$. Θα δείξουμε ότι $c = 0$. Έστω $a \in F$, $a \neq 0_F$, $a \neq 1_F$. Γνωρίζουμε ότι το σύνολο $F \setminus \{0_F\}$ είναι ομαδα ως προς τον πολλαπλασιασμό του σώματος $F$. Άρα,

$$b\,(F \setminus \{0\}) = F \setminus \{0\}.$$

Επομένως,

$$b \cdot c = c \Rightarrow (b-1)c = 0 \overset{(b-1 \neq 0)}{\Rightarrow} c = 0.$$

□

**11**. Να βρείτε όλα τα πολυώνυμα $f(x) \in \mathbb{Z}_2[x]$ βαθμού 5, με

$$\text{μκδ}(f(x), x^3+x+1) \neq 1 \qquad \text{και} \qquad \text{μκδ}(f(x), x^2+1) \neq 1.$$

*Λύση.* Παρατηρήστε ότι,

$$\text{μκδ}(f(x), x^3+x+1) \neq 1 \Leftrightarrow x^3+x+1 \mid f(x),$$

αφού το $x^3+x+1$ είναι ανάγωγο στο $\mathbb{Z}_2[x]$. Επίσης στο $\mathbb{Z}_2[x]$,

$$\mu\kappa\delta(f(x),x^2+1)=\mu\kappa\delta(f(x),(x+1)^2)\neq 1\Leftrightarrow x+1\mid f(x).$$

Επομένως και οι δύο συνθήκες ισχύουν αν και μόνο αν

$$(x+1)(x^3+x+1)\mid f(x)\Leftrightarrow \mathrm{beg}g(x)=5\ \Leftrightarrow f(x)=\begin{cases}x(x+1)(x^3+x+1)\\ \text{ή}\\ (x+1)^2(x^3+x+1)\end{cases}$$

□

**12**. Να βρείτε πόσες ρίζες έχει το $f(x)=x^p+x+1\in\mathbb{Z}_p[x]$ στο $\mathbb{Z}_p$, όπου $p$ πρώτος.

*Λύση.* Παρατηρήστε ότι για κάθε $\alpha\in\mathbb{Z}_p$, το

$$f(\alpha)=\alpha^p+a+1=2\alpha+1$$

έχει το πολύ μια ρίζα. □

**13**. Έστω $R$ δακτύλιος και $S\subseteq R$. Στα ακόλουθα ερωτήματα να εξετάσετε αν ο $S$ είναι υποδακτύλιος του $R$, αν είναι μεταθετικός δακτύλιος με $1_S$, ακεραία περιοχή και σώμα.

(i) $R=M_2(\mathbb{R}),\ S=\left\{\begin{pmatrix}0&0\\0&\alpha\end{pmatrix},\ \alpha\in\mathbb{R}\right\}$.

(ii) $R=M_2(\mathbb{R}),\ S=\left\{\begin{pmatrix}1&0\\0&\alpha\end{pmatrix},\ \alpha\in\mathbb{R}\right\}$.

(iii) $R=\mathbb{Z}[\sqrt{2}],\ S=\{\alpha+\beta\sqrt{2},\ \beta\ \text{άρτιος}\}$.

(iv) $R=\mathbb{Z}[\sqrt{2}],\ S=\{\alpha+\beta\sqrt{2},\ \alpha,\beta\ \text{άρτιοι}\}$.

(v) $R=\mathbb{Z}[i],\ S=\{\alpha=\beta i: a\equiv 0\mathrm{mod}10,\ b\equiv 0\mathrm{mod}10\}$.

(vi) $R=F(\mathbb{R},\mathbb{R})=\{f:\mathbb{R}\to\mathbb{R}\},\ S=\{f\in F(\mathbb{R},\mathbb{R}): f(1)=1\}$ είναι υποδακτύλιος;

(vii) $R=\mathbb{Z}_{12},\ S=\{[0],[4],[8]\}$.

*Λύση.* (i). Παρατηρήστε ότι, $S\neq\emptyset$, $\begin{pmatrix}0&0\\0&1\end{pmatrix}\in S$. Έστω $s_1,s_2\in S$, $s_1=\begin{pmatrix}0&0\\0&\alpha\end{pmatrix}$, $s_2=\begin{pmatrix}0&0\\0&\beta\end{pmatrix}$, $\alpha,\beta\in\mathbb{R}$. Παρατηρήστε ότι,

$$s_1-s_2=\begin{pmatrix}0&0\\0&\alpha\end{pmatrix}-\begin{pmatrix}0&0\\0&\beta\end{pmatrix}=\begin{pmatrix}0&0\\0&\alpha-\beta\end{pmatrix}\in S,\ \ \alpha-\beta\in\mathbb{R}.$$

και

$$s_1s_2=\begin{pmatrix}0&0\\0&\alpha\end{pmatrix}\begin{pmatrix}0&0\\0&\beta\end{pmatrix}=\begin{pmatrix}0&0\\0&\alpha\cdot\beta\end{pmatrix}\in S,\ \ \alpha\cdot\beta\in\mathbb{R}.$$

Άρα ο $S$ είναι υποδακτύλιος του $R$. Παρατηρήστε ότι,

$$S_2 \cdot S_1 = \begin{pmatrix} 0 & 0 \\ 0 & \beta \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & \alpha \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & \beta\alpha \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & \alpha\beta \end{pmatrix} = S_1 \cdot S_2.$$

Άρα ο $S$ είναι μεταθετικός. Έστω $S_1 = \begin{pmatrix} 0 & 0 \\ 0 & \alpha \end{pmatrix}$. Για να δείξουμε ότι έχει $1_S$ αρκεί να βρούμε ένα $S_2 = \begin{pmatrix} 0 & 0 \\ 0 & \beta \end{pmatrix}$ ώστε

$$\begin{aligned} S_1 \cdot S_2 &= S_2 \Rightarrow \begin{pmatrix} 0 & 0 \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & \beta \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & \alpha \end{pmatrix} \Rightarrow \\ \begin{pmatrix} 0 & 0 \\ 0 & \alpha\beta \end{pmatrix} &= \begin{pmatrix} 0 & 0 \\ 0 & \alpha \end{pmatrix} \Rightarrow \alpha\beta = \alpha \Rightarrow \beta = 1. \end{aligned}$$

Άρα,

$$1_S = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = S_2.$$

Πράγματι,

$$S_1 \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot S_1 = S_1.$$

Ελέγχουμε τώρα αν είναι σώμα. Έστω $S = \begin{pmatrix} 0 & 0 \\ 0 & \alpha \end{pmatrix}$, $S' = \begin{pmatrix} 0 & 0 \\ 0 & \beta' \end{pmatrix}$ ώστε,

$$S \cdot S' = 1_S \Rightarrow \begin{pmatrix} 0 & 0 \\ 0 & \alpha\beta \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \alpha\beta = 1 \Rightarrow \beta = \alpha^{-1}.$$

Άρα, $S' = S^{-1}$. Επομένως είναι σώμα (άρα και ακεραία περιοχή).

(ii). Παρατηρήστε ότι, $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin S$ ( θα έπρεπε $0_S = 0_R$). Διαφορετικά, αν $S_1 = \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}$, $S_2 = \begin{pmatrix} 1 & 0 \\ 0 & \beta \end{pmatrix}$, τότε

$$S_1 - S_2 = \begin{pmatrix} 0 & 0 \\ 0 & \alpha - \beta \end{pmatrix} \notin S.$$

(iii). Παρατηρήστε ότι $S \neq \emptyset$, αφού το $2\sqrt{2} \in S$. Έστω $s_1 = \alpha_1 + \beta_1\sqrt{2}$, $s_2 = \alpha_2 + \beta_2\sqrt{2} \in S$. Τότε,

$$s_1 - s_2 = (\alpha_1 + \beta_1\sqrt{2}) - (\alpha_2 + \beta_2\sqrt{2}) = (\alpha_1 - \alpha_2) + (\beta_1 - \beta_2)\sqrt{2} \in S$$

($\alpha_1 - \alpha_2 \in \mathbb{Z}$, $b_1 - b_2$ άρτιος) και

$$s_1 s_2 = (\alpha_1 + \beta_1\sqrt{2})(\alpha_2 + \beta_2\sqrt{2}) = (\alpha_1\alpha_2 + 2\beta_1\beta_2) + (\alpha_1\beta_2 + \alpha_2\beta_1)\sqrt{2} \in S$$

($\alpha_1\alpha_2 + 2\beta_1\beta_2 \in \mathbb{Z}$ και $\alpha_1\beta_2 + \alpha_2\beta_1$ άρτιος). Άρα ο $S$ είναι υποδακτύλιος του $R$. Παρατηρήστε ότι,

$$\begin{aligned} s_2 s_1 &= (\alpha_2 + \beta_2\sqrt{2})(\alpha_1 + \beta_1\sqrt{2}) = (\alpha_2\alpha_1 + 2\beta_2\beta_1) + (\alpha_2\beta_1 + \alpha_1\beta_2) \\ &= (\alpha_1\alpha_2 + 2\beta_1\beta_2) + (\alpha_1\beta_2 + \alpha_2\beta_1)\sqrt{2} = s_1 s_2, \end{aligned}$$

άρα ο $S$ είναι μεταθετικός. Επίσης $1 \in \mathbb{R}$ είναι μονάδα του $S$. Πράγματι, αν $s = \alpha + \beta\sqrt{2}$, τότε $s \cdot 1 = 1 \cdot s = s$. Ο $S \subseteq \mathbb{Z}[\sqrt{2}] \subseteq \mathbb{R}$ και ο $\mathbb{R}$ δεν έχει μηδενοδιαιρέτες. Άρα και ο $S$ δεν έχει μηδενοδιαιρέτες. Επομένως ο $S$ ακεραία περιοχή. Όμως δεν είναι σώμα. Πράγματι,

$$2 \in S,\ \ 2^{-1} = \frac{1}{2} \notin \mathbb{Z},\ \ 2\sqrt{2} \in S,\ \ \frac{1}{2\sqrt{2}} = \frac{1\sqrt{2}}{4} \notin S.$$

(iv). $S \neq \emptyset$ $(2 + 2\sqrt{2} \in S)$. Έστω $s_1 = \alpha_1 + \beta_1\sqrt{2}$, $s_2 = \alpha_2 + \beta_2\sqrt{2} \in S$. Τότε,

$$s_1 - s_2 = (\alpha_1 - \alpha_2) + (\beta_1 - \beta_2)\sqrt{2} \in S$$

και

$$s_1 s_2 = (\alpha_1\alpha_2 + 2\beta_1\beta_2) + (\alpha_1\beta_2 + \alpha_2\beta_1)\sqrt{2} \in S.$$

Άρα ο $S$ είναι υποδακτύλιος του $R$. Ο $S$ είναι μεταθετικός ($s_1 s_2 = s_2 s_1$). Έστω ότι ο $S$ έχει μονάδα. Τότε πρέπει,

$$\begin{aligned} (2 + 2\sqrt{2})(\alpha + \beta\sqrt{2}) &= (2 + \sqrt{2}) \Rightarrow \\ (2\alpha + 4\beta) + (2\beta + 2\alpha)\sqrt{2} &= 2 + 2\sqrt{2} \Rightarrow \\ 2\beta + 2\alpha &= 2 \Rightarrow \\ \beta + \alpha &= 1, \end{aligned}$$

άτοπο. Επομένως ο $S$ δεν έχει $1_S$, άρα δεν είναι σώμα ούτε ακεραία περιοχή.

(v). Έστω $s_1 = \alpha_1 + \beta_1 i$, $s_2 = \alpha_2 + \beta_2 i \in S$. Τότε,

$$s_1 - s_2 = (\alpha_1 - \alpha_2) + (\beta_1 - \beta_2) \cdot i \in S$$

(αφού $\alpha_1 - \alpha_2 \equiv 0 \bmod 10$ και $b_1 - b_1 \equiv 0 \bmod 10$) και

$$s_1 \cdot s_2 = (\alpha_1\alpha_2 - \beta_1\beta_2) + (\alpha_1\beta_2 + \beta_1\alpha_2)i \in S.$$

Επομένως ο $S$ είναι υποδακτύλιος του $R$. Επίσης $s_1 \cdot s_2 = s_2 \cdot s_1$, δηλαδή ο $S$ είναι μεταθετικός. Έστω ότι ο $S$ έχει μονάδα. Τότε πρέπει,

$$\begin{aligned} (10+10i)(\alpha+\beta i) &= 10+10i \Rightarrow \\ (10\alpha-10\beta)+(10\beta+10\alpha)i &= 10+10i \Rightarrow \\ 10\beta+10\alpha &= 10 \\ \beta+\alpha &= 1, \end{aligned}$$

άτοπο. Επομένως ο $S$ δεν έχει $1_S$.

(vi). Έστω $f, g \in S$. Τότε $f(1) = 1 = g(1)$. Παρατηρήστε ότι, $f-g \notin S$. Πράγματι,

$$(f-g)(1) = f(1) - g(1) = 0.$$

Επομένως ο $S$ δεν είναι υποδακτύλιος.

(vii). Κάνοντας πράξεις βλέπουμε ότι,

$$[\alpha]-[\beta],\ \ [\alpha]\cdot[\beta] \in S,\ \ \text{για κάθε}\ \ [\alpha],[\beta] \in S$$

και

$$[\alpha][\beta] = [\beta][\alpha],$$

δηλαδή ο $S$ είναι μεταθετικός. Το $[4]$ είναι μοναδιαίο στοιχείο. Παρατηρήστε ότι,

$$[4][4] = [16] = [4],$$

$$[4][8] = [32] = [8],$$

$$[8][8] = [64] = [4].$$

Επομένως ο $S$ δεν έχει μηδενοδιαιρέτες, οπότε είναι ακεραία περιοχή. Επίσης ο $S$ είναι σώμα, κάθε στοιχείο του $S$ είναι αντιστρέψιμο. □

# Κεφάλαιο 3

# Ομάδες

Η θεωρία ομάδων αφορά την μελέτη της συμμετρίας, για παράδειγμα ενός υποσυνόλου του $\mathbb{R}^n$, των ριζών ενός πολυωνύμου, μιας αλγεβρικής δομής, των λύσεων ενός συστήματος διαφορικών εξισώσεων.

## 3.1 Παραδείγματα ομάδων και συμμετρικές ομάδες

**Ορισμός 3.1.1.** (i) *Μια απεικόνιση $f : \mathbb{R}^n \to \mathbb{R}^n$ λέγεται ισομετρία αν $d(x, y) = d(f(x), f(y))$ για κάθε $x, y \in \mathbb{R}^n$, όπου $d(x, y)$ η συνήθης ευκλείδεια απόσταση των $x, y$ .*

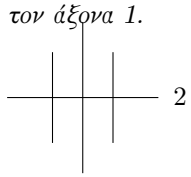
(ii) *Έστω $M \neq \emptyset$, $M \subseteq \mathbb{R}^n$. Μια ισομετρία $f : \mathbb{R}^n \to \mathbb{R}^n$, ώστε $f(M) = M$ λέγεται συμμετρία του $M$. Το σύνολο των συμμετριών του $M$ συμβολίζεται με $S(M)$.*

**Παραδείγματα 3.1.2.** *(Διαισθητικά. Δεν δικαιολογούμε γιατί οι αναγραφόμενες συμμετρίες του $M$ είναι όλες συμμετρίες του $M$.)*

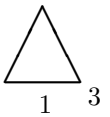
(i)


$S(M) = \{1, \varrho\}$, $1 : \mathbb{R}^2 \to \mathbb{R}^2$, $1(x) = x$, *όπου* $\varrho : \mathbb{R}^2 \to \mathbb{R}^2$ *η ανάκλαση ως προς τον άξονα 1.*

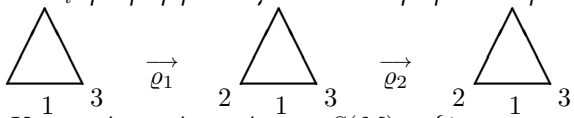
(ii)




$S(M) = \{1, \varrho_1, \varrho_2, \sigma\}$, *όπου* $\varrho_i$ *η ανάκλαση ως προς τον άξονα* $i$ *και* $\sigma$ *η στροφή κατά γωνία* $180^o$.

(iii) *Ισόπλευρο τρίγωνο.* 


$S(M) = \{1, \varrho_1, \varrho_2, \varrho_3, \sigma_1, \sigma_2\}$, *όπου* $\varrho_i$ *η ανάκλαση ως προς τον άξονα* $i$ $(i = 1, 2, 3)$ *και* $\sigma_i$ *η στροφή κατά γωνία* $120 \cdot i$ *μοιρών. Παρατηρήστε ότι* $\varrho_2 \circ \varrho_1 = \sigma_2$. *Πράγματι,*




$=$ *εικόνα του* $\sigma_2$

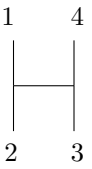
(iv) *Κανονικό κυρτό πεντάγωνο.* $S(M) = \{1, \varrho_1, \cdots, \varrho_5, \sigma_1, \cdots, \sigma_4\}$, *όπου* $\varrho_i$ *η ανάκλαση ως προς τον άξονα* $i$ *και* $\sigma_i$ *η στροφή κατά γωνία* $72 \cdot i$ *μοιρών (*$i$ *οι κορυφές του πενταγώνου).*

(v) *Κανονικό πεντάγωνο (όχι κυρτό). Το* $S(M)$ *είναι ίδιο με το παράδειγμα (iv).*

(vi) 

$S(M) = \{1, \tau_i, \tau_i^{-1}, \tau_i^2, \tau_i^{-2}, \cdots\}$, *όπου* $\tau_i$ *η μετατόπιση του άξονα κατά 1 μονάδα.*

*Σημείωση.*




$S(M) = \{1, \varrho_1, \varrho_2, \sigma\}$

**Ερώτηση 3.1.3.** *Υπάρχει ισομετρία* $f$ *του* $M$ *ώστε* $f(1) = 4, f(2) = 2, f(3) = 3, f(4) = 1$*;*

*Δεν υπάρχει τέτοια ισομετρία, αφού*

$$d(1,2) \neq d(f(1), f(2)) = d(4,2).$$

**Ορισμός 3.1.4.** *Έστω* $G$ *ένα σύνολο με* $G \times G \to G$, $(a, b) \mapsto a \star b$ *μια πράξη του* $G$. *Το ζεύγος* $(G, \star)$ *λέγεται ομάδα αν ισχύουν τα ακόλουθα.*

(i) $(a \star b) \star c = a \times (b \star c)$, *για κάθε* $a, b, c \in G$ *(προσεταιριστική ιδιότητα).*

(ii) *Υπάρχει* $e \in G$ *ώστε* $a \star e = e \star a = a$, *για κάθε* $a \in G$ *(ύπαρξη ουδέτερου στοιχείου).*

(iii) *Για κάθε* $a \in G$, *υπάρχει* $a' \in G$ *ώστε* $a \star a' = a' \star a = e$ *(ύπαρξη αντιστρόφου στοιχείου).*

*Αν επιπλέον ισχύει $a \star b = b \star a$, για κάθε $a, b \in G$ θα λέμε ότι η ομάδα $G$ είναι αβελιανή.*

**Παρατηρήσεις 3.1.5.** *Έστω $(G, \star)$ μια ομάδα.*

(i) *Το $e$ του παραπάνω ορισμού είναι μοναδικό. Πράγματι, αν $e_1, e_2 \in G$ με*

$$e_i \star a = a \star e_i,$$

*για κάθε $a \in G$, τότε $e_1 = e_1 \star e_2 = e_2$.*

(ii) *Το $a \in G$ του ορισμού είναι μοναδικό. Πράγματι, αν*

$$a \star a' = a' \star a = e \qquad \text{και} \qquad a \star a'' = a'' \star a = e,$$

*τότε*

$$a'' = e \star a'' = (a' \star a) \star a'' = a' \star (a \star a'') = a' \star e = a'.$$

(iii) *Για κάθε $a, b \in G$ ισχύει, $(a \star b)^{-1} = b^{-1} \star a^{-1}$. Πράγματι,*

$$\begin{aligned} (a \star b) \star (b^{-1} \star a^{-1}) &= a \star ((b \star b^{-1}) \star a^{-1}) \\ &= a \star (e \star a^{-1}) \\ &= a \star a^{-1} = e. \end{aligned}$$

*(Σημείωση. Αν $c, d \in G$ ($G$ ομάδα) και $c \star d = e$, τότε $c = d^{-1}$.)*

**Παραδείγματα 3.1.6.** *1. Τα σύνολα $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ είναι αβελιανές ομάδες με πράξη την πρόσθεση αριθμών (ουδέτερο στοιχειο το $0$). Τα σύνολα $\{1, -1\}$, $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$ είναι αβελιανές ομάδες με πράξη τον πολλαπλασιασμό αριθμών (ουδέτερο στοιχείο το $1$).*

*2. Γενικότερα, αν $(R, +, \cdot)$ δακτύλιος τότε $(R, +)$ είναι αβελιανή ομάδα (ουδέτερο στοιχείο το $0_R$). Αν $(R, +, \cdot)$ έχει μονάδα $1_R$, τότε το $(U(R), \cdot)$ είναι ομάδα (όχι γενικά αβελιανή) (ουδέτερο στοιχείο είναι το $1_R$). Υπενθμίζουμε ότι $U(R) =$ το σύνολο των αντιστρέψιμων στοιχείων του $R$. Ειδικότερα, αν $R = \mathbb{Z}_n$, τότε $(\mathbb{Z}_n, +)$ και $(U(\mathbb{Z}_n), \cdot)$ είναι αβελιανές ομάδες. Αν $R = M_n(F)$, όπου $F$ σώμα τότε $(M_n(F), +)$ είναι αβελιανή ομάδα και $(U(M_n(F)), \cdot)$ είναι ομάδα. Υπενθμίζουμε ότι,*

$$U(M_n(F)) = \{A \in M_n(F) : \det A \neq 0\}.$$

*Συμβολισμός. $GL_n(F) = U(M_n(F))$, όπου $GL_n(F)$ η γενική γραμμική ομάδα.*

*3. Έστω $X \neq 0$ ένα σύνολο. Έστω*

$$S(X) = \{f : X \to X : f \ \ 1-1 \ \ \text{και επί}\}.$$

*Με πράξη την σύνθεση συναρτήσεων, το $S(X)$ είναι σύνθεση συναρτήσεων. Πράγματι έχουμε,*

(α′)
$$(f \circ g) \circ h = f \circ (g \circ h),$$
για κάθε $f, g, h \in S(X)$.

(β′) Αν $1_x : X \to X$ είναι η απεικόνιση $1_x(x) = x$ για κάθε $x \in X$, τότε
$$f \circ 1_x = 1_x \cdot f = f,$$
για κάθε $f \in S(X)$.

(γ′) Αν $f \in S(X)$, τότε η $f$ ως 1-1 και επί έχει αντιστροφη συνάρτηση $f^{-1} : X \to X$. Η $f^{-1}$ είναι 1-1 και επί, δηλαδή $f^{-1} \in S(X)$ και
$$f^{-1} \circ f = f \circ f^{-1} = 1_x.$$

4. Έστω $E = \{z \in \mathbb{C} : |z| = 1\}$ ο μοναδιαίος κύκλος. Τότε ως προς τον πολλαπλασιασμό μιγαδικών το $E$ είναι ομάδα. Πράγματι,

(α′) αν $z_1, z_2 \in E$, τότε $|z_1 z_2| = |z_1||z_2| = 1$. Άρα $z_1 z_2 \in E$.

(β′) Προφανώς ισχύει $z_1(z_2 z_3) = (z_1 z_2)z_3$, για κάθε $z_i \in E$.

(γ′) $1 \cdot z = z \cdot 1 = z$, για κάθε $z \in E$.

(δ′) Αν $z \in E$ τότε $z \neq 0$ και το $\frac{1}{z} (\in \mathbb{C})$ ικανοποιεί την
$$\left|\frac{1}{z}\right| = \frac{1}{|z|} = \frac{1}{1} = 1.$$

Άρα $\frac{1}{z} \in E$. Επίσης έχουμε $z \cdot \frac{1}{z} = 1$.

5. Έστω $n \in \mathbb{Z}_{>0}$. Θέτουμε $E_n = \{z \in \mathbb{C} : z^n = 1\}$. Είναι σαφές ότι το $E_n$ είναι μια ομάδα ως προς τον πολλαπλασιασμό μιγαδικών (όπως πριν). Εδώ έχουμε, $|E_n| = n$ (οι $n$- οστές ρίζες του 1 είναι οι $z_\kappa = \cos\frac{2\pi}{n}\kappa + i\sin\frac{2\pi}{n}$, $\kappa = 0, 1, \ldots, n-1$). Τα $z_0, \cdots, z_{n-1}$ είναι ανά δύο διάφορα και από το θεώρημα De Moivre ισχύει $z_\kappa^n = 1$ για κάθε $\kappa$. Άρα $z_\kappa \in E_n$ για κάθε $\kappa$ και $|E_n| \geqslant n$. Επειδή το $\mathbb{C}$ είναι σώμα και $x^n - 1 \in \mathbb{C}[x]$ βαθμού $n$, παίρνουμε $|E_n| \leqslant n$. Άρα $|E_n| = n$.

6. Έστω $a, b \in \mathbb{R}$, $a \neq 0$. Ορίζουμε
$$T_{a,b} : \mathbb{R} \to \mathbb{R}, \;\; T_{a,b}(x) = ax + b.$$
Έστω $G = \{T_{a,b} : a, b \in \mathbb{R}, \; a \neq 0\}$. Θα δείξουμε ότι ως προς την σύνθεση συναρτήσεων η $G$ είναι ομάδα. Έστω $T_{a,b}$ και $T_{c,d} \in G$. Τότε,
$$\begin{aligned} T_{a,b} \circ T_{c,d}(x) &= T_{a,b}\left(T_{c,d}(x)\right) = T_{a,b}(cx + d) \\ &= a(cx + d) + b = acx + ad + b. \end{aligned}$$

*Επειδή* $a \neq 0,\ c \neq 0$, *έχουμε* $ac \neq 0$. *Τότε*

$$T_{a,b} \circ T_{c,d}(x) = T_{ac,ad+b} \in G.$$

*Παρατηρήστε ότι,*

$$(T_{a,b} \circ T_{c,d}) \circ T_{e,f} = T_{ac,ad+b} \circ T_{e,f} = T_{ace,acf+ad+b}$$

*και*

$$(T_{a,b} \circ (T_{c,d} \circ T_{e,f}) = T_{a,b} \circ T_{ce,cf+d} = T_{ace,acf+ad+b}$$

*Άρα ισχύει η προσεταιριστική ιδιότητα. Για την* $T_{1,0}$ *ισχύει* $T_{1,0}(x) = x$ *για κάθε* $x \in \mathbb{R}$, *άρα*

$$T_{1,0} \cdot T_{a,b} = T_{a,b} \cdot T_{1,0} = T_{a,b}$$

*για κάθε* $T_{a,b} \in G$. *Το στοιχείο* $T_{a,b}$ *έχει αντίστροφο το* $T_{a^{-1},-ba^{-1}}$. *Πράγματι,*

$$T_{a,b} \circ T_{a^{-1},-ba^{-1}} = T_{a^{-1},-ba^{-1}} \circ T_{a,b} = T_{1,0}.$$

7. *Έστω* $G = \mathbb{R} \setminus \{1\}$ *με πράξη* $a \star b = a + b + ab$. *Τότε* $(G, \star)$ *είναι αβελιανή ομάδα. Παρατηρήστε ότι αν* $a, b \in\in \mathbb{R} \setminus \{1\}$ *και* $a \star b = -1$, *τότε*

$$\begin{aligned} a + b + ab &= -1 \Rightarrow \\ a + b + ab + 1 &= 0 \Rightarrow \\ (a+1)(b+1) &= 0 \Rightarrow \\ a = 1 \quad &\acute{\eta} \quad b = 1. \end{aligned}$$

*Άρα πράγματι η* $\star$ *είναι πράξη στο* $G$. *Έστω* $a, b, c \in G$. *Τότε,*

$$(a \star b) \star c = (a + b + ab) \star c = a + b + ab + c + ac + bc + abc$$

*και*

$$a \star (b \star c) = a \star (b + c + bc) = a + b + c + bc + ab + ac + abc.$$

*Άρα,*

$$(a \star b) \star c = a \star (b \star c).$$

*Για* $e = 0$, *έχουμε*

$$a \star e = e \star a = a,$$

*για κάθε* $a \in G$. *Έστω* $a \in G$. *Θεωρούμε το* $a' = -\frac{a}{1+a}$. *Τότε* $a' \in \mathbb{R} \setminus \{1\}$ *και*

$$a \star a' = a' \star a = 0.$$

**Παρατήρηση 3.1.7.** *Το σύνολο* $\mathbb{R}$ *με πράξη* $a \star b = a + b + ab$ *δεν είναι ομάδα γιατί το* $-1$ *δεν έχει αντίστροφο.*

*8. Έστω*

$$G = \{A \subset M_n(\mathbb{R}) : AA^t = A^tA = I_n\}.$$

*Ως προς τον γινόμενο πινάκων η $G$ είναι ομάδα.*

*Έστω $A, B \in G$. Τότε*

$$AA^t = A^tA = I_n \qquad \text{και} \qquad BB^t = B^tB = I_n.$$

*Τότε,*

$$(AB)(AB)^t = ABB^tA^t = AI_nA^t = AA^t = I_n.$$

*Ομοίως παίρνουμε,*

$$(AB)^t(AB) = I_n.$$

*Άρα $AB \in G$, δηλαδή το γινόμενο πινάκων ορίζει πράξη στο σύνολο $G$. Αν $A, B, C \in G$, τότε*

$$(AB)C = A(BC) \qquad (\text{γενική ιδιότητα πολλαπλασιασμού πινάκων}).$$

*Έχουμε $I_n \in G$ και $I_nA = AI_n = A$. Έστω $A \in G$. Τότε ο $A$ είναι αντιστρέψιμος και $A^{-1} \in G$. Πράγματι έχουμε $A^{-1} = A^t$ ($AA^t = A^tA = I_n$) και*

$$(A^{-1})(A^{-1})^t = A^t(A^t)^t = I_n.$$

*Ομοίως,*

$$(A^{-1})^t(A^{-1}) = I_n.$$

*9. Έστω $M \subseteq \mathbb{R}^n$, $M \neq \emptyset$. Έστω*

$$S(M) = \{f : \mathbb{R}^n \to \mathbb{R}^n : f \ \text{ συμμετρία}\}.$$

*Ως προς την σύνθεση συναρτήσεων το $S(M)$ είναι ομάδα. Πράγματι εύκολα ελέγχουμε ότι αν $f, g \in S(M)$, τότε $f \circ g \in S(M)$. Επίσης η ταυτοτική απεικόνιση $1 : \mathbb{R}^n \to \mathbb{R}^n$ ανήκει στον $S(M)$ και $f \circ 1 = 1 \circ f = f$, για κάθε $f \in S(M)$. Τέλος εύκολα ελέγχουμε ότι αν $f \in S(M)$, τότε η $f$ είναι αντιστρέψιμη (είναι άμεσο ότι η $f$ είναι 1-1 και επί) και $f^{-1} \in S(M)$.*

Είδαμε στο παράδειγμα 3 ότι αν $X \neq \emptyset$ είναι ένα σύνολο και

$$S(X) = \{f : X \to X : f \ \text{ 1 − 1 και επί}\},$$

τότε ως προς την σύνθεση συναρτήσεων το $S(X)$ είναι ομάδα. Θα μελετήσουμε τώρα την $S(X)$ όταν το σύνολο $X$ είναι πεπερασμένο.

### 3.1α′ Συμμετρικές ομάδες $S_n$

**Ορισμός 3.1.8.** *Θέτουμε*

$$S_n = \{f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} : f \ \ 1-1 \ \ \textit{και επί}\}$$

*με πράξη την σύνθεση συναρτήσεων. Τότε η $S_n$ είναι ομάδα ($S_n = S(X)$, όπου $X = \{1, 2, \ldots, n\}$ και ονομάζεται συμμετρική ομάδα βαθμού $n$. Κάθε στοιχείο της $S_n$ λέγεται μετάθεση των ($\{1, 2, \ldots, n\}$). Συμβολισμός.*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}.$$

**Παράδειγμα 3.1.9.**

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in S_3.$$

*(Το στοιχείο $\sigma \in S_3$ ώστε $\sigma(1) = 3,\ \sigma(2) = 2,\ \sigma(3) = 1$.)*

**Παρατηρήσεις 3.1.10.** (i)

$$\begin{aligned} S_1 &= \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\} = \{1\}, \\ S_2 &= \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\} = \left\{ 1, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}, \\ S_3 &= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}. \end{aligned}$$

(ii) *Σύνθεση με τον συμβολισμό $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$. Αν*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \textit{και} \qquad \rho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

*τότε*

$$\sigma \cdot \rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

*αφού $1 \xrightarrow{\rho} 3 \xrightarrow{\sigma} 3,\ 2 \xrightarrow{\rho} 2 \xrightarrow{\sigma} 1,\ 3 \xrightarrow{\rho} 1 \xrightarrow{\sigma} 2$.*

(iii) *Υπολογισμός της μετάθεσης $\sigma^{-1}$ με τον συμβολισμό $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$.*
*Αν*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix},$$

*τότε*

$$\sigma^{-1} = \begin{pmatrix} 3 & 4 & 5 & 2 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}.$$

(iv) *Αν* $n \geqslant 3$, *τότε η ομάδα* $S_n$ *δεν είναι αβελιανή. Πράγματι, έστω*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{pmatrix} \qquad \textit{και} \qquad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix},$$

*τότε*

$$\sigma \circ \rho(3) = \sigma(\rho(3)) = \sigma(2) = 1$$

*και*

$$\rho \circ \sigma(3) = \rho(\sigma(3)) = \rho(3) = 2.$$

*Άρα,* $\sigma \circ \rho(3) \neq \rho \circ \sigma(3)$, *οπότε* $\sigma \circ \rho \neq \rho \circ \sigma$.

**Πρόταση 3.1.11.** $\left|S_n\right| = n!$.

*Απόδειξη.* $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & (n-1) & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n-1) & \sigma(n) \end{pmatrix}$. Για το $\sigma(1)$ υπάρχουν $n$ περιπτώσεις.

Για το $\sigma(2)$ υπάρχουν $n-1$ περιπτώσεις, αφού $\sigma(2) \neq \sigma(1)$ ($\sigma$ $1-1$).

Για το $\sigma(3)$ υπάρχουν $n-2$ περιπτώσεις, αφού $\sigma(3) \neq \sigma(2), \sigma(3) \neq \sigma(1)$.

Συνεχίζοντας με τον ίδιο τρόπο βλέπουμε ότι για το $\sigma(n-1)$ υπάρχουν 2 περιπτώσεις και για το $\sigma(n)$ υπάρχει 1 περίπτωση. Επομένως,

$$\left|S_n\right| = n(n-1)\cdots 3 \cdot 2 \cdot 1 = n!.$$

□

**Παράδειγμα 3.1.12.** $\left|S_3\right| = 3! = 6,\ \left|S_4\right| = 24.$

### 3.1β′ Κυκλικές μεταθέσεις (ή κύκλοι)

**Ορισμός 3.1.13.** *Μια μετάθεση* $\sigma \in S_n$ *λέγεται κυκλική μετάθεση (ή κύκλος) αν υπάρχουν* $a_1, a_2, \cdots, a_m \in \{1, 2, \cdots, n\}$, *ώστε*

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \sigma(a_3) = a_4, \cdots, \sigma(a_{m-1}) = a_m, \sigma(a_m) = a_1$$

*και*

$$\sigma(i) = i \ \ \textit{για κάθε}\ \ i \in \{1, 2, 3, \cdots, n\} \setminus \{a_1, \cdots, a_m\}.$$

*Το* $m$ *λέγεται το μήκος της κυκλικής μετάθεσης. Συμβολίζουμε με* $\sigma = (a_1, a_2, \cdots, a_m)$.

**Παραδείγματα 3.1.14.** (i) $\sigma = (4\ 2\ 1\ 3) \in S_4$ *είναι η* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$.

(ii) $\sigma = (4\ 2\ 1\ 3) \in S_5$ *είναι η* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix}$.

(iii) *Η μετάθεση* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in S_4$ *δεν είναι κύκλος.*

**Παρατήρηση 3.1.15.** *Τα* $a_i$ *στην παράσταση* $(a_1, a_2, \cdots, a_m)$ *ενός κύκλου δεν είναι μοναδικά. Πράγματι,*

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

*ενώ* $(4\ 2\ 1\ 3) \neq (2\ 1\ 3\ 4)$. *Γενικά,*

$$(a_1\ a_2\ a_3 \cdots a_m) = (a_2\ a_3 \cdots a_m\ a_n) = (a_3 \cdots a_m\ a_1\ a_2) = \cdots = (a_m\ a_1\ a_2 \cdots a_{m-1}).$$

$\sigma = (4\ 2\ 1\ 3) = (2\ 1\ 3\ 4)$, *όμως για την* $(4\ 2\ 1\ 3)$ *έχουμε* $4 \mapsto 2$, *ενώ για την* $(2\ 1\ 3\ 4)$ *έχουμε* $4 \mapsto 1$ *άρα* $(4\ 2\ 1\ 3) \neq (2\ 1\ 3\ 4)$.

**Παρατήρηση 3.1.16.** *Αν* $\sigma = (a_1\ a_2 \cdots a_{m-1}\ a_m)$, *τότε* $\sigma^{-1}$ *είναι πάλι κύκλος και μάλιστα* $\sigma^{-1} = (a_m\ a_{m-1} \cdots a_2\ a_1)$.

**Πρόταση 3.1.17.** *Έστω* $\sigma \in S_n$ *κύκλος μήκους* $m$. *Τότε,*

(i) $\sigma^m = 1$ *και*

(ii) $\sigma^\kappa \neq 1$, *για κάθε* $\kappa = 1, 2, \cdots, m-1$.

*Απόδειξη.* Έστω $\sigma = (a_1\ a_2\ a_3 \cdots a_m)$. Τότε, $\sigma(a_1) = a_2$,

$$\sigma^2(a_1) = \sigma(\sigma(a_1)) = \sigma(a_2) = a_3.$$

Συνεχίζοντας με τον ίδιο τρόπο βλέπουμε ότι,

$$\sigma^{n-1}(a_1) = \sigma(\sigma^{n-2}(a_1)) = \sigma(a_{m-1}) = a_m.$$

Άρα,

$$\sigma,\ \sigma^2, \cdots, \sigma^{m-1} \neq 1.$$

Επίσης,

$$\sigma^m(a_1) = \sigma(\sigma^{m-1}(a_1)) = \sigma(a_m) = a_1.$$

Ομοίως,

$$\sigma^m(a_i) = a_i, \ \text{ για κάθε } \ i = 1, 2, \cdots, m.$$

Άρα, $\sigma^m = 1$ (θυμίζουμε ότι $\sigma(b) = b$, για κάθε $b \neq a_1, \cdots, a_m$). □

**Ορισμός 3.1.18.** *Έστω* $\sigma, \tau \in S_n$. *Οι* $\sigma, \tau$ *λέγονται ξένες, αν*

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

**Παρατήρηση 3.1.19.** *Έστω $\sigma, \tau$ ξένες. Τότε όποιο στοιχείο μετακινεί η μία, η άλλη το αφήνει σταθερό, δηλαδή*

$$\sigma(i) \neq i \Rightarrow \tau(i) = i \qquad \textit{και} \qquad \tau(i) \neq i \Rightarrow \sigma(i) = i.$$

**Παραδείγματα 3.1.20.** (i) *Οι*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} \qquad \textit{και} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$

*είναι ξένες, αφού*

$$\{i : \sigma(i) \neq i\} = \{1, 3, 5\} \qquad \textit{και} \qquad \{j : \tau(j) \neq i\} = \{2, 4\}.$$

(ii) *Οι*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} \qquad \textit{και} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix}$$

*δεν είναι ξένες, αφού $\sigma(1) \neq 1$ και $\tau(1) \neq 1$.*

Είδαμε ότι για $n \geqslant 3$ η ομάδα $S_n$ δεν είναι αβελιανή. Όμως ισχύει η ακόλουθη πρόταση.

**Πρόταση 3.1.21.** *Έστω $\sigma, \tau \in S_n$ ξένες. Τότε, $\sigma\tau = \tau\sigma$.*

*Απόδειξη.* Έστω $i \in \{1, 2, \cdots, n\}$. Διακρίνουμε τις δύο ακόλουθες περιπτώσεις.

1. Έστω $\tau(i) = i$. Τότε $\sigma\tau(i) = \sigma(i)$. Έστω

   $$\tau(\sigma(i)) \neq \sigma(i). \tag{3.1.1}$$

   Επειδή $\sigma, \tau$ ξένες και $\tau(\sigma(i)) \neq \sigma(i)$, έπεται $\sigma(\sigma(i)) = \sigma(i)$. Επειδή όμως η $\sigma$ είναι 1-1, έπεται $\sigma(i) = i$. Επομένως,

   $$\tau(\sigma(i)) = \tau(i) = i = \sigma(i),$$

   άτοπο λόγω της (3.1.1). Άρα $\tau\sigma(i) = \sigma(i)$, δηλαδή δείξαμε ότι αν $\tau(i) = i$, τότε $\sigma\tau(i) = \tau\sigma(i)$.

2. Έστω $\tau(i) \neq i$. Επειδή οι $\tau, \sigma$ είναι ξένες μεταθέσεις, έχουμε $\sigma(i) = i$. Από αυτό που δείξαμε στην περίπτωση 1 (εναλλάσοντας τους ρόλους των $\tau, \sigma$), προκύπτει ότι $\sigma\tau(i) = \tau\sigma(i)$.

□

**Θεώρημα 3.1.22.** *Κάθε $\sigma \in S_n$ γράφεται σαν γινόμενο ξένων ανά δύο κύκλων,*

$$\sigma = \sigma_1\sigma_2 \cdots \sigma_n,$$

*όπου οι $\sigma_i$ είναι μοναδικοί.*

**Παρατήρηση 3.1.23.** *Οι κύκλοι* $(a_1\ a_2 \cdots a_\kappa),\ (b_1\ b_2 \cdots b_\kappa)$ *είναι ξένοι αν και μόνο αν*

$$\{a_1, a_2, \cdots, a_\kappa\} \cap \{b_1, b_2, \cdots, b_\kappa\} = \emptyset.$$

*Απόδειξη του θεωρήματος* 3.1.22. Έστω $a_1 \in \{1, 2, \cdots, n\}$ και

$$B_{a_1} = \{\sigma^t(a_1) : t \in \mathbb{N}\}\ \ (\text{για}\ \ t = 0\ \ \sigma^0 = 1).$$

Επειδή $B_{a_1} \subseteq \{1, 2, \cdots, n\}$, υπάρχουν $s, t$ με $0 \leqslant s \leqslant t$ ώστε $\sigma^s(a_1) = \sigma^t(a_1)$.Επιλέγουμε το $t_1 > 0$ ως προς αυτήν την ιδιότητα. Ισχυριζόμαστε ότι $\sigma^t(a_1) = a_1$. Πράγματι, αν $\sigma^s(a_1) = \sigma^t(a_1)$ με $0 \leqslant s \leqslant t$, τότε $\sigma^{s-1}(a_1) = \sigma^{t-1}(a_1)$, άτοπο από τον ορισμό του $t_1$. Άρα,

$$B_{a_1} = \{a_1, \sigma(a_1), \sigma^2(a_1), \cdots, \sigma^{t_1-1}(a_1)\}.$$

Έστω $a_2 \in \{1, 2, \cdots, n\} \setminus B_{a_1}$. Εφαρμόζοντας την ίδια διαδικασία, προκύπτει ότι

$$B_{a_2} = \{a_2, \sigma(a_2), \sigma^2(a_2), \cdots, \sigma^{t_2-1}(a_2)\}.$$

Συνεχίζοντας με τον ίδιο τρόπο προκύπτουν $B_{a_1}, \cdots, B_{a_m} \in \{1, 2, \cdots, n\}$ ώστε

(i) $Ba_i \cap B_{a_j} = \emptyset$, για κάθε $i \neq j$ και

(ii) $B_{a_1} \cup B_{a_2} \cup \cdots \cup B_{a_m} = \{1, 2, \cdots, n\}$

Το (ii) είναι άμεσο. Για το (i), αν $\sigma^t(a_i) = \sigma^s(a_j)$, αφού $t \leqslant s$, έχουμε $a_i = \sigma^{s-t}(a_j) \in B_{a_j}$, άτοπο. Θέτουμε

$$\sigma_i = (a_i\ \sigma(a_i)\ \sigma^2(a_i) \cdots \sigma^{t_i-1}(a_i))$$

που είναι κύκλος (αφού $\sigma^{t_i}(a_i) = 1$). Οι κύκλοι $\sigma_1, \cdots, \sigma_m$ είναι ξένοι λόγω του (i). Από τον ορισμό και από το (ii), έπεται ότι $\sigma = \sigma_1\sigma_2 \cdots \sigma_m$.

Θα δείξουμε τώρα την μοναδικότητα των $\sigma_i$. Έστω

$$\sigma_1\sigma_2 \cdots \sigma_m = \sigma_1^{'}\sigma_2^{'} \cdots \sigma_m^{'},$$

όπου $\sigma_1, \cdots, \sigma_m$ και $\sigma_1^{'}, \cdots, \sigma_m^{'}$ ξένοι ανά δύο κύκλοι μήκους $\geqslant 2$. Τότε θα δείξουμε ότι $m = m'$ και μετά από ενδεχόμενη αναδιάταξη $\sigma_i = \sigma_i^{'}$, για κάθε $i$.

Με επαγωγή στο $M = \max\{m, m'\}$. Αν $M = 1$ προφανώς ισχύει. Έστω $M \geqslant 2$ και $\sigma_1\sigma_2 \cdots \sigma_m = \sigma_1^{'}\sigma_2^{'} \cdots \sigma_m^{'}$. Επειδή το μήκος $\sigma_i$ είναι διάφορο του 1, υπάρχει $i \in \{1, 2, \cdots, n\}$ ώστε $\sigma_1(i) \neq i$. Επειδή $\sigma_1, \sigma_2, \cdots, \sigma_m$ είναι ανά δύο ξένοι, έχουμε $\sigma_j(i) = i$, για κάθε $j \neq 1$. Τότε έχουμε,

$$\sigma_1\sigma_2 \cdots \sigma_m(i) = \sigma_1(i) \neq i.$$

Άρα

$$\sigma_1^{'}\sigma_2^{'} \cdots \sigma_m^{'} \neq i,$$

άρα υπάρχει $q$ ώστε $\sigma_q^{'}(i) \neq i$. Τότε $\sigma_1 = \sigma_q^{'}$ (αφού είναι κύκλοι). Με μια αναδιάταξη μπορούμε να υποθέσουμε ότι $q = 1$. Άρα από την $\sigma_1\sigma_2 \cdots \sigma_m = \sigma_1^{'}\sigma_2^{'} \cdots \sigma_m^{'}$, έπεται

$$\sigma_2 \cdots \sigma_m = \sigma_2^{'} \cdots \sigma_m^{'}.$$

Από επαγωγική υπόθεση προκύπτει το ζητούμενο. □

**Παραδείγματα 3.1.24.** *1. Έστω* $\sigma \in S_9$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 2 & 9 & 8 & 6 & 7 & 1 \end{pmatrix}.$$

*Επιλέγουμε* $a_1 = 1$. *Τότε έχουμε,*

$$\sigma(1) = 3,\ \sigma(3) = 5,\ \sigma(5) = 9,\ \sigma(9) = 1.$$

*Τότε,*

$$B_{a_1} = \{1, 3, 5, 9\} \qquad \sigma_1 = (1\ 3\ 5\ 9).$$

*Αν* $a_2 = 2$ *τότε,*

$$\sigma(2) = 4,\ \sigma(4) = 2.$$

*Τότε,*

$$B_{a_2} = \{2, 4\} \qquad \sigma_2 = (2\ 4).$$

*Αν* $a_3 = 6$, *τότε*

$$\sigma(6) = 8,\ \sigma(8) = 7,\ \sigma(7) = 6.$$

*Άρα,*

$$B_{a_3} = \{6, 8, 7\} \qquad \sigma_3 = (6\ 8\ 7).$$

*Επομένως*

$$\sigma = \sigma_1\sigma_2\sigma_3 = (1\ 3\ 5\ 9)(2\ 4)(6\ 8\ 7).$$

□

*2. Να βρεθεί η ανάλυση της*

$$\sigma = (1\ 2\ 3)(2\ 3\ 4)(3\ 4\ 5)(4\ 5\ 6)(5\ 6\ 7) \in S_7.$$

*Λύση. Έχουμε,*

$$\sigma(1) = 2,\ \sigma(2) = 1,\ \sigma(3) = 3,\ \sigma(4) = 4,\ \sigma(5) = 5,\ \sigma(6) = 7,\ \sigma(7) = 7.$$

$$\sigma = (1\ 2)(3)(4)(5)(6\ 7) = (1\ 2)(6\ 7).$$

*Σημείωση. Κάθε κύκλος μήκους* 1 *είναι το ταυτοτικό στοιχείο της* $S_n$. □

*3. Έστω* $[a] \in \mathbb{Z}_n$. *Θεωρούμε την απεικόνιση* $\sigma : \mathbb{Z}_n \to \mathbb{Z}_n$, $n \geqslant 1$, *με* $\sigma([b]) = [ab]$.

*(i) Να δείξετε ότι η $\sigma$ είναι μετάθεση αν και μόνο αν $\mu\kappa\delta(a,n)=1$,*

*(ii) Για $n=9$ και $a=4$ να βρείτε την ανάλυση της $\sigma^{2011}$ σε γινόμενο ξένων ανά δύο κύκλων.*

*Απόδειξη.(i). Έστω $\mu\kappa\delta(a,n)=d>1$. Παρατηρήστε ότι,*

$$\sigma\left(\left[\frac{n}{d}\right]\right)=\left[a\frac{n}{d}\right]=\left[\frac{a}{d}\cdot n\right]=[0].$$

*Δηλαδή,*

$$\sigma([0])=([0]) \qquad \text{και} \qquad \sigma\left(\left[\frac{n}{d}\right]\right)=([0]),$$

*με $\left[\frac{n}{d}\right]\neq 0$ αφού $d>1$. Άρα η $\sigma$ δεν είναι 1-1 (άρα δεν είναι μετάθεση).*
*Αντίστροφα, έστω $\mu\kappa\delta(a,n)=1$. Θα δείξουμε ότι η $\sigma$ είναι μετάθεση του $\mathbb{Z}_n$. Παρατηρήστε πρώτα ότι η $\sigma$ είναι 1-1. Πράγματι, έστω $\sigma([b_1])=\sigma([b_2])$ . Τότε,*

$$[ab_1]=[ab_2]\Rightarrow n|ab_1-ab_2\Rightarrow n|a(b_1-b_2)\overset{(\mu\kappa\delta(a,n)=1)}{\Longrightarrow} n|b_1-b_2\Rightarrow [b_1]=[b_2].$$

*Επίσης η $\sigma$ είναι επί. Πράγματι είναι 1-1 και το $\mathbb{Z}_n$ είναι πεπερασμένο σύνολο.*
*(ii). Για $n=9$ και $a=4$ έχουμε,*

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&8&3&7&2&6&1&5&9\end{pmatrix}.$$

*(Για παράδειγμα $\sigma[5]=[4\cdot 5]=[20]=[2]$.) Παρατηρήστε ότι,*

$$\sigma(1)=4,\ \sigma(4)=7,\ \sigma(7)=1,$$

$$\sigma(2)=8,\ \sigma(8)=5,\ \sigma(5)=2$$

*και*

$$\sigma(3)=3,\ \sigma(6)=6,\ \sigma(9)=9.$$

*Επομένως η ανάλυση της $\sigma$ σε ξένους κύκλους είναι,*

$$\sigma=(1\ 4\ 7)(2\ 8\ 5).$$

*Επειδή οι ξένες μεταθέσεις αντιμετατίθενται έχουμε,*

$$\sigma^{2011}=((1\ 4\ 7)(2\ 8\ 5))^{2011}=(1\ 4\ 7)^{2011}(2\ 8\ 5)^{2011}.$$

*Από την πρόταση 3.1.17, έπεται $(1\ 4\ 7)^3=1$, άρα*

$$(1\ 4\ 7)^{2011}=(1\ 4\ 7)^{2010}(1\ 4\ 7)=\left((1\ 4\ 7)^3\right)^{670}=1^{670}(1\ 4\ 7)=(1\ 4\ 7).$$

*Ομοίως, $(2\ 8\ 5)^{2011}=(2\ 8\ 5)$. Άρα,*

$$\sigma^{2011}=(1\ 4\ 7)(2\ 8\ 5).$$

□

### 3.1γ′ Τάξη στοιχείου ομάδας

**Ορισμός 3.1.25.** *Έστω $G$ ομάδα και $g \in G$. Αν υπάρχει $m \in \mathbb{Z}_{>0}$ με $g^m = 1$ (το ουδέτερο στοιχείο της $G$), τότε ο ελάχιστος τέτοιος λέγεται η τάξη της $G$ και συμβολίζεται με $|g| = m$. Αν δεν υπάρχει τέτοιο $m$ θα λέμε ότι η τάξη του $g$ είναι άπειρη.*

**Παραδείγματα 3.1.26.** (i) *Έστω $\sigma \in S_n$ κύκλος μήκους $\kappa$. Τότε $\sigma^\kappa = 1$ και $\sigma^j \neq 1$, για κάθε $j = 1, 2, \ldots, \kappa - 1$ . Δηλαδή $|\sigma| = \kappa$.*

(ii) *Έστω $G = \mathbb{R} \setminus \{0\}$ με πράξη τον πολλαπλασιασμό. Το στοιχείο 2 έχει άπειρη τάξη, ενώ το στοιχείο $-1$ έχει τάξη 2.*

(iii) *$U(\mathbb{Z}_8) =$ το σύνολο των αντοστρέψιμων στοιχείων του δακτυλίου $\mathbb{Z}_8$. Είναι ομάδα με πράξη τον πολλαπλασιασμό του $\mathbb{Z}_8$. Γνωρίζουμε ότι,*

$$U(\mathbb{Z}_8) = \{[1], [3], [5], [7]\} = \{[a] \in \mathbb{Z}_8 : \mu\kappa\delta(a, 8) = 1\}.$$

*Παρατηρήστε ότι,*

| $g$ | $[1]$ | $[3]$ | $[5]$ | $[7]$ |
|---|---|---|---|---|
| $\lvert g\rvert$ | 1 | 2 | 2 | 2 |

*για παράδειγμα $3^2 = 9 = 1 \mathrm{mod} 8$, δηλαδή $[3]^2 = [1]$ ($[3] \neq [1]$). Για παράδειγμα για το 1 έχουμε,*

| $g \in S_3$ | $1$ | $(1\ 2)$ | $(1\ 3)$ | $(2\ 3)$ | $(1\ 2\ 3)$ | $(2\ 1\ 3)$ |
|---|---|---|---|---|---|---|
| $\lvert g\rvert$ | 1 | 2 | 2 | 2 | 3 | 3 |

(iv) *$E_n = \{z \in \mathbb{C} : z^n = 1\}$ είναι ομάδα ως προς τον πολλαπλασιασμό μιγαδικών. Για $n = 4$,*

| $g$ | $1$ | $-1$ | $i$ | $-i$ |
|---|---|---|---|---|
| $\lvert g\rvert$ | 1 | 2 | 4 | 4 |

*για παράδειγμα $i^2 = -1 \neq 1$, $i^3 = -i \neq 1$, $i^4 = 1$.*

**Θεώρημα 3.1.27.** *Έστω $G$ ομάδα και $g \in G$. Έστω ότι $|g| = \kappa < \infty$. Τότε ισχύουν τα ακόλουθα.*

(i) *Έστω $m \in \mathbb{Z}_{>0}$. Τότε $g^m = 1 \Leftrightarrow \kappa | m$.*

(ii) *Έστω $m \in \mathbb{Z}_{>0}$. Τότε $|g^m| = \frac{\kappa}{\mu\kappa\delta(\kappa, m)}$.*

*Απόδειξη.* (i). Από τον αλγόριθμο της ευκλείδειας διαίρεσης υπάρχουν $q, r \in \mathbb{Z}$ ώστε $m = q\kappa + r,\ 0 \leqslant r < \kappa$. Τότε,

$$g^m = (g^\kappa)^q \cdot g^r = 1^q g^r = g^r.$$

Αν $g^m = 1$, τότε $g^r = 1$ και επειδή $0 \leqslant r < \kappa$, όπου $\kappa = |g|$ παίρνουμε $r = 0$. Αν $\kappa | m$, τότε $r = 0$ και $g^m = 1$.

(ii). Παρατηρήστε ότι,

$$(g^m)^{\frac{\kappa}{\mu\kappa\delta(\kappa,m)}} = (g^\kappa)^{\frac{m}{\mu\kappa\delta(\kappa,m)}} = 1^{\frac{m}{\mu\kappa\delta(\kappa,m)}} = 1.$$

Άρα,

$$|g^m| \leqslant \frac{\kappa}{\mu\kappa\delta(\kappa, m)}. \tag{3.1.2}$$

Έστω $(g^m)^s = 1,\ s \in \mathbb{Z}_{>0}$. Τότε $g^{ms} = 1$, οπότε από το ερώτημα (i) έπεται $\kappa | ms$. Τότε,

$$\frac{\kappa}{\mu\kappa\delta(\kappa, m)} \Big| \frac{m}{\mu\kappa\delta(\kappa, m)} \cdot s.$$

Όμως $\mu\kappa\delta\left(\frac{\kappa}{\mu\kappa\delta(\kappa,m)}, \frac{m}{\mu\kappa\delta(\kappa,m)}\right) = 1$, άρα

$$\frac{\kappa}{\mu\kappa\delta(\kappa, m)} \Big| s \Rightarrow \frac{\kappa}{\mu\kappa\delta(\kappa, m)} \leqslant s. \tag{3.1.3}$$

Από τις (3.1.2) και (3.1.3) έπεται ότι $|g^m| = \frac{\kappa}{\mu\kappa\delta(\kappa,m)}$. □

**Παράδειγμα 3.1.28.** *Αν $s \in S_n$ κύκλος μήκους 8, τότε*

$$\left|\sigma^{50}\right| = \frac{8}{\mu\kappa\delta(50, 8)} = \frac{8}{2} = 4.$$

**Θεώρημα 3.1.29.** *Έστω $\sigma, \tau$ ξένοι κύκλοι στην ομάδα $S_n$ με αντίστιχα μήκη $\kappa_1, \kappa_2$. Τότε $|\sigma\tau| = \epsilon\kappa\pi(\kappa_1, \kappa_2)$.*

**Πόρισμα 3.1.30.** *Αν $\sigma \in S_n,\ \sigma = \sigma_1\sigma_2 \cdots \sigma_n$, όπου $\sigma_i$ ξένοι ανά δύο κύκλοι με μήκη $\kappa_1, \kappa_2, \cdots, \kappa_n$, τότε $|\sigma| = \epsilon\kappa\pi(\kappa_1, \kappa_2, \cdots, \kappa_n)$.*

(Το πόρισμα προκύπτει άμεσα από το θεώρημα 3.1.29, με επαγωγή.)

*Απόδειξη του θεωρήματος* 3.1.29. Έστω $\kappa = \epsilon\kappa\pi(\kappa_1, \kappa_2)$. Οι ξένες μεταθέσεις αντιμετατίθενται, οπότε

$$(\sigma\tau)^\kappa = \sigma^\kappa \cdot \tau^\kappa = 1 \cdot 1 = 1$$

(αφού $\kappa$ πολλαπλάσιο του $\kappa_1$ και $\kappa$ πολλαπλάσιο του $\kappa_2$.) Άρα, $|\sigma\tau| \leqslant \kappa$.

Έστω $(\sigma\tau)^s = 1$. Τότε,

$$\sigma^s \cdot \tau^s = 1 \Rightarrow \sigma^s = \tau^{-s} = (\tau^{-1})^s.$$

Επειδή οι $\sigma, \tau$ είναι ξένοι κύκλοι και οι $\sigma$ και $\tau^{-1}$ είναι ξένοι κύκλοι, άρα οι μεταθέσεις $\sigma^s$ και $(\tau^{-1})^s$ είναι ξένες. Δηλαδή έχουμε, $\sigma^s = (\tau^{-1})^s$ και $\sigma^s$, $(\tau^{-1})^s$ ξένες, άρα η καθεμιά ισούται με την ταυτοτική μετάθεση. Άρα $\sigma^s = 1$ και $(\tau^{-1})^s = 1$. Τότε $|\sigma||s$, δηλαδή $\kappa_1|s$. Ομοίως $\tau^s = 1$, άρα $\kappa_2|s$. Επομένως $\text{εκπ}(\kappa_1, \kappa_2) \subseteq s$. Άρα $|\sigma\tau| = \text{εκπ}(\kappa_1, \kappa_2)$. □

**Παράδειγμα 3.1.31.** *Να βρείτε την τάξη του*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 1 & 9 & 7 & 6 & 8 & 2 & 4 \end{pmatrix} \in S_9$$

*και του* $\sigma^{50}$.

*Λύση.* Βρίσκουμε πρώτα την ανάλυση του $\sigma$ σε γινόμενο ξένων κύκλων. Παρατηρήστε ότι,

$$\sigma(1) = 3,\ \sigma(3) = 1,$$

$$\sigma(2) = 5,\ \sigma(5) = 7,\ \sigma(7) = 8,\ \sigma(8) = 2,$$

$$\sigma(4) = 9,\ \sigma(9) = 4$$

και $\sigma(6) = 6$. Επομένως,

$$\sigma = (1\ 3)(2\ 5\ 7\ 8)(4\ 9).$$

Από το πόρισμα 3.1.30, έχουμε $|\sigma| = \text{εκπ}(2\ 4\ 2) = 4$. Από το θεώρημα 3.1.27 έχουμε $\left|\sigma^{50}\right| = \frac{4}{\text{μκδ}(50,4)} = 2$. □

### Ασκήσεις

1. Έστω $\sigma_1\ \sigma_2 \cdots \sigma_n$ όπου $\sigma_i$ ξένοι ανά δύο κύκλοι. Τότε $\sigma = \sigma^{-1}$ αν και μόνο αν κάθε $\sigma_i$ έχει μήκος $\leqslant 2$.

   *Απόδειξη.* Έστω $\sigma = \sigma^{-1}$. Τότε

   $$\sigma = (\sigma_1\ \sigma_2 \cdots \sigma_m)^{-1} = \sigma_m^{-1} \cdots \sigma_2^{-1}\sigma_1^{-1}.$$

   Γνωρίζουμε ότι

   (α′) $\sigma_i$ κύκλος μήκους $\kappa_i$ και $\sigma_i^{-1}$ κύκλος μήκους $\kappa_i$. Ειδικότερα

   $$(a_1\ a_2 \cdots a_\kappa)^{-1} = (a_\kappa\ a_{\kappa-1} \cdots a_2 a_1).$$

   (β′) Αν $\sigma_i$ κύκλος, τότε οι $\sigma_i$ και $\sigma_i^{-1}$ μετακινούν τα ίδια στοιχεία (ισχύει γενικά για μεταθέσεις).

(γ′) $\sigma_1, \sigma_2, \cdots, \sigma_m$ και$\sigma_1^{-1}, \sigma_2^{-1}, \cdots, \sigma_m^{-1}$ ανά δύο ξένοι κύκλοι.

Έχουμε,

$$\sigma_1\, \sigma_2 \cdots \sigma_m = \sigma_m^{-1}\, \sigma_{m-1}^{-1} \cdots \sigma_1^{-1}.$$

Από το θεώρημα 3.1.22 έπεται ότι $\sigma_i = \sigma_q^{-1}$ για κάποιο $q \in \{1, 2, \cdots, m\}$. Από την παρατήρηση 3.1.23 έπεται ότι η μετάθεση $\sigma_i$ είναι ξένη ως προς τις $\sigma_2^{-1}, \sigma_3^{-1}, cdots, \sigma_m^{-1}$. Άρα $\sigma_1 = \sigma_1^{-1}$, δηλαδή $\sigma_1^2 = 1$. Άρα ο $\sigma_1$ είναι κύκλος μήκους 1 ή 2. Ομοίως για τα άλλα $\sigma_i$.

Αντίστροφα, έστω $\sigma_i$ κύκλος μήκους 1 ή 2. Τότε $\sigma_i^2 = 1$, άρα $\sigma_i^{-1} = \sigma_i$. Τότε,

$$\sigma = \sigma_1 \cdots \sigma_m,$$

άρα

$$\sigma^{-1} = (\sigma_1 \cdots \sigma_m)^{-1} = \sigma_m^{-1} \cdots \sigma_2^{-1}\sigma_1^{-1} = \sigma_m \cdots \sigma_2\sigma_1 = \sigma_1\sigma_2 \cdots \sigma_m = \sigma,$$

όπου στο τελευταίο βήμα χρησιμοποιήσαμε το γεγονός ότι οι ξένες μεταθέσεις αντιμετατίθενται. Επίσης χρησιμοποιήσαμε το γεγονός ότι αν $g \in G$ με $g^2 = 1$ ή $gg = 1$, τότε πολλαπλασιάζοντας με $g^{-1}$ παίρνουμε $g = g^{-1}$. □.

**Παρατήρηση 3.1.32.** *Έστω $\sigma_1^2 = 1$, $\sigma_1$ κύκλος. Άρα το μήκος της $\sigma_1$ είναι 1 ή 2. Γνωρίζουμε ότι το μήκος $\kappa$ του $\sigma_1$ είναι ο ελάχιστος θετικός ακέραιος ώστε $\sigma_1^\kappa = 1$. Άρα $\kappa = 1$ ή $\kappa = 2$ .*

**2**. Έστω $G$ ομάδα και $a, b \in G$. Τότε,

(i) $|a| = |a^{-1}|$.

(ii) $|b^{-1}ab| = |a|$.

(iii) $|ab| = |ba|$.

(iv) Αν $b^{-1}a^2b = a^3$ και $a \neq 1$, τότε $|a| \geqslant 5$.

*Απόδειξη.* (i). Παρατηρήστε ότι,

$$a^s = 1 \Leftrightarrow (a^s)^{-1} = 1 \Leftrightarrow (a^{-1})^s = 1.$$

Δηλαδή,

$$a^s = 1 \Leftrightarrow (a^{-1})^s = 1,$$

άρα $|a| = |a^{-1}|$.

(ii). Παρατηρήστε ότι,

$$(b^{-1}ab)^2 = b^{-1}abb^{-1}ab = b^{-1}a^2b.$$

Γενικά με επαγωγή παίρνουμε,

$$(b^{-1}ab)^s = b^{-1}a^s b,$$

για κάθε $s \in \mathbb{Z}_{>0}$. Επομένως,

$$(b^{-1}ab)^s = 1 \Leftrightarrow b^{-1}a^s b = 1 \Leftrightarrow a^s = 1,$$

δηλαδή

$$(b^{-1}ab)^s = 1 \Leftrightarrow a^s = 1.$$

Επομένως, $|b^{-1}ab| = |a|$.

(iii). Παρατηρήστε ότι,

$$b^{-1}(ba)b = ab \overset{\text{(ii)}}{\Rightarrow} |ba| = |ab|.$$

(iv). Έστω $a = |\kappa| < \infty$. Από την $b^{-1}a^2b = a^3$ και από το δεύτερο ερώτημα, έχουμε

$$|a^2| = |a^3| \Rightarrow \frac{\kappa}{\text{μκδ}(\kappa, 2)} = \frac{\kappa}{\text{μκδ}(\kappa, 3)} \Rightarrow \text{μκδ}(\kappa, 2) = \text{μκδ}(\kappa, 3).$$

Επομένως, $2 \nmid \kappa$ και $3 \nmid \kappa$. Επειδή $a > 1$, έπεται $\kappa \geqslant 5$. □

**3**. Έστω $G$ ομάδα ώστε υπάρχει μοναδικό στοιχείο $a \in G$ με $|a| = 2$. Τότε $ab = ba$, για κάθε $a \in G$.

*Απόδειξη.* Έστω $b \in G$. Τότε από το δεύτερο ερώτημα της άσκησης 2, παίρνουμε $|b^{-1}ab| = |a|$, άρα $|b^{-1}ab| = 2$. Από μοναδικότητα έπεται $b^{-1}ab = a$, δηλαδή $ab = ba$. □

**4**. (i) Πόσα στοιχεία τάξης 2 έχει η $S_4$;

(ii) Πόσα στοιχεία τάξης 3 έχει η $S_5$;

*Λύση.* Γνωρίζουμε ότι κάθε $\sigma \in S_n$ γράφεται ως γινόμενο ξένων κύκλων και αν $\sigma = \sigma_1\sigma_2 \cdots \sigma_n$, όπου $\sigma_i$ κύκλοι ανά δύο ξένοι, τότε $|\sigma| = \text{εκπ}(\kappa_1, \kappa_2, \cdots, \kappa_n)$.

(i). Κάθε $\sigma \in S_4$ τάξης 2 είναι ή κύκλος μήκους 2 ή γινόμενο 2 ξένων κύκλων μήκους 2. Επομένως έχουμε $6 + 3 = 9$ στοιχεία τάξης 2.

(ii). Μια μετάθεση $\sigma \in S_5$ έχει $|\sigma| = 3$ αν και μόνο αν $\sigma$ είναι κύκλος μήκους 3 και αφού $3 + 3 > 5$ δεν μπορούμε να έχουμε 2 κύκλους τάξης 3. Άρα $\sigma = (a_1\ a_2\ a_3)$. Υπενθυμίζουμε ότι αν $A$ πεπερασμένο σύνολο με $n$ στοιχεία, τότε το πλήθος των υποσυνόλων του $A$ που έχουν $\kappa$ στοιχεία είναι $\binom{n}{\kappa}$, $1 \leqslant \kappa \leqslant n$. Για το σύνολο $\{a_1, a_2, a_3\} \subseteq \{1, 2, \cdots, 5\}$ υπάρχουν $\binom{5}{3} = 10$ επιλογές.

*Ερώτημα.* Πόσοι κύκλοι $(b_1\ b_2\ b_3)$ υπάρχουμε με $(b_1\ b_2\ b_3) = (a_1\ a_2\ a_3)$;

Παρατηρήστε ότι,

$$(a_1\ a_2\ a_3) \neq (a_2\ a_1\ a_3),$$

$$(a_1\ a_2\ a_3) = (a_2\ a_3\ a_1) = (a_3\ a_1\ a_2),$$
$$(a_2\ a_1\ a_3) = (a_1\ a_3\ a_2) = (a_3\ a_2\ a_1).$$

Τελικά υπάρχουν $\binom{5}{3} \cdot 2 = 20$ στοιχεία της $S_5$ τάξης 3. □

**5**. Αν $\sigma \in S_{10}$ έχει τάξη 14, να δείξετε ότι υπάρχει μοναδικό $i \in \{1, 2, \cdots, 10\}$ ώστε $\sigma(i) = i$.

*Απόδειξη.* Αφού $\sigma \in S_{10}$ έχει τάξη 14, έπεται ότι

$$\sigma = \sigma_1\sigma_2 \cdots \sigma_m,$$

όπου $\sigma_i$ είναι ξένοι κύκλοι και αν $\kappa_i$ το μήκος του $\sigma_i$, τότε $14 = \text{εκπ}\{\kappa_1, \cdots, \kappa_m\}$. Γνωρίζουμε ότι $1 \leqslant \kappa_i \leqslant 10,\ \kappa_1 + \kappa_2 + \cdots + \kappa_m = 10$. (Στην ανάλυση συμπεριλαμβάνουμε και τους 1- κύκλους αν υπάρχουν.) Επειδή $7|14$ υπαρχει $\kappa_i$ ώστε $7|\kappa_i$, δηλαδή $\kappa_i = 7$. Εστω ότι $\kappa_1 = 7$. Ομοίως το $2|14$, άρα υπάρχει $\kappa_j$ ώστε $2|\kappa_j$. Έχουμε $j \neq 1$, αφού $\kappa_1 < 14$. Έστω $2|\kappa_2$. Άρα $\kappa_2 = 2$. (Αν $\kappa_2 \geqslant 4$, τότε $\kappa_1 + \kappa_2 > 10$.) Επειδή $\kappa_1 = 7,\ \kappa_2 = 2$ και $\sum \kappa_i = 10$, έπεται ότι $m = 3$ και $\kappa_3 = 1$. Δηλαδή $\sigma = \sigma_1\sigma_2\sigma_3$ και $\sigma_3 = (i)$, όπου

$$i \notin \{a_1, \cdots, a_7\} \cup \{b_1, b_2\},$$

όπου $\sigma_1 = (a_1\ a_2 \cdots a_7),\ \sigma_2 = (b_1\ b_2)$. Επειδή

$$\{a_1, \cdots, a_7\} \cap \{b_1, b_2\} = \emptyset,$$

για το $i$ υπάρχει μοναδική επιλογή. □

**6**. Έστω $G$ ομάδα ώστε κάθε $g \in G \setminus \{1\}$ έχει τάξη 2. Τότε η $G$ είναι αβελιανή.

*Απόδειξη.* Έστω $a, b \in G$. Από την υπόθεση έπεται ότι $(ab)^2 = 1$. Άρα,

$$abab = 1 \Rightarrow ba = a^{-1}b^{-1} = ab,$$

αφού $a^2 = b^2 = 1$. □

**7**. Έστω $G$ πεπερασμένη ομάδα και $A \subseteq G$ με $|A| > \frac{|G|}{2}$. Τότε για κάθε $g \in G$, υπάρχουν $a, a' \in A$ ώστε $g = aa'$.

*Απόδειξη.* Θεωρούμε το σύνολο $B = \{a^{-1}g \in G : a \in A\}$. Έστω $g \in G$. Θα δείξουμε ότι $|B| > \frac{|G|}{2}$. Η απεικόνιση $f : A \to B$ με $f(a) = a^{-1}g$ είναι 1-1. Πράγματι, έστω $a_1, a_2 \in A$ με $f(a_1) = f(a_2)$. Τότε,

$$a_1^{-1}g = a_2^{-1}g \Rightarrow a_1^{-1} = a_2^{-1} \Rightarrow a_1 = a_2.$$

Προφανώς η $f$ είναι και επί. Άρα $|B| = |A| > \frac{|G|}{2}$. Επομένως $A \cap B \neq \emptyset$. Δηλαδή υπάρχει $a' \in A$ και $a^{-1}g \in B$ $(a \in A)$ ώστε

$$a^{-1}g = a' \Rightarrow g = aa'.$$

□

**8**. Να χαρακτηρίσετε τις επόμενες προτάσεις ως σωστό ή λάθος.

(i) Υπάρχει ομάδα με μοναδικό στοιχείο τάξης 3.

(ii) Αν $G$ ομάδα, $\alpha, \beta \in G$ και $\alpha^3 = \beta^3$, τότε $\alpha = \beta$.

(iii) Αν $G$ ομάδα, $\alpha, \beta \in G$ με $\alpha^3 = \beta^3$ και $\alpha^5 = \beta^5$, τότε $\alpha = \beta$.

(iv) Το μέγιστο στοιχείο του $\{|\sigma| : \sigma \in S_6\}$ είναι το 6.

*Λύση.* (i). Λάθος. Αν το $a \in G$ έχει $|a| = 3$, τότε

$$|a^2| = \frac{3}{\mu\kappa\delta(3,2)} = 3 \qquad \text{και} \qquad a \neq a^2.$$

(Αν $a = a^2$, τότε $a = 1$ που δεν έχει τάξη 3.)

*Σημείωση.* Αν η $G$ έχει στοιχεία τάξης $m(< \infty)$, τότε η $G$ έχει τουλάχιστον $\varphi(m)$ στοιχεία τάξης $m$. Αυτό έπεται από την $|a^\kappa| = \frac{m}{\mu\kappa\delta(\kappa,m)}$.

(ii). Λάθος. Έστω $G = S_3$ και $\alpha = (1\ 2\ 3)$, $\beta = (2\ 1\ 3)$. Τότε $\alpha \neq \beta$, ενώ $\alpha^3 = \beta^3 = 1$.

(iii). Σωστό. Υπάρχουν $m, n \in \mathbb{Z}$ ώστε $1 = 3m + 5n$. Τότε,

$$\alpha = \alpha^1 = (\alpha^3)^m(\alpha^5)^n = (\beta^3)^m(\beta^5)^n = \beta^{3m+5n} = \beta.$$

(iv). Σωστό. Υπενθυμίζουμε ότι κάτι $\sigma \in S_6$ γράφεται ως γινόμενο κύκλων ξένων ανά δύο, $\sigma = \sigma_1\sigma_2\cdots\sigma_m$. Επίσης $|\sigma| = \varepsilon\kappa\pi(\kappa_1, \kappa_2, \cdots, \kappa_m)$, όπου $\kappa_i$ το μήκος του κύκλου $\sigma_i$. Καταγράφουμε όλες τις δυνατές περιπτώσεις για το στοιχείο $(\kappa_1, \kappa_2, \cdots, \kappa_m) \in \mathbb{Z}^m_{>0}$ με τον προηγούμενο συμβολισμό. Επειδή οι ξένοι κύκλοι αντιμετατίθενται μπορούμε να υποθέσουμε ότι, $\kappa_1 \geqslant \kappa_2 \geqslant \cdots \geqslant \kappa_m$. Έχουμε,

$$6 = 6\ \ (6),\ \ 6 = 5+1\ \ (5),\ \ 6 = 4+2\ \ (4),\ \ 6 = 4+1+1\ \ (4),$$

$$6 = 3{+}3\ \ (3),\ \ 6 = 3{+}2{+}1\ \ (6),\ \ 6 = 3{+}1{+}1{+}1\ \ (3),\ \ 6 = 2{+}2{+}2\ \ (2),\ \ 6 = 2{+}2{+}1{+}1\ \ (2),$$

$$6 = 2+1+1+1+1\ \ (2),\ \ 6 = 1+1+1+1+1+1\ \ (1).$$

(Στις παρενθέσεις είναι οι τάξεις.) Άρα το max του $\{|\sigma| : \sigma \in S_6\}$ είναι το 6. □

## 3.2 Υποομάδες και το θεώρημα του Lagrange

**Ορισμός 3.2.1.** *Έστω $(G, \star)$ μια ομάδα. Ένα $H \subseteq G$ λέγεται κλειστό υποσύνολο του $(G, \star)$, αν $h_1 \star h_2 \in H$ για κάθε $h_1, h_2 \in H$.*

**Παρατήρηση 3.2.2.** *Αν το $H \subseteq G$ είναι κλειστό, τότε ορίζεται μια πράξη*

$$\star : H \times H \to H,\ (h_1, h_2) \mapsto h_1h_2.$$

**Ορισμός 3.2.3.** *Έστω $(G,\star)$ μια ομάδα και $H \subseteq G$ κλειστό. Το $H$ λέγεται υποομάδα της $(G,\star)$, αν το ζεύγος $(H,\star)$ είναι ομάδα.*
*Συμβολισμός. Αν $H$ είναι υποομάδα της $G$, θα γράφουμε $H \leq G$. Θα γράφουμε $G$ στην θέση του $(G,\star)$.*

**Παρατηρήσεις 3.2.4.** *Έστω $H \leq G$. Τότε ισχύουν τα ακόλουθα.*

(i) $1_H = 1_G$ *( $H$ και $G$ έχουν το ίδιο ουδέτερο στοιχείο).*

(ii) *Έστω $h \in H$. Τότε το αντίστροφο του $h$ στην $H$ είναι ίσο με το αντίστροφο του $h$ στην $G$.*

**Παραδείγματα 3.2.5.** (i) *Έστω $G = \mathbb{Z}$ (με πράξη την πρόσθεση). Το $\mathbb{N}$ είναι κλειστό, αλλά όχι υποομάδα.*

(ii) $\mathbb{Z} \leq \mathbb{Q}$, $\mathbb{Z} \leq \mathbb{R}$, $\mathbb{Z} \leq \mathbb{C}$, $\mathbb{Q} \leq \mathbb{R}$.

(iii) $\mathbb{R} \setminus \{0\}$ *(ως προς τον πολλαπλασιασμό) είναι υποομάδα του* $\mathbb{C} \setminus \{0\}$.

(iv) *Έστω* $E_n = \{z \in \mathbb{C} : z^n = 1\}$. *Τότε,* $E_n \leq \mathbb{C} \setminus \{0\}$.

**Πρόταση 3.2.6.** *Έστω $G$ ομάδα και $H \subseteq G$, $H \neq \emptyset$. Τότε τα ακόλουθα είναι ισοδύναμα.*

(i) $H \leq G$.

(ii) *Για κάθε* $h_1, h_2 \in H$, *ισχύει* $h_1 h_2 \in H$ *και* $h_1^{-1} \in H$.

(iii) *Για κάθε* $h_1, h_2 \in H$, *ισχύει* $h_1 h_2^{-1} \in H$.

*Απόδειξη.* (i) $\Rightarrow$ (ii). Άμεσο από τον ορισμό.

(ii) $\Rightarrow$ (iii). Έστω $h_1, h_2 \in H$. Τότε από την υπόθεση έπεται ότι $h_1, h_2^{-1} \in H$. Επομένως πάλι από την υπόθεση παίρνουμε ότι, $h_1 h_2^{-1} \in H$.

(iii) $\Rightarrow$ (i). Έστω $h \in H$ ($H \neq \emptyset$). Τότε $hh^{-1} \in H$, δηλαδή $1_G \in H$.

Έστω $h \in H$. Από πριν έχουμε $1_G \in H$, άρα $1_G h^{-1} \in H$, οπότε $h^{-1} \in H$.

Έστω $h_1, h_2 \in H$. Τότε $h_1 h_2^{-1} \in H$, άρα $h_1 (h_2^{-1})^{-1} \in H$, δηλαδή $h_1 h_2 \in H$, άρα $H$ κλειστό.

Τέλος, αν $h_1, h_2, h_3 \in H$, τότε

$$h_1(h_2 h_3) = (h_1 h_2) h_3,$$

αφού $H \subseteq G$ και $G$ ομάδα. Έπεται ότι $H \leq G$. □

**Παραδείγματα 3.2.7.** (i) *Έστω $G = GL_2(\mathbb{R}) = \{A \in M_2(\mathbb{R}) : \det A \neq 0\}$. Τότε η $G$ είναι ομάδα ως προς τον πολλαπλασιασμό πινάκων (εδώ $G = U(M_2(\mathbb{R}))$. Έστω $H = SL_2(\mathbb{R}) = \{A \in M_2(\mathbb{R}) : \det A = 1\}$. Τότε $SL_2(\mathbb{R}) \leq GL_2(\mathbb{R})$.*

*Πράγματι, έστω $A, B \in SL_2(\mathbb{R})$. Τότε* $\det A = \det B = 1$. *Άρα,*

$$\det(AB) = (\det A)(\det B) = 1 \Rightarrow AB \in SL_2(\mathbb{R})$$

*και*

$$\det A^{-1} = \frac{1}{\det A} = 1 \Rightarrow A^{-1} \in SL_2(\mathbb{R}).$$

(ii) *Έστω* $G = S_n$ *και* $H = \{\sigma \in S_n : \sigma(n) = n\}$. *Τότε* $H \leq S_n$.

*Πράγματι, έστω* $\sigma, \tau \in S_n$. *Τότε,* $\sigma(n) = n$, $\tau(n) = n$. *Έχουμε* $H \neq \emptyset$,*άρα*

$$\sigma\tau(n) = \sigma(\tau(n)) = \sigma(n) = n.$$

*Επομένως* $\sigma\tau \in H$. *Επίσης,*

$$\sigma(n) = n \Rightarrow \sigma^{-1}(n) = n,$$

*άρα* $\sigma^{-1} \in H$. *Επομένως* $H \leq S_n$.

(iii) *Έστω* $G$ *αβελιανή ομάδα και* $H = \{g \in G : g^2 = 1\}$. *Τότε* $H \leq G$.

*Πράγματι,* $H \neq \emptyset$, *αφού* $1 \in H$. *Έστω* $g_1, g_2 \in H$. *Τότε* $g_1^2 = g_2^2 = 1$. *Επειδή η* $G$ *είναι αβελιανή έπεται,*

$$(g_1 g_2)^2 = g_1^2 = g_2^2 = 1,$$

*άρα* $g_1 g_2 \in H$. *Έστω* $g \in H$. *Τότε* $g^2 = 1$, *άρα*

$$(g^{-1})^2 = (g^2)^{-1} = 1.$$

*Επομένως* $g^{-1} \in H$.

*Σημείωση. Αν η* $G$ *δεν είναι αβελιανή και* $H = \{g \in G : g^2 = 1\}$ *δεν είναι αναγκαστικά υποομάδα.*

*Πράγματι έστω* $G = S_3$. *Τότε* $H = \{1, (1\ 2), (1\ 3), (2\ 3)\}$. *Παρατηρήστε ότι,* $(1\ 2)(1\ 3) = (1\ 3\ 2) \notin H$, *άρα* $H \not\leq G$. *Δηλαδή το* $H$ *δεν είναι κλειστό.*

(iv) *Έστω* $G$ *ομάδα και*

$$Z(G) = \{a \in G : ag = ga, \quad \textit{για κάθε } a \in G\}.$$

*(Το* $Z(G)$ *λέγεται το κέντρο της ομάδας* $G$.*) Τότε* $Z(G) \leq G$.

*Πράγματι,* $Z(G) \neq \emptyset$, *αφού* $1g = g1(= g)$ *για κάθε* $g \in G$. *Άρα* $1 \in Z(G)$. *Έστω* $a, b \in Z(G)$. *Τότε*

$$ag = ga \qquad \textit{και} \qquad bg = gb \qquad \textit{για κάθε} \qquad g \in G.$$

*Τότε,*

$$(ab)g = a(bg) = a(gb) = (agb) = (gab) = g(ab).$$

*Άρα* $ab \in Z(G)$. *Έστω* $a \in Z(G)$. *Τότε* $ag = ga$ *για κάθε* $g \in G$ . *Επομένως,*

$$(ag)^{-1} = (ga)^{-1} \Rightarrow g^{-1}a^{-1} = a^{-1}g^{-1},$$

*που ισχύει για κάθε $g \in G$. Γράφοντας την παραπάνω σχέση για $g^{-1}$ στην θέση του $g$ παίρνουμε,*

$$(g^{-1})^{-1}a^{-1} = a^{-1}(g^{-1})^{-1} \Rightarrow ga^{-1} = a^{-1}g.$$

*Δηλαδή, $a^{-1} \in Z(G)$.*

*Σημείωση. $Z(S_n) = \{1\}$, αν $n \geqslant 3$. $Z(G) = G$ αν και μόνο αν $G$ αβελιανή.*

$$Z(GL_2(\mathbb{R})) = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \in GL_2(\mathbb{R}) : \alpha \in \mathbb{R}, \alpha \neq 0 \right\}.$$

(v) *Έστω $m, n \in \mathbb{Z}_{>0}$ και $E_n = \{z \in \mathbb{C} : z^n = 1\}$. Τότε $E_m \leq E_n$ αν και μόνο αν $m|n$.*

*Πράγματι, έστω $E_m \leq E_n$. Έχουμε $z = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}$. Είδαμε ότι (παράδειγμα (3.1.6)(5) ), $z \in E_n$ έχει τάξη $m$ . Αφού $z \in E_n$ έπεται $z^n = 1$, οπότε από το θεώρημα 3.1.27 παίρνουμε $m|n$.*

*Αντίστροφα, έστω $m|n$. Τότε $E_m \subseteq E_n$ (αν $a \in \mathbb{C}$ και $a^m = 1$, τότε $a^n = (a^m)^{n/m}$. Παρατηρήστε ότι, $E_m \neq \emptyset$ ($1 \in E_m$). Έστω $a, b \in E_m$. Τότε $a^m = b^m = 1$, άρα*

$$(ab)^m = a^m b^m = 1,$$

*δηλαδή $ab \in E_m$. Έστω $a \in E_m$. Τότε,*

$$a^m = 1 \Rightarrow a^{-m} = 1 \Rightarrow (a^{-1})^m = 1.$$

*Επομένως $a^{-1} \in E_m$.*

*Σημείωση. Αφού $E_m, E_n$ ομάδες ως προς τον πολλαπλασιασμό, για να δείξουμε ότι $E_m \leq E_n$ (όπου $m|n$) ήταν αρκετό να παρατηρήσουμε ότι $E_m \subseteq E_n$.*

**Θεώρημα 3.2.8.** *(Lagrange.) Έστω $G$ πεπεραμένη ομάδα και $H \leq G$. Τότε $|H| \mid |G|$.*

**Πόρισμα 3.2.9.** *Έστω $G$ πεπεραμένη ομάδα και $g \in G$. Τότε $|g| \mid |G|$ και $g^n = 1$, όπου $n = |G|$.*

**Πόρισμα 3.2.10.** *(Euler.) Έστω $\alpha, m \in \mathbb{Z}$ με μκδ$(\alpha, m) = 1$. Τότε $\alpha^{\varphi(m)} \equiv 1 \mathrm{mod} m$.*

*Απόδειξη του θεωρήματος* 3.2.8. Θα δείξουμε ότι το σύνολο $G$ είναι ξένη ένωση υποσυνόλων καθένα από τα οποία έχει $|H|$ στοιχεία. Έστω $G$ ομάδα και $H \leq G$. Έστω $a, b \in G$. Ορίζουμε την σχέση

$$a \sim b \Leftrightarrow b^{-1}a.$$

Αυτή είναι μια σχέση ισοδυναμίας. Πράγματι,

(i) $a \sim a$ για κάθε $a \in G$, αφού $a^{-1}a = 1 \in H$.

(ii) Αν $a \sim b$, τότε

$$b^{-1}a \in H \Rightarrow (b^{-1}a)^{-1} \in H \Rightarrow a^{-1}(b^{-1})^{-1} = a^{-1}b \in H.$$

Δηλαδή $b \sim a$.

(iii) Αν $a \sim b$ και $b \sim c$, τότε $b^{-1}a \in H$ και $c^{-1}b \in H$. Τότε,

$$(c^{-1}b)(b^{-1}a) = c^{-1}a \in H,$$

Δηλαδή $a \sim c$.

Γνωρίζουμε ότι αν $[a] = \{g \in G : g \sim a\}$ (η κλάση ισοδυναμίας περιέχει το $a$), τότε

(i) $[a] = [b] \Leftrightarrow a \sim b \Leftrightarrow b^{-1}a \in H$.

(ii) Αν $a \nsim b$, τότε $[a] \cap [b] = \emptyset$.

Άρα $G = \bigcup_{a \in A}[a]$ (ξένη ένωση) για κάποιο $A \subseteq G$. Αν $a \in G$, θέτουμε

$$aH = \{ah : h \in G\}.$$

Τότε $[a] = aH$. Πράγματι, $[a] = \{g \in G : g \sim a\}$ και

$$g \sim a \Leftrightarrow a^{-1}g \in H \quad \Leftrightarrow \quad \text{υπάρχει } \ h \in H \ \text{ ώστε } \ g = ah.$$

Άρα έχουμε από πριν μια ξένη ένωση,

$$G = \bigcup aH, \ \ a \in A. \tag{3.2.1}$$

Θα δείξουμε τώρα ότι

$$|aH| = |H|, \qquad \text{για κάθε} \qquad g \in G. \tag{3.2.2}$$

Πράγματι, η απεικόνιση $f : H \to aH, \quad f(h) = ah$ είναι 1-1 (αν $f(h_1) = f(h_2)$ τότε $ah_1 = ah_2 \Rightarrow h_1 = h_2$ ) και επί.

Έστω $G$ πεπερασμένη. Λόγω της (3.2.1) έχουμε μια ξένη ένωση,

$$G = a_1H \cup a_2H \cup \cdots \cup a_\kappa H$$

και από την (3.3.2), έπεται $|a_iH| = |H|$ για κάθε $i$. Άρα,

$$|G| = |a_1H| + \cdots + |a_\kappa H| = |H| + \cdots + |H| = \kappa|H|.$$

Άρα $|H| \mid |G|$. □

Για την απόδειξη του πορίσματος 3.2.9 χρειαζόμαστε πρώτα μια πρόταση.

Έστω $G$ ομάδα και $g \in G$. Έστω ότι το $g$ έχει πεπερασμένη τάξη $\kappa$, $|g| = \kappa$. Θέτουμε,

$$< g >= \{g^m \in G : m \in \mathbb{Z}\} \qquad (g^0 = 1).$$

Παρατηρήστε ότι , $< g > \leq G$. Πράγματι, αν $g^{m_1} \in < G >$ και $g^{m_2} \in < G >$ , τότε

$$(g^{m_1})(g^{m_2})^{-1} = g^{m_1} \cdot g^{-m_2} = g^{m_1 - m_2} \in < G > .$$

Άρα $< g > \leq G$.

**Πρόταση 3.2.11.** $| < g > | = \kappa$.

*Απόδειξη.* Ισχυριζόμαστε ότι,

$$| < g > | = \{1, g, g^2, \cdots, g^{\kappa-1}\}.$$

Πράγματι τα στοιχεία στο δεξί σύνολο είναι ανά δύο διαφορετικά (αφού $\kappa = |g|$). Ο εγκλεισμός $\supseteq$ είναι προφανής. Έστω $g^m \in < g >$. Επειδή $g^\kappa = 1$, έπεται $g^m = g^r$, όπου το $r$ είναι το υπόλοιπο της διαίρεσης του $m$ με το $\kappa$. Άρα $g^m = g^r \in \{1, g, g^2, \cdots, g^{\kappa-1}\}$, δηλαδή $| < g > | \subseteq \{1, g, g^2, \cdots, g^{\kappa-1}\}$. □

*Απόδειξη του πορισματος* 3.2.9. Επειδή η $G$ είναι πεπερασμένη, το $g$ έχει πεπερασμένη τάξη (από τον ορισμό της τάξης, αφού υπάρχουν $i, j \in \mathbb{Z}_{>0}$ με $g^i = g^j \Rightarrow g^{i-j} = 1$). Από την πρόταση 3.2.11 έπεται $| < g > | = |g| = \kappa$. Από το θεώρημα Lagrange, παίρνουμε $| < g > | \,|\, |G|$, δηλαδή $\kappa \mid |G|$. Αφού $\kappa \mid n$ και $g^\kappa = 1$, έπεται $g^n = 1$. □

*Απόδειξη του πορισματος* 3.2.10. Θεωρούμε την ομάδα $U(\mathbb{Z}_m)$ των αντιστρέψιμων στοιχείων του δακτυλίου $\mathbb{Z}_m$ (με πράξη τον πολλαπλασιασμό του $\mathbb{Z}_m$). Γνωρίζουμε ότι $|U(\mathbb{Z}_m)| = \varphi(m)$. Επίσης γνωρίζουμε ότι,

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

Από το πόρισμα 3.2.9, έπεται $[\alpha]^{\varphi(m)} = [1]$, δηλαδή $\alpha^{\varphi(m)} \equiv 1 \mathrm{mod} m$ (όταν $\mu\kappa\delta(\alpha, m) = 1$). □

Έστω $G$ ομάδα και $g \in G$. Είδαμε ότι το σύνολο $< g >= \{g^m : m \in \mathbb{Z}\}$ είναι υποομάδα της $G$.

**Ορισμός 3.2.12.** *$H < g >$ λέγεται η κυκλική υποομάδα της $G$ που παράγεται από το $g$.*

**Ορισμός 3.2.13.** *Η ομάδα $G$ λέγεται κυκλική, αν υπάρχει $g \in G$ ώστε $G =< g >$.*

Είδαμε πριν ότι,

**Πρόταση 3.2.14.** *Αν $g \in G$ και $|g| = \kappa < \infty$, τότε $| < g > | = \kappa$. Το ίδιο ισχύει και όταν το $g$ έχει άπειρη τάξη.*

**Παράδειγμα 3.2.15.** *(Στην απόδειξη του θεωρήματος Lagrange.) Είδαμε ότι αν $G$ πεπερασμένη ομάδα και $H \leq G$, τότε υπάρχει ξένη ένωση της μορφής*

$$G = a_1 H \cup a_2 H \cup \cdots \cup a_\kappa H.$$

*Το $\kappa$ είναι μοναδικό (αφού $|G| = \kappa|H|$) και λέγεται ο δείκτης της $H$ στην $G$. Συμβολίζουμε με $\kappa = [G : H]$*

*Έστω $G = S_4$ και $H = \{\sigma \in S_4 : \sigma(4) = 4\}$. Τότε $H \leq G$ (παράδειγμα 3.2.7(ii) ). Παρατηρήστε ότι,*

$$[G : H] = \frac{|G|}{|H|} = \frac{4!}{3!} = 4.$$

*Ας βρούμε στοιχεία $a_1, a_2, a_3, a_4$ όπως στην (3.2.1). Θα δείξουμε ότι έχουμε την ξένη ένωση*

$$S_4 = H \cup (1\ 4)H \cup (2\ 4)H \cup (3\ 4)H \ \ (a_1 = 1, a_2 = (1\ 4), a_3 = (2\ 4), a_4 = (3\ 4)).$$

*Πράγματι στο δεξί μέλος έχουμε μια ξένη ένωση, για παράδειγμα*

$$\text{για κάθε } \sigma \in H, \sigma(4) = 4,$$

$$\text{για κάθε } \sigma \in (1\ 4), \sigma(4) = 1,$$

$$\text{για κάθε } \sigma \in (2\ 4), \sigma(4) = 2,$$

$$\text{για κάθε } \sigma \in (3\ 4), \sigma(4) = 3.$$

*(Ανά δύο στέλνουν το 4 σε διαφορετική εικόνα.) Επίσης στο ίδιο συμπέρασμα καταλήγουμε αν θεωρήσουμε τα $a_i^{-1}a_j$ δείχνοντας ότι $a_i^{-1}a_j(4) \neq 4$, δηλαδή $a_i^{-1}a_j \notin H$. Παρατηρήστε ότι,*

$$S_4 \supseteq a_1H \cup \cdots \cup a_4H$$

*και επειδή*

$$|S_4| = |a_1H| + \cdots + |a_4H|$$

*(αφού $|a_1H| + \cdots + |a_4H| \overset{\text{(ξένη ένωση)}}{=} 3! + 3! + 3! + 3! = 4! = 24$), έπεται*

$$S_4 = a_1H \cup \cdots \cup a_4H.$$

□

### 3.2α΄ Άρτιες και περιττές μεταθέσεις

**Ορισμός 3.2.16.** *Μια μετάθεση $\sigma \in S_n$ λέγεται αντιμετάθεση αν η $\sigma$ είναι κύκλος μήκους 2, δηλαδή αν $\sigma = (i\ j)$.*

**Πρόταση 3.2.17.** *Κάθε μετάθεση είναι γινόμενο αντιμεταθέσεων.*

*Απόδειξη.* Γνωρίζουμε ότι κάθε μετάθεση είναι γινόμενο κύκλων. Αρκεί να δείξουμε ότι κάθε κύκλος είναι γινόμενο αντιμεταθέσεων. Εύκολα αποδεικνύεται ότι,

$$(a_1\ a_2 \cdots a_{\kappa-1}\ a_\kappa) = (a_1\ a_\kappa)(a_1\ a_{\kappa-1}) \cdots (a_1\ a_3)(a_1\ a_2). \tag{3.2.3}$$

□

**Ορισμός 3.2.18.** *Έστω $\sigma \in S_n$. Η $\sigma$ λέγεται*

(i) *άρτια αν είναι γινόμενο άρτιου πλήθους αντιμεταθέσεων,*

(ii) *περιττή αν είναι γινόμενο περιττού πλήθους αντιμεταθέσεων,*

**Παράδειγμα 3.2.19.** *Η $\sigma = (1\ 2\ 3)$ είναι άρτια αφού $\sigma = (1\ 2)(1\ 3)$.*

*Έστω*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 6 & 1 & 2 & 5 & 4 \end{pmatrix} \in S_7.$$

*Βρίσκοντας κατά τα γνωστά την ανάλυση της $\sigma$ σε γινόμενο ξένων κύκλων, έχουμε*

$$\sigma = (1\ 7\ 4)(2\ 3\ 6\ 5).$$

*Λόγω της (3.2.3) παίρνουμε,*

$$\sigma = ((1\ 4)(1\ 7))\,((2\ 5)(2\ 6)(2\ 3))\,.$$

*Άρα η $\sigma$ είναι περιττή.*

**Παρατήρηση 3.2.20.** *Στο τελευταίο παράδειγμα χρειαζόμαστε μια ανάλυση της $\sigma$ σε γινόμενο κύκλων, όχι αναγκαστικά ξένων.*

**Πρόταση 3.2.21.** *Δεν υπάρχει $\sigma \in S_n$ ώστε η $\sigma$ να είναι άρτια και περιττή.*

*Απόδειξη.* Έστω

$$\sigma = \sigma_1\sigma_2\cdots\sigma_s, \tag{3.2.4}$$

$\sigma_i$ αντιμετάθεση για κάθε $i$ και

$$\sigma = \tau_1\tau_2\cdots\tau_t, \tag{3.2.5}$$

$\tau_j$ αντιμετάθεση για κάθε $j$. Θα δείξουμε ότι $s \equiv t \bmod 2$. Αν $A \in M_n(\mathbb{R})$ με $\sigma(A)$ συμβολίζουμε τον πίνακα που έχει $\sigma(i)$- στήλη την $i$- στήλη του $A$. Για παράδειγμα, για $n = 3$ και $A = I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, αν $\sigma = (1\ 2)$ τότε,

$$\sigma(I_3) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

και αν $\sigma = (2\ 1\ 3)$ τότε,

$$\sigma(I_3) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Δηλαδή ο $\sigma(I_n)$ προκύπτει από τον $I_n$ εναλλάσσοντας τις στήλες του $I_n$ κατά την μετάθεση $\sigma$. Από την Γραμμική Άλγεβρα θυμίζουμε ότι αν ο πίνακας $B$ προκύπτει εναλλάσσοντας τις θέσεις δύο στηλών ενός πίνακα τότε $\det B = -\det A$. Άρα,

$$\det\sigma(I_n) = (-1)^s$$

από την (3.2.4) και

$$\det\sigma(I_n) = (-1)^t$$

από την (3.2.5). Επομένως,

$$(-1)^s = (-1)^t \Rightarrow s \equiv t \mathrm{mod} 2.$$

□

**Ορισμός 3.2.22.** *$A_n = \{\sigma \in S_n : \sigma$ άρτιος$\}$. Για παράδειγμα,*

$$A_1 = \{1\},\ A_2 = \{1\},\ A_3 = \{1, (1\ 2\ 3), (2\ 1\ 3)\}.$$

$$\sigma = (1\ 2\ 3\ 4) \notin A_4,\ \text{αφού } \sigma = (1\ 4)(1\ 3)(1\ 2).$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \in A_4,\ \text{αφού } \sigma = (1\ 4)(2\ 3).$$

**Θεώρημα 3.2.23.** *Ισχύει $A_n \leq S_n$ και $n \geqslant 2$, $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$.*

*Απόδειξη.* Έστω $\sigma, \tau \in A_n$. Τότε

$$\sigma = \sigma_1\sigma_2\cdots\sigma_s,$$

$\sigma_i$ αντιμετάθεση για κάθε $i$ και

$$\tau = \tau_1\tau_2\cdots\tau_t,$$

$\tau_j$ αντιμετάθεση για κάθε $j$ και $s, t$ άρτιοι. Άρα,

$$\sigma\tau = \sigma_1\sigma_2\cdots\sigma_s\tau_1\tau_2\cdots\tau_t \in A_n,$$

αφού $s + t$ άρτιος. Επίσης,

$$\sigma^{-1} = (\sigma_1\sigma_2\cdots\sigma_s)^{-1} = \sigma_s^{-1}\cdots\sigma_2^{-1}\sigma_1^{-1} = \sigma_s\cdots\sigma_2\sigma_1 \in A_n,$$

αφού $s$ άρτιος. Άρα $A_n \leq S_n$.

Θα δείξουμε τώρα ότι $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$. Έστω

$$B_n = \{\sigma \in S_n : \sigma \text{ περιττός}\}.$$

Από την πρόταση 3.2.18, $S_n = A_n \cup B_n$. Από την πρόταση 3.2.22 η ένωση $S_n = A_n \cup B_n$ είναι ξένη ένωση. Άρα

$$|S_n| = |A_n| + |B_n|.$$

Αρκεί να δείξουμε ότι $|A_n| = |B_n|$. Θεωρούμε την απεικόνιση

$$f : A_n \to B_n,\ \ f(\sigma) = (1\ 2)\sigma.$$

Παρατηρήστε ότι αν $\sigma \in A_n$, τότε $(1\ 2)\sigma \in B_n$. Επίσης αν $f(\sigma) = f(\tau)$, τότε

$$(1\ 2)\sigma = (1\ 2)\tau \Rightarrow \sigma = \tau,$$

δηλαδή η $f$ είναι 1-1. Έστω $\tau \in B_n$. Τότε $(1\ 2)\tau \in A_n$ και

$$f\left((1\ 2)\tau\right) = (1\ 2)(1\ 2)\tau = \tau.$$

Άρα η $f$ είναι επί. Επομένως $|A_n| = |B_n|$. □

**Παρατηρήσεις 3.2.24.** (i) *Στην θέση του* $(1\ 2)$ *στην τελευταία απόδειξη θα μπορούσαμε να πάρουμε οποιαδήποτε περιττή μετάθεση.*

(ii) *Από την απόδειξη έπεται ότι για κάθε* $\sigma \in S_n$ *περιττή μετάθεση έχουμε την ξένη ένωση* $S_n = A_n \cup \sigma(A_n)$.

### Ασκήσεις

**1**. Ποιες από τις παρακάτω ομάδες είναι κυκλικές;

(i) $\mathbb{Z}$

(ii) $\mathbb{Z}_n$

(iii) $E_n$

(iv) $U(\mathbb{Z}_5)$

(v) $U(\mathbb{Z}_8)$

(vi) $S_3$

(vii) $\left\{ \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{Z}) : m \in \mathbb{Z} \right\}$

*Λύση.* (i). Η ομάδα $\mathbb{Z}$ είναι κυκλική, αφού

$$\mathbb{Z} =< 1 >= \{m \cdot 1 : m \in \mathbb{Z}\}.$$

(ii). Η $\mathbb{Z}_n$ είναι κυκλική, αφού

$$\mathbb{Z}_n =< [1] >= \{m[1] = [m] : m \in \mathbb{Z}\}.$$

(iii). Έστω $z_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

$$E_n = \{1, z_1, z_1^2, \cdots, z_1^{n-1}\}.$$

Άρα η $E_n$ είναι κυκλική και $E_n =< z_1 >$.

(iv). Γνωρίζουμε ότι $|U(\mathbb{Z}_5)| = \varphi(5) = 4$. Θα εξετάσουμε αν υπάρχει $\alpha \in \mathbb{Z}_5$ τάξης 4. Έστω $\alpha = [2] \in U(\mathbb{Z}_5)$ τυχόν. Παρατηρήστε ότι,

$$\alpha^2 = [2]^2 = [4],\ \alpha^3 = [2]^3 = [8] = [3],\ \alpha^4 = [2]^4 = [16] = [1].$$

Άρα $|\alpha| = 4$ για $\alpha = 2$. Επομένως η $U(\mathbb{Z}_5)$ είναι κυκλική και ένας γεννήτορας είναι το 2, $U(\mathbb{Z}_5) =< [2] >$.

(v).

**Παρατήρηση 3.2.25.** *Αν $G$ κυκλική, τότε $G$ αβελιανή.*

*Πράγματι, έστω $G =< g >$ και $a, b \in G$. Τότε $a = g^m$ και $b = g^n$ για κάποια $m, n \in \mathbb{Z}$. Άρα,*

$$ab = g^m \cdot g^n = g^{m+n} = g^n \cdot g^m = ba.$$

Γνωρίζουμε ότι $U(\mathbb{Z}_8) = \{[1], [3], [5], [7]\}$.

| $g \in U(\mathbb{Z}_8)$ | $[1]$ | $[3]$ | $[5]$ | $[7]$ |
|---|---|---|---|---|
| $\lvert g\rvert$ | 1 | 2 | 2 | 2 |

Παρατηρήστε ότι δεν υπάρχει στοιχείο τάξης $4 = U(\mathbb{Z}_8)$ (τάξη ίση με το πλήθος των στοιχείων της ομάδας), άρα $\mathbb{Z}_8$ όχι κυκλική.

(vi). Υπενθυμίζουμε ότι αν $G$ ομάδα και $g \in G$, τότε $|g| =< g >$. Η $S_3$ δεν είναι κυκλική (δεν είναι αβελιανή).

(vii). Παρατηρήστε ότι,

$$\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m$$

για κάθε $m \in \mathbb{Z}$. Επομένως η $\left\{ \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{Z}) : m \in \mathbb{Z} \right\}$ είναι κυκλική. □

**2**. Έστω $G$ ομάδα και $H \leq G,\ K \leq G$.

(i) $H \cap K \leq G$.

(ii) Αν $|H| = m,\ |K| = n,\ \mu\kappa\delta(m, n) = 1$, τότε $H \cap K = \{1\}$.

*Απόδειξη.* Παρατηρήστε ότι, $H \cap K \leq H$ και $H \cap K \leq K$. Από το θεώρημα Lagrange έχουμε,

$$|H \cap K| \mid m \qquad \text{και} \qquad |H \cap K| \mid n.$$

Τότε,

$$|H \cap K| \mid \mu\kappa\delta(m, n) \Rightarrow |H \cap K| = 1 \Rightarrow H \cap K = \{1\}.$$

□

**3**. Έστω $G$ πεπερασμένη ομάδα και $H \leq G,\ K \leq G$.

(i) Αν $H \subseteq K$, τότε $[G : H] = [G : K][K : H]$.

(ii) $[G : H \cap K] \leq [G : H][G : K]$.

*Απόδειξη.* (i). Αφού $H \leq G$, $H \subseteq K$ και $K \leq G$ έπεται $H \leq K$. Από το θεώρημα Lagrange έχουμε $[G : H] = \frac{|G|}{|H|}$, $[G : K] = \frac{|G|}{|K|}$ και $[K : H] = \frac{|K|}{|H|}$. Παρατηρήστε ότι,

$$[G : K] = \frac{G}{K} = \frac{\frac{G}{H}}{\frac{K}{H}} = \frac{[G : H]}{[K : H]}.$$

Επομένως,

$$[G : H] = [G : K][K : H].$$

(ii). Από το ερώτημα (i) έχουμε,

$$[G : H \cap K] = [G : H][H : H \cap K].$$

Επομένως αρκεί να δείξουμε ότι $[H : H \cap K] \leq [G : K]$. Ορίζουμε την απεικόνιση

$$\varphi : \{h(H \cap K)\} \to \{gK : g \in G\},\ \ \varphi\left(h(H \cap K)\right) = hK.$$

Θα δείξουμε ότι η $\varphi$ είναι καλώς ορισμένη και 1-1.

Πράγματι, έστω $h_1(H \cap K) = h_2(H \cap K)$. Τότε $h_2^{-1}h_1 \in H \cap K$. Άρα,

$$h_2^{-1}h_1 \in K \Rightarrow h_1K = h_2K.$$

Άρα η $\varphi$ είναι καλώς ορισμένη.

Έστω $h_1K = h_2K$ $(h_i \in H)$. Τότε $h_2^{-1}h_1 \in K$. Αλλα $h_2^{-1}h_1 \in H$, άρα $h_2^{-1}h_1 \in H \cap K$. Συνεπώς $h_1(H \cap K) = h_2(H \cap K)$ .Άρα η $\varphi$ είναι και 1-1. □

**4**. Έστω $G$ ομάδα, $a, b \in G$ με $ab = ba$, $|a| = m$, $|b| = n$, μκδ$(m, n) = 1$. Τότε $|ab| = m \cdot n$.

*Απόδειξη.* Αφού $ab = ba$, έπεται

$$(ab)^{mn} = a^{mn} \cdot b^{mn} = (a^m)^n \cdot (b^m)^n = 1 \cdot 1 = 1.$$

Άρα $|ab| \geqslant m \cdot n$.

Έστω ότι $(ab)^s = 1,\ s \in \mathbb{Z}_{>0}$. Τότε $a^s b^s = 1$, άρα $a^s = b^{-s} \in < a > \cap < b >$. Από το πόρισμα 3.2.9 παιρνουμε $|a^s| \mid | < a > |$, δηλαδή $|a^s| \mid m$. Ομοίως $a^s = b^{-s} \in < b >$, άρα $|a^s| \mid n$. Επομένως,

$$|a^s| \mid \text{μκδ}(m, n) \Rightarrow |a^s| = 1.$$

Άρα $a^s = b^{-s} = 1$. Άρα $m \mid s$ και $n \mid s$. Επειδή μκδ$(m, n) = 1$, έπεται $mn \mid s$, άρα $|ab| \geqslant mn$. Συνεπώς $|ab| = mn$. □

**5**. Έστω $G$ μια πεπερασμένη ομάδα και $p$ πρώτος.

(i) Έστω $a, b \in G$ με $|a| = |b| = p$. Τότε,

$$< a > \cap < b >= \{1\} \qquad \text{ή} \qquad < a >=< b > .$$

(ii) Το πλήθος των στοιχείων της $G$ τάξης $p$ είναι πολλαπλάσιο του $p-1$.

(iii) Αν $|G| = 33$, τότε η $G$ έχει στοιχείο τάξης 3 .

*Απόδειξη*. (i). Επειδή $< a > \cap < b > \leq < a >$ και $| < a > | = p$, από το θεώρημα Lagrange παίρνουμε,

$$| < a > \cap < b > | \; | \; | < a > | \Rightarrow | < a > \cap < b > | = 1 \;\; \text{ή} \;\; p.$$

Αν $| < a > \cap < b > | = 1$, τότε $< a > \cap < b >= \{1\}$. Έστω $| < a > \cap < b > | = p$. Τότε $< a > \cap < b > \leq < a >$ και $| < a > \cap < b > | = | < a > |$. Άρα $< a > \cap < b >=< a >$, οπότε $< a > \subseteq < b >$. Δηλαδή $< a >=< b >$.

(ii). Παρατηρήστε ότι αν $a \in G$ έχει τάξη $p$ τότε κάθε στοιχείο $\neq 1$ της $< a >$ έχει τάξη $p$ (έπεται από το πόρισμα 3.2.9). Έστω $G_p = \{g \in G : |g| = p\}$. Τότε από αυτό που παρατηρήσαμε παραπάνω έπεται,

$$G_p = \bigcup_{a \in G_p} (< a > -1).$$

Από το πρώτο ερώτημα έπεται η ύπαρξη της ξένης ένωσης

$$G_p = \bigcup_{a \in G_p} (< a > -1),$$

όπου $A \subseteq G_p$. Επειδή το σύνολο $< a > -1$ έχει $p-1$ στοιχεία, έπεται ότι το πλήθος των στοιχείων του $G_p$ είναι πολλαπλάσιο του $p-1$.

(iii). Έστω $g \in G,\ g \neq 1$. Τότε $|g| \mid 33$, δηλαδή $|g| = 33, 11, 3$.

Έστω ότι υπάρχει $g \in G$, με $|g| = 33$. Τότε το στοιχείο $h = g''$ έχει τάξη

$$\frac{33}{\text{μκδ}(33, 11)} = \frac{33}{11} = 3.$$

Έστω ότι κάθε $g \in G, g \neq 1$ έχει τάξη 11. Τότε από το δεύτερο ερώτημα, $|G \setminus \{1\}| =$ πολλαπλάσιο του 10. Δηλαδή $32 =$ πολλαπλάσιο του 10, άτοπο. □

**6**. Έστω $G$ ομάδα τάξης $2m$.

(i) Δείξτε ότι η $G$ έχει στοιχείο τάξης 2.

(ii) Δείξτε ότι το πλήθος των στοιχείων της $G$ τάξης 2 είναι περιττός.

(iii) Δείξτε ότι αν το $m$ είναι περιττός και η $G$ αβελιανή, τότε υπάρχει μοναδικό στοιχείο τάξης 2.

*Απόδειξη.* (i) και (ii).

**Παρατήρηση 3.2.26.** *(α′) Αν $a, b \in G$ τότε $a = b \Leftrightarrow a^{-1} = b^{-1}$.*

*(β′) Αν $a \in G$ τότε $|a| = |a^{-1}|$.*

*(γ′) Αν $a \in G$ τότε $a \neq a^{-1} \Leftrightarrow |a| > 2$.*

Προφανώς αφού $|G| = 2m$, η $G$ έχει στοιχείο τάξης 2. Έστω $A = \{g \in G : |g| > 2\}$. Παρατηρήστε ότι $g \in A \Leftrightarrow g^{-1} \in A$. Από την παρατήρηρση έπεται ότι $|A| =$ άρτιος. Όμως τα

$$\{g \in G : |g| = 2\} = G \setminus A \setminus \{1\}.$$

Άρα $\Big|\{g \in G : |g| = 2\}\Big| =$ περιττός.

(iii). Έστω ότι υπάρχουν $a, b \in G$, $a \neq b$ και $|a| = |b| = 2$. Θεωρούμε το

$$H = \{1, a, b, ab\}.$$

Παρατηρήστε ότι $|H| = 4$ (για παράδειγμα αν $ab = a \Rightarrow b = 1$, άτοπο). Εύκολα ελέγχουμε (χρησιμοποιώντας το γεγονός ότι η $G$ είναι αβελιανή) ότι $H \leq G$. Από το θεώρημα Lagrange έπεται ότι $4|2m$, άτοπο αφού ο $m$ είναι περιττός. □

*Σημείωση.* Στο ερώτημα (iii)της προηγούμενης άσκησης, αν η $G$ δεν είναι αβελιανή η $H$ δεν είναι αναγκαστικά υποομάδα της $G$.

Πράγματι, έστω τα στοιχεία τάξης 2 της $S_3$ είναι $(1\ 2), (1\ 3), (2\ 3)$ και $\{1, (1\ 2), (1\ 3), (2\ 3)\}$ δεν είναι υποομάδα της $S_3$.

**7**. Έστω $G$ ομάδα και $H \leq G$ με $[G : H] = n < \infty$. Δείξτε ότι για κάθε $g \in G$ υπάρχει $m \in \mathbb{Z}$, $1 \leqslant m \leqslant n$ ώστε $g^m \in H$.

*Απόδειξη.* Επειδή το σύνολο $\{aH : a \in G\}$ έχει $[G : H] = n < \infty$ στοιχεία, ανάμεσα στα $H, gH, g^2H, \cdots, g^nH$ υπάρχουν δύο που είναι ίσα. Άρα $g^iH = g^jH$ για κάποια $0 \leqslant i,\ j \leqslant n,\ i > j$. Άρα $g^{i-j} \in H$ και $1 \leqslant i - j \leqslant n$. □

**8**. Εστω $\sigma \in S_n$, $\sigma = \sigma_1\sigma_2 \cdots \sigma_m$, $\sigma_i$ κύκλος μήκους $\kappa_i$ για κάθε $i$. Τότε

$$\sigma \ \text{ άρτια} \qquad \Leftrightarrow \qquad \sum_{i=1}^{m}(\kappa_i - 1) \ \text{ άρτιος}$$

και

$$\sigma \ \text{ περιττή} \qquad \Leftrightarrow \qquad \sum_{i=1}^{m}(\kappa_i - 1) \ \text{ περιττός.}$$

*Απόδειξη.* Είδαμε ότι,

$$(a_1\ a_2 \cdots a_{\kappa-1}\ a_\kappa) = (a_1\ a_\kappa)(a_1\ a_{\kappa-1}) \cdots (a_1\ a_3)(a_1\ a_2).$$

Δηλαδή ένας $\kappa$- κύκλος είναι γινόμενο $(\kappa - 1)$ αντιμεταθέσεων. Άρα αν $\sigma$ όπως στην εκφώνηση, τότε $\sigma =$ γινόμενο αντιμεταθέσεων πλήθους $\sum_{i=1}^{m}(\kappa_i - 1)$. □

**9**. Εστω $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 5 & 2 & 6 & 3 & 1 \end{pmatrix} \in S_7$.

(i) Εξετάστε αν η $\sigma$ είναι περιττή.

(ii) Να βρεθούν όλοι οι $m \in \mathbb{Z}$ ώστε $< \sigma^m > \leq A_7$.

*Απόδειξη.* (i). Έχουμε $\sigma = (1\ 4\ 2\ 7)(3\ 5\ 6)$. Άρα

$$\sigma = ((1\ 7)(1\ 2)(1\ 4))\ ((3\ 6)(3\ 5))$$

περιττή, αφού έχουμε γινόμενο 5 αντιμεταθέσεων και ο 5 ειναι περιττός.

(ii). Παρατηρήστε ότι,

$$< \sigma^m > \leq A_7 \Leftrightarrow < \sigma^m > \subseteq A_7 \Leftrightarrow \sigma^m \in A_7 \ \ (\text{αφού} \ \ A_7 \ \ \text{ομάδα}).$$

Επίσης,

$$\sigma^m \in A_7 \Leftrightarrow \sigma^m \ \ \text{άρτια} \Leftrightarrow 5m \ \ \text{άρτιος},$$

γιατί είδαμε πριν ότι $\sigma =$ γινόμενο $5m$ αντιμεταθέσεων. Άρα,

$$< \sigma^m > \leq A_7 \Leftrightarrow m \ \ \text{άρτιος}.$$

□

**10**. Εστω $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & \alpha & 1 & \beta & 6 & 7 & 3 \end{pmatrix} \in S_7$.

(i) Να βρείτε τα $\alpha, \beta$ ώστε η $\sigma$ να είναι άρτια.

(ii) Αν η $\sigma$ είναι άρτια, αληθεύει ότι $(1\ 5)(5\ 6)(6\ 7) \in < \sigma >$;

*Απόδειξη.* (i). Για το ζεύγος $(\alpha\ \beta)$ έχουμε

$$(\alpha\ \beta) = (2\ 4) \qquad \text{ή} \qquad (\alpha\ \beta) = (4\ 2).$$

Έστω $(\alpha\ \beta) = (2\ 4)$. Τότε η ανάλυση της $\sigma$ (μετά από λίγες πράξεις) είναι $\sigma = (1\ 5\ 6\ 7\ 3)$. Έστω $(\alpha\ \beta) = (4\ 2)$. Τότε $\sigma = (1\ 5\ 6\ 7\ 3)(2\ 4)$. Παρατηρήστε ότι,

$$(1\ 5\ 6\ 7\ 3) = (1\ 3)(1\ 7)(1\ 6)(1\ 5) \in A_7$$

και

$$(1\ 5\ 6\ 7\ 3)(2\ 4) = (1\ 3)(1\ 7)(1\ 6)(1\ 5)(2\ 4) \notin A_7.$$

Άρα $\alpha = 2,\ \beta = 4$.

(ii). Επειδή $\sigma \in A_7$, έχουμε $< \sigma > \leq A_7$. Αλλά $(1\ 5)(5\ 6)(6\ 7)$ περιττή, δηλαδή $(1\ 5)(5\ 6)(6\ 7) \notin A_7$. Άρα δεν αληθεύει ότι $(1\ 5)(5\ 6)(6\ 7) \in < \sigma >$. □

**11**. Βρείτε αν υπάρχουν τα στοιχεία τάξης 6 στην $A_6$.

*Απόδειξη.* Ας βρούμε πρώτα τα στοιχεία τάξης 6 στην $S_6$. Γνωρίζουμε ότι αν

$$\sigma = \sigma_1\sigma_2\cdots\sigma_m,$$

$\sigma_i$ κύκλοι ανά δύο ξένοι, τότε

$$|\sigma| = \text{εκπ}(\kappa_1, \kappa_2, \cdots, \kappa_m),$$

όπου $\kappa_i$ το μήκος του κύκλου $\sigma_i$. Άρα $\sigma \in S_6$ έχει τάξη 6 αν και μόνο αν

(α′) $\sigma = (a_1\ a_2\cdots a_6)$ κύκλος μήκους 6

(β′) $\sigma = (a_1\ a_2\ a_3)(b_1\ b_2)$ ξένοι κύκλοι με μήκη 3 και 2.

Παρατητήστε ότι,

$$(a_1\ a_2\cdots a_6) \notin A_6,$$

αφού

$$(a_1\ a_2\cdots a_6) = (a_1\ a_6)(a_1\ a_5)(a_1\ a_4)(a_1\ a_3)(a_1\ a_2)$$

(5 αντιμεταθέσεις, 5 περιττός) και

$$(a_1\ a_2\ a_3)(b_1\ b_2) = (a_1\ a_3)(a_1\ a_2)(b_1\ b_2) \notin A_6$$

(3 αντιμεταθέσεις, 3 περιττός). □

**Παρατήρηση 3.2.27.** *Είδαμε ότι η $S_6$ δεν έχει στοιχείο τάξης 6. Άρα, αν $G$ ομάδα με $|G| = n < \infty$ και $m|n,\ m \neq n$, τότε δεν υπάρχει αναγκαστικά στοιχείο τάξης $m$.*

## 3.3 Ομομορφισμοί ομάδων - περισσότερα για κυκλικές ομάδες

Οι ομομορφισμοί ομάδων μας επιτρέπουν να συγκρίνουμε δύο ομάδες.

**Ορισμός 3.3.1.** *$(G, \cdot)$ και $(H, *)$ ομάδες. Μια απεικόνιση $f : G \to H$ λέγεται,*

(i) *ομομορφισμός αν $f(a \cdot b) = f(a) * f(b)$ για κάθε $a, b \in G$.,*

(ii) *μονομορφισμός αν είναι ομομορφισμός και 1-1.*

(iii) *επιμορφισμός αν είναι ομομορφισμός και επί,*

(iv) *ισομορφισμός αν είναι ομομορφισμός, 1-1 και επί*

*Σημείωση. Στα επόμενα θα γράφουμε $ab$ στην θέση του $a \cdot b$ και $f(a)f(b)$ στην θέση του $f(a) * f(b)$.*

**Παραδείγματα 3.3.2.** (i) *Έστω $\varphi : R \to S$ ομομορφισμός δακτυλίων. Τότε η $\varphi$ είναι ομομορφισμός ομάδων (με πράξη την $+$ των δακτυλίων). Για παράδειγμα, η απεικόνιση $\mathbb{Z} \to \mathbb{Z}_n$, $a \mapsto [a]$ είναι ομομορφισμός ομάδων ($[a+b] = [a] + [b]$, για κάθε $a, b \in G$).*

(ii) *Η απεικόνιση $\mathbb{Z} \to n\mathbb{Z}$ $(n \neq 0)$, $a \mapsto an$ είναι ομομορφισμός ομάδων. Μάλιστα είναι ισομορφισμός.*

*Η απεικόνιση $\mathbb{Z} \to n\mathbb{Z}$ $(n \neq 0)$, $a \mapsto 2an$ είναι μονομορφισμός, αλλά όχι αναγκαστικά επιμορφισμός.*

(iii) *Η απεικόνιση $\varphi : \mathbb{Z} \to E_n$, $\varphi(a) = z^\alpha$, όπου*

$$z = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \in E_n$$

*είναι επιμορφισμός ομάδων. Πράγματι,*

$$\varphi(a+b) = z^{a+b} = z^a \cdot z^b = \varphi(a)\varphi(b).$$

*Άρα $\varphi$ ομομορφισμός. Επειδή $E_n =< z >$, η $\varphi$ είναι επί.*

(iv) *Η $\varphi : \mathbb{Z}_n \to E_n$ $(n > 0)$, $\varphi([a]) = z^a$, με $z$ όπως στο (iii) είναι (καλώς ορισμένη) ισομορφισμός ομάδων. Πράγματι, έστω*

$$[a] = [b] \Rightarrow n \mid a - b \overset{(n=|E_n|)}{\Longrightarrow} z^{a-b} = 1 \Rightarrow z^a = z^b.$$

*Η $\varphi$ είναι προφανώς επί, αφού $E_n =< z >$. Τέλος η $\varphi$ είναι ομομορφισμός δακτυλίων. Πράγματι,*

$$\varphi([a+b]) = z^{a+b} = z^a z^b = \varphi([a])\varphi([b]).$$

(v) *Η $\varphi : (\mathbb{R}, \cdot) \to (\mathbb{R}, +)$, $\varphi(x) = \ln(x)$ είναι ομομορφισμός ομάδων ($\ln(xy) = \ln x + \ln y$).*

(vi) *Έστω $\sigma \in S_n$. Ορίζουμε,*

$$\operatorname{sign}(\sigma) = \begin{cases} 1, & \text{αν } \sigma \text{ άρτια} \\ -1, & \text{αν } \sigma \text{ περιττή} \end{cases}$$

*Αφού κάθε $\sigma \in S_n$ είναι ή άρτια ή περιττή (όχι και τα δύο), έχουμε την απεικόνιση $\operatorname{sign} : S_n \to \{1, -1\} = E_2$, η οποία είναι επιμορφισμός ομάδων ($n \geqslant 2$). Πράγματι, το γινόμενο*

*(α′) δύο άρτιων μεταθέσεων είναι άρτια μετάθεση,*

*(β′) δύο περιττών μεταθέσεων είναι περιττή μετάθεση,*

*(γ′) μιας άρτιας και μιας περιττής είναι περιττή (με οποιαδήποτε σειρά).*

□

**Ορισμός 3.3.3.** *Έστω $\varphi : G \to H$ ομομορφισμός ομάδων. Ορίζουμε,*

$$\mathrm{Ker}\varphi = \{g \in G : \varphi(g) = 1\} \qquad (\textit{ο πυρήνας της } \varphi)$$

*και*

$$\mathrm{Im}\varphi = \{\varphi(g) \in H : g \in G\} \qquad (\textit{η εικόνα της } \varphi).$$

**Πρόταση 3.3.4.** *Έστω $\varphi : G \to H$ ομομορφισμός ομάδων. Τότε,*

(i) $\mathrm{Ker}\varphi \leq G$.

(ii) $\mathrm{Im}\varphi \leq H$.

(iii) *$H$ $\varphi$ είναι 1-1 αν και μόνο αν* $\mathrm{Ker}\varphi = \{1\}$.

**Παρατήρηση 3.3.5.** *Έστω $\varphi : G \to H$ ομομορφισμός ομάδων. Τότε,*

(i) $\varphi(1_G) = 1_H$.

(ii) $\varphi(a^{-1}) = \varphi(a)^{-1}$ *για κάθε* $a \in G$.

(iii) $\varphi(a^m) = \varphi(a)^m$ *για κάθε* $m \in \mathbb{Z}$.

*Πράγματι, για το (i) αν $a \in G$, έχουμε*

$$a \cdot 1_G = a \Rightarrow \varphi(a \cdot 1_G) = \varphi(a) \Rightarrow \varphi(a)\varphi(1_G) = \varphi(a) \Rightarrow \varphi(1_G) = 1_H.$$

*Για το (ii) αν $a \in G$, έχουμε*

$$aa^{-1} = 1_G \Rightarrow \varphi(aa^{-1}) = \varphi(1_G) \Rightarrow \varphi(a)\varphi(a^{-1}) = 1_H \Rightarrow \varphi(a^{-1}) = (\varphi(a))^{-1}.$$

*Απόδειξη της πρότασης* 3.3.4. Ας δείξουμε ενδεικτικά το (ii).
Παρατηρήστε ότι $\mathrm{Im}\varphi \neq \emptyset$, αφού $\varphi(1_G) = 1_H$, δηλαδή $1_H \in \mathrm{Im}\varphi$.
Εστω $a, b \in \mathrm{Im}\varphi$. Τότε $\varphi(g_a) = a$ και $\varphi(g_b) = b$ για κάποια $g_a, g_b \in G$. Επομένως,

$$ab = \varphi(g_a)\varphi(g_b) = \varphi(g_a g_b) \in \mathrm{Im}\varphi.$$

Έστω $a \in \mathrm{Im}\varphi$. Τότε $a = \varphi(g_a)$ για κάποιο $g_a \in G$. Επομένως,

$$a^{-1} = (\varphi(g_a))^{-1} = \varphi(g_a^{-1}) \in \mathrm{Im}\varphi.$$

□

**Παραδείγματα 3.3.6.** (i) *Η απεικόνιση* $\varphi : \mathbb{Z} \to E_n$ *που είδαμε στο παράδειγμα 3.3.2(iii) έχει* $\mathrm{Ker}\varphi =< n >= n\mathbb{Z}$. *Πράγματι,*

$$z^a = 1 \Leftrightarrow |z| \mid a \Leftrightarrow n|a.$$

(ii) *Η απεικόνιση* $\varphi : \mathbb{R} \to \mathbb{C} \setminus \{0\}$,

$$\varphi(a) = \cos(2\pi a) + i\sin(2\pi a)$$

*είναι ομομορφισμός ομάδων. Έχουμε,*

$$\mathrm{Im}\varphi = E = \{z \in \mathbb{C} : |z| = 1\},$$

*όπου* $|z|$ *το μέτρο του* $z \in \mathbb{C}$. *Γεωμετρικά η* $\varphi$ *επιμηκύνει τον άξονα* $\mathbb{R}$ *κατά* $2\pi$ *και τον τυλίγει γύρω από τον κύκλο.*

(iii) *Έστω* $\varphi : \mathbb{Z}_{24} \to S_5$, $\varphi([a]) = \sigma^a$, *όπου* $\sigma = (1\ 3)(2\ 4\ 5)$. *Η* $\varphi$ *είναι καλώς ορισμένη, ομομορφισμός ομάδων και* $\mathrm{Ker}\varphi =< [\sigma] >$. *Επίσης* $\mathrm{Im}\varphi =< \sigma >$.

*Πράγματι, παρατηρήστε ότι* $|\sigma| = \epsilon\kappa\pi(2,3) = 6$ *((*1 3)(2 4 5) *είναι γινόμενο ξένων κύκλων). Έστω* $[a] = [b]$. *Τότε,*

$$24 \mid a - b \Rightarrow 6 \mid a - b \Rightarrow \sigma^a = \sigma^b.$$

*Η* $\varphi$ *είναι ομομορφισμός ομάδων (είναι σαφές ότι* $\sigma^{a+b} = \sigma \cdot \sigma^b$*). Επίσης,*

$$\mathrm{Ker}\varphi = \{[a] \in \mathbb{Z}_{24} : \sigma^a = 1\} = \{[a] \in \mathbb{Z}_{24} : |\sigma| \mid a\} = \{[a] \in \mathbb{Z}_{24} : \sigma \mid a\} =< [b] >$$

*και*

$$\mathrm{Im}\varphi = \{\sigma^a : [a] \in \mathbb{Z}_{24}\} = \{\sigma^a : a \in \mathbb{Z}\} =< \sigma > .$$

□

**Ορισμός 3.3.7.** *Έστω* $(G_1, *)$, $(G_2, \circledast)$ *δύο ομάδες. Στο σύνολο* $G_1 \times G_2$ *(καρτεσιανό γινόμενο συνόλων) θεωρούμε την πράξη που ορίζεται ως εξής.*

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 * g_1 \circledast g_2').$$

*Το* $(G_1 \times G_2, \cdot)$ *είναι ομάδα που λέγεται το εξωτερικό ευθύ γινόμενο των* $G_1, G_2$.

**Παρατήρηση 3.3.8.** $1_{G_1 \times G_2} = (1_{G_1}, 1_{G_2})$, $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$.

**Θεώρημα 3.3.9.** *(Cayley) Έστω* $G$ *μια πεπερασμένη ομάδα. Τότε η* $G$ *είναι ισόμορφη με μια υποομάδα κάποιας* $S_n$.

*Απόδειξη.* Έστω $g \in G$. Θεωρούμε την απεικόνιση $L_g : G \to G$, με $L_g(a) = ga$ για κάθε $a \in G$. Θα δείξουμε ότι η $L_g$ είναι 1-1 και επί. Πράγματι, αν $L_g(a) = L_g(a')$ τότε,

$$ga = ga' \Rightarrow a = a'.$$

Αφού η $L_g : G \to G$ είναι 1-1 και $|G| < \infty$, έπεται ότι η $G$ είναι επί. (Επίσης η $G$ είναι επί αφού αν $a \in G$ τότε, $L_g(g^{-1}a) = g(g^{-1}a) = a$.) Άρα η $L_g$ είναι μια μετάθεση του συνόλου $G$, δηλαδή $L_g \in S(G) = S_n =$ το σύνολο των μεταθέσεων του συνόλου $G$. Ορίζουμε τώρα την απεικόνιση

$$\varphi : G \to S(G), \;\; \varphi(g) = L_g.$$

Η $\varphi$ είναι μονομορφισμός ομάδων (η $S(G)$ είναι ομάδα με πράξη την σύνθεση). Πράγματι, $\varphi(g_1g_2) = L_{g_1g_2}$ και $\varphi(g_1)\varphi(g_2) = L_{g_1}L_{g_2}$. Παρατηρήστε ότι,

$$L_{g_1}L_{g_2}(a) = L_{g_1}(g_2a) = g_1(g_2a) = (g_1g_2)a = L_{g_1g_2}(a).$$

Επίσης έχουμε $\mathrm{Ker}\varphi = \{g \in G : L_g = 1_{S(G)}\}$. Παρατηρήστε ότι,

$$L_g = 1_{S(G)} \Leftrightarrow L_g(a) = 1_{S(G)}(a) \;\text{ για κάθε }\; a \in G \Leftrightarrow ga = a \Leftrightarrow g = 1_G.$$

Επομένως, $\mathrm{Ker}\varphi = \{1_G\}$. □

**Παράδειγμα 3.3.10.** *Έστω* $G =< g >$, $|G| = 3$. *Δηλαδή* $G = \{1, g, g^2\}$.

$$L_1 = \textit{η ταυτοτική απεικόνιση } G \to G \;\; \begin{pmatrix} 1 & g & g^2 \\ 1 & g & g^2 \end{pmatrix},$$

$$L_g = \begin{pmatrix} 1 & g & g^2 \\ g & g^2 & 1 = g^3 \end{pmatrix},$$

$$L_g^2 = \begin{pmatrix} 1 & g & g^2 \\ g^2 & 1 = g^3 & g = g^4 \end{pmatrix}.$$

$$G \simeq \left\{1, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\} \leq S_3.$$

□

### 3.3α′ Κυκλικές ομάδες

**Θεώρημα 3.3.11.** (i) *Κάθε άπειρη κυκλική ομάδα είναι ισόμορφη με την ομάδα* $\mathbb{Z}$.

(ii) *Κάθε πεπερασμένη κυκλική ομάδα τάξης* $n$ *είναι ισόμορφη με την* $\mathbb{Z}_n$.

*Απόδειξη.* (i). Έστω $G =< a >$ άπειρη κυκλική ομάδα. Θεωρούμε την απεικόνιση

$$\varphi : \mathbb{Z} \to G, \;\; \varphi(\kappa) = a^\kappa.$$

Η $\varphi$ είναι ομομορφισμός ομάδων. Πράγματι,

$$\varphi(\kappa+\kappa') = a^{\kappa+\kappa'} = a^{\kappa}\cdot a^{\kappa'} = \varphi(\kappa)\cdot\varphi(\kappa').$$

Είναι σαφές ότι η $\varphi$ είναι επί. Τέλος η $\varphi$ είναι 1-1. Πράγματι έστω $\kappa \in \mathrm{Ker}\varphi$. Τότε,

$$\varphi(\kappa) = 1_G \Rightarrow a^{\kappa} = 1_G.$$

Επειδή $G =< a >$ έχουμε $\kappa = 0$. Επομένως $\mathrm{Ker}\varphi = \{0\}$.

(ii). Έστω $G =< a >$ πεπερασμένη κυκλική ομάδα τάξης $n$. Θεωρούμε την απεικόνιση

$$\varphi : \mathbb{Z}_n \to G,\ \ \varphi([\kappa]) = a^{\kappa}.$$

Η $\varphi$ είναι καλώς ορισμένη. Πράγματι, αν $[\kappa] = [\kappa']$ τότε $a^{\kappa} = a^{\kappa'}$ αφού $a^n = 1_G$. Η $\varphi$ είναι ομομορφισμός ομάδων, αφού

$$\varphi([\kappa]+[\kappa']) = a^{\kappa+\kappa'} = a^{\kappa}\cdot a^{\kappa'} = \varphi([\kappa])\cdot\varphi([\kappa']).$$

Είναι σαφές ότι η $\varphi$ είναι επί. Επίσης η $\varphi$ είναι 1-1. Πράγματι,

$$[\kappa] \in \mathrm{Ker}\varphi \Leftrightarrow a^{\kappa} = 1_G \Leftrightarrow n \mid \kappa \ \text{ αφού } \ |a| = n.$$

Επομένως $\mathrm{Ker}\varphi = \{[0]\}$, δηλαδή η $\varphi$ είναι 1-1. □

**Πόρισμα 3.3.12.** *Δύο κυκλικές ομάδες είναι ισόμορφες αν και μόνο αν έχουν την ίδια διάταξη.*

**Θεώρημα 3.3.13.** *Κάθε υποομάδα κυκλικής ομάδας είναι κυκλική.*

*Απόδειξη.* Έστω $G$ κυκλική ομάδα και $H \leq G,\ H \neq \{1_G\}$. Τότε υπάρχει $m \in \mathbb{Z}$ ώστε $a^m \in H,\ m \neq 0$. Άρα $a^{-m} \in H$. Επομένως υπάρχει ελάχιστος θετικός ακέραιος, έστω $m$, τέτοιος ώστε $a^m \in H$. Θα δείξουμε ότι $H =< a^m >$. Πράγματι, $< a^m > \subseteq H$ αφού $a^m \in H$ και $H \leq G$. Μένει να δείξουμε ότι $H \subseteq < a^m >$. Έστω $a^{\kappa} \in H$. Από τον αλγόριθμο της ευκλείδειας διαίρεσης υπάρχουν $q, r \in \mathbb{N}$ ώστε

$$\kappa = qm + r,\ \ 0 \leqslant r < m.$$

Επομένως,

$$a^r = a^{\kappa}\cdot a^{-qm} = a^{\kappa}(a^m)^{-q} \in < a^m > .$$

Από το ελάχιστο στον ορισμό του $m$, έπεται $r = 0$. Δηλαδή, $\kappa = qm$ και $a^{\kappa} = (a^m)^q \in < a^m >$, αφού $a^{\kappa} \in < a^m >$. □

**Θεώρημα 3.3.14.** *Για κάθε διαιρέτη $m$ της τάξης μιας πεπερασμένης κυκλικής ομάδας $G$, υπάρχει μοναδική $H \leq G$ με $|H| = m$.*

*Απόδειξη.* Έστω $G =< a >$ πεπερασμένη κυκλική ομάδα, $|G| = n$ και $m|n$. Θα δείξουμε ότι υπάρχει $H \leq G$, με $|H| = m$. Θεωρούμε $H =< a^{n/m} >$. Από τον ορισμό της τάξης ($|a| = n$) έχουμε,

$$|a^{n/m}| = \frac{n}{\text{μκδ}(n, \frac{n}{m})} = \frac{n}{\frac{n}{m}} = m.$$

Επομένως $|H| = m$. Έστω τώρα $K \leq G$, με $|K| = m$. Θα δείξουμε ότι $K =< a^{n/m} >$. Από το θεώρημα 3.3.13, η $K$ είναι κυκλική, δηλαδή $K =< a^{\kappa} >$, για κάποιο $\kappa \in \mathbb{Z}$. Παρατηρήστε ότι $|K| = m$, άρα

$$(a^{\kappa})^m = 1 \Rightarrow a^{\kappa m} = 1 \Rightarrow n \mid \kappa m \Rightarrow \frac{n}{m} \mid \kappa \Rightarrow a^{\kappa} \in < a^{n/m} > .$$

Επομένως $K \subseteq < a^{n/m} >$ και επειδή $|K| = | < a^{n/m} >= m < \infty$, έπεται $K =< a^{n/m} >$. □

### Διάγραμμα υποομάδων μιας ομάδας $G$

Το διάγραμμα υποομάδων της $G$ ορίζεται ως εξής.

• Κορυφές είναι οι υποομάδες της $G$.

• Δύο $H, K \leq G$ συνδέονται με ακμή

$K$ ή $K$ ή $K$

/ | \

$H$ $H$ $H$ αν $H \leq K$ και δεν υπάρχει $L \leq G$ με $H \leq L \leq K$, $L \neq H$, $L \neq K$.

Όταν η $G$ είναι κυκλική τάξης $|G| < \infty$ έχουμε πλήρη εικόνα του διαγράμματος, για παράδειγμα

• αν $G = \mathbb{Z}_{18}$ τότε το διάγραμμα είναι το ακόλουθο.

$G = \mathbb{Z}_{18}$ $\quad 18 = 2 \cdot 3^2$ $\quad (\mathbb{Z}, \mathbb{Z}_n$ κυκλικές ομάδες)

/ \

$< [2] >$ $< [3] >$

\ / \

$< [6] >$ $< [9] >$

\ /

$\{[0]\}$

• Αν $G = \mathbb{Z}_{pq^2}$ όπου $(p, q)$ πρώτοι τότε το διάγραμμα είναι το ακόλουθο.

$G = \mathbb{Z}_{pq^2}$

/ \

$< [p] >$ $< [q] >$

\ / \

$< [pq] >$ $< [q^2] >$

\ /

$\{[0]\}$

• Αν $G = \mathbb{Z}_{p^3}$ όπου $p$ πρώτος τότε το διάγραμμα είναι το ακόλουθο.

$$
\begin{array}{l}
G = \mathbb{Z}_{p^3} \\
\quad\quad | \\
\quad < [p] > \\
\quad\quad | \\
\quad < [p^2] > \\
\quad\quad | \\
\quad\quad \{[0]\}
\end{array}
$$

**Ασκήσεις**

**1**. Έστω $\varphi : G \to H$ ομομορφισμός πεπερασμένων ομάδων.

(i) Να δείξετε ότι για καθε $g \in G$, $|\varphi(g)| \mid |g|$.

(ii) Να δείξετε ότι αν η $\varphi$ είναι επί και η $H$ έχει στοιχείο τάξης $m$, τότε η $G$ έχει στοιχείο τάξης $m$.

(iii) Να δείξετε ότι αν μκδ$(|G|, |H|) = 1$, τότε $\varphi(g) = 1_H$ για κάθε $g \in G$.

(iv) Έστω $G = S_6$ και $H = S_3$. Δείξτε ότι $\sigma \in \mathrm{Ker}\varphi$, όπου $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix}$.

*Απόδειξη.* (i). Έστω $|g| = n$ ($n < \infty$ αφού $|G| < \infty$). Τότε,

$$
\begin{array}{rcl}
g^n & = & 1_G \Rightarrow \varphi(g^n) = \varphi(1_G) = 1_H \Rightarrow \\
\varphi(g)^n & = & 1 \Rightarrow |\varphi(g)| \mid n \Rightarrow |\varphi(g)| \mid |g|.
\end{array}
$$

(ii). Έστω $h \in H$. Αφού η $\varphi$ είναι επί υπάρχει $g \in G$ ώστε $h = \varphi(g)$. Από το ερώτημα (i), έπεται $|h| \mid |g|$. Έστω,

$$
|g| = m \cdot |h|,\ m \in \mathbb{Z}_{>0}. \tag{3.3.1}
$$

Θεωρούμε το $g^m$. Τότε,

$$
|g^m| = \frac{|g|}{\text{μκδ}(|g|, m)} \overset{(3.3.1)}{=} \frac{|g|}{m} \overset{(3.3.1)}{=} |h|.
$$

(iii). Έστω $g \in G$. Τότε από το ερώτημα (i) παίρνουμε $|\varphi(g)| \mid |g|$. Επειδή $|g| \mid |G|$, έπεται

$$
|\varphi(g)| \mid |G|. \tag{3.3.2}
$$

Επίσης ισχύει,

$$
|\varphi(g)| \mid |H|. \tag{3.3.3}
$$

Από τις (3.3.2) και (3.3.3) έπεται,

$$|\varphi(g)| \mid \mu\kappa\delta(|G|, |H|) \Rightarrow |\varphi(g)| \mid 1 \Rightarrow \varphi(g) = 1_H.$$

(iv). Από την ανάλυση της $\sigma$ σε γινόμενο ξένων κύκλων έχουμε $\sigma = (1\ 2\ 3\ 4\ 5)$. Άρα $|\sigma| = 5$. Από το ερώτημα (i) παίρνουμε ότι $|\varphi(\sigma)| \mid 5$. Αλλά,

$$|\varphi(\sigma)| \mid |S_3| \Rightarrow |\varphi(\sigma)| \mid 6.$$

Επομένως,

$$|\varphi(\sigma)| = 1 \Rightarrow \varphi(\sigma) = 1.$$

□

**2**. Έστω $\varphi : \mathbb{Z}_{24} \to \mathbb{Z}_{20},\ \varphi([m]_{24}) = [5m]_{20}$. Να δείξετε τα ακόλουθα.

(i) Η $\varphi$ είναι καλώς ορισμένη.

(ii) Η $\varphi$ είναι ομομορφισμός ομάδων.

(iii) $\mathrm{Ker}\varphi =< [4]_{24} >$.

(iv) $\mathrm{Im}\varphi =< [5]_{20} >$.

*Απόδειξη*. (i). Έστω $[m]_{24} = [m']_{24}$. Τότε,

$$24 \mid m - m' \Rightarrow 4 \mid m - m' \Rightarrow 20 \mid 5(m - m') \Rightarrow [5m]_{20} = [5m']_{20}.$$

(ii). Παρατηρήστε ότι,

$$\begin{aligned} \varphi([a]_{24} + [b]_{24}) &= \varphi([a + b]_{24}) = [5(a + b)]_{20} \\ &= [5a]_{20} + [5b]_{20} \\ &= \varphi([a]_{24}) + \varphi([b]_{24}). \end{aligned}$$

(iii). Ο πυρήνας της $\varphi$ είναι, $\mathrm{Ker}\varphi = \{[a]_{24} : \varphi([a]_{24}) = [0]_{20}\}$. Τότε,

$$\varphi([a]_{24}) = [0]_{20} \Leftrightarrow [5a]_{20} = [0]_{20} \Leftrightarrow 20 \mid 5a \Leftrightarrow 4 \mid a.$$

Επομένως, $[a]_{24} \in < [4]_{24} >$.

(iv). Έχουμε,

$$\mathrm{Im}\varphi = \{[b]_{20} \in \mathbb{Z}_{20} : \exists\ [a]_{24} \in \mathbb{Z}_{24},\ \varphi([a]_{24}) = [b]_{20}\}.$$

Παρατηρήστε ότι,

$$\varphi([a]_{24}) = [5a]_{20}.$$

Άρα, $\mathrm{Im}\varphi =< [5]_{20} >$. □

**3**. Να βρεθούν όλοι οι ομομορφισμοί ομάδων $\mathbb{Z} \to \mathbb{Z}$. Ποιοι από αυτούς είναι

(i) μονομορφισμοί ομάδων;

(ii) επιμορφισμοί ομάδων;

(iii) ισομορφισμοί ομάδων;

(iv) ομομορφισμοί δακτυλίων;

*Λύση.* Έστω $\varphi : \mathbb{Z} \to \mathbb{Z}$ ομομορφισμός ομάδων. Τότε,

$$\varphi(m) = \varphi(1 + \cdots + 1) = \varphi(1) + \cdots + \varphi(1) = m\varphi(1),$$

για κάθε $m \geqslant 0$. Επίσης, $\varphi(m) = m\varphi(1)$, για κάθε $m \leqslant 0$. Επομένως,

$$\varphi(m) = m\varphi(1),$$

για κάθε $m \in \mathbb{Z}$. Άρα αν $\varphi : \mathbb{Z} \to \mathbb{Z}$ ομομορφισμός ομάδων υπάρχει $a \in \mathbb{Z}$ ώστε $\varphi(m) = ma$. Αντίστροφα, έστω $a \in \mathbb{Z}$. Ορίζουμε,

$$\varphi_a : \mathbb{Z} \to \mathbb{Z}, \;\; \varphi_a(m) = ma.$$

Τότε,

$$\varphi_a(m+n) = (m+n)a = ma + na = \varphi_a(m) + \varphi_a(n).$$

(i).

$$\varphi_a \text{ μονομορφισμός } \Leftrightarrow \; \mathrm{Ker}\varphi_a = \{0\} \; \Leftrightarrow \; a \neq 0.$$

(ii).

$$\varphi_a \text{ επιμορφισμός } \Leftrightarrow \; \mathrm{Im}\varphi_a = \mathbb{Z} \; \Leftrightarrow \; < a >= \mathbb{Z} \; \Leftrightarrow \; a = 1 \text{ ή } a = -1.$$

(iii).

$$\varphi_a \text{ ισομορφισμός } \Leftrightarrow \; \varphi_a \text{ μονομορφισμός και επιμορφισμός } \Leftrightarrow \; a = 1 \text{ ή } a = -1.$$

(iv). Παρατηρήστε ότι,

$$\varphi_a(1 \cdot 1) = \varphi_a(1)\varphi_a(1) \Leftrightarrow a = a^2 \Leftrightarrow a = 0 \text{ ή } a = 1.$$

Συνεπώς, αν $\varphi_a$ είναι ομομορφισμός δακτυλίων τότε $a = 0$ ή $a = 1$. Αντίστροφα, αν $a = 0$ ή $a = 1$ η $\varphi$ είναι ομομορφισμός δακτυλίων. □

**4**. Έστω $G, H$ πεπερασμένες κυκλικές ομάδες με τάξεις $m, n$ αντίστοιχα.

(i) Δείξτε ότι το πλήθος των ομομορφισμών ομάδων $G \to H$ είναι ίσο με μκδ$(m, n)$.

(ii) Έστω $G = \mathbb{Z}_{24}$ και $H = \mathbb{Z}_{20}$. Βρείτε όλους τους ομομορφισμούς ομάδων $G \to H$.

*Απόδειξη.* (i). Έστω $G =< g >$ και $H =< h >$. Έστω $\varphi : G \to H$ ομομορφισμός ομάδων. Έστω $\varphi(g) = g^a,\ \ 0 \leqslant a < n$. $(H = \{1, h, h^2, \ldots, h^{n-1}\}.)$ Γνωρίζουμε ότι $g^m = 1_G$. Άρα,

$$\varphi(g)^m = \varphi(g^m) = \varphi(1_G) = 1_H,$$

άρα

$$(h^a)^m = 1_H \Rightarrow h^{am} = 1.$$

Επομένως $n \mid am$. Έστω $d = \text{μκδ}(m, n)$. Τότε $\frac{n}{d} \mid a\frac{m}{d}$ $(\frac{n}{d}, \frac{m}{d} \in \mathbb{Z})$. Επειδή οι $\frac{n}{d}, \frac{m}{d}$ είναι σχετικά πρώτοι παίρνουμε $\frac{n}{d} \mid a$. Άρα,

$$a = \frac{n}{d} \cdot i,\ \ i = 0, 1, 2, \ldots, (d-1). \tag{3.3.4}$$

Για κάθε $i = 0, 1, 2, \ldots, (d-1)$ ορίζουμε την απεικόνιση

$$\varphi_i(g^\kappa) = h^{\frac{n}{d}i\kappa},\ \ (\kappa \in \mathbb{Z}).$$

• Η $\varphi_i$ είναι καλώς ορισμένη. Πράγματι, έστω $g^\kappa = g^{\kappa'}$. Τότε,

$$m \mid \kappa - \kappa' \Rightarrow m\frac{n}{d} \mid \frac{n}{d}i(\kappa - \kappa') \Rightarrow \left(\frac{m}{d}\right) n \mid \frac{n}{d}i(\kappa - \kappa') \Rightarrow n \mid \frac{n}{d}i(\kappa - \kappa').$$

Επομένως,

$$h^{\frac{n}{d}i\kappa} = h^{\frac{n}{d}i\kappa'}.$$

• Εύκολα ελέγχουμε ότι η $\varphi_i$ είναι ομομορφισμός ομάδων.

• $\varphi_i \neq \varphi_j$ για κάθε $i \neq j,\ 0 \leqslant i, j \leqslant d-1$. Πράγματι, έστω $\varphi_i = \varphi_j,\ 0 \leqslant i, j \leqslant d-1$. Τότε,

$$\varphi_i(g) = \varphi_j(g) \Rightarrow h^{n/d \cdot i} = h^{n/d \cdot j} \Rightarrow n \mid \frac{n}{d}(i-j) \Rightarrow i = j,$$

αφού $0 \leqslant i, j \leqslant d-1$.

• Κάθε ομομορφισμός ομάδων $G \to H$ είναι ένας από τους $\varphi_i$. Πράγματι, έστω $\varphi_i : G \to H$ ομομορφισμός ομάδων. Τότε από την (3.3.4), $\varphi = \varphi_i$ για κάποιο $i = 0, 1 \cdots, d-1$, αφού

$$\varphi(g^\kappa) = h^{a\kappa} = h^{n/d \cdot i\kappa}.$$

(ii). Με τον συμβολισμό της λύσης του πρώτου ερωτήματος, έχουμε $m = 24, n = 20, d = \text{μκδ}(24, 20) = 4, \frac{n}{d} = \frac{20}{4} = 5$. Επίσης $i = 0, 1, 2, 3$. Σύμφωνα με την λύση, υπάρχουν ακριβώς 4 ομομορφισμοί ομάδων $\mathbb{Z}_{24} \to \mathbb{Z}_{20}$, οι εξής.

$$\begin{aligned}
\varphi_0 &: \quad \varphi_0([\kappa]_{24}) = [0]_{20} \\
\varphi_1 &: \quad \varphi_1([\kappa]_{24}) = [5\kappa]_{20} \\
\varphi_2 &: \quad \varphi_2([\kappa]_{24}) = [10\kappa]_{20} \\
\varphi_3 &: \quad \varphi_3([\kappa]_{24}) = [15\kappa]_{20}
\end{aligned}$$

*Σημείωση.* Στην άσκηση 2 είχαμε $\varphi = \varphi_1$. □

**5**. Να βρείτε για ποια $n$ υπάρχει

(i) επιμορφισμός ομάδων $G \to S_n$, όπου $S_n$ αβελιανή,

(ii) μονομορφισμός ομάδων $S_n \to G$, όπου $S_n$ αβελιανή.

*Λύση.*

**Παρατήρηση 3.3.15.** *Έστω $\varphi : G \to H$ ομομορφισμός ομάδων.*

*(i) Αν $\varphi$ επί και $G$ αβελιανή, τότε η $H$ είναι αβελιανή.*

*(ii) Αν $\varphi$ 1-1 και $H$ αβελιανή, τότε η ομάδα $\varphi^{-1}(H)(\leq G)$ είναι αβελιανή.*

*Ας δείξουμε το (i). Έστω $h, h' \in H$. Αφού η $G$ είναι επί, υπάρχουν $g, g' \in G$ με $h = \varphi(g),\ h' = \varphi(g')$. Επομένως,*

$$hh' = \varphi(g)\varphi(g') = \varphi(gg') = \varphi(g')\varphi(g) = h'h.$$

*Επομένως η $H$ είναι αβελιανή.*

(i). Από την παρατήρηση 3.3.15(i), αν $\varphi : G \to S_n$ επιμορφισμός και $G$ αβελιανή τότε $S_n$ αβελιανή. Άρα $n = 1, 2$.

(ii). Από την παρατήρηση 3.3.15(ii) η $S_n = \varphi^{-1}(G)$ είναι αβελιανή, άρα $n = 1, 2$. □

**6**. Δείξτε ότι η ομάδα $G = \{2^m \cdot 3^n \in \mathbb{Q} : m, n \in \mathbb{Z}\}$ με πράξη τον πολλαπλασιασμό είναι ισόμορφη με την ομάδα $\mathbb{Z} \times \mathbb{Z}$.

*Απόδειξη.* Θεωρούμε την απεικόνιση,

$$\varphi : G \to \mathbb{Z} \times \mathbb{Z},\ \ \varphi(2^m \cdot 3^n) = (m, n).$$

Η $\varphi$ είναι καλώς ορισμένη. Πράγματι, έστω

$$2^m \cdot 3^n = 2^{m'} \cdot 3^{n'} \Rightarrow m = m',\ n = n' \Rightarrow (m, n) = (m', n').$$

Η $\varphi$ είναι ομομορφισμός ομάδων. Πράγματι,

$$\begin{aligned} \varphi(2^m 3^n \cdot 2^{m'} 3^{n'}) &= \varphi(2^{m+m'} 3^{n+n'}) = (m + m', n + n') \\ &= (m, n) + (m', n') = \varphi(2^m 3^n)\varphi(2^{m'} 3^{n'}). \end{aligned}$$

Είναι σαφές ότι η $\varphi$ είναι επί. Τέλος η $\varphi$ είναι 1-1. Πράγματι,

$$\mathrm{Ker}\varphi = \{2^m 3^n : (m, n) = (0, 0)\} = \{1\}.$$

Άρα $G \simeq \mathbb{Z} \times \mathbb{Z}$. □

**7**. Να δείξετε ότι η $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z},\ \varphi(x, y) = 28x + 49y$ είναι ομομορφισμός ομάδων. Ποια είναι η $\mathrm{Im}\varphi$;

*Απόδειξη.* Παρατηρήστε ότι,

$$\begin{aligned} \varphi\left((x, y) + (x', y')\right) &= \varphi(x + x', y + y') \\ &= 28(x + x') + 49(y + y') \\ &= (28x + 49y) + (28x' + 49y') \\ &= \varphi(x, y) + \varphi(x', y'). \end{aligned}$$

$$\mathrm{Im}\varphi = \{28x + 49y : x, y \in \mathbb{Z}\} =< d >, \tag{3.3.5}$$

όπου $d = \mu\kappa\delta(28, 49) = 7$. Δηλαδή, $\mathrm{Im}\varphi =< 7 >= 7\mathbb{Z}$.

*Σημείωση.* Η δεύτερη ισότητα στην (3.3.5) μας είναι γνωστή από την απόδειξη του θεωρήματος για τον μκδ. Διαφορετικά,

$$\{28x + 49y : x, y \in \mathbb{Z}\} \supseteq < d >,$$

αφού υπάρχουν $a, b$ ώστε $d = 28a + 49b$ και

$$\{28x + 49y : x, y \in \mathbb{Z}\} \subseteq < d >,$$

αφού $7 \mid 28$ και $7 \mid 49$. □

**8**. Έστω $G =< a >$ κυκλική τάξης 36 και $H =< a^{32} >$.

(i) Ποια είναι η τάξη της $m$;

(ii) Να βρείτε όλα τα $g \in G$ ώστε $< g >= H$

*Λύση.* (i). Παρατηρήστε ότι,

$$|H| = |a^{32}| = \frac{|a|}{\mu\kappa\delta(|a|, 32)} = \frac{36}{\mu\kappa\delta(36, 32)} = \frac{36}{4} = 9.$$

(ii). Παρατηρήστε ότι,

$$< g >= H \Leftrightarrow |g| = H \Leftrightarrow |g| = 9.$$

Το $(\Rightarrow)$ στην πρώτη συνεπαγωγή είναι άμεσο, ενώ το $(\Leftarrow)$ έπεται από το θεώρημα 3.3.14. Έχουμε $g = a^{\kappa},\ \kappa \in \mathbb{Z}$, άρα

$$|g| = 9 \Leftrightarrow |a^{\kappa}| = 9 \Leftrightarrow \frac{36}{\mu\kappa\delta(36, \kappa)} = 9 \Leftrightarrow \mu\kappa\delta(36, \kappa) = 4 \Leftrightarrow \kappa = 4n,$$

όπου $\mu\kappa\delta(m, 9) = 1$.

*Σημείωση.* Μπορούμε να υποθέσουμε ότι $\kappa \in \{0, 1, \ldots, 35\}$ και να βρούμε τα $\kappa$ για τα οποία ισχύει $\mu\kappa\delta(m, 9) = 1$. □

**9**. Έστω $G$ μια πεπερασμένη ομάδα κυκλική ομάδα και έστω $H, K \leq G$. Πόσα στοιχεία έχει η ομάδα $H \cap K$;

*Λύση.* Θα δείξουμε ότι $|H \cap K| = d$, όπου $d = \mu\kappa\delta(|H|, |K|)$. Αν $m \mid n$, τότε υπάρχει μοναδική υποομάδα $H_m \leq G$ με $|H_m| = m$ (θεώρημα 3.3.14). Παρατηρήστε ότι $H \cap K \leq H$, οπότε από το θεώρημα Lagrange $|H \cap K| \mid |H|$. Ομοίως επειδή $H \cap K \leq K$, έπεται $|H \cap K| \mid |K|$. Επομένως,

$$|H \cap K| \mid \mu\kappa\delta(|H|, |K|).$$

Επομένως, $H \cap K \leq H_d$, όπου $d = \mu\kappa\delta(m, n)$. Επειδή $d \mid |H|$ έχουμε $H_d \subseteq H$. Ομοίως $H_d \subseteq K$. Επομένως $H_d \in H \cap K$. Τελικά $H \cap K = H_d$.

**10**. Έστω $G$ κυκλική ομάδα τάξης 100, $G =< a >$

(i) Αληθεύει ότι $< a^{28} >=< a^{36} >$;

(ii) Να βρείτε έναν γεννήτορα της ομάδας $< a^{22} > \cap < a^{55} >$.

*Λύση.* (i). Αφού $G$ κυκλική από το θεώρημα 3.3.14 έχουμε ότι,

$$\begin{aligned} < a^{28} > &= < a^{36} > \Leftrightarrow | < a^{28} > | = | < a^{36} > | \Leftrightarrow \\ \frac{100}{\mu\kappa\delta(100, 28)} &= \frac{100}{\mu\kappa\delta(100, 36)} \Leftrightarrow 25 = 25. \end{aligned}$$

Άρα αληθεύει ότι $< a^{28} >=< a^{36} >$.

(ii). Από την άσκηση 9 παίρνουμε,

$$| < a^{22} > \cap < a^{55} > | = \mu\kappa\delta(| < a^{22} |, | < a^{55} > |).$$

Όμως,

$$| < a^{22} > | = \frac{100}{\mu\kappa\delta(100, 22)} = 50 \qquad \text{και} \qquad | < a^{55} > | = \frac{100}{\mu\kappa\delta(100, 55)} = 20.$$

Επομένως,

$$| < a^{22} > \cap < a^{55} > | = 10.$$

Τότε $< a^{22} > \cap < a^{55} >=< a^{10} >$, αφού

$$| < a^{22} > \cap < a^{55} > | = 10 = | < a^{10} > |$$

και η $G$ είναι κυκλική και ισχύει το θεώρημα 3.3.14. □

**11**. Να βρείτε όλες τις υποομάδες της ομάδας

$$G = \left\{ \begin{pmatrix} [1] & [m] \\ [0] & [1] \end{pmatrix} \in GL_2(\mathbb{Z}_{18}), [m] \in \mathbb{Z}_{18} \right\}.$$

*Λύση.* Θεωρούμε την απεικόνιση,

$$\varphi : \mathbb{Z}_{18} \to G, \;\; \varphi([m]) = \begin{pmatrix} [1] & [m] \\ [0] & [1] \end{pmatrix}.$$

Ευκολα δείχνουμε ότι η $\varphi$ είναι ισομορφισμός ομάδων. Επομένως $G \simeq \mathbb{Z}_{18}$ κυκλική τάξης 18. Άρα οι υποομάδες της $G$ είναι οι

$$\left\{ \left\{ \begin{pmatrix} [1] & [m] \\ [0] & [1] \end{pmatrix} \in G : [m] \in H \right\} \text{ όταν } \; H \leq \mathbb{Z}_{18} \right\}.$$

Έχουμε,

$$H = \mathbb{Z}_{18}, \; < [2] >, < [3] >, < [6] >, < [9] >, < [0] > .$$

□

## 3.4 Κανονικές υποομάδες - ομάδα πηλίκο

Γνωρίζουμε ότι το σύνολο $\mathbb{Z}_n = \{[a] : a \in \mathbb{Z}\}$ είναι ομάδα με πράξη την

$$\mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, \; ([a], [b]) \mapsto [a + b]. \tag{3.4.1}$$

Έχουμε,

$$[a] = \{a + \kappa n : \kappa \in \mathbb{Z}\} = a + n\mathbb{Z}.$$

Τότε η πράξη (3.4.1) παίρνει την μορφή

$$(a + n\mathbb{Z}, b + n\mathbb{Z}) \mapsto (a + b) + n\mathbb{Z}.$$

*Επώτηση.* Έστω $G$ ομάδα, $H \leq G$ και $G/H = \{aH : a \in G\}$. Αληθεύει ότι η αντιστοιχία

$$G/H \times G/H \to G/H : \;\; (aH, bH) \mapsto abH \tag{3.4.2}$$

καθιστά το σύνολο $G/H$ ομάδα; Θα δούμε ότι η (3.4.2) δεν είναι γενικά απεικόνιση. Θα εξετάσουμε πότε είναι απεικόνιση.

**Ορισμός 3.4.1.** *Έστω $G$ ομάδα και $S \subseteq G$ (υποσύνολο του $G$) και $a, b \in G$. Θέτουμε,*

$$aSb = \{asb : s \in S\} \subseteq G.$$

**Παρατήρηση 3.4.2.** *Αν $b = 1_G$ και $S \leq G$, τότε έχουμε την (αριστερή) κλαση $aS$.*

**Πρόταση 3.4.3.** *Έστω $H \leq G$. Τα ακόλουθα είναι ισοδύναμα.*

*(i) Η αντιστοιχία (3.4.2) είναι απεικόνιση.*

*(ii) Για κάθε $g \in G$ ισχύει, $g^{-1}Hg \subseteq H$.*

*(iii) Για κάθε $g \in G$ ισχύει, $g^{-1}Hg = H$.*

*(iv) Για κάθε $g \in G$ ισχύει, $gH = Hg$.*

*Απόδειξη.* (i) $\Rightarrow$ (ii). Έστω $a_1H = a_2H$ και $b_1H = b_2H$. Τότε $a_1b_1H = a_2b_2H$. Ισοδύναμα,

$$a_2^{-1}a_1 \in H \text{ και } b_2^{-1}b_1 \in H \Rightarrow b_2^{-1}a_2^{-1}a_1b_1 \in H. \tag{3.4.3}$$

Έστω $g \in G$ και $h \in H$. Θα δείξουμε ότι $g^{-1}hg \in H$. Από την (3.4.3) για $a_2^{-1}a_1 = h$ και $b_1 = b_2 = g$ έχουμε $g^{-1}hg \in H$.

(ii) $\Rightarrow$ (iii). Έστω $g^{-1}Hg \subseteq H$ για κάθε $g \in G$. Τότε για $g^{-1}$ στην θέση του $g$ παίρνουμε,

$$(g^{-1})^{-1}Hg^{-1} \subseteq H \Rightarrow gHg^{-1} \subseteq H \Rightarrow gH \subseteq Hg \Rightarrow H \subseteq g^{-1}Hg.$$

Επομένως $g^{-1}Hg = H$.

(iii) $\Rightarrow$ (iv). Έπεται άμεσα.

(iv) $\Rightarrow$ (i). Επειδή $a_2^{-1}a_1 \in H$ και $gH = Hg$ για κάθε $g \in G$, υπάρχει $h \in H$ ώστε

$$b_2^{-1}(a_2^{-1}a_1) = h \cdot b_2^{-1}.$$

Επομένως,

$$b_2^{-1}a_2^{-1}a_1b_1 = hb_2^{-1} \cdot b_1 \in H,$$

αφού $h \in H$, $b_2^{-1}b_1 \in H$ και $H \leq G$. Επομένως ισχύει η (3.4.3), άρα η (3.4.2) είναι πράγματι απεικόνιση. □

*Σημείωση.* Η σχέση $gH = Hg$ δεν σημαίνει αναγκαστικά ότι $gh = hg$ για κάθε $g \in G$ και για κάθε $h \in H$. Το σωστό είναι ότι για κάθε $g \in G$ και για κάθε $h \in H$ υπάρχει $h' \in H$ ώστε $gh = h'g$.

**Ορισμός 3.4.4.** *Έστω $G$ ομάδα και $H \leq G$. Η $H$ λέγεται κανονική υποομάδα της $G$ (συμβολίζουμε με $H \trianglelefteq G$) αν αληθεύει μία (και άρα όλες) από τις συνθήκες της πρότασης 3.4.3.*

**Παραδείγματα 3.4.5.** *1. Αν η $G$ είναι αβελιανή, τότε κάθε $H \leq G$ είναι κανονική.*

*2. Έστω $\varphi : G \to H$ ομομορφισμός ομάδων. Τότε* $\mathrm{Ker}\varphi \trianglelefteq G$.

*Πράγματι, έστω $g \in G$ και $h \in \mathrm{Ker}\varphi$. Θα δείξουμε ότι $g^{-1}hg \in \mathrm{Ker}\varphi$. Παρατρήστε ότι,*

$$\begin{aligned} \varphi(g^{-1}hg) &= \varphi(g^{-1})\varphi(h)\varphi(g) = \varphi(g^{-1})1_H\varphi(g) \\ &= \varphi(g^{-1})\varphi(g) = \varphi(g)^{-1}\varphi(g) = 1_H. \end{aligned}$$

*Άρα $g^{-1}hg \in \mathrm{Ker}\varphi$.*

3. $A_n \trianglelefteq S_n \qquad (A_n = \{\sigma \in A_n : \sigma \ \ \textit{άρτια}\})$.

   *Γνωρίζουμε ότι* $A_n \leq S_n$. *Έστω* $\sigma \in S_n$ *και* $\tau \in A_n$. *Η μετάθεση* $\sigma^{-1}\tau\sigma$ *είναι άρτια αφού οι* $\sigma^{-1}$, $\sigma$ *είναι ή και οι δύο άρτιες ή και οι δύο περιττές. Δηλαδή* $\sigma^{-1}\tau\sigma \in A_n$ *για κάθε* $\sigma \in S_n$ *και για κάθε* $\tau \in A_n$. *Άρα* $A_n \trianglelefteq S_n$.

   *Σημείωση. Το γεγονός ότι* $A_n \trianglelefteq S_n$ *προκύπτει και από το παράδειγμα 2. Πράγματι,* $A_n = \mathrm{Ker}(\mathrm{sign})$, *όπου* $\mathrm{sign} : S_n \to \{-1, 1\}$ *ο ομομορφισμός προσήμου.*

4. *Η υποομάδα* $H = \{1, (1\ 2)\}$ *της* $S_3$ *δεν είναι κανονική.*

   *Αρκεί να δείξουμε ότι* $\sigma^{-1}(1\ 2)\sigma \notin H$ *για κάποιο* $\sigma \in S_3$. *Για παράδειγμα θεωρήστε το* $\sigma = (1\ 3)$. *Τότε,*

$$(1\ 3)^{-1}(1\ 2)(1\ 3) = (1\ 3)(1\ 2)(1\ 3) = (2\ 3) \notin H.$$

5. *Η υποομάδα* $H =< \sigma >$ *της* $S_4$, *όπου* $\sigma = (1\ 2\ 3\ 4)$ *δεν είναι κανονική.*

   *Αρκεί να δείξουμε ότι* $g^{-1}\tau g \notin H$ *για κάποιο* $g \in S_4$ *και* $\tau \in H$. *Παρατηρήστε ότι για* $g = (1\ 2)$ *και* $\tau = \sigma = (1\ 2\ 3\ 4)$,

$$(1\ 2)^{-1}(1\ 2\ 3\ 4)(1\ 2) = (2\ 1\ 3\ 4).$$

   *Έχουμε*

$$H =< \sigma >= \{1, \sigma, \sigma^2, \sigma^3\}$$

   *αφού η* $\sigma$ *έχει τάξη* 4. *Επίσης,*

$$\begin{aligned} \sigma^2 &= (1\ 2\ 3\ 4)(1\ 2\ 3\ 4) = (1\ 3)(2\ 4) \\ \sigma^2 &= \sigma^{-1} = (4\ 3\ 2\ 1) \end{aligned}$$

   *Επομένως* $(2\ 1\ 3\ 4) \notin H$, *άρα η* $H$ *δεν είναι κανονική.*

6. *Η υποομάδα* $H = \{\sigma \in S_4 : \sigma(4) = 4\}$ *δεν είναι κανονική.*

   *Έστω* $h \in H$. *Επιλέγουμε* $h \in H$ *με* $h(1) \neq 1$. *Θέτουμε,*

$$\tau = (1\ 4)^{-1}h(1\ 4) = (1\ 4)h(1\ 4).$$

   *Επειδή* $h(4) = 4$ *έπεται* $\tau(4) \neq 4$, *δηλαδή* $\tau \notin H$. *Πράγματι, αν* $\tau(4) = 4$ *τότε* $(1\ 4)(4) = h(1\ 4)(4)$, *δηλαδή* $1 = h(1)$ *το οποίο είναι άτοπο.*

7. *Η υποομάδα* $H = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} : \alpha\delta \neq 0 \right\}$ *της*

$$GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \alpha, \beta, \gamma, \delta \in \mathbb{R},\ \alpha\delta - \beta\gamma \neq 0 \right\}$$

   *δεν είναι κανονική.*

*Πράγματι,*

$$g^{-1}hg = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} \notin H.$$

8. *Η* $SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \alpha\delta - \beta\gamma = 1 \right\}$ *είναι κανονική υποομάδα της* $GL_2(\mathbb{R})$.

   *Πράγματι,* $SL_2(\mathbb{R}) = \mathrm{Ker}\det$, *όπου* $\det : GL_2(\mathbb{R}) \to \mathbb{R} \setminus \{0\}$ *είναι η απεικόνιση της ορίζουσας. Η* det *είναι ομομορφισμός ομάδων και* $\mathrm{Ker}\det = SL_2(\mathbb{R})$. *Από το παράδειγμα 2,* $SL_2(\mathbb{R}) \trianglelefteq GL_2(\mathbb{R})$. □

Έστω $H \trianglelefteq G$. Δείξαμε ότι η

$$G/H \times G/H \to G/H : \quad (aH, bH) \mapsto abH \tag{3.4.4}$$

είναι απεικόνιση. Θα δούμε ότι με αυτήν την πράξη το $G/H$ είναι ομάδα.

**Θεώρημα 3.4.6.** *Έστω* $H \trianglelefteq G$. *Τότε με την πράξη της (3.4.4) το* $G/H$ *είναι ομάδα.*

*Απόδειξη.* Παρατηρήστε ότι,

$$\begin{aligned} (aH)\left((bH)(cH)\right) &= (aH)(bcH) = a(bc)H \\ \left((aH)(bH)\right)(cH) &= (ab)H(cH) = (ab)cH. \end{aligned}$$

Επειδή $a(bc) = (ab)c$, ισχύει η προσεταιριστική ιδιότητα στο $G/H$.

Για κάθε $aH \in G/H$ έχουμε,

$$(aH)(1_G H) = (1_G h)(aH) = aH.$$

(Το μοναδιαίο στοιχείο είναι το $1_G H = H$, αφού $1_G \in H$.)

Τέλος, για κάθε $a \in H$,

$$(aH)(a^{-1}H) = aa^{-1}H = H$$

και

$$(a^{-1}H)(aH) = aa^{-1}H = H.$$

□

**Θεώρημα 3.4.7.** *(Πρώτο θεώρημα ισομορφισμών ομάδων.) Έστω* $\varphi : G \to H$ *ομομορφισμός ομάδων. Τότε η απεικόνιση*

$$\psi : G/\mathrm{Ker}\varphi \to \mathrm{Im}\varphi, \;\; \psi(g\,\mathrm{Ker}\varphi) = \varphi(g)$$

*είναι ισομορφισμός ομάδων.*

*Απόδειξη.* Γνωρίζουμε ότι $\mathrm{Ker}\varphi \trianglelefteq G$. Άρα $G/\mathrm{Ker}\varphi$ είναι ομάδα με πράξη

$$(g_1\mathrm{Ker}\varphi) = (g_2\mathrm{Ker}\varphi).$$

Επίσης $\mathrm{Im}\varphi \trianglelefteq H$.

Η $\psi$ είναι καλώς ορισμένη. Πράγματι,

$$\begin{aligned} g_1\mathrm{Ker}\varphi &= g_2\mathrm{Ker}\varphi \Leftrightarrow \\ g_2^{-1}g_1 &\in \mathrm{Ker}\varphi \Leftrightarrow \\ \varphi(g_2^{-1}g_1) &= 1_H \Leftrightarrow \\ \varphi(g_2)^{-1}\varphi(g_1) &= 1_H \Leftrightarrow \\ \varphi(g_1) &= \varphi(g_2). \end{aligned}$$

Η $\psi$ είναι ομομορφισμός ομάδων. Πράγματι,

$$\begin{aligned} \psi\left((g_1\mathrm{Ker}\varphi)(g_2\mathrm{Ker}\varphi)\right) &= \psi(g_1g_2\mathrm{Ker}\varphi) \\ &= \varphi(g_1g_2) \\ &= \varphi(g_1)\varphi(g_2) \\ &= \psi(g_1\mathrm{Ker}\varphi)\psi(g_1\mathrm{Ker}\varphi). \end{aligned}$$

Η $\psi$ είναι 1-1. Πράγματι, οι συνεπαγωγές στην $\psi$ είναι καλά ορισμένες και αντιστρέφονται. □

**Πόρισμα 3.4.8.** *Έστω $N \trianglelefteq G$. Τότε το $N$ είναι ο πυρήνας κάποιου ομομορφισμού ομάδων $\psi : G \to G'$ (για κάποια ομάδα $G'$).*

*Απόδειξη.* Έστω $\psi : G \to G/N,\ \psi(g) = gN$. Τότε $\psi$ είναι ομομορφισμός ομάδων και $\mathrm{Ker}\psi = N$. □

### Ασκήσεις

1. Να δείξετε ότι η ομάδα $\mathbb{Q}/\mathbb{Z}$ είναι άπειρη και κάθε στοιχείο της έχει πεπερασμένη τάξη.

   *Απόδειξη.* Παρατηρήστε ότι,

   $$a + \mathbb{Z} = b + \mathbb{Z} \Leftrightarrow a - b \in \mathbb{Z}.$$

   Για παράδειγμα, $\frac{8}{3} + \mathbb{Z} = \frac{2}{3} + \mathbb{Z}$. Τα στοιχεία

   $$\frac{1}{2} + \mathbb{Z}, \frac{1}{2^2} + \mathbb{Z}, \frac{1}{2^3} + \mathbb{Z}, \cdots$$

   είναι ανά δύο διαφορετικά. Άρα το $\mathbb{Q}/\mathbb{Z}$ είναι άπειρο σύνολο.

Έστω $\frac{a}{b}+\mathbb{Z}\in\mathbb{Q}/\mathbb{Z}$, όπου $a,b\in\mathbb{Z},\ b\neq 0$. Τότε,

$$b\left(\frac{a}{b}+\mathbb{Z}\right)=a+\mathbb{Z}=\mathbb{Z}\ \ (=\text{το ταυτοτικό στοιχείο της ομάδας }\ \mathbb{Q}/\mathbb{Z}).$$

Επομένως το $\mathbb{Q}/\mathbb{Z}$ έχει πεπερασμένη τάξη. □

**2**. Έστω $G=<a>$ κυκλική τάξης 12 και $H\leq G,\ |H|=3$.

(i) Να βρείτε την $H$ και να περιγράψετε επακριβώς τα στοιχεία της ομάδας $G/H$.

(ii) Να βρείτε όλους τους $m\in\mathbb{Z}$ ώστε $a^m\in H$.

*Απόδειξη.* (i). Γνωρίζουμε ότι για κάθε διαιρέτη $d\mid|G|$ υπάρχει μοναδική υποομάδα της $G$ τάξης $d$ (γιατί $G$ κυκλική). Άρα,

$$H=<a^4>=\{1,a^4,a^8\}. \tag{3.4.5}$$

Επειδή η $G$ είναι κυκλική, η $G$ είναι αβελιανή. Άρα $H\trianglelefteq G$, επομένως $G/H$ ομάδα. Παρατηρήστε ότι,

$$|G/H|=\frac{|G|}{|H|}=\frac{12}{3}=4.$$

Θα δείξουμε ότι,

$$G/H=\{H,aH,a^2H,a^3H\}.$$

Πράγματι, τα στοιχεία $H,aH,a^2H,a^3H$ είναι ανά δυό διαφορετικά (για παράδειγμα, αν $a^2H=a^3H\Rightarrow a^{-3+2}\in H\Rightarrow a^{-1}\in h\Rightarrow a\in H$, άτοπο). Λόγω της (3.4.5) παίρνουμε,

$$\begin{aligned} aH &= \{a,a^5,a^9\},\\ a^2H &= \{a^2,a^6,a^{10}\},\\ a^3H &= \{a^3,a^7,a^{11}\}. \end{aligned}$$

(ii). Παρατηρήστε ότι στην ομάδα $G/H$,

$$a^m\in H\Leftrightarrow a^mH=H\Leftrightarrow(aH)^m=1_{G/H}\Leftrightarrow|aH|\mid m.$$

Αλλά $|aH|=4$ (από τον ορισμό της τάξης στοιχείου το $aH$ είναι ο ελάχιστος θετικός ακέραιος $\kappa$ ώστε $(aH)^\kappa=H\Leftrightarrow a^\kappa\in H$. Δηλαδή $\kappa=4$, αφού $H=\{1,a^4,a^8\}$. Επομένως,

$$|aH|\mid m\Leftrightarrow 4\mid m.$$

□

**3**. Έστω $H \leq Z(G)$, όπου $G$ ομάδα και $Z(G) = \{a \in G : ag = ga \ \text{ για κάθε } \ g \in G\}$ το κέντρο της ομάδας της $G$. Τότε $H \trianglelefteq G$.

*Απόδειξη.* $Z(G) \leq G$. Αφού $H \leq Z(G)$, έπεται $H \leq G$. Έστω $g \in G$ και $h \in H$. Τότε,

$$g^{-1}hg = hg^{-1}g = h \in H \ \ (\text{αφού } \ g^{-1}h = hg^{-1}).$$

Άρα $H \trianglelefteq G$. □

**4**. Έστω $H \leq Z(G)$. Αν $G/H$ κυκλική, τότε $G$ αβελιανή.

*Απόδειξη.* Από την άσκηση 3, $H \trianglelefteq G$, άρα η $G/H$ είναι ομάδα. Έστω $G/H =< aH >$. Έστω $g_1, g_2 \in G$. Θα δείξουμε ότι $g_1g_2 = g_2g_1$ (δηλαδή $G$ αβελιανή). Παρατηρήστε ότι, $g_1H \in G/H$, άρα $g_1H = a^mH$ για κάποιο $m \in \mathbb{Z}_{>0}$. Επομένως,

$$g_1 \in g_1H = a^mH \qquad \text{και} \qquad g_1 = a^mh_1,$$

για κάποιο $h_1 \in H$. Ομοίως $g_2 = a^nh_2$, για κάποιο $h_2 \in H$. Τότε,

$$g_1g_2 = a^mh_1a^nh_2 \overset{H \leq Z(G)}{=} a^ma^nh_1h_2 = a^{m+n}h_1h_2.$$

Ομοίως,

$$g_2g_1 = a^nh_2a^mh_1 = a^{m+n}h_1h_2.$$

Άρα $g_1g_2 = g_2g_1$. □

**5**. Έστω $|G| = 210, \ N \trianglelefteq G, \ |N| = 7$.

(i) Να δείξετε ότι $g^{30} \in N$ για κάθε $g \in G$.

(i) Να δείξετε ότι αν $g^7 \in N$, τότε $g \in N$.

*Απόδειξη.* (i). Αφού $N \trianglelefteq G$, η $G/N$ είναι ομάδα (με την συνήθη πράξη). Επίσης,

$$|G/N| = \frac{|G|}{|N|} = \frac{210}{7} = 30. \tag{3.4.6}$$

Επομένως για κάθε $g \in G$,

$$(gN)^{30} = 1_{G/N} \Rightarrow g^{30}N = N \Rightarrow g^{30} \in N.$$

(ii). Παρατηρήστε ότι,

$$g^7 \in N \Rightarrow g^7N = N \Rightarrow (gN)^7 = N = 1_{G/N}.$$

Επομένως στην ομάδα $G/N$, $|gN| \mid 7$. Λόγω της (3.4.6) έπεται $|gN| \mid 30$. Αφού $\mu\kappa\delta(7, 30) = 1$,

$$|gN| = 1 \Rightarrow gN = 1_{G/N} = N \Rightarrow g \in N.$$

□

**6**. Έστω $H \trianglelefteq G,\ K \trianglelefteq G$.

(i) Να δείξετε ότι $H \cap K \trianglelefteq G$.

(ii) Αν $H \cap K = \{1\}$, να δείξετε ότι $h\kappa = \kappa h$ για κάθε $h \in H$ και για κάθε $\kappa \in K$.

*Απόδειξη.* (i). Έχουμε $H \leq G$ και $K \leq G$. Τότε $H \cap K \leq G$. Έστω $a \in H \cap K$ και $g \in G$. Τότε $a \in H$ και αφού $H \trianglelefteq G$, παίρνουμε

$$g^{-1}ag \in H.$$

Ομοίως,

$$g^{-1}ag \in K,$$

άρα

$$g^{-1}ag \in H \cap K.$$

Δηλαδή, $H \cap K \trianglelefteq G$.

(ii). Έστω $h \in H$ και $\kappa \in K$. Τότε $\kappa^{-1}h\kappa \in H$, αφού $H \trianglelefteq G \ \ (\kappa \in K)$. Άρα, $h^{-1}(\kappa^{-1}h\kappa) \in H$, αφού $H \leq G$. Ομοίως, $h^{-1}\kappa^{-1}h\kappa \in K$ (αφού $h^{-1}\kappa^{-1}h \in K$). Επομένως,

$$h^{-1}\kappa^{-1}h\kappa \in H \cap K = \{1\} \Rightarrow h^{-1}\kappa^{-1}h\kappa = 1 \Rightarrow h\kappa = \kappa h.$$

□

**7**. (Θεώρημα Cayley για αβελιανές ομάδες.) Έστω $G$ πεπερασμένη αβελιανή ομάδα και $p \mid |G|$, όπου $p$ πρώτος. Τότε υπάρχει $g \in G$ ώστε $|g| = p$.

*Σημείωση.* Το συμπέρασμα της άσκησης ισχύει και χωρίς την υπόθεση ότι η $G$ είναι αβελιανή.

*Απόδειξη.* Η απόδειξη θα γίνει με επαγωγή στην $|G|$. Έστω ότι το θεώρημα ισχύει για κάθε αβελιανή ομάδα με τάξη $< |G|$. Έστω $p$ πρώτος, με $p \mid |G|$. Έστω $a \in G,\ a \neq 1$. Διακρίνουμε τις δύο ακόλουθες περιπτώσεις.

1. Έστω $p \mid |a|$. Τότε το $g = a^{\frac{|a|}{p}}$ έχει τάξη $p$.

2. Έστω $p \nmid |a|$. Θεωρούμε την ομάδα $G/ < a >$ (είναι ομάδα, αφού $G$ αβελιανή). Παρατηρήστε ότι,

$$|G/ < a > | < |G| \ \ (\text{αφού} \ \ a \neq 1).$$

Επίσης η $G/ < a >$ είναι αβελιανή και $p \mid |G/ < a > |$, αφού $p \mid |G|$ και $p \nmid a$. Από την επαγωγική υπόθεση υπάρχει $b < a > \in G/ < a >$ τάξης $p$. Άρα,

$$(b < a >)^p = < a > \ \Rightarrow \ \ b^p \in < a > .$$

Αν $b^p = 1$, τότε το $b \in G$ έχει τάξη $p$. Πράγματι, $|b| = 1$ ή $p$. Αν $|b| = 1$, τότε $b = 1$ και το $b < a > \in G/ < a >$ έχει τάξη 1 (και όχι $p$).

Αν $b^p \neq 1$, τότε το στοιχείο $b^{|a|} \in G$ έχει τάξη $p$. Πράγματι,

$$(b^{|a|})^p = (b^p)^{|a|} = 1, \text{ αφού } b^p \in < a > .$$

Επομένως, $b^{|a|} = 1$ ή $p$. Παρατηρήστε ότι,

• $b < a >$ έχει τάξη $p$ στην $G/ < a >$.

• $p \nmid |a|$.

Επομένως $b^{|a|} \neq 1$, άρα $b^{|a|} = p$. □

**8**. Αληθεύει ότι υπάρχει ομομορφισμός $\varphi : S_5 \to G$ με $\text{Ker}\varphi =< \sigma >$, όπου $\sigma = (2\ 3\ 4\ 5)$;

*Λύση.* Θα δείξουμε ότι η $< \sigma >$ δεν είναι κανονική στην $S_5$. Παρατηρήστε ότι,

$$(1\ 2)^{-1}(2\ 3\ 4\ 5)(1\ 2) = (1\ 3\ 4\ 5) \notin < \sigma >,$$

αφού για παράδειγμα κάθε $\tau \in < \sigma >$ έχει την ιδιότητα $\tau(1) = 1$ (κι εδώ δεν ισχύει) ή αλλιώς $< \sigma >= \{1, \sigma, \sigma^2, \sigma^3\}$, όπου $\sigma^2 = (2\ 4)(3\ 5)$, $\sigma^3 = \sigma^{-1} = (5\ 4\ 3\ 2)$. □

**9**. Έστω $G$ ομάδα και $m \in \mathbb{Z}_{>0}$ ώστε υπάρχει μοναδική $H \leq G$ με $|H| = m$. Τότε $H \trianglelefteq G$.

*Απόδειξη.* Παρατηρήστε ότι αν $g \in G$, τότε $g^{-1}Hg \leq G$ και $|g^{-1}Hg| = |H|$. Πράγματι, $g^{-1}Hg \neq \emptyset$, αφού $H \neq \emptyset$. Έστω $g^{-1}h_1g$, $g^{-1}h_2g \in g^{-1}Hg$. Τότε,

$$g^{-1}h_1gg^{-1}h_2g = g^{-1}(h_1h_2)g \in g^{-1}Hg,$$

αφού $H \leq G$. Επίσης,

$$(g^{-1}h_1g)^{-1} = g^{-1}h_1^{-1}(g^{-1})^{-1} = g^{-1}h_1^{-1}g \in g^{-1}Hg,$$

αφού $H \leq G$. Η απεικόνιση $f : H \to g^{-1}Hg$, $f(h) = g^{-1}hg$ είναι 1-1 και επί. Πράγματι, έστω $f(h_1) = f(h_2)$. Τότε,

$$g^{-1}h_1g = g^{-1}h_2g \Rightarrow h_1 = h_2.$$

Δηλαδή η $f$ είναι 1-1. Από τον ορισμό της $f$ είναι άμεσο ότι είναι επί. Επομένως, αφού $g^{-1}Hg \leq G$ και $|g^{-1}Hg| = |H|$ και από την μοναδικότητα της υπόθεσης έπεται ότι $g^{-1}Hg = H$ για κάθε $g \in G$. Δηλαδή $H \trianglelefteq G$. □

**10**. Να δείξετε ότι υπάρχει ισομορφισμός ομάδων.

(i) $\mathbb{R}/\mathbb{Z} \simeq E$, $E = \{z \in \mathbb{C} : |z| = 1\}$.

(ii) $\mathbb{R}/ < 2\pi > \simeq E$.

*Απόδειξη.* (i). Έχουμε δει ότι η απεικόνιση

$$\varphi : \mathbb{R} \to E, \;\; \varphi(r) = \cos(2\pi r) + i\sin(2\pi r)$$

είναι ομομορφισμός ομάδων. Είναι επί, δηλαδή $\mathrm{Im}\varphi = E$. Παρατηρήστε ότι,

$$\mathrm{Ker}\varphi = \{r \in R : \cos(2\pi r) + i\sin(2\pi r) = 1\} = \mathbb{Z}$$

Από το πρώτο θεώρημα ισομορφισμών ομάδων, έπεται ότι $\mathbb{R}/\mathbb{Z} \simeq E$.

(ii). Ομοίως θεωρώντας την απεικόνιση,

$$\psi : \mathbb{R} \to E, \;\; \psi(r) = \cos r + i\sin r$$

παίρνουμε ότι $\mathbb{R}/ < 2\pi > \simeq E$. □

**11**. Να δείξετε ότι η $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det A = 1\}$ είναι κανονική υποομάδα της $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A \neq 0\}$ και $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R} \setminus \{0\}$.

*Απόδειξη.* Η απεικόνιση $\det : GL_n(\mathbb{R}) \to \mathbb{R} \setminus \{0\}$, $\det A =$ η ορίζουσα του $A$ είναι ομομορφισμός ομάδων αφού $\det AB = (\det A)(\det B)$ και $\mathrm{Ker}det = SL_n(\mathbb{R})$. Άρα $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$ και $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$. Επίσης η απεικόνιση det είναι επί. Πράγματι, αν $a \in \mathbb{R} \setminus \{0\}$ τότε,

$$\det \begin{pmatrix} a & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} = a.$$

Από το πρώτο θεώρημα ισομορφισμών ομαδων παιρνουμε ότι,

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R} \setminus \{0\}.$$

□

**12**. Έστω $m, n \in \mathbb{Z}_{>0}$ . Τότε, $\mathbb{Z}_n/ < [m] > \simeq \mathbb{Z}_m$.

*Απόδειξη.* Πρώτος τρόπος. Θεωρούμε την απεικόνιση $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m, \;\; [a]_n \mapsto [a]_m$. Η $\varphi$ είναι καλώς ορισμένη. Πράγματι, αν

$$[a]_n = [b]_n \Rightarrow n \mid a - b \Rightarrow m \mid a - b \Rightarrow [a]_m = [b]_m.$$

Η $\varphi$ είναι ομομορφισμός ομάδων. Πράγματι,

$$\varphi([a]_n + [b]_n) = \varphi([a + b]_n) = [a + b]_m = [a]_m + [b]_m = \varphi([a]_n) + \varphi([b]_n).$$

Είναι σαφές ότι η $\varphi$ είναι επί. Παρατηρήστε ότι,

$$\text{Ker}\varphi = \{[a]_n : [a]_m = [0]_m\} = \{[a]_n : m \mid a\} =< [m]_n > .$$

Επομένως από το πρώτο θεώρημα ισομορφισμών ομάδων, $\mathbb{Z}_n/ < [m] > \simeq \mathbb{Z}_m$.

Δεύτερος τρόπος. Η $\mathbb{Z}_m$ είναι κυκλική ομάδα.

Ισχυρισμός. Αν $G$ κυκλική και $N \leq G$, τότε $G/N$ κυκλική. Πράγματι, η $G$ είναι αβελιανή άρα $N \trianglelefteq G$. Αν $G =< a >$, τότε $G/N =< aN >$. Πράγματι, αν $g \in G$ τότε $g = a^\kappa$ για κάποιο $\kappa \in \mathbb{Z}$. Άρα,

$$gN = a^\kappa N = (aN)^\kappa.$$

Επομένως από τον ισχυρισμό έπεται ότι η $\mathbb{Z}_n/ < [m] >$ είναι κυκλική. Όμως δύο ομάδες είναι ισόμορφες αν και μόνο αν έχουν την ίδια διάταξη. Επειδή,

$$\left|\frac{\mathbb{Z}_n}{< [m] >}\right| = \frac{\mathbb{Z}_n}{| < [m] > |} = \frac{n}{\frac{n}{m}} = m = \mathbb{Z}_m,$$

το ζητούμενο έπεται. □

**13**. (i) Έστω $\varphi : G \to H$ ομομορφισμός ομάδων και $K \trianglelefteq H$. Τότε το σύνολο $\varphi^{-1}(K) = \{g \in G : \varphi(g) \in K\}$ είναι κανονική υποομαδα της $G$.

(ii) Έστω $\varphi : G \to \mathbb{Z}_n$ επιμορφισμός ομάδων, όπου $G$ πεπερασμένη. Τότε για κάθε θετικό διαιρέτη $d$ του $n$ υπαρχει $N \trianglelefteq G$ με $[G : N] = d$.

*Σημείωση*. Το (ii) ισχύει και για άπειρες $G$.

*Απόδειξη*. (i). Πρώτα θα δείξουμε ότι $\varphi^{-1}(K) \leq G$. Πράγματι, $\varphi^{-1}(K) \neq \emptyset$ ($1_G \in \varphi^{-1}(K)$ αφού $\varphi(1_G) = 1_H \in K$). Έστω $\varphi(a), \varphi(b) \in K$. Τότε,

$$\varphi(a)\varphi(b) \in K \overset{(K \leq H)}{\Rightarrow} \varphi(ab) \in K \Rightarrow ab \in \varphi^{-1}(K).$$

Έστω $a \in \varphi^{-1}(K)$. Τότε,

$$\varphi(a) \in K \overset{(K \leq H)}{\Rightarrow} \varphi(a)^{-1} \in K \Rightarrow \varphi(a^{-1}) \in K \Rightarrow a^{-1} \in \varphi^{-1}(K).$$

Έστω $a \in \varphi^{-1}(K)$. Τότε $\varphi(a) \in K$. Για κάθε $g \in G$ έχουμε,

$$\varphi(g^{-1}ag) = \varphi(g)^{-1}\varphi(a)\varphi(g) \in K,$$

αφού $K \trianglelefteq H$. Άρα $g^{-1}ag \in \varphi^{-1}(K)$, δηλαδή $\varphi^{-1}(K) \trianglelefteq G$.

(ii). Επειδή $\mathbb{Z}_n$ κυκλική και το $\frac{n}{d} \mid n$, υπάρχει $K \leq \mathbb{Z}_n$ ώστε $|K| = \frac{n}{d}$. Έστω $N = \varphi^{-1}(K)$. Από το ερώτημα (i) έχουμε $N \trianglelefteq G$ (αφού $K \trianglelefteq \mathbb{Z}_n$ γιατί $\mathbb{Z}_n$ αβελιανή). Θα δείξουμε ότι $[G : N] = d$. Παρατηρήστε ότι,

$$G/\text{Ker}\varphi \simeq \mathbb{Z}_n,$$

άρα

$$\big|G/\mathrm{Ker}\varphi\big| = n,$$

Δηλαδή, $[G : \mathrm{Ker}\varphi] = n$. Επίσης έχουμε,

$$[G : \mathrm{Ker}\varphi] = [G : N][N : \mathrm{Ker}\varphi]. \tag{3.4.7}$$

Παρατηρήστε ότι οι ομάδες $K$ και $N/\mathrm{Ker}\varphi$ είναι ισόμορφες. Πράγματι, ο περιορισμός της $\psi$ του πρώτου θεωρήματος ισομορφισμών ομάδων δίνει ισομορφισμό $N/\mathrm{Ker}\varphi \simeq K$. Άρα,

$$[N : \mathrm{Ker}\varphi] = |K| = \frac{n}{d}.$$

Τότε από την (3.4.7) παίρνουμε $[G : N] = d$. □

**14**. Έστω $\varphi : G \to H$ ομομορφισμός ομάδων.

(i) Αν η $\varphi$ είναι επί και όχι 1-1 και $|G| = 77$, τότε η $H$ είναι αβελιανή.

(ii) Αν $|G| = 20$, $|H| = 26$, τότε $|\mathrm{Im}\varphi| = 1$ ή 2.

*Απόδειξη*. (i). Από το πρώτο θεώρημα ισομορφισμών ομάδων,

$$G/\mathrm{Ker}\varphi \simeq \mathrm{Im}\varphi = H \ \ (\varphi \ \text{επί}).$$

Η $\varphi$ δεν είναι 1-1, άρα $|\mathrm{Ker}\varphi| > 1$ (ο πυρήνας έχει τουλάχιστον δύο στοιχεία). Επομένως,

$$|G/\mathrm{Ker}\varphi| = 1, 7, 11.$$

Δηλαδή $|H| = 1, 7, 11$, άρα $H$ κυκλική (οι $7, 11$ είναι πρώτοι), οπότε $H$ αβελιανή.

(ii). Παρατηρήστε ότι $\mathrm{Im}\varphi \leq H$, άρα από το θεώρημα Lagrange παίρνουμε,

$$|\mathrm{Im}\varphi| \mid |H| \Rightarrow |\mathrm{Im}\varphi| \mid 26.$$

Επειδή $G/\mathrm{Ker}\varphi \simeq \mathrm{Im}\varphi$ έπεται,

$$|\mathrm{Im}\varphi| \mid |G| \Rightarrow |\mathrm{Im}\varphi| \mid 20.$$

Επομένως $|\mathrm{Im}\varphi| = 1$ ή 2. □

**15**. Αν $G$ ομάδα και $a \in G$, θέτουμε $\varphi_a : G \to G$, $\varphi_a(g) = a^{-1}ga$. Να αποδείξετε τα ακόλουθα.

(i) $\varphi_a$ ισομορφισμός ομάδων.

(ii) Το $\mathrm{Inn}G = \{\varphi_a : a \in G\}$ είναι ομάδα ως προς την σύνθεση απεικονίσεων.

(iii) $G/Z(G) \simeq \mathrm{Inn}G$ $\quad (Z(G) = \{a \in G : ag = ga \ \forall g \in G\})$.

*Απόδειξη.* (i). Παρατηρήστε ότι,

$$\varphi_a(g_1g_2) = a^{-1}(g_1g_2)a = (a^{-1}g_1a)(a^{-1}g_2a) = \varphi_a(g_1)\varphi_a(g_2),$$

δηλαδή η $\varphi$ είναι ομομορφισμός ομάδων.

Η $\varphi_a$ είναι 1-1. Πράγματι, έστω $g \in \mathrm{Ker}\varphi_a$. Τότε,

$$a^{-1}ga = 1_G \Rightarrow g = 1_G \Rightarrow \mathrm{Ker}\varphi_a = \{1_G\}.$$

Δηλαδή η $\varphi$ είναι 1-1.

Η $\varphi_a$ είναι επί. Πράγματι, έστω $g' \in G$. Τότε, $\varphi_a(ag'a^{-1}) = g'$.

(ii). $\mathrm{Inn}G \neq \emptyset$. Έστω $\varphi_a, \varphi_b \in \mathrm{Inn}G$. Τότε,

$$\begin{aligned}(\varphi_a \circ \varphi_b)(g) &= \varphi_a(\varphi_b(g)) = \varphi_a(b^{-1}gb)\\ &= a^{-1}b^{-1}gba = (ba)^{-1}gba\\ &= \varphi_{ba}(g)\end{aligned}$$

για κάθε $g \in G$. Επομένως,

$$\varphi_a \circ \varphi_b = \varphi_{ba} \in \mathrm{Inn}(G). \tag{3.4.8}$$

Έστω $\varphi_a \in \mathrm{Inn}(G)$. Τότε, $\varphi_a^{-1} = \varphi_{a^{-1}} \in \mathrm{Inn}G$. Πράγματι, $\varphi_a(\varphi_a^{-1}(g)) = g$ (αφού η $\varphi_a^{-1}$ είναι η αντίστροφη απεικόνιση της $\varphi_a$). Επομένως,

$$\begin{aligned}\varphi_a(\varphi_a^{-1}(g)) &= g \Rightarrow a^{-1}\varphi_a^{-1}(g)a = g \Rightarrow\\ \varphi_a^{-1}(g) &= aga^{-1} = (a^{-1})^{-1}ga^{-1}\\ &= \varphi_{a^{-1}}(g)\end{aligned}$$

για κάθε $g \in G$.

(iii). Θα δείξουμε ότι η απεικόνιση $\psi : G \to \mathrm{Inn}G,\ \ \psi(a) = \varphi_{a^{-1}}$ είναι επιμορφισμός ομάδων με $\mathrm{Ker}\psi = Z(G)$. Παρατηρήστε ότι,

$$\psi(ab) = \varphi_{(ab)^{-1}} = \varphi_{b^{-1}a^{-1}} \overset{(3.4.8)}{=} \varphi_{a^{-1}}\varphi_{b^{-1}} = \psi(a)\psi(b).$$

Η $\psi$ είναι επί ($\psi(a^{-1}) = \varphi_a$). Τέλος εχουμε,

$$\mathrm{Ker}\psi = \{a \in G : \varphi_{a^{-1}} = I_G\},$$

όπου $I_G : G \to G,\ I_G(a) = a$. Παρατηρήστε ότι,

$$\begin{aligned}\varphi_{a^{-1}} &= I_G \Leftrightarrow \varphi_{a^{-1}}(g) = g \ \text{ για κάθε } \ g \in G \Leftrightarrow\\ aga^{-1} &= g \Leftrightarrow a \in Z(G).\end{aligned}$$

Από το πρώτο θεώρημα ισομορφισμών ομάδων έπεται ότι, $G/Z(G) \simeq \mathrm{Inn}G$. □

**16**. Να βρείτε όλους τους $n \in \mathbb{Z}_{>0}$ ώστε $9^n = 1 \mathrm{mod} 14$

*Λύση.* Παρατηρήστε ότι, $[9] \in U(\mathbb{Z}_{14})$ αφού μκδ$(9, 14) = 1$. Υπολογίζουμε την τάξη του $[9] \in U(\mathbb{Z}_{14})$.

$$\begin{aligned} [9]^2 &= [81] = [11] \neq [1] \\ [9]^3 &= [99] = [1] \end{aligned}$$

Άρα $\big|[9]\big| = 3$. Επομένως,

$$g^n = 1 \mathrm{mod} 14 \ (n \in \mathbb{Z}_{>0}) \ \Leftrightarrow \ n \in \mathbb{Z}_{>0} \ \text{πολλαπλάσιο του } 3.$$

(Είδαμε άλλη λύση της άσκησης όταν μιλούσαμε για ισοτιμίες.) □

**17**. Έστω $G$ κυκλική ομάδα τάξης $n^5 - n, \ n > 1$. Να δείξετε ότι υπάρχει $H \leq G$ με $|H| = 30$.

*Απόδειξη.* Επειδή η $G$ είναι κυκλική, αρκεί να δείξουμε ότι $30 \mid |G|$, δηλαδή $30 \mid n^5 - n$. Πράγματι, επειδή $30 = 2 \cdot 3 \cdot 5$ και οι $2, 3, 5$ είναι ανά δύο σχετικά πρώτοι αρκεί να δείξουμε ότι,

$$2 \mid n^5 - n, \ \ 3 \mid n^5 - n, \ \ 5 \mid n^5 - n.$$

Προφανώς $2 \mid n^5 - n$. Εφαρμόζοντας δύο φορές το μικρό θεώρημα του Fermat παίρνουμε την $3 \mid n^5 - n \ \ (n^5 = n^3 n^2 \equiv nn^2 \equiv n^3 \equiv n \mathrm{mod} 3)$. Τέλος από το μικρό θεώρημα του Fermat για $p = 5$ παίρνουμε την $5 \mid n^5 - n$. □

**18**. Να εξετάσετε αν ισχύουν οι ακόλουθες προτάσεις.

(i) Υπάρχει ομάδα $G$ ώστε $G \times \mathbb{Z}_4 \simeq \mathbb{Z}_{40} \times \mathbb{Z}_2$.

(ii) Αν μια ομάδα έχει τουλάχιστον δύο στοιχεία τάξης 2, τότε δεν είναι κυκλική.

(iii) Αν $\varphi : \mathbb{Z}_{10} \to S_4$ είναι ομομορφισμός ομάδων, τότε $\varphi([2]) = 1$

*Απόδειξη.* (i). Έστω ότι υπάρχει τέτοια $G$. Τότε,

$$|G \times \mathbb{Z}_4| = |\mathbb{Z}_{40} \times \mathbb{Z}_2|,$$

δηλαδή $|G| = 20$. Επομένως κάθε στοιχείο της $G \times \mathbb{Z}_4$ έχει τάξη $\leqslant 20$ (αφού $4 \mid 20$). Αλλά το στοιχείο $([1]_{40}, [0]_2) \in \mathbb{Z}_{40} \times \mathbb{Z}_2$ έχει τάξη 40, το οποίο είναι άτοπο, αφού αν $\varphi : H \to K$ ισομορφισμός ομάδων τότε για κάθε $h \in H, \ |h| = |\varphi(h)|$.

(ii). Έστω $a, b \in G \ |a| = |b| = 2, \ a \neq b$. Παρατηρήστε ότι,

$$< a >= \{1, a\}, \ \ < b >= \{1, b\}.$$

Γνωρίζουμε ότι αν $G$ κυκλική πεπερασμένη ομάδα και $d \mid |G|$, τότε υπάρχει μοναδική υποομάδα $H$ με $|H| = d$. Έστω ότι η $G$ είναι κυκλική. Τότε,

$$< a >=< b > \Rightarrow a \in \{1, b\} \Rightarrow a = 1 \ \ \text{ή} \ \ b \Rightarrow a = b$$

(αφού $|a| \neq 1$), άτοπο.

*Σημείωση.* (Παρόμοιο ερώτημα.) Αν η ομάδα $G$ έχει τουλάχιστον 3 στοιχεία τάξης 6, τότε η $G$ δεν είναι κυκλική.

Πράγματι, έστω $G$ κυκλική. Αν το $a \in G$ έχει $|a| = 6$, τότε $| < a > | = 6$ και άρα υπάρχει μοναδική υποομάδα της $G$ τάξης 6. Επομένως η $< a >$ περιέχει τουλάχιστον 3 στοιχεία τάξης 6, το οποίο είναι άτοπο. Πράγματι, $< a >= \{1, a, a^2, a^3, a^4, a^5\}$ με τάξεις $1, 6, 3, 2, 3, 6$. Δηλαδή μόνο δύο στοιχεία έχουν τάξη 6 (για παράδειγμα $|a^4| = \frac{|a|}{\text{μκδ}(|a|,4|)}$).

(iii). Παρατηρήστε ότι,

$$\varphi([2]) \in S_4 \Rightarrow |\varphi([2])| \mid |S_4| \Rightarrow |\varphi([2])| \mid 24.$$

Επίσης $|[2]| = 5$, άρα $|\varphi([2])| \mid 5$. Επειδή $\text{μκδ}(24, 5) = 1$, έπεται $|\varphi([2])| = 1$, δηλαδή $\varphi([2]) = 1$. □