

# Ομομορφισμοί ομάδων και δακτυλίων

Σημειώσεις

Σημειώσεις που συνοδεύουν το βιβλίο «Εισαγωγή στη Θεωρία Κατηγοριών» των εκδόσεων ΔΙΑΥΛΟΣ.

Σεπτέμβριος 2026

## 1 Τρία παραδείγματα με κοινό χαρακτηριστικό

Ξεκινάμε από τρεις ισότητες που έχουμε γράψει αμέτρητες φορές. Η πρώτη είναι ο νόμος των εκθετών,

$$e^{x+y} = e^x e^y.$$

Λέει ότι η εκθετική συνάρτηση μετατρέπει ένα άθροισμα σε γινόμενο.

Για τη δεύτερη ας θυμηθούμε ότι με  $[a]_n$  συμβολίζουμε την κλάση υπολοίπων του ακεραίου  $a$  ως προς  $n$ , δηλαδή το σύνολο των ακεραίων που αφήνουν το ίδιο υπόλοιπο με το  $a$  όταν διαιρεθούν με το  $n$ . Η ισότητα

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

λέει ότι το υπόλοιπο ενός αθροίσματος καθορίζεται από τα υπόλοιπα των προσθετέων. Δηλαδή για να βρούμε το υπόλοιπο του  $a + b$  δεν χρειάζεται να υπολογίσουμε πρώτα το άθροισμα. Αρκεί να προσθέσουμε τα υπόλοιπα των  $a$  και  $b$ .

Η τρίτη είναι ο κανόνας του γινομένου για τις ορίζουσες,

$$\det(AB) = \det A \det B,$$

που ισχύει για κάθε ζεύγος τετραγωνικών μητρώων του ίδιου μεγέθους.

Σε καθεμία από τις τρεις περιπτώσεις έχουμε μια απεικόνιση ανάμεσα σε δύο σύνολα εφοδιασμένα με πράξη. Το σύνολο από το οποίο ξεκινά η απεικόνιση το λέμε **πηγή** και εκείνο στο οποίο καταλήγει **στόχο**. Ας δούμε τι κοινό έχουν οι τρεις περιπτώσεις. Η πράξη δίνει το ίδιο αποτέλεσμα, είτε την υπολογίσουμε πρώτα στην πηγή και μετά απεικονίσουμε, είτε απεικονίσουμε πρώτα και μετά την υπολογίσουμε στον στόχο. Στην πρώτη ισότητα η πρόσθεση των πραγματικών γίνεται πολλαπλασιασμός των θετικών πραγματικών. Στη δεύτερη η πρόσθεση των ακεραίων περνά στην πρόσθεση των κλάσεων υπολοίπων. Στην τρίτη ο πολλαπλασιασμός των μητρώων περνά σε πολλαπλασιασμό αριθμών.

Μια τυχαία απεικόνιση δεν έχει κανέναν λόγο να συμπεριφέρεται έτσι. Για παράδειγμα, η  $x \mapsto x^2$  από τους πραγματικούς στους πραγματικούς δεν διατηρεί την πρόσθεση, αφού  $(1+1)^2 = 4$  ενώ  $1^2 + 1^2 = 2$ . Οι απεικονίσεις που διατηρούν την πράξη λέγονται ομομορφισμοί (*homomorphisms*).

Σκοπός μας σε αυτό το κείμενο είναι να καταλάβουμε τι διατηρεί και τι χάνει ένας ομομορφισμός. Θα ξεκινήσουμε από τις ομάδες, θα φτάσουμε στο πρώτο θεώρημα ισομορφισμού και μετά θα δούμε ότι το ίδιο σχήμα επαναλαμβάνεται στους δακτυλίδες.

## 2 Ομομορφισμοί ομάδων

**Ορισμός 2.1** (Ομομορφισμός ομάδων). Έστω  $(G, *)$  και  $(H, \circ)$  δύο ομάδες. Μια απεικόνιση  $f : G \rightarrow H$  λέγεται **ομομορφισμός ομάδων** αν για κάθε  $x, y \in G$  ισχύει

$$f(x * y) = f(x) \circ f(y).$$

Ο ορισμός λέει το εξής με λόγια. Το γινόμενο  $x * y$  υπολογίζεται στην  $G$  και το γινόμενο  $f(x) \circ f(y)$  στην  $H$ , και ο  $f$  είναι ομομορφισμός όταν οι δύο υπολογισμοί καταλήγουν στο ίδιο στοιχείο. Από εδώ και πέρα γράφουμε τις πράξεις πολλαπλασιαστικά, οπότε η συνθήκη γίνεται  $f(xy) = f(x)f(y)$ . Το γινόμενο του αριστερού μέλους υπολογίζεται στην  $G$  και το γινόμενο του δεξιού στην  $H$ .

Ας ελέγξουμε ότι οι τρεις ισότητες της πρώτης ενότητας είναι πράγματι ομομορφισμοί ομάδων. Με  $\mathbb{R}^\times$  συμβολίζουμε την ομάδα των μη μηδενικών πραγματικών ως προς τον πολλαπλασιασμό και με  $GL_n(\mathbb{R})$  την ομάδα των αντιστρέψιμων  $n \times n$  μητρών ως προς τον πολλαπλασιασμό μητρών.

- (i) Η εκθετική απεικόνιση  $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \cdot)$  είναι ομομορφισμός, αφού  $e^{x+y} = e^x e^y$ .
- (ii) Η αναγωγή  $(\mathbb{Z}, +) \rightarrow (\mathbb{Z}/n\mathbb{Z}, +)$  με  $a \mapsto [a]_n$  είναι ομομορφισμός, αφού  $[a+b]_n = [a]_n + [b]_n$ .
- (iii) Η ορίζουσα  $\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$  είναι ομομορφισμός, αφού  $\det(AB) = \det A \det B$ .

Ας δούμε και πώς φαίνεται ο ορισμός σε ένα διάγραμμα. Αν  $\mu_G$  και  $\mu_H$  είναι οι δύο πράξεις, ο ορισμός λέει ότι το διάγραμμα

$$\begin{array}{ccc} G \times G & \xrightarrow{\mu_G} & G \\ f \times f \downarrow & & \downarrow f \\ H \times H & \xrightarrow{\mu_H} & H \end{array}$$

είναι αντιμεταθετικό. Ας ξεκινήσουμε από ένα ζεύγος  $(x, y)$  στην πάνω αριστερή γωνία. Αν πάμε πρώτα δεξιά και μετά κάτω, παίρνουμε  $f(xy)$ . Αν πάμε πρώτα κάτω και μετά δεξιά, παίρνουμε  $f(x)f(y)$ . Η αντιμεταθετικότητα του διαγράμματος σημαίνει ότι οι δύο δρόμοι καταλήγουν στο ίδιο στοιχείο.

Ο ορισμός ζητά μόνο τη διατήρηση της πράξης. Θα περίμενε κανείς ότι πρέπει να ζητήσουμε και τη διατήρηση του ουδέτερου στοιχείου και των αντιστρώφων. Δεν χρειάζεται όμως, γιατί προκύπτουν μόνα τους, όπως δείχνει η επόμενη πρόταση.

**Πρόταση 2.2** (Πρώτες συνέπειες). Έστω  $f : G \rightarrow H$  ομομορφισμός ομάδων. Τότε

- (i)  $f(e_G) = e_H$ ,
- (ii)  $f(x^{-1}) = f(x)^{-1}$  για κάθε  $x \in G$ ,
- (iii)  $f(x^n) = f(x)^n$  για κάθε  $x \in G$  και κάθε  $n \in \mathbb{Z}$ .<sup>1</sup>

*Απόδειξη.* (i) Ξεκινάμε από το ουδέτερο. Αφού  $e_G e_G = e_G$ , έχουμε

$$f(e_G) = f(e_G e_G) = f(e_G) f(e_G).$$

Πολλαπλασιάζουμε και τα δύο μέλη από αριστερά με  $f(e_G)^{-1}$ , που υπάρχει στην  $H$  επειδή η  $H$  είναι ομάδα. Το αριστερό μέλος γίνεται  $e_H$  και το δεξιό γίνεται  $f(e_G)$ . Άρα  $e_H = f(e_G)$ .

(ii) Έστω  $x \in G$ . Τότε

$$f(x)f(x^{-1}) = f(xx^{-1}) = f(e_G) = e_H,$$

και ομοίως  $f(x^{-1})f(x) = f(x^{-1}x) = e_H$ . Άρα το  $f(x^{-1})$  είναι το αντίστροφο του  $f(x)$  στην  $H$ , δηλαδή  $f(x^{-1}) = f(x)^{-1}$ .

(iii) Θα εξετάσουμε πρώτα την περίπτωση  $n \geq 0$  με επαγωγή στο  $n$ . Για  $n = 0$  το ζητούμενο είναι το (i), αφού  $f(x^0) = f(e_G) = e_H = f(x)^0$ . Αν υποθέσουμε ότι  $f(x^n) = f(x)^n$ , τότε

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

<sup>1</sup>Βλ. Θεώρημα 5.1.2, σ. 141, στο D. S. Malik, J. N. Mordeson και M. K. Sen, *Fundamentals of Abstract Algebra*, McGraw-Hill International Editions, 1997.

Έστω τώρα  $n < 0$  και  $m = -n > 0$ . Τότε  $x^n = (x^m)^{-1}$ , οπότε από το (ii) και από την προηγούμενη περίπτωση έχουμε

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

Έτσι το (iii) ισχύει για κάθε  $n \in \mathbb{Z}$ . □

Ο ομομορφισμός μεταφέρει επίσης τις σχέσεις μεταθετικότητας. Αν  $xy = yx$  στην  $G$ , τότε

$$f(x)f(y) = f(xy) = f(yx) = f(y)f(x).$$

Δηλαδή αν δύο στοιχεία μετατίθενται στην  $G$ , οι εικόνες τους μετατίθενται στην  $H$ . Το αντίστροφο δεν ισχύει γενικά. Αν ο  $f$  στέλνει κάθε στοιχείο στο  $e_H$ , οι εικόνες μετατίθενται πάντοτε, ακόμη και όταν η  $G$  δεν είναι αβελιανή.

Ας δούμε τώρα τι κάνει ο ομομορφισμός με την τάξη ενός στοιχείου. Ας θυμηθούμε πρώτα ότι η **τάξη** (order) ενός στοιχείου  $x$  μιας ομάδας είναι ο μικρότερος θετικός ακέραιος  $m$  με  $x^m = e$ . Αν δεν υπάρχει τέτοιος ακέραιος, λέμε ότι το  $x$  έχει άπειρη τάξη. Για παράδειγμα, το  $[2]_6$  στην προσθετική ομάδα  $\mathbb{Z}/6\mathbb{Z}$  έχει τάξη 3, αφού  $[2]_6 + [2]_6 + [2]_6 = [6]_6 = [0]_6$  ενώ  $[2]_6$  και  $[2]_6 + [2]_6 = [4]_6$  δεν είναι μηδέν.

**Λήμμα 2.3.** Αν το  $h$  έχει τάξη  $d$  και  $h^m = e$  για κάποιο  $m \geq 1$ , τότε το  $d$  διαιρεί το  $m$ .

*Απόδειξη.* Γράφουμε  $m = qd + r$  με  $0 \leq r < d$ . Τότε  $h^r = h^m(h^d)^{-q} = e$ . Επειδή το  $d$  είναι ο μικρότερος θετικός ακέραιος με αυτή την ιδιότητα και  $r < d$ , δεν μπορεί να είναι  $r > 0$ . Άρα  $r = 0$  και  $d \mid m$ . □

**Πρόταση 2.4.** Έστω  $f : G \rightarrow H$  ομομορφισμός ομάδων και  $x \in G$  στοιχείο με πεπερασμένη τάξη  $m$ . Τότε η τάξη του  $f(x)$  διαιρεί το  $m$ .

*Απόδειξη.* Από την Πρόταση 2.2 έχουμε  $f(x)^m = f(x^m) = f(e_G) = e_H$ . Από το Λήμμα 2.3, η τάξη του  $f(x)$  διαιρεί το  $m$ . □

Ας δώσουμε τώρα ονόματα στους ομομορφισμούς ανάλογα με τις ιδιότητες της απεικόνισης.

**Ορισμός 2.5** (Είδη ομομορφισμών). Ένας ομομορφισμός  $f : G \rightarrow H$  λέγεται **μονομορφισμός** αν είναι έρριψη, **επιμορφισμός** αν είναι επίρριψη και **ισομορφισμός** αν είναι αμφίρριψη. Αν  $G = H$ , λέγεται **ενδομορφισμός** (endomorphism), και **αυτομορφισμός** (automorphism) όταν είναι επιπλέον ισομορφισμός.

**Παράδειγμα 2.6** (Περισσότεροι ομομορφισμοί ομάδων). (i) Ο λογάριθμος  $\ln : (\mathbb{R}_{>0}, \cdot) \rightarrow (\mathbb{R}, +)$  είναι ομομορφισμός, αφού  $\ln(ab) = \ln a + \ln b$ . Είναι η αντίστροφη της εκθετικής απεικόνισης της πρώτης ενότητας.

(ii) Στη συμμετρική ομάδα  $S_n$  των μεταθέσεων του  $\{1, \dots, n\}$  το πρόσημο  $\text{sgn}(\sigma)$  είναι 1 όταν η  $\sigma$  γράφεται ως γινόμενο άρτιου πλήθους αντιμεταθέσεων και  $-1$  όταν γράφεται ως γινόμενο περιττού πλήθους. Η ισότητα  $\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$  λέει ότι η  $\text{sgn} : S_n \rightarrow (\{\pm 1\}, \cdot)$  είναι ομομορφισμός.

(iii) Ας συμβολίσουμε με  $S^1$  τον κύκλο των μιγαδικών αριθμών με μέτρο 1, που είναι ομάδα ως προς τον πολλαπλασιασμό. Η  $t \mapsto e^{it}$  από την  $(\mathbb{R}, +)$  στον  $S^1$  είναι ομομορφισμός, γιατί  $e^{i(s+t)} = e^{is}e^{it}$ .

(iv) Για κάθε  $g \in G$  η απεικόνιση  $\mathbb{Z} \rightarrow G$  με  $n \mapsto g^n$  είναι ομομορφισμός. Οι νόμοι των εκθετών  $g^{m+n} = g^m g^n$  είναι ακριβώς η συνθήκη του ομομορφισμού. Αντίστροφα, κάθε ομομορφισμός  $\varphi : \mathbb{Z} \rightarrow G$  είναι αυτής της μορφής, αφού από την Πρόταση 2.2(iii) ισχύει  $\varphi(n) = \varphi(1)^n$ . Ένας ομομορφισμός με πηγή τη  $\mathbb{Z}$  καθορίζεται λοιπόν πλήρως από την τιμή του στο 1.

- (v) Για κάθε  $a \in G$  η απεικόνιση  $g \mapsto aga^{-1}$  είναι ομομορφισμός  $G \rightarrow G$ , γιατί  $agha^{-1} = ag(a^{-1}a)ha^{-1} = (aga^{-1})(aha^{-1})$ . Είναι επιπλέον αμφίρριψη, αφού η απεικόνιση  $g \mapsto a^{-1}ga$  είναι αντίστροφη της. Είναι λοιπόν αυτομορφισμός της  $G$ , και λέγεται **εσωτερικός αυτομορφισμός** (*inner automorphism*).

Ας δούμε και δύο απεικονίσεις που φαίνονται φυσικές αλλά δεν είναι ομομορφισμοί. Τα παραδείγματα αυτά δείχνουν πώς ελέγχουμε στην πράξη μια υποψήφια απεικόνιση.

**Παράδειγμα 2.7** (Απεικονίσεις που δεν είναι ομομορφισμοί). (i) Η  $x \mapsto x + 1$  στην  $(\mathbb{R}, +)$  δεν είναι ομομορφισμός, γιατί το 0 δεν πηγαίνει στο 0. Από την Πρόταση 2.2(i), ο έλεγχος του ουδέτερου είναι ο ταχύτερος τρόπος να απορρίψουμε μια υποψήφια απεικόνιση.

- (ii) Έστω  $f: G \rightarrow G$  με  $f(x) = x^2$ . Τότε  $f(xy) = xyxy$  και  $f(x)f(y) = xxyy$ . Αν πολλαπλασιάσουμε την ισότητα  $xyxy = xxyy$  από αριστερά με  $x^{-1}$  και από δεξιά με  $y^{-1}$ , παίρνουμε  $yx = xy$ . Άρα αν η  $f$  είναι ομομορφισμός, η  $G$  είναι αβελιανή. Αντίστροφα, αν η  $G$  είναι αβελιανή, τότε  $(xy)^2 = xyxy = xxyy = x^2y^2$ . Η  $f$  είναι λοιπόν ομομορφισμός αν και μόνο αν η  $G$  είναι αβελιανή.

### 3 Πυρήνας και εικόνα

Ας πάρουμε ξανά την αναγωγή  $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  με  $a \mapsto [a]_n$ . Τα στοιχεία  $a$  και  $a + n$  έχουν την ίδια εικόνα, και η διαφορά τους είναι πολλαπλάσιο του  $n$ , δηλαδή στοιχείο που πηγαίνει στο  $[0]_n$ . Το ίδιο συμβαίνει με την ορίζουσα. Δύο αντιστρέψιμες μήτρες  $A$  και  $B$  έχουν την ίδια ορίζουσα ακριβώς όταν  $\det(B^{-1}A) = 1$ . Σε κάθε περίπτωση το σύνολο των στοιχείων που πηγαίνουν στο ουδέτερο ελέγχει τότε δύο στοιχεία ταυτίζονται. Το σύνολο αυτό αξίζει ένα όνομα.

**Ορισμός 3.1** (Πυρήνας και εικόνα). Έστω  $f: G \rightarrow H$  ομομορφισμός ομάδων. Ο **πυρήνας** (*kernel*) και η **εικόνα** (*image*) της  $f$  είναι τα σύνολα

$$\ker f = \{x \in G \mid f(x) = e_H\}, \quad \text{Im } f = \{f(x) \mid x \in G\}.$$

Ας δούμε πότε δύο στοιχεία  $x, y \in G$  έχουν την ίδια εικόνα. Από την Πρόταση 2.2 έχουμε

$$f(x) = f(y) \iff f(y)^{-1}f(x) = e_H \iff f(y^{-1}x) = e_H \iff y^{-1}x \in \ker f.$$

Η πρώτη ισοδυναμία προκύπτει αν πολλαπλασιάσουμε με  $f(y)^{-1}$ , η δεύτερη από το ότι  $f(y)^{-1} = f(y^{-1})$  και ο  $f$  είναι ομομορφισμός, και η τρίτη από τον ορισμό του πυρήνα. Η τελευταία συνθήκη λέει ότι  $x = yk$  για κάποιο  $k \in \ker f$ . Τα στοιχεία που έχουν την ίδια εικόνα με το  $y$  είναι λοιπόν ακριβώς τα γινόμενα  $yk$ , όπου το  $y$  μένει σταθερό και το  $k$  διατρέχει τον πυρήνα.

Σύνολα αυτής της μορφής ορίζονται για κάθε υποομάδα και όχι μόνο για πυρήνες, οπότε θα τα μελετήσουμε γενικά. Χρειαζόμαστε δύο έννοιες από τη θεωρία ομάδων και ας τις θυμηθούμε. Η πρώτη είναι το σύμπλοκο.

**Ορισμός 3.2** (Σύμπλοκο). Έστω  $K$  υποομάδα της  $G$  και  $x \in G$ . Με  $xK$  συμβολίζουμε το σύνολο όλων των γινομένων  $xk$ , όπου το  $x$  μένει σταθερό και το  $k$  διατρέχει την  $K$ . Το σύνολο αυτό λέγεται **σύμπλοκο** (*coset*) του  $x$  ως προς την  $K$ .<sup>2</sup>

Ένα παράδειγμα θα βοηθήσει. Στην προσθετική ομάδα  $\mathbb{Z}$  ας πάρουμε την υποομάδα  $3\mathbb{Z}$  των πολλαπλασίων του 3. Το σύμπλοκο του 1 γράφεται, με προσθετικό συμβολισμό,  $1 + 3\mathbb{Z}$  και είναι το σύνολο

<sup>2</sup>Για μια αναλυτική παρουσίαση των συμπλόκων βλ. κεφ. 13 του C. C. Pinter, *A Book of Abstract Algebra*, 2η έκδοση, McGraw-Hill, 1990.

$\{\dots, -5, -2, 1, 4, 7, \dots\}$ . Το σύμπλοκο του 4 είναι το ίδιο σύνολο. Τα σύμπλοκα της  $3\mathbb{Z}$  είναι λοιπόν τρία, τα  $3\mathbb{Z}$ ,  $1 + 3\mathbb{Z}$  και  $2 + 3\mathbb{Z}$ , δηλαδή οι κλάσεις υπολοίπων ως προς 3.

Επειδή κάθε σύμπλοκο είναι υποσύνολο της  $G$ , για να δείξουμε ότι δύο σύμπλοκα ταυτίζονται πρέπει να δείξουμε ότι είναι ίσα σύνολα. Το κριτήριο είναι το εξής.

**Πρόταση 3.3** (Κριτήριο ισότητας συμπλόκων). Έστω  $K$  υποομάδα της  $G$  και  $x, y \in G$ . Τότε

$$xK = yK \iff y^{-1}x \in K.$$

Επιπλέον δύο σύμπλοκα της  $K$  είτε ταυτίζονται είτε είναι ξένα, και η  $G$  είναι η ξένη ένωση των συμπλόκων της  $K$ .

*Απόδειξη.* Αν  $xK = yK$ , τότε  $x = xe_G \in yK$ , οπότε  $x = yk$  για κάποιο  $k \in K$  και  $y^{-1}x = k \in K$ . Αντίστροφα, αν  $y^{-1}x = k \in K$ , τότε  $x = yk$  και  $xK = ykK = yK$ , αφού  $kK = K$ .

Για το δεύτερο μέρος έστω  $z \in xK \cap yK$ . Τότε  $z = xk_1 = yk_2$  για κάποια  $k_1, k_2 \in K$ , οπότε  $y^{-1}x = k_2k_1^{-1} \in K$  και από το κριτήριο  $xK = yK$ . Άρα δύο σύμπλοκα που έχουν κοινό στοιχείο ταυτίζονται. Τέλος, επειδή κάθε  $x \in G$  ανήκει στο  $xK$ , η  $G$  είναι η ένωση των συμπλόκων της  $K$ , και η ένωση αυτή είναι ξένη.  $\square$

Η δεύτερη έννοια περιγράφει μια επιπλέον ιδιότητα του πυρήνα, που θα τη χρειαστούμε παρακάτω για να ορίσουμε την ομάδα πηλίκου.

**Ορισμός 3.4** (Κανονική υποομάδα). Μια υποομάδα  $N$  της  $G$  λέγεται **κανονική** (*normal*) αν  $gNg^{-1} \subseteq N$  για κάθε  $g \in G$ , δηλαδή αν  $gng^{-1} \in N$  για κάθε  $g \in G$  και κάθε  $n \in N$ . Τότε γράφουμε  $N \trianglelefteq G$ .

Σε μια αβελιανή ομάδα κάθε υποομάδα είναι κανονική, αφού  $gng^{-1} = n$ . Ας δούμε τώρα ότι ο πυρήνας έχει αυτή την ιδιότητα.

**Πρόταση 3.5.** Έστω  $f : G \rightarrow H$  ομομορφισμός ομάδων. Ο  $\ker f$  είναι κανονική υποομάδα της  $G$  και η  $\operatorname{Im} f$  είναι υποομάδα της  $H$ . Επιπλέον, για  $x, y \in G$  ισχύει

$$x \ker f = y \ker f \iff f(x) = f(y).$$

*Απόδειξη.* Το  $e_G$  ανήκει στον  $\ker f$  από την Πρόταση 2.2(i). Αν  $x, y \in \ker f$ , τότε από τον ορισμό και την Πρόταση 2.2(ii)

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = e_H e_H^{-1} = e_H,$$

άρα  $xy^{-1} \in \ker f$ . Επομένως ο  $\ker f$  είναι υποομάδα. Αν επιπλέον  $g \in G$  και  $x \in \ker f$ , τότε

$$f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)e_H f(g)^{-1} = e_H,$$

οπότε  $gxg^{-1} \in \ker f$  και ο  $\ker f$  είναι κανονική υποομάδα.

Για την εικόνα,  $e_H = f(e_G) \in \operatorname{Im} f$ . Αν  $f(x)$  και  $f(y)$  είναι δύο στοιχεία της εικόνας, τότε  $f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$ , που ανήκει κι αυτό στην εικόνα.

Για την ισοδυναμία, από το κριτήριο ισότητας συμπλόκων έχουμε  $x \ker f = y \ker f$  ακριβώς όταν  $y^{-1}x \in \ker f$ . Όπως είδαμε παραπάνω, αυτό σημαίνει  $f(y^{-1}x) = e_H$ , δηλαδή  $f(y)^{-1}f(x) = e_H$ , δηλαδή  $f(x) = f(y)$ .  $\square$

Η ισοδυναμία λέει ότι ο ομομορφισμός ταυτίζει δύο στοιχεία ακριβώς όταν αυτά ανήκουν στο ίδιο σύμπλοκο του πυρήνα. Για κάθε  $h$  στην εικόνα, το σύνολο  $f^{-1}(h)$  των στοιχείων που πηγαίνουν στο  $h$  είναι λοιπόν ένα σύμπλοκο του  $\ker f$ . Επειδή η  $k \mapsto xk$  είναι αμφίρριψη από τον  $\ker f$  στο  $x \ker f$ , όλα αυτά τα σύνολα έχουν τον ίδιο πληθάριθμο με τον πυρήνα.

### Διαισθητική εικόνα

Ο πυρήνας μετρά την πληροφορία που χάνεται όταν περνάμε από την  $G$  στην  $H$ . Όσο μεγαλύτερος είναι, τόσο περισσότερα στοιχεία της  $G$  καταλήγουν στο ίδιο στοιχείο της  $H$ . Η εικόνα είναι το μέρος της  $H$  που ο ομομορφισμός πράγματι βλέπει.

Από την ισοδυναμία της Πρότασης 3.5 προκύπτει άμεσα ένα χρήσιμο κριτήριο για την έρριψη.

**Πρόταση 3.6** (Κριτήριο έρριψης). Ένας ομομορφισμός  $f : G \rightarrow H$  είναι έρριψη αν και μόνο αν  $\ker f = \{e_G\}$ .

*Απόδειξη.* Αν ο πυρήνας είναι τετριμμένος και  $f(x) = f(y)$ , τότε  $x\{e_G\} = y\{e_G\}$ , δηλαδή  $x = y$ . Αντίστροφα, αν η  $f$  είναι έρριψη και  $f(x) = e_H = f(e_G)$ , τότε  $x = e_G$ .  $\square$

Για να ελέγξουμε λοιπόν ότι ένας ομομορφισμός είναι έρριψη, δεν χρειάζεται να συγκρίνουμε όλα τα ζεύγη στοιχείων. Αρκεί να βρούμε ποια στοιχεία πηγαίνουν στο ουδέτερο.

## 4 Ισομορφισμοί

Ο Ορισμός 2.5 ονόμασε τους ομομορφισμούς ανάλογα με τις ιδιότητες της απεικόνισης, και τώρα ξέρουμε ότι ο πυρήνας ελέγχει την έρριψη και η εικόνα την επίρριψη. Ας δούμε από κοντά τους ισομορφισμούς.

Οι ισομορφισμοί έχουν μια ιδιότητα που δεν ισχύει σε κάθε μαθηματική δομή. Στην Τοπολογία, για παράδειγμα, η απεικόνιση  $[0, 2\pi) \rightarrow S^1$  με  $t \mapsto e^{it}$  είναι συνεχής αμφίρριψη, αλλά η αντίστροφή της δεν είναι συνεχής. Στις ομάδες αυτό δεν μπορεί να συμβεί.

**Πρόταση 4.1.** (i) Η ταυτοτική απεικόνιση  $G \rightarrow G$  είναι ομομορφισμός.

(ii) Η σύνθεση δύο ομομορφισμών  $f : G \rightarrow H$  και  $g : H \rightarrow K$  είναι ομομορφισμός.

(iii) Η αντίστροφη μιας αμφίρριψης  $f : G \rightarrow H$  που είναι ομομορφισμός είναι και αυτή ομομορφισμός.

*Απόδειξη.* Το (i) είναι φανερό. Για το (ii),

$$g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)).$$

Για το (iii) έστω  $u, v \in H$ . Επειδή η  $f$  είναι επίρριψη, υπάρχουν  $x, y \in G$  με  $u = f(x)$  και  $v = f(y)$ . Τότε

$$f^{-1}(uv) = f^{-1}(f(x)f(y)) = f^{-1}(f(xy)) = xy = f^{-1}(u)f^{-1}(v).$$

$\square$

Γράφουμε  $G \cong H$  όταν υπάρχει ισομορφισμός από την  $G$  στην  $H$ . Η σχέση  $\cong$  είναι ανακλαστική, γιατί η ταυτοτική απεικόνιση είναι ισομορφισμός. Είναι συμμετρική, γιατί η αντίστροφη ενός ισομορφισμού είναι ισομορφισμός. Είναι και μεταβατική, γιατί η σύνθεση δύο ισομορφισμών είναι ομομορφισμός και ταυτόχρονα αμφίρριψη, αφού η σύνθεση αμφίρριψεων είναι αμφίρριψη. Δύο ισόμορφες ομάδες είναι από αλγεβρική άποψη η ίδια ομάδα με διαφορετικά ονόματα στα στοιχεία της.

### Προσοχή

Το  $G \cong H$  δεν σημαίνει ότι  $G = H$ . Σημαίνει ότι υπάρχει ισομορφισμός  $f : G \rightarrow H$ . Η  $\exp$  είναι γνησίως αύξουσα, άρα έρριψη, και κάθε  $y > 0$  γράφεται  $y = e^{\ln y}$ , άρα είναι και επίρριψη. Επομένως  $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$ , παρότι οι δύο πράξεις φαίνονται εντελώς διαφορετικές.

## 5 Ομάδες πηλίκου και το πρώτο θεώρημα ισομορφισμού

Είδαμε στην Πρόταση 3.5 ότι ένας ομομορφισμός  $f : G \rightarrow H$  ταυτίζει δύο στοιχεία ακριβώς όταν αυτά ανήκουν στο ίδιο σύμπλοκο του  $\ker f$ . Δηλαδή ο  $f$  δεν διακρίνει τα στοιχεία ενός συμπλόκου του πυρήνα. Είναι φυσικό λοιπόν να θεωρήσουμε κάθε σύμπλοκο ως ένα νέο στοιχείο. Το σύνολο αυτών των νέων στοιχείων θα είναι το πηλίκο της  $G$  ως προς τον πυρήνα, και το ερώτημα είναι πώς θα το κάνουμε ομάδα. Για να γίνει αυτό, πρέπει τα σύμπλοκα να πολλαπλασιάζονται μεταξύ τους. Ο πιο φυσικός κανόνας είναι να πολλαπλασιάζουμε τους αντιπροσώπους.

Έστω  $N \trianglelefteq G$  και  $G/N$  το σύνολο των συμπλόκων της  $N$ .<sup>3</sup> Ορίζουμε

$$(aN)(bN) = (ab)N.$$

Ο ορισμός χρησιμοποιεί αντιπροσώπους. Το σύμπλοκο  $aN$  έχει πολλούς αντιπροσώπους, αφού  $aN = a'N$  για κάθε  $a' \in aN$ . Αν το αποτέλεσμα εξαρτιόταν από την επιλογή των αντιπροσώπων, ο ορισμός δεν θα είχε νόημα. Πρέπει λοιπόν να ελέγξουμε ότι δεν εξαρτάται από αυτήν. Έστω  $a'N = aN$  και  $b'N = bN$ . Τότε  $a' \in aN$  και  $b' \in bN$ , δηλαδή  $a' = an_1$  και  $b' = bn_2$  για κάποια  $n_1, n_2 \in N$ , και

$$a'b' = an_1bn_2 = ab(b^{-1}n_1b)n_2.$$

Επειδή η  $N$  είναι κανονική, το  $b^{-1}n_1b$  ανήκει στην  $N$ , οπότε το  $(b^{-1}n_1b)n_2$  ανήκει στην  $N$ . Άρα  $a'b' \in abN$  και  $a'b'N = abN$ . Εδώ ακριβώς χρησιμοποιείται η κανονικότητα. Χωρίς αυτήν το επιχείρημα δεν περνά.

Τα αξιώματα της ομάδας μεταφέρονται από την  $G$ . Το γινόμενο δύο συμπλόκων είναι σύμπλοκο, οπότε η πράξη είναι εσωτερική. Η προσεταιριστικότητα ισχύει γιατί

$$((aN)(bN))(cN) = (ab)cN = a(bc)N = (aN)((bN)(cN)).$$

Ουδέτερο στοιχείο είναι το σύμπλοκο  $e_GN = N$  και αντίστροφο του  $aN$  είναι το  $a^{-1}N$ . Η  $G/N$  λέγεται **ομάδα πηλίκου** (quotient group) της  $G$  ως προς την  $N$ .

Η απεικόνιση  $\pi : G \rightarrow G/N$  με  $\pi(g) = gN$  είναι ομομορφισμός, αφού  $\pi(ab) = abN = (aN)(bN) = \pi(a)\pi(b)$ . Είναι προφανώς επίρριψη, και  $\pi(g) = N$  ακριβώς όταν  $g \in N$ , οπότε  $\ker \pi = N$ . Κάθε κανονική υποομάδα είναι λοιπόν πυρήνας ενός ομομορφισμού, και από την Πρόταση 3.5 κάθε πυρήνας είναι κανονική υποομάδα. Οι δύο έννοιες συμπίπτουν.

Το γνωστότερο παράδειγμα είναι η  $\mathbb{Z}/n\mathbb{Z}$ . Η υποομάδα  $n\mathbb{Z}$  των πολλαπλασίων του  $n$  είναι κανονική, αφού η  $\mathbb{Z}$  είναι αβελιανή. Το σύμπλοκο του  $a$  είναι το σύνολο  $a + n\mathbb{Z}$ , που ταυτίζεται με την κλάση υπολοίπων  $[a]_n$ . Η ιδιότητα  $[a + b]_n = [a]_n + [b]_n$  της αρχής είναι ακριβώς ο ορισμός της πράξης στην ομάδα πηλίκου.

Είμαστε τώρα έτοιμοι να διατυπώσουμε το βασικό αποτέλεσμα αυτής της ενότητας.

**Θεώρημα 5.1** (Πρώτο θεώρημα ισομορφισμού). Έστω  $f : G \rightarrow H$  ομομορφισμός ομάδων. Η απεικόνιση

$$\bar{f} : G/\ker f \longrightarrow \operatorname{Im} f, \quad \bar{f}(g\ker f) = f(g),$$

είναι καλά ορισμένος ισομορφισμός. Επομένως

$$G/\ker f \cong \operatorname{Im} f.$$

*Απόδειξη.* Γράφουμε  $K = \ker f$ . Ο  $K$  είναι κανονική υποομάδα από την Πρόταση 3.5, οπότε η  $G/K$  είναι ομάδα. Η ίδια πρόταση δίνει  $gK = hK \iff f(g) = f(h)$ , και χρησιμοποιούμε τις δύο κατευθύνσεις χωριστά.

<sup>3</sup>Για μια αναλυτική παρουσίαση των ομάδων πηλίκου, με πολλά παραδείγματα, βλ. κεφ. 15 και 16 του C. C. Pinter, *A Book of Abstract Algebra*.

Ας ξεκινήσουμε από το ότι η  $\bar{f}$  ορίζεται καλά. Η συνεπαγωγή  $gK = hK \Rightarrow f(g) = f(h)$  λέει ότι η τιμή  $\bar{f}(gK)$  δεν εξαρτάται από τον αντιπρόσωπο  $g$  του συμπλόκου. Άρα η  $\bar{f}$  είναι καλά ορισμένη.

Η συνεπαγωγή  $f(g) = f(h) \Rightarrow gK = hK$  λέει ότι αν  $\bar{f}(gK) = \bar{f}(hK)$ , τότε  $gK = hK$ . Άρα η  $\bar{f}$  είναι έρριψη.

Κάθε στοιχείο της  $\text{Im } f$  είναι της μορφής  $f(g) = \bar{f}(gK)$ , οπότε η  $\bar{f}$  είναι και επίρριψη.

Τέλος

$$\bar{f}((gK)(hK)) = \bar{f}(ghK) = f(gh) = f(g)f(h) = \bar{f}(gK)\bar{f}(hK),$$

οπότε η  $\bar{f}$  είναι ομομορφισμός. Ως αμφίρριψη που είναι ομομορφισμός, είναι ισομορφισμός.  $\square$

Το θεώρημα λέει ότι κάθε ομομορφισμός γράφεται ως σύνθεση

$$G \xrightarrow{\pi} G/\ker f \xrightarrow{\bar{f}} \text{Im } f \xrightarrow{\iota} H,$$

δηλαδή ενός επιμορφισμού, ενός ισομορφισμού και ενός μονομορφισμού. Η  $\iota$  στέλνει κάθε στοιχείο της εικόνας στον εαυτό του. Πράγματι, για κάθε  $g \in G$  έχουμε  $\iota(\bar{f}(\pi(g))) = \bar{f}(gK) = f(g)$ . Ο μόνος όρος που δεν είναι τετριμμένος είναι ο ισομορφισμός, και αυτός δείχνει ότι το πηλίκο μέσω του πυρήνα δεν χάνει τίποτε άλλο.

Ας δούμε τώρα πώς δουλεύει το θεώρημα σε συγκεκριμένα παραδείγματα. Σε κάθε περίπτωση βρίσκουμε έναν ομομορφισμό, υπολογίζουμε τον πυρήνα και την εικόνα του, και το θεώρημα μας δίνει έναν ισομορφισμό.

**Παράδειγμα 5.2** (Εφαρμογές του θεωρήματος). (i) Ας συμβολίσουμε με  $\mu_n$  το σύνολο των μιγαδικών  $z$  με  $z^n = 1$ , δηλαδή των ριζών της μονάδας τάξης  $n$ . Η  $k \mapsto e^{2\pi i k/n}$  από τη  $(\mathbb{Z}, +)$  στην  $(\mathbb{C}^\times, \cdot)$  είναι ομομορφισμός. Ισχύει  $e^{2\pi i k/n} = 1$  ακριβώς όταν το  $k/n$  είναι ακέραιος, οπότε ο πυρήνας είναι  $n\mathbb{Z}$ . Η εικόνα αποτελείται από τους αριθμούς  $e^{2\pi i k/n}$  για  $k = 0, 1, \dots, n-1$ , που είναι  $n$  διαφορετικές ρίζες της  $z^n = 1$ . Επειδή η εξίσωση έχει το πολύ  $n$  ρίζες, η εικόνα είναι ακριβώς η  $\mu_n$ . Άρα  $\mathbb{Z}/n\mathbb{Z} \cong \mu_n$ .

(ii) Η  $t \mapsto e^{it}$  από την  $(\mathbb{R}, +)$  στον  $S^1$  είναι επίρριψη, γιατί κάθε μιγαδικός με μέτρο 1 γράφεται  $e^{it}$ . Ο πυρήνας της είναι  $2\pi\mathbb{Z}$ . Άρα  $\mathbb{R}/2\pi\mathbb{Z} \cong S^1$ .

(iii) Ας συμβολίσουμε με  $\text{SL}_n(\mathbb{R})$  την υποομάδα της  $\text{GL}_n(\mathbb{R})$  που αποτελείται από τις μήτρες με ορίζουσα 1. Η ορίζουσα  $\det : \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$  είναι επίρριψη, γιατί η διαγώνια μήτρα  $\text{diag}(t, 1, \dots, 1)$  έχει ορίζουσα  $t$ . Ο πυρήνας της είναι η  $\text{SL}_n(\mathbb{R})$ . Άρα  $\text{GL}_n(\mathbb{R})/\text{SL}_n(\mathbb{R}) \cong \mathbb{R}^\times$ .

(iv) Για  $n \geq 2$  το πρόσημο  $S_n \rightarrow \{\pm 1\}$  είναι επίρριψη, γιατί μια αντιμετάθεση έχει πρόσημο  $-1$ . Ο πυρήνας του είναι το σύνολο  $A_n$  των άρτιων μεταθέσεων, που λέγεται εναλλάσσουσα ομάδα. Άρα  $S_n/A_n \cong \{\pm 1\}$ , και ειδικότερα οι άρτιες μεταθέσεις είναι ακριβώς οι μισές.

## 6 Ομομορφισμοί δακτυλίων

Η αναγωγή  $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  διατηρεί και μια δεύτερη πράξη, αφού  $[ab]_n = [a]_n[b]_n$ . Το ίδιο κάνει η αποτίμηση  $\text{ev}_r : \mathbb{R}[x] \rightarrow \mathbb{R}$  με  $p \mapsto p(r)$ , γιατί η τιμή ενός αθροίσματος ή γινομένου πολυωνύμων στο  $r$  είναι το άθροισμα ή το γινόμενο των τιμών.<sup>4</sup> Ο κανόνας  $\det(AB) = \det A \det B$  της αρχής, αντίθετα, δεν έχει ανάλογο για την πρόσθεση, αφού γενικά  $\det(A+B) \neq \det A + \det B$ . Όταν λοιπόν η δομή έχει δύο πράξεις, ο ομομορφισμός πρέπει να σέβεται και τις δύο.

Ας θυμηθούμε τον ορισμό του δακτυλίου.

<sup>4</sup>Την ίδια απεικόνιση τη συναντάμε και στο παράδειγμα του διπλού δυϊκού, βλ. σελ. 104 του βιβλίου *Εισαγωγή στη Θεωρία Κατηγοριών*.

**Ορισμός 6.1** (Δακτύλιος). Ένας **δακτύλιος** είναι ένα σύνολο  $R$  με δύο πράξεις, πρόσθεση και πολλαπλασιασμό, ώστε η  $(R, +)$  να είναι αβελιανή ομάδα, ο πολλαπλασιασμός να είναι προσεταιριστικός, να ισχύουν οι επιμεριστικές ιδιότητες  $a(b + c) = ab + ac$  και  $(a + b)c = ac + bc$ , και να υπάρχει μοναδιαίο στοιχείο  $1$  με  $1a = a1 = a$  για κάθε  $a$ .

Δεν υποθέτουμε ότι ο πολλαπλασιασμός είναι αντιμεταθετικός, γιατί θέλουμε να συμπεριλάβουμε και δακτυλίους μητρώων. Παραδείγματα δακτυλίων είναι οι  $\mathbb{Z}$ ,  $\mathbb{Z}/n\mathbb{Z}$ ,  $\mathbb{R}[x]$  και οι  $n \times n$  μήτρες με πραγματικά στοιχεία.

**Ορισμός 6.2** (Ομομορφισμός δακτυλίων). Έστω  $R$  και  $S$  δύο δακτύλιοι. Μια απεικόνιση  $\varphi : R \rightarrow S$  λέγεται **ομομορφισμός δακτυλίων** αν για κάθε  $a, b \in R$  ισχύουν

$$\varphi(a + b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b), \quad \varphi(1_R) = 1_S.$$

Η πρώτη συνθήκη λέει ότι η  $\varphi$  είναι ομομορφισμός των προσθετικών ομάδων  $(R, +) \rightarrow (S, +)$ . Όλα όσα δείξαμε για ομάδες ισχύουν λοιπόν ως προς την πρόσθεση. Από την Πρόταση 2.2, γραμμένη προσθετικά, παίρνουμε  $\varphi(0_R) = 0_S$ ,  $\varphi(-a) = -\varphi(a)$  και  $\varphi(na) = n\varphi(a)$  για κάθε  $n \in \mathbb{Z}$ .

Η δεύτερη και η τρίτη συνθήκη μαζί δίνουν κάτι για τα αντιστρέψιμα στοιχεία. Αν το  $a$  είναι αντιστρέψιμο στον  $R$ , τότε

$$\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(1_R) = 1_S \quad \text{και} \quad \varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(1_R) = 1_S.$$

Χρειαζόμαστε και τις δύο ισότητες, επειδή ο δακτύλιος δεν είναι αναγκαστικά αντιμεταθετικός. Επομένως το  $\varphi(a)$  είναι αντιστρέψιμο στον  $S$  και  $\varphi(a^{-1}) = \varphi(a)^{-1}$ .

Η τρίτη συνθήκη του ορισμού, η διατήρηση της μονάδας, μπορεί να φανεί περιττή. Στις ομάδες η διατήρηση του ουδέτερου προέκυπτε μόνη της. Θα δούμε στην επόμενη παρατήρηση ότι στους δακτυλίους δεν συμβαίνει το ίδιο.

**Παρατήρηση 6.3** (Η συνθήκη για τη μονάδα). Στη βιβλιογραφία υπάρχουν δύο συμβάσεις, και ορισμένοι συγγραφείς δεν ζητούν την τρίτη συνθήκη. Η διαφορά δεν είναι τυπική. Η  $h : \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$  με  $h(n) = (n, 0)$  διατηρεί πρόσθεση και πολλαπλασιασμό, αλλά  $h(1) = (1, 0) \neq (1, 1)$ . Στην ομάδα, η διατήρηση του ουδέτερου προέκυπτε από τη διατήρηση της πράξης, γιατί μπορούσαμε να πολλαπλασιάσουμε με  $f(e_G)^{-1}$ . Στον δακτύλιο το  $\varphi(1_R)$  δεν είναι γενικά αντιστρέψιμο, και το ίδιο επιχείρημα δεν περνά. Εδώ ακολουθούμε τη σύμβαση που ζητά τη διατήρηση της μονάδας. Όταν διαβάζουμε ένα βιβλίο, ελέγχουμε ποια σύμβαση χρησιμοποιεί.

Ας δούμε μερικά παραδείγματα.

**Παράδειγμα 6.4** (Ομομορφισμοί δακτυλίων). (i) Η απεικόνιση  $\mathbb{Z} \rightarrow \mathbb{R}$  με  $n \mapsto n$  είναι μονομορφισμός αλλά όχι επιμορφισμός, αφού το  $\frac{1}{2}$  δεν ανήκει στην εικόνα.

(ii) Η αναγωγή  $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  είναι επιμορφισμός, αφού κάθε κλάση  $[a]_n$  είναι η εικόνα του  $a$ . Η αποτίμηση  $\text{ev}_r$  είναι επίσης επιμορφισμός, αφού κάθε πραγματικός  $c$  είναι η τιμή στο  $r$  του σταθερού πολυωνύμου  $c$ .

(iii) Η μιγαδική συζυγία  $z \mapsto \bar{z}$  είναι αυτομορφισμός του  $\mathbb{C}$ . Διατηρεί τις πράξεις, αφού  $\overline{z + w} = \bar{z} + \bar{w}$ ,  $\overline{zw} = \bar{z}\bar{w}$  και  $\bar{1} = 1$ . Είναι αμφίρριψη, γιατί η σύνθεσή της με τον εαυτό της είναι η ταυτοτική απεικόνιση.

(iv) Για κάθε δακτύλιο  $R$  υπάρχει ακριβώς ένας ομομορφισμός  $\mathbb{Z} \rightarrow R$ . Με  $n \cdot 1_R$  συμβολίζουμε το άθροισμα  $n$  αντιγράφων του  $1_R$  όταν  $n > 0$ , το  $0_R$  όταν  $n = 0$  και το  $-((-n) \cdot 1_R)$  όταν  $n < 0$ . Ας δούμε πρώτα τη μοναδικότητα. Ένας ομομορφισμός  $\varphi$  πρέπει να στείλει το  $1$  στο  $1_R$ , και τότε από τη διατήρηση της πρόσθεσης  $\varphi(n) = \varphi(n \cdot 1) = n \cdot \varphi(1) = n \cdot 1_R$ . Για την ύπαρξη, πρέπει να ελέγξουμε ότι η  $n \mapsto n \cdot 1_R$  είναι ομομορφισμός. Η πρόσθεση διατηρείται από τους νόμους των πολλαπλασίων στην αβελιανή ομάδα  $(R, +)$ . Για τον πολλαπλασιασμό, η επιμεριστική ιδιότητα δίνει  $(m \cdot 1_R)(n \cdot 1_R) = mn \cdot (1_R 1_R) = mn \cdot 1_R$ .

Όπως και στις ομάδες, ας δούμε και τι δεν είναι ομομορφισμός.

**Παράδειγμα 6.5** (Απεικονίσεις που δεν είναι ομομορφισμοί δακτυλίων). Η  $x \mapsto x^2$  στους πραγματικούς διατηρεί τον πολλαπλασιασμό και τη μονάδα, αλλά όχι την πρόσθεση, γιατί  $(x + y)^2 = x^2 + 2xy + y^2$  και αυτό διαφέρει από το  $x^2 + y^2$  όταν  $xy \neq 0$ . Η  $n \mapsto 2n$  στους ακέραιους διατηρεί την πρόσθεση αλλά όχι τον πολλαπλασιασμό, γιατί  $2 \cdot (1 \cdot 1) = 2 \neq 4 = 2 \cdot 2$ . Ούτε τη μονάδα διατηρεί, αφού στέλνει το 1 στο 2. Δεν αρκεί λοιπόν να διατηρείται μία μόνο πράξη, και ένας ομομορφισμός των προσθετικών ομάδων δεν είναι γενικά ομομορφισμός δακτυλίων.

## 7 Πυρήνας, ιδεώδη και το πρώτο θεώρημα ισομορφισμού

Ο πυρήνας ενός ομομορφισμού δακτυλίων  $\varphi : R \rightarrow S$  ορίζεται όπως στις ομάδες, με το μηδέν στη θέση του ουδέτερου,

$$\ker \varphi = \{a \in R \mid \varphi(a) = 0_S\}, \quad \text{Im } \varphi = \{\varphi(a) \mid a \in R\}.$$

Ως πυρήνας του ομομορφισμού των προσθετικών ομάδων είναι υποομάδα της  $(R, +)$ . Ο πολλαπλασιασμός όμως επιβάλλει κάτι παραπάνω. Αν  $a \in \ker \varphi$  και  $r \in R$ , τότε

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0_S = 0_S,$$

και ομοίως  $\varphi(ar) = \varphi(a)\varphi(r) = 0_S$ . Ο πυρήνας απορροφά λοιπόν τον πολλαπλασιασμό από αριστερά και από δεξιά με οποιοδήποτε στοιχείο του δακτυλίου, όχι μόνο με στοιχεία του ίδιου του πυρήνα. Στην αναγωγή  $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ , για παράδειγμα, κάθε ακέραιος πολλαπλασιασμένος με ένα πολλαπλάσιο του  $n$  δίνει πάλι πολλαπλάσιο του  $n$ . Η ιδιότητα αυτή αξίζει ένα όνομα.

**Ορισμός 7.1** (Ιδεώδες). Έστω  $R$  δακτύλιος. Ένα υποσύνολο  $I \subseteq R$  λέγεται **ιδεώδες** (*ideal*) του  $R$  αν είναι υποομάδα της  $(R, +)$  και για κάθε  $r \in R$  και  $a \in I$  ισχύει  $ra \in I$  και  $ar \in I$ .

Γράφουμε  $I \trianglelefteq R$ . Ο πυρήνας κάθε ομομορφισμού δακτυλίων είναι λοιπόν ιδεώδες. Για την εικόνα χρειαζόμαστε μια ακόμη έννοια. Ένα υποσύνολο  $T$  ενός δακτυλίου  $S$  λέγεται **υποδακτύλιος** αν είναι υποομάδα της  $(S, +)$ , είναι κλειστό ως προς τον πολλαπλασιασμό και περιέχει το  $1_S$ . Η  $\text{Im } \varphi$  είναι υποδακτύλιος του  $S$ . Είναι υποομάδα της  $(S, +)$  από την περίπτωση των ομάδων, είναι κλειστή ως προς τον πολλαπλασιασμό αφού  $\varphi(a)\varphi(b) = \varphi(ab)$ , και περιέχει το  $1_S = \varphi(1_R)$ . Το κριτήριο της έρριψης ισχύει όπως πριν, δηλαδή η  $\varphi$  είναι έρριψη αν και μόνο αν  $\ker \varphi = \{0_R\}$ . Πράγματι, αυτό είναι η Πρόταση 3.6 για τον ομομορφισμό των προσθετικών ομάδων.

ΑΣ προσέξουμε ότι ο πυρήνας και η εικόνα δεν έχουν την ίδια συμπεριφορά. Η εικόνα είναι υποδακτύλιος, ενώ ο πυρήνας σχεδόν ποτέ.

### Προσοχή

Ο πυρήνας είναι ιδεώδες, αλλά είναι υποδακτύλιος μόνο όταν ο  $S$  είναι ο μηδενικός δακτύλιος. Πράγματι, αν  $1_R \in \ker \varphi$ , τότε  $1_S = \varphi(1_R) = 0_S$ , και τότε κάθε  $s \in S$  ικανοποιεί  $s = s1_S = s0_S = 0_S$ . Ο  $S$  είναι λοιπόν ο μηδενικός δακτύλιος. Σε κάθε άλλη περίπτωση ο πυρήνας δεν περιέχει τη μονάδα, άρα δεν είναι υποδακτύλιος.

Όπως στις ομάδες, κάθε ιδεώδες είναι πυρήνας. Έστω  $I \trianglelefteq R$ . Στο σύνολο  $R/I = \{a + I \mid a \in R\}$  ορίζουμε

$$(a + I) + (b + I) = (a + b) + I, \quad (a + I)(b + I) = ab + I.$$

Η πρόσθεση ορίζεται καλά επειδή η  $I$  είναι υποομάδα της αβελιανής ομάδας  $(R, +)$ , άρα κανονική, και βρισκόμαστε στην περίπτωση της ομάδας πηλίκο. Ο πολλαπλασιασμός θέλει περισσότερη προσοχή,

γιατί πρέπει και εδώ να ελέγξουμε ότι το αποτέλεσμα δεν εξαρτάται από τους αντιπροσώπους. Αν  $a' = a + i$  και  $b' = b + j$  με  $i, j \in I$ , τότε

$$a'b' = ab + aj + ib + ij.$$

Το  $aj$  ανήκει στο  $I$  λόγω απορρόφησης από αριστερά, το  $ib$  λόγω απορρόφησης από δεξιά και το  $ij$  για οποιονδήποτε από τους δύο λόγους. Άρα  $a'b' \in ab + I$ . Εδώ χρειάζεται ότι η  $I$  είναι ιδεώδες και όχι απλώς υποομάδα, όπως στις ομάδες χρειαζόταν η κανονικότητα. Τα αξιώματα του δακτυλίου μεταφέρονται από τον  $R$ , αφού κάθε αξίωμα ελέγχεται σε αντιπροσώπους. Το μηδέν του  $R/I$  είναι το σύμπλοκο  $0 + I = I$  και η μονάδα του το σύμπλοκο  $1 + I$ . Ο  $R/I$  λέγεται **δακτύλιος πηλίκου**, και η  $\pi : R \rightarrow R/I$  με  $\pi(a) = a + I$  είναι επιμορφισμός δακτυλίων με  $\ker \pi = I$ . Για  $R = \mathbb{Z}$  και  $I = n\mathbb{Z}$  ξαναβρίσκουμε τον δακτύλιο  $\mathbb{Z}/n\mathbb{Z}$ , με πολλαπλασιασμό  $[a]_n[b]_n = [ab]_n$ .

Έχουμε τώρα όλα τα στοιχεία που χρειαζόμαστε για την αντίστοιχη μορφή του θεωρήματος.

**Θεώρημα 7.2** (Πρώτο θεώρημα ισομορφισμού για δακτυλίους). Έστω  $\varphi : R \rightarrow S$  ομομορφισμός δακτυλίων. Η απεικόνιση  $\bar{\varphi} : R/\ker \varphi \rightarrow \operatorname{Im} \varphi$  με  $\bar{\varphi}(a + \ker \varphi) = \varphi(a)$  είναι καλά ορισμένος ισομορφισμός δακτυλίων. Επομένως

$$R/\ker \varphi \cong \operatorname{Im} \varphi.$$

*Απόδειξη.* Εφαρμόζουμε το Θεώρημα 5.1 στον ομομορφισμό των προσθετικών ομάδων. Η  $\bar{\varphi}$  είναι λοιπόν καλά ορισμένη αμφίρριψη που διατηρεί την πρόσθεση. Μένει ο πολλαπλασιασμός και η μονάδα. Με  $K = \ker \varphi$  έχουμε

$$\bar{\varphi}((a + K)(b + K)) = \bar{\varphi}(ab + K) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(a + K)\bar{\varphi}(b + K)$$

και  $\bar{\varphi}(1 + K) = \varphi(1_R) = 1_S$ . Άρα η  $\bar{\varphi}$  είναι ομομορφισμός δακτυλίων και αμφίρριψη. Η αντίστροφη απεικόνιση διατηρεί και τις δύο πράξεις με το ίδιο επιχείρημα που δώσαμε για τις ομάδες στην Πρόταση 4.1(iii). Διατηρεί και τη μονάδα, αφού από την  $\bar{\varphi}(1 + K) = 1_S$  έπεται  $\bar{\varphi}^{-1}(1_S) = 1 + K$ . Άρα η  $\bar{\varphi}$  είναι ισομορφισμός δακτυλίων.  $\square$

Ας δούμε και εδώ συγκεκριμένες εφαρμογές.

**Παράδειγμα 7.3** (Εφαρμογές του θεωρήματος). (i) Στην αναγωγή  $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  ισχύει  $[a]_n = [0]_n$  ακριβώς όταν  $n \mid a$ , άρα ο πυρήνας είναι  $n\mathbb{Z}$ . Το θεώρημα επιβεβαιώνει ότι ο δακτύλιος πηλίκου  $\mathbb{Z}/n\mathbb{Z}$  ταυτίζεται με την εικόνα της αναγωγής.

(ii) Έστω  $r \in \mathbb{R}$  και  $p \in \mathbb{R}[x]$ . Η διαίρεση του  $p$  με το  $x - r$  δίνει  $p = (x - r)q + c$ , όπου  $q$  πολυώνυμο και  $c$  σταθερά, αφού το υπόλοιπο έχει βαθμό μικρότερο του 1. Αν αποτιμήσουμε στο  $r$ , βρίσκουμε  $c = p(r)$ . Άρα  $p(r) = 0$  ακριβώς όταν το  $x - r$  διαιρεί το  $p$ . Αυτό σημαίνει ότι ο πυρήνας της  $\operatorname{ev}_r$  είναι το σύνολο  $(x - r)$  των πολλαπλασίων του  $x - r$ , που λέγεται ιδεώδες που παράγεται από το  $x - r$ . Επειδή η  $\operatorname{ev}_r$  είναι επίρριψη, το θεώρημα δίνει  $\mathbb{R}[x]/(x - r) \cong \mathbb{R}$ . Δηλαδή αν στο  $\mathbb{R}[x]$  θεωρήσουμε ίσα δύο πολυώνυμα που η διαφορά τους διαιρείται με το  $x - r$ , το μόνο που απομένει από κάθε πολυώνυμο είναι η τιμή του στο  $r$ .

(iii) Με το ίδιο επιχείρημα, η αποτίμηση στο 0 από το  $\mathbb{Z}[x]$  στο  $\mathbb{Z}$  στέλνει κάθε πολυώνυμο στον σταθερό του όρο. Είναι επίρριψη, και ο πυρήνας της είναι το ιδεώδες  $(x)$  των πολυωνύμων χωρίς σταθερό όρο. Άρα  $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ .

## 8 Προς τη γλώσσα των κατηγοριών

Ας κοιτάξουμε τώρα ό,τι κάναμε με μια ευρύτερη ματιά. Οι ομάδες με τους ομομορφισμούς τους σχηματίζουν κατηγορία, την **Grp**. Τα αντικείμενά της είναι οι ομάδες, τα βέλη της οι ομομορφισμοί, και

η σύνθεση είναι η συνήθης σύνθεση απεικονίσεων. Είδαμε στην Πρόταση 4.1 ότι η σύνθεση ομομορφισμών είναι ομομορφισμός και ότι η ταυτοτική απεικόνιση είναι ομομορφισμός, οπότε τα αξιώματα της κατηγορίας ισχύουν. Το ίδιο ισχύει για τους δακτυλίους και την κατηγορία **Ring**. Οι ισομορφισμοί των δύο κατηγοριών, δηλαδή τα βέλη που έχουν αντίστροφο βέλος, είναι ακριβώς οι αμφιριπτικοί ομομορφισμοί, αφού η αντίστροφη απεικόνιση είναι πάλι ομομορφισμός.

Ας δούμε ένα αποτέλεσμα που ήδη έχουμε αποδείξει με αυτή τη γλώσσα. Ένα αντικείμενο μιας κατηγορίας λέγεται *αρχικό* αν από αυτό υπάρχει ακριβώς ένα βέλος προς κάθε άλλο αντικείμενο. Το Παράδειγμα 6.4(iv) λέει ότι για κάθε δακτύλιο  $R$  υπάρχει ακριβώς ένας ομομορφισμός  $\mathbb{Z} \rightarrow R$ . Άρα ο  $\mathbb{Z}$  είναι αρχικό αντικείμενο της **Ring**. Και ο δακτύλιος πηλίκου  $R/I$  χαρακτηρίζεται από μια καθολική ιδιότητα, που θα τη συναντήσουμε στη γλώσσα των κατηγοριών.

Υπάρχει όμως μια λεπτότητα που αξίζει να τη δούμε με προσοχή. Η λέξη επιμορφισμός έχει στη Θεωρία Κατηγοριών διαφορετικό ορισμό από αυτόν που δώσαμε ως τώρα.

**Παρατήρηση 8.1** (Επιμορφισμός με την κατηγορική έννοια). Στη Θεωρία Κατηγοριών ένα βέλος  $e : A \rightarrow B$  λέγεται επιμορφισμός αν για κάθε ζεύγος βελών  $g, h : B \rightarrow C$  με  $g \circ e = h \circ e$  έπεται  $g = h$ . Το  $e$  απλοποιείται λοιπόν όταν συντίθεται από δεξιά. Κάθε επιμορφισμός με την έννοια του κειμένου, δηλαδή κάθε επιριπτικός ομομορφισμός, έχει αυτή την ιδιότητα, γιατί δύο απεικονίσεις που συμφωνούν σε όλη την εικόνα του  $e$  συμφωνούν σε όλο το  $B$ . Στην **Ring** όμως ισχύει και κάτι λιγότερο αναμενόμενο.

Ας πάρουμε την  $e : \mathbb{Z} \rightarrow \mathbb{Q}$  με  $e(n) = n$ , που δεν είναι επίρριψη. Έστω  $g, h : \mathbb{Q} \rightarrow S$  δύο ομομορφισμοί δακτυλίων που συμφωνούν στους ακεραίους. Για κάθε ακεραίο  $n \neq 0$  έχουμε  $g(n)g(1/n) = g(1) = 1_S$ , και ομοίως  $g(1/n)g(n) = 1_S$ . Άρα το  $g(n)$  είναι αντιστρέψιμο και  $g(1/n) = g(n)^{-1}$ . Το ίδιο ισχύει για την  $h$ . Επειδή  $g(n) = h(n)$  και το αντίστροφο ενός στοιχείου είναι μοναδικό, παίρνουμε

$$g\left(\frac{m}{n}\right) = g(m)g(n)^{-1} = h(m)h(n)^{-1} = h\left(\frac{m}{n}\right).$$

Άρα  $g = h$ , και η  $e$  είναι επιμορφισμός με την κατηγορική έννοια χωρίς να είναι επίρριψη. Για τον λόγο αυτό, όταν περάσουμε στη γλώσσα των κατηγοριών, θα διακρίνουμε προσεκτικά τις δύο έννοιες.

Οι δύο θεωρίες που περιγράψαμε έχουν την ίδια δομή, και ο παρακάτω πίνακας βάζει τα αντίστοιχα στοιχεία δίπλα δίπλα.

|                                       | Ομάδες                               | Δακτύλιοι                                        |
|---------------------------------------|--------------------------------------|--------------------------------------------------|
| Πράξεις που διατηρούνται              | μία                                  | δύο και η μονάδα                                 |
| Στοιχείο στόχου που ορίζει τον πυρήνα | $e_H$                                | $0_S$                                            |
| Πυρήνας                               | κανονική υποομάδα                    | ιδεώδες                                          |
| Εικόνα                                | υποομάδα                             | υποδακτύλιος                                     |
| Κριτήριο έρριψης                      | $\ker f = \{e_G\}$                   | $\ker \varphi = \{0_R\}$                         |
| Πηλίκος                               | ομάδα $G/N$                          | δακτύλιος $R/I$                                  |
| Πρώτο θεώρημα                         | $G/\ker f \cong \operatorname{Im} f$ | $R/\ker \varphi \cong \operatorname{Im} \varphi$ |

#### Βασική ιδέα

Ένας ομομορφισμός μεταφέρει τη δομή από μια άλγεβρα σε μια άλλη. Ο πυρήνας καταγράφει ό,τι χάνεται και είναι πάντα κανονική υποομάδα ή ιδεώδες. Το πηλίκος μέσω του πυρήνα εξαλείφει ακριβώς αυτή την απώλεια, και το πρώτο θεώρημα ισομορφισμού λέει ότι αυτό που μένει ταυτίζεται με την εικόνα. Το ίδιο σχήμα εμφανίζεται στους διανυσματικούς χώρους και σε άλλες αλγεβρικές δομές, και η Θεωρία Κατηγοριών θα το διατυπώσει σε γενική μορφή.