

Σύνολα, Αριθμοί και Αλγεβρικές Δομές — μια εισαγωγή στα μαθηματικά

Χρίστος Α. Παλλήκαρος, Νατάλια Μ. Ιβανόβα

Πρόλογος

Οι σημειώσεις αυτές, που βρίσκονται ακόμη σε προκαταρκτικό στάδιο και δεν έχουν πάρει την τελική τους μορφή, έχουν σκοπό να βοηθήσουν σε μια ‘ομαλή’ μετάβαση από τα σχολικά μαθηματικά στα πιο ‘αυστηρά’ μαθηματικά όπου απαιτείται πλήρης τεκμηρίωση όλων των συλλογισμών. Αποτελούν επίσης μια πρώτη εισαγωγή στα σύνολα και τις συναρτήσεις, τα συστήματα αριθμών (φυσικοί, ακέραιοι, ρητοί, πραγματικοί και μιγαδικοί αριθμοί) και τις αλγεβρικές δομές. Σε σχέση με τα μαθήματα που περιλαμβάνονται στο πρόγραμμα σπουδών του τμήματος Μαθηματικών και Στατιστικής του Πανεπιστημίου Κύπρου, καλύπτουν ολόκληρη την ύλη του ΜΑΣ133, μέρος της ύλης του ΜΑΣ321 και αποτελούν, πιστεύουμε, μια καλή προπαρασκευή για τα ΜΑΣ101 και ΜΑΣ222.

Αφού γίνουν οι απαραίτητες τροποποιήσεις, βελτιώσεις και διορθώσεις, παράλληλα με την ενσωμάτωση νέου υλικού, ο στόχος μας είναι τελικά οι σημειώσεις αυτές να πάρουν την μορφή ενός εισαγωγικού βιβλίου για τα μαθηματικά.

Περιεχόμενα

1	Εισαγωγικό κεφάλαιο	6
1.1	Προτάσεις, λογικοί σύνδεσμοι	6
1.2	Λογικές συνεπαγωγές	10
1.3	Πρωταρχικές έννοιες και αξιώματα	12
	Σημειώσεις και Σχόλια	13
	Ασκήσεις	14
2	Σύνολα	16
2.1	Εισαγωγικά σχόλια και ορισμοί	16
2.2	Καρτεσιανά γινόμενα	18
2.3	Η άλγεβρα Boole των συνόλων	18
2.4	Ποσοδείκτες	21
	Σημειώσεις και Σχόλια	23
	Ασκήσεις	23
3	Συναρτήσεις	25
3.1	Ορισμοί, παραδείγματα	25
3.2	Σύνθεση συναρτήσεων, αντίστροφη συνάρτηση, αντίστροφη εικόνα συνάρτησης	27
3.3	Ακολουθίες	31
	Σημειώσεις και Σχόλια	32
	Ασκήσεις	32
4	Διμελείς πράξεις	35
4.1	Ορισμοί, παραδείγματα	35
4.2	Μεταθέσεις	38
	Ασκήσεις	40
5	Μαθηματική επαγωγή	41
5.1	Αξίωμα της επαγωγής, αρχή καλής διάταξης	41
5.2	Αρχή αναδρομικού ορισμού	46
	Σημειώσεις και Σχόλια	48
	Ασκήσεις	49
6	Διμελείς σχέσεις, σχέσεις ισοδυναμίας	50
6.1	Ορισμοί, παραδείγματα, διαμερίσεις	50
6.2	Κατασκευή των ακεραίων και ρητών	54
	Ασκήσεις	57

7 Το σύνολο των πραγματικών αριθμών	58
7.1 Ιδιότητες των πραγματικών αριθμών	58
7.2 Δεκαδική παράσταση πραγματικού αριθμού	61
7.3 Επέκταση του σώματος $\mathbb{R}$ στο $\mathbb{C}$	62
Σημειώσεις και Σχόλια	64
Ασκήσεις	65
8 Περισσότερα για σύνολα	66
8.1 Αριθμήσιμα σύνολα	66
8.2 Σχέσεις διάταξης	70
Σημειώσεις και Σχόλια	72
Ασκήσεις	72
9 Αριθμητική στο $\mathbb{Z}$	74
9.1 Διαιρετότητα ακεραίων	74
9.2 Ισοτιμίες	80
Σημειώσεις και Σχόλια	82
Ασκήσεις	82
10 Αριθμητική στο $\mathbb{Z}_n$	84
10.1 Πρόσθεση και πολλαπλασιασμός στο $\mathbb{Z}_n$	84
10.2 Αντιστρέψιμα στοιχεία στο $\mathbb{Z}_n$	85
10.3 Μια εφαρμογή — ο κώδικας ISBN-10	87
Σημειώσεις και Σχόλια	89
Ασκήσεις	89
11 Συμμετρίες στο επίπεδο	91
11.1 Ανακλάσεις και περιστροφές στον $\mathbb{R}^2$ (xy -επίπεδο)	91
11.2 Ρίζες της μονάδας στο $\mathbb{C}$	93
11.3 Κινήσεις και συμμετρίες	95
Σημειώσεις και Σχόλια	99
Ασκήσεις	100
12 Ομάδες	101
12.1 Ορισμοί, παραδείγματα, βασικές ιδιότητες	101
12.2 Η συμμετρική ομάδα	104
12.3 Υποομάδες, κυκλική υποομάδα	107
Σημειώσεις και Σχόλια	113
Ασκήσεις	113
13 Γεννήτριες και σχέσεις, ομομορφισμοί ομάδων	115
13.1 Γεννήτριες και σχέσεις	115
13.2 Ομομορφισμοί ομάδων	118
13.3 Θεώρημα Cayley	122
Ασκήσεις	123
14 Κανονικές υποομάδες, θεωρήματα ομομορφισμών	125
14.1 Σύμπλοκα, θεώρημα Lagrange	125
14.2 Κανονικές υποομάδες, ομάδα πηλίκο	128
14.3 Θεωρήματα ομομορφισμών	132
Ασκήσεις	135

15 Δακτύλιοι και σώματα	137
15.1 Ορισμοί, παραδείγματα, βασικές ιδιότητες	137
15.2 Ομομορφισμοί δακτυλίων	141
Σημειώσεις και Σχόλια	142
Ασκήσεις	143
16 Δακτύλιοι πολυνύμων	145
16.1 Ορισμοί, βασικές ιδιότητες	145
16.2 Πολυνυμικοί δακτύλιοι πάνω σε σώματα	147
Ασκήσεις	150
17 Ιδεώδη, επεκτάσεις σωμάτων	152
17.1 Ιδεώδη, Δακτύλιος πηλίκο	152
17.2 Περιοχές κυρίων ιδεωδών, Ευκλείδειες περιοχές	156
17.3 Μεγιστικά ιδεώδη, επεκτάσεις σωμάτων	158
Ασκήσεις	162
Λύσεις ασκήσεων	163
Βιβλιογραφία	192

1. Εισαγωγικό κεφάλαιο

Στο κεφάλαιο αυτό θα χρησιμοποιήσουμε κάποιες στοιχειώδεις ιδιότητες συστημάτων αριθμών όπως οι φυσικοί, οι ακέραιοι, οι ρητοί και οι πραγματικοί αριθμοί τις οποίες έχετε ήδη συναντήσει στην μέχρι τώρα σχολική σας διαδρομή. Στα επόμενα κεφάλαια θα μελετήσουμε με πιο συστηματικό τρόπο τις ιδιότητες αυτές.

1.1. Προτάσεις, λογικοί σύνδεσμοι

Ορισμός. *Πρόταση* είναι μια φράση (ή δήλωση) που επιδέχεται τιμή αλήθειας, δηλαδή μπορεί να χαρακτηριστεί *αληθής* ή *ψευδής*.

Παράδειγμα 1.1. (i) Τα πιο κάτω είναι προτάσεις:

- (a) $1 + 1 = 2$ (αληθής)
- (b) $1 + 1 = 3$ (ψευδής)
- (c) Το κόκκινο είναι ένα από τα χρώματα (αληθής)
- (d) $\sqrt{2}$ είναι ρητός (ψευδής, όπως θα δείξουμε στην συνέχεια)
- (e) Κάθε θετικός ακέραιος ισούται με το άθροισμα των τετραγώνων δύο φυσικών αριθμών (ψευδής)

(ii) Τα πιο κάτω *δεν* είναι προτάσεις:

- (a) $2 + 3$
- (b) Από την Λευκωσία στην Λάρνακα
- (c) Τι ώρα είναι;
- (d) Ο ακέραιος x είναι θετικός

(iii) Είναι η φράση “Λέω ένα ψέμα” μια πρόταση; (Είναι δύσκολο να αποφασίσει κάποιος.)

Σημείωση. (i) Για να δείξουμε ότι δεν ισχύει η δήλωση στο Παράδειγμα 1.1(i)(e) αρκεί να βρούμε ένα μόνο *αντιπαράδειγμα* — δηλαδή ένα θετικό ακέραιο που δεν ισούται με το άθροισμα των τετραγώνων δύο φυσικών αριθμών. Ο αριθμός 3 είναι ένα τέτοιο αντιπαράδειγμα. Δεν χρειάζεται δηλαδή να θεωρήσουμε όλους τους θετικούς ακέραιους, μόνο ένα αντιπαράδειγμα είναι αρκετό.

(ii) Η δήλωση στο Παράδειγμα 1.1(ii)(d) *δεν* είναι πρόταση επειδή η τιμή αλήθειας της (αληθής ή ψευδής) δεν μπορεί να καθοριστεί πριν προσδιορίσουμε κάποια αριθμητική τιμή

στο x . Αν θέσουμε $x = 7$ (αντίστοιχα, $x = -1$) τότε η φράση μετατρέπεται σε πρόταση η οποία είναι αληθής (αντίστοιχα, ψευδής).

Μια και υπάρχουν φράσεις οι οποίες είναι προτάσεις σύμφωνα με τον ορισμό μας, προχωρούμε στο να εξετάσουμε τρόπους με τους οποίους μπορούμε να συνδέσουμε προτάσεις για να κατασκευάσουμε νέες προτάσεις:

Για την συζήτηση που ακολουθεί τα p και q συμβολίζουν προτάσεις.

ΑΡΝΗΣΗ: Χρησιμοποιούμε το σύμβολο $\sim$. Γράφουμε $\sim p$ για την άρνηση της πρότασης p , και διαβάζουμε “όχι p ”. Η άρνηση μετατρέπει μια αληθή πρόταση σε ψευδή και μια ψευδή πρόταση σε αληθή. Για παράδειγμα, η άρνηση της “ $1 + 1 = 2$ ” είναι “ $1 + 1 \neq 2$ ”, και η άρνηση της “ $\sqrt{2}$ είναι ρητός” είναι η “ $\sqrt{2}$ είναι άρρητος”.

ΣΥΖΕΥΞΗ: Χρησιμοποιούμε το σύμβολο $\wedge$. Γράφουμε $p \wedge q$ και διαβάζουμε “ p και q ”. Η πρόταση $p \wedge q$ είναι αληθής οποτεδήποτε οι προτάσεις p , q είναι και οι δύο αληθείς, και είναι ψευδής διαφορετικά. Για παράδειγμα, η πρόταση “ $2 + 2 = 4$ και $2 + 3 = 5$ ” είναι αληθής, ενώ η πρόταση “ $2 + 2 = 4$ και $\sqrt{2}$ είναι ρητός” είναι ψευδής.

ΔΙΑΖΕΥΞΗ: Χρησιμοποιούμε το σύμβολο $\vee$. Γράφουμε $p \vee q$ και διαβάζουμε “ p ή q ”. Η πρόταση $p \vee q$ είναι αληθής οποτεδήποτε τουλάχιστον μια από τις προτάσεις p , q είναι αληθής, και είναι ψευδής διαφορετικά. Για παράδειγμα, η πρόταση “ $2 + 2 = 4$ ή $\sqrt{2}$ είναι ρητός” είναι αληθής, ενώ η πρόταση “ $1 + 1 = 1$ ή $2 + 2 = 2$ ” είναι ψευδής.

ΣΥΝΕΠΑΓΩΓΗ: Χρησιμοποιούμε το σύμβολο $\rightarrow$. Γράφουμε $p \rightarrow q$ και διαβάζουμε “αν p τότε q ”. Η πρόταση $p \rightarrow q$ είναι ψευδής στην περίπτωση που η p είναι αληθής και η q είναι ψευδής, και είναι αληθής σε όλες τις άλλες περιπτώσεις. Για παράδειγμα, η πρόταση “αν $\sqrt{2}$ είναι άρρητος, τότε $2 + 2 = 4$ ” είναι αληθής όπως και η πρόταση “αν $\sqrt{2}$ είναι ρητός, τότε $2 + 2 \neq 4$ ”, ενώ η πρόταση “αν $\sqrt{2}$ είναι άρρητος, τότε $2 + 2 \neq 4$ ” είναι ψευδής.

ΙΣΟΔΥΝΑΜΙΑ: Χρησιμοποιούμε το σύμβολο $\leftrightarrow$. Γράφουμε $p \leftrightarrow q$ και διαβάζουμε “ p αν και μόνο αν q ”. Η πρόταση $p \leftrightarrow q$ είναι αληθής οποτεδήποτε οι προτάσεις p , q έχουν την ίδια τιμή αλήθειας, και είναι ψευδής διαφορετικά.

Τα πιο πάνω μπορούν να κωδικοποιηθούν στην μορφή ενός αληθοπίνακα. Με την βοήθεια τέτοιων πινάκων μπορούμε επίσης εύκολα να υπολογίσουμε την τιμή αλήθειας προτάσεων που προκύπτουν συνδέοντας διάφορες προτάσεις (και τις αρνήσεις τους).

p	q	$p \wedge q$	$p \vee q$	$\sim p$	$\sim q$	$p \rightarrow q$	$(\sim q) \rightarrow (\sim p)$	$(\sim p) \vee q$	$p \vee (\sim p)$	$q \rightarrow p$	$p \leftrightarrow q$
α	α	α	α	ψ	ψ	α	α	α	α	α	α
α	ψ	ψ	α	ψ	α	ψ	ψ	ψ	α	α	ψ
ψ	α	ψ	α	α	ψ	α	α	α	α	ψ	ψ
ψ	ψ	ψ	ψ	α	α	α	α	α	α	α	α

Παρατηρούμε ότι υπάρχουν προτάσεις (οι οποίες προκύπτουν από σύνδεση προτάσεων $p, q, r, \dots$) οι οποίες είναι πάντα αληθείς ανεξάρτητα από ποια τιμή αλήθειας παίρνουν οι προτάσεις $p, q, r, \dots$.

Θεώρημα 1.2. Έστω p, q, r προτάσεις. Οι πιο κάτω προτάσεις είναι πάντα αληθείς (ανεξάρτητα από την τιμή αλήθειας των p, q και r).

- (i) $p \vee (\sim p)$
- (ii) $(p \rightarrow q) \leftrightarrow ((\sim q) \rightarrow (\sim p))$
- (iii) $(p \rightarrow q) \leftrightarrow ((\sim p) \vee q)$
- (iv) $(\sim (p \wedge q)) \leftrightarrow ((\sim p) \vee (\sim q))$
- (v) $(\sim (p \vee q)) \leftrightarrow ((\sim p) \wedge (\sim q))$
- (vi) $(p \vee (q \wedge r)) \leftrightarrow ((p \vee q) \wedge (p \vee r))$
- (vii) $(p \wedge (q \vee r)) \leftrightarrow ((p \wedge q) \vee (p \wedge r))$
- (viii) $(p \leftrightarrow q) \leftrightarrow ((p \rightarrow q) \wedge (q \rightarrow p))$

Σημείωση. Τα (iv) και (v) στο πιο πάνω θεώρημα είναι γνωστά ως νόμοι De Morgan, από τον Augustus De Morgan (1806–1871). Τα (vi) και (viii) είναι γνωστά ως επιμεριστικοί νόμοι.

Απόδειξη. Τα (i), (ii) και (iii) προκύπτουν εύκολα από τον πιο πάνω αληθοπίνακα. Για το (vi) μπορούμε να χρησιμοποιήσουμε τον αληθοπίνακα πιο κάτω. Τα υπόλοιπα τα αφήνουμε ως άσκηση.

p	q	r	$q \wedge r$	$p \vee (q \wedge r)$	$p \vee q$	$p \vee r$	$(p \vee q) \wedge (p \vee r)$
α	α	α	α	α	α	α	α
α	α	ψ	ψ	α	α	α	α
α	ψ	α	ψ	α	α	α	α
α	ψ	ψ	ψ	α	α	α	α
ψ	α	α	α	α	α	α	α
ψ	α	ψ	ψ	ψ	α	ψ	ψ
ψ	ψ	α	ψ	ψ	ψ	α	ψ
ψ	ψ	ψ	ψ	ψ	ψ	ψ	ψ

□

Η παρατήρηση ότι οι προτάσεις $p \rightarrow q$ και $(\sim q) \rightarrow (\sim p)$ έχουν πάντα την ίδια τιμή αλήθειας είναι πολύ σημαντική:

Εις άτοπον απαγωγή (Reductio ad absurdum): Για να αποδείξουμε ότι η δήλωση q είναι αληθής, είναι κάποτε βολικό να υποθέσουμε ότι $\sim q$ είναι αληθής και να αποδείξουμε ότι τότε $\sim p$ είναι αληθής, όπου είναι γνωστό ότι p είναι αληθής. Η μέθοδος αυτή μπορεί να χρησιμοποιηθεί διότι οι τρεις προτάσεις $\sim q, (\sim q) \rightarrow (\sim p), p$ δεν μπορούν να είναι ταυτόχρονα αληθείς (κοιτάζτε τον αληθοπίνακα αμέσως πριν από το Θεώρημα 1.2).

Παραδείγματα 1.3. (i) Δίνεται ότι $x^2 \neq y^2$ όπου x, y είναι ακέραιοι αριθμοί. Για να αποδείξουμε ότι τότε $x \neq y$, υποθέτουμε ότι $x = y$. Όμως έχουμε ότι $x^2 = y^2$ οποτεδήποτε $x = y$, που είναι άτοπο.

(ii) Έστω x ένας ακέραιος αριθμός. Αν x^2 είναι άρτιος τότε x είναι άρτιος.

Απόδειξη: Υποθέτουμε ότι x^2 είναι άρτιος όπου ο ακέραιος x είναι περιττός. Έχουμε τότε ότι $x = 2m + 1$ για κάποιο ακέραιο m . Συνεπώς, έχουμε ότι $x^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$, όπου $2m^2 + 2m$ είναι ακέραιος. Συνάγουμε ότι x^2 είναι περιττός, που είναι άτοπο.

(iii) Θα αποδείξουμε ότι δεν υπάρχει ρητός α με την ιδιότητα $\alpha^2 = 2$: Έστω ότι υπάρχει τέτοιος ρητός αριθμός α . Τότε $\alpha = u/v$ όπου u είναι ακέραιος και v φυσικός. Μπορούμε να υποθέσουμε ότι έχουμε κάνει όλες τις δυνατές απλοποιήσεις στο κλάσμα u/v , δηλαδή ότι u και v δεν έχουν κοινούς θετικούς διαιρέτες εκτός από το 1. Επειδή $\alpha^2 = 2$, έχουμε $u^2 = 2v^2$. Από το (ii) πιο πάνω, ο u είναι άρτιος αφού ο u^2 είναι άρτιος. Συνεπώς $u = 2u_1$ για κάποιο ακέραιο u_1 . Έπεται ότι $4u_1^2 = 2v^2$. Συμπεραίνουμε ότι ο v^2 είναι άρτιος, και επομένως ο v είναι επίσης άρτιος. Έχουμε φτάσει σε άτοπο (ο ακέραιος 2 είναι κοινός διαιρέτης των u και v), δείχνοντας έτσι ότι δεν υπάρχει ρητός α με την ιδιότητα $\alpha^2 = 2$.

Σημείωση. (i) Στο Παράδειγμα 1.3(iii) θέλουμε να αποδείξουμε τον ισχυρισμό

s : Ο πραγματικός αριθμός $\sqrt{2}$ είναι άρρητος.

Για να το πετύχουμε αυτό έχουμε χρησιμοποιήσει την δήλωση (υπόθεση)

r : Ο μόνος κοινός θετικός διαιρέτης των u και v είναι ο ακέραιος 1.

Στην απόδειξη μας, έχουμε δείξει ότι η πρόταση $(\sim s) \rightarrow (\sim r)$ είναι αληθής ενώ στην υπόθεση μας έχουμε δεχθεί ότι και η πρόταση r είναι αληθής (πράγμα που μπορούσαμε να κάνουμε αφού οποιοδήποτε κλάσμα μπορεί να απλοποιηθεί στην μορφή αυτή απαλείφοντας πιθανούς κοινούς διαιρέτες του αριθμητή και παρονομαστή — θα επανέλθουμε στο σημείο αυτό στο Κεφάλαιο 9). Το συμπέρασμα ήταν ότι η $\sim s$ δεν μπορεί να είναι επίσης αληθής αφού, όπως έχουμε δει, οι τρεις προτάσεις $\sim s$, $(\sim s) \rightarrow (\sim r)$, r δεν μπορούν να είναι ταυτόχρονα αληθείς.

(ii) Αν α είναι το μήκος της διαγωνίου ενός τετραγώνου με πλευρά 1, τότε $\alpha^2 = 2$ και επομένως υπάρχει πραγματικός αριθμός α με την ιδιότητα $\alpha^2 = 2$. (Χρησιμοποιήσαμε εδώ την διαισθητική εικόνα που έχουμε για τους πραγματικούς αριθμούς ως σημεία κατά μήκος μιας ευθείας η οποία μπορεί να θεωρηθεί και ως ένας ιδεώδης κανόνας ο οποίος μπορεί να μετρά το μήκος ευθυγράμμων τμημάτων στην Ευκλείδεια γεωμετρία.) Στο Κεφάλαιο 7 θα δώσουμε μια εναλλακτική απόδειξη για την ύπαρξη πραγματικού αριθμού α με την ιδιότητα $\alpha^2 = 2$ χρησιμοποιώντας το αξίωμα της συνέχειας. Με παρόμοιο τρόπο μπορεί κάποιος να δείξει ότι για κάθε θετικό ακέραιο c και κάθε φυσικό αριθμό n μπορούμε να βρούμε μοναδικό θετικό πραγματικό αριθμό α με την ιδιότητα $\alpha^n = c$ (γράφουμε τότε $\alpha = \sqrt[n]{c}$, και στην περίπτωση που $n = 2$ συνήθως παραλείπουμε το n στον συμβολισμό αυτό).

Σε κάποιες περιπτώσεις έχουμε δηλώσει οι οποίες περιέχουν μια ή περισσότερες μεταβλητές x . Αυτές μπορεί να είναι αληθείς για ορισμένες τιμές του x και ψευδείς για άλλες. Τις

ονομάζουμε *προτασιακούς τύπους*. Γί' αυτό είναι σημαντικό να καθορίσουμε το πεδίο της συζήτησής μας, τον χώρο ή σύμπαν για το x (ποιοί δηλαδή είναι οι περιορισμοί για το x).

Παράδειγμα. Θεωρούμε τον προτασιακό τύπο “Ο θετικός ακέραιος n ισούται με το άθροισμα των τετραγώνων δύο φυσικών αριθμών.” Το πεδίο της συζήτησής μας στην περίπτωση αυτή είναι όλοι οι θετικοί ακέραιοι (φυσικοί) αριθμοί. Όπως έχουμε δει, αν θέσουμε $n = 3$ η πρόταση που προκύπτει είναι ψευδής. Αν όμως θέσουμε $n = 5$ η πρόταση που προκύπτει είναι αληθής αφού $5 = 2^2 + 1^2$. Ένα από τα πιο γνωστά αποτελέσματα σε αυτή την κατεύθυνση είναι το “θεώρημα των δύο τετραγώνων” του Fermat (κοιτάζτε επίσης τις Σημειώσεις και Σχόλια στο τέλος του κεφαλαίου).

1.2. Λογικές συνεπαγωγές

Πολύ συχνά, κατά την διάρκεια ενός μαθηματικού συλλογισμού προκύπτουν δύο δηλώσεις P και Q οι οποίες με κάποιο τρόπο “συνδέονται” μεταξύ τους. Οι δηλώσεις αυτές θα μπορούσαν για παράδειγμα να είναι προτάσεις ή προτασιακοί τύποι. Εξετάζουμε τέτοιες περιπτώσεις:

Ικανή συνθήκη: Λέμε ότι “η P είναι μια ικανή συνθήκη για την Q ” (συμβολισμός: $P \Rightarrow Q$) αν η Q είναι αληθής οποτεδήποτε η P είναι αληθής. Λέμε επίσης “ P συνεπάγεται την Q ” ή “ Q αν P ” ή “αν P , τότε Q ”. [Το τελευταίο (“αν P , τότε Q ”) δεν θα δημιουργεί σύγχυση σε σχέση με τον συμβολισμό της Παραγράφου 1.1 αφού, από το πλαίσιο της συζήτησής μας, θα είναι φανερό ότι αυτό που εννοούμε στην πραγματικότητα είναι “Αν η P είναι αληθής τότε και η Q είναι αληθής” με άλλα λόγια “αν ισχύει η P τότε ισχύει και η Q ”].

Στην περίπτωση που δεν ισχύει “ $P \Rightarrow Q$ ”, χρησιμοποιούμε τον συμβολισμό “ $P \not\Rightarrow Q$ ”.

Παράδειγμα. Μια απ’ ευθείας απόδειξη για το αποτέλεσμα στο Παράδειγμα 1.3(i) θα μπορούσε να ήταν η εξής: Έστω x, y ακέραιοι αριθμοί με $x^2 \neq y^2$. Όμως, $x^2 - y^2 \neq 0 \Rightarrow (x + y)(x - y) \neq 0 \Rightarrow x - y \neq 0 \Rightarrow x \neq y$.

Αναγκαία συνθήκη: Λέμε ότι “η P είναι μια αναγκαία συνθήκη για την Q ” αν Q συνεπάγεται την P . (Αυτό είναι το “αντίστροφο” του “ P συνεπάγεται την Q ”.) Λέμε επίσης “ Q μόνο αν P ”.

Ικανή και αναγκαία συνθήκη: Λέμε ότι “η P είναι μια ικανή και αναγκαία συνθήκη για την Q ” (συμβολισμός: $P \Leftrightarrow Q$) αν ισχύουν και τα δύο πιο πάνω, δηλαδή ισχύουν “ P συνεπάγεται την Q ” και “ Q συνεπάγεται την P ”. Λέμε επίσης “ P αν, και μόνο αν, Q ” και κάποτε γράφουμε πιο απλά “ P αν-ν Q ”. [Και πάλι δεν δημιουργείται σύγχυση σε σχέση με τον συμβολισμό της Παραγράφου 1.1 — συγκρίνετε με το αντίστοιχο σχόλιο πιο πάνω σχετικά με την ικανή συνθήκη.]

Σημειώσεις και παραδείγματα σε σχέση με τους πιο πάνω ορισμούς:

(1) Εξετάζουμε την περίπτωση που οι δηλώσεις P, Q είναι και οι δύο προτάσεις και, επιπλέον, ισχύει $P \Rightarrow Q$. Έχουμε τότε ότι η πρόταση $P \rightarrow Q$ είναι πάντα αληθής, ανεξάρτητα από την

τιμή αληθείας των P και Q . (Εξήγηση: Αν P είναι ψευδής, τότε $P \rightarrow Q$ είναι οπωσδήποτε αληθής. Αν P είναι αληθής, η υπόθεση μας ότι ισχύει $P \Rightarrow Q$ μας εξασφαλίζει ότι και η Q είναι αληθής.) Σε τέτοια περίπτωση αναφερόμαστε στην συνεπαγωγή ότι η πρόταση $P \rightarrow Q$ είναι πάντα αληθής ως μια λογική συνεπαγωγή. Αντίστροφα, αν P, Q είναι προτάσεις τέτοιες ώστε η πρόταση $P \rightarrow Q$ είναι πάντα αληθής, τότε ισχύει $P \Rightarrow Q$ και, σε τέτοια περίπτωση, η συνεπαγωγή $P \Rightarrow Q$ είναι επίσης μια λογική συνεπαγωγή.

Παράδειγμα. Έστω p, q και r προτάσεις. Εύκολα μπορούμε να ελέγξουμε ότι ισχύουν τα εξής: (i) $(p \wedge (p \rightarrow q)) \Rightarrow q$, και (ii) $((p \rightarrow q) \wedge (q \rightarrow r)) \Rightarrow (p \rightarrow r)$. Παρατηρούμε επίσης ότι η προτάσεις $(p \wedge (p \rightarrow q)) \rightarrow q$ και $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$ είναι πάντα αληθείς, ανεξάρτητα από την τιμή αληθείας των προτάσεων p, q και r .

(2) Έστω ότι P, Q είναι προτασιακοί τύποι. Όπως έχουμε δει, είναι πολύ σημαντικό να καθορίσουμε το πεδίο της συζήτησης μας (τις επιτρεπτές τιμές ή το σύμπαν) για κάθε μια από τις εμπλεκόμενες μεταβλητές. Στην περίπτωση αυτή, “ $P \Rightarrow Q$ ” σημαίνει “ $P(\cdot) \Rightarrow Q(\cdot)$ ” για όλες τις επιτρεπτές τιμές των εμπλεκόμενων μεταβλητών” το οποίο ισχύει αν, και μόνο αν, “η πρόταση $P(\cdot) \rightarrow Q(\cdot)$ είναι αληθής για όλες τις επιτρεπτές τιμές των εμπλεκόμενων μεταβλητών.”

Παραδείγματα. (i) Θέτουμε $P(= P(\Delta))$: “Το τρίγωνο Δ είναι ισόπλευρο” και $Q(= Q(\Delta))$: “Το τρίγωνο Δ είναι ισοσκελές” όπου το πεδίο της συζήτησης μας (το σύμπαν για την μεταβλητή Δ) είναι όλα τα τρίγωνα στο επίπεδο. Τώρα, από τον ορισμό, κάθε ισόπλευρο τρίγωνο είναι και ισοσκελές. Συνεπώς $P(\Delta) \Rightarrow Q(\Delta)$ για όλες τις επιτρεπτές τιμές της μεταβλητής Δ (έχουμε δηλαδή ότι $P(\Delta) \Rightarrow Q(\Delta)$ οποτεδήποτε Δ είναι ένα τρίγωνο στο επίπεδο). Μόλις έχουμε δείξει ότι $P \Rightarrow Q$.

Στην περίπτωση αυτή δεν ισχύει το αντίστροφο $Q \Rightarrow P$, έχουμε δηλαδή $Q \not\Rightarrow P$. [Εξήγηση: Επιλέγουμε ένα ορθογώνιο ισοσκελές τρίγωνο, έστω το Δ_1 , στο επίπεδο. Θέτοντας $\Delta = \Delta_1$, παρατηρούμε ότι η πρόταση $Q(\Delta_1)$ είναι αληθής ενώ η πρόταση $P(\Delta_1)$ είναι ψευδής. Αυτό δείχνει ότι P δεν είναι υποχρεωτικά αληθής οποτεδήποτε Q είναι αληθής.]

(ii) Θέτουμε $P(= P(x, y))$: “ x και y είναι και οι δύο άρτιοι” και $Q(= Q(x, y))$: “ $x+y$ είναι άρτιος”, όπου το σύμπαν και για τις δύο μεταβλητές x, y είναι όλοι οι ακέραιοι. Παρατηρούμε ότι $P \Rightarrow Q$. Έχουμε όμως ότι $Q \not\Rightarrow P$.

(iii) Θέτουμε $P(= P(x))$: “ $x^2 = 9$ ” και $Q(= Q(x))$: “ $2x = 6$ ”, όπου το σύμπαν για την μεταβλητή x είναι όλοι οι ακέραιοι. Προφανώς $P \not\Rightarrow Q$. Αν όμως το σύμπαν για την μεταβλητή x ήταν όλοι οι θετικοί ακέραιοι τότε ισχύει $P \Rightarrow Q$.

(3) Αν P, Q είναι και οι δύο προτάσεις και επιπλέον ισχύει $P \Leftrightarrow Q$ τότε η πρόταση $P \leftrightarrow Q$ είναι πάντα αληθής αφού προφανώς οι προτάσεις P και Q έχουν την ίδια τιμή αληθείας. Αντίστροφα, αν P, Q είναι προτάσεις τέτοιες ώστε $P \leftrightarrow Q$ είναι πάντα αληθής (ανεξάρτητα από την τιμή αληθείας των P, Q), τότε ισχύει $P \Leftrightarrow Q$.

(4) Έστω P, Q προτασιακοί τύποι. Παρατηρούμε τότε ότι $P \Leftrightarrow Q$ αν, και μόνο αν, η πρόταση $P(\cdot) \leftrightarrow Q(\cdot)$ είναι αληθής για κάθε μια από τις επιτρεπτές τιμές των εμπλεκόμενων μεταβλητών. (Προσδιορίζοντας συγκεκριμένες τιμές από το πεδίο της συζήτησης μας στις μεταβλητές, μετατρέπουμε τον προτασιακό τύπο σε πρόταση.)

Παραδείγματα. (i) Θεωρούμε τους προτασιακούς τύπους P, Q όπου $P (= P(x)) : “2x = 6”$ και $Q (= Q(x)) : “3x - 1 = 8”$, όπου το σύμπαν για την μεταβλητή x είναι και πάλι όλοι οι ακέραιοι. Εύκολα παρατηρούμε ότι στην περίπτωση αυτή ισχύει $P \Leftrightarrow Q$.

(ii) Θεωρούμε τους προτασιακούς τύπους P, Q όπου $P (= P(x)) : “2x = 6”$ και $Q (= Q(x)) : “x^2 = 9”$. Στην περίπτωση που το σύμπαν για την μεταβλητή x είναι όλοι οι φυσικοί (θετικοί ακέραιοι) ισχύει $P \Leftrightarrow Q$, ενώ στην περίπτωση που το σύμπαν για την μεταβλητή x είναι όλοι οι ακέραιοι, προφανώς δεν ισχύει $P \Leftrightarrow Q$.

Σημείωση. Όπως έχουμε δει, χρειάζεται μεγάλη προσοχή όταν χρησιμοποιούμε τα σύμβολα $\rightarrow$ και $\leftrightarrow$ μια και σημαίνουν διαφορετικά πράγματα. Στην περίπτωση όμως που έχουμε κάποιο **ορισμό** οι δύο αυτές έννοιες μπορούν να συναντηθούν. Για παράδειγμα, αν θέλουμε να δώσουμε ένα ορισμό για το “ισόπλευρο τρίγωνο” μπορούμε να γράψουμε: “Αν και οι τρεις πλευρές ενός τριγώνου έχουν το ίδιο μήκος, τότε το τρίγωνο αυτό καλείται ισόπλευρο.” Αυτό που κατανοούμε όμως είναι ότι αν ένα τρίγωνο έχει περιγραφεί ως ισόπλευρο, τότε θα πρέπει και οι τρεις πλευρές του να έχουν το ίδιο μήκος.

1.3. Πρωταρχικές έννοιες και αξιώματα

Στις αποδείξεις που είχαμε στις προηγούμενες παραγράφους του κεφαλαίου αυτού χρησιμοποιήσαμε διάφορες ιδιότητες των αριθμών, για παράδειγμα ότι κάθε κλάσμα μπορεί να απλοποιηθεί απαλείφοντας κοινούς παράγοντες. Η διαδικασία της εξέτασης των υποθέσεων που χρησιμοποιούμε “σιωπηρά” είναι πολύ σημαντική στα μαθηματικά, αφού για να τεκμηριώσουμε κάποιο βήμα ενός μαθηματικού συλλογισμού συχνά βασιζόμαστε σε άλλες πιο “βασικές” έννοιες και σχέσεις.

Για να αποφευχθεί ένας φαύλος κύκλος, η μόνη λύση είναι να αποδεχτούμε ορισμένες έννοιες και σχέσεις (όσο το δυνατόν λιγότερες) ως “πρωταρχικές” ή “θεμελιώδεις”, κρίνοντας έτσι ότι δεν χρειάζεται να τις καθορίσουμε επιπλέον. Παρόμοια, η απόδειξη μιας πρότασης χρησιμοποιεί άλλες προτάσεις και επομένως κάποιες “πρωταρχικές” ή “θεμελιώδεις” προτάσεις τις οποίες ονομάζουμε **αξιώματα** και δεχόμαστε χωρίς απόδειξη.

Κάποτε θεωρούνταν ότι οι βασικές υποθέσεις ή αξιώματα των μαθηματικών ήταν αληθείς δηλώσεις για τον πραγματικό κόσμο στον οποίο ζούμε. Η γεωμετρία του Ευκλείδη ήταν το πρότυπο και αποτελούσε το θεμέλιο της μαθηματικής εκπαίδευσης για πολλούς αιώνες (κοιτάξτε επίσης τις Σημειώσεις και Σχόλια στο τέλος του κεφαλαίου). Ο Ευκλείδης ξεκινά με αξιώματα, τα οποία θεωρούσε ως “αυταποδείκτες αλήθειες” και από αυτά συνήγαγε ένα τεράστιο αριθμό θεωρημάτων.

Ωστόσο, το σύστημα αξιωμάτων του Ευκλείδη είχε κάποιες αδυναμίες και ατέλειες τις οποίες οι μαθηματικοί του 19ου αιώνα αναγνώρισαν, προτείνοντας επίσης τρόπους με τους οποίους αυτές μπορούν να διορθωθούν (όπως για παράδειγμα ο μαθηματικός David Hilbert). Το θαυμαστό όμως είναι ότι ένα τόσο μεγάλο μέρος της δουλειάς του Ευκλείδη παραμένει απόλυτα έγκυρο μέχρι και σήμερα. Στην σύγχρονη παρουσίαση της Ευκλείδειας γεωμετρίας,

συνήθως, το σημείο θεωρείται ως πρωταρχική έννοια, ενώ οι πρωταρχικές σχέσεις περιλαμβάνουν την έννοια του μεταξύ (ένα σημείο μπορεί να βρίσκεται μεταξύ δύο άλλων σημείων) ή της ισότητας (για παράδειγμα, δύο ευθύγραμμα τμήματα μπορεί να έχουν το ίδιο μήκος).

Σήμερα θεωρούμε τα αξιώματα ως αφετηρίες που επιλέγουμε, ανάλογα με τον κλάδο των μαθηματικών που μελετάμε. Τα θεωρήματα που αποδεικνύουμε είναι αληθή σε οποιοδήποτε σύστημα ικανοποιεί τα αξιώματα αυτά. Είναι πολύ σημαντικό, ωστόσο, να μην παρεισφρήσουν στην θεωρία μας ή στους συλλογισμούς μας διάφορες “κρυφές υποθέσεις”. Για παράδειγμα, αν κάνουμε γεωμετρία, τα αξιώματα πιθανά να αναφέρονται σε σημεία και ευθείες. Θα πρέπει τότε, στην τελική μορφή της διατύπωσης μιας απόδειξης, να χρησιμοποιούμε μόνο τις ιδιότητες των σημείων και των ευθειών που καθορίζονται στα αξιώματα, αντί για την κοινή μας αντίληψη για το πως συμπεριφέρονται τα σημεία και οι ευθείες.

Κλείνουμε την παράγραφο αυτή με ένα απλό παράδειγμα. Ας υποθέσουμε ότι κάνουμε γεωμετρία χρησιμοποιώντας (εκτός από τις πρωταρχικές έννοιες του σημείου και της ευθείας) μόνο τα παρακάτω τρία αξιώματα της Ευκλείδειας γεωμετρίας (στην σύγχρονη τους διατύπωση):

(E1) Κάθε δύο σημεία βρίσκονται σε μία μοναδική ευθεία γραμμή.

(E2) Αν το σημείο P δεν βρίσκεται στην ευθεία L , τότε υπάρχει ακριβώς μία ευθεία L_1 που διέρχεται από το P και είναι παράλληλη προς την L .

(E3) Υπάρχουν τρία σημεία που δεν βρίσκονται στην ίδια ευθεία.

Χρησιμοποιούμε επίσης τον ορισμό ότι δύο ευθείες είναι παράλληλες εάν δεν υπάρχει κάποιο σημείο που να βρίσκεται και στις δύο.

Από αυτά τα αξιώματα, και τον ορισμό μας, μπορούμε να αποδείξουμε το εξής

Θεώρημα: Δύο ευθείες παράλληλες προς την ίδια ευθεία είναι παράλληλες μεταξύ τους.

Απόδειξη: Έστω L_1 και L_2 δύο (διακεκριμένες) ευθείες που είναι και οι δύο παράλληλες προς την L . Υποθέτουμε, με σκοπό να φτάσουμε σε άτοπο, ότι οι L_1 και L_2 δεν είναι παράλληλες. Τότε, έχουν ένα κοινό σημείο P , σύμφωνα με τον ορισμό μας. Αλλά τώρα υπάρχουν δύο ευθείες, οι L_1 και L_2 , που περιέχουν το P και είναι παράλληλες προς την L , γεγονός που αντιφάσκει με το Αξίωμα (E2).

Μπορείτε να αποδείξετε χρησιμοποιώντας μόνο τα πιο πάνω τρία αξιώματα (και ορισμό) ότι οποιεσδήποτε δύο (διακεκριμένες) ευθείες οι οποίες δεν είναι παράλληλες έχουν ακριβώς ένα κοινό σημείο;

Σημειώσεις και Σχόλια

1. Οι προτάσεις και οι λογικοί σύνδεσμοι χρησιμοποιούνται ευρέως στα μαθηματικά και την επιστήμη αλλά και πιο γενικά στην ανάλυση και επεξεργασία πληροφοριών. Στα πλαίσια μιας μαθηματικής απόδειξης, χρησιμοποιούνται για να δημιουργήσουν ακολουθίες συλλογισμών που αποδεικνύουν την αλήθεια μιας μαθηματικής πρότασης. Οι λογικοί συνδέσμοι μας επιτρέπουν να δημιουργήσουμε σύνθετες προτάσεις από απλές και να εφαρμόσουμε κανόνες συλλογισμού που μας βοηθούν να φτάσουμε στο ζητούμενο.

2. Το αποτέλεσμα ότι $\sqrt{2}$ είναι άρρητος απέδειξε ο Πυθαγόρας ή πιθανά κάποιος από τους μαθητές του. Σύμφωνα με ένα από τους πολλούς θρύλους σχετικά με το αποτέλεσμα αυτό, ο Ίππασος, από την σχολή του Πυθαγόρα, “τιμωρήθηκε από τους θεούς” διότι διέδιδε τα συνταρακτικά, για την εποχή, νέα ότι υπάρχουν “άρρητοι αριθμοί”.

3. Ο Ευκλείδης (περίπου 330-270 π.Χ.) ήταν ένας σπουδαίος αρχαίος Έλληνας μαθηματικός. Το πιο σημαντικό από τα βιβλία του είναι τα “Στοιχεία” που είναι ένα από τα δημοφιλέστερα βιβλία μαθηματικών στον κόσμο. Αποτελείται από δεκατρείς τόμους οι έξι πρώτοι από τους οποίους είναι αφιερωμένοι στη γεωμετρία. Το έργο αυτό θεωρείται εξαιρετικά σημαντικό αφού ο Ευκλείδης συγχέντρωσε και οργάνωσε τις γνώσεις της γεωμετρίας της εποχής του σε ένα καλά δομημένο σύστημα αξιωμάτων και αποδείξεων, θέτοντας τις βάσεις για την μελέτη της γεωμετρίας για πολλούς αιώνες. Επέμεινε στην χρήση αυστηρά τεκμηριωμένων συλλογισμών στις αποδείξεις των θεωρημάτων του με τα πρότυπα αυτά να εξακολουθούν να ισχύουν στον τομέα των μαθηματικών μέχρι και σήμερα.

4. Το “θεώρημα των δύο τετραγώνων” του Fermat δηλώνει ότι ένας περιττός πρώτος p είναι το άθροισμα δύο τετραγώνων, $p = a^2 + b^2$, όπου a, b είναι ακέραιοι αν, και μόνο αν, $p = 4m + 1$ για κάποιο ακέραιο m . Η πρώτη δημοσιευμένη απόδειξη του αποτελέσματος αυτού είναι από τον Euler. Ο Gauss απέδειξε ότι υπάρχει μοναδικό ζεύγος φυσικών a, b με $p = a^2 + b^2$. Θα ξανασυναντήσουμε το θεώρημα αυτό στο Κεφάλαιο 17 στο πλαίσιο της συζήτησης μας σχετικά με Ευκλείδειες περιοχές.

Ασκήσεις

1.1 Ποιά από τα πιο κάτω είναι προτάσεις;

- (i) Ο ακέραιος αριθμός 35 είναι άρτιος
- (ii) Ποιός απέδειξε το τελευταίο θεώρημα του Fermat;
- (iii) Αν x είναι ένας ακέραιος τέτοιος ώστε $x + 2$ είναι θετικός, τότε ο ακέραιος $x + 5$ είναι επίσης θετικός
- (iv) Ο Αρχιμήδης είχε μια τσιπούρα για δείπνο στα εικοστά του γενέθλια

1.2 Συμπληρώστε την απόδειξη του Θεωρήματος 1.2.

1.3 Δείξτε ότι ο πραγματικός αριθμός $\sqrt{3}$ είναι άρρητος.

1.4 Δείξτε ότι δεν υπάρχουν ρητοί r, s τέτοιοι ώστε $\sqrt{3} = r + s\sqrt{2}$.

1.5 Έστω a, a' και b πραγματικοί αριθμοί. Αν a, a' είναι ρητοί και b είναι άρρητος, δείξτε ότι: (i) $a + a'$ είναι ρητός, (ii) aa' είναι ρητός, (iii) $a + b$ είναι άρρητος, (iv) αν $a \neq 0$, τότε ab είναι άρρητος.

1.6 Έστω p, q, r προτάσεις. Εξετάστε κατά πόσον οι πιο κάτω προτάσεις είναι πάντα αληθείς (ανεξάρτητα από την τιμή αλήθειας των p, q και r).

- (i) $((p \vee q) \wedge r) \leftrightarrow (p \vee (q \wedge r))$
- (ii) $((\sim p) \wedge q) \leftrightarrow (p \vee (\sim q))$
- (iii) $((p \vee q) \vee r) \leftrightarrow (p \vee (q \vee r))$
- (iv) $((p \wedge q) \wedge r) \leftrightarrow (p \wedge (q \wedge r))$

1.7 Εξετάστε πιο από τα πιο κάτω ισχύει

- (a) $P \Leftrightarrow Q$
- (b) $P \Rightarrow Q, Q \neq P$
- (c) $Q \Rightarrow P, P \neq Q$
- (d) $P \neq Q, Q \neq P$

στις περιπτώσεις:

- (i) P : Το τρίγωνο Δ είναι ισόπλευρο
 Q : Το τρίγωνο Δ έχει όλες τις γωνίες του ίσες
- (ii) P : Το τρίγωνο Δ είναι ισόπλευρο
 Q : Το τρίγωνο Δ είναι ισοσκελές

(iii) P : Το τετράπλευρο Γ είναι ένα τετράγωνο

Q : Το τετράπλευρο Γ είναι ένας ρόμβος

(iv) P : Το τετράπλευρο Γ είναι ισόπλευρο

Q : Το τετράπλευρο Γ έχει όλες τις γωνίες του ίσες

(v) P : Το τετράπλευρο Γ είναι ένα ορθογώνιο

Q : Το τετράπλευρο Γ έχει όλες τις γωνίες του ίσες

όπου το σύμπαν για την μεταβλητή Δ (αντίστοιχα, για την μεταβλητή Γ) είναι όλα τα τρίγωνα (αντίστοιχα, τετράπλευρα) στο επίπεδο.

- 1.8 Εξετάστε κατά πόσον είναι σωστός ο ισχυρισμός: “Αν n είναι ένας πρώτος αριθμός, τότε ο ακέραιος $2^n - 1$ είναι επίσης πρώτος αριθμός.” [Λέμε ότι ο ακέραιος p είναι πρώτος αν (i) $p > 1$ και (ii) p δεν έχει άλλους θετικούς διαιρέτες εκτός από τους 1 και p .]

- 1.9 Έστω p, q, r, s και t προτάσεις. Συμπληρώστε τους συλλογισμούς σε κάθε ένα από τα βήματα (i)–(viii) της απόδειξης του πιο κάτω θεωρήματος:

$$\left((p \wedge (p \rightarrow q)) \wedge ((s \vee r) \wedge (r \rightarrow (\sim q))) \right) \Rightarrow (s \vee t)$$

Βήματα:

- (i) p , (ii) $p \rightarrow q$, (iii) q , (iv) $r \rightarrow (\sim q)$, (v) $q \rightarrow (\sim r)$, (vi) $\sim r$,
(vii) $s \vee r$, (viii) s , (viii) άρα, $s \vee t$.

2. Σύνολα

2.1. Εισαγωγικά σχόλια και ορισμοί

Το 1895 στην εργασία του “Beiträge zur Begründung der transfiniten Mengenlehre” ο Georg Cantor έδωσε τον ακόλουθο ορισμό: “Σύνολο είναι μια συλλογή από διακεκριμένα αντικείμενα τα οποία ονομάζονται στοιχεία του συνόλου.” (Τα στοιχεία αυτά μπορούν να είναι αριθμοί, γράμματα, λέξεις, αντικείμενα ή οποιαδήποτε άλλη μαθηματική έννοια.)

Ίσως να προκαλεί έκπληξη ότι από ένα τόσο απλό ορισμό μπορεί να προκύψουν αντιφάσεις. Ο ίδιος ο Cantor το είχε αντιληφθεί αυτό, όμως το πιο γνωστό παράδειγμα διατυπώθηκε από τον φιλόσοφο και μαθηματικό Bertrand Russell και είναι γνωστό ως το παράδοξο του Russell. (Κοιτάξτε επίσης τις Σημειώσεις και Σχόλια στο τέλος του Κεφαλαίου 2.)

Για να αποφύγουμε τέτοιου είδους αντιφάσεις, συνήθως στις συζητήσεις στο βιβλίο αυτό θα σταθεροποιούμε ένα σύμπαν ή χώρο $\mathcal{U}$ (καθολικό σύνολο) και θα θεωρούμε μόνο σύνολα τα στοιχεία των οποίων είναι στοιχεία του $\mathcal{U}$, ή σύνολα (συλλογές) τα στοιχεία των οποίων είναι υποσύνολα του $\mathcal{U}$, ή σύνολα (οικογένειες) τα στοιχεία των οποίων είναι συλλογές υποσυνόλων του $\mathcal{U}$ κ.ο.κ.

Ένα σύνολο καθορίζεται πλήρως όταν ξέρουμε όλα τα στοιχεία του, γι’ αυτό είναι πολύ σημαντικό να μπορούμε να αποφασίσουμε κατά πόσον ένα συγκεκριμένο στοιχείο ανήκει ή όχι στο σύνολο που μας ενδιαφέρει.

Αν x είναι στοιχείο του συνόλου A , αυτό το συμβολίζουμε με $x \in A$, λέμε επίσης ότι x ανήκει στο σύνολο A . Όταν το x δεν ανήκει στο A , γράφουμε $x \notin A$.

Υπάρχουν τρεις κυρίως τρόποι για να περιγραφεί ένα σύνολο:

- (i) Με αναγραφή των στοιχείων του, για παράδειγμα $A = \{1, 2, 3\}$.
- (ii) Με αναγραφή αρκετών στοιχείων του συνόλου (όχι όλων), έτσι ώστε να γίνει σαφής η ιδιότητα που χαρακτηρίζει τα στοιχεία. Για παράδειγμα, $\{1, 2, 3, \dots, n\}$ είναι μια περιγραφή του συνόλου των πρώτων n φυσικών αριθμών ενώ $\{1, 2, 3, \dots, n, \dots\}$ είναι μια περιγραφή του συνόλου όλων των φυσικών αριθμών.
- (iii) Με περιγραφή των στοιχείων του: Αν $p(x)$ είναι μια ιδιότητα (προτασιακός τύπος), τότε μπορούμε να θεωρήσουμε το σύνολο P που απαρτίζεται από όλα τα αντικείμενα (και μόνο αυτά) που ικανοποιούν αυτή την ιδιότητα. Εδώ είναι σημαντικό να καθορίσουμε το σύμπαν (καθολικό σύνολο) $\mathcal{U}$ στο οποίο όλα τα x πρέπει να ανήκουν.

Γράφουμε $P = \{x: x \in \mathcal{U} \text{ και } p(x) \text{ είναι αληθής}\}$, ή $P = \{x \in \mathcal{U}: p(x) \text{ είναι αληθής}\}$, ή πιο απλά $P = \{x: p(x)\}$.

Το σύνολο που δεν περιέχει οποιοδήποτε στοιχείο ονομάζεται *κενό σύνολο* και το συμβολίζουμε με $\emptyset$. (Έχουμε δηλαδή ότι $\emptyset = \{x \in \mathcal{U}: p(x) \wedge (\sim p(x)) \text{ είναι αληθής}\}$ όπου $p(x)$ είναι μια ιδιότητα.)

Σημείωση. Ορισμένα σύνολα έχουν σταθερά σύμβολα, για παράδειγμα:

- (i) $\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$, το σύνολο των φυσικών αριθμών
- (ii) $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$, το σύνολο των ακεραίων
- (iii) $\mathbb{Q} = \{p/q: p \in \mathbb{Z} \text{ και } q \in \mathbb{N}\}$, το σύνολο των ρητών αριθμών
- (iv) $\mathbb{R}$, το σύνολο των πραγματικών αριθμών
- (v) $\mathbb{C}$, το σύνολο των μιγαδικών αριθμών

Έστω A ένα μη-κενό σύνολο. Λέμε ότι το A είναι *πεπερασμένο* αν έχει ακριβώς n στοιχεία για κάποιο $n \in \mathbb{N}$. Διαφορετικά λέμε ότι το A είναι *άπειρο*. Το κενό σύνολο — κατά συνθήκη — θεωρείται ως πεπερασμένο.

- Παραδείγματα.** (i) $S_1 = \{x: x \in \mathbb{N} \text{ και } -2 < x < 2\} (= \{x \in \mathbb{N}: -2 < x < 2\}) = \{1\}$
(ii) $S_2 = \{x: x \in \mathbb{Z} \text{ και } -2 < x < 2\} = \{-1, 0, 1\}$
(iii) $S_3 = \{x: x \in \mathbb{N} \text{ και } -1 < x < 1\} = \emptyset$
(iv) $S_4 = \{0, \pm 2, \pm 4, \dots\} = \{x: x \text{ είναι άρτιος ακέραιος αριθμός}\} = \{2k: k \in \mathbb{Z}\}$

Τα σύνολα S_1 , S_2 και S_3 είναι πεπερασμένα, ενώ το σύνολο S_4 είναι άπειρο.

Ορισμός. Λέμε ότι το σύνολο P είναι *υποσύνολο* ενός άλλου συνόλου Q , και γράφουμε $P \subseteq Q$, όταν κάθε στοιχείο του P είναι και στοιχείο του Q .

Δύο σύνολα P , Q λέγονται *ίσα* (συμβολισμός: $P = Q$) όταν περιέχουν τα ίδια ακριβώς στοιχεία. Γράφουμε $P \neq Q$ όταν τα σύνολα P , Q δεν είναι ίσα.

Όταν $P \subseteq Q$ και $P \neq Q$, τότε P λέγεται *γνήσιο υποσύνολο* του Q (συμβολισμός: $P \subsetneq Q$).

Σημείωση. Παρατηρούμε ότι $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$.

Πρόταση 2.1. Αν A , B , C είναι υποσύνολα ενός καθολικού συνόλου $\mathcal{U}$, ισχύουν τα ακόλουθα:

- (i) $A \subseteq A$, $\emptyset \subseteq A$, $A \subseteq \mathcal{U}$,
- (ii) αν $A \subseteq B$ και $B \subseteq A$ τότε $A = B$,
- (iii) αν $A \subseteq B$ και $B \subseteq C$ τότε $A \subseteq C$.

Απόδειξη. Θα δείξουμε ότι $\emptyset \subseteq A$. (Τα υπόλοιπα τα αφήνουμε ως άσκηση.) Υποθέτουμε ότι $\emptyset$ δεν αποτελεί υποσύνολο του A . Επομένως το $\emptyset$ περιέχει κάποιο στοιχείο το οποίο δεν ανήκει στο A . Έχουμε φτάσει σε άτοπο αφού το $\emptyset$ δεν περιέχει στοιχεία. $\square$

Σημείωση. Χρησιμοποιώντας την Πρόταση 2.1, μπορούμε όμως να δείξουμε ότι υπάρχει μόνο ένα κενό σύνολο: Έστω $\emptyset_1$ κάποιο άλλο κενό σύνολο. Αφού $\emptyset$ είναι κενό, έχουμε ότι $\emptyset \subseteq \emptyset_1$. Αφού $\emptyset_1$ είναι κενό, έχουμε επίσης ότι $\emptyset_1 \subseteq \emptyset$. Έπεται ότι $\emptyset = \emptyset_1$. Επομένως μπορούμε να μιλούμε για το (μοναδικό) κενό σύνολο.

Ορισμός. Το σύνολο με στοιχεία τα υποσύνολα ενός συνόλου S λέγεται *δυναμοσύνολο* του S και συμβολίζεται με $\mathcal{P}(S)$.

Παράδειγμα. Έστω $S = \{1, 2\}$. Τότε $\mathcal{P}(S) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

2.2. Καρτεσιανά γινόμενα

Έστω A, B δύο σύνολα. Το σύμβολο (a, b) με $a \in A$ και $b \in B$ καλείται *διατεταγμένο ζεύγος* με *πρώτη συντεταγμένη* το a και *δεύτερη συντεταγμένη* το b .

Αν (a, b) και (a', b') είναι δύο διατεταγμένα ζεύγη (όπου $a, a' \in A$ και $b, b' \in B$), τότε $(a, b) = (a', b')$ αν, και μόνο αν, $a = a'$ και $b = b'$.

Το καρτεσιανό γινόμενο των συνόλων A και B είναι το σύνολο με στοιχεία τα διατεταγμένα ζεύγη (a, b) όπου $a \in A$ και $b \in B$, και συμβολίζεται με $A \times B$. Έχουμε δηλαδή $A \times B = \{(a, b) : a \in A \text{ και } b \in B\}$.

Το καρτεσιανό γινόμενο ονομάστηκε από τον René Descartes ο οποίος είχε αντιληφθεί ότι το Ευκλείδειο επίπεδο είναι “ουσιαστικά το ίδιο” με το σύνολο $\mathbb{R} \times \mathbb{R}$.

Παράδειγμα 2.2. Έστω $A = \{1, 2, 3\}$ και $B = \{\alpha, \beta\}$. Τότε $A \times B = \{(1, \alpha), (1, \beta), (2, \alpha), (2, \beta), (3, \alpha), (3, \beta)\}$ και $B \times A = \{(\alpha, 1), (\alpha, 2), (\alpha, 3), (\beta, 1), (\beta, 2), (\beta, 3)\}$.

Σημείωση 2.3. Οι πιο πάνω ορισμοί μπορούν να επεκταθούν στην περίπτωση που έχουμε n (όπου $n \geq 2$) σύνολα $A_1, \dots, A_n$ και μπορούμε με αυτό τον τρόπο να ορίσουμε το καρτεσιανό γινόμενο $A_1 \times \dots \times A_n$.

Αν $A_1, \dots, A_n$ είναι σύνολα, τότε το σύμβολο $(\alpha_1, \dots, \alpha_n)$ με $\alpha_1 \in A_1, \dots, \alpha_n \in A_n$ καλείται *διατεταγμένη n -άδα* με *i -συντεταγμένη* το α_i για $1 \leq i \leq n$.

Αν $(\alpha_1, \dots, \alpha_n)$ και $(\alpha'_1, \dots, \alpha'_n)$ είναι διατεταγμένες n -άδες (όπου $\alpha_1, \alpha'_1 \in A_1, \dots, \alpha_n, \alpha'_n \in A_n$) τότε $(\alpha_1, \dots, \alpha_n) = (\alpha'_1, \dots, \alpha'_n)$ αν, και μόνο αν $\alpha_1 = \alpha'_1, \dots, \alpha_n = \alpha'_n$.

Γράφουμε $A_1 \times \dots \times A_n = \{(\alpha_1, \dots, \alpha_n) : \alpha_1 \in A_1, \dots, \alpha_n \in A_n\}$. Το σύνολο $A_1 \times \dots \times A_n$ καλείται το *καρτεσιανό γινόμενο των συνόλων $A_1, \dots, A_n$* .

Στην περίπτωση που $A_i = A$ για $1 \leq i \leq n$, συνήθως γράφουμε A^n αντί για $A_1 \times \dots \times A_n$.

Σημείωση 2.4. Έστω X, Y, Z μη-κενά σύνολα. Τότε τα σύνολα $X \times (Y \times Z)$ και $(X \times Y) \times Z$ είναι διαφορετικά, όμως υπάρχει μια φυσιολογική αντιστοιχία μεταξύ του κάθε ενός από αυτά και του συνόλου $X \times Y \times Z$.

2.3. Η άλγεβρα Boole των συνόλων

Θα εξετάσουμε τρόπους με τους οποίους σύνολα μπορούν να συνδυαστούν μεταξύ τους και να δημιουργήσουν νέα σύνολα. Για ολόκληρη την συζήτηση που ακολουθεί σταθεροποιούμε

ένα δοσμένο σύνολο $\mathcal{U}$ (καθολικό σύνολο) και θεωρούμε το δυναμοσύνολο $\mathcal{P}(\mathcal{U})$. Πιο ειδικά, όλα τα σύνολα που θα εμφανιστούν στην συζήτηση αυτή θα είναι υποσύνολα του $\mathcal{U}$.

Υποθέτουμε τώρα ότι οι ιδιότητες $p(x)$, $q(x)$ σχετίζονται αντίστοιχα με τα σύνολα P , Q (ως προς το σύμπαν $\mathcal{U}$) δηλαδή $P(x) = \{x: p(x)\}$ και $Q(x) = \{x: q(x)\}$.

Ορισμός. Ορίζουμε

- (i) την τομή $P \cap Q = \{x: p(x) \wedge q(x)\}$
- (ii) την ένωση $P \cup Q = \{x: p(x) \vee q(x)\}$
- (iii) το συμπλήρωμα $P' = \{x: \sim p(x)\}$
- (iv) την διαφορά $P - Q = \{x: p(x) \wedge (\sim q(x))\}$

Τα πιο πάνω είναι επίσης σύνολα τα οποία ανήκουν στο δυναμοσύνολο $\mathcal{P}(\mathcal{U})$.

Δεν είναι δύσκολο να δούμε ότι

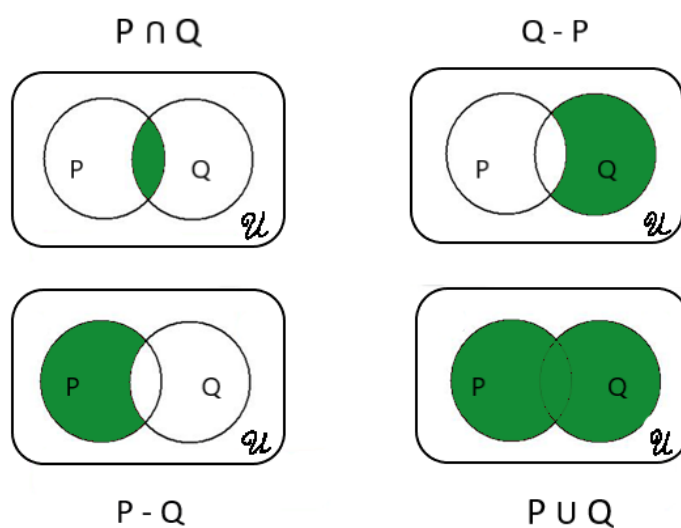
- (i) $P \cap Q = \{x: x \in P \text{ και } x \in Q\}$
- (ii) $P \cup Q = \{x: x \in P \text{ ή } x \in Q\}$
- (iii) $P' = \{x: x \notin P\}$
- (iv) $P - Q = \{x: x \in P \text{ και } x \notin Q\}$

Σημείωση. (i) Αν $\mathcal{U}$ είναι το καθολικό σύνολο και $P \subseteq \mathcal{U}$, τότε $P' = \mathcal{U} - P$. Στην ειδική περίπτωση που $\mathcal{U} = \mathbb{R}$ και $P = \mathbb{Q}$, έχουμε ότι $\mathbb{R} - \mathbb{Q}$ είναι ακριβώς το σύνολο των άρρητων αριθμών.

(ii) Το κενό σύνολο $\emptyset$ και το καθολικό σύνολο $\mathcal{U}$ έχουν πολύ ξεχωριστούς ρόλους αφού παρατηρούμε, ως άμεση συνέπεια των πιο πάνω ορισμών, ότι οποτεδήποτε $A \subseteq \mathcal{U}$ ισχύουν

(a) $A \cup \emptyset = A$, (b) $A \cap \emptyset = \emptyset$, (c) $A \cup \mathcal{U} = \mathcal{U}$, (d) $A \cap \mathcal{U} = A$.

(Συγκρίνετε με την συζήτηση στο Κεφάλαιο 4.)



Σχήμα 1: Διαγράμματα του Venn για ένωση, τομή και διαφορά. Κοιτάξτε επίσης τις Σημειώσεις και Σχόλια στο τέλος του κεφαλαίου.

Αν $A, B \subseteq \mathcal{U}$ με $A \cap B = \emptyset$, τότε λέμε ότι τα σύνολα A, B είναι ξένα μεταξύ τους. Μια συλλογή $\mathcal{C}$ υποσυνόλων του $\mathcal{U}$ καλείται μια συλλογή συνόλων ξένων μεταξύ τους ή μια συλλογή συνόλων ξένων ανά δύο μεταξύ τους αν οποιαδήποτε δύο σύνολα στην $\mathcal{C}$ είναι ξένα μεταξύ τους.

Στην πιο κάτω πρόταση συμπεριλαμβάνουμε κάποιες στοιχειώδεις ιδιότητες της ένωσης, τομής και συμπληρώματος.

Πρόταση 2.5. Αν A, B και C είναι υποσύνολα του σύμπαντος $\mathcal{U}$, ισχύουν τα ακόλουθα:

- (i) $A \cup B = B \cup A$
- (ii) $A \cup (B \cap C) = (A \cup B) \cap C$
- (iii) $A \subseteq B$ αν, και μόνο αν, $A \cup B = B$
- (iv) $A \cap B = B \cap A$
- (v) $A \cap (B \cap C) = (A \cap B) \cap C$
- (vi) $(A \cap B)' = A' \cup B'$
- (vii) $(A \cup B)' = A' \cap B'$
- (viii) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- (ix) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Απόδειξη. Θα αποδείξουμε το (vii): Θα αποδείξουμε πρώτα ότι $(A \cup B)' \subseteq A' \cap B'$: Έστω $x \in (A \cup B)'$. Τότε $x \notin A \cup B$. Άρα $x \notin A$ και $x \notin B$. Δηλαδή $x \in A'$ και $x \in B'$. Άρα $x \in A' \cap B'$.

Για να αποδείξουμε τώρα ότι $A' \cap B' \subseteq (A \cup B)'$: Έστω $x \in A' \cap B'$. Αυτό σημαίνει ότι $x \in A'$ και $x \in B'$. Δηλαδή $x \notin A$ και $x \notin B$. Άρα $x \notin A \cup B$, δηλαδή $x \in (A \cup B)'$.

Τα υπόλοιπα τα αφήνουμε ως άσκηση. □

Σημείωση. Συγκρίνοντας με το σχόλιο κάτω από το Θεώρημα 1.2, θα αναφερόμαστε στα (vi) και (vii) στην πιο πάνω πρόταση ως νόμους De Morgan, και στα (viii) και (ix) ως επιμεριστικούς νόμους.

Η παρατήρηση ότι $(A \cap B) \cap C = A \cap (B \cap C)$ μας οδηγεί στον ορισμό του συνόλου $A \cap B \cap C$ ως το σύνολο όλων των στοιχείων του $\mathcal{U}$ που ανήκουν στο κάθε ένα από τα σύνολα A, B και C . Προφανώς $A \cap B \cap C = (A \cap B) \cap C = A \cap (B \cap C)$.

Παρόμοια, ορίζουμε το σύνολο $A \cup B \cup C$ ως το σύνολο όλων των στοιχείων του $\mathcal{U}$ που ανήκουν σε τουλάχιστον ένα από τα A, B, C . Έχουμε τότε $A \cup B \cup C = (A \cup B) \cup C = A \cup (B \cup C)$.

Οι ορισμοί αυτοί μπορούν να επεκταθούν στην περίπτωση που έχουμε μια τυχαία (όχι υποχρεωτικά πεπερασμένη) συλλογή $\mathcal{C}$ υποσυνόλων του $\mathcal{U}$:

Ορίζουμε την τομή της συλλογής $\mathcal{C}$ (συμβολισμός: $\cap_{A \in \mathcal{C}} A$ ή $\cap\{A: A \in \mathcal{C}\}$) ως το σύνολο όλων των στοιχείων του $\mathcal{U}$ με την ιδιότητα ότι ανήκουν σε κάθε μέλος της $\mathcal{C}$.

Ορίζουμε την ένωση της συλλογής $\mathcal{C}$ (συμβολισμός: $\cup_{A \in \mathcal{C}} A$ ή $\cup\{A: A \in \mathcal{C}\}$) ως το σύνολο όλων των στοιχείων του $\mathcal{U}$ με την ιδιότητα ότι ανήκουν σε τουλάχιστον ένα από τα μέλη της $\mathcal{C}$.

Στην περίπτωση που η συλλογή $\mathcal{C}$ είναι κενή προφανώς η ένωση της συλλογής είναι το κενό σύνολο και η τομή της ολόκληρο το σύνολο $\mathcal{U}$.

Οι νόμοι του De Morgan και οι επιμεριστικοί νόμοι εξακολουθούν να ισχύουν για τυχαίες ενώσεις και τομές: Έχουμε δηλαδή ότι αν $\mathcal{C} \subseteq \mathcal{P}(\mathcal{U})$ και $B \subseteq \mathcal{U}$, ισχύουν

$$\begin{aligned}(\cup_{A \in \mathcal{C}} A)' &= \cap_{A \in \mathcal{C}} A', & (\cap_{A \in \mathcal{C}} A)' &= \cup_{A \in \mathcal{C}} A', \\ B \cap (\cup_{A \in \mathcal{C}} A) &= \cup_{A \in \mathcal{C}} (B \cap A), & B \cup (\cap_{A \in \mathcal{C}} A) &= \cap_{A \in \mathcal{C}} (B \cup A).\end{aligned}$$

Σημείωση. Στην περίπτωση που $\mathcal{C}$ είναι μια πεπερασμένη συλλογή υποσυνόλων του $\mathcal{U}$, έστω $\mathcal{C} = \{A_1, \dots, A_n\}$, συνήθως γράφουμε $\cap_{i=1}^n A_i$ ή $A_1 \cap A_2 \cap \dots \cap A_n$ αντί για $\cap_{A \in \mathcal{C}} A$. Παρόμοια, στην θέση του $\cup_{A \in \mathcal{C}} A$, συνήθως χρησιμοποιούμε τους συμβολισμούς $\cup_{i=1}^n A_i$ ή $A_1 \cup A_2 \cup \dots \cup A_n$. Ανακύπτει τώρα το εξής ερώτημα αν εξετάσουμε για παράδειγμα την περίπτωση $n = 4$. Είναι τα σύνολα $A_1 \cup A_2 \cup A_3 \cup A_4$, $(A_1 \cup A_2) \cup (A_3 \cup A_4)$ και $((A_1 \cup A_2) \cup A_3) \cup A_4$ ίσα; Επίσης, τι συμβαίνει στην περίπτωση που $n > 4$ ή αν αντικαταστήσουμε την ένωση υποσυνόλων με την τομή υποσυνόλων; (Κοιτάξτε επίσης τις Ασκήσεις 2.7–2.13.) Θα μελετήσουμε σε ένα πιο γενικό πλαίσιο τέτοιου είδους ερωτήματα στα Κεφάλαια 4 και 5.

Μια συλλογή $\mathcal{B}$ υποσυνόλων του $\mathcal{U}$ καλείται *άλγεβρα Boole* αν (i) $A \cup B$ ανήκει στην $\mathcal{B}$ οποτεδήποτε τα A, B ανήκουν στην $\mathcal{B}$, και (ii) A' ανήκει στην $\mathcal{B}$ οποτεδήποτε το A ανήκει στην $\mathcal{B}$. Έπεται τώρα, από τους νόμους De Morgan, ότι $A \cap B$ ανήκει στην $\mathcal{B}$ οποτεδήποτε τα A και B ανήκουν στην $\mathcal{B}$. Προφανώς το δυναμοσύνολο $\mathcal{P}(\mathcal{U})$ αποτελεί μια άλγεβρα Boole.

Αφήνουμε την απόδειξη της επόμενης πρότασης ως άσκηση.

Πρόταση 2.6. Έστω $\mathcal{B}$ μια συλλογή υποσυνόλων του $\mathcal{U}$. Υποθέτουμε, επιπλέον, ότι $\mathcal{B}$ είναι μια άλγεβρα Boole. Αν $A_1, A_2, \dots, A_n$ είναι σύνολα στην συλλογή $\mathcal{B}$, τότε τα σύνολα $A_1 \cap A_2 \cap \dots \cap A_n$ και $A_1 \cup A_2 \cup \dots \cup A_n$ επίσης ανήκουν στην $\mathcal{B}$.

2.4. Ποσοδείκτες

Για τους ποσοδείκτες θεωρούμε ότι $p(x)$ είναι μια ιδιότητα (προτασιακός τύπος) όπου το x ανήκει σε ένα καθολικό σύνολο (σύμπαν) $\mathcal{U}$.

Καθολικός ποσοδείκτης: Χρησιμοποιούμε το σύμβολο $\forall$ (για κάθε). Γράφουμε $\forall_x p(x)$. Η $\forall_x p(x)$ είναι αληθής αν και μόνο αν για κάθε $x \in \mathcal{U}$, η $p(x)$ είναι αληθής.

Υπαρξιακός ποσοδείκτης: Χρησιμοποιούμε το σύμβολο $\exists$ (υπάρχει). Γράφουμε $\exists_x p(x)$. Η $\exists_x p(x)$ είναι αληθής αν και μόνο αν η $p(x)$ είναι αληθής για ένα τουλάχιστον $x \in \mathcal{U}$.

Οι ποσοδείκτες μετατρέπουν ένα προτασιακό τύπο σε πρόταση: Για παράδειγμα, θεωρούμε και πάλι τον προτασιακό τύπο $p(n)$: “ο φυσικός αριθμός n ισούται με το άθροισμα των

τετραγώνων δύο φυσικών αριθμών” — εδώ το σύμπαν $\mathcal{U}$ για την μεταβλητή n είναι το σύνολο $\mathbb{N}$ των φυσικών αριθμών. Χρησιμοποιώντας τον καθολικό ποσοδείκτη, μπορούμε να μετατρέψουμε τον πιο πάνω προτασιακό τύπο σε πρόταση ως εξής: “Κάθε φυσικός αριθμός n μπορεί να εκφραστεί ως το άθροισμα των τετραγώνων δύο φυσικών αριθμών”. Η πρόταση αυτή είναι ψευδής. Μπορείτε, χρησιμοποιώντας τώρα τον υπαρξιακό ποσοδείκτη, να μετατρέψετε τον πιο πάνω προτασιακό τύπο σε μια πρόταση η οποία είναι αληθής;

Παράδειγμα 2.7. (i) Το θεώρημα του Lagrange, ότι κάθε φυσικός αριθμός είναι το άθροισμα των τετραγώνων τεσσάρων ακεραίων μπορεί να διατυπωθεί με τον ακόλουθο τρόπο:

$$\forall n \in \mathbb{N} \exists x_1 \in \mathbb{Z} \exists x_2 \in \mathbb{Z} \exists x_3 \in \mathbb{Z} \exists x_4 \in \mathbb{Z} \quad (n = x_1^2 + x_2^2 + x_3^2 + x_4^2)$$

$$\text{ή} \quad \forall n \in \mathbb{N} \exists x_1, x_2, x_3, x_4 \in \mathbb{Z} \quad (n = x_1^2 + x_2^2 + x_3^2 + x_4^2)$$

Παρατήρηση: Έχει σημασία με ποια σειρά εμφανίζονται οι ποσοδείκτες $\forall$ και $\exists$ (και δεν μπορούμε απλά να ανταλλάξουμε την σειρά τους). Η πρόταση $\exists x_1, x_2, x_3, x_4 \in \mathbb{Z} \forall n \in \mathbb{N} (n = x_1^2 + x_2^2 + x_3^2 + x_4^2)$ που είναι προφανώς λανθασμένη, μας λέει ότι υπάρχουν τέσσερις πολύ ξεχωριστοί ακέραιοι που μας δίνουν το ζητούμενο για κάθε $n \in \mathbb{N}$.

(ii) Η εικασία του Goldbach, ότι κάθε άρτιος φυσικός αριθμός > 2 είναι το άθροισμα δύο πρώτων:

$$\forall n \in \mathbb{N}, n > 1 \exists p_1, p_2 \text{ πρώτοι} \quad (2n = p_1 + p_2).$$

(iii) Αν $\mathcal{C}$ είναι μια συλλογή υποσυνόλων ενός (καθολικού) συνόλου $\mathcal{U}$ έχουμε, σύμφωνα με τους ορισμούς που δώσαμε στην προηγούμενη παράγραφο, ότι $\bigcap_{A \in \mathcal{C}} A = \{x \in \mathcal{U} : \forall A \in \mathcal{C} (x \in A)\}$ και $\bigcup_{A \in \mathcal{C}} A = \{x \in \mathcal{U} : \exists A \in \mathcal{C} (x \in A)\}$.

Συχνά ενδιαφερόμαστε να βρούμε την *άρνηση* προτάσεων που περιέχουν ποσοδείκτες. Εύκολα μπορούμε να δείξουμε, για παράδειγμα χρησιμοποιώντας αληθοπίνακες, ότι

(i) η άρνηση της πρότασης $\forall x p(x)$ είναι η πρόταση $\exists x \sim p(x)$

(ii) η άρνηση της πρότασης $\exists x p(x)$ είναι η πρόταση $\forall x \sim p(x)$

[Ελέγχουμε ότι $\forall x p(x)$ είναι αληθής αν, και μόνο αν, $\exists x \sim p(x)$ είναι ψευδής. Επίσης, η πρόταση $\exists x p(x)$ είναι αληθής αν, και μόνο αν, η πρόταση $\forall x \sim p(x)$ είναι ψευδής.]

Παράδειγμα 2.8. (i) Η άρνηση του θεωρήματος του Lagrange:

$$\begin{aligned} \text{Θεώρημα Lagrange (L):} \quad & \forall n \in \mathbb{N} (\exists x_1, x_2, x_3, x_4 \in \mathbb{Z} \quad (n = x_1^2 + x_2^2 + x_3^2 + x_4^2)) \\ \text{Άρνηση:} \quad & \exists n \in \mathbb{N} \sim (\exists x_1, x_2, x_3, x_4 \in \mathbb{Z} \quad (n = x_1^2 + x_2^2 + x_3^2 + x_4^2)) \\ \text{Επομένως, άρνηση του L:} \quad & \exists n \in \mathbb{N} \forall x_1, x_2, x_3, x_4 \in \mathbb{Z} \quad (n \neq x_1^2 + x_2^2 + x_3^2 + x_4^2) \end{aligned}$$

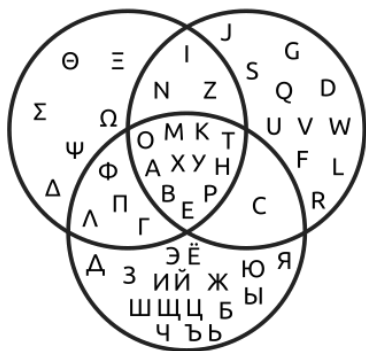
(ii) Η άρνηση της εικασίας του Goldbach:

$$\begin{aligned} \text{Εικασία του Goldbach (G):} \quad & \forall n \in \mathbb{N}, n > 1 (\exists p_1, p_2 \text{ πρώτοι} \quad (2n = p_1 + p_2)) \\ \text{Άρνηση:} \quad & \exists n \in \mathbb{N}, n > 1 \sim (\exists p_1, p_2 \text{ πρώτοι} \quad (2n = p_1 + p_2)) \\ \text{Επομένως, άρνηση της G:} \quad & \exists n \in \mathbb{N}, n > 1 \forall p_1, p_2 \text{ πρώτοι} \quad (2n \neq p_1 + p_2) \end{aligned}$$

Σημειώσεις και Σχόλια

1. Το παράδοξο του Russell σχετίζεται με το ερώτημα κατά πόσον ένα σύνολο μπορεί να είναι μέλος του ίδιου του εαυτού του. Πιο συγκεκριμένα, αν θεωρήσουμε ένα σύνολο R που περιλαμβάνει όλα τα σύνολα που δεν περιέχουν τον εαυτό τους, τότε ανακύπτει το ερώτημα κατά πόσον το R περιλαμβάνει τον εαυτό του ή όχι. Αν προσπαθήσουμε να το απαντήσουμε, θα προκύψει αντίφαση. [Μια από τις πιο γνωστές παραλλαγές του παραδόξου αυτού είναι η εξής: Υποθέτουμε ότι ένας κουρέας ξυρίζει όλους τους άντρες στο χωριό του που δεν ξυρίζονται μόνοι τους (και μόνο αυτούς). Άραγε, ο ίδιος ο κουρέας ξυρίζει τον εαυτό του;] Διάφορα συστήματα αξιωματικοποίησης της θεωρίας συνόλων έχουν προταθεί, για παράδειγμα από τον Zermelo, με σκοπό να αποκλειστούν τέτοια παράδοξα.

2. Τα διαγράμματα του Venn δείχνουν τις σχέσεις (ένωση, τομή, διαφορά) ανάμεσα σε μια πεπερασμένη συλλογή από υποσύνολα ενός καθολικού συνόλου. Το διάγραμμα αποτελείται από κύκλους (συνήθως δύο ή τρεις) κάθε ένας από τους οποίους αναπαριστά κάποιο από τα σύνολα. Αν δύο σύνολα έχουν μη-κενή τομή, οι αντίστοιχοι κύκλοι (δίσκοι) στο διάγραμμα του Venn τέμνονται.



Σχήμα 2: Διάγραμμα του Venn που δείχνει τα γράμματα που μοιράζονται το ελληνικό, το λατινικό και το κυριλλικό αλφάβητο.

Τα διαγράμματα αυτής της μορφής εμφανίστηκαν στο βιβλίο “Symbolic Logic” του John Venn (1834–1923) που εκδόθηκε στο Λονδίνο το 1881. Είναι σημαντικά αφού μπορούν να συμπυκνώσουν πολύπλοκες πληροφορίες σε μια απλή και ευανάγνωστη μορφή και να μας δώσουν έτσι πολύ καλή διαισθητική εικόνα του προβλήματος. Δεν μπορούν όμως να αποτελούν μέρος μιας αυστηρής απόδειξης.

3. Η άλγεβρα Boole ονομάστηκε από τον George Boole ο οποίος με την δουλειά του προσπάθησε να ενοποιήσει την λογική (και την θεωρία συνόλων) με την άλγεβρα.

4. Το σύμβολο $\exists$ για τον υπαρξιακό ποσοδείκτη είναι η “ανάκλαση” του πρώτου γράμματος της αγγλικής λέξης Exists – υπάρχει) και προτάθηκε από τον Charles Peirce το 1885. Το σύμβολο $\forall$ για τον καθολικό ποσοδείκτη (από τον γερμανικό Alle – όλα, όλοι) προτάθηκε από τον Gerhard Gentzen το 1935, κατ’ αναλογία με το σύμβολο του υπαρξιακού ποσοδείκτη.

Ασκήσεις

2.1 Αναγράψτε τα στοιχεία των ακόλουθων συνόλων:

- (i) $\{x : x \in \mathbb{Z} \text{ και } 1 + x^2 = 0\}$
- (ii) $\{x : x \in \mathbb{N} \text{ και } x^4 = 1\}$
- (iii) $\{x : x \in \mathbb{Z} \text{ και } x^4 = 1\}$
- (iv) $\{n \in \mathbb{N} : \frac{n+9}{n+1} \in \mathbb{N}\}$

2.2 Βρείτε όλα τα στοιχεία του συνόλου $\{x \in \mathbb{Z} : \exists y \in \mathbb{Z} (|x| + |y| = 2)\}$.

2.3 Πόσα στοιχεία έχουν τα πιο κάτω σύνολα;

- (i) (a) $\emptyset$, (b) $\{\emptyset\}$, (c) $\{\{\emptyset\}\}$, (d) $\{\emptyset, \{\emptyset\}\}$,
(ii) (a) $\mathcal{P}(A)$ όπου $A = \{1, 2, 3\}$, (b) $\mathcal{P}(\emptyset)$, (c) $\mathcal{P}(\mathcal{P}(\emptyset))$.

2.4 Έστω $A = \{1, 2, 3\}$, $B = \{a, b, c\}$. Βρείτε τα στοιχεία των καρτεσιανών γινομένων $A \times B$ και $A \times A$.

2.5 Έστω A, B μη-κενά σύνολα. Εξετάστε κατά πόσον ισχύουν τα ακόλουθα

- (i) $A \times B = B \times A$ αν, και μόνο αν, $A = B$
(ii) Αν $S \subseteq A \times B$ τότε $S = C \times D$, όπου $C \subseteq A$ και $D \subseteq B$.

2.6 Έστω A, B, C υποσύνολα ενός καθολικού συνόλου $\mathcal{U}$. Αποδείξτε τα ακόλουθα:

- (i) $(A \cup B)' = A' \cap B'$, (ii) $(A \cap B)' = A' \cup B'$,
(iii) $C - (A \cup B) = (C - A) \cap (C - B)$, (iv) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
(v) $C - (A \cap B) = (C - A) \cup (C - B)$, (vi) $B - (B - A) = A \cap B$

2.7 Έστω A, B, C και D υποσύνολα ενός καθολικού συνόλου $\mathcal{U}$. Εξετάστε κατά πόσον ισχύουν τα ακόλουθα:

- (i) $A \cup A = A$,
(ii) $A \cap A = A$,
(iii) $(A \cup B) \cup (C \cup D) = A \cup B \cup C \cup D$,
(iv) $(A \cap B) \cap (C \cap D) = ((A \cap B) \cap C) \cap D$,
(v) $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

2.8 Διατυπώστε τα ακόλουθα χρησιμοποιώντας λογικά σύμβολα:

- (i) Υπάρχει κάποιος ακέραιος μεγαλύτερος από όλους τους άλλους ακεραίους.
(ii) Κάθε άρτιος αριθμός είναι το άθροισμα δυο περιττών αριθμών.

Γράψτε την άρνηση των πιο πάνω προτάσεων και εξετάστε κατά πόσον η πρόταση ή η άρνηση της είναι αληθής.

2.9 Διατυπώστε τα ακόλουθα με λόγια και εξετάστε κατά πόσον είναι αληθή:

- (i) $\forall_{z \in \mathbb{N}} (z^2 \in \mathbb{N})$
(ii) $\forall_{x, y \in \mathbb{Z}} \exists_{z \in \mathbb{Z}} (z^2 = x^2 + y^2)$
(iii) $\forall_{x, y, z \in \mathbb{R}} \exists_{w \in \mathbb{R}} (x^2 + y^2 + z^2 = 8w)$

2.10 Δείξτε ότι σε οποιοδήποτε μη-κενό πεπερασμένο σύνολο το πλήθος των υποσυνόλων με άρτιο αριθμό στοιχείων ισούται με το πλήθος των υποσυνόλων με περιττό αριθμό στοιχείων.

2.11 Έστω A, B και C υποσύνολα του συνόλου $\mathcal{U}$. Θέτουμε $A \Delta B = (A \cup B) - (A \cap B)$ (το σύνολο αυτό καλείται η *συμμετρική διαφορά* των A, B). Δείξτε τα πιο κάτω:

- (i) $A \Delta B = (A - B) \cup (B - A)$, (ii) $A \Delta B = B \Delta A$, (iii) $(A \Delta B) \Delta C = A \Delta (B \Delta C)$,
(iv) $(A \Delta B) \cap C = (A \cap B) \Delta (B \cap C)$.

2.12 Αποδείξτε την Πρόταση 2.6.

2.13 Έστω $A_1, \dots, A_n$ μια (πεπερασμένη) συλλογή υποσυνόλων ενός καθολικού συνόλου $\mathcal{U}$. Μπορείτε να βρείτε μια συλλογή υποσυνόλων $B_1, \dots, B_n$ του $\mathcal{U}$, ξένων μεταξύ τους ανά δύο, τέτοια ώστε $A_1 \cup A_2 \cup \dots \cup A_n = B_1 \cup B_2 \cup \dots \cup B_n$;

3. Συναρτήσεις

3.1. Ορισμοί, παραδείγματα

Έστω X, Y δύο μη-κενά σύνολα. Μια *συνάρτηση* (ή *απεικόνιση*) f από το X στο Y είναι ένας κανόνας που αντιστοιχίζει σε κάθε $x \in X$ ακριβώς ένα στοιχείο $f(x)$ του Y .

Γράφουμε $f: X \rightarrow Y: x \mapsto f(x)$ ή πιο απλά $f: X \rightarrow Y$. Το σύνολο X ονομάζεται *πεδίο ορισμού* της f ενώ το σύνολο Y ονομάζεται *πεδίο τιμών* της f .

Αν $x \in X$, το στοιχείο $f(x)$ ονομάζεται *εικόνα* του x μέσω της f , και το σύνολο $f(X) = \{y \in Y: y = f(x) \text{ για κάποιο } x \in X\}$ ονομάζεται *εικόνα* του X μέσω της f .

Οι συναρτήσεις $f: X \rightarrow Y$ και $g: A \rightarrow B$ (όπου A, B είναι μη-κενά) λέγονται *ίσες* αν $X = A, Y = B$ και $f(x) = g(x)$ για κάθε $x \in X$.

Στην συνέχεια, με την δήλωση “η συνάρτηση $f: X \rightarrow Y$ ” θα υπονοείται πάντα ότι τα σύνολα X και Y είναι μη-κενά.

Παράδειγμα. (i) $f_1: \mathbb{Z} \rightarrow \mathbb{R}: x \mapsto x^2, (x \in \mathbb{Z})$. Τότε $f_1(\mathbb{Z}) = \{0, 1, 4, 9, \dots\}$.

(ii) $f_2: \mathbb{N} \rightarrow \mathbb{Z}: n \mapsto -n (n \in \mathbb{N})$. Τότε $f_2(\mathbb{N}) = \{-n: n \in \mathbb{N}\} = \{-1, -2, -3, \dots\}$.

(iii) $f_3: \mathbb{R} \rightarrow \mathbb{R}: x \mapsto \begin{cases} 1, & \text{αν } x \in \mathbb{Q} \\ 0, & \text{αν } x \in \mathbb{R} - \mathbb{Q} \end{cases}$. Τότε $f_3(\mathbb{R}) = \{0, 1\}$.

(iv) Έστω T το σύνολο των άρτιων φυσικών αριθμών. Θέτουμε $f_4: T \rightarrow \mathbb{Z}: 2n \mapsto 3n (n \in \mathbb{N})$. Ποια είναι η εικόνα του συνόλου T μέσω της f_4 ;

Αν η συνάρτηση g ορίζεται με $g: T \rightarrow \mathbb{Z}: x \mapsto \frac{3}{2}x, (x \in T)$, παρατηρούμε τότε ότι οι συναρτήσεις g και f_4 είναι ίσες.

(v) Ελέγξτε ότι οι ακόλουθοι κανόνες δεν μας δίνουν συναρτήσεις από το $\mathbb{N}$ στο $\mathbb{N}$:

(a) $y = 3x - 5$, και (b) $y = x + \frac{1}{3}$.

Τι μπορείτε να πείτε για τον κανόνα $y = \pm\sqrt{x}$ από το σύνολο $\{0, 2, 4, 9\}$ στο σύνολο $\{-3, -2, -\sqrt{2}, 0, \sqrt{2}, 2, 3\}$;

Το *γράφημα* Γ της συνάρτησης $f: X \rightarrow Y$ είναι το υποσύνολο του καρτεσιανού γινομένου $X \times Y$ που ορίζεται με $\Gamma = \{(x, f(x)) \in X \times Y: x \in X\} = \{(x, y) \in X \times Y: x \in X \text{ και } y = f(x)\}$.

Παράδειγμα. Θέτουμε $A = \{1, 2, 3\}$ και $B = \{1, 2, 3, 4\}$. Το υποσύνολο $\{(1, 1), (2, 1), (3, 1)\}$ του $A \times B$ είναι το γράφημα μιας συνάρτησης από το A στο B (ποια είναι αυτή η συνάρτηση;). Δεν συμβαίνει όμως το ίδιο με τα υποσύνολα $\{(1, 1), (1, 2), (2, 3), (3, 4)\}$ και $\{(1, 1), (2, 2)\}$ του $A \times B$.

Σημείωση. Ένα υποσύνολο Γ_1 του καρτεσιανού γινομένου $X \times Y$ είναι το γράφημα μιας συνάρτησης από το X στο Y αν, και μόνο αν, για κάθε $x \in X$ υπάρχει μοναδικό διατεταγμένο ζεύγος στο Γ_1 που να έχει πρώτη συντεταγμένη το x . Προφανώς, μια συνάρτηση καθορίζεται πλήρως από το γράφημα της. (Επομένως δεν αποτελεί έκπληξη ότι αρκετά συχνά στην βιβλιογραφία ο ορισμός που δίνεται για την συνάρτηση συμπίπτει με τον ορισμό που έχουμε δώσει εδώ για το γράφημα της συνάρτησης — κοιτάξτε επίσης τις Σημειώσεις και Σχόλια στο τέλος του κεφαλαίου.)

Παράδειγμα 3.1. (i) Θέτουμε $f: \mathbb{N} \rightarrow \mathbb{N} : x \mapsto 2x$, ($x \in \mathbb{N}$). Το πεδίο ορισμού και το πεδίο τιμών της f είναι το $\mathbb{N}$, ενώ $f(\mathbb{N})$ είναι το σύνολο όλων των άρτιων θετικών ακεραίων. Το γράφημα Γ της f είναι το υποσύνολο $\{(1, 2), (2, 4), (3, 6), (4, 8), \dots\} (= \{(n, 2n) : n \in \mathbb{N}\})$ του $\mathbb{N} \times \mathbb{N}$.

(ii) Αν $a \neq b$, $X = \{a, b\}$ και $Y = \{1, 2\}$, τότε υπάρχουν ακριβώς 4 συναρτήσεις από το X στο Y . Από τις συναρτήσεις αυτές οι δύο έχουν εικόνα η οποία περιέχει ακριβώς δύο στοιχεία και οι υπόλοιπες δύο έχουν εικόνα με ακριβώς ένα στοιχείο.

(iii) Θέτουμε $f: \mathbb{Z} \rightarrow \mathbb{Z} : x \mapsto |x| = \begin{cases} x, & \text{αν } x \geq 0, \\ -x, & \text{αν } x < 0 \end{cases}$, ($x \in \mathbb{Z}$). Τότε $f(\mathbb{Z}) = \mathbb{N} \cup \{0\} \neq \mathbb{Z}$.

Παρατήρηση. Από το Παράδειγμα 3.1(iii) μπορούμε να κάνουμε τις εξής παρατηρήσεις: Αν $f: X \rightarrow Y$ είναι μια συνάρτηση, μπορεί να συμβαίνει ότι $f(X) \neq Y$. Επίσης δύο διακεκριμένα στοιχεία του X μπορεί να έχουν την ίδια εικόνα μέσω της f .

Ορισμός. (i) Μια συνάρτηση $f: X \rightarrow Y$ λέγεται *ένριψη* (πιο απλά 1-1) αν η σχέση $f(x) = f(x')$, όπου $x, x' \in X$, συνεπάγεται ότι $x = x'$.

(ii) Μια συνάρτηση $f: X \rightarrow Y$ λέγεται *επίρριψη* (πιο απλά επί) αν για κάθε $y \in Y$ υπάρχει $x \in X$ τέτοιο ώστε $f(x) = y$.

(iii) Μια συνάρτηση λέγεται *αμφιμονοσήμαντη* αν είναι 1-1 και επί.

(iv) Έστω M ένα μη-κενό σύνολο. Τότε η συνάρτηση $M \rightarrow M : x \mapsto x$ ($x \in M$) λέγεται *ταυτοτική συνάρτηση* του M και συμβολίζεται με i_M .

Παράδειγμα 3.2. (i) $f: \mathbb{N} \rightarrow \mathbb{Z} : x \mapsto x$, ($x \in \mathbb{N}$) είναι 1-1 αλλά δεν είναι επί.

(ii) $f: \mathbb{Z} \rightarrow (\mathbb{N} \cup \{0\}) : x \mapsto |x|$, ($x \in \mathbb{Z}$) είναι επί αλλά δεν είναι 1-1.

(iii) $f: \mathbb{R} \rightarrow \mathbb{R} : x \mapsto \frac{1}{3}x$, ($x \in \mathbb{R}$) είναι αμφιμονοσήμαντη.

(iv) Θέτουμε $f: \mathbb{N} \rightarrow \mathbb{N} : x \mapsto [\frac{1}{2}x + 1]$, ($x \in \mathbb{N}$) όπου, για κάθε $u \in \mathbb{R}$, ορίζουμε $[u]$ να είναι ο μεγαλύτερος ακέραιος που είναι μικρότερος ή ίσος με το u . Τότε f είναι μια επί συνάρτηση αφού $2m - 1 \in \mathbb{N}$ οποτεδήποτε $m \in \mathbb{N}$ και, επιπλέον, ισχύει $f(2m - 1) = m$. Δεν είναι όμως 1-1 αφού $f(6) = 4 = f(7)$.

(v) Η συνάρτηση $i_X: X \rightarrow X$ είναι αμφιμονοσήμαντη.

(vi) Αν $f: X \rightarrow Y$ είναι μια αμφιμονοσήμαντη συνάρτηση και το σύνολο X είναι πεπερασμένο, τότε και το σύνολο Y είναι πεπερασμένο και έχει ακριβώς το ίδιο πλήθος στοιχείων με το X .

Ορισμός. Έστω $f: X \rightarrow Y$ μια συνάρτηση και $A \subseteq X$. Ορίζουμε την *εικόνα* $f(A)$ του υποσυνόλου A του X μέσω της f με $f(A) = \{f(x): x \in A\}$.

Για την απόδειξη της πιο κάτω πρότασης κοιτάζετε την Άσκηση 3.9.

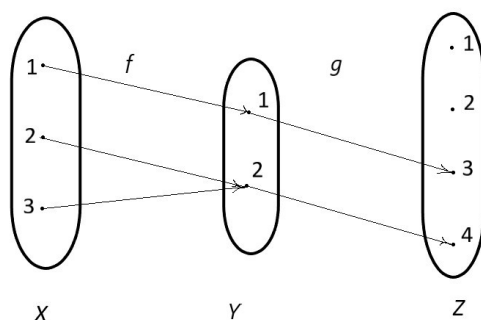
Πρόταση 3.3. Έστω η συνάρτηση $f: X \rightarrow Y$. Υποθέτουμε επίσης ότι $A, B \subseteq X$. Τότε

- (i) $f(\emptyset) = \emptyset$, $f(X) \subseteq Y$,
- (ii) $f(A \cup B) = f(A) \cup f(B)$,
- (iii) $f(A \cap B) \subseteq f(A) \cap f(B)$,
- (iv) αν, επιπλέον, $A \subseteq B$, τότε $f(A) \subseteq f(B)$.

3.2. Σύνθεση συναρτήσεων, αντίστροφη συνάρτηση, αντίστροφη εικόνα συνάρτησης

Ορισμός. Έστω $f: X \rightarrow Y$ και $g: Y \rightarrow Z$ συναρτήσεις. Τότε ορίζεται η συνάρτηση $g \circ f: X \rightarrow Z$ με $(g \circ f)(x) = g(f(x))$ για κάθε $x \in X$, και λέγεται *σύνθεση* των f και g .

Παράδειγμα. (i) Θέτουμε $X = \{1, 2, 3\}$, $Y = \{1, 2\}$ και $Z = \{1, 2, 3, 4\}$.



Θεωρούμε τις συναρτήσεις f και g που ορίζονται με

$$f(1) = 1, \quad f(2) = 2, \quad f(3) = 2, \quad g(1) = 3, \quad g(2) = 4.$$

Έχουμε τότε

$$\begin{aligned} (g \circ f)(1) &= g(f(1)) = g(1) = 3, \\ (g \circ f)(2) &= g(f(2)) = g(2) = 4, \\ (g \circ f)(3) &= g(f(3)) = g(2) = 4 \end{aligned}$$

(ii) Έστω οι συναρτήσεις f, g από το $\mathbb{N}$ στο $\mathbb{N}$ που ορίζονται με $g(x) = x^2$ και $f(x) = 3x+2$, ($x \in \mathbb{N}$). Έχουμε τότε ότι

$$(f \circ g)(x) = f(g(x)) = f(x^2) = 3x^2 + 2,$$

$$(g \circ f)(x) = g(f(x)) = g(3x+2) = (3x+2)^2.$$

(iii) Έστω f, g, h συναρτήσεις από το $\mathbb{N}$ στο $\mathbb{N}$ όπου $f(x) = x+1$, $g(x) = x^2$, $h(x) = 3x$ για κάθε $x \in \mathbb{N}$. Δείξτε ότι, στην ειδική αυτή περίπτωση, $h \circ (g \circ f) = (h \circ g) \circ f$. Στην πραγματικότητα, το αποτέλεσμα αυτό ισχύει πιο γενικά όπως θα δούμε στην συνέχεια.

Παρατηρήσεις 3.4. (i) Έστω $f: A \rightarrow B$ μια συνάρτηση. Τότε $i_B \circ f = f = f \circ i_A$.

(ii) Υποθέτουμε ότι f και g είναι συναρτήσεις και ότι ορίζεται η συνάρτηση $g \circ f$. Δεν ισχύει απαραίτητα ότι ορίζεται η συνάρτηση $f \circ g$, όμως ακόμη και στην περίπτωση που ορίζεται η $f \circ g$ είναι δυνατό να ισχύει $f \circ g \neq g \circ f$, όπως έχουμε δει στο πιο πάνω παράδειγμα.

(iii) Η σύνθεση συναρτήσεων είναι *προσεταιριστική*. (Έχουμε δηλαδή ότι αν $f: A \rightarrow B$, $g: B \rightarrow C$ και $h: C \rightarrow D$ είναι συναρτήσεις, τότε οι συναρτήσεις $h \circ (g \circ f): A \rightarrow D$ και $(h \circ g) \circ f: A \rightarrow D$ είναι ίσες.) Για να το δείξουμε αυτό αρκεί να παρατηρήσουμε ότι για κάθε $x \in A$, η εικόνα του x μέσω και των δύο συναρτήσεων $h \circ (g \circ f)$ και $(h \circ g) \circ f$ ισούται με $h(g(f(x)))$ — προφανώς οι δύο πιο πάνω συναρτήσεις έχουν το ίδιο πεδίο ορισμού και το ίδιο πεδίο τιμών.

Πρόταση 3.5. Έστω $f: X \rightarrow Y$ και $g: Y \rightarrow X$ συναρτήσεις. Υποθέτουμε επιπλέον ότι $g \circ f = i_X$. Τότε η συνάρτηση f είναι ενριπτική και η συνάρτηση g είναι επιρριπτική.

Απόδειξη. Θα δείξουμε πρώτα ότι η f είναι ενριπτική. Έστω $x_1, x_2 \in X$ με $f(x_1) = f(x_2)$. Έχουμε τότε ότι $x_1 = i_X(x_1) = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = i_X(x_2) = x_2$. Για να δείξουμε ότι η g είναι επιρριπτική υποθέτουμε ότι $x \in X$. Όμως τότε $x = i_X(x) = (g \circ f)(x) = g(f(x))$, όπου $f(x) \in Y$. $\square$

Πρόταση 3.6. Έστω $f: X \rightarrow Y$ και $g: Y \rightarrow Z$ δύο συναρτήσεις.

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

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

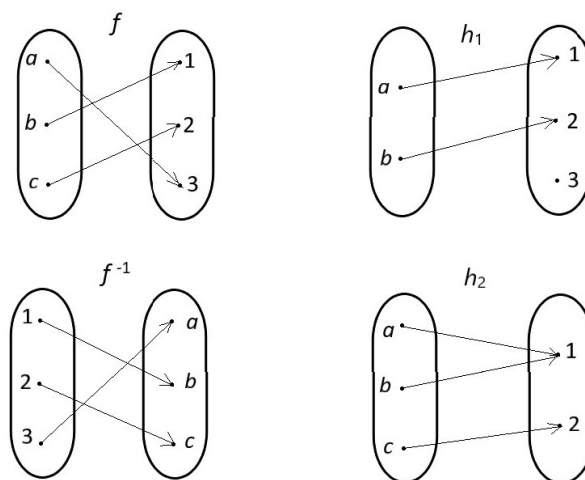
(iii) Αν οι f, g είναι αμφιμονοσήμαντες, τότε και η $g \circ f$ είναι αμφιμονοσήμαντη.

Απόδειξη. (i) Υποθέτουμε ότι οι f και g είναι και οι δύο 1-1. Έστω τώρα $x_1, x_2 \in X$ με $(g \circ f)(x_1) = (g \circ f)(x_2)$. Από τον ορισμό της σύνθεσης συναρτήσεων έχουμε ότι $g(f(x_1)) = g(f(x_2))$. Αφού η g είναι 1-1, έχουμε $f(x_1) = f(x_2)$. Συνάγουμε ότι $x_1 = x_2$ αφού και η f είναι 1-1. Αφήνουμε τα (ii) και (iii) στις Ασκήσεις. $\square$

Έστω τώρα $f: X \rightarrow Y$ μια συνάρτηση. Αν $g: Y \rightarrow X$ είναι επίσης μια συνάρτηση, τότε ορίζονται οι συναρτήσεις $g \circ f: X \rightarrow X$ και $f \circ g: Y \rightarrow Y$. Στην περίπτωση που $g \circ f = i_X$ και $f \circ g = i_Y$, τότε η g λέγεται μια *αντίστροφη* της f και η f λέγεται μια *αντίστροφη* της g . Σε τέτοια περίπτωση λέμε επίσης ότι οι συναρτήσεις f και g είναι *αντιστρέψιμες*.

Σημείωση. Αν μια συνάρτηση $f: X \rightarrow Y$ έχει αντίστροφη, τότε η αντίστροφη αυτή είναι μοναδική. [Εξήγηση: Έστω $g_1, g_2: Y \rightarrow X$ δύο αντίστροφες της f . Έχουμε τότε, χρησιμοποιώντας την προσεταιριστική ιδιότητα, ότι $g_1 = g_1 \circ i_Y = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = i_X \circ g_2 = g_2$.] Επομένως σε τέτοια περίπτωση μιλάμε για την (μοναδική) αντίστροφη της f την οποία συμβολίζουμε με f^{-1} .

Παράδειγμα. (Συγκρίνετε με την Πρόταση 3.5.) Στο πιο κάτω παράδειγμα παρατηρούμε ότι η συνάρτηση f είναι αντιστρέψιμη με αντίστροφη συνάρτηση την f^{-1} , ενώ οι συναρτήσεις h_1, h_2 δεν είναι αντιστρέψιμες. Παρατηρούμε επίσης ότι η συνάρτηση f είναι αμφιμονοσήμαντη, όχι όμως οι συναρτήσεις h_1, h_2 (η h_1 δεν είναι επιρριπτική ενώ η h_2 δεν είναι ενριπτική).



Πρόταση 3.7. Μια συνάρτηση $f: X \rightarrow Y$ έχει αντίστροφη αν, και μόνο αν, η f είναι αμφιμονοσήμαντη.

Απόδειξη. Υποθέτουμε πρώτα ότι η f έχει αντίστροφη, έστω την g . Από τον ορισμό, $g \circ f = i_X$ και $f \circ g = i_Y$ και το ζητούμενο είναι άμεση συνέπεια της Πρότασης 3.5.

Υποθέτουμε τώρα ότι η f είναι αμφιμονοσήμαντη. Έστω $y \in Y$. Αφού $f: X \rightarrow Y$ είναι επί, υπάρχει $x \in X$ τέτοιο ώστε $f(x) = y$. Αν $x_1 \in X$ επίσης ικανοποιεί $f(x_1) = y$, τότε $f(x_1) = y = f(x)$ και επομένως $x_1 = x$ αφού η f είναι ενριπτική. Άρα υπάρχει μοναδικό $x \in X$ τέτοιο ώστε $f(x) = y$. Θέτουμε $h(y) = x$. Τότε h είναι μια (καλά ορισμένη) συνάρτηση από το Y στο X και εύκολα παρατηρούμε ότι ισχύουν $h \circ f = i_X$ και $f \circ h = i_Y$.

□

Παρατήρηση. Από τα πιο πάνω έπεται ότι αν $f: X \rightarrow Y$ είναι αμφιμονοσήμαντη τότε και η $f^{-1}: Y \rightarrow X$ είναι αμφιμονοσήμαντη και η αντίστροφη της f^{-1} είναι η f .

Παράδειγμα. (i) Η αντίστροφη της ταυτοτικής συνάρτησης $i_X: X \rightarrow X$ είναι ίδια η i_X .

(ii) Θέτουμε $Y = \{n^2: n \in \mathbb{N}\}$. Η συνάρτηση $f: \mathbb{N} \rightarrow Y: x \mapsto x^2$ ($x \in \mathbb{N}$) είναι αμφιμονοσήμαντη με αντίστροφη συνάρτηση την $g: Y \rightarrow \mathbb{N}: x \mapsto \sqrt{x}$, ($x \in Y$).

Παρατήρηση. Έστω $f: X \rightarrow Y$ μια συνάρτηση η οποία είναι ενριπτική όμως δεν είναι επιριπτική. Τότε η f δεν είναι αμφιμονοσήμαντη και επομένως δεν έχει αντίστροφη. Μπορούμε όμως να κατασκευάσουμε μια συνάρτηση η οποία ‘δεν διαφέρει πολύ’ από την f και η οποία έχει αντίστροφη: θέτουμε $\hat{f}: X \rightarrow f(X): x \mapsto f(x), (x \in X)$. Τότε η $\hat{f}$ είναι επιριπτική από τον τρόπο που την έχουμε ορίσει, και είναι επίσης ενριπτική αφού προφανώς κληρονομεί αυτή την ιδιότητα από την f . Έπεται ότι η $\hat{f}$ είναι αμφιμονοσήμαντη και επομένως έχει αντίστροφη.

Παράδειγμα. Θέτουμε $T = \{2n: n \in \mathbb{N}\}$ και $f: \mathbb{N} \rightarrow \mathbb{N}: n \mapsto 2n, (n \in \mathbb{N})$. Προφανώς η f είναι ενριπτική όχι όμως επιριπτική, αφού $f(\mathbb{N}) = T \subsetneq \mathbb{N}$. Έπεται ότι η f δεν έχει αντίστροφη. Ορίζουμε τώρα $\hat{f}: \mathbb{N} \rightarrow T: n \mapsto f(n), (n \in \mathbb{N})$. Τότε η $\hat{f}$ είναι αμφιμονοσήμαντη και $(\hat{f})^{-1}: T \rightarrow \mathbb{N}: 2n \mapsto n, (n \in \mathbb{N})$. Παρατηρούμε επίσης εδώ ότι υπάρχει μια αμφιμονοσήμαντη συνάρτηση από το $\mathbb{N}$ σε ένα γνήσιο υποσύνολο του (κάτι που δεν μπορεί να συμβεί στην περίπτωση ενός πεπερασμένου συνόλου).

Σε κάποιες περιπτώσεις είναι χρήσιμο για τους σκοπούς μας να εστιάσουμε την προσοχή μας στην συμπεριφορά μιας συνάρτησης πάνω σε ένα γνήσιο υποσύνολο του πεδίου ορισμού της. Αν $f: X \rightarrow Y$ είναι μια συνάρτηση και A είναι ένα (μη-κενό) γνήσιο υποσύνολο του X ορίζουμε την συνάρτηση $f|_A$, την οποία ονομάζουμε *περιορισμό της f στο A* , με $f|_A: A \rightarrow Y: x \mapsto f(x), (x \in A)$. Προφανώς οι συναρτήσεις f και $f|_A$ δεν είναι ίσες αφού έχουν διαφορετικό πεδίο ορισμού. Επιπλέον, μπορεί να έχουν πολύ διαφορετικές ιδιότητες όπως θα δούμε στο επόμενο παράδειγμα.

Παράδειγμα 3.8. Έστω $f: \mathbb{N} \rightarrow \mathbb{N}: x \mapsto [\frac{1}{2}x+1], (x \in \mathbb{N})$. Θέτουμε $T = \{2n: n \in \mathbb{N}\}$, το σύνολο των άρτιων φυσικών αριθμών. Τότε $f|_T$ είναι η συνάρτηση που ορίζεται με $f|_T: T \rightarrow \mathbb{N}: x \mapsto [\frac{1}{2}x+1], (x \in T)$. Παρατηρούμε στην περίπτωση αυτή ότι η f είναι επιριπτική, όχι όμως η $f|_T$ αφού το στοιχείο 1 δεν ανήκει στην εικόνα του T μέσω της $f|_T$. Επιπλέον, η $f|_T$ είναι ενριπτική σε αντίθεση με την f . Κοιτάζτε επίσης την Άσκηση 3.15.

Πρόταση 3.9. Έστω $f: A \rightarrow B$ και $g: B \rightarrow C$ αμφιμονοσήμαντες συναρτήσεις. Τότε η συνάρτηση $g \circ f: A \rightarrow C$ έχει αντίστροφη και $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Απόδειξη. Η συνάρτηση $g \circ f$ είναι σύνθεση αμφιμονοσήμαντων συναρτήσεων και επομένως είναι αμφιμονοσήμαντη. Έπεται ότι $g \circ f$ έχει αντίστροφη. Για να δείξουμε ότι $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$, αρκεί να δείξουμε ότι $(g \circ f) \circ (f^{-1} \circ g^{-1}) = i_C$ και ότι $(f^{-1} \circ g^{-1}) \circ (g \circ f) = i_A$. Χρησιμοποιώντας την προσεταιριστική ιδιότητα παρατηρούμε ότι $(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ (f^{-1} \circ g^{-1})) = g \circ ((f \circ f^{-1}) \circ g^{-1}) = g \circ (i_B \circ g^{-1}) = g \circ g^{-1} = i_C$. Με παρόμοιο τρόπο δείχνουμε ότι $(f^{-1} \circ g^{-1}) \circ (g \circ f) = i_A$. $\square$

Ορισμός. Έστω η συνάρτηση $f: X \rightarrow Y$. Αν $B \subseteq Y$, τότε η *αντίστροφη εικόνα* $f^{-1}(B)$ του B μέσω της f είναι το υποσύνολο του X που ορίζεται με $f^{-1}(B) = \{x \in X: f(x) \in B\}$.

Σημείωση. Έστω $f: X \rightarrow Y$ μια συνάρτηση και $B \subseteq Y$. Η αντίστροφη εικόνα $f^{-1}(B)$ ορίζεται πάντα, ακόμη και στην περίπτωση που δεν υπάρχει αντίστροφη συνάρτηση της f . Στην περίπτωση που η f έχει αντίστροφη, έστω την $g: Y \rightarrow X$, τότε η *αντίστροφη εικόνα*

$f^{-1}(B)$ του υποσυνόλου B μέσω της f ισούται με την εικόνα $g(B)$ του υποσυνόλου B μέσω της g , όπου όμως $g = f^{-1}$. (Επομένως δεν μπορεί να δημιουργηθεί οποιαδήποτε σύγχυση με τον συμβολισμό αυτό).

Παράδειγμα. Θέτουμε $f: \mathbb{N} \rightarrow \mathbb{N}: x \mapsto [\frac{1}{2}x + 1]$, ($x \in \mathbb{N}$). Θέτουμε επίσης $B = \{4, 5\} \subseteq \mathbb{N}$. Τότε $f^{-1}(B) = \{6, 7, 8, 9\}$.

Πρόταση 3.10. Έστω $f: X \rightarrow Y$ μια συνάρτηση και $A, B \subseteq Y$.

- (i) $f^{-1}(\emptyset) = \emptyset$,
- (ii) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$,
- (iii) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$,
- (iv) $f^{-1}(Y - B) = X - f^{-1}(B)$,
- (v) αν επιπλέον $A \subseteq B$, τότε $f^{-1}(A) \subseteq f^{-1}(B)$.

Απόδειξη. Θα αποδείξουμε το (iii) (τα υπόλοιπα τα αφήνουμε ως άσκηση). Υποθέτουμε πρώτα ότι $x \in f^{-1}(A \cap B)$. Τότε $f(x) \in A \cap B$, άρα $f(x) \in A$ και $f(x) \in B$. Έπεται ότι $x \in f^{-1}(A)$ και $x \in f^{-1}(B)$ και επομένως $x \in f^{-1}(A) \cap f^{-1}(B)$. Συμπεραίνουμε ότι $f^{-1}(A \cap B) \subseteq f^{-1}(A) \cap f^{-1}(B)$. Έστω τώρα $y \in f^{-1}(A) \cap f^{-1}(B)$. Τότε $y \in f^{-1}(A)$ και $y \in f^{-1}(B)$. Έπεται ότι $f(y) \in A$ και $f(y) \in B$. Συνεπώς $f(y) \in A \cap B$. Συνάγουμε ότι $y \in f^{-1}(A \cap B)$, δείχνοντας έτσι ότι $f^{-1}(A) \cap f^{-1}(B) \subseteq f^{-1}(A \cap B)$. $\square$

3.3. Ακολουθίες

Μια πεπερασμένη ακολουθία είναι μια συνάρτηση με πεδίο ορισμού το σύνολο $\{1, 2, \dots, n\}$ των πρώτων n φυσικών αριθμών (ένα τέτοιο σύνολο καλείται *τμήμα* του $\mathbb{N}$). Παρόμοια, μια άπειρη ακολουθία είναι μια συνάρτηση με πεδίο ορισμού το σύνολο $\mathbb{N}$. Με τον όρο *ακολουθία* θα εννοούμε είτε μια πεπερασμένη ακολουθία (που είναι στην πραγματικότητα μια διατεταγμένη n -άδα) ή μια άπειρη ακολουθία. Αν το πεδίο τιμών της ακολουθίας είναι το σύνολο Y , συνήθως μιλάμε για μια ακολουθία στοιχείων του Y .

Έστω τώρα f μια ακολουθία στοιχείων ενός συνόλου Y . Συνήθως γράφουμε y_i αντί για $f(i)$ και καλούμε την τιμή αυτή τον i -όρο της ακολουθίας. Συμβολίζουμε μια πεπερασμένη ακολουθία με $(y_1, \dots, y_n)$ ή $(y_i)_{i=1}^n$ και μια άπειρη ακολουθία με $(y_i)_{i=1}^\infty$ (ή πιο απλά με (y_i) αν δεν υπάρχει περιθώριο για σύγχυση).

Παράδειγμα. Θέτουμε $a: \mathbb{N} \rightarrow \mathbb{Z}: n \mapsto (-1)^n n^2$, ($n \in \mathbb{N}$). Έχουμε τότε ότι $a_1 (= a(1)) = -1$, $a_2 (= a(2)) = 4$, $\dots$, $a_n (= a(n)) = (-1)^n n^2$, $\dots$ είναι μια ακολουθία στοιχείων του $\mathbb{Z}$.

Ακολουθίες συνόλων. Έστω τώρα $\mathcal{U}$ ένα μη-κενό σύνολο. Μια ακολουθία υποσυνόλων του $\mathcal{U}$ είναι μια ακολουθία στοιχείων του δυναμοσυνόλου $\mathcal{P}(\mathcal{U})$, δηλαδή μια συνάρτηση με πεδίο ορισμού το $\mathbb{N}$ (ή τμήμα του $\mathbb{N}$) και πεδίο τιμών το $\mathcal{P}(\mathcal{U})$. Έστω τώρα (X_i) μια

άπειρη ακολουθία στοιχείων του $\mathcal{P}(\mathcal{U})$. Με άλλα λόγια (X_i) είναι μια άπειρη ακολουθία υποσυνόλων του $\mathcal{U}$. Τότε η εικόνα της ακολουθίας αυτής αποτελεί μια συλλογή $\mathcal{C}$ υποσυνόλων του $\mathcal{U}$. Σε τέτοια περίπτωση, συνήθως γράφουμε $\bigcup_{i \in \mathbb{N}} X_i$ ή $\bigcup_{i=1}^{\infty} X_i$ αντί για $\bigcup_{X \in \mathcal{C}} X$. Παρόμοια γράφουμε $\bigcap_{i \in \mathbb{N}} X_i$ ή $\bigcap_{i=1}^{\infty} X_i$ αντί για $\bigcap_{X \in \mathcal{C}} X$. Αν τώρα $(Y_i)_{i=1}^n$ είναι μια πεπερασμένη ακολουθία υποσυνόλων του $\mathcal{U}$ γράφουμε $\bigcup_{i=1}^n Y_i = Y_1 \cup Y_2 \cup \dots \cup Y_n$ και $\bigcap_{i=1}^n Y_i = Y_1 \cap Y_2 \cap \dots \cap Y_n$.

Παράδειγμα. Θέτουμε $A: \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N}) : n \mapsto \{1, 2, \dots, n\}$, ($n \in \mathbb{N}$). Έχουμε τότε ότι $A_1 (= A(1)) = \{1\}$, $A_2 (= A(2)) = \{1, 2\}$, $A_3 = \{1, 2, 3\}$, $\dots$, $A_n = \{1, 2, \dots, n\}$, $\dots$ είναι μια ακολουθία υποσυνόλων του $\mathbb{N}$. Εύκολα παρατηρούμε ότι $A_n \subseteq A_{n+1}$ για κάθε $n \in \mathbb{N}$. Έχουμε επίσης ότι $\bigcup_{i=1}^{\infty} A_n = \mathbb{N}$ και $\bigcap_{i=1}^{\infty} A_n = \{1\}$.

Σύνολα δεικτών. Έστω τώρα Λ ένα σύνολο δεικτών και $\{A_\lambda\}_{\lambda \in \Lambda}$ μια συλλογή υποσυνόλων του μη-κενού συνόλου $\mathcal{U}$. (Αυτό σημαίνει ότι θεωρούμε εδώ μια συνάρτηση από το μη-κενό σύνολο Λ στο δυναμοσύνολο του $\mathcal{U}$ και, επεκτείνοντας τον συμβολισμό που έχουμε για ακολουθίες, γράφουμε A_λ αντί για $A(\lambda)$, όπου το υποσύνολο $A(\lambda)$ του $\mathcal{U}$ είναι η εικόνα του $\lambda \in \Lambda$ μέσω της συνάρτησης αυτής.)

Με παρόμοιο τρόπο όπως στην περίπτωση που έχουμε ακολουθίες υποσυνόλων, γράφουμε $\bigcup_{\lambda \in \Lambda} A_\lambda$ και $\bigcap_{\lambda \in \Lambda} A_\lambda$ αντίστοιχα για την ένωση και την τομή της συλλογής $\{A_\lambda\}_{\lambda \in \Lambda}$. Έχουμε δηλαδή (συγκρίνετε με την συζήτηση στο Κεφάλαιο 2), ότι $\bigcup_{\lambda \in \Lambda} A_\lambda = \{x \in \mathcal{U} : x \in A_\lambda \text{ για κάποιο } \lambda \in \Lambda\}$ και $\bigcap_{\lambda \in \Lambda} A_\lambda = \{x \in \mathcal{U} : x \in A_\lambda \text{ για όλα τα } \lambda \in \Lambda\}$.

Στην ειδική περίπτωση που Λ είναι το σύνολο $\mathbb{N}$ των φυσικών αριθμών, ο συμβολισμός αυτός συμπίπτει με τον συμβολισμό που έχουμε εισαγάγει πιο πάνω στην περίπτωση που θεωρούμε ακολουθίες υποσυνόλων του $\mathcal{U}$.

Σημειώσεις και Σχόλια

1. Η μαθηματική έννοια της συνάρτησης εμφανίστηκε τον 17^ο αιώνα μαζί με την ανάπτυξη του λογισμού (calculus). Ο όρος αυτός (με μια κάπως πιο στενή έννοια) χρησιμοποιήθηκε για πρώτη φορά από τον Leibniz το 1692. Λίγο αργότερα, σε μια επιστολή του προς τον Leibniz, ο Johann Bernoulli έδωσε σε αυτόν τον όρο μια έννοια που είναι πιο κοντά στην σύγχρονη.

2. Ο τρόπος που έχουμε ορίσει την συνάρτηση, μας βοηθά να έχουμε πιο εύκολα μια διαισθητική εικόνα για την έννοια αυτή. Στην βιβλιογραφία συναντάμε συχνά και τον εξής ορισμό: “Έστω X, Y δύο (μη-κενά) σύνολα. Μια συνάρτηση f από το X στο Y είναι ένα (μη-κενό) υποσύνολο του καρτεσιανού γινομένου $X \times Y$ με την ιδιότητα ότι για κάθε $x \in X$ υπάρχει ακριβώς ένα $y \in Y$ τέτοιο ώστε $(x, y) \in f$.” (Πολύ συχνά δεν τίθεται ο περιορισμός τα σύνολα X, Y να είναι μη-κενά.)

Ασκήσεις

3.1 Έστω Y το σύνολο των περιττών φυσικών αριθμών. Θέτουμε $f: \mathbb{N} \rightarrow Y : n \mapsto 2n - 1$, ($n \in \mathbb{N}$). Δείξτε ότι f είναι αμφιμονοσήμαντη και βρείτε την αντίστροφη συνάρτηση.

- 3.2 Είναι το σύνολο $\{(x, 1) : x \in \mathbb{N}\} \cup \{(x, 0) : x \in \mathbb{R} - \mathbb{N}\}$ το γράφημα μιας συνάρτησης από το $\mathbb{R}$ στο $\mathbb{Z}$;
- 3.3 Το πλήθος των στοιχείων των συνόλων X και Y είναι 4 και 3 αντίστοιχα.
 (i) Υπάρχει επί συνάρτηση από το X στο Y ;
 (ii) Υπάρχει 1-1 συνάρτηση από το X στο Y ;
 (iii) Βρείτε το πλήθος των συναρτήσεων που έχουν πεδίο ορισμού το X και πεδίο τιμών το Y .
 (iv) Αν Γ είναι το γράφημα μιας συνάρτησης από το X στο Y , βρείτε το πλήθος των στοιχείων του Γ .
- 3.4 Έστω οι συναρτήσεις f, g, h από το $\mathbb{N}$ στο $\mathbb{N}$ ορισμένες με

$$f(x) = \begin{cases} 1, & (x > 100), \\ 2, & (x \leq 100) \end{cases}, \quad g(x) = x^2 + 1, \quad h(x) = 2x + 1 \text{ για κάθε } x \in \mathbb{N}.$$
 (i) Εξετάστε κατά πόσον οι συναρτήσεις αυτές είναι (a) 1-1 (b) επί.
 (ii) Επαληθεύστε ότι $h \circ (g \circ f) = (h \circ g) \circ f$.
- 3.5 Μπορείτε να βρείτε μια αμφιμονοσήμαντη συνάρτηση από τους άρτιους φυσικούς στους περιττούς φυσικούς;
- 3.6 Το πλήθος των στοιχείων των συνόλων X και Y είναι 3 και 5 αντίστοιχα.
 (i) Υπάρχει επί συνάρτηση από το X στο Y ;
 (ii) Υπάρχει 1-1 συνάρτηση από το X στο Y ;
 (iii) Υπάρχει αμφιμονοσήμαντη συνάρτηση από το X στο Y ;
 (iv) Βρείτε το πλήθος των στοιχείων του καρτεσιανού γινομένου $X \times Y$.
- 3.7 (i) Βρείτε μια συνάρτηση από το $\mathbb{N}$ στο $\mathbb{N}$ η οποία είναι 1-1, όμως δεν είναι επί.
 (ii) Βρείτε μια συνάρτηση από το $\mathbb{N}$ στο $\mathbb{N}$ η οποία είναι επί, όμως δεν είναι 1-1.
 (iii) Βρείτε δυο αμφιμονοσήμαντες συναρτήσεις f, g από το $\mathbb{N}$ στο $\mathbb{N}$ με $f \circ g \neq g \circ f$.
- 3.8 Έστω οι συναρτήσεις $f : X \rightarrow Y$ και $g : Y \rightarrow Z$. Δείξτε ότι
 (i) Αν f και g είναι 1-1, τότε $g \circ f$ είναι 1-1.
 (ii) Αν $g \circ f$ είναι 1-1, τότε f είναι 1-1.
 (iii) Αν f και g είναι επί, τότε $g \circ f$ είναι επί.
 (iv) Αν $g \circ f$ είναι επί, τότε g είναι επί.
 Να δώσετε επίσης παράδειγμα συναρτήσεων f, g , όπου $g \circ f$ είναι 1-1, όμως g δεν είναι 1-1.
- 3.9 Έστω $f : X \rightarrow Y$ μια απεικόνιση, $A, B \subseteq X$ και $\Gamma, \Delta \subseteq Y$. Δείξτε ότι
 (i) $f(A \cup B) = f(A) \cup f(B)$
 (ii) $f(A \cap B) \subseteq f(A) \cap f(B)$
 (iii) $f^{-1}(\Gamma \cup \Delta) = f^{-1}(\Gamma) \cup f^{-1}(\Delta)$
 (iv) $f^{-1}(\Gamma \cap \Delta) = f^{-1}(\Gamma) \cap f^{-1}(\Delta)$
 (v) $f^{-1}(Y - \Gamma) = X - f^{-1}(\Gamma)$
 (vi) $f(f^{-1}(\Gamma)) \subseteq \Gamma$
 (vii) $A \subseteq f^{-1}(f(A))$
 (viii) αν, επιπλέον, η f είναι 1-1, τότε $f(A \cap B) = f(A) \cap f(B)$
- 3.10 Βρείτε παραδείγματα συναρτήσεων $f : X \rightarrow Y$ και $g : Y \rightarrow X$ που ικανοποιούν $g \circ f = i_X$ με την f (αντίστοιχα, την g) να μην είναι επιρριπτική (αντίστοιχα, να μην είναι ενριπτική). Συγκρίνετε με την Πρόταση 3.5.
- 3.11 Για κάθε $n \in \mathbb{N}$, θέτουμε $A_n = \{n, n+1, n+2, \dots\} (= \mathbb{N} - \{1, 2, \dots, n\})$.
 (i) Δείξτε ότι $A_{n+1} \subseteq A_n$ για κάθε $n \in \mathbb{N}$. Δείξτε επίσης ότι $\bigcup_{i=1}^{\infty} A_i = \mathbb{N}$ και ότι $\bigcap_{i=1}^{\infty} A_i = \emptyset$.
 (ii) Θέτουμε $B_n = \{-x : x \in A_n\} (\subseteq \mathbb{Z})$. Βρείτε τα $\bigcup_{i=1}^{\infty} B_i$ και $\bigcap_{i=1}^{\infty} B_i$.
- 3.12 Έστω $f : X \rightarrow Y$ μια συνάρτηση. Αν $(A_i)_{i=1}^{\infty}$ (αντίστοιχα, $(B_i)_{i=1}^{\infty}$) είναι μια ακολουθία υποσυνόλων του X (αντίστοιχα, υποσυνόλων του Y) και $n \in \mathbb{N}$, δείξτε ότι $f(\bigcup_{i=1}^n A_i) = \bigcup_{i=1}^n f(A_i)$ και ότι $f^{-1}(\bigcap_{i=1}^n B_i) = \bigcap_{i=1}^n f^{-1}(B_i)$.

- 3.13 Έστω $\mathcal{B}$ μια άλγεβρα Boole υποσυνόλων ενός συνόλου $\mathcal{U}$. Αν $(A_i)_{i=1}^{\infty}$ είναι μια άπειρη ακολουθία στοιχείων της $\mathcal{B}$, δείξτε ότι υπάρχει ακολουθία $(B_i)_{i=1}^{\infty}$ στοιχείων της $\mathcal{B}$ τέτοια ώστε $B_n \cap B_m = \emptyset$ οποτεδήποτε $n \neq m$, και $\bigcup_{i=1}^{\infty} B_i = \bigcup_{i=1}^{\infty} A_i$. [Υπόδειξη: Θέτουμε $B_1 = A_1$, και για κάθε $n \in \mathbb{N}$ με $n > 1$ θέτουμε $B_n = A_n - (\bigcup_{i=1}^{n-1} A_i)$.]
- 3.14 Έστω X ένα σύνολο. Θέτουμε $f: \mathcal{P}(X) \rightarrow \mathcal{P}(X) : A \mapsto X - A$ ($A \subseteq X$). Δείξτε ότι f είναι αμφιμονοσήμαντη συνάρτηση και, επιπλέον, έχει τις εξής ιδιότητες:
- (i) $f(A) \supseteq f(B)$ οποτεδήποτε $A \subseteq B$,
 - (ii) $f(A \cup B) = f(A) \cap f(B)$, και
 - (iii) $f(A \cap B) = f(A) \cup f(B)$, (όπου $A, B \subseteq X$).
- 3.15 Θέτουμε $T = \{2n : n \in \mathbb{N}\}$, το σύνολο των άρτιων φυσικών αριθμών. Δείξτε ότι η συνάρτηση $g: T \rightarrow \mathbb{N} - \{1\} : t \mapsto [\frac{1}{2}t + 1]$, $t \in T$, είναι αμφιμονοσήμαντη και βρείτε την συνάρτηση g^{-1} .

4. Διμελείς πράξεις

4.1. Ορισμοί, παραδείγματα

Ορισμός. Έστω S ένα μη-κενό σύνολο. Μια διμελής πράξη (ή εσωτερική πράξη) πάνω στο σύνολο S είναι μια συνάρτηση $\phi: S \times S \rightarrow S$. Έτσι, για κάθε διατεταγμένο ζεύγος $(a, b) \in S \times S$ αντιστοιχεί ένα στοιχείο $\phi((a, b)) \in S$.

Συνήθως για την εικόνα $\phi((a, b))$ χρησιμοποιούμε το συμβολισμό $a \circ b$, όπου $\circ$ είναι σύμβολο χαρακτηριστικό της πράξης. Τέτοια σύμβολα είναι επίσης τα $\cdot, +, \bullet, *$.

Παραδείγματα 4.1. (i) Οι συναρτήσεις

$$\phi_1: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}: (x, y) \mapsto x + y \text{ (συννηθισμένη πρόσθεση ακεραίων)}$$

$$\phi_2: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}: (x, y) \mapsto xy \text{ (συννηθισμένος πολλαπλασιασμός ακεραίων)}$$

$$\phi_3: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}: (x, y) \mapsto (x + y) + xy (= \phi_1(\phi_1(x, y), \phi_2(x, y))),$$

(όπου $x, y \in \mathbb{Z}$), αποτελούν διμελείς πράξεις πάνω στο σύνολο $\mathbb{Z}$.

(ii) Έστω X ένα σύνολο. Θέτουμε $S = \mathcal{P}(X)$. Τότε οι συναρτήσεις

$$\psi_1: S \times S \rightarrow S: (A, B) \mapsto A \cap B,$$

$$\psi_2: S \times S \rightarrow S: (A, B) \mapsto A \cup B,$$

$$\psi_3: S \times S \rightarrow S: (A, B) \mapsto A \Delta B (= (A \cup B) - (A \cap B)),$$

(όπου $A, B \subseteq X$), είναι διμελείς πράξεις πάνω στο S .

(iii) Θέτουμε $Y = \{1, 2, 3\}$. Έστω S το σύνολο όλων των συναρτήσεων από το Y στο Y . Τότε η συνάρτηση $\chi: S \times S \rightarrow S: (f, g) \mapsto g \circ f$, όπου $g \circ f$ είναι η σύνθεση συναρτήσεων ($g, f \in S$), είναι μια διμελής πράξη στο S .

(iv) Έστω $T = \{s, t\}$ (όπου $s \neq t$). Τότε η συνάρτηση $\sigma: T \times T \rightarrow T$, όπου $\sigma(s, s) = t$, $\sigma(s, t) = s$, $\sigma(t, s) = t$ και $\sigma(t, t) = t$, είναι μια διμελής πράξη πάνω στο σύνολο T .

Συχνά μας ενδιαφέρουν οι ιδιότητες που έχει κάποια διμελής πράξη.

Παράδειγμα 4.2. Θεωρούμε την συνάρτηση ϕ_3 στο Παράδειγμα 4.1(i). Για $x, y \in \mathbb{Z}$ γράφουμε $x \circ y = (x + y) + xy$. Αν τώρα $a, b, c \in \mathbb{Z}$, παρατηρούμε ότι ισχύουν τα πιο κάτω:

(i) $a \circ b = b \circ a$, (ii) αν $a \neq -1$, τότε ισχύει $a \circ b = a \circ c$ αν, και μόνο αν, $b = c$

(iii) $(a \circ b) \circ c = a \circ (b \circ c)$.

Εξήγηση για τα (i) και (ii). Το (iii) το αφήνουμε ως άσκηση.

(i) $a \circ b = (a + b) + ab = (b + a) + ba = b \circ a$. (Χρησιμοποιήσαμε εδώ ότι η συνηθισμένη πρόσθεση και ο συνηθισμένος πολλαπλασιασμός ακεραίων ικανοποιούν την αντιμεταθετική ιδιότητα.)

(ii) Αν $b = c$, τότε $a \circ b = a \circ c$ για κάθε a , αφού ϕ_3 είναι μια συνάρτηση. Υποθέτουμε τώρα ότι $a \neq -1$. Αν $a \circ b = a \circ c$, τότε $(a + b) + ab = (a + c) + ac$. Χρησιμοποιώντας τώρα ότι η συνηθισμένη πρόσθεση ακεραίων ικανοποιεί την προσεταιριστική ιδιότητα, βλέπουμε ότι $a + (b + ab) = a + (c + ac)$. Έπεται (κοιτάζτε το Σχόλιο 4.5(i) πιο κάτω) ότι, $b + ab = c + ac$ ή, ισοδύναμα, $b(1 + a) = c(1 + a)$ από την επιμεριστική ιδιότητα ως προς την συνηθισμένη πρόσθεση και συνηθισμένο πολλαπλασιασμό ακεραίων. Συνάγουμε ότι $(b - c)(1 + a) = 0$, και επειδή $1 + a \neq 0$, έχουμε ότι $b - c = 0$. (Χρησιμοποιήσαμε εδώ ότι το γινόμενο δύο μη-μηδενικών ακεραίων είναι ένας μη-μηδενικός ακέραιος — συγκρίνετε με την συζήτηση στα Κεφάλαια 10 και 15). $\square$

Ορισμός. Έστω ρ μια διμελής πράξη πάνω στο μη-κενό σύνολο A . (Γράφουμε $a \circ b$ αντί για $\rho(a, b)$.)

- (i) Αν $a \circ b = b \circ a$ για όλα τα $a, b \in A$, τότε λέμε ότι ρ είναι *αντιμεταθετική*.
- (ii) Αν $(a \circ b) \circ c = a \circ (b \circ c)$ για όλα τα $a, b, c \in A$, τότε λέμε ότι ρ είναι *προσεταιριστική*.
- (iii) Αν υπάρχει στοιχείο $e \in A$ τέτοιο ώστε $a \circ e = a = e \circ a$ για όλα τα $a \in A$, τότε λέμε ότι e είναι ένα *ουδέτερο* στοιχείο του A ως προς την διμελή πράξη ρ .

Πρόταση 4.3. Έστω ρ μια διμελής πράξη πάνω στο μη-κενό σύνολο A . (Γράφουμε $a \circ b$ αντί για $\rho(a, b)$.) Στην περίπτωση που υπάρχει ουδέτερο στοιχείο ως προς την ρ , αυτό είναι *μοναδικό* με την ιδιότητα αυτή.

Απόδειξη. Αν $e, e' \in A$ είναι ουδέτερα στοιχεία ως προς την ρ έχουμε τότε, από την ιδιότητα των e, e' ως ουδέτερα στοιχεία, ότι $e = e \circ e' = e'$.] $\square$

Παράδειγμα 4.4. (i) (Κοιτάζτε το Παράδειγμα 4.1(i).) Ο ακέραιος 0 (αντίστοιχα, ο ακέραιος 1) αποτελεί ουδέτερο στοιχείο του $\mathbb{Z}$ ως προς την συνηθισμένη πρόσθεση ϕ_1 των ακεραίων (αντίστοιχα, πολλαπλασιασμό ϕ_2 των ακεραίων). Οι διμελείς πράξεις ϕ_1, ϕ_2 είναι και οι δύο αντιμεταθετικές και προσεταιριστικές.

(ii) Όπως έχουμε δει στο Κεφάλαιο 2, οι συναρτήσεις ψ_1, ψ_2, ψ_3 στο Παράδειγμα 4.1(ii) ικανοποιούν την αντιμεταθετική ιδιότητα και επίσης την προσεταιριστική ιδιότητα. Για ποιές από αυτές υπάρχει ουδέτερο στοιχείο;

(iii) Η διμελής πράξη χ στο Παράδειγμα 4.1(iii) δεν είναι αντιμεταθετική, είναι όμως προσεταιριστική. Η συνάρτηση i_Y είναι το ουδέτερο στοιχείο του συνόλου S ως προς την χ .

(iv) Θεωρούμε την διμελή πράξη σ πάνω στο σύνολο T στο Παράδειγμα 4.1(iv). Γράφουμε $\sigma(x, y) = x * y$ για $x, y \in T$. Προφανώς η σ δεν είναι αντιμεταθετική. Παρατηρούμε επίσης ότι $(s * s) * s = t * s = t$ και $s * (s * s) = s * t = s$ συνεπώς η σ δεν είναι προσεταιριστική.

Ένα συμπέρασμα από το παράδειγμα αυτό είναι ότι γενικά εκφράσεις της μορφής s^3 , αν δεν έχουμε ήδη ορίσει το σύμβολο αυτό, δεν έχουν νόημα.

Σχόλιο 4.5. (i) Στο Παράδειγμα 4.2 (στο τμήμα (ii) της εξήγησης) χρησιμοποιήσαμε τον εξής συλλογισμό “αν $a + x = a + y$ τότε $x = y$ (όπου $a, x, y \in \mathbb{Z}$)”. Αυτό ισχύει διότι υπάρχει ο ακέραιος $-a$ (με $a + -a = 0 (= -a + a)$) τον οποίο μπορούμε “να προσθέσουμε και στα δύο μέλη της εξίσωσης.” Στο πλαίσιο της συζήτησής μας έχουμε: $x = 0 + x = (-a + a) + x = -a + (a + x) = -a + (a + y) = (-a + a) + y = 0 + y = y$.

(ii) Συγκρίνουμε τώρα το πιο πάνω με το Παράδειγμα 4.1(iii): Θεωρούμε τις συναρτήσεις $f, g, h \in S$ που ορίζονται με $f(1) = 1, f(2) = 1, f(3) = 1, g(1) = 1, g(2) = 1, g(3) = 3, h(1) = 2, h(2) = 3$ και $h(3) = 1$. Έχουμε τότε ότι $f \circ g = f \circ h$, όμως $g \neq h$. Παρατηρούμε εδώ ότι δεν υπάρχει συνάρτηση $f_1 \in S$ με την ιδιότητα $f_1 \circ f = i_Y$ η οποία θα μπορούσε να παίξει τον ρόλο του ακεραίου $-a$ στο πρώτο μέρος του σχολίου αυτού. (Η f δεν είναι ενριπτική — συγκρίνετε με την Πρόταση 3.5.)

Ορισμός. Έστω A ένα μη-κενό σύνολο και ρ μια διμελής πράξη πάνω στο A . Υποθέτουμε, επιπλέον, ότι υπάρχει στο A ουδέτερο στοιχείο ως προς την ρ , έστω το e . Λέμε τότε ότι το στοιχείο $a \in A$ έχει συμμετρικό στοιχείο ως προς την ρ , αν υπάρχει $b \in A$ τέτοιο ώστε $\rho(a, b) = e = \rho(b, a)$.

Παράδειγμα 4.6. (i) Διατηρούμε τον συμβολισμό που είχαμε στο Σχόλιο 4.5(ii) (και στο Παράδειγμα 4.1(iii)). Τότε η συνάρτηση $f \in S$ δεν έχει συμμετρικό στοιχείο ως προς την διμελή πράξη χ (σύνθεση συναρτήσεων), ενώ η συνάρτηση h έχει (μοναδικό) συμμετρικό στοιχείο την συνάρτηση $h_1 \in S$ που ορίζεται με $h_1(1) = 3, h_1(2) = 1$ και $h_1(3) = 2$.

(ii) Στο Παράδειγμα 4.1(iv) το σύνολο T δεν έχει ουδέτερο στοιχείο ως προς την διμελή πράξη σ (επομένως δεν μπορούμε να μιλάμε για την ύπαρξη συμμετρικών στοιχείων στην περίπτωση αυτή).

Πρόταση 4.7. Έστω A ένα μη-κενό σύνολο και ϕ μια προσεταιριστική διμελής πράξη πάνω στο A . Υποθέτουμε επιπλέον ότι το A έχει ουδέτερο στοιχείο ως προς την ϕ . Αν το στοιχείο $a \in A$ έχει συμμετρικό στοιχείο ως προς την ϕ , τότε το συμμετρικό στοιχείο του a είναι μοναδικό.

Απόδειξη. Γράφουμε $x \circ y$ στην θέση του $\phi(x, y)$, για $x, y \in A$. Έστω e το ουδέτερο στοιχείο του A . Αν b_1, b_2 συμμετρικά του στοιχείου $a \in A$ έχουμε τότε, $b_1 = b_1 \circ e = b_1 \circ (a \circ b_2) = (b_1 \circ a) \circ b_2 = e \circ b_2 = b_2$. $\square$

Εξωτερικές πράξεις. Έστω S, T μη-κενά σύνολα. Σε ορισμένες περιπτώσεις είναι χρήσιμο να θεωρήσουμε συναρτήσεις της μορφής $\eta: T \times S \rightarrow S$. Μια τέτοια συνάρτηση ονομάζεται *εξωτερική πράξη* πάνω στο σύνολο S .

Παράδειγμα. Έστω T ένα μη-κενό σύνολο εφοδιασμένο με μια διμελή πράξη ϕ (την οποία συμβολίζουμε με $\circ$). Έστω επίσης $n \in \mathbb{N}$. Θεωρούμε την συνάρτηση $\eta: T \times T^n \rightarrow T^n: (t, (t_1, \dots, t_n)) \rightarrow (t \circ t_1, \dots, t \circ t_n)$ (όπου $t, t_1, \dots, t_n \in T$). Τότε η είναι μια εξωτερική πράξη πάνω στο σύνολο $T^n (= T \times \dots \times T$ (n φορές)). Θα δούμε πιο συγκεκριμένα παραδείγματα τέτοιων συναρτήσεων στην συνέχεια.

Με τον όρο *αλγεβρικές δομές* εννοούμε μη-κενά σύνολα εφοδιασμένα με τουλάχιστον μια (εσωτερική ή εξωτερική) πράξη. Παραδείγματα αλγεβρικών δομών είναι οι *διανυσματικοί χώροι*, οι *ομάδες*, οι *δακτύλιοι* και τα *σώματα*, που θα μελετήσουμε με περισσότερη λεπτομέρεια στην συνέχεια.

4.2. Μεταθέσεις

Διάσημοι μαθηματικοί όπως οι Lagrange, Ruffini, Cauchy, Abel είχαν ήδη μελετήσει τις μεταθέσεις, κυρίως σε σχέση με την θεωρία των αλγεβρικών εξισώσεων, όμως ο Galois το 1830 ήταν ο πρώτος που πραγματικά κατανόησε ότι η αλγεβρική λύση μιας εξίσωσης συνδεόταν στενά με την *δομή* της ομάδας μεταθέσεων της. Στο Κεφάλαιο 12 θα μελετήσουμε με περισσότερη λεπτομέρεια τις ομάδες μεταθέσεων. Προς το παρόν θα περιοριστούμε σε κάποιους βασικούς ορισμούς.

Έστω X ένα μη-κενό σύνολο. Μια *αμφιμονοσήμαντη* συνάρτηση $\alpha: X \rightarrow X$ ονομάζεται *μετάθεση* του X . Το σύνολο όλων των μεταθέσεων του X συμβολίζεται με $\text{Sym}(X)$.

Μπορούμε να κάνουμε τις εξής παρατηρήσεις:

(i) Αν $\alpha, \beta \in \text{Sym}(X)$, τότε $\alpha \circ \beta \in \text{Sym}(X)$, αφού η σύνθεση δύο αμφιμονοσήμαντων συναρτήσεων από το X στο X είναι μια αμφιμονοσήμαντη συνάρτηση από το X στο X . Συνεπώς, η συνάρτηση $\psi: \text{Sym}(X) \times \text{Sym}(X) \rightarrow \text{Sym}(X) : (\alpha, \beta) \mapsto \alpha \circ \beta$ ($\alpha, \beta \in \text{Sym}(X)$) ορίζει μια διμελή πράξη πάνω στο σύνολο $\text{Sym}(X)$.

(ii) Έπαρξη ουδέτερου στοιχείου: Από τις ιδιότητες της ταυτοτικής συνάρτησης βλέπουμε ότι $i_X \in \text{Sym}(X)$ και $\alpha \circ i_X = \alpha = i_X \circ \alpha$ για όλα τα $\alpha \in \text{Sym}(X)$.

(iii) Έπαρξη συμμετρικών στοιχείων: Αν $\alpha \in \text{Sym}(X)$, τότε υπάρχει $\beta \in \text{Sym}(X)$ τέτοια ώστε $\alpha \circ \beta = i_X = \beta \circ \alpha$, αφού α είναι αμφιμονοσήμαντη και επομένως έχει αντίστροφη η οποία είναι επίσης αμφιμονοσήμαντη. (Έχουμε επίσης ήδη δείξει ότι η αντίστροφη μιας συνάρτησης, αν η αντίστροφη πράγματι υπάρχει, είναι μοναδική.)

(iv) Παρατηρούμε ότι $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$ για όλα τα $\alpha, \beta, \gamma \in \text{Sym}(X)$, αφού η σύνθεση συναρτήσεων είναι προσεταιριστική όπως έχουμε δει στο Κεφάλαιο 3.

Σημείωση. (Συγκρίνετε με το (ii) πιο πάνω.) Έστω $\alpha \in \text{Sym}(X)$. Τότε υπάρχει η α^{-1} και $\alpha^{-1} \in \text{Sym}(X)$. Αν τώρα $\beta \in \text{Sym}(X)$ ικανοποιεί $\alpha \circ \beta = \alpha$, έχουμε ότι $\beta = i_X \circ \beta = (\alpha^{-1} \circ \alpha) \circ \beta = \alpha^{-1} \circ (\alpha \circ \beta) = \alpha^{-1} \circ \alpha = i_X$. Συνεπώς, η συνάρτηση i_X είναι το *μοναδικό* στοιχείο της $\text{Sym}(X)$ που ικανοποιεί $\gamma \circ i_X = \gamma$ για όλα τα $\gamma \in \text{Sym}(X)$.

Έστω τώρα $n \in \mathbb{N}$. Στην πολύ σημαντική ειδική περίπτωση που $X = \{1, 2, \dots, n\}$, γράφουμε S_n αντί για $\text{Sym}(X)$. Προφανώς το σύνολο S_n έχει ακριβώς $n!$ στοιχεία.

Μια μετάθεση $\pi \in S_n$ μπορεί να παρασταθεί στην μορφή $\pi = \begin{bmatrix} 1 & 2 & \dots & n \\ x_1 & x_2 & \dots & x_n \end{bmatrix}$ όπου $x_i = \pi(i)$, για όλα τα i με $1 \leq i \leq n$ (παράσταση γραμμής).

Αν $\rho, \sigma \in S_n$, γράφουμε πιο απλά $\rho\sigma$ στην θέση της σύνθεσης $\rho \circ \sigma$ και αναφερόμαστε στην έκφραση $\rho\sigma$ ως το *γινόμενο* των δύο μεταθέσεων.

Παράδειγμα. (i) Έστω $X = \{1, 2, \dots, n\}$. Τότε $i_X = \begin{bmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{bmatrix}$.

(ii) Έστω $\pi = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix} \in S_4$. Τότε π είναι η μετάθεση του συνόλου $X = \{1, 2, 3, 4\}$ που ορίζεται με $\pi(1) = 4$, $\pi(2) = 3$, $\pi(3) = 2$ και $\pi(4) = 1$ ή, ισοδύναμα, με $\pi(i) = 5 - i$, ($1 \leq i \leq 4$). Ελέγξτε ότι $\pi\pi (= \pi \circ \pi) = i_X$.

(iii) Έστω $\alpha, \beta \in S_3$ όπου $\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$ και $\beta = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$. Έχουμε τότε $(\alpha\beta)(1) = \alpha(\beta(1)) = \alpha(2) = 2$, $(\alpha\beta)(2) = \alpha(\beta(2)) = \alpha(3) = 1$, $(\alpha\beta)(3) = \alpha(\beta(3)) = \alpha(1) = 3$. Συνεπώς $\alpha\beta = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$. Παρατηρούμε επίσης ότι $\beta\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$, και επομένως $\alpha\beta \neq \beta\alpha$. Ελέγξτε ότι $\alpha^{-1} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \alpha$ και ότι $\beta^{-1} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$.

Ορισμός. Έστω X ένα μη-κενό σύνολο, $y \in X$ και $\alpha \in \text{Sym}(X)$. Λέμε ότι η α *σταθεροποιεί* το y αν $\alpha(y) = y$, και ότι η α *μετακινεί* το y αν $\alpha(y) \neq y$.

Ορισμός. Έστω $n \in \mathbb{N}$. Έστω επίσης $i_1, i_2, \dots, i_k$ διακεκριμένοι ακέραιοι μεταξύ του 1 και του n συμπεριλαμβανομένων. (Έχουμε δηλαδή ότι $\{i_1, \dots, i_k\} \subseteq \{1, 2, \dots, n\}$.) Θεωρούμε την μετάθεση $\rho \in S_n$ που ορίζεται με $\rho(i_1) = i_2$, $\rho(i_2) = i_3$, $\dots$, $\rho(i_{k-1}) = i_k$, $\rho(i_k) = i_1$ και $\rho(j) = j$ οποτεδήποτε $j \in \{1, 2, \dots, n\} - \{i_1, \dots, i_k\}$. (Έχουμε δηλαδή ότι ρ σταθεροποιεί τους υπόλοιπους $n - k$ ακραίους.) Τότε η μετάθεση ρ ονομάζεται *k-κύκλος* (ή *κύκλος μήκους k*). Γράφουμε $\rho = (i_1 \ i_2 \ \dots \ i_k)$. Προφανώς, $\rho^{-1} = (i_k \ i_{k-1} \ \dots \ i_2 \ i_1)$.

Κάθε 1-κύκλος σταθεροποιεί κάθε στοιχείο του μη-κενού συνόλου X , επομένως όλοι οι 1-κύκλοι ισούνται με την i_X (ταυτοτική συνάρτηση).

Παράδειγμα 4.8. (i) Στην S_7 ,

$$\rho = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 5 & 4 & 7 & 6 & 2 \end{bmatrix} = (1 \ 3 \ 5 \ 7 \ 2) = (3 \ 5 \ 7 \ 2 \ 1) = (5 \ 7 \ 2 \ 1 \ 3) = (7 \ 2 \ 1 \ 3 \ 5) = (2 \ 1 \ 3 \ 5 \ 7).$$

Παρατηρούμε ότι ρ είναι ένας 5-κύκλος (και μπορεί να εκφραστεί με ακριβώς 5 διαφορετικούς τρόπους μέσω του συμβολισμού αυτού).

Θέτοντας $\rho^1 = \rho$ και $\rho^k = \rho^{k-1} \circ \rho$ για $2 \leq k \leq 5$, παρατηρούμε ότι $\rho^2 = (1 \ 5 \ 2 \ 3 \ 7)$, $\rho^3 = (1 \ 7 \ 3 \ 2 \ 5)$, $\rho^4 = (1 \ 2 \ 7 \ 5 \ 3)$ και $\rho^5 = i_X$, (όπου $X = \{1, 2, 3, 4, 5, 6, 7\}$).

(ii) Η μετάθεση $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \in S_4$ δεν ισούται με κάποιο k -κύκλο για οποιοδήποτε k .

Ορισμός. Ένας 2-κύκλος (δηλαδή ένας κύκλος της μορφής $(i_1 \ i_2)$) ονομάζεται *αντιμετάθεση* (αφού αντιμεταθέτει τα σύμβολα i_1 και i_2 ενώ σταθεροποιεί όλα τα υπόλοιπα σύμβολα).

Παράδειγμα. Θέτουμε $\rho = (1 \ 2) \in S_5$. Τότε ρ είναι μια αντιμετάθεση. Προφανώς $\rho^{-1} = \rho$ και $\rho \circ \rho = i_X$, (όπου $X = \{1, 2, 3, 4, 5\}$).

Ορισμός. (i) Οι κύκλοι $(i_1 i_2 \dots i_k)$ και $(j_1 j_2 \dots j_l)$ στην S_n ονομάζονται *ξένοι μεταξύ τους* αν η τομή υποσυνόλων $\{i_1, i_2, \dots, i_k\} \cap \{j_1, j_2, \dots, j_l\} = \emptyset$.

[Αν οι κύκλοι ρ_1, ρ_2 στην S_n είναι ξένοι μεταξύ τους, παρατηρούμε τότε ότι κάθε $x \in \{1, \dots, n\}$ που μετακινείται από τον ένα σταθεροποιείται από τον άλλο — μπορεί όμως να υπάρχουν x που σταθεροποιούνται και από τους δύο.]

(ii) Οι κύκλοι $\alpha_1, \alpha_2, \dots, \alpha_m$ (όπου $m > 2$) στην S_n καλούνται *ξένοι μεταξύ τους* αν είναι ξένοι μεταξύ τους ανά δύο (αν δηλαδή οποιοιδήποτε δύο από αυτούς είναι ξένοι μεταξύ τους).

Παράδειγμα 4.9. Θεωρούμε τους κύκλους $\rho_1, \rho_2, \sigma_1, \sigma_2$ στην S_7 , όπου $\rho_1 = (1\ 2)$, $\rho_2 = (1\ 3\ 4\ 2\ 5)$, $\sigma_1 = (1\ 3\ 4)$ και $\sigma_2 = (2\ 5)$. Παρατηρούμε ότι $\rho_1\rho_2 = (1\ 2)(1\ 3\ 4\ 2\ 5) = (1\ 3\ 4)(2\ 5) = \sigma_1\sigma_2 = (2\ 5)(1\ 3\ 4) = \sigma_2\sigma_1$. [Έχουμε δηλαδή ότι $\sigma_1\sigma_2 = \sigma_2\sigma_1$. Λέμε ότι οι μεταθέσεις σ_1, σ_2 αντιμετατίθενται.] Παρατηρούμε επίσης ότι οι κύκλοι σ_1, σ_2 είναι ξένοι μεταξύ τους αφού $\{1, 3, 4\} \cap \{2, 5\} = \emptyset$, όμως οι κύκλοι ρ_1, ρ_2 δεν είναι ξένοι μεταξύ τους αφού $\{1, 2\} \cap \{1, 3, 4, 2, 5\} \neq \emptyset$.

Αναφερόμαστε στην σύνθεση $(2\ 5)(1\ 3\ 4)$ στο Παράδειγμα 4.9 ως ένα *γινόμενο κύκλων ξένων μεταξύ τους*.

Σημείωση. Είναι εύκολο ναδειχθεί ότι κύκλοι ξένοι μεταξύ τους αντιμετατίθενται.

Ασκήσεις

4.1 Συμπληρώστε το Παράδειγμα 4.2(iii).

4.2 Εξετάστε κατά πόσον η συνάρτηση ψ_3 στο Παράδειγμα 4.1 ικανοποιεί (i) την αντιμεταθετική ιδιότητα και (ii) την προσεταιριστική ιδιότητα. Υπάρχει ουδέτερο στοιχείο ως προς την πράξη αυτή;

4.3 Βρείτε παράδειγμα μη-κενού συνόλου S με $*$ μια διμελή πράξη στο S η οποία δεν είναι προσεταιριστική, για την οποία όμως υπάρχουν ουδέτερο στοιχείο και συμμετρικά στοιχεία.

4.4 (i) Θέτουμε $S = \{x \in \mathbb{Z} : x > 0\}$. Δείξτε ότι η συνηθισμένη πρόσθεση ακεραίων ορίζει μια διμελή πράξη στο S . Υπάρχει ουδέτερο στοιχείο ως προς την πράξη αυτή;

(ii) Εξετάστε κατά πόσον η συνηθισμένη πρόσθεση ακεραίων ορίζει μια διμελή πράξη στα σύνολα
(a) $\{x \in \mathbb{Z} : x > -1\}$, και (b) $\{x \in \mathbb{Z} : x \geq -1\}$.

4.5 Εστω $X = \{1, 2, 3, 4, 5\}$. Εστω επίσης οι συναρτήσεις π_1, π_2 από το X στο X όπου $\pi_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix}$ και $\pi_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{bmatrix}$. Βρείτε τις συναρτήσεις $\pi_1^{-1}, \pi_2^{-1}, \pi_1 \circ \pi_2, \pi_2 \circ \pi_1, \pi_1^{-1} \circ \pi_2^{-1}, \pi_2^{-1} \circ \pi_1^{-1}$ και $\pi_1 \circ (1\ 2\ 4)$.

4.6 Ορίζουμε τις πιο κάτω διμελείς πράξεις στο $\mathbb{Q}$

$$\phi_1(a, b) = (a - b) + ab, \quad \phi_2(a, b) = \frac{1}{3}(a + b) \text{ όπου } a, b \in \mathbb{Q}.$$

Εξετάστε κατά πόσον οι ϕ_1, ϕ_2 ικανοποιούν

(i) την προσεταιριστική ιδιότητα (ii) την αντιμεταθετική ιδιότητα.

4.7 Εστω S ένα μη-κενό σύνολο και $\circ : S \times S \rightarrow S : (a, b) \mapsto a \circ b$ ($a, b \in S$) μια διμελής πράξη στο S η οποία ικανοποιεί την προσεταιριστική ιδιότητα. Αν $a_1, a_2, a_3, a_4 \in S$, δείξτε ότι “η σύνθεση $a_1 \circ a_2 \circ a_3 \circ a_4$ ” είναι ανεξάρτητη από τις θέσεις στις οποίες επιλέγουμε να τοποθετήσουμε τις παρενθέσεις.

5. Μαθηματική επαγωγή

5.1. Αξίωμα της επαγωγής, αρχή καλής διάταξης

Το σύνολο των φυσικών αριθμών $\mathbb{N}$ είναι ένα σημαντικό υποσύνολο του συνόλου $\mathbb{R}$ των πραγματικών. Το σύνολο $\mathbb{N}$ ικανοποιεί τις συνθήκες **(N1)**, **(N2)**, **(N3)** και **(I)** πιο κάτω:

(N1) $1 \in \mathbb{N}$,

(N2) αν $n \in \mathbb{N}$, τότε ο αριθμός $n + 1$, που καλείται ο επόμενος του n , επίσης ανήκει στο $\mathbb{N}$,

(N3) κάθε $n \in \mathbb{N} - \{1\}$ είναι ο επόμενος κάποιου στοιχείου του $\mathbb{N}$, και

Αξίωμα της επαγωγής

(I) Έστω U ένα υποσύνολο του $\mathbb{N}$ που ικανοποιεί

(i) $1 \in U$, και

(ii) για κάθε $a \in \mathbb{N}$ ισχύει: αν $a \in U$, τότε $a + 1 \in U$.

Τότε $U = \mathbb{N}$.

Το αξίωμα της επαγωγής μας οδηγεί στην

Αρχή της Μαθηματικής Επαγωγής:

(PI) Έστω ότι σε κάθε φυσικό αριθμό n αντιστοιχεί μια πρόταση $p(n)$, η τιμή αλήθειας της οποίας εξαρτάται από το n , και έστω ότι

(i) $p(1)$ είναι αληθής, και

(ii) για κάθε $k \in \mathbb{N}$ ισχύει: αν $p(k)$ είναι αληθής, τότε $p(k + 1)$ είναι αληθής.

Τότε $p(n)$ είναι αληθής για κάθε $n \in \mathbb{N}$.

Εξήγηση. Θέτουμε $U = \{n \in \mathbb{N} : p(n) \text{ είναι αληθής}\} (\subseteq \mathbb{N})$. Τότε $1 \in U$ αφού έχουμε υποθέσει ότι $p(1)$ είναι αληθής. Έστω τώρα $k \in \mathbb{N}$. Αν $k \in U$ (δηλαδή αν $p(k)$ είναι αληθής), τότε $k + 1 \in U$ διότι έχουμε υποθέσει ότι $p(k + 1)$ είναι αληθής οποτεδήποτε $p(k)$ είναι αληθής. Το αξίωμα **(I)** μας εξασφαλίζει τώρα ότι $U = \mathbb{N}$, δηλαδή ότι $p(n)$ είναι αληθής για κάθε $n \in \mathbb{N}$.

Παραδείγματα. (i) Δείξτε ότι $1 + 2 + \dots + n = \frac{1}{2}n(n + 1)$ για κάθε $n \in \mathbb{N}$.

Λύση. Για κάθε $n \in \mathbb{N}$, θέτουμε $p(n)$ να είναι η πρόταση “ $1 + 2 + \dots + n = \frac{1}{2}n(n + 1)$ ”. Έχουμε ότι $1 = \frac{1}{2} \cdot 1 \cdot 2$, άρα $p(1)$ είναι αληθής. Υποθέτουμε τώρα ότι $k \in \mathbb{N}$ και ότι

$p(k)$ είναι αληθής, υποθέτουμε δηλαδή ότι ισχύει $1 + 2 + \dots + k = \frac{1}{2}k(k+1)$. Έπεται ότι $1 + 2 + \dots + k + 1 = (1 + 2 + \dots + k) + (k+1) = \frac{1}{2}k(k+1) + (k+1) = (k+1)(\frac{1}{2}k+1) = \frac{1}{2}(k+1)(k+2)$. Επομένως $p(k+1)$ είναι αληθής. Η **(PI)** μας εξασφαλίζει τώρα ότι $p(n)$ είναι αληθής για κάθε $n \in \mathbb{N}$.

(ii) Συμβολίζουμε με $|T|$ το πλήθος των στοιχείων ενός πεπερασμένου συνόλου T . Θα δείξουμε ότι αν ένα σύνολο S έχει ακριβώς n στοιχεία, όπου $n \in \mathbb{N}$, τότε $|\mathcal{P}(S)| = 2^n$.

Λύση. Για κάθε $n \in \mathbb{N}$, έστω $p(n)$ η πρόταση: αν S είναι ένα (πεπερασμένο) σύνολο με $|S| = n$ τότε $|\mathcal{P}(S)| = 2^n$. [Προφανώς αν S_1, S_2 είναι (πεπερασμένα) σύνολα με $|S_1| = n = |S_2|$ τότε τα σύνολα $\mathcal{P}(S_1), \mathcal{P}(S_2)$ είναι επίσης πεπερασμένα και, επιπλέον, ισχύει ότι $|\mathcal{P}(S_1)| = |\mathcal{P}(S_2)|$.] Θέλουμε να δείξουμε ότι $p(n)$ είναι αληθής για κάθε $n \in \mathbb{N}$. Αν $n = 1$, τότε το S έχει $2 = 2^1$ υποσύνολα, τα $\emptyset, S$, άρα $p(1)$ είναι αληθής. Υποθέτουμε τώρα ότι $p(k)$ είναι αληθής για κάποιο $k \geq 1$. Έστω ότι το σύνολο S έχει ακριβώς $k+1$ στοιχεία και έστω c ένα από τα στοιχεία του S . Τότε το σύνολο $S - \{c\}$ έχει ακριβώς k στοιχεία και επομένως ακριβώς 2^k υποσύνολα σύμφωνα με την επαγωγική υπόθεση. Τώρα ένα υποσύνολο του S είτε περιέχει το στοιχείο c είτε δεν περιέχει το c . Αυτά που δεν περιέχουν το c είναι υποσύνολα του $S - \{c\}$, επομένως υπάρχουν ακριβώς 2^k τέτοια υποσύνολα του S (αφού κάθε υποσύνολο του $S - \{c\}$ είναι και υποσύνολο του S). Επιπλέον, κάθε υποσύνολο του S που περιέχει το c αποτελείται από ένα από τα 2^k υποσύνολα του S που δεν περιέχουν το c , με το c ως επιπρόσθετο στοιχείο. Συνεπώς, υπάρχουν ακριβώς 2^k τέτοια υποσύνολα επίσης. Έπεται ότι ο αριθμός των υποσυνόλων του S είναι $2^k + 2^k = 2(2^k) = 2^{k+1}$. Η **(PI)** μας εξασφαλίζει τώρα ότι $p(n)$ είναι αληθής για κάθε $n \in \mathbb{N}$.

Γενίκευση της μεθόδου. Συνήθως θέλουμε να δείξουμε ότι για κάθε $n \in \mathbb{N}$ η πρόταση $p(n)$ είναι αληθής. Κάποτε όμως μπορεί να συμβεί ότι θέλουμε να δείξουμε ότι $p(n)$ είναι αληθής για όλα τα n με $n \geq n_0$, όπου $n_0 \in \mathbb{Z}$. Στην περίπτωση αυτή αποδεικνύουμε ότι $p(n_0)$ είναι αληθής και ότι, για όλα τα $k \in \mathbb{Z}$ με $k \geq n_0$, ισχύει: $p(k+1)$ είναι αληθής οποτεδήποτε $p(k)$ είναι αληθής. Το ότι με αυτό τον τρόπο έχουμε δείξει ότι $p(n)$ είναι αληθής για όλα τα $n \in \mathbb{Z}$ με $n \geq n_0$ προκύπτει από τον εξής συλλογισμό: Θέτουμε $m = n - n_0 + 1$. Τότε η πρόταση $p(m)$, ως πρόταση που εξαρτάται από το m , έχει δειχτεί για $m = 1$, και για $m + 1$ οποτεδήποτε ισχύει για m (όπου $m \in \mathbb{N}$).

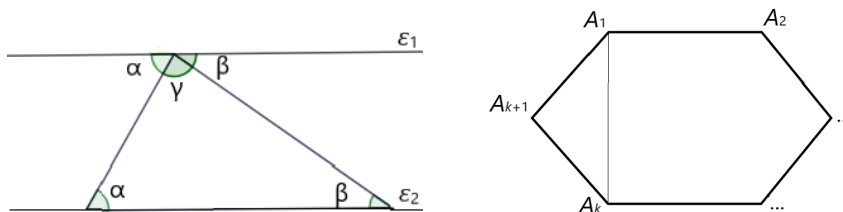
Παράδειγμα. Έστω $x \in \mathbb{R}$ με $x > -1$ και $x \neq 0$. Θα δείξουμε ότι $(1+x)^n > 1+nx$ για όλα τα $n \in \mathbb{N}$ με $n \geq 2$.

Λύση. Για κάθε $n \in \mathbb{N}$ έστω $p(n)$ η πρόταση: $(1+x)^n > 1+nx$ (όπου $x \in \mathbb{R}, x > -1$ και $x \neq 0$). (Σημειώστε ότι $p(1)$ είναι ψευδής.) Τώρα $p(2)$ είναι η πρόταση $(1+x)^2 > 1+2x$. Όμως $(1+x)^2 = 1+2x+x^2$ και $x^2 > 0$ αφού $x \neq 0$. Έπεται ότι $(1+x)^2 > 1+2x$. Συνεπώς η $p(2)$ είναι αληθής.

Έστω τώρα $k \in \mathbb{N}$ με $k \geq 2$. Υποθέτουμε ότι η $p(k)$ είναι αληθής. Έχουμε υποθέσει δηλαδή ότι $(1+x)^k > 1+kx$. Τώρα $1+x > 0$ αφού $x > -1$, επομένως $(1+x)^{k+1} > (1+kx)(1+x) = 1+(k+1)x+kx^2 > 1+(k+1)x$ (έχουμε χρησιμοποιήσει επίσης ότι $kx^2 > 0$). Βλέπουμε λοιπόν ότι η $p(k+1)$ είναι αληθής. Επομένως η $p(n)$ είναι αληθής για κάθε $n \geq 2$.

Παράδειγμα. Δείξτε ότι το άθροισμα των γωνιών ενός κυρτού n -γώνου (όπου $n \geq 3$) είναι $180(n-2)$ μοίρες. [Κυρτά σχήματα είναι αυτά που δεν διαθέτουν ευθύγραμμο τμήμα το οποίο να έχει και τα δύο του άκρα μέσα στο σχήμα, και κάποια σημεία του εκτός σχήματος.]

Λύση. Για κάθε $n \in \mathbb{N}$ με $n \geq 3$ θέτουμε $p(n)$: “ το άθροισμα των γωνιών ενός κυρτού n -γώνου είναι $180(n-2)$ μοίρες”. Η $p(n)$ είναι αληθής για $n = 3$ αφού $180(3-2) = 180$ και το άθροισμα των γωνιών οποιουδήποτε τριγώνου ισούται με 180 μοίρες όπως βλέπουμε στο σχήμα πιο κάτω χρησιμοποιώντας εντός εναλλάξ γωνίες (οι ευθείες $\varepsilon_1, \varepsilon_2$ είναι παράλληλες). Υποθέτουμε τώρα ότι $p(k)$ είναι αληθής για κάποιο $k \in \mathbb{N}$ με $k \geq 3$ και θεωρούμε ένα (τυχαίο) κυρτό $(k+1)$ -γώνο με κορυφές $A_1, A_2, A_3, \dots, A_k$ και A_{k+1} .



Επειδή το πολύγωνο $A_1A_2A_3 \dots A_kA_{k+1}$ είναι κυρτό, το ευθύγραμμο τμήμα A_1A_k , που περιέχεται ολόκληρο μέσα στο πολύγωνο, το χωρίζει σε ένα τρίγωνο $A_1A_kA_{k+1}$ και ένα k -γώνο $A_1A_2A_3 \dots A_k$ με τέτοιο τρόπο ώστε το άθροισμα των γωνιών του $A_1A_2A_3 \dots A_kA_{k+1}$ ισούται με το άθροισμα των γωνιών του $A_1A_kA_{k+1}$ και των γωνιών του $A_1A_2A_3 \dots A_k$ (κοιτάζτε το σχήμα πιο πάνω). Έχουμε δηλαδή, παρεμβάλλοντας την υπόθεση μας ότι $p(k)$ είναι αληθής, ότι το άθροισμα των γωνιών του $(k+1)$ -γώνου είναι ίσο με $180 + 180(k-2) = 180((k+1)-2)$ μοίρες, που είναι το ζητούμενο.

Θα μελετήσουμε τώρα δυο παραλλαγές του **(I)**:

(I₁) Έστω V ένα υποσύνολο του $\mathbb{N}$ που ικανοποιεί

(i) $1 \in V$, και

(ii) για κάθε $a \in \mathbb{N}$ ισχύει: αν $x \in V$ για κάθε $x \in \mathbb{N}$ με $1 \leq x < a+1$, τότε $a+1 \in V$.

Τότε $V = \mathbb{N}$.

(W) Αν θεωρήσουμε οποιοδήποτε σύνολο φυσικών αριθμών που δεν είναι κενό, πάντοτε ο ένας από αυτούς είναι ο πιο μικρός. (Δηλαδή, αν $T \subseteq \mathbb{N}$ με $T \neq \emptyset$, τότε υπάρχει $t \in T$ τέτοιο ώστε $t < z$ για κάθε άλλο $z \in T$.)

Θεώρημα 5.1. Τα **I**, **I₁**, **W** είναι ισοδύναμα.

Παρατήρηση 5.2. (i) Η **W** είναι γνωστή ως η αρχή της καλής διάταξης. Η **W** δεν ισχύει για οποιοδήποτε υποσύνολο του $\mathbb{R}$, για παράδειγμα τα σύνολα $A_1 = \{2k : k \in \mathbb{Z}\}$ και $A_2 = \{x \in \mathbb{R} : x > 0\}$ δεν περιέχουν ελάχιστο στοιχείο (ως προς την συνηθισμένη διάταξη που έχουμε στο $\mathbb{Z}$ και στο $\mathbb{R}$ — κοιτάζτε επίσης την Παράγραφο 8.2).

[Εξήγηση: Αν $2m_0$, όπου $m_0 \in \mathbb{Z}$, ήταν το ελάχιστο στοιχείο του A_1 , τότε το $2m_0 - 2 (\in A_1)$ θα ήταν μικρότερο. Επίσης, αν x_0 ήταν το ελάχιστο στοιχείο του A_2 , τότε θα είχαμε $x_0 > 0$ και $\frac{x_0}{2} \geq x_0$, αφού $\frac{x_0}{2} \in A_2$. Θα είχαμε δηλαδή ότι $1 \geq 2$ που είναι άτοπο.]

(ii) Το Θεώρημα 5.1 λέει ότι ισχύουν όλα τα πιο κάτω:

$$\mathbf{I} \Rightarrow \mathbf{I}_1, \quad \mathbf{I}_1 \Rightarrow \mathbf{I}, \quad \mathbf{I} \Rightarrow \mathbf{W}, \quad \mathbf{W} \Rightarrow \mathbf{I}, \quad \mathbf{I}_1 \Rightarrow \mathbf{W}, \quad \mathbf{W} \Rightarrow \mathbf{I}_1.$$

Για να αποδείξουμε το Θεώρημα 5.1 είναι αρκετό να δείξουμε ότι $\mathbf{W} \Leftrightarrow \mathbf{I}_1$ και $\mathbf{I} \Leftrightarrow \mathbf{W}$. Θα ήταν επίσης αρκετό να δείξουμε τα εξής: $\mathbf{I} \Rightarrow \mathbf{I}_1$, $\mathbf{I}_1 \Rightarrow \mathbf{W}$, $\mathbf{W} \Rightarrow \mathbf{I}$.

Απόδειξη Θεωρήματος 5.1. Αφήνουμε ως άσκηση την απόδειξη ότι $\mathbf{W} \Leftrightarrow \mathbf{I}_1$. Θα δείξουμε ότι $\mathbf{I} \Leftrightarrow \mathbf{W}$.

($\mathbf{I} \Rightarrow \mathbf{W}$) Υποθέτουμε ότι ισχύει το $\mathbf{I}$. Έστω ότι T είναι ένα μη-κενό υποσύνολο του $\mathbb{N}$. Θέλουμε να δείξουμε ότι το T περιέχει ελάχιστο στοιχείο. Προχωρούμε με απαγωγή σε άτοπο και υποθέτουμε ότι το T δεν έχει ελάχιστο στοιχείο. Προφανώς $1 \notin T$ (αν το 1 ήταν στοιχείο του T τότε θα ήταν και το ελάχιστο στοιχείο του T). Θέτουμε $V = \{a \in \mathbb{N} : a < t \text{ για όλα τα } t \in T\}$. Ξέρουμε ότι $1 \in V$. Ισχύει επίσης ότι $a + 1 \notin T$ οποτεδήποτε $a \in V$ (αν το $a + 1$ ήταν στοιχείο του T , τότε το $a + 1$ θα ήταν το ελάχιστο στοιχείο του T). Συμπεραίνουμε ότι $a + 1 \in V$ οποτεδήποτε $a \in V$. Το αξίωμα $\mathbf{I}$ μας εξασφαλίζει τώρα ότι $V = \mathbb{N}$. Συνάγουμε ότι $T = \emptyset$, που είναι άτοπο. [Εξήγηση: Αν $T \neq \emptyset$, τότε $t_1 \in T$, για κάποιο $t_1 \in \mathbb{N}$, άρα $V \neq \mathbb{N}$.]

($\mathbf{W} \Rightarrow \mathbf{I}$) Υποθέτουμε ότι ισχύει η $\mathbf{W}$. Έστω U ένα υποσύνολο του $\mathbb{N}$ που ικανοποιεί τις ιδιότητες (i) $1 \in U$, και (ii) για κάθε φυσικό a ισχύει ότι $a + 1 \in U$ οποτεδήποτε $a \in U$. Προχωρούμε και πάλι με απαγωγή σε άτοπο και υποθέτουμε ότι $U \subsetneq \mathbb{N}$. Τότε το σύνολο $T = \{a \in \mathbb{N} : a \notin U\}$ είναι ένα μη-κενό υποσύνολο του $\mathbb{N}$. Επομένως το T έχει ελάχιστο στοιχείο (αφού ισχύει η $\mathbf{W}$). Έστω ότι $t (\in T \subseteq \mathbb{N})$ είναι το ελάχιστο στοιχείο του T . Όμως $t \neq 1$ αφού έχουμε υποθέσει ότι $1 \in U$. Έπεται ότι $t \geq 2$ και επομένως $t - 1 \in \mathbb{N}$ και $t - 1 \notin T$. Συμπεραίνουμε ότι $t - 1 \in U$. Η ιδιότητα (ii) του συνόλου U μας εξασφαλίζει τώρα ότι $t \in U$, αφού $t = (t - 1) + 1$. Συνάγουμε ότι $t \notin T$, που είναι άτοπο. $\square$

Παράδειγμα 5.3. Έστω X ένα μη-κενό σύνολο και $\alpha_1, \dots, \alpha_n$ συναρτήσεις από το X στο X . Μπορούμε, διατηρώντας την σειρά των $\alpha_1, \dots, \alpha_n$ να κατασκευάσουμε νέες συναρτήσεις από το X στο X χρησιμοποιώντας την σύνθεση συναρτήσεων. Για παράδειγμα, στην περίπτωση που $n = 5$, ορίζονται οι συναρτήσεις $((\alpha_1 \circ \alpha_2) \circ (\alpha_3 \circ \alpha_4)) \circ \alpha_5$ και $(\alpha_1 \circ \alpha_2) \circ (\alpha_3 \circ (\alpha_4 \circ \alpha_5))$. Θα δείξουμε ότι, ανεξάρτητα από τις θέσεις στις οποίες επιλέγουμε να τοποθετήσουμε τις παρενθέσεις (διατηρώντας όμως πάντα την σειρά των $\alpha_1, \dots, \alpha_n$), οι διάφορες πιθανές “συνθέσεις $\alpha_1 \circ \alpha_2 \circ \dots \circ \alpha_n$ ” που προκύπτουν είναι ίσες.

Για να το πετύχουμε αυτό θα χρησιμοποιήσουμε επαγωγή στο n , και στην περίπτωση μας εδώ είναι πιο βολικό να χρησιμοποιήσουμε την παραλλαγή $\mathbf{I}_1$. Δεν υπάρχει τίποτα να δείξουμε όταν $n = 1$ ή $n = 2$. Για $n = 3$ υπάρχουν δύο ενδεχόμενα: $(\alpha_1 \circ \alpha_2) \circ \alpha_3$ και $\alpha_1 \circ (\alpha_2 \circ \alpha_3)$ και οι δύο αυτές συναρτήσεις είναι ίσες αφού, όπως έχουμε δείξει στο Κεφάλαιο 3, η σύνθεση

συναρτήσεων είναι προσεταιριστική. Υποθέτουμε λοιπόν ότι $n \geq 4$ και ότι το αποτέλεσμα ισχύει για όλα τα $k \in \mathbb{N}$ με $k < n$. Θεωρούμε δύο διαφορετικές τοποθετήσεις παρενθέσεων για την “σύνθεση $\alpha_1 \circ \alpha_2 \circ \dots \circ \alpha_n$ ” (διατηρώντας πάντα την σειρά των $\alpha_1, \dots, \alpha_n$). Στο προτελευταίο βήμα του υπολογισμού (σε κάθε μια από τις περιπτώσεις) θα έχουμε δύο εκφράσεις: την “σύνθεση” των $\alpha_1, \dots, \alpha_r$ και την “σύνθεση” των $\alpha_{r+1}, \dots, \alpha_n$ (ως προς κάποιες επιλογές παρενθέσεων) για κάποιο r με $1 \leq r < n$, τις οποίες και θα συνθέσουμε (χρησιμοποιώντας τώρα τον ορισμό της σύνθεσης συναρτήσεων) στο τελευταίο βήμα. Από την επαγωγική υπόθεση, κάθε μια από τις “μικρότερες εκφράσεις” είναι ανεξάρτητη από την επιλογή των παρενθέσεων, έτσι μπορούμε να γράψουμε “ολόκληρη” την σύνθεση, στην πρώτη από τις δύο περιπτώσεις που εξετάζουμε, ως $(\alpha_1 \circ \dots \circ \alpha_m) \circ (\alpha_{m+1} \circ \dots \circ \alpha_n)$ για κάποιο m με $1 \leq m < n$. Παρόμοια, η άλλη σύνθεση (που έχει προκύψει από διαφορετική τοποθέτηση των παρενθέσεων) μπορεί να εκφραστεί ως $(\alpha_1 \circ \dots \circ \alpha_l) \circ (\alpha_{l+1} \circ \dots \circ \alpha_n)$ όπου $1 \leq l < n$. Αν $m = l$, οι δύο πιο πάνω συναρτήσεις είναι ίσες. Υποθέτουμε χωρίς βλάβη της γενικότητας ότι $m < l$. Τότε $1 \leq l - m \leq n - 2$. Από την επαγωγική υπόθεση η πρώτη σύνθεση μπορεί να γραφτεί ως $(\alpha_1 \circ \dots \circ \alpha_m) \circ ((\alpha_{m+1} \circ \dots \circ \alpha_l) \circ (\alpha_{l+1} \circ \dots \circ \alpha_n))$, και η δεύτερη ως $((\alpha_1 \circ \dots \circ \alpha_m) \circ (\alpha_{m+1} \circ \dots \circ \alpha_l)) \circ (\alpha_{l+1} \circ \dots \circ \alpha_n)$, με τις εκφράσεις αυτές να ορίζουν (με μοναδικό τρόπο) συναρτήσεις από το X στο X . Όμως $(f \circ g) \circ h = f \circ (g \circ h)$ οποτεδήποτε f, g, h είναι συναρτήσεις από το X στο X , αφού η σύνθεση συναρτήσεων είναι προσεταιριστική.

Σημείωση 5.4. (i) Παρατηρούμε ότι, χωρίς να χρειάζεται οποιαδήποτε αλλαγή στην απόδειξη, το αποτέλεσμα στο Παράδειγμα 5.3 εξακολουθεί να ισχύει στην περίπτωση που έχουμε τις συναρτήσεις $\alpha_i: X_{(n+1)-i} \rightarrow X_{(n+2)-i}$ ($1 \leq i \leq n$).

(ii) Διατηρούμε τον συμβολισμό στο Παράδειγμα 5.3. Αν S είναι το σύνολο όλων των συναρτήσεων από το X στο X , η σύνθεση συναρτήσεων είναι μια διμελής πράξη πάνω στο S . Παρόμοια, θεωρούμε τώρα την “έκφραση” $\alpha_1 * \alpha_2 * \dots * \alpha_n$ (όπου η σειρά των $\alpha_1, \dots, \alpha_n$ διατηρείται) σε διαφορετικές περιπτώσεις, όπως για παράδειγμα

- (a) $\alpha_i \in \mathbb{Z}$ ($1 \leq i \leq n$) και $*$ είναι η συνηθισμένη πρόσθεση ακεραίων,
- (b) $\alpha_i \in \mathbb{Z}$ ($1 \leq i \leq n$) και $*$ είναι ο συνηθισμένος πολλαπλασιασμός ακεραίων,
- (c) $\alpha_i \in \mathcal{P}(X)$, όπου X είναι ένα σύνολο, και $*$ είναι η ένωση υποσυνόλων,
- (d) $\alpha_i \in \mathcal{P}(X)$, όπου X είναι ένα σύνολο, και $*$ είναι η τομή υποσυνόλων.

Με μια απλή προσαρμογή του συλλογισμού στο Παράδειγμα 5.3, μπορούμε να δείξουμε ότι σε κάθε μια από τις πιο πάνω περιπτώσεις το αποτέλεσμα είναι ανεξάρτητο από τις θέσεις στις οποίες επιλέγουμε να τοποθετήσουμε τις παρενθέσεις. [Συγκρίνετε επίσης τις εκφράσεις (c) και (d) με τον ορισμό των $\cup_{i=1}^n \alpha_i$ και $\cap_{i=1}^n \alpha_i$ που έχουμε δώσει στο Κεφάλαιο 2.]

Πιο γενικά, πάλι ουσιαστικά με την ίδια απόδειξη, έχουμε το εξής αποτέλεσμα:

Πρόταση 5.5. Εστω S ένα μη-κενό σύνολο και $\circ: S \times S \rightarrow S: (a, b) \mapsto a \circ b$ ($a, b \in S$) μια διμελής πράξη στο S η οποία ικανοποιεί την προσεταιριστική ιδιότητα. Αν $\alpha_1, \dots, \alpha_n \in S$, τότε “η σύνθεση $\alpha_1 \circ \dots \circ \alpha_n$ ” (όπου η σειρά των $\alpha_1, \dots, \alpha_n$ διατηρείται) είναι ανεξάρτητη από τις θέσεις στις οποίες επιλέγουμε να τοποθετήσουμε τις παρενθέσεις.

Χρησιμοποιώντας την αρχή της καλής διάταξης μπορούμε να αποδείξουμε τα ακόλουθα αποτελέσματα.

Πρόταση 5.6. Έστω $n \in \mathbb{N}$ με $n > 1$. Τότε υπάρχει πρώτος αριθμός p ο οποίος είναι διαιρέτης του n . [Λέμε ότι ο ακέραιος p είναι πρώτος αν (i) $p > 1$ και (ii) p δεν έχει άλλους θετικούς διαιρέτες εκτός από τους 1 και p . Οι πρώτοι αριθμοί έχουν πολύ σημαντικό ρόλο να παίζουν στην συνέχεια — κοιτάξτε στο Κεφάλαιο 9.]

Απόδειξη. Θέτουμε $S = \{m \in \mathbb{N} - \{1\} : m \text{ δεν έχει πρώτους διαιρέτες}\}$. Προχωρούμε με απαγωγή σε άτοπο και υποθέτουμε ότι $S \neq \emptyset$. Η αρχή της καλής διάταξης μας εξασφαλίζει ότι το σύνολο S έχει ελάχιστο στοιχείο, έστω το m_0 . Προφανώς το m_0 δεν είναι πρώτος αφού m_0 είναι διαιρέτης του m_0 . Έπεται ότι $m_0 = kl$ όπου $k, l \in \mathbb{N}$ με $1 < k < m_0$ και $1 < l < m_0$. Από την επιλογή του m_0 ως ελαχίστου στοιχείου του S , βλέπουμε ότι το k ανήκει στο σύνολο $(\mathbb{N} - \{1\}) - S$ και επομένως υπάρχει πρώτος αριθμός p ο οποίος είναι διαιρέτης του k . Έπεται ότι το p είναι επίσης διαιρέτης του m_0 , που είναι άτοπο. Συνάγουμε ότι $S = \emptyset$. $\square$

Πρόταση 5.7. Έστω $a \in \mathbb{Z}$ και $A = \{x \in \mathbb{Z} : x \geq a\}$. Τότε κάθε $S \subseteq A$ με $S \neq \emptyset$ έχει ελάχιστο στοιχείο.

Απόδειξη. Έστω $S \subseteq A$ με $S \neq \emptyset$ όπου $A = \{x \in \mathbb{Z} : x \geq a\}$. Θέτουμε $S_1 = \{x - a + 1 : x \in S\}$. Αν $y \in S_1$, τότε $y = x - a + 1$ για κάποιο $x \in S$ και επομένως $y \geq a - a + 1 = 1$. Άρα $S_1 \subseteq \mathbb{N}$. Προφανώς $S_1 \neq \emptyset$ αφού $S \neq \emptyset$. Επομένως S_1 έχει ελάχιστο στοιχείο, έστω το s_1 (αρχή της καλής διάταξης). Έπεται τότε ότι το $s = s_1 + a - 1$ είναι το ελάχιστο στοιχείο του S . [Εξήγηση: αν $x \in S$, τότε $x - a + 1 \in S_1$, άρα $s_1 \leq x - a + 1$. Έπεται ότι $s = s_1 + (a - 1) \leq x - a + 1 + (a - 1) = x$. Τέλος, το s είναι πράγματι στοιχείο του S αφού το $s_1 \in S_1$ και $s_1 = s - a + 1$.] $\square$

Στην πραγματικότητα, στην πιο πάνω πρόταση έχουμε δείξει ότι κάθε μη-κενό υποσύνολο των ακεραίων που είναι κάτω φραγμένο έχει ελάχιστο στοιχείο (ως προς την συνηθισμένη διάταξη στο $\mathbb{Z}$).

5.2. Αρχή αναδρομικού ορισμού

Στην πράξη δεν είναι πάντα βολικό να ορίσουμε μια άπειρη ακολουθία δίνοντας ένα κανόνα (τύπο) για τον n -οστό όρο της. Συχνά ορίζουμε την ακολουθία μέσω μιας αναδρομικής σχέσης η οποία συνδέει δύο ή περισσότερους διαδοχικούς όρους της ακολουθίας:

Αρχή αναδρομικού ορισμού: Έστω, για κάθε $n \in \mathbb{N}$, μια συνάρτηση $f_n : X \rightarrow X$ και έστω $c \in X$. Τότε υπάρχει μοναδική άπειρη ακολουθία (x_n) στοιχείων του X τέτοια ώστε $x_1 = c$ και $x_{n+1} = f_n(x_n)$ για κάθε $n \in \mathbb{N}$.

Είναι διαισθητικά προφανές ότι υπάρχει τέτοια ακολουθία: Ορίζουμε $x_1 = c$, $x_2 = f_1(c)$, $x_3 = f_2(f_1(c))$ κ.ο.κ. Μπορούμε όμως να δώσουμε μια απόδειξη για την ύπαρξη και μοναδικότητα τέτοιας ακολουθίας ως εξής:

Έστω U το σύνολο των φυσικών n για τα οποία ο n -οστος όρος x_n της άπειρης ακολουθίας είναι καλός ορισμένος (δηλαδή, πρώτα απ' όλα έχουμε ορισμό για τον όρο x_n και, επιπλέον, ο ορισμός που έχουμε δώσει προσδιορίζει τον x_n με μοναδικό τρόπο). Τότε $1 \in U$ (αφού $x_1 = c$). Έστω τώρα ότι $k \in U$. Αυτό σημαίνει ότι ο όρος x_k έχει προσδιοριστεί μοναδικά και επομένως και x_{k+1} προσδιορίζεται μοναδικά, αφού $x_{k+1} = f_k(x_k)$ και f_k είναι μια συνάρτηση. Συνάγουμε ότι $k+1 \in U$, οπότεδήποτε $k \in U$. Το αξίωμα της επαγωγής μας εξασφαλίζει τώρα ότι $U = \mathbb{N}$ ή, ισοδύναμα, μας εξασφαλίζει την ύπαρξη και την μοναδικότητα της ακολουθίας (x_n) .

[Για να δείξουμε την μοναδικότητα θα μπορούσαμε επίσης να χρησιμοποιήσουμε την αρχή της καλής διάταξης: Αν (y_i) είναι επίσης μια άπειρη ακολουθία φυσικών που ικανοποιεί $y_1 = c$ και $y_{i+1} = f_i(y_i)$ για κάθε $i \in \mathbb{N}$, θεωρούμε το σύνολο $S = \{k \in \mathbb{N} : x_k \neq y_k\}$. Αν $S \neq \emptyset$, τότε S έχει ελάχιστο στοιχείο, έστω το t . Τότε $t > 1$ αφού $x_1 = y_1 = c$ και, επιπλέον, έχουμε ότι $x_i = y_i$ για όλα τα i με $1 \leq i < t$. Πιο ειδικά, $x_{t-1} = y_{t-1}$ και επομένως $x_t = f_{t-1}(x_{t-1}) = f_{t-1}(y_{t-1}) = y_t$, που είναι άτοπο.]

Παραδείγματα 5.8. (i) Έστω $\alpha: Y \rightarrow Y$ μια συνάρτηση. Για κάθε $n \in \mathbb{N}$ ορίζουμε την συνάρτηση $\alpha^n: Y \rightarrow Y$ ως εξής: $\alpha^1 = \alpha$ και, για κάθε $k \in \mathbb{N}$, θέτουμε $\alpha^{k+1} = \alpha \circ (\alpha^k)$, η σύνθεση των δύο συναρτήσεων. [Στην περίπτωση αυτή, X είναι το σύνολο των συναρτήσεων από το Y στο Y , $c = \alpha$ και $f_n = f$ για όλα τα $n \in \mathbb{N}$ όπου $f: X \rightarrow X : g \mapsto \alpha \circ g$, ($g \in X$).] Η αρχή αναδρομικού ορισμού μας εξασφαλίζει ότι η συνάρτηση α^n ορίζεται με μοναδικό τρόπο για κάθε $n \in \mathbb{N}$. Συγκρίνοντας με το Παράδειγμα 5.3 βλέπουμε ότι $\alpha^n = \alpha \circ \alpha \circ \dots \circ \alpha$ (n φορές), ανεξάρτητα από τις θέσεις στις οποίες επιλέγουμε να τοποθετήσουμε τις παρενθέσεις.

(ii) Για κάθε $n \in \mathbb{N}$ ορίζουμε τον αριθμό $n!$ χρησιμοποιώντας τις ακόλουθες δύο ιδιότητες (a) $1!$ ορίζεται να είναι ίσο με 1, και (b) για κάθε $k \in \mathbb{N}$ ορίζουμε $(k+1)!$ να είναι ίσο με $(k+1)k!$. [Θέτουμε $X = \mathbb{N}$, $c = 1$ και, για κάθε $n \in \mathbb{N}$, ορίζουμε $f_n: X \rightarrow X : x \mapsto (n+1)x$, ($x \in \mathbb{N}$).]

Επέκταση της αρχής αναδρομικού ορισμού (που επίσης μπορεί να αποδειχθεί χρησιμοποιώντας μαθηματική επαγωγή — είναι όμως πιο βολικό να χρησιμοποιήσουμε την παραλλαγή **I₁** στην περίπτωση αυτή): Για κάθε φυσικό αριθμό n , έστω $f_n: X^n \rightarrow X$ μια συνάρτηση και έστω $c \in X$. Τότε υπάρχει μοναδική άπειρη ακολουθία (x_i) στοιχείων του X τέτοια ώστε $x_1 = c$ και $x_{i+1} = f_i(x_1, \dots, x_i)$ για κάθε $i \in \mathbb{N}$.

Παραδείγματα 5.9. (i) Ορίζουμε την άπειρη ακολουθία (x_n) χρησιμοποιώντας την πιο πάνω επέκταση της αρχής αναδρομικού ορισμού: Θέτουμε $X = \mathbb{N}$, $c = 1$, $f_1 = i_X$ και $f_i: X^i \rightarrow X : (x_1, \dots, x_i) \mapsto x_{i-1} + x_i$ για κάθε $i \geq 2$. Έχουμε τότε ότι οι πρώτοι πέντε όροι της ακολουθίας αυτής είναι: $x_1 = 1$, $x_2 = f_1(x_1) = x_1 = 1$, $x_3 = f_2(x_1, x_2) = x_1 + x_2 = 2$, $x_4 = f_3(x_1, x_2, x_3) = x_2 + x_3 = 3$ και $x_5 = x_3 + x_4 = 5$. Η ακολουθία αυτή είναι γνωστή ως ακολουθία Fibonacci.

(ii) Θέτουμε $X = \mathbb{N}$, $c = 1$, $f_1: X \rightarrow X : x \mapsto 5$ ($x \in X$) και $f_n: X^n \rightarrow X : (x_1, \dots, x_n) \mapsto x_n + 2x_{n-1}$ για κάθε $n \in \mathbb{N}$ με $n \geq 2$. Τότε η αντίστοιχη ακολουθία (x_i) που ορίζεται μέσω της επέκτασης της αρχής του αναδρομικού ορισμού έχει ως πρώτους πέντε όρους τους $x_1 =$

$1, x_2 = f_1(x_1) = 5, x_3 = f_2(x_1, x_2) = x_2 + 2x_1 = 7, x_4 = f_3(x_1, x_2, x_3) = x_3 + 2x_2 = 17$ και $x_5 = 31$. Χρησιμοποιώντας μαθηματική επαγωγή μπορούμε να δείξουμε ότι $x_n = 2^n + (-1)^n$ για κάθε $n \in \mathbb{N}$.

Σημειώσεις και Σχόλια

1. Η προσέγγιση μας, μέχρι το σημείο αυτό τουλάχιστον, ήταν να θεωρήσουμε ως γνωστά τα σύνολα των φυσικών, των ακεραίων, των ρητών και των πραγματικών με κάποιες στοιχειώδεις ιδιότητες που έχουν οι διμελείς πράξεις $+, \cdot$ πάνω σε αυτά, όπως επίσης και η διάταξη $<$. Σε μια προσέγγιση αξιωματικής θεμελίωσης, το σύνολο $\mathbb{N}$ ορίζεται συνήθως με τα αξιώματα (i)–(iv) πιο κάτω, που είναι γνωστά ως αξιώματα του Peano:

Το σύνολο $\mathbb{N}$ είναι ένα σύνολο τέτοιο ώστε υπάρχει μια συνάρτηση $\sigma: \mathbb{N} \rightarrow \mathbb{N}$ (ο φυσικός $\sigma(n)$ καλείται ο *επόμενος* του n , όπου $n \in \mathbb{N}$) με τις εξής ιδιότητες:

(i) υπάρχει στοιχείο $1 \in \mathbb{N}$, (ii) $\sigma(n) \neq 1$, για κάθε $n \in \mathbb{N}$, (iii) σ είναι ενριπτική, και (iv) ισχύει το αξίωμα της επαγωγής: αν $U \subseteq \mathbb{N}$ και ισχύει (a) $1 \in U$, και (b) $\sigma(x) \in U$ οποτεδήποτε $x \in U$, τότε $U = \mathbb{N}$.

Χρησιμοποιώντας τα αξιώματα αυτά μπορούμε να ορίσουμε δύο διμελείς πράξεις (πρόσθεση και πολλαπλασιασμό) στο σύνολο αυτό και να αποδείξουμε διάφορες ιδιότητες των πράξεων αυτών όπως, για παράδειγμα, την αντιμεταθετική, προσεταιριστική και επιμεριστική ιδιότητα. [Ορισμός πρόσθεσης $+$ στο $\mathbb{N}$: Για όλα τα $a, b \in \mathbb{N}$ ορίζουμε $a + 1 = \sigma(a)$ και $a + \sigma(b) = \sigma(a + b)$ — το αξίωμα (iv) μας εξασφαλίζει τότε ότι έχουμε ορίσει το άθροισμα $a + b$ για όλα $a, b \in \mathbb{N}$.] Επιπλέον, μέσω της πρόσθεσης που έχουμε ορίσει, μπορούμε να ορίσουμε την *διάταξη* $m < n$, όπου $m, n \in \mathbb{N}$ και να αποδείξουμε ιδιότητες της διάταξης αυτής όπως, για παράδειγμα, ότι για οποιαδήποτε $a, b \in \mathbb{N}$ ισχύει ακριβώς ένα από τα ακόλουθα: $a > b$, $a = b$, $a < b$. [Ορισμός διάταξης: Αν $a, b \in \mathbb{N}$, γράφουμε $a < b$ αν $a + x = b$ για κάποιο $x \in \mathbb{N}$, όπου $+$ συμβολίζει την πρόσθεση που έχουμε ορίσει προηγουμένως.]

Μια εναλλακτική προσέγγιση για το σύνολο $\mathbb{N}$ των φυσικών είναι να το *κατασκευάσουμε* (εντελώς από την αρχή) χρησιμοποιώντας μόνο εργαλεία από την θεωρία συνόλων (κοιτάξτε για παράδειγμα, το βιβλίο του P. Halmos “Naive Set Theory”).

2. Ίσως ένας από τους πρώτους που χρησιμοποίησε την επαγωγή συστηματικά ήταν ο Μαυρόλυκος το 1557, ο οποίος απέδειξε ότι “το άθροισμα ενός πλήθους περιττών σε διαδοχική σειρά, με αφετηρία τη μονάδα, δίνει το τετράγωνο του πλήθους των περιττών” (δηλαδή, με σύγχρονο συμβολισμό, $1 + 3 + 5 + \dots + (2n - 1) = n^2$), ένα αποτέλεσμα που ήταν ήδη γνωστό στους αρχαίους Πυθαγορείους. Για την απόδειξη, ο Μαυρόλυκος χρησιμοποίησε την πρόταση “κάθε τετράγωνο, όταν αυξάνεται με τον επόμενο του στην τάξη περιττό, δίνει το επόμενο στην τάξη τετράγωνο” και έτσι έδειξε ότι υπάρχει ένας γενικός τρόπος μετάβασης από μια περίπτωση στην αμέσως επόμενη.

3. Ο Pascal διατύπωσε την μαθηματική επαγωγή με πιο αυστηρό τρόπο. Η απόδειξη του ότι “το διπλάσιο του n -οστού τριγωνικού αριθμού μείον το n ισούται με n^2 ” είναι μια από τις πρώτες γνωστές εφαρμογές της μαθηματικής επαγωγής. Ο ίδιος περιέγραψε την γνωστή του απόδειξη για την πιο πάνω πρόταση ως εξής: “Αν η πρόταση αυτή έχει άπειρο αριθμό περιπτώσεων, θα δώσω μια πολύ σύντομη απόδειξη υποθέτοντας δύο λήμματα. Το πρώτο, που είναι προφανές, είναι ότι αυτή η ιδιότητα ισχύει στην $2^{\text{η}}$ γραμμή. Το δεύτερο είναι ότι αν η ιδιότητα ισχύει σε μια τυχαία γραμμή, τότε θα ισχύει απαραίτητα και στην επόμενη γραμμή. Από αυτό γίνεται φανερό ότι η πρόταση αληθεύει σε κάθε περίπτωση, διότι η ιδιότητα ισχύει στην $2^{\text{η}}$ γραμμή, λόγω του πρώτου λήμματος. Έτσι, λόγω του δευτέρου λήμματος θα ισχύει και στην $3^{\text{η}}$ γραμμή, άρα και στην $4^{\text{η}}$ κ.ο.κ., μέχρι το άπειρο.”

Ασκήσεις

5.1 Βρείτε το λάθος στον παρακάτω συλλογισμό με τον οποίο αποδεικνύεται ότι: Για οποιαδήποτε n διακεκριμένα σημεία στο ίδιο επίπεδο (όπου $n \geq 1$), υπάρχει μια ευθεία που τα ενώνει.

“Απόδειξη”: Προφανώς ισχύει για $n = 1$ και $n = 2$. Θεωρούμε ότι ισχύει για κάποιο $n = k$ και θα δείξουμε ότι ισχύει και για $n = k+1$. Έστω ότι $M_1, M_2, \dots, M_k, M_{k+1}$ είναι $k+1$ διακεκριμένα σημεία στο ίδιο επίπεδο. Από την επαγωγική υπόθεση, μπορούμε να βρούμε μια ευθεία l η οποία διέρχεται από τα πρώτα k σημεία $M_1, M_2, \dots, M_k$. Επίσης, υπάρχει μια ευθεία l' η οποία διέρχεται από τα k σημεία $M_2, \dots, M_k, M_{k+1}$. Και οι δύο ευθείες αυτές έχουν τουλάχιστον δύο κοινά σημεία, τα M_2 και M_k . Όμως υπάρχει μοναδική ευθεία που ενώνει τα M_2 και M_k . Άρα, οι ευθείες l, l' συμπίπτουν και επομένως τα $k+1$ σημεία $M_1, M_2, \dots, M_k, M_{k+1}$ ανήκουν στην ίδια ευθεία.

5.2 Δείξτε ότι για κάθε φυσικό n ισχύει:

- (i) $1 + 3 + 5 + \dots + (2n-1) = n^2$,
- (ii) $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{1}{6}n(n+1)(2n+1)$,
- (iii) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + n(n+1) = \frac{n(n+1)(n+2)}{3}$,
- (iv) $\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \dots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$.

5.3 Δείξτε ότι για κάθε ακέραιο $k > 0$, υπάρχει $a_k \in \mathbb{Z}$ τέτοιο ώστε $10^k = 9a_k + 1$.

5.4 Δείξτε ότι $2^n > n^3$ για κάθε $n \in \mathbb{N}$ με $n > 9$.

5.5 Δείξτε ότι τα $\mathbf{W}$ και $\mathbf{I}_1$ είναι ισοδύναμα.

5.6 Δείξτε, χρησιμοποιώντας μαθηματική επαγωγή, ότι αν $a, r \in \mathbb{R}$ με $r \neq 1$ τότε, για κάθε $n \in \mathbb{N}$,

$$a + ar + ar^2 + \dots + ar^n = \frac{a(1 - r^{n+1})}{1 - r}.$$

5.7 Εξετάστε κατά πόσον ισχύουν τα πιο κάτω για κάθε φυσικό n :

- (i) $5^n - 3^n + 2n$ είναι πολλαπλάσιο του 4
- (ii) n ευθείες, που βρίσκονται στον ίδιο επίπεδο, έτσι ώστε οποιεσδήποτε δύο από αυτές τέμνονται και οποιεσδήποτε τρεις από αυτές δεν τέμνονται στο ίδιο σημείο, τέμνονται σε ακριβώς $\frac{n(n-1)}{2}$ σημεία.

5.8 Θεωρούμε, για κάθε $n \in \mathbb{N}$, την εικασία $p(n)$: “ο φυσικός n είναι ίσος με $8k + 3l$ για κάποια $k, l \in \mathbb{N} \cup \{0\}$ ”. Δείξτε ότι $p(n)$ είναι αληθής για όλα τα $n \geq 14$.

5.9 Δείξτε ότι υπάρχει μοναδική άπειρη ακολουθία στοιχείων του $\mathbb{N}$ η οποία ικανοποιεί τις προϋποθέσεις: $a_1 = 1, a_2 = 2$ και $a_i = a_{i-1} + a_{i-2}$ ($i \geq 3$). Βρείτε τις τιμές των a_j ($3 \leq j \leq 7$) και δείξτε ότι $a_n < (\frac{7}{4})^n$ για κάθε $n \in \mathbb{N}$.

5.10 Διατηρούμε τον συμβολισμό και την υπόθεση στην Πρόταση 5.5 ότι $\circ$ είναι προσεταιριστική. Έστω επίσης $\sigma \in S_n$. Αν, επιπλέον, η διμελής πράξη $\circ$ είναι αντιμεταθετική, δείξτε ότι “η σύνθεση $a_{\sigma(1)} \circ a_{\sigma(2)} \circ \dots \circ a_{\sigma(n)}$ ” είναι ανεξάρτητη όχι μόνο από την επιλογή των παρενθέσεων αλλά και από την επιλογή της μετάθεσης σ .

6. Διμελείς σχέσεις, σχέσεις ισοδυναμίας

6.1. Ορισμοί, παραδείγματα, διαμερίσεις

Ορισμός. Έστω A ένα μη-κενό σύνολο. Μια διμελής σχέση στο A είναι ένα υποσύνολο του καρτεσιανού γινομένου $A \times A$.

Παράδειγμα 6.1. (i) $R_1 = \{(x, y) \in P \times P : x \text{ είναι προπαππούς του } y\}$ είναι μια διμελής σχέση στο P , όπου P συμβολίζει το σύνολο του πληθυσμού μιας πόλης,

(ii) $R_2 = \{(x, y) \in \mathbb{N} \times \mathbb{N} : x < y\}$, όπου $<$ συμβολίζει την συνηθισμένη διάταξη που έχουμε στο $\mathbb{N}$, είναι μια διμελής σχέση στο $\mathbb{N}$,

(iii) $R_3 = \{(x, y) \in \mathbb{N} \times \mathbb{N} : x \leq y\}$ είναι μια άλλη διμελής σχέση στο $\mathbb{N}$,

(iv) $R_4 = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x - y \text{ είναι άρτιος ακέραιος}\}$ είναι μια διμελής σχέση στο $\mathbb{Z}$,

(v) $R_5 = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x - y \text{ είναι πολλαπλάσιο του } 5\}$ είναι μια άλλη διμελής σχέση στο $\mathbb{Z}$. [Ο ακέραιος a είναι πολλαπλάσιο του 5 σημαίνει ότι $a = 5k$ για κάποιο ακέραιο k .]

(vi) Έστω $G = S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ και $H = \{(1), (1\ 2)\} \subseteq G$. Θέτουμε $R_6 = \{(g, f) \in G \times G : gf^{-1} (= g \circ f^{-1}) \in H\} (\subseteq G \times G)$. Τότε R_6 είναι μια διμελής σχέση στο G .

(vii) $R_7 = \{(A, B) \in \mathcal{P}(X) \times \mathcal{P}(X) : A \subseteq B\}$, όπου X είναι ένα σύνολο, είναι μια διμελής σχέση στο σύνολο $\mathcal{P}(X)$.

(viii) Έστω T το σύνολο όλων των τριγώνων στο Ευκλείδειο επίπεδο. (Μέσω της ταύτισης του Ευκλείδειου επιπέδου με το καρτεσιανό γινόμενο $\mathbb{R} \times \mathbb{R}$ μπορούμε να σκεφτούμε το T ως ένα σύνολο τα στοιχεία του οποίου είναι υποσύνολα του $\mathbb{R}^2$.) Θέτουμε $R_8 = \{(t_1, t_2) \in T \times T : \text{το } t_1 \text{ είναι όμοιο προς το } t_2\}$. Τότε R_8 είναι μια διμελής σχέση στο T .

Ορισμός. Έστω A ένα μη-κενό σύνολο και $R \subseteq A \times A$ μια διμελής σχέση στο A .

(i) Η R λέγεται *αυτοπαθής* αν $(x, x) \in R$ για όλα τα $x \in A$.

(ii) Η R λέγεται *συμμετρική* αν για όλα τα $x, y \in A$ ισχύει: αν $(x, y) \in R$, τότε $(y, x) \in R$.

(iii) Η R λέγεται *μεταβατική* αν για όλα τα $x, y, z \in A$ ισχύει: αν $(x, y) \in R$ και $(y, z) \in R$, τότε $(x, z) \in R$.

Μια διμελής σχέση στο A η οποία είναι αυτοπαθής, συμμετρική και μεταβατική καλείται *σχέση ισοδυναμίας* στο A .

Για σχέσεις ισοδυναμίας χρησιμοποιούμε συνήθως το σύμβολο $\sim$ (δηλαδή αν R είναι μια σχέση ισοδυναμίας στο A , τότε στην θέση του $(x, y) \in R$ γράφουμε $x \sim y$). Πιο ειδικά, έχουμε ότι $x \sim x$ για όλα τα $x \in A$.

Παρατηρήσεις 6.2. Διατηρούμε το συμβολισμό από το Παράδειγμα 6.1.

(i) Έχουμε ότι $(4, 4) \in R_3$, όμως $(4, 4) \notin R_2$. Έχουμε επίσης ότι $(6, -3) \notin R_5$, όμως $(m, m) \in R_5$ για όλα τα $m \in \mathbb{Z}$.

(ii) Η διμελής σχέση R_3 δεν είναι συμμετρική, αφού το στοιχείο $(3, 4)$ του $\mathbb{N} \times \mathbb{N}$ ανήκει στην R_3 , ενώ δεν συμβαίνει το ίδιο με το στοιχείο $(4, 3)$ του $\mathbb{N} \times \mathbb{N}$.

(iii) Για να δείξουμε ότι η διμελής σχέση R_5 είναι μεταβατική: Έστω $(x, y), (y, z) \in \mathbb{Z} \times \mathbb{Z}$ με $(x, y), (y, z) \in R_5$. Τότε $x - y = 5k_1$ και $y - z = 5k_2$ για κάποια $k_1, k_2 \in \mathbb{Z}$. Θέτουμε $k = k_1 + k_2$. Τότε $k \in \mathbb{Z}$ και $(x - z) = (x - y) + (y - z) = 5k_1 + 5k_2 = 5(k_1 + k_2) = 5k$.

(iv) Οι σχέσεις R_1, R_2, R_3 και R_7 δεν αποτελούν σχέσεις ισοδυναμίας ενώ οι σχέσεις R_4, R_5, R_6 και R_8 είναι σχέσεις ισοδυναμίας.

(v) Για να δείξουμε ότι η R_6 είναι μια σχέση ισοδυναμίας χρησιμοποιούμε (i) ότι η ταυτοτική συνάρτηση η οποία ισούται με την μετάθεση (1) ανήκει στο H , (ii) η αντίστροφη συνάρτηση οποιουδήποτε στοιχείου του H ανήκει στο H , και (iii) η σύνθεση δύο στοιχείων (συναρτήσεων) του H ανήκει στο H (κοιτάζτε επίσης την Άσκηση 6.7).

Ορισμός. Έστω X ένα μη-κενό σύνολο και Δ μια συλλογή μη-κενών υποσυνόλων του X τέτοια ώστε

(i) Για κάθε $X_1, X_2 \in \Delta$, είτε $X_1 = X_2$ ή $X_1 \cap X_2 = \emptyset$.

(ii) $\cup_{A \in \Delta} A = X$.

Τότε Δ ονομάζεται **διαμέριση** του συνόλου X .

Παραδείγματα 6.3. (i) Τα υποσύνολα $\{\mathbb{Z}_\alpha, \mathbb{Z}_\pi\}$ και $\{\mathbb{N}, \{0\}, \{-n : n \in \mathbb{N}\}\}$ του $\mathcal{P}(\mathbb{Z})$ είναι δύο διαφορετικές διαμερίσεις του $\mathbb{Z}$. [Συμβολίζουμε με $\mathbb{Z}_\alpha$ (αντίστοιχα, $\mathbb{Z}_\pi$) το σύνολο των άρτιων ακεραίων (αντίστοιχα, περιττών ακεραίων)].

(ii) Θέτουμε $A = \{1, 2, 3\}$. Τότε τα υποσύνολα $D_1 = \{\{1\}, \{2, 3\}\}$ και $D_2 = \{\{1\}, \{2\}, \{3\}\}$ του $\mathcal{P}(A)$ αποτελούν δύο διαφορετικές διαμερίσεις του συνόλου A .

(iii) Το υποσύνολο $\{\mathbb{Q}, \mathbb{R} - \mathbb{Q}\}$ του $\mathcal{P}(\mathbb{R})$ αποτελεί μια διαμέριση του $\mathbb{R}$.

(iv) Θέτουμε $A_1 = \{x \in \mathbb{R} : x \geq 0\}$, $A_2 = \{x \in \mathbb{R} : x \leq 0\}$, $A_3 = \{x \in \mathbb{R} : x > 0\}$ και $A_4 = \{x \in \mathbb{R} : x < 0\}$. Τότε οι συλλογές $\{A_1, A_4\}$ και $\{A_2, A_3\}$ υποσυνόλων του $\mathbb{R}$ αποτελούν διαμερίσεις του $\mathbb{R}$, δεν συμβαίνει όμως το ίδιο με τις συλλογές $\{A_1, A_2\}$ και $\{A_3, A_4\}$.

Στην συνέχεια θα δείξουμε ότι κάθε σχέση ισοδυναμίας ορίζει μια διαμέριση του συνόλου A :

Ορισμός. Έστω R μια σχέση ισοδυναμίας στο μη-κενό σύνολο A . Για κάθε $a \in A$ ορίζουμε $\bar{a} = \{x \in A : x \sim a\}$. Το υποσύνολο $\bar{a}$ του A ονομάζεται *κλάση ισοδυναμίας* του a (ως προς την σχέση R). Κάθε στοιχείο μιας κλάσης ισοδυναμίας καλείται *αντιπρόσωπος* αυτής της κλάσης. [Σημείωση: Η κλάση $\bar{a}$ μπορεί να ισούται με την κλάση $\bar{b}$ για πολλά διαφορετικά b , όπου a, b είναι στοιχεία του A .]

Παράδειγμα 6.4. Διατηρούμε το συμβολισμό από το Παράδειγμα 6.1.

(i) Οι κλάσεις ισοδυναμίας ως προς την σχέση R_5 είναι οι ακόλουθες:

$$\begin{aligned}\bar{0} &= \{x : x \in \mathbb{Z} \text{ και } x - 0 \text{ είναι πολλαπλάσιο του } 5\} \\ &= \{5k : k \in \mathbb{Z}\} = \{\dots, -10, -5, 0, 5, 10, \dots\} = \bar{5} = \overline{-15} \\ \bar{1} &= \{5k + 1 : k \in \mathbb{Z}\} = \{\dots, -9, -4, 1, 6, 11, \dots\} = \bar{6} = \overline{-29} \\ \bar{2} &= \{5k + 2 : k \in \mathbb{Z}\} = \{\dots, -8, -3, 2, 7, 12, \dots\} = \bar{7} \\ \bar{3} &= \{5k + 3 : k \in \mathbb{Z}\} = \{\dots, -7, -2, 3, 8, 13, \dots\} = \overline{-107} \\ \bar{4} &= \{5k + 4 : k \in \mathbb{Z}\} = \{\dots, -6, -1, 4, 9, 14, \dots\} = \overline{-46}\end{aligned}$$

Εύκολα παρατηρούμε επίσης ότι το υποσύνολο $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ του $\mathcal{P}(\mathbb{Z})$ είναι μια διαμέριση του $\mathbb{Z}$.

(ii) Η κλάση ισοδυναμίας ενός τριγώνου $t_1 \in T$ ως προς την σχέση R_8 αποτελείται από όλα τα τρίγωνα στο T που είναι όμοια προς το τρίγωνο t_1 .

Θεώρημα 6.5. Έστω R μια σχέση ισοδυναμίας στο μη-κενό σύνολο A . Τότε:

- (i) $\bar{a} \neq \emptyset$ για κάθε $a \in A$.
- (ii) Αν $a, b \in A$ με $b \in \bar{a}$, τότε $\bar{a} = \bar{b}$.
- (iii) Για όλα τα $a, b \in A$ έχουμε ότι $\bar{a} = \bar{b}$ αν, και μόνο αν, $(a, b) \in R$.
- (iv) Για όλα τα $a, b \in A$, είτε $\bar{a} \cap \bar{b} = \emptyset$ ή $\bar{a} = \bar{b}$.
- (v) $A = \cup_{a \in A} \bar{a}$.

Απόδειξη. Έστω $a, b \in A$. Χρησιμοποιούμε το σύμβολο $\sim$ για την σχέση ισοδυναμίας R .

- (i) Προφανώς $a \in \bar{a}$ αφού $a \sim a$.
- (ii) Αν $b \in \bar{a}$, τότε $b \sim a$ και $a \sim b$. Θα αποδείξουμε πρώτα ότι $\bar{a} \subseteq \bar{b}$: Έστω $x \in \bar{a}$. Τότε $x \sim a$. Αφού $a \sim b$ επίσης, έπεται ότι $x \sim b$ από την μεταβατική ιδιότητα. Συνάγουμε ότι $x \in \bar{b}$. Με παρόμοιο συλλογισμό μπορούμε να δείξουμε ότι $\bar{b} \subseteq \bar{a}$.
- (iii) Υποθέτουμε πρώτα ότι $\bar{a} = \bar{b}$. Τότε $a \in \bar{a} = \bar{b}$, άρα $a \sim b$. Έστω τώρα ότι $a \sim b$. Τότε $a \in \bar{b}$ και επομένως $\bar{a} = \bar{b}$ από το (ii).
- (iv) Υποθέτουμε ότι υπάρχει $c \in A$ με $c \in \bar{a} \cap \bar{b}$. Έχουμε τότε ότι $\bar{a} = \bar{c} = \bar{b}$ χρησιμοποιώντας και πάλι το (ii).
- (v) Παρατηρούμε ότι αν $c \in A$, τότε $c \in \bar{c}$, άρα $c \in \cup_{a \in A} \bar{a}$. Έπεται ότι $A \subseteq \cup_{a \in A} \bar{a}$. Προφανώς $\cup_{a \in A} \bar{a} \subseteq A$, αφού $\bar{a} \subseteq A$ για κάθε $a \in A$. □

Πόρισμα 6.6. Αν $\sim$ είναι μια σχέση ισοδυναμίας σε ένα μη-κενό σύνολο A , τότε το σύνολο των διακεκριμένων κλάσεων ισοδυναμίας ως προς την σχέση $\sim$ (το οποίο συμβολίζεται με $A/\sim$) αποτελεί μια διαμέριση του A .

Παράδειγμα 6.7. Έχουμε τις εξής κλάσεις ισοδυναμίας ως προς την πιο σχέση R_6 στο Παράδειγμα 6.1:

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

Παρατηρούμε ότι η συλλογή των αντίστοιχων κλάσεων ισοδυναμίας $\{\overline{(1)}, \overline{(1\ 3)}, \overline{(2\ 3)}\}$ αποτελεί μια διαμέριση του συνόλου $G = S_3$.

Στην επόμενη πρόταση θα δείξουμε ότι ισχύει και το αντίστροφο του Πορίσματος 6.6

Πρόταση 6.8. Έστω Δ μια διαμέριση του μη-κενού συνόλου A . Τότε υπάρχει μια σχέση ισοδυναμίας στο A οι αντίστοιχες κλάσεις ισοδυναμίας της οποίας είναι τα στοιχεία της Δ .

Απόδειξη. Θέτουμε $R = \{(a, b) \in A \times A : \text{το } a \text{ ανήκει στο ίδιο στοιχείο της } \Delta \text{ στο οποίο ανήκει και το } b\}$. Τότε R είναι μια σχέση ισοδυναμίας στο A με τις αντίστοιχες κλάσεις ισοδυναμίας να είναι τα στοιχεία της Δ . $\square$

Ορισμός. Έστω A ένα μη-κενό σύνολο. Μια διμελής σχέση R στο A καλείται *αντισυμμετρική* αν, για όλα τα $a, b \in A$, ισχύει: αν $(a, b) \in R$ και $(b, a) \in R$, τότε $a = b$.

Παράδειγμα 6.9. (i) Η σχέση R_3 στο Παράδειγμα 6.1 είναι αντισυμμετρική.

(ii) Έστω R μια σχέση ισοδυναμίας στο μη-κενό σύνολο A . Αν υπάρχει $a \in A$ με την κλάση ισοδυναμίας $\bar{a}$ του a ως προς την σχέση R να περιέχει τουλάχιστον 2 στοιχεία, τότε η σχέση R δεν είναι αντισυμμετρική.

Κλείνουμε την παράγραφο αυτή με μια σημαντική εφαρμογή της έννοιας της σχέσης ισοδυναμίας:

Ο προβολικός χώρος. Για $(x_0, x_1), (y_0, y_1) \in \mathbb{R}^2 - \{(0, 0)\}$ γράφουμε $(x_0, x_1) \sim (y_0, y_1)$ αν (και μόνο αν) υπάρχει $\lambda \in \mathbb{R} - \{0\}$ τέτοιο ώστε $y_0 = \lambda x_0$ και $y_1 = \lambda x_1$.

Εύκολα μπορούμε να δείξουμε ότι $\sim$ ορίζει μια σχέση ισοδυναμίας στο σύνολο $\mathbb{R}^2 - \{(0, 0)\}$.

Το σύνολο $(\mathbb{R}^2 - \{(0, 0)\})/\sim$ των διακεκριμένων κλάσεων ισοδυναμίας ως προς την πιο πάνω σχέση ισοδυναμίας $\sim$ συμβολίζεται με $\mathbb{P}^1(\mathbb{R})$ και ονομάζεται ο *προβολικός 1-χώρος*.

Παρατηρούμε ότι το σύνολο $\mathbb{P}^1(\mathbb{R})$ μπορεί να ταυτιστεί (χρησιμοποιώντας την αντιστοιχία μεταξύ των σημείων $P(x, y)$ στο επίπεδο και των διατεταγμένων ζευγών (x, y) στο $\mathbb{R}^2$) με την συλλογή όλων των ευθειών που διέρχονται από την αρχή των αξόνων (στην πραγματικότητα θεωρούμε τις τομές των ευθειών αυτών με το σύνολο $\mathbb{R}^2 - \{(0, 0)\}$) αφού, για $(x_0, x_1), (y_0, y_1) \in \mathbb{R}^2 - \{(0, 0)\}$ έχουμε ότι $(x_0, x_1) \sim (y_0, y_1)$ αν, και μόνο αν, τα σημεία $P(x_0, x_1)$ και $P(y_0, y_1)$ βρίσκονται στην ίδια ευθεία η οποία διέρχεται από το σημείο $O(0, 0)$.

Ο ορισμός αυτός μπορεί να επεκταθεί:

Για $(x_0, x_1, \dots, x_n), (y_0, y_1, \dots, y_n) \in \mathbb{R}^{n+1} - \{(0, 0, \dots, 0)\}$ γράφουμε $(x_0, x_1, \dots, x_n) \sim (y_0, y_1, \dots, y_n)$ αν (και μόνο αν) υπάρχει $\lambda \in \mathbb{R} - \{0\}$ τέτοιο ώστε $y_i = \lambda x_i$ για $0 \leq i \leq n$. Τότε $\sim$ ορίζει μια σχέση ισοδυναμίας στο σύνολο $\mathbb{R}^{n+1} - \{(0, 0, \dots, 0)\}$ και το σύνολο $(\mathbb{R}^{n+1} - \{(0, 0, \dots, 0)\})/\sim$ των διακεκριμένων κλάσεων ισοδυναμίας του $\mathbb{R}^{n+1} - \{(0, 0, \dots, 0)\}$ ως προς την πιο πάνω σχέση καλείται ο *προβολικός n -χώρος* $\mathbb{P}^n(\mathbb{R})$.

6.2. Κατασκευή των ακεραίων και ρητών

Στην παράγραφο αυτή θα μελετήσουμε δύο κατασκευές που χρησιμοποιούν και οι δύο την έννοια της σχέσης ισοδυναμίας: των ακεραίων από τους φυσικούς, και των ρητών από τους ακεραίους (η τελευταία αποτελεί ειδική περίπτωση της πιο γενικής κατασκευής του σώματος των πηλίκων μιας ακέραιας περιοχής).

Κατασκευή των ακεραίων. Έχοντας καθορίσει ένα σύστημα αξιωμάτων για το σύνολο $\mathbb{N}$ των φυσικών και στην συνέχεια ορίσει την πρόσθεση, τον πολλαπλασιασμό και την διάταξη, μπορούμε να αποδείξουμε τις βασικές ιδιότητες που διέπουν το σύστημα αυτό. Σε κάποιο στάδιο φυσιολογικά προκύπτουν ερωτήματα όπως, δοσμένων $a, b \in \mathbb{N}$, να βρεθεί φυσικός x με την ιδιότητα ότι $b + x = a$. Αν $b < a$, τότε υπάρχει τέτοιος φυσικός x , όχι όμως στην περίπτωση που $b \geq a$. Θέλουμε να *επεκτείνουμε* το σύστημα αριθμών $\mathbb{N}$ (με αυτό εννοούμε όχι μόνο το σύνολο $\mathbb{N}$, αλλά και την πρόσθεση, πολλαπλασιασμό και διάταξη που έχουμε ορίσει σε αυτό) σε ένα νέο σύστημα όπου όλες οι εξισώσεις της μορφής $b + x = a$ έχουν λύση (όπου, δηλαδή, η ‘διαφορά $a - b$ ’ ορίζεται πάντα). Μια πρώτη σκέψη θα ήταν να παραστήσουμε την λύση της πιο πάνω εξίσωσης (ή την ‘διαφορά $a - b$ ’) με το διατεταγμένο ζεύγος $(a, b) \in \mathbb{N} \times \mathbb{N}$. Ανακύπτει όμως το πρόβλημα ότι υπάρχουν πολλά διαφορετικά διατεταγμένα ζεύγη στο σύνολο $\mathbb{N} \times \mathbb{N}$ που θα αποτελούσαν λύσεις αυτής της εξίσωσης όπως, για παράδειγμα, το διατεταγμένο ζεύγος $(a+1, b+1)$. Θα ήταν βολικό για εμάς όλα αυτά τα διατεταγμένα ζεύγη να παριστούν τον *ίδιο ακεραίο*, με άλλα λόγια θα ήταν επιθυμητό, στο νέο μας σύστημα, τα διατεταγμένα ζεύγη (a, b) και (c, d) , όπου $a, b, c, d \in \mathbb{N}$, να *ταυτίζονται* ακριβώς στην περίπτωση που ισχύει $a + d = b + c$.

Η έννοια της σχέσης ισοδυναμίας από την Παράγραφο 6.1 παίζει καθοριστικό ρόλο στην προσπάθεια μας να το πετύχουμε αυτό: Ορίζουμε μια διμελή σχέση $\sim$ στο καρτεσιανό γινόμενο $\mathbb{N} \times \mathbb{N}$ με τον κανόνα ότι $(a, b) \sim (c, d)$ αν (και μόνο αν) $a + d = b + c$. Είναι εύκολο να ελέγξουμε τότε ότι $\sim$ είναι μια σχέση ισοδυναμίας στο σύνολο $\mathbb{N} \times \mathbb{N}$.

Ορισμός. Ένας *ακεραίος* είναι μια κλάση ισοδυναμίας ως προς την σχέση $\sim$. Συμβολίζουμε με $\mathbb{Z}$ το σύνολο των διακεκριμένων κλάσεων ισοδυναμίας ως προς την σχέση αυτή.

Είναι βολικό επίσης να ορίσουμε πρόσθεση (+) και πολλαπλασιασμό ($\cdot$) των ακεραίων (δηλαδή, των κλάσεων ισοδυναμίας που προκύπτουν από την σχέση $\sim$) ως εξής:

$$\begin{aligned}\overline{(a, b)} + \overline{(c, d)} &= \overline{(a + c, b + d)} \\ \overline{(a, b)} \cdot \overline{(c, d)} &= \overline{(ac + bd, ad + bc)}.\end{aligned}$$

[Η προσπάθειά μας, μέσω του πιο πάνω ορισμού των $+$, $\cdot$, είναι να επανακάμψουν οι γνωστές σχέσεις $(a - b) + (c - d) = (a + c) - (b + d)$ και $(a - b)(c - d) = (ac + bd) - (ad + bc)$.]

Είναι πολύ σημαντικό να ελέγξουμε ότι οι 'πράξεις' $+$, $\cdot$ που έχουμε ορίσει στο σύνολο $\mathbb{Z}$ είναι πράγματι διμελείς πράξεις στο $\mathbb{Z}$ (ότι δηλαδή πράγματι αποτελούν συναρτήσεις από το $\mathbb{Z} \times \mathbb{Z}$ στο $\mathbb{Z}$). Είναι όμως στερεότυπη η απόδειξη ότι αν $(a_1, b_1) \sim (a_2, b_2)$ και $(c_1, d_1) \sim (c_2, d_2)$ τότε, σύμφωνα με τον ορισμό μας, ισχύει $\overline{(a_1, b_1)} + \overline{(c_1, d_1)} = \overline{(a_2, b_2)} + \overline{(c_2, d_2)}$ και $\overline{(a_1, b_1)} \cdot \overline{(c_1, d_1)} = \overline{(a_2, b_2)} \cdot \overline{(c_2, d_2)}$.

Εύκολα μπορούμε επίσης να ελέγξουμε ότι ισχύουν όλες οι γνωστές ιδιότητες των ακεραίων όπως, για παράδειγμα, ότι ισχύει η αντιμεταθετική και προσεταιριστική ιδιότητα ως προς και τις δύο διμελείς πράξεις που έχουμε ορίσει πιο πάνω.

Η διάταξη στο $\mathbb{Z}$ μπορεί να οριστεί με τον κανόνα ότι $\overline{(a, b)} < \overline{(c, d)}$ αν (και μόνο αν) $a + d < b + c$ ισχύει στο $\mathbb{N}$. [Πρέπει όμως να ελεγχθεί ότι και αυτός ο ορισμός είναι ανεξάρτητος από τον αντιπρόσωπο που έχουμε επιλέξει για κάθε μια από τις αντίστοιχες κλάσεις ισοδυναμίας.]

Ο τρόπος με τον οποίο έχουμε ορίσει το σύστημα αριθμών $\mathbb{Z}$ ήταν εστιασμένος στον στόχο να είναι πράγματι το νέο σύστημα μια επέκταση του συστήματος $\mathbb{N}$ (όχι απλά μόνο ως σύνολα, αλλά και ως προς τις διμελείς πράξεις και την σχέση διάταξης στο $\mathbb{N}$). Στην πραγματικότητα το 'νέο' αυτό σύστημα $\mathbb{Z}$ περιέχει ένα 'ισομορφικό αντίγραφο' του $\mathbb{N}$: Παρατηρούμε πρώτα ότι συνάρτηση $\phi: \mathbb{N} \rightarrow \mathbb{Z} : a \mapsto \overline{(a+1, 1)}$, ($a \in \mathbb{N}$) είναι μια ενριπτική συνάρτηση αφού $\overline{(a+1, 1)} = \overline{(b+1, 1)}$, όπου $a, b \in \mathbb{N}$, συνεπάγεται ότι $(a+1)+1 = (b+1)+1$ ή, ισοδύναμα, ότι $a = b$. [Χρησιμοποιούμε εδώ τον νόμο της διαγραφής που προκύπτει και αυτός ως συνέπεια των αξιωμάτων Peano.] Μέσω της συνάρτησης ϕ 'ταυτίζουμε' το σύνολο $\mathbb{N}$ με το υποσύνολο του $\mathbb{Z}$ που αποτελείται ακριβώς από τις κλάσεις $\overline{(a+1, 1)}$, καθώς το a διατρέχει τα στοιχεία του $\mathbb{N}$.

Παρατηρούμε επίσης ότι, για όλα τα $a, b \in \mathbb{N}$, ισχύουν $\phi(a+b) = \phi(a) + \phi(b)$ και $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$, (όπου $+$, $\cdot$ στα αριστερά μέλη (αντίστοιχα, δεξιά μέλη) των πιο πάνω εξισώσεων είναι οι αντίστοιχες πράξεις στο $\mathbb{N}$ (αντίστοιχα, στο $\mathbb{Z}$)). Επιπλέον, έχουμε ότι $\phi(a) < \phi(b)$ (διάταξη στο $\mathbb{Z}$) αν, και μόνο αν, $a < b$ (διάταξη στο $\mathbb{N}$). Με άλλα λόγια, προσθέτοντας, πολλαπλασιάζοντας ή συγκρίνοντας (ως προς την αντίστοιχη ορισθείσα διμελή πράξη ή διάταξη) τους φυσικούς a, b έχουμε το ίδιο αποτέλεσμα είτε θεωρούμε τα a, b ως στοιχεία του συστήματος $\mathbb{N}$ είτε ως στοιχεία του συστήματος $\mathbb{Z}$ (μέσω της ταύτισης που έχουμε κάνει).

Τέλος, γράφοντας $\overline{(a, b)} = b - a$, προκύπτει το γνωστό μας σύστημα των ακεραίων $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.

Κατασκευή των ρητών. Έχοντας κατασκευάσει το σύστημα $\mathbb{Z}$, προκύπτει τώρα η ανάγκη να επεκταθεί το σύστημα αυτό σε ένα νέο σύστημα στο οποίο όλες οι εξισώσεις της μορφής $bx = a$, όπου $a, b \in \mathbb{Z}$ με $b \neq 0$, έχουν λύση.

Θέτουμε $\hat{\mathbb{Z}} = \mathbb{Z} - \{0\}$. Θεωρούμε το σύνολο $P = \mathbb{Z} \times \hat{\mathbb{Z}}$ και την διμελή σχέση $\sim$ στο σύνολο P που ορίζεται με $(a, b) \sim (a', b')$ αν (και μόνο αν) $ab' = a'b$, ($a, a' \in \mathbb{Z}$ και $b, b' \in \hat{\mathbb{Z}}$). Είναι εύκολο να ελεγχθεί ότι $\sim$ αποτελεί μια σχέση ισοδυναμίας στο σύνολο P .

Συμβολίζουμε με $[a/b]$ την κλάση ισοδυναμίας στην οποία ανήκει το στοιχείο (a, b) του P . Για παράδειγμα, $(3, 2) \sim (6, 4)$ και επομένως $[3/2] = [6/4]$. Έστω τώρα $F = P/\sim$, το σύνολο των διακεκριμένων κλάσεων ισοδυναμίας ως προς την πιο πάνω σχέση $\sim$. Μέσω της συνηθισμένης πρόσθεσης και του συνηθισμένου πολλαπλασιασμού ακεραίων (συγκρίνετε με το πρώτο μέρος της παραγράφου αυτής) θα προσπαθήσουμε να ορίσουμε δύο διμελείς πράξεις, πρόσθεση $\oplus$ και πολλαπλασιασμό $\odot$ πάνω στο σύνολο F ως εξής:

$$[a/b] \oplus [c/d] = [(ad + bc)/bd], \quad [a/b] \odot [c/d] = [ac/bd].$$

Παρατηρούμε πρώτα ότι $bd \neq 0$ οποτεδήποτε $b \neq 0$ και $d \neq 0$, αφού το γινόμενο δύο μη-μηδενικών ακεραίων είναι ένας μη-μηδενικός ακέραιος. Συνεπώς, στα δεξιά μέλη των πιο πάνω εξισώσεων έχουμε πράγματι στοιχεία του F .

Χρειάζεται όμως περισσότερη προσοχή: Έστω ότι $[c'/d'] = [c/d]$, όπου $c \neq c'$ ή $d \neq d'$. Αφού μια διμελής πράξη είναι μια συνάρτηση, θα πρέπει να ισχύει ότι $[a/b] \oplus [c/d] (= [a/b] \oplus [c'/d']) = [(ad + bc)/bd]$. Αν το τελευταίο δεν ισούται με $[(ad + bc)/bd]$, τότε υπάρχει πρόβλημα και ο ορισμός μας δεν έχει νόημα. Παρόμοιο πρόβλημα θα μπορούσε να εμφανιστεί και ως προς τον πολλαπλασιασμό $\odot$.

Όπως και στην περίπτωση των αντίστοιχων πράξεων πάνω στο $\mathbb{Z}$, είναι λοιπόν απαραίτητο να ελέγξουμε ότι οι $\oplus, \odot$ είναι καλά ορισμένες. Με άλλα λόγια ότι πράγματι ορίζουν συναρτήσεις από το $F \times F$ στο F . Θα ελέγξουμε εδώ ότι ο πολλαπλασιασμός $\odot$ είναι καλά ορισμένος και θα αφήσουμε για τις Ασκήσεις το αντίστοιχο αποτέλεσμα για την πρόσθεση $\oplus$. Υποθέτουμε λοιπόν ότι $[a/b] = [a'/b']$ και $[c/d] = [c'/d']$. Συνεπώς, $(a, b) \sim (a', b')$ και $(c, d) \sim (c', d')$. Άρα ισχύουν $ab' = ba'$ και $cd' = dc'$. Έπεται ότι $(ac)(b'd') = (bd)(a'c')$, και επομένως $(ac, bd) \sim (a'c', b'd')$. Συμπεραίνουμε ότι $[ac/bd] = [a'c'/b'd']$ όπως ήταν το ζητούμενο.

Είναι εύκολο επίσης να ελεγχθεί ότι ισχύουν τα ακόλουθα.

(i) Οι διμελείς πράξεις $\oplus, \odot$ είναι αντιμεταθετικές όπως επίσης και προσεταιριστικές (κληρονομούν, από τον τρόπο που τις έχουμε ορίσει, τις ιδιότητες αυτές από τις αντίστοιχες ιδιότητες που έχουν η πρόσθεση και ο πολλαπλασιασμός στο $\mathbb{Z}$).

(ii) Υπάρχει ουδέτερο στοιχείο στο F ως προς τον πολλαπλασιασμό και το στοιχείο αυτό είναι το $[1/1]$.

(iii) Αν $a \neq 0$, τότε το στοιχείο $[a/1]$ του F έχει συμμετρικό στοιχείο ως προς τον πολλαπλασιασμό, και το στοιχείο αυτό είναι το $[1/a]$. Υπάρχουν στοιχεία του F που δεν έχουν συμμετρικό ως προς τον πολλαπλασιασμό;

Σημείωση. (i) Παρατηρούμε ότι το σύνολο F ως προς τις διμελείς πράξεις $\oplus, \odot$ είναι “ουσιαστικά το ίδιο” με το σύνολο των ρητών $\mathbb{Q}$ ως προς την συνηθισμένη πρόσθεση και πολλαπλασιασμό ρητών αριθμών (ταυτίζουμε το στοιχείο $[a/b]$ του F με τον ρητό a/b). Στην πραγματικότητα, στην πιο πάνω συζήτηση έχουμε κατασκευάσει ένα “ισομορφικό αντίγραφο” (στο Κεφάλαιο 15 θα δώσουμε τον ορισμό του ισομορφισμού σωμάτων) του $\mathbb{Q}$ χρησιμοποιώντας το σύνολο $\mathbb{Z}$ και τις διμελείς πράξεις $+, \cdot$ πάνω στο $\mathbb{Z}$.

(ii) Ορίζουμε μια διάταξη στο $\mathbb{Q}$, μέσω της διάταξης που έχουμε ορίσει στο $\mathbb{Z}$, με $a/b > c/d$ αν (και μόνο αν) $ad > bc$ και $bd > 0$ ή $ad < bc$ και $bd < 0$. Παρατηρούμε τότε ότι το σύστημα αριθμών $\mathbb{Q}$ αποτελεί επέκταση του συστήματος $\mathbb{Z}$ ως προς την πρόσθεση, τον πολλαπλασιασμό και την διάταξη που έχουμε ορίσει στα συστήματα αυτά.

Ασκήσεις

- 6.1 Έστω $S = \{1, 2, 3\}$ και έστω οι σχέσεις R_1, R_2 στο S , όπου
 $R_1 = \{(1, 2), (2, 1), (3, 3), (1, 1), (1, 3), (2, 2)\}$
 $R_2 = \{(1, 1), (2, 3), (3, 2), (2, 2), (3, 3)\}$
Είναι οι R_1, R_2 σχέσεις ισοδυναμίας;
- 6.2 Ποιες από τις πιο κάτω σχέσεις στο $\mathbb{Z}$ είναι σχέσεις ισοδυναμίας;
(Για $a, b \in \mathbb{Z}$, γράφουμε $a|b$ αν υπάρχει $c \in \mathbb{Z}$ τέτοιο ώστε $b = ca$.)
(i) $R_1 = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : ab \geq 0\}$
(ii) $R_2 = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : ab > 0\}$
(iii) $R_3 = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : 2|(a-b) \text{ και } 3|(a-b)\}$
(iv) $R_4 = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : b \geq a\}$
(v) $R_5 = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a = b + 15\}$
(vi) $R_6 = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : 2|(a-b) \text{ ή } 3|(a-b)\}$
Στις περιπτώσεις που η σχέση είναι σχέση ισοδυναμίας, βρείτε την αντίστοιχη διαμέριση του $\mathbb{Z}$.
- 6.3 Έστω A ένα μη-κενό σύνολο. Εξετάστε κατά πόσον $R = \{(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(A) : X \subseteq Y\}$ είναι μια σχέση ισοδυναμίας στο $\mathcal{P}(A)$.
- 6.4 Θέτουμε $S = \mathbb{Z} \times (\mathbb{Z} - \{0\})$ και $R = \{((r, s), (t, u)) \in S \times S : ru = st\}$. Δείξτε ότι R είναι μια σχέση ισοδυναμίας στο S .
- 6.5 Ορίζουμε την σχέση $\sim$ στο $\mathbb{R}^2 - \{(0, 0)\}$ ως εξής: Για $(a, b), (c, d) \in \mathbb{R}^2 - \{(0, 0)\}$ γράφουμε $(a, b) \sim (c, d)$ αν (και μόνο αν) $\exists \lambda \in \mathbb{R}, \lambda > 0$ τέτοιο ώστε $a = \lambda c, b = \lambda d$. Δείξτε ότι η σχέση $\sim$ είναι σχέση ισοδυναμίας και περιγράψτε ένα γεωμετρικό τόπο στο xy -επίπεδο που να αποτελείται από ακριβώς ένα αντιπρόσωπο από κάθε μια από τις διακεκριμένες κλάσεις ισοδυναμίας της σχέσης $\sim$.
- 6.6 Θέτουμε $R = \{(a, b) \in \mathbb{R} \times \mathbb{R} : b - a \in \mathbb{Q}\}$. Δείξτε ότι R είναι μια σχέση ισοδυναμίας στο $\mathbb{R}$. Μπορείτε να βρείτε μια διαμέριση του $\mathbb{R} - \mathbb{Q}$ που να αποτελείται από κλάσεις ισοδυναμίας (ως προς την σχέση R);
- 6.7 Έστω $G = S_3$ και $H_1, H_2 \subseteq G$ όπου $H_1 = \{(1), (1\ 2)\}$ και $H_2 = \{(1\ 2), (1\ 3)\}$. Θεωρούμε τις διμελείς σχέσεις R_1, R_2 πάνω στο σύνολο G που ορίζονται με $R_i = \{(g, h) \in G \times G : g^{-1}h \in H_i\}, (i = 1, 2)$. Εξετάστε κατά πόσον R_1, R_2 αποτελούν σχέσεις ισοδυναμίας. Σε περίπτωση που κάποια από αυτές είναι πράγματι σχέση ισοδυναμίας βρείτε την αντίστοιχη διαμέριση του συνόλου G και συγκρίνετε με το Παράδειγμα 6.1.
- 6.8 Έστω S ένα μη-κενό σύνολο και R_1, R_2 σχέσεις ισοδυναμίας στο S . Εξετάστε κατά πόσον (i) $R_1 \cap R_2$, και (ii) $R_1 \cup R_2$ είναι σχέσεις ισοδυναμίας στο S .
- 6.9 Συμπληρώστε τους συλλογισμούς που έχουμε παραλείψει στην συζήτηση της Παραγράφου 6.2.

7. Το σύνολο των πραγματικών αριθμών

7.1. Ιδιότητες των πραγματικών αριθμών

Θεωρούμε τους πραγματικούς αριθμούς ως ένα μη-κενό σύνολο $\mathbb{R}$ με τις εξής χαρακτηριστικές ιδιότητες:

- (i) Το $\mathbb{R}$ είναι διατεταγμένο σώμα.
- (ii) Κάθε μη-κενό φραγμένο προς τα πάνω υποσύνολο του $\mathbb{R}$ έχει άνω πέρασ (αξίωμα συνέχειας).

Προχωρούμε στην εξήγηση των πιο πάνω όρων:

Διατεταγμένο σώμα. Με τον όρο αυτό εννοούμε ότι το σύνολο $\mathbb{R}$ ικανοποιεί τις ακόλουθες δύο ομάδες αξιωμάτων.

Η πρώτη ομάδα από αξιώματα είναι τα *αξιώματα σώματος*: Το σύνολο $\mathbb{R}$ είναι εφοδιασμένο με δύο διμελείς πράξεις, πρόσθεση (+) και πολλαπλασιασμό ($\cdot$), τέτοιες ώστε για κάθε $a, b, c \in \mathbb{R}$

$$(A1) \quad (a + b) + c = a + (b + c)$$

$$(A2) \quad 0 + a = a$$

$$(A3) \quad \text{υπάρχει } -a \in \mathbb{R} \text{ τέτοιο ώστε } a + (-a) = 0$$

$$(A4) \quad a + b = b + a$$

$$(M1) \quad (ab)c = a(bc)$$

$$(M2) \quad 1 \cdot a = a$$

$$(M3) \quad \text{αν } a \neq 0, \text{ υπάρχει } a^{-1} \in \mathbb{R} \text{ τέτοιο ώστε } aa^{-1} = 1$$

$$(M4) \quad ab = ba$$

$$(D) \quad (a + b)c = ac + bc.$$

Η δεύτερη ομάδα από τα αξιώματα είναι τα *αξιώματα διάταξης*: Έστω $a, b, c \in \mathbb{R}$.

$$(O1) \quad \text{ακριβώς ένα από } a < b, a = b, a > b \text{ ισχύει,}$$

$$(O2) \quad \text{αν } a > b \text{ και } b > c, \text{ τότε } a > c,$$

(O3) αν $a > b$, τότε $a + c > b + c$,

(O4) αν $a > b$ και $c > 0$, τότε $ac > bc$.

Οποιοδήποτε σύστημα ικανοποιεί τις δύο πιο πάνω ομάδες αξιωμάτων καλείται *διατεταγμένο σώμα*. Παρατηρούμε ότι το σύστημα των ρητών $\mathbb{Q}$ είναι επίσης ένα διατεταγμένο σώμα. Στην πραγματικότητα, μπορεί να αποδειχθεί ότι κάθε διατεταγμένο σώμα περιέχει 'ισομορφικά αντίγραφα' των φυσικών, των ακεραίων και των ρητών. Πιο ειδικά, στην περίπτωση των πραγματικών αριθμών έχουμε ότι $\mathbb{Q} \subseteq \mathbb{R}$ και, επιπλέον, η πρόσθεση και ο πολλαπλασιασμός στο $\mathbb{R}$, όταν περιοριστούν σε στοιχεία του $\mathbb{Q}$, συμπίπτουν με τις αντίστοιχες διμελείς πράξεις στο $\mathbb{Q}$. Παρόμοια για τον περιορισμό στο $\mathbb{Q}$ της διάταξης $<$ που έχουμε στο $\mathbb{R}$.

Ορισμός. Ένα υποσύνολο A του $\mathbb{R}$ λέγεται *φραγμένο προς τα πάνω* (ή *άνω φραγμένο*) αν υπάρχει $a \in \mathbb{R}$ τέτοιο ώστε για κάθε $x \in A$, να ισχύει $x \leq a$. Κάθε τέτοιος αριθμός a λέγεται *άνω φράγμα* του A .

Το αξίωμα που ξεχωρίζει τους ρητούς από τους πραγματικούς είναι το ακόλουθο.

Αξίωμα συνέχειας. Έστω S ένα φραγμένο προς τα πάνω, μη-κενό υποσύνολο των πραγματικών. Τότε υπάρχει ένας αριθμός $M \in \mathbb{R}$ τέτοιος ώστε

(B1) ο αριθμός M είναι ένα άνω φράγμα του S ,

(B2) για κάθε $\epsilon > 0$, υπάρχει $s \in S$ τέτοιο ώστε $s > M - \epsilon$.

Ορισμός. Ο αριθμός M που ικανοποιεί τις συνθήκες (B1) και (B2) πιο πάνω ονομάζεται το *άνω πέρασ* ή *supremum* του συνόλου S και συμβολίζεται με $M = \sup S$.

Παρατήρηση. [Άμεση συνέπεια του πιο πάνω ορισμού.]

(i) Το άνω πέρασ, αν υπάρχει, είναι μοναδικό.

(ii) Έστω A ένα μη-κενό, άνω φραγμένο υποσύνολο των πραγματικών. Αν a είναι οποιοδήποτε άνω φράγμα του A , τότε $\sup A \leq a$.

Παράδειγμα. Θέτουμε $S = \{x \in \mathbb{R} : x^2 < 2\}$. Τότε $0 \in S$, άρα $S \neq \emptyset$. Παρατηρούμε επίσης ότι $x \leq 2$ για όλα τα $x \in S$. [Εξήγηση: Αν $x > 2$, τότε $x \cdot x > 2 \cdot x > 2 \cdot 2 = 4$ (αξιώματα διάταξης).] Το αξίωμα της συνέχειας (S είναι ένα μη-κενό, άνω-φραγμένο υποσύνολο του $\mathbb{R}$) μας εξασφαλίζει την ύπαρξη του $\sup S$. Θέτουμε $M = \sup S$. Προφανώς $M > 0$, αφού $1 \in S$. Θα δείξουμε ότι $M^2 = 2$. Προχωρούμε με απαγωγή σε άτοπο και υποθέτουμε ότι $M^2 \neq 2$. Έχουμε τότε ότι είτε $M^2 < 2$ ή $M^2 > 2$.

(i) Αν $M^2 < 2$, τότε $(M + \epsilon)^2 = M^2 + 2M\epsilon + \epsilon^2 < M^2 + (2M + 1)\epsilon < 2$, οποτεδήποτε $0 < \epsilon < \min\left(1, \frac{2-M^2}{2M+1}\right)$. Επομένως $M + \epsilon \in S$, το οποίο προφανώς αντιφάσκει με την συνθήκη (B1).

(ii) Αν $M^2 > 2$, τότε $(M - \epsilon)^2 = M^2 - 2M\epsilon + \epsilon^2 \geq M^2 - 2M\epsilon > 2$ αν $(0 <) \epsilon < \frac{M^2-2}{2M}$, το οποίο προφανώς αντιφάσκει με το ότι $M = \sup S$.

Έχουμε δείξει στο παράδειγμα αυτό ότι στο $\mathbb{R}$ η εξίσωση $x^2 = 2$ έχει λύση, κάτι που δεν συμβαίνει στο $\mathbb{Q}$ όπως έχουμε δει στο Κεφάλαιο 1.

Ο πιο πάνω συλλογισμός μπορεί να προσαρμοστεί για να αποδειχθεί το εξής αποτέλεσμα:

Θεώρημα 7.1. Υποθέτουμε ότι $n \in \mathbb{N}$, $c \in \mathbb{R}$ και $c > 0$. Τότε η εξίσωση $x^n = c$ έχει μοναδική λύση για $x \in \mathbb{R}$, $x > 0$.

Ορισμός. Συμβολίζουμε με $\sqrt[n]{c}$ (ή με $c^{1/n}$) την μοναδική θετική λύση της εξίσωσης $x^n = c$ στο πιο πάνω θεώρημα. Αν $p \in \mathbb{Z}$ και $q \in \mathbb{N}$, ορίζουμε $c^{p/q} = (c^{1/q})^p$.

[Υπενθύμιση: Για $y \in \mathbb{R}$, $y > 0$ θέτουμε $y^0 = 1$. Θέτουμε επίσης, για $r \in \mathbb{Z}$, $r > 0$ $y^{-r} = \frac{1}{y^r}$.]

Μπορεί να δειχθεί ότι:

(i) Ο ορισμός του c^m , όπου $m = p/q$ όπου $p \in \mathbb{Z}$ και $q \in \mathbb{N}$ δεν εξαρτάται από την επιλογή των p και q . [Αν $m = \frac{p}{q} = \frac{p_1}{q_1}$, $(c^{1/q})^p = (c^{1/q_1})^{p_1}$.]

(ii) Οι νόμοι των εκθετών ικανοποιούνται, δηλαδή $c^a c^b = c^{a+b}$ και $(c^a)^b = c^{ab}$ οποτεδήποτε $c \in \mathbb{R}$, $c > 0$ και $a, b \in \mathbb{Q}$.

Ακόμα μια συνέπεια του αξιώματος της συνέχειας είναι η

Αρχιμήδεια ιδιότητα. Για κάθε $x \in \mathbb{R}$, υπάρχει $n \in \mathbb{N}$ τέτοιο ώστε $n > x$.

Απόδειξη. Προχωρούμε με απαγωγή σε άτοπο και υποθέτουμε ότι υπάρχει $x \in \mathbb{R}$ τέτοιο ώστε $n \leq x$ για όλα τα $n \in \mathbb{N}$. Τότε το $\mathbb{N}$ είναι ένα μη-κενό άνω φραγμένο υποσύνολο των πραγματικών. Το αξίωμα της συνέχειας μας εξασφαλίζει την ύπαρξη του $\sup \mathbb{N}$. Θέτουμε $M = \sup \mathbb{N}$. Τότε $M \geq n$ για κάθε $n \in \mathbb{N}$, και επομένως $M \geq n + 1$ για κάθε $n \in \mathbb{N}$, αφού $n + 1 \in \mathbb{N}$ οποτεδήποτε $n \in \mathbb{N}$. Έπεται ότι $M - 1 \geq n$ για κάθε $n \in \mathbb{N}$ που προφανώς αντιφάσκει με την επιλογή του M ως supremum του συνόλου $\mathbb{N}$. $\square$

Είμαστε τώρα σε θέση να αποδείξουμε το ακόλουθο σημαντικό

Θεώρημα 7.2. Αν $a < b$ είναι δύο τυχαίοι πραγματικοί αριθμοί, τότε υπάρχει ρητός q τέτοιος ώστε $a < q < b$. [Η ιδιότητα αυτή εκφράζεται και ως εξής “Οι ρητοί αποτελούν πυκνό υποσύνολο των πραγματικών.”]

Απόδειξη. Από την αρχιμήδεια ιδιότητα των πραγματικών, ξέρουμε ότι υπάρχει $n \in \mathbb{N}$ τέτοιος ώστε $n > \frac{2}{b-a}$. Έχουμε δηλαδή ότι $n(b-a) > 2$ και επομένως $nb > na + 2 > [na] + 1 > na$. Έπεται ότι $b > \frac{[na]+1}{n} > a$. Γράφοντας $q = \frac{[na]+1}{n}$, έχουμε ότι q είναι ρητός και ότι $a < q < b$. $\square$

Σημείωση. Το Θεώρημα 7.2 μας εξασφαλίζει όσο θέλουμε καλή “προσέγγιση” των πραγματικών με ρητούς: Δοσμένου $x \in \mathbb{R}$ και $\epsilon > 0$ υπάρχει ρητός q τέτοιος ώστε $|x - q| < \epsilon$. (Συγκρίνετε επίσης με την σηζήτηση στην Παράγραφο 7.2.)

Για παράδειγμα, $\frac{141}{100}$, $\frac{1414}{1000}$ και $\frac{14142}{10000}$ είναι ρητές προσεγγίσεις του $\sqrt{2} = 1,414213\dots$

Είναι επίσης εύκολο να δείξουμε ότι “μεταξύ δύο ρητών $q_1 < q_2$ υπάρχει άρρητος”: Θέτουμε $a = q_1 + \frac{1}{\sqrt{2}}(q_2 - q_1)$. Είναι φανερό ότι a είναι άρρητος και ικανοποιεί $q_1 < a < q_2$.

Πόρισμα 7.3. Οι άρρητοι αποτελούν πυκνό υποσύνολο των πραγματικών.

Απόδειξη. Αν $a < b$ είναι δύο τυχαίοι πραγματικοί, τότε υπάρχουν $q_1, q_2 \in \mathbb{Q}$ τέτοιοι ώστε $a < q_1 < q_2 < b$ (χρησιμοποιούμε το Θεώρημα 7.2, δύο διαδοχικές εφαρμογές).

Θέτουμε $u = q_1 + \frac{1}{\sqrt{2}}(q_2 - q_1)$. Τότε u είναι άρρητος και $a < q_1 < u < q_2 < b$. □

Τελειώς ανάλογα με τον ορισμό των φραγμένων προς τα πάνω συνόλων και του supremum, ορίζονται τα φραγμένα προς τα κάτω σύνολα και το infimum (κάτω πέρας). Πιο συγκεκριμένα:

Ορισμός. Λέμε ότι το υποσύνολο S του $\mathbb{R}$ είναι *φραγμένο προς τα κάτω* αν υπάρχει πραγματικός αριθμός k τέτοιος ώστε $x \geq k$ για κάθε $x \in S$. Σε τέτοια περίπτωση λέμε ότι k είναι ένα *κάτω φράγμα* του S .

Το αξίωμα της συνέχειας μπορεί να διατυπωθεί και με την πιο κάτω μορφή: Έστω T ένα μη-κενό υποσύνολο των πραγματικών το οποίο είναι *φραγμένο προς τα κάτω*. Τότε υπάρχει ένας αριθμός $m \in \mathbb{R}$ τέτοιος ώστε

(b1) m είναι ένα κάτω φράγμα του T ,

(b2) δοσμένου $\epsilon > 0$, υπάρχει $t \in T$ τέτοιο ώστε $t < m + \epsilon$.

Ο αριθμός m που ικανοποιεί τις συνθήκες (b1) και (b2) καλείται το *κάτω πέρας* ή *infimum* του T (συμβολισμός: $m = \inf T$).

Ορισμός. Λέμε ότι το υποσύνολο S του $\mathbb{R}$ είναι *φραγμένο* αν S είναι φραγμένο προς τα πάνω και φραγμένο προς τα κάτω.

Σημαντικό ρόλο θα παίζουν στην συνέχεια υποσύνολα του $\mathbb{R}$ τα οποία ονομάζονται *διαστήματα*. Με τον όρο αυτό εννοούμε υποσύνολα του $\mathbb{R}$ της μορφής (πιο κάτω a, b είναι πραγματικοί αριθμοί με $a < b$):

Σύνολο	Σύμβολο	Ονομασία
$\{x \in \mathbb{R} : a < x < b\}$	(a, b)	ανοιχτό διάστημα a, b
$\{x \in \mathbb{R} : a < x\}$	$(a, +\infty)$	ανοιχτό διάστημα $a, +\infty$
$\{x \in \mathbb{R} : a > x\}$	$(-\infty, a)$	ανοιχτό διάστημα $-\infty, a$
$\{x \in \mathbb{R} : a < x \leq b\}$	$(a, b]$	ανοιχτό αριστερά, κλειστό δεξιά διάστημα a, b

7.2. Δεκαδική παράσταση πραγματικού αριθμού

Έστω $x \in \mathbb{R}$ με $0 \leq x < 1$. Θέτουμε $a_1 = [10x]$, με άλλα λόγια ορίζουμε a_1 να είναι το ακέραιο μέρος του $10x$, δηλαδή ο μεγαλύτερος ακέραιος που είναι μικρότερος ή ίσος του $10x$. [Στην πραγματικότητα μια αυστηρή τεκμηρίωση της ύπαρξης τέτοιου ακεραίου a_1 χρησιμοποιώντας τα αξιώματα διατεταγμένου σώματος για το $\mathbb{R}$, εμπλέκει την αρχιμήδεια ιδιότητα των πραγματικών (και την αρχή της καλής διάταξης για το $\mathbb{N}$).]

Χρησιμοποιούμε τώρα μαθηματική επαγωγή: Υποθέτουμε ότι $k \in \mathbb{N}$ με $k > 1$. Έχοντας επιλέξει ακέραιους $a_1, \dots, a_{k-1}$, έστω τώρα a_k ο μεγαλύτερος ακέραιος τέτοιος ώστε $\frac{a_1}{10} + \frac{a_2}{10^2} + \dots + \frac{a_k}{10^k} \leq x$. (Ελέγξτε ότι $a_2 = [10^2(x - \frac{a_1}{10})]$, $a_3 = [10^3(x - \frac{a_1}{10} - \frac{a_2}{10^2})]$, $\dots$, $a_k = [10^k(x - \sum_{i=1}^{k-1} \frac{a_i}{10^i})]$, $\dots$, όπου ως συνήθως, συμβολίζουμε με $[u]$ το ακέραιο μέρος του πραγματικού αριθμού u .) Η αρχή αναδρομικού ορισμού μας εξασφαλίζει ότι η ακολουθία μη-αρνητικών ακεραίων (a_i) ορίζεται μοναδικά.

Παρατήρηση. Από τον τρόπο που έχουν επιλεγεί οι ακέραιοι a_i έχουμε ότι, για κάθε $k \in \mathbb{N}$, ισχύει ότι $0 \leq x - \sum_{i=1}^{k-1} \frac{a_i}{10^i} < \frac{1}{10^k}$.

Για κάθε $k \in \mathbb{N}$, θέτουμε $s_k = \frac{a_1}{10} + \frac{a_2}{10^2} + \dots + \frac{a_k}{10^k}$. Προφανώς, $s_k \leq s_{k+1}$ για όλα τα $k \in \mathbb{N}$. Θέτουμε επίσης $S = \{s_k : k \in \mathbb{N}\}$. Έχουμε τότε ότι S είναι ένα μη-κενό, άνω φραγμένο (αφού $t \leq x$ για όλα τα $t \in S$) υποσύνολο των πραγματικών. Το αξίωμα της συνέχειας μας εξασφαλίζει ότι το $\sup S$ υπάρχει. Χρησιμοποιώντας, για παράδειγμα, την πιο πάνω παρατήρηση μαζί με την αρχιμήδεια ιδιότητα των πραγματικών μπορούμε εύκολα να συμπεράνουμε ότι $\sup S = x$. Μέσω της ακολουθίας (a_i) προκύπτει η δεκαδική παράσταση $x = 0, a_1 a_2 a_3 \dots$ για τον πραγματικό αριθμό x . Επιπλέον, ο τρόπος με τον οποίο έχουμε ορίσει την ακολουθία (a_i) , μας εξασφαλίζει ότι δεν υπάρχει αριθμός n_0 τέτοιος ώστε $a_i = 9$ για όλα τα $i \geq n_0$. Ως προς την ιδιότητα αυτή, να μην υπάρχουν δηλαδή επαναλαμβανόμενα 9άρια, η δεκαδική παράσταση που έχουμε πετύχει με την πιο πάνω διαδικασία για τον πραγματικό αριθμό x είναι μοναδική.

Αντίστροφα, μπορούμε να αποδείξουμε το εξής αποτέλεσμα:

Έστω (b_i) μια ακολουθία ακεραίων τέτοια ώστε $0 \leq b_i < 10$ για όλα τα i , και με την επιπλέον ιδιότητα ότι δοσμένου $n_0 \in \mathbb{N}$, υπάρχει $i \geq n_0$ τέτοιο ώστε $a_i \neq 9$. Τότε υπάρχει πραγματικός αριθμός y , με $0 \leq y < 1$, τέτοιος ώστε, για κάθε $k \geq 1$, έχουμε ότι $x = \frac{b_1}{10} + \frac{b_2}{10^2} + \dots + \frac{b_k}{10^k} + \gamma_k$, όπου ο αριθμός γ_k ικανοποιεί $0 \leq \gamma_k < \frac{1}{10^k}$.

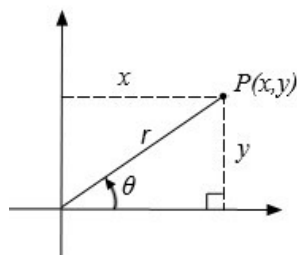
7.3. Επέκταση του σώματος $\mathbb{R}$ στο $\mathbb{C}$

Μιγαδικοί αριθμοί. Αφού το τετράγωνο οποιουδήποτε πραγματικού αριθμού είναι μη-αρνητικός πραγματικός, δεν υπάρχει $x \in \mathbb{R}$ τέτοιο ώστε $x^2 = -1$.

“Επεκτείνουμε” το σύνολο $\mathbb{R}$ στο σύνολο $\mathbb{C}$ των μιγαδικών αριθμών “προσαρτώντας” ένα ξεχωριστό αριθμό i ο οποίος ικανοποιεί αυτή την εξίσωση (δηλαδή, $i^2 = -1$). Έχουμε λοιπόν ότι οι μιγαδικοί αριθμοί είναι εκφράσεις της μορφής $x + iy$, όπου $x, y \in \mathbb{R}$. Δύο στοιχεία $x + iy$ και $u + iv$ του $\mathbb{C}$ (έχουμε δηλαδή $x, y, u, v \in \mathbb{R}$) είναι, από τον ορισμό, ίσα αν, και μόνο αν, $x = u$ και $y = v$.

Αν $a, b \in \mathbb{R}$ και $z = a + ib (\in \mathbb{C})$, τότε a καλείται το πραγματικό μέρος του z και b το φανταστικό μέρος του z . Συνήθως χρησιμοποιούμε τον εξής απλοποιημένο συμβολισμό: γράφουμε x για $x + i0$, iy για $0 + iy$, και i για $0 + i1$. Η πρώτη από αυτές τις απλοποιήσεις συνεπάγεται ότι θεωρούμε το σύνολο $\mathbb{R}$ των πραγματικών αριθμών ως υποσύνολο του $\mathbb{C}$. (Κοιτάξτε στο Κεφάλαιο 15 για περισσότερες λεπτομέρειες σχετικά με το σημείο αυτό.)

Γεωμετρική παράσταση. Όπως έχουμε δει πιο πάνω, ένας μιγαδικός αριθμός z καθορίζεται (με μοναδικό τρόπο) από ένα διατεταγμένο ζεύγος πραγματικών αριθμών (x, y) . Η αμφιμονοσήμαντη αντιστοίχιση σε κάθε μιγαδικό αριθμό $z = x + iy$ του διατεταγμένου ζεύγους $(x, y) \in \mathbb{R}^2$ οδηγεί στην γεωμετρική παράσταση των μιγαδικών αριθμών ως σημεία ενός επιπέδου: Εφοδιάζουμε, ως συνήθως, το επίπεδο $\mathbb{R}^2$ με καρτεσιανούς άξονες συντεταγμένων και ταυτίζουμε τον μιγαδικό αριθμό $z = x + iy$ με το σημείο $P(x, y)$ στο επίπεδο (το οποίο έχει καρτεσιανές συντεταγμένες $(x, y) \in \mathbb{R}^2$):



Το σημείο $P(x, y)$ ταυτίζεται με τον μιγαδικό αριθμό $z = x + iy (= r \cos \theta + ir \sin \theta)$, όπου $r = \sqrt{x^2 + y^2}$ και, για $(x, y) \neq (0, 0)$, $\cos \theta = \frac{x}{\sqrt{x^2 + y^2}}$, $\sin \theta = \frac{y}{\sqrt{x^2 + y^2}}$, $0 \leq \theta < 2\pi$.

Πρόταση 7.4. (Τριγωνομετρική μορφή — πολικές συντεταγμένες). Κάθε μιγαδικός αριθμός z έχει μια παραγοντοποίηση της μορφής $z = r(\cos \theta + i \sin \theta)$ όπου $r \geq 0$ και $0 \leq \theta < 2\pi$.

[Τα στοιχεία του ζεύγους (r, θ) ονομάζονται πολικές συντεταγμένες του μιγαδικού αριθμού $z = x + iy$. Ειδικότερα το r ονομάζεται *μέτρο* του z , το οποίο συμβολίζεται επίσης με $|z|$ (έχουμε δηλαδή $r = |z| = \sqrt{x^2 + y^2}$ αν $z = x + iy \in \mathbb{C}$). Επίσης, στην περίπτωση που $z = x + iy \in \mathbb{C}$ με $(x, y) \neq (0, 0)$, στην περίπτωση δηλαδή που $z \neq 0$, η γωνία θ ονομάζεται *πρωτεύον όρισμα* του z . Αν $z = 0$ τότε η γωνία θ στην πιο πάνω πρόταση μπορεί να επιλεγεί αυθαίρετα. Προφανώς, αν $z = x + iy \in \mathbb{C}$ με $(x, y) \neq (0, 0)$, τότε το z καθορίζει μοναδικό ζεύγος (r, θ) με $r > 0$ και $0 \leq \theta < 2\pi$.]

Η αλγεβρική δομή των μιγαδικών αριθμών. Επεκτείνοντας τις αντίστοιχες πράξεις στο $\mathbb{R}$, πρόσθεση και πολλαπλασιασμός στο $\mathbb{C}$ ορίζονται με

$$(x + iy) + (u + iv) = (x + u) + i(y + v),$$

$$(x + iy)(u + iv) = (xu - yv) + i(xv + yu),$$

(όπου $x, y, u, v \in \mathbb{R}$).

Θέτοντας $x = u = 0$ και $y = v = 1$, παίρνουμε την ταυτότητα $i^2 = -1$.

Άμεση συνέπεια του πιο πάνω ορισμού και των αντίστοιχων ιδιοτήτων της πρόσθεσης και πολλαπλασιασμού στο $\mathbb{R}$ είναι το εξής αποτέλεσμα.

Πρόταση 7.5. Έστω $z_1, z_2, z_3 \in \mathbb{C}$. Τότε ισχύουν:

- (i) $z_1 + z_2 = z_2 + z_1$, (ii) $z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3$, (iii) $z_1 z_2 = z_2 z_1$,
 (iv) $z_1(z_2 z_3) = (z_1 z_2) z_3$, (v) $z_1(z_2 + z_3) = z_1 z_2 + z_1 z_3$.

Παράδειγμα. (Απόδειξη επιμεριστικής ιδιότητας στο $\mathbb{C}$.) Έστω $z_1, z_2, z_3 \in \mathbb{C}$ με $z_1 = x_1 + iy_1$, $z_2 = x_2 + iy_2$, $z_3 = x_3 + iy_3$, ($x_i, y_i \in \mathbb{R}$). Έχουμε τότε

$$\begin{aligned} z_1(z_2 + z_3) &= (x_1 + iy_1)((x_2 + x_3) + i(y_2 + y_3)) \\ &= (x_1(x_2 + x_3) - y_1(y_2 + y_3)) + i(x_1(y_2 + y_3) + y_1(x_2 + x_3)), \quad \text{και} \\ z_1 z_2 + z_1 z_3 &= ((x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1)) + ((x_1 x_3 - y_1 y_3) + i(x_1 y_3 + x_3 y_1)) \\ &= (x_1 x_2 - y_1 y_2 + x_1 x_3 - y_1 y_3) + i(x_1 y_2 + x_2 y_1 + x_1 y_3 + x_3 y_1). \end{aligned}$$

Χρησιμοποιώντας τις ιδιότητες της πρόσθεσης και του πολλαπλασιασμού πραγματικών αριθμών (όπως επιμεριστική ιδιότητα, $\cdot$ είναι αντιμεταθετικός, $+$ είναι προσεταιριστική), βλέπουμε ότι οι δύο εκφράσεις είναι ίσες.

Παράδειγμα. Έστω $z = x + iy \in \mathbb{C}$ με $(x, y) \neq (0, 0)$. Θέτουμε $w = \left(\frac{x}{x^2+y^2}\right) + i\left(\frac{-y}{x^2+y^2}\right)$. Ελέγξτε ότι $zw = 1 (= 1 + i0)$.

Σημείωση. Το σύνολο $\mathbb{C}$, ως προς την πρόσθεση και πολλαπλασιασμό που έχουμε ορίσει σ' αυτό, αποτελεί σώμα (συγκρίνετε με την συζήτηση στην Παράγραφο 7.1).

Συζυγείς μιγαδικοί αριθμοί. Αν $z = x + iy$ ($x, y \in \mathbb{R}$) είναι ένας μιγαδικός αριθμός, τότε ο μιγαδικός αριθμός $x + i(-y)$ καλείται ο συζυγής του και συμβολίζεται με $\bar{z}$.

Πρόταση 7.6. Έστω $z, w \in \mathbb{C}$. Έχουμε τότε

- (i) $\bar{\bar{z}} = z$, (ii) $|\bar{z}| = |z|$, (iii) $z\bar{z} = |z|^2$, (iv) $\overline{z+w} = \bar{z} + \bar{w}$, (v) $\overline{zw} = \bar{z}\bar{w}$.

Σημειώσεις και Σχόλια

1. Στην αρχή της Παραγράφου 7.1 περιγράψαμε κάποιες σημαντικές ιδιότητες του σώματος $\mathbb{R}$ των πραγματικών αριθμών. Πιο ειδικά το $\mathbb{R}$ είναι ένα διατεταγμένο σώμα εφοδιασμένο με την ιδιότητα του “ελάχιστου άνω φράγματος” (που ικανοποιεί, δηλαδή, το αξίωμα της συνέχειας). Ανακύπτει όμως το εξής ερώτημα: Είναι οι ιδιότητες αυτές αρκετές για να χαρακτηρίσουν πλήρως το σώμα $\mathbb{R}$; Στην πραγματικότητα, στην κατεύθυνση αυτή, μπορεί να αποδεχθεί το εξής αποτέλεσμα: Οποιαδήποτε δύο διατεταγμένα σώματα που έχουν την ιδιότητα του “ελάχιστου άνω φράγματος” είναι *ισομορφικά* (είναι, δηλαδή, “ουσιαστικά τα ίδια”).

2. Ξεχνώντας προς στιγμήν την οποιαδήποτε αντίληψη έχουμε αποκομήσει για τους πραγματικούς αριθμούς από την σχολική μας πείρα, είναι φανερό ότι δεν είναι καθόλου εύκολο το εγχείρημα να κατασκευάσει κάποιος “από την αρχή” ένα τόσο πλούσια δομημένο σύστημα (εφοδιασμένο με όλες αυτές τις ιδιότητες που έχουμε προαναφέρει), όπως είναι οι πραγματικοί αριθμοί. Το πρώτο βήμα είναι η κατασκευή του συστήματος $\mathbb{N}$ των φυσικών αριθμών. Όπως έχουμε δει, αυτό μπορεί να επιτευχθεί χρησιμοποιώντας εργαλεία από την θεωρία συνόλων ή, εναλλακτικά, αρχίζοντας από το σύνολο $\mathbb{N}$ και κάνοντας κάποιες παραδοχές όπως τα αξιώματα Peano. Στην συνέχεια, με απλές αλγεβρικές κατασκευές μπορούμε διαδοχικά να κατασκευάσουμε το σύστημα των ακεραίων $\mathbb{Z}$ από το $\mathbb{N}$, και το σύστημα των ρητών $\mathbb{Q}$ από το $\mathbb{Z}$.

Ο Cantor κατασκεύασε τους πραγματικούς αριθμούς από τους ρητούς χρησιμοποιώντας *ακολουθίες Cauchy*.

Σε κατασκευές αυτής της μορφής, ένας πραγματικός αριθμός ορίζεται ως μια κλάση ισοδυναμίας ακολουθιών Cauchy ρητών αριθμών. Μια άλλη μέθοδος κατασκευής των πραγματικών από τους ρητούς είναι μέσω κατάλληλων υποσυνόλων του $\mathbb{Q}$ που καλούνται *τομές* και τα οποία εισήγαγε ο Dedekind. Μια *τομή Dedekind* είναι ένα υποσύνολο A του $\mathbb{Q}$ με τις εξής ιδιότητες: (i) $\emptyset \subsetneq A \subsetneq \mathbb{Q}$, (ii) Αν $p \in A$, $q \in \mathbb{Q}$ και $q < p$, τότε $q \in A$, και (iii) Αν $p \in A$, τότε $p < r$ για κάποιο $r \in A$.

Οι Cantor και Dedekind δημοσίευσαν τις κατασκευές τους το 1872.

3. Μια αλγεβρική κατασκευή του σώματος $\mathbb{C}$ από το σώμα $\mathbb{R}$ χρησιμοποιεί τις έννοιες του *δακτυλίου πηλίκου* και του *μεγιστικού ιδεώδους* (κοιτάζτε στο Κεφάλαιο 17).

Ασκήσεις

7.1 Δείξτε ότι $\sqrt{2} + \sqrt{6} > \sqrt{15}$.

7.2 Θέτουμε $f: (-1, \infty) \rightarrow (0, \infty): x \mapsto \frac{1}{x+1}$, ($x \in (-1, \infty)$). Δείξτε ότι η f είναι αμφιμονοσήμαντη και βρείτε την αντίστροφη συνάρτηση.

7.3 Έστω A, B μη-κενά, φραγμένα σύνολα πραγματικών αριθμών. Δείξτε ότι υπάρχει το $\sup(A \cup B)$ και ότι $\sup(A \cup B) = \max\{\sup A, \sup B\}$.

7.4 (i) Έστω A ένα μη-κενό υποσύνολο των πραγματικών. Έστω επίσης $b \in \mathbb{R}$ με $b > 0$ και $C = \{bx : x \in A\}$. Αν A είναι άνω φραγμένο (αντίστοιχα, κάτω φραγμένο) βρείτε το $\sup C$ (αντίστοιχα, $\inf C$) αν αυτό υπάρχει.

(ii) Έστω B ένα μη-κενό φραγμένο υποσύνολο του $\mathbb{R}$. Δείξτε ότι το σύνολο $\{-b : b \in B\}$ είναι φραγμένο και ότι $\sup\{-b : b \in B\} = -\inf B$.

7.5 Θέτουμε $A = \{2^{-m} + 3^{-n} : m, n \in \mathbb{N}\}$. Βρείτε το $\sup A$ και $\inf A$ (αν αυτά υπάρχουν).

7.6 (i) Δείξτε ότι η πρόσθεση και ο πολλαπλασιασμός μιγαδικών αριθμών ικανοποιούν την προσεταιριστική ιδιότητα.

(ii) Δείξτε τα πιο κάτω.

(a) Αν $z \in \mathbb{C}$, τότε υπάρχει μοναδικό $z' \in \mathbb{C}$ με $z + z' = 0$. [Σε τέτοια περίπτωση γράφουμε $z' = -z$.]

(b) Υπάρχει μοναδικό $e \in \mathbb{C}$ τέτοιο ώστε $ze = z$ για όλα τα $z \in \mathbb{C}$.

(c) Για κάθε $z \in \mathbb{C}$ με $z \neq 0$, υπάρχει μοναδικό $w \in \mathbb{C}$ τέτοιο ώστε $zw = 1$.

7.7 Θέτουμε $R_1 = \{(z, w) \in \mathbb{C} \times \mathbb{C} : z - w (= z + (-w)) \in \mathbb{R}\}$.

(i) Δείξτε ότι R_1 είναι μια σχέση ισοδυναμίας στο $\mathbb{C}$.

(ii) Έστω $a \in \mathbb{R}$. Βρείτε την κλάση ισοδυναμίας $\bar{a}$ (ως προς την σχέση R_1).

(iii) Βρείτε ένα αντιπρόσωπο από κάθε κλάση ισοδυναμίας που προκύπτει από την σχέση R_1 .

(iv) Μπορείτε να βρείτε γεωμετρική ερμηνεία για τις κλάσεις ισοδυναμίας ως προς την σχέση R_1 ;

7.8 Θέτουμε $G = \mathbb{C} - \{0\}$ και $N = \{z \in G : |z| = 1\}$. Θέτουμε επίσης $R = \{(a, b) \in G \times G : a^{-1}b \in N\}$.

(i) Δείξτε ότι R είναι μια σχέση ισοδυναμίας στο σύνολο G .

(ii) Βρείτε ένα υποσύνολο T του G που να αποτελείται από ακριβώς ένα αντιπρόσωπο από κάθε μια από τις διακεκριμένες κλάσεις ισοδυναμίας ως προς την σχέση R .

8. Περισσότερα για σύνολα

8.1. Αριθμήσιμα σύνολα

Υπενθύμιση. Έστω A ένα μη-κενό σύνολο. Σύμφωνα με τον ορισμό που έχουμε δώσει, λέμε ότι το A είναι *πεπερασμένο* αν υπάρχει αμφιμονοσήμαντη συνάρτηση από το σύνολο $\{1, 2, \dots, n\}$ στο A για κάποιο $n \in \mathbb{N}$. Διαφορετικά λέμε ότι το A είναι *άπειρο*. (Θεωρούμε το κενό σύνολο — κατά συνθήκη — ως πεπερασμένο.)

Ορισμός. Έστω A, B μη-κενά σύνολα. Λέμε ότι το σύνολο A είναι *όμοιο* προς το σύνολο B (συμβολισμός: $A \sim B$) αν υπάρχει αμφιμονοσήμαντη συνάρτηση $f: A \rightarrow B$.

Πρόταση 8.1. Για οποιαδήποτε μη-κενά σύνολα A, B και C ισχύουν

(i) $A \sim A$, (ii) αν $A \sim B$, τότε $B \sim A$, (iii) αν $A \sim B$ και $B \sim C$, τότε $A \sim C$.

Απόδειξη. Άσκηση. □

Παραδείγματα 8.2. (i) $(0, 1) \sim (a, b)$, όπου $a, b \in \mathbb{R}$ με $a < b$: Θέτουμε $f(x) = (b - a)x + a$, ($x \in (0, 1)$).

(ii) $(-\frac{\pi}{2}, \frac{\pi}{2}) \sim \mathbb{R}$: Θέτουμε $f(x) = \tan x$, ($x \in (-\frac{\pi}{2}, \frac{\pi}{2})$).

(iii) $\mathbb{R} \sim (0, \infty)$: Θέτουμε $f(x) = e^x$, ($x \in \mathbb{R}$).

(iv) $\mathbb{N} \sim \{2n : n \in \mathbb{N}\}$: Θέτουμε $f(x) = 2x$, ($x \in \mathbb{N}$).

Σημειώσεις. (i) Αν περιοριστούμε σε μια δοσμένη συλλογή $\mathcal{C}$ μη-κενών συνόλων, τότε η ομοιότητα $\sim$ ορίζει μια διμελή σχέση στην $\mathcal{C}$, η οποία είναι μια σχέση ισοδυναμίας στην $\mathcal{C}$ από την Πρόταση 8.1.

(ii) Αν A, B είναι μη-κενά σύνολα με $A \sim B$, λέμε επίσης ότι τα σύνολα A, B είναι *όμοια*.

(iii) Δύο πεπερασμένα σύνολα είναι όμοια αν, και μόνο αν, αυτά έχουν το ίδιο πλήθος στοιχείων. Πιο ειδικά, ένα πεπερασμένο σύνολο δεν μπορεί να είναι όμοιο προς ένα γνήσιο υποσύνολο του (κάτι που δεν ισχύει στην περίπτωση που έχουμε ένα άπειρο σύνολο όπως έχουμε δει). Στην συνέχεια θα δείξουμε ότι άπειρα σύνολα πάντα περιέχουν γνήσια υποσύνολα προς τα οποία είναι όμοια.

Ορισμός. (i) Λέμε ότι το σύνολο A είναι *αριθμήσιμο άπειρο* αν $A \sim \mathbb{N}$.

(ii) Λέμε ότι το σύνολο B είναι *αριθμήσιμο* αν το B είναι είτε πεπερασμένο ή αριθμήσιμο άπειρο.

Σημείωση. Έπεται από τον πιο πάνω ορισμό ότι ένα αριθμήσιμα άπειρο σύνολο A είναι ένα άπειρο σύνολο με την ιδιότητα ότι όλα τα στοιχεία του μπορούν να διευθετηθούν ως μια (άπειρη) ακολουθία. Έχουμε δηλαδή $A = \{a_1, a_2, \dots, a_n, \dots\}$. [Εξήγηση: Αν A είναι αριθμήσιμα άπειρο, τότε υπάρχει αμφιμονοσήμαντη συνάρτηση $f: \mathbb{N} \rightarrow A$. Γράφουμε $f(1) = a_1$, $f(2) = a_2$ και, πιο γενικά, $f(n) = a_n$ για κάθε $n \in \mathbb{N}$.]

Παραδείγματα. (i) Το σύνολο $\{2n: n \in \mathbb{N}\}$ είναι αριθμήσιμα άπειρο.

(ii) Το σύνολο $\mathbb{Z}$ είναι αριθμήσιμα άπειρο: Παρατηρούμε ότι όλα τα στοιχεία του $\mathbb{Z}$ μπορούν να διευθετηθούν ως μια άπειρη ακολουθία ως εξής: $0, 1, -1, 2, -2, 3, -3, \dots$. Αντίστοιχα, θα μπορούσαμε να ορίσουμε την συνάρτηση $f: \mathbb{N} \rightarrow \mathbb{Z}$ όπου $f(n) = \frac{n}{2}$ αν n είναι άρτιος φυσικός, και $f(n) = \frac{1}{2}(1 - n)$ αν n είναι περιττός φυσικός. Προφανώς η συνάρτηση f είναι αμφιμονοσήμαντη.

Λήμμα 8.3. Κάθε υποσύνολο του $\mathbb{N}$ είναι αριθμήσιμο.

Απόδειξη. Έστω $A \subseteq \mathbb{N}$. Το αποτέλεσμα προφανώς ισχύει όταν A είναι πεπερασμένο, επομένως υποθέτουμε ότι το A είναι άπειρο. Έστω ότι ο φυσικός a_1 είναι το ελάχιστο στοιχείο του A (αρχή της καλής διάταξης). Το σύνολο $A - \{a_1\}$ είναι μη-κενό, επομένως έχει ελάχιστο στοιχείο, έστω το a_2 . Παρόμοια θέτουμε a_3 να είναι το ελάχιστο στοιχείο του $A - \{a_1, a_2\}$ και, πιο γενικά a_n να είναι το ελάχιστο στοιχείο του $A - \{a_1, \dots, a_{n-1}\}$ για $n \geq 2$. Παρατηρούμε ότι η συνάρτηση $f: \mathbb{N} \rightarrow A: n \mapsto a_n$, ($n \in \mathbb{N}$) είναι αμφιμονοσήμαντη. [Εξήγηση: Η άπειρη ακολουθία (a_n) που έχουμε κατασκευάσει πιο πάνω ικανοποιεί $a_{n+1} > a_n \geq n$ για κάθε $n \in \mathbb{N}$. Έπεται ότι η συνάρτηση f είναι ενριπτική. Έστω ότι f δεν είναι επιρριπτική. Τότε υπάρχει $a \in A - \{a_n: n \in \mathbb{N}\}$. Από την κατασκευή της (a_n) θα είχαμε ότι $a_n \leq a$ για όλα τα $n \in \mathbb{N}$, που προφανώς αντιφάσκει με τις ιδιότητες της άπειρης ακολουθίας (a_n) .] □

Θεώρημα 8.4. Έστω A ένα μη-κενό σύνολο. Τότε τα (i), (ii) και (iii) πιο κάτω είναι ισοδύναμα:

(i) A είναι αριθμήσιμο, (ii) υπάρχει επίρριψη $g: \mathbb{N} \rightarrow A$, (iii) υπάρχει ένριψη $f: A \rightarrow \mathbb{N}$.

Απόδειξη. Έστω A ένα μη-κενό σύνολο. Είναι αρκετό να δείξουμε τα ακόλουθα: (i) $\Rightarrow$ (ii), (ii) $\Rightarrow$ (iii) και (iii) $\Rightarrow$ (i).

(i) $\Rightarrow$ (ii): Υποθέτουμε ότι A είναι αριθμήσιμο. Αν A είναι πεπερασμένο τότε, αφού $A \neq \emptyset$, υπάρχει αμφιμονοσήμαντη συνάρτηση $g_1: \{1, 2, \dots, n\} \rightarrow A$, για κάποιο $n \in \mathbb{N}$. Θέτουμε $h: \mathbb{N} \rightarrow \{1, 2, \dots, n\}$ όπου $h(i) = i$ αν $1 \leq i \leq n$, και $h(i) = 1$ αν $i > n$ ($i \in \mathbb{N}$). Τότε η συνάρτηση $g: \mathbb{N} \rightarrow A$ που ορίζεται με $g = g_1 \circ h$ είναι επιρριπτική, αφού είναι η σύνθεση δύο επιρριπτικών συναρτήσεων. Αν τώρα το A δεν είναι πεπερασμένο, τότε το A είναι αριθμήσιμα άπειρο. Έχουμε δηλαδή ότι $\mathbb{N} \sim A$ από το οποίο έπεται άμεσα το ζητούμενο.

(ii) $\Rightarrow$ (iii): Υποθέτουμε ότι υπάρχει επίρριψη $g: \mathbb{N} \rightarrow A$. Παρατηρούμε ότι για κάθε $a \in A$, το σύνολο $g^{-1}(\{a\}) (= \{x \in \mathbb{N}: g(x) = a\})$ είναι ένα μη-κενό υποσύνολο του $\mathbb{N}$. Χρησιμοποιώντας την αρχή της καλής διάταξης το σύνολο αυτό έχει ελάχιστο στοιχείο, το οποίο συμβολίζουμε με n_a . Ορίζουμε τώρα την συνάρτηση $f: A \rightarrow \mathbb{N}$ με $f(a) = n_a$,

($a \in A$). Έχουμε τότε ότι f είναι ενριπτική. [Εξήγηση: Αν $f(b) = f(b')$ όπου $b, b' \in A$, τότε $g(f(b)) = g(f(b'))$. Όμως $g(f(a)) = a$ για κάθε $a \in A$.]

(iii) $\Rightarrow$ (i): Έστω $f: A \rightarrow \mathbb{N}$ μια ενριπτική συνάρτηση. Αν το σύνολο A είναι πεπερασμένο δεν υπάρχει κάτι να αποδείξουμε, επομένως υποθέτουμε ότι το σύνολο A είναι άπειρο. Θεωρούμε την εικόνα $f(A) = \{f(a) : a \in A\}$. Η συνάρτηση $\hat{f}: A \rightarrow f(A) : a \mapsto f(a)$ είναι αμφιμονοσήμαντη. Αφού το σύνολο A είναι άπειρο, το σύνολο $f(A)$ είναι ένα άπειρο υποσύνολο του $\mathbb{N}$ και επομένως $f(A) \sim \mathbb{N}$ (κοιτάξτε την απόδειξη του Λήμματος 8.3). Όμως $A \sim f(A)$ αφού η συνάρτηση $\hat{f}: A \rightarrow f(A)$ είναι αμφιμονοσήμαντη. Συνάγουμε ότι $A \sim \mathbb{N}$. $\square$

Πόρισμα 8.5. Κάθε υποσύνολο ενός αριθμήσιμου συνόλου είναι αριθμήσιμο.

Πρόταση 8.6. Κάθε άπειρο σύνολο περιέχει ένα αριθμήσιμα άπειρο υποσύνολο.

Απόδειξη. Έστω A ένα άπειρο σύνολο. Επιλέγουμε κάποιο στοιχείο του A και το ονομάζουμε a_1 . Το σύνολο $A - \{a_1\}$ είναι μη-κενό. Συμβολίζουμε με a_2 ένα από τα στοιχεία του. Η διαδικασία αυτή μπορεί να συνεχιστεί επ' αόριστο (συγκρίνετε με την Άσκηση 8.8): Στο n -οστό στάδιο, το σύνολο $A - \{a_1, \dots, a_{n-1}\}$ είναι μη-κενό αφού το σύνολο A είναι άπειρο. Το σύνολο $\{a_1, a_2, \dots, a_n, \dots\}$ είναι τότε ένα αριθμήσιμα άπειρο υποσύνολο του A . $\square$

Πρόταση 8.7. Κάθε άπειρο σύνολο περιέχει γνήσιο υποσύνολο προς το οποίο είναι όμοιο.

Απόδειξη. Έστω A ένα άπειρο σύνολο και $B = \{a_1, a_2, \dots\}$ ένα αριθμήσιμα άπειρο υποσύνολο του A . Ορίζουμε $f: A \rightarrow A - \{a_1\}$ με $f(x) = \begin{cases} a_{n+1}, & \text{αν } x = a_n \ (n \in \mathbb{N}), \\ x, & \text{αν } x \in A - B. \end{cases}$ Προφανώς η συνάρτηση f είναι αμφιμονοσήμαντη. Συνάγουμε ότι $A \sim A - \{a_1\}$. $\square$

Πρόταση 8.8. Η ένωση δύο αριθμήσιμων συνόλων είναι ένα αριθμήσιμο σύνολο.

Απόδειξη. Έστω B_1, B_2 μη-κενά αριθμήσιμα σύνολα (το αποτέλεσμα προφανώς ισχύει αν $B_1 = \emptyset$ ή $B_2 = \emptyset$). Σύμφωνα με το Θεώρημα 8.4, υπάρχουν επιρριπτικές συναρτήσεις $g_1: \mathbb{N} \rightarrow B_1$ και $g_2: \mathbb{N} \rightarrow B_2$. Αν $b \in B_1$ (αντίστοιχα, $b \in B_2$) τότε $b = g_1(\frac{k+1}{2})$ για κάποιο περιττό φυσικό k (αντίστοιχα, $b = g_2(\frac{k}{2})$ για κάποιο άρτιο φυσικό k). Θέτουμε $h: \mathbb{N} \rightarrow B_1 \cup B_2$, όπου $h(n) = \begin{cases} g_1(\frac{n+1}{2}), & \text{αν } n \text{ είναι περιττός φυσικός,} \\ g_2(\frac{n}{2}), & \text{αν } n \text{ είναι άρτιος φυσικός.} \end{cases}$ Τότε h είναι μια επιρριπτική συνάρτηση και το αποτέλεσμα είναι άμεση συνέπεια του Θεωρήματος 8.4. $\square$

Παράδειγμα 8.9. Το σύνολο $\{0, 1, 2, \dots\} (= \{0\} \cup \mathbb{N})$ είναι αριθμήσιμο από την Πρόταση 8.8. Το σύνολο $-\mathbb{N} = \{-1, -2, \dots\}$ είναι όμοιο προς το $\mathbb{N}$ επομένως είναι επίσης αριθμήσιμο. Βλέπουμε και πάλι ότι το σύνολο $\mathbb{Z}$ είναι αριθμήσιμο αφού $\mathbb{Z} = -\mathbb{N} \cup (\{0\} \cup \mathbb{N})$. (Επειδή το $\mathbb{Z}$ είναι ένα άπειρο σύνολο, έπεται ότι το $\mathbb{Z}$ είναι αριθμήσιμα άπειρο.)

Χρησιμοποιώντας μαθηματική επαγωγή προκύπτει εύκολα το ακόλουθο αποτέλεσμα.

Πόρισμα 8.10. Η ένωση ενός πεπερασμένου πλήθους αριθμήσιμων συνόλων είναι ένα αριθμήσιμο σύνολο.

Θεώρημα 8.11. Το καρτεσιανό γινόμενο $\mathbb{N} \times \mathbb{N}$ είναι ένα αριθμήσιμο άπειρο σύνολο. (Έχουμε, δηλαδή, ότι $(\mathbb{N} \times \mathbb{N}) \sim \mathbb{N}$.)

Απόδειξη. Έχουμε ότι $\mathbb{N} \times \mathbb{N} = \{(i, j) : i \in \mathbb{N} \text{ και } j \in \mathbb{N}\}$. Όλα τα στοιχεία του συνόλου $\mathbb{N} \times \mathbb{N}$ εμφανίζονται στην (διπλά άπειρη) διάταξη:

$$\begin{array}{cccc} (1, 1), & (1, 2), & (1, 3), & (1, 4), & \dots \\ (2, 1), & (2, 2), & (2, 3), & (2, 4), & \dots \\ (3, 1), & (3, 2), & (3, 3), & (3, 4), & \dots \\ (4, 1), & (4, 2), & (4, 3), & (4, 4), & \dots \\ \vdots & \vdots & \vdots & \vdots & \end{array}$$

και επομένως μπορούν να διευθετηθούν ως μια άπειρη ακολουθία με αρκετούς διαφορετικούς τρόπους. Για παράδειγμα, προχωρώντας κατά μήκος των διαγωνίων προκύπτει η ακολουθία $(1, 1), (2, 1), (1, 2), (3, 1), (2, 2), (1, 3), \dots, (n, 1), (n - 1, 2), \dots, (1, n), \dots$. $\square$

Πόρισμα 8.12. Το καρτεσιανό γινόμενο δύο αριθμήσιμων συνόλων είναι ένα αριθμήσιμο σύνολο.

Απόδειξη. Έστω A, B μη-κενά αριθμήσιμα σύνολα (αν $A = \emptyset$ ή $B = \emptyset$ τότε $A \times B = \emptyset$). Τότε τα στοιχεία των A και B μπορούν να διευθετηθούν αντίστοιχα σε ακολουθίες $(a_i)_{i \geq 1}$ και $(b_j)_{j \geq 1}$, οι οποίες μπορεί να είναι πεπερασμένες ή άπειρες ανάλογα αν τα A, B είναι πεπερασμένα ή άπειρα. Θεωρούμε τώρα την συνάρτηση $f: A \times B \rightarrow \mathbb{N} \times \mathbb{N} : (a_i, b_j) \mapsto (i, j)$, $((a_i, b_j) \in A \times B)$. Η συνάρτηση f είναι ενριπτική. Αφού $(\mathbb{N} \times \mathbb{N}) \sim \mathbb{N}$ από το Θεώρημα 8.11, εύκολα μπορούμε να κατασκευάσουμε μια ενριπτική συνάρτηση από το $A \times B$ στο $\mathbb{N}$. $\square$

Πόρισμα 8.13. Το σύνολο $\mathbb{Q}$ είναι αριθμήσιμο.

Απόδειξη. Θέτουμε $\mathbb{Q}^+ = \{q \in \mathbb{Q} : q > 0\}$. Τότε $\mathbb{Q}^+ = \{r/s : r, s \in \mathbb{N}\}$. Θεωρούμε την συνάρτηση $g: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Q}^+ : (r, s) \mapsto r/s$ ($r, s \in \mathbb{N}$). Η συνάρτηση g είναι επιρριπτική. Αφού $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$, υπάρχει μια αμφιμονοσήμαντη συνάρτηση $h: \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$. Έπεται ότι συνάρτηση $g \circ h: \mathbb{N} \rightarrow \mathbb{Q}^+$ είναι επιρριπτική. Από το Θεώρημα 8.4, το σύνολο $\mathbb{Q}^+$ είναι αριθμήσιμο. Τέλος, παρατηρούμε ότι $\mathbb{Q} = \{-q : q \in \mathbb{Q}^+\} \cup \{0\} \cup \mathbb{Q}^+$. $\square$

Πρόταση 8.14. Η ένωση μιας αριθμήσιμης συλλογής αριθμήσιμων συνόλων είναι ένα αριθμήσιμο σύνολο.

Απόδειξη. Έστω $\mathcal{C}$ μια αριθμήσιμα άπειρη συλλογή μη-κενών αριθμήσιμων συνόλων. [Η περίπτωση που η συλλογή των αριθμήσιμων συνόλων είναι πεπερασμένη καλύπτεται από το Πόρισμα 8.10. Επίσης σε περίπτωση που κάποια από τα σύνολα στην συλλογή αριθμήσιμων συνόλων είναι κενά, απλώς τα παραλείπουμε αφού δεν έχουν οποιαδήποτε συνεισφορά.] Θεωρούμε πρώτα την περίπτωση που η συλλογή $\mathcal{C}$ αποτελείται από τα αριθμήσιμα άπειρα σύνολα $A_1, A_2, A_3, \dots$ όπου $A_i = \{a_{i1}, a_{i2}, a_{i3}, \dots\}$. Η συνάρτηση $f: \mathbb{N} \times \mathbb{N} \rightarrow \cup_{i \in \mathbb{N}} A_i : (i, j) \mapsto a_{ij}$ είναι επιρριπτική, και επομένως υπάρχει επιρριπτική συνάρτηση από το $\mathbb{N}$ στην

ένωση $\cup_{i \in \mathbb{N}} A_i$. Τέλος, στην περίπτωση που κάποιο από τα A_i στην συλλογή $\mathcal{C}$ είναι πεπερασμένο με ακριβώς $n(i) \geq 1$ στοιχεία, έχουμε δηλαδή ότι $A_i = \{a_{i1}, a_{i2}, \dots, a_{in(i)}\}$, μπορούμε να θεωρήσουμε και πάλι την άπειρη ακολουθία $(a_{ij})_{j \in \mathbb{N}}$ θέτοντας $a_{ij} = a_{i1}$ αν $j > n(i)$. $\square$

Θεώρημα 8.15. Το σύνολο $\mathbb{R}$ δεν είναι αριθμήσιμο.

Απόδειξη. Από το Πρόρισμα 8.5, αρκεί να δείξουμε ότι το σύνολο $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$ δεν είναι αριθμήσιμο. [Θα μπορούσαμε επίσης να χρησιμοποιήσουμε ότι $(0, 1) \sim (-\pi/2, \pi/2)$ και $(-\pi/2, \pi/2) \sim \mathbb{R}$, από τα Παραδείγματα 8.2.] Προχωρούμε με απαγωγή σε άτοπο και υποθέτουμε ότι το σύνολο $(0, 1)$ είναι αριθμήσιμο. Το σύνολο αυτό είναι προφανώς άπειρο και επομένως τα στοιχεία του μπορούν να διευθετηθούν ως μια άπειρη ακολουθία $a_1, a_2, a_3, \dots$. Από την Παράγραφο 7.2 ξέρουμε ότι κάθε ένας από τους αριθμούς a_n μπορεί να παρασταθεί σε (άπειρη) δεκαδική μορφή $a_n = 0, a_{n1}a_{n2}a_{n3} \dots$ στην οποία δεν χρησιμοποιούνται επαναλαμβανόμενα 9-άρια. Επιπλέον, τέτοια δεκαδική παράσταση για τον a_n είναι μοναδική. Ορίζουμε, για $n \geq 1$, τον αριθμό b_n με $b_n = 1$ αν $a_{nn} \neq 1$ και $b_n = 2$ αν $a_{nn} = 1$. Τότε ο αριθμός $b = 0, b_1b_2b_3 \dots$ ικανοποιεί $0 < b < 1$ και διαφέρει από τον αριθμό a_n στην n -οστή δεκαδική θέση. Έπεται ότι ο αριθμός b δεν είναι κάποιος από τους αριθμούς $a_1, a_2, a_3, \dots$. [Προφανώς η δεκαδική παράσταση $0, b_1b_2b_3 \dots$ για τον b δεν διαθέτει επαναλαμβανόμενα 9-άρια. Σημειώστε επίσης ότι υπάρχει πραγματικός αριθμός με αυτή την δεκαδική παράσταση, πάλι από την Παράγραφο 7.2.] Έχουμε φτάσει σε άτοπο. Συνάγουμε ότι το σύνολο $(0, 1)$ δεν είναι αριθμήσιμο και επομένως το σύνολο $\mathbb{R}$ δεν είναι αριθμήσιμο. $\square$

Πρόρισμα 8.16. Το σύνολο $\mathbb{R} - \mathbb{Q}$ δεν είναι αριθμήσιμο.

8.2. Σχέσεις διάταξης

Ορισμός. Ένα μερικά διατεταγμένο σύνολο είναι ένα μη-κενό σύνολο L με μια διμελή σχέση R στο L η οποία είναι αυτοπαθής, μεταβατική και αντισυμμετρική. Σε τέτοια περίπτωση λέμε ότι R είναι μια μερική διάταξη στο σύνολο L .

Συμβολισμός. Αν R είναι μια μερική διάταξη στο μη-κενό σύνολο L , συνήθως γράφουμε $a \preceq b$ στην θέση του $(a, b) \in R$ (όπου $a, b \in L$) και λέμε ότι το ζεύγος $(L, \preceq)$ είναι ένα μερικά διατεταγμένο σύνολο. Επίσης, για $a, b \in L$, με τον συμβολισμό $a \prec b$ εννοούμε ότι $a \preceq b$ και $a \neq b$, ενώ $b \succ a$ σημαίνει το ίδιο με $a \prec b$.

Παρατήρηση. Αν $(L, \preceq)$ είναι ένα μερικά διατεταγμένο σύνολο, τότε (για όλα τα $a, b, c \in L$) ισχύουν:

- (i) $a \preceq a$, (ii) αν $a \preceq b$ και $b \preceq c$, τότε $a \preceq c$, και (iii) αν $a \preceq b$ και $b \preceq a$, τότε $a = b$.

Για ολόκληρη την συζήτηση μας μέχρι και το τέλος της Παραγράφου 8.2, το ζεύγος $(A, \preceq)$ (όπου A είναι ένα μη-κενό σύνολο) θα συμβολίζει ένα μερικά διατεταγμένο σύνολο.

Λέμε ότι τα στοιχεία $a, b \in A$ είναι συγκρίσιμα αν ισχύει $a \preceq b$ ή $b \preceq a$. Δύο δοσμένα στοιχεία του A δεν είναι όμως υποχρεωτικά συγκρίσιμα. Λέμε ότι $\preceq$ αποτελεί μια ολική διάταξη στο σύνολο A (ή ότι το ζεύγος $(A, \preceq)$ αποτελεί ένα ολικά διατεταγμένο σύνολο) αν οποιαδήποτε δύο στοιχεία του A είναι συγκρίσιμα ως προς την μερική διάταξη $\preceq$.

Παράδειγμα 8.17. (i) Έστω X ένα μη-κενό σύνολο και L η οικογένεια όλων των υποσυνόλων του X (έχουμε δηλαδή $L = \mathcal{P}(X)$, το δυναμοσύνολο του X). Για $A, B \in L$ ορίζουμε $A \preceq B$ να σημαίνει ότι $A \subseteq B$ (το A είναι υποσύνολο του B). Τότε $(L, \preceq)$ είναι ένα μερικά διατεταγμένο σύνολο το οποίο όμως δεν είναι ολικά διατεταγμένο οποτεδήποτε το X περιέχει τουλάχιστον δύο στοιχεία.

(ii) Το ζεύγος $(\mathbb{R}, \preceq)$, όπου $\preceq$ είναι η συνηθισμένη διάταξη $\leq$ στο $\mathbb{R}$, αποτελεί ένα ολικά διατεταγμένο σύνολο.

Παρατήρηση 8.18. Αν $(L, \preceq)$ είναι ένα ολικά διατεταγμένο σύνολο και $a, b \in L$, τότε είναι εύκολο να δείξουμε ότι ισχύει ακριβώς ένα από τα ακόλουθα: $a \prec b$, $a = b$, $a \succ b$.

Συνεχίζουμε με $(A, \preceq)$ ένα μερικά διατεταγμένο σύνολο. Ένα στοιχείο $a \in A$ καλείται *μεγιστικό* αν για κάθε $c \in A$ το οποίο είναι συγκρίσιμο με το a , ισχύει $c \preceq a$ (με άλλα λόγια, για όλα τα $c \in A$ ισχύει: $a \preceq c \Rightarrow a = c$). Προφανώς, αν το στοιχείο $a \in A$ είναι μεγιστικό, δεν ισχύει υποχρεωτικά ότι $c \preceq a$ για όλα τα $c \in A$, αφού μπορεί να υπάρχουν $c \in A$ τα οποία δεν είναι συγκρίσιμα με το a . Επιπλέον, δεν μπορούμε να αποκλείσουμε την περίπτωση να υπάρχουν περισσότερα από ένα ή καθόλου μεγιστικά στοιχεία στο σύνολο A (κοιτάξτε το Παράδειγμα 8.19 πιο κάτω). Ένα *άνω φράγμα* για το μη-κενό υποσύνολο B του A είναι ένα στοιχείο $d \in A$ τέτοιο ώστε $b \preceq d$ για κάθε $b \in B$. Μια αλυσίδα στο μερικά διατεταγμένο σύνολο $(A, \preceq)$ είναι ένα μη-κενό υποσύνολο B του A το οποίο είναι ολικά διατεταγμένο ως προς την $\preceq$.

Παράδειγμα 8.19. (i) Το σύνολο $\mathbb{Z}$, ως προς την συνηθισμένη διάταξη $\leq$, δεν περιέχει μεγιστικά στοιχεία.

(ii) Θέτουμε $L = \{(x, y) \in \mathbb{R}^2 : y \leq 0\}$ και $R = \{((x_1, y_1), (x_2, y_2)) \in L \times L : x_1 = x_2 \text{ και } y_1 \leq y_2\}$. Τότε R είναι μια μερική διάταξη στο σύνολο L , και το σύνολο L έχει άπειρο πλήθος μεγιστικών στοιχείων ως προς την R .

Το επόμενο αποτέλεσμα είναι χρήσιμο σε αρκετές περιπτώσεις που θέλουμε να αποδείξουμε την ύπαρξη μεγιστικού στοιχείου.

Λήμμα του Zorn. Αν L είναι ένα (μη-κενό) μερικά διατεταγμένο σύνολο τέτοιο ώστε κάθε αλυσίδα στο L έχει ένα άνω φράγμα στο L , τότε το L περιέχει ένα μεγιστικό στοιχείο.

Έστω τώρα B ένα μη-κενό υποσύνολο του μερικά διατεταγμένου συνόλου $(A, \preceq)$. Ένα στοιχείο c του B καλείται *ελάχιστο στοιχείο* του B αν $c \preceq b$ για κάθε $b \in B$. Αν κάθε μη-κενό υποσύνολο του A περιέχει ελάχιστο στοιχείο, τότε λέμε ότι A είναι *καλά διατεταγμένο*. Προφανώς κάθε καλά διατεταγμένο σύνολο είναι ολικά διατεταγμένο (το αντίστροφο όμως δεν ισχύει γενικά).

Παραδείγματα 8.20. (i) Η αρχή της καλής διάταξης, όπως την έχουμε διατυπώσει στο Κεφάλαιο 5, μας λέει ότι το σύνολο $\mathbb{N}$, ως προς την συνηθισμένη διάταξη $\leq$, είναι καλά διατεταγμένο.

(ii) Το σύνολο $\mathbb{Z}$, ως προς την συνηθισμένη διάταξη $\leq$, είναι ολικά διατεταγμένο όμως δεν είναι καλά διατεταγμένο αφού το υποσύνολο των αρνητικών ακεραίων δεν περιέχει ελάχιστο στοιχείο.

(iii) Το σύνολο $\mathbb{Z}$ είναι καλά διατεταγμένο ως προς την διάταξη $0, 1, -1, 2, -2, 3, -3, \dots, n, -n, \dots$ (όπου $a < b$ αν-ν το a βρίσκεται στα αριστερά του b).

Πιο γενικά, αν D είναι ένα αριθμήσιμα άπειρο σύνολο, τότε οποιαδήποτε αμφιμονοσήμαντη αντιστοιχία μεταξύ του $\mathbb{N}$ και του D επάγει μια καλή διάταξη στο D . [Εξήγηση: Έστω D ένα αριθμήσιμα άπειρο σύνολο και $f: \mathbb{N} \rightarrow D$ μια αμφιμονοσήμαντη συνάρτηση. Ορίζουμε μια διάταξη στο D με $a < b$ αν (και μόνο αν) $f^{-1}(a) < f^{-1}(b)$, όπου $a, b \in D$ και $<$ είναι η συνηθισμένη διάταξη στο $\mathbb{N}$. Τότε $a \leq b$ (όπου $a \leq b$ σημαίνει είτε $a < b$ ή $a = b$) είναι μια μερική διάταξη στο σύνολο D . Επιπλέον, το σύνολο D είναι καλά διατεταγμένο ως προς την διάταξη $\leq$. Για να το δούμε αυτό, υποθέτουμε ότι B είναι ένα μη-κενό υποσύνολο του D , και θεωρούμε το (μη-κενό) υποσύνολο $f^{-1}(B) = \{f^{-1}(b) : b \in B\}$ του $\mathbb{N}$. Η αρχή της καλής διάταξης (**W**) μας εξασφαλίζει ότι υπάρχει ελάχιστο στοιχείο στο σύνολο $f^{-1}(B)$, έστω το $i_0 \in \mathbb{N}$. Τότε το στοιχείο $f(i_0) \in B$ είναι το ελάχιστο στοιχείο του B ως προς την διάταξη $\leq$.]

Σημειώσεις και Σχόλια

1. Το αξίωμα της επιλογής. Θεωρούμε μια συλλογή $\{X_i\}_{i \in I}$ μη-κενών συνόλων X_i , όπου I είναι ένα μη-κενό σύνολο δεικτών. Μια συνάρτηση επιλογής για την συλλογή αυτή είναι μια συνάρτηση με πεδίο ορισμού το σύνολο I , με την επιπλέον ιδιότητα ότι $f(i) \in X_i$ για όλα τα $i \in I$. Διαισθητικά, η συνάρτηση f “επιλέγει ένα μέλος από κάθε ένα από τα μη-κενά σύνολα X_i ”. Το αξίωμα της επιλογής λέει ότι οποιαδήποτε μη-κενή συλλογή μη-κενών συνόλων έχει μια συνάρτηση επιλογής. Ο P.J. Cohen το 1963 απέδειξε ότι το αξίωμα αυτό είναι ανεξάρτητο από τα υπόλοιπα αξιώματα της θεωρίας συνόλων: Χρησιμοποιώντας μια κοινά αποδεκτή λίστα αξιωμάτων για την θεωρία συνόλων, όπως είναι αυτά των Zermelo και Fraenkel, δεν μπορούμε να αποδείξουμε ότι ισχύει ή ότι δεν ισχύει το αξίωμα της επιλογής. Σημειώστε όμως ότι δεν χρειαζόμαστε το αξίωμα της επιλογής για να επιλέξουμε ένα στοιχείο από ένα μόνο μη-κενό σύνολο, ή ακόμη για να επιλέξουμε στοιχεία από μια πεπερασμένη συλλογή μη-κενών συνόλων, αφού αυτά δικαιολογούνται από τα υπόλοιπα αξιώματα της θεωρίας συνόλων.

2. Η αρχή ελάχιστου στοιχείου λέει ότι σε οποιοδήποτε μη-κενό σύνολο μπορεί να οριστεί μια καλή διάταξη. Μπορεί να αποδειχθεί ότι το αξίωμα της επιλογής, το λήμμα του Zorn και η αρχή ελάχιστου στοιχείου είναι όλα ισοδύναμα.

Ασκήσεις

8.1 Θέτουμε $A = \{r \in \mathbb{R} : r > 0\} \times [0, 2\pi)$ και $B = \mathbb{C} - \{0\}$. Δείξτε ότι τα σύνολα A και B είναι όμοια.

8.2 Εξετάστε κατά πόσον το σύνολο $\mathbb{N} \times \mathbb{N} \times \mathbb{Z} \times \mathbb{Q}$ είναι αριθμήσιμο.

- 8.3 Έστω $A, B \subseteq \mathcal{U}$. Βρείτε, αν υπάρχει, μια αμφιμονοσήμαντη συνάρτηση $f: A \cup B \rightarrow \mathbb{N}$ στις πιο κάτω περιπτώσεις:
- (i) Το σύνολο A είναι όμοιο προς το $\mathbb{N}$ και το B είναι ένα πεπερασμένο σύνολο.
 - (ii) Τα σύνολα A, B είναι και τα δύο όμοια προς το $\mathbb{N}$.
- 8.4 Συμπληρώστε τους συλλογισμούς στα αποτελέσματα 8.1 και 8.10.
- 8.5 (i) Βρείτε, αν υπάρχει, μια αμφιμονοσήμαντη συνάρτηση $f: \mathbb{Z} \rightarrow \mathbb{Z} - \mathbb{N}$.
- (ii) Εξετάστε κατά πόσον τα σύνολα $\mathbb{R}$ και $\mathbb{R} - \mathbb{N}$ είναι όμοια.
- 8.6 Εξετάστε κατά πόσον το σύνολο των πεπερασμένων ακολουθιών ακέραιων αριθμών είναι αριθμήσιμο.
- 8.7 Εξετάστε κατά πόσον τα πιο κάτω σύνολα S είναι αριθμήσιμα.
- (i) $S = \{x \in \mathbb{R}: x = \sqrt{2^a 3^b} \text{ για κάποια } a, b \in \mathbb{N}\}$.
 - (ii) $T = \{x \in \mathbb{R}: x^2 = 2^\alpha 3^\beta 5^\gamma \text{ για κάποια } \alpha, \beta, \gamma \in \mathbb{N}\}$.
- 8.8 Έστω A ένα άπειρο σύνολο. Με δεδομένο ότι για κάθε μη-κενό υποσύνολο T του A έχει επιλεγεί ένα στοιχείο x_T του T (συγκρίνετε με το αξίωμα της επιλογής) κατασκευάστε ένα αριθμήσιμο άπειρο υποσύνολο του A .
- 8.9 Έστω A_1, A_2, B_1, B_2 μη-κενά σύνολα τέτοια ώστε $A_1 \sim A_2$ και $B_1 \sim B_2$. Δείξτε ότι $(A_1 \times B_1) \sim (A_2 \times B_2)$.
- 8.10 Έστω S ένα μη-κενό σύνολο. Έστω επίσης L το σύνολο όλων των γνήσιων υποσυνόλων του S . Δείξτε ότι $(L, \subseteq)$, όπου “ $\subseteq$ ” είναι συνηθισμένη σχέση “περιέχεται”, είναι ένα μερικά διατεταγμένο σύνολο και βρείτε όλα τα μεγιστικά στοιχεία του L ως προς την διάταξη αυτή (αν υπάρχουν τέτοια).

9. Αριθμητική στο $\mathbb{Z}$

9.1. Διαιρετότητα ακεραίων

Υπενθύμιση. Λέμε ότι ο ακέραιος p είναι *πρώτος αριθμός* αν ισχύουν:

- (i) $p > 1$, και
- (ii) οποτεδήποτε $p = ab$ με $a, b \in \mathbb{Z}$, τότε είτε $a \in \{1, -1\}$ ή $b \in \{1, -1\}$.

Επίσης λέμε ότι $a \in \mathbb{N}$ είναι “*γινόμενο πρώτων*” αν υπάρχει $k \in \mathbb{N}$ και πρώτοι $p_1, \dots, p_k$ τέτοιοι ώστε $a = p_1 \dots p_k$.

Λήμμα 9.1. Έστω $n \in \mathbb{Z}$, $n > 1$. Τότε n μπορεί να εκφραστεί ως γινόμενο πρώτων αριθμών.

Απόδειξη. Δεχόμαστε την υπόθεση. Έστω, για κάθε $n \in \mathbb{N}$, η πρόταση $p(n)$: “ο ακέραιος n είναι γινόμενο πρώτων αριθμών”. Παρατηρούμε ότι $p(2)$ είναι αληθής. Υποθέτουμε τώρα ότι $k \in \mathbb{N}$ με $k > 1$ και ότι $p(x)$ είναι αληθής για κάθε φυσικό x με $2 \leq x < k + 1$. Αν ο φυσικός $k + 1$ είναι πρώτος, τότε $p(k + 1)$ είναι αληθής. Αν $k + 1$ δεν είναι πρώτος, τότε $k + 1 = ab$, όπου a, b φυσικοί με $1 < a < k + 1$ και $1 < b < k + 1$. Όμως $a = p_1 \dots p_r$ και $b = q_1 \dots q_s$ για κάποιους πρώτους p_i, q_j από την επαγωγική υπόθεση. Έπεται ότι $k + 1 = p_1 \dots p_r q_1 \dots q_s$ είναι γινόμενο πρώτων. Συνάγουμε ότι $p(n)$ είναι αληθής για κάθε $n \geq 2$. □

Σχόλιο. Διατηρώντας τον συμβολισμό και την υπόθεση στην απόδειξη του Λήμματος 9.1 θα μπορούσαμε να είχαμε προχωρήσει ως εξής: Αν ο φυσικός $k + 1$ δεν είναι πρώτος τότε, από την Πρόταση 5.6, έχουμε ότι $k + 1 = pr$ όπου p πρώτος και r φυσικός με $1 < r < k + 1$ (αφού $p \geq 2$). Χρησιμοποιούμε τέλος την επαγωγική υπόθεση.

Θεώρημα 9.2. (Θεώρημα διαίρεσης.) Έστω $a, b \in \mathbb{Z}$ με $b > 0$. Τότε υπάρχουν μοναδικοί $q, r \in \mathbb{Z}$ με τις ιδιότητες $a = qb + r$ και $0 \leq r < b$.

Απόδειξη. Δεχόμαστε την υπόθεση. Θέτουμε $S = \{a - xb : x \in \mathbb{Z} \text{ και } a - xb \geq 0\}$. Τότε $S \neq \emptyset$. [Εξήγηση: Αν $a \geq 0$, τότε $a = a - 0 \cdot b \in S$. Αν $a < 0$, τότε $0 \leq (1 - b)a = a - ab \in S$ αφού $1 - b \leq 0$.] Έπεται ότι S είναι ένα μη-κενό κάτω φραγμένο υποσύνολο των ακεραίων και επομένως S έχει ελάχιστο στοιχείο. Έστω r το ελάχιστο στοιχείο του S . Τότε $0 \leq r$ και $r = a - qb$ για κάποιο $q \in \mathbb{Z}$ από τον ορισμό του συνόλου S .

Ισχυρισμός: Ισχύει ότι $r < b$.

Απόδειξη ισχυρισμού: Έστω ότι $r \geq b$. Τότε $0 \leq r - b = a - (q+1)b \in S$ (αφού $q+1 \in \mathbb{Z}$) που προφανώς αντιφάσκει με την επιλογή του r ως ελάχιστου στοιχείου του S .

Μέχρι το σημείο αυτό έχουμε δείξει ότι $a = qb + r$ για κάποια $q, r \in \mathbb{Z}$ με $0 \leq r < b$.

Υποθέτουμε τώρα ότι $a = q'b + r'$ με $0 \leq r' < b$ για κάποιους αμέριστους q', r' . Έχουμε τότε ότι $(q - q')b = r' - r$. Ισχύει επίσης ότι

$$-b < -r \leq r' - r \leq r' < b \quad (*)$$

Αφού $q, q' \in \mathbb{Z}$, ακριβώς ένα από τα πιο κάτω ισχύει:

$$(q - q') > 0, \quad (q - q') = 0, \quad (q - q') < 0.$$

Τώρα $b \in \mathbb{Z}$, $b > 0$ συνεπώς ακριβώς ένα από τα πιο κάτω ισχύει:

$$(q - q')b \geq b, \quad (q - q')b = 0, \quad (q - q')b \leq -b.$$

Συγκρίνοντας με την (*) συνάγουμε ότι $(q - q')b = 0$. Συνεπώς $q = q'$ και $r = r'$ αφού $b > 0$. □

Ορισμός. Έστω $a, b \in \mathbb{Z}$. Λέμε ότι a διαιρεί τον b (συμβολισμός: $a|b$) αν υπάρχει $c \in \mathbb{Z}$ τέτοιο ώστε $b = ac$. Σε περίπτωση που a δεν διαιρεί τον b γράφουμε $a \nmid b$.

Παράδειγμα. $-5|30$, $6 \nmid 44$, $17|0$.

Λήμμα 9.3. Έστω $a, b, c, d, s, t \in \mathbb{Z}$. Τότε ισχύουν

- (i) $a|0$, (ii) $0|b$ αν $b = 0$, (iii) $1|a$, (iv) $a|1$ αν $a \in \{-1, 1\}$,
(v) αν $a|b$ και $b|c$, τότε $a|c$, (vi) αν $d|a$ και $d|b$, τότε $d|(sa + tb)$.

Θεώρημα 9.4. Υπάρχει άπειρο πλήθος πρώτων αριθμών.

Απόδειξη. Υποθέτουμε ότι υπάρχει πεπερασμένο πλήθος πρώτων. Έστω $\{p_1, \dots, p_k\}$ όπου k πεπερασμένο, το σύνολο όλων των πρώτων αριθμών. Θέτουμε $a = p_1 p_2 \dots p_k + 1$. Τότε $a \in \mathbb{Z}$, $a > 1$. Συνεπώς a μπορεί να εκφραστεί ως γινόμενο πρώτων αριθμών. Έστω τώρα q ένας από αυτούς τους πρώτους. Τότε $q = p_i$ για κάποιο i με $1 \leq i \leq k$. Έπεται ότι $q|p_1 \dots p_k$ και αφού $q|a$, συνάγουμε ότι $q|1$ (από την σχέση $1 = a - p_1 p_2 \dots p_k$). Άτοπο: $q > 1$ από τον ορισμό του πρώτου αριθμού. □

Σχόλιο. Με μια απλή προσαρμογή της απόδειξης του Θεωρήματος 9.4 μπορούμε να αποδείξουμε ότι για κάθε $n \in \mathbb{N}$ με $n > 2$ υπάρχει πρώτος p με $n < p < n!$: Θεωρούμε τον φυσικό $m = n! - 1$. Τότε $1 < n < m < n!$ και, επιπλέον, $p|m$ για κάποιο πρώτο p αφού $m > 1$. Προφανώς $n < p \leq m$. [Εξήγηση: Αν $p \leq n$ τότε $p|m$ και $p|(m+1)$, που είναι άτοπο.]

Ορισμός. Ο αμέριστος c ονομάζεται *μέγιστος κοινός διαρέτης* (μκδ) των ακεραίων a, b αν ισχύουν

- (i) $c > 0$, (ii) $c|a$ και $c|b$, και (iii) αν $x \in \mathbb{Z}$ με $x|a$ και $x|b$, τότε $x|c$.

Σημείωση. Το ότι έχουμε δώσει τον ορισμό του $\mu\kappa\delta$, αυτό από μόνο του δεν μας εξασφαλίζει την ύπαρξη του. Όμως είναι προφανές από τον ορισμό, ότι όταν υπάρχει $\mu\kappa\delta$ δύο ακέραιων, τότε αυτός είναι μοναδικός.

Συμβολισμός. Έστω $a, b, c \in \mathbb{Z}$. Με τον συμβολισμό $c = \mu\kappa\delta(a, b)$ θα εννοούμε ότι ο $\mu\kappa\delta$ των a και b υπάρχει και ότι αυτός ισούται με c .

Παραδείγματα. (i) Παρατηρούμε ότι $12 = \mu\kappa\delta(60, 24) = \mu\kappa\delta(60, -24) = \mu\kappa\delta(24, 60)$.

(ii) Έστω $a, b, d \in \mathbb{N}$. Αν $d|(a+b)$ και $\mu\kappa\delta(a, b) = 1$, θα δείξουμε ότι $\mu\kappa\delta(a, d) = 1$: Παρατηρούμε πρώτα ότι $a+b = kd$ για κάποιο $k \in \mathbb{Z}$. Έστω τώρα $x \in \mathbb{Z}$ με $x|a$ και $x|d$. Τότε $x|b$ από το Λήμμα 9.3(vi). Αφού $x|a$ και $x|b$ τότε $x|\mu\kappa\delta(a, b)$.

Λήμμα 9.5. (i) $\mu\kappa\delta(0, 0)$ δεν υπάρχει.

(ii) Έστω $a, b \in \mathbb{Z}$. Τότε ισχύουν τα πιο κάτω

$$(a) \mu\kappa\delta(0, a) = \begin{cases} a & \text{αν } a > 0, \\ -a & \text{αν } a < 0. \end{cases}$$

$$(b) \text{ Αν } c = \mu\kappa\delta(a, b), \text{ τότε } c = \mu\kappa\delta(-a, b) = \mu\kappa\delta(a, -b) = \mu\kappa\delta(-a, -b) = \mu\kappa\delta(b, a).$$

Θεώρημα 9.6. Έστω $a, b \in \mathbb{Z}$ όπου a, b δεν είναι και οι δυο ίσοι με μηδέν. Τότε ο $\mu\kappa\delta(a, b)$ υπάρχει. Επιπλέον, υπάρχουν $w, z \in \mathbb{Z}$ τέτοια ώστε $\mu\kappa\delta(a, b) = wa + zb$.

Απόδειξη. Δεχόμαστε την υπόθεση. Θέτουμε $M = \{ma + nb : m, n \in \mathbb{Z}\}$. Αφού $(a, b) \neq (0, 0)$, υπάρχει $x \in M$ με $x \neq 0$. Επίσης $-x \in M$. Επομένως $S = \{k \in \mathbb{N} : k \in M\} \neq \emptyset$. Έστω c το ελάχιστο στοιχείο του S (αρχή καλής διάταξης). Τότε $c > 0$ και, αφού $c \in M$, έχουμε ότι $c = wa + zb$ για κάποια $w, z \in \mathbb{Z}$. Αν $d \in \mathbb{Z}$ με $d|a$ και $d|b$, τότε προφανώς $d|c$. Επομένως για να δείξουμε ότι $c = \mu\kappa\delta(a, b)$ αρκεί να δείξουμε ότι $c|a$ και $c|b$. Στην πραγματικότητα θα δείξουμε ότι $c|x$ για κάθε $x \in M$. Έστω $x = ma + nb \in M$ (όπου $m, n \in \mathbb{Z}$). Σύμφωνα με το θεώρημα διαίρεσης, $x = qc + r$ με $q, r \in \mathbb{Z}$ και $0 \leq r < c$. Έχουμε δηλαδή, $ma + nb = q(wa + zb) + r$. Έπεται ότι $r = (m - qw)a + (n - qz)b \in M$. Αφού $0 \leq r < c$, υποχρεωτικά $r = 0$ λόγω της επιλογής του c . (Αν $r > 0$, τότε $r \in S$ και $r < c$.) Συνάγουμε ότι $x = qc$ (άρα $c|x$). $\square$

Παρατηρήσεις 9.7. (i) Έστω $a, b \in \mathbb{Z}$ με $(a, b) \neq (0, 0)$. Θέτουμε $c = \mu\kappa\delta(a, b)$. Μια άμεση συνέπεια της απόδειξης του Θεωρήματος 9.6 είναι ότι τα σύνολα $\{ma + nb : m, n \in \mathbb{Z}\}$ και $\{kc : k \in \mathbb{Z}\}$ είναι ίσα. Για παράδειγμα, έχουμε ότι $\{9m + 15n : m, n \in \mathbb{Z}\} = \{3k : k \in \mathbb{Z}\}$.

(ii) Συνεχίζουμε με τα $a, b, c \in \mathbb{Z}$ από το (i) και υποθέτουμε ότι $t \in \mathbb{N}$. Τότε, από το Θεώρημα 9.6 και την απόδειξη του, υπάρχει ο $\mu\kappa\delta(ta, tb)$ και ισούται με τον ελάχιστο θετικό ακέραιο στο σύνολο $T_1 = \{mta + ntb : m, n \in \mathbb{Z}\}$. Θέτοντας $T_2 = \{ma + nb : m, n \in \mathbb{Z}\}$, παρατηρούμε ότι $T_1 = \{tx : x \in T_2\}$. Επιπλέον, το ελάχιστο στοιχείο του $T_1 \cap \mathbb{N}$ ισούται με tc , αφού $c (= \mu\kappa\delta(a, b))$ είναι το ελάχιστο στοιχείο του $T_2 \cap \mathbb{N}$. Έπεται ότι $\mu\kappa\delta(ta, tb) = t\mu\kappa\delta(a, b)$.

Ορισμός. Δύο ακέραιοι a, b λέγονται *σχετικά πρώτοι* αν $\mu\kappa\delta(a, b) = 1$. (Για παράδειγμα οι ακέραιοι 40, 9 είναι σχετικά πρώτοι, ενώ οι ακέραιοι 40, 15 δεν είναι σχετικά πρώτοι.)

Λήμμα 9.8. Έστω $a, b \in \mathbb{Z}$. Τότε ισχύει ότι $\mu\kappa\delta(a, b) = 1$ αν, και μόνο αν, υπάρχουν $s, t \in \mathbb{Z}$ με $sa + tb = 1$.

Απόδειξη. Υποθέτουμε πρώτα ότι $\mu\kappa\delta(a, b) = 1$. Το ζητούμενο είναι τότε άμεση συνέπεια του Θεωρήματος 9.6.

Αντίστροφα, υποθέτουμε ότι $sa + tb = 1$ για κάποια $s, t \in \mathbb{Z}$. Έστω ότι ο ακέραιος x ικανοποιεί $x|a$ και $x|b$. Τότε $x|(sa + tb)$, άρα $x|1$. Προφανώς $1|a$ και $1|b$. $\square$

Ασκήσεις. (i) Έστω $a, b, c \in \mathbb{Z}$. Αν $\mu\kappa\delta(a, b) = 1$ και $a|bc$, δείξτε ότι $a|c$.
(ii) Έστω $m, n \in \mathbb{Z}$ με $\mu\kappa\delta(m, n) = 1$. Έστω επίσης $d \in \mathbb{Z}$ τέτοιο ώστε $m|d$ και $n|d$. Δείξτε ότι $mn|d$.

Πρόταση 9.9. Έστω $a, b \in \mathbb{Z}$ με $b > 0$. Γράφουμε $a = qb + r$ όπου $q, r \in \mathbb{Z}$ και $0 \leq r < b$ σύμφωνα με το θεώρημα της διαίρεσης. Τότε $\mu\kappa\delta(a, b) = \mu\kappa\delta(b, r)$.

Απόδειξη. Θέτουμε $c = \mu\kappa\delta(b, r)$. Τότε $c|b$ και $c|r$, επομένως $c|a$ επίσης, αφού $a = qb + r$. Έστω τώρα ότι $x|a$ και $x|b$, όπου $x \in \mathbb{Z}$. Τότε $x|r$ αφού $r = a - qb$. Έπεται ότι $x|c$. Συνάγουμε ότι $c = \mu\kappa\delta(a, b)$. $\square$

Ευκλείδειος Αλγόριθμος

Έστω $a, b \in \mathbb{Z}$ με $(a, b) \neq (0, 0)$. Ο Ευκλείδειος αλγόριθμος μας παρέχει μια μέθοδο μέσω της οποίας μπορούμε όχι μόνο να υπολογίσουμε τον $\mu\kappa\delta(a, b)$, αλλά και να εντοπίσουμε ακέραιους x, y με την ιδιότητα ότι $\mu\kappa\delta(a, b) = xa + yb$, σύμφωνα με το Θεώρημα 9.6.

Παράδειγμα 9.10. Έστω $a = 100$, $b = 28$. Χρησιμοποιώντας το θεώρημα διαίρεσης προκύπτουν διαδοχικά οι εξισώσεις

$$\begin{aligned} 100 &= 3 \cdot 28 + 16 \\ 28 &= 1 \cdot 16 + 12 \\ 16 &= 1 \cdot 12 + 4 \\ 12 &= 3 \cdot 4 + 0 \end{aligned}$$

Από την Πρόταση 9.9, $\mu\kappa\delta(100, 28) = \mu\kappa\delta(28, 16) = \mu\kappa\delta(16, 12) = \mu\kappa\delta(12, 4) = \mu\kappa\delta(4, 0) = 4$.

Μέσω τώρα μιας αντίστροφης διαδικασίας αντανάιρεσης μπορούμε να προσδιορίσουμε ακέραιους x, y τέτοιους ώστε $4 = 100x + 28y$. Έχουμε, $4 = 16 - 12 = 16 - (28 - 16) = 2 \cdot 16 - 28 = 2(100 - 3 \cdot 28) - 28 = 2 \cdot 100 + -7 \cdot 28$. Θέτουμε $x = 2$ και $y = -7$.

Παρατηρούμε ότι ο $\mu\kappa\delta$ δύο ακέραιων a και b (όπου $b > 0$), ισούται με το τελευταίο μη-μηδενικό υπόλοιπο (r_n) που προκύπτει στον αντίστοιχο Ευκλείδειο αλγόριθμο: [Στο Παρά-

δειγμα 9.10, το υπόλοιπο αυτό ήταν ο ακέραιος 4.]

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

Τότε $\mu\kappa\delta(a, b) = \mu\kappa\delta(b, r_1) = \mu\kappa\delta(r_1, r_2) = \dots = \mu\kappa\delta(r_{n-1}, r_n) = \mu\kappa\delta(r_n, 0) = r_n$.

Παρατηρήσεις. (1) Τα υπόλοιπα r_k που προκύπτουν στην πιο πάνω διαδικασία σχηματίζουν μια γνήσια φθίνουσα ακολουθία φυσικών αριθμών η οποία έχει τον b ως τον πρώτο της όρο. Έχουμε δηλαδή $b > r_1 > \dots > r_n$. Αφού b είναι πεπερασμένο με $b > 0$, θα φτάσουμε στο υπόλοιπο 0, που σημαίνει ότι η διαδικασία τερματίζεται, μετά από πεπερασμένο πλήθος επαναλήψεων. Έχουμε δηλαδή πράγματι ένα αλγόριθμο.

(2) Ο Ευκλείδειος αλγόριθμος μας δίνει επίσης μια εναλλακτική απόδειξη όχι μόνο για την ύπαρξη του $\mu\kappa\delta(a, b)$ όπου $a, b \in \mathbb{Z}$ με $(a, b) \neq (0, 0)$, αλλά και για την ύπαρξη $x, y \in \mathbb{Z}$ με την ιδιότητα $\mu\kappa\delta(a, b) = ax + by$. Οι ακέραιοι x, y δεν είναι υποχρεωτικά μοναδικοί, για παράδειγμα ισχύει $ax + by = a(x + b) + b(y - a)$. Έχουμε όμως πάντα ότι $\mu\kappa\delta(x, y) = 1$ (κοιτάζτε την Άσκηση 9.7).

Παράδειγμα. Υποθέτουμε ότι $a, b, t \in \mathbb{N}$. Αν η γνήσια φθίνουσα ακολουθία των μη-μηδενικών υπολοίπων που προκύπτει όταν χρησιμοποιήσουμε τον Ευκλείδειο αλγόριθμο για τους ακραίους a, b είναι η $b > r_1 > \dots > r_n$ όπως πιο πάνω, τότε η αντίστοιχη ακολουθία με τους ακραίους ta, tb στην θέση των a, b αντίστοιχα είναι η $tb > tr_1 > \dots > tr_n$. Έπεται ότι $\mu\kappa\delta(ta, tb) = t\mu\kappa\delta(a, b)$, συγκρίνετε με την Παρατήρηση 9.7(ii).

Λήμμα 9.11. Έστω $a, b, p \in \mathbb{Z}$ όπου p είναι πρώτος αριθμός. Έστω επίσης ότι $p|ab$. Τότε p διαιρεί τουλάχιστον ένα από τους a και b .

Απόδειξη. Δεχόμαστε την υπόθεση. Έστω ότι $p \nmid a$. Αφού p είναι πρώτος, έχουμε ότι $\mu\kappa\delta(a, p) = 1$. Συνεπώς $1 = sa + tp$ για κάποιους ακραίους s, t από το Λήμμα 9.8. Άρα $b = sab + tpb$. Όμως $p|sab$ και $p|tpb$. Συνάγουμε ότι $p|b$. $\square$

Πόρισμα 9.12. Έστω $n \in \mathbb{N}$. Έστω επίσης $a_1, \dots, a_n \in \mathbb{Z}$, και p πρώτος με $p|a_1 a_2 \dots a_n$. Τότε $p|a_i$ για κάποιο i με $1 \leq i \leq n$.

Απόδειξη. Δεχόμαστε την υπόθεση. Για κάθε $k \in \mathbb{N}$ με $1 \leq k \leq n$, θεωρούμε την πρόταση $p(k)$: “αν $p|a_1 \dots a_k$ τότε $p|a_i$ για κάποιο i με $1 \leq i \leq k$ ”. Προφανώς $p(1)$ είναι αληθής. Υποθέτουμε τώρα ότι $p(k)$ είναι αληθής για κάποιο $k \in \mathbb{N}$ με $1 \leq k < n$. Έστω επίσης ότι $p|a_1 a_2 \dots a_{k+1}$. (Σημειώστε ότι $\{a_1, a_2, \dots, a_{k+1}\} \subseteq \{a_1, \dots, a_n\}$.) Θεωρούμε το γινόμενο $a_1 a_2 \dots a_{k+1}$ ως ένα γινόμενο της μορφής ab όπου $a = a_1 a_2 \dots a_k$ και $b = a_{k+1}$. Τότε $p|ab$ και επομένως $p|a$ ή $p|b$ από το Λήμμα 9.11. Αν $p|b$

τότε $p|a_{k+1}$. Αν $p|a$ τότε $p|a_1 \dots a_k$ και επομένως $p|a_i$ για κάποιο i με $1 \leq i \leq k$ από την επαγωγική υπόθεση. Έχουμε δείξει ότι αν $p(k)$ είναι αληθής, όπου $k \in \mathbb{N}$ με $1 \leq k < n$, τότε $p(k+1)$ είναι αληθής. Συνάγουμε ότι η πρόταση $p(n)$ είναι αληθής. $\square$

Θεώρημα 9.13. (Θεμελιώδες θεώρημα της Αριθμητικής.) Έστω a ακέραιος, $a \geq 2$.

(i) Τότε a ισούται με το γινόμενο πρώτων : Έχουμε $a = p_1 \dots p_k$ όπου $p_1, \dots, p_k$ είναι πρώτοι και $p_1 \leq p_2 \leq \dots \leq p_k$.

(ii) Η πιο πάνω παραγοντοποίηση σε πρώτους είναι μοναδική. Με άλλα λόγια, αν $a = p_1 \dots p_k = q_1 \dots q_l$ όπου p_i και q_j είναι όλοι πρώτοι με $p_1 \leq p_2 \leq \dots \leq p_k$ και $q_1 \leq q_2 \leq \dots \leq q_l$ τότε $k = l$ και $p_i = q_i$ για όλα τα $i = 1, \dots, k$.

Απόδειξη. Έστω $a > 1$ ένας ακέραιος αριθμός. Έχουμε ήδη δείξει (Λήμμα 9.1) ότι υπάρχουν πρώτοι $p_1, \dots, p_k$ που έχουν την ιδιότητα $a = p_1 \dots p_k$. Θα δείξουμε τώρα την μοναδικότητα της παράστασης αυτής με απαγωγή σε άτοπο. Υποθέτουμε λοιπόν ότι a έχει δύο διαφορετικές παραγοντοποιήσεις σε γινόμενο πρώτων, έστω $a = p_1 \dots p_k = q_1 \dots q_l$ όπου $p_1 \leq p_2 \leq \dots \leq p_k$ και $q_1 \leq q_2 \leq \dots \leq q_l$ και, επιπλέον, η ακολουθία των πρώτων $(p_1, \dots, p_k)$ δεν είναι η ίδια με την ακολουθία των πρώτων $(q_1, \dots, q_l)$. Στην εξίσωση $p_1 \dots p_k = q_1 \dots q_l$ διαγράφουμε πρώτους (μια φορά από κάθε πλευρά) που είναι κοινοί στις δύο πλευρές μέχρι να φτάσουμε σε μια εξίσωση της μορφής $r_1 \dots r_a = s_1 \dots s_b$ όπου κάθε $r_i \in \{p_1, \dots, p_k\}$, κάθε $s_j \in \{q_1, \dots, q_l\}$ και $r_i \neq s_j$ για όλα τα i, j . Τώρα $r_1 | r_1 \dots r_a$, επομένως $r_1 | s_1 \dots s_b$. Παρεμβάλλοντας το Πρόσχημα 9.12, βλέπουμε ότι $r_1 | s_j$ για κάποιο j , και επομένως $r_1 = s_j$ αφού r_1, s_j είναι πρώτοι (άτοπο). $\square$

Παρατήρηση 9.14. Έστω $a \in \mathbb{Z}$ με $a \geq 2$. Μια άμεση συνέπεια του Θεωρήματος 9.13 είναι ότι υπάρχει για το a μοναδική παραγοντοποίηση της μορφής $a = p_1^{\alpha_1} \dots p_m^{\alpha_m}$, όπου p_i είναι πρώτοι με $p_1 < p_2 < \dots < p_m$, και $\alpha_i \in \mathbb{N}$ για $1 \leq i \leq m$. Αν $b|a$, όπου $b \in \mathbb{N}$, τότε $b = p_1^{\beta_1} \dots p_m^{\beta_m}$ όπου $\beta_i \in \mathbb{N} \cup \{0\}$ και $0 \leq \beta_i \leq \alpha_i$ για όλα τα i .

Παράδειγμα 9.15. (i) Θέλουμε να βρούμε όλους τους θετικούς διαιρέτες του 180. Παρατηρούμε πρώτα ότι $180 = 2^2 3^2 5^1$. Επομένως το 180 έχει ακριβώς 18 θετικούς διαιρέτες που δίνονται με $2^\alpha 3^\beta 5^\gamma$, όπου $0 \leq \alpha, \beta \leq 2$ και $0 \leq \gamma \leq 1$.

(ii) Θα δώσουμε μια εναλλακτική απόδειξη ότι το καρτεσιανό γινόμενο δύο αριθμήσιμων συνόλων είναι ένα αριθμήσιμο σύνολο χρησιμοποιώντας το θεμελιώδες θεώρημα της αριθμητικής: Έστω A, B μη-κενά αριθμήσιμα σύνολα. Σύμφωνα με το Θεώρημα 8.4 υπάρχουν ενριπτικές συναρτήσεις $f: A \rightarrow \mathbb{N}$ και $g: B \rightarrow \mathbb{N}$. Ορίζουμε την συνάρτηση $h: A \times B \rightarrow \mathbb{N}$ με $h((a, b)) = 2^{f(a)} 3^{g(b)}$. Ελέγξτε ότι η συνάρτηση h είναι ενριπτική.

Ορισμός. Το ελάχιστο κοινό πολλαπλάσιο δύο θετικών ακεραίων a και b (συμβολισμός: $\text{εκπ}(a, b)$), είναι ο ελάχιστος θετικός ακέραιος που διαιρείται και από τον a και από τον b .

Αν $a, b \in \mathbb{N}$, παρατηρούμε ότι το σύνολο $S = \{c \in \mathbb{N}: a|c \text{ και } b|c\}$ είναι μη-κενό αφού $ab \in S$. Έπεται ότι το $\text{εκπ}(a, b)$ υπάρχει για όλα τα $a, b \in \mathbb{N}$ (αρχή καλής διάταξης).

Παράδειγμα. $\text{εκπ}(24, 36) = 72$, $\text{εκπ}(2, 20) = 20$ και $\text{εκπ}(7, 11) = 77$.

Πιο γενικά, το ελάχιστο κοινό πολλαπλάσιο των θετικών ακεραίων $a_1, \dots, a_n$ (συμβολισμός: $\text{εκπ}(a_1, \dots, a_n)$) ορίζεται ως ο ελάχιστος θετικός ακέραιος ο οποίος διαιρείται από όλους τους ακέραιους $a_1, \dots, a_n$. [Παρατηρούμε πρώτα ότι κάθε ένα από τα a_i διαιρεί το γινόμενο $a_1 a_2 \dots a_n$.]

Πρόταση 9.16. Έστω $a, b \in \mathbb{N}$. Θεωρούμε τις παραγοντοποιήσεις $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ και $b = p_1^{\beta_1} \dots p_n^{\beta_n}$ όπου p_i διακεκριμένοι πρώτοι και όλα τα $\alpha_i, \beta_i \in \mathbb{N} \cup \{0\}$. [Επιτρέπουμε κάποια από τα α_i, β_i να είναι 0 για να μπορούν να περιέχουν και οι δύο παραγοντοποιήσεις ακριβώς τους ίδιους πρώτους. Υπάρχει τότε τέτοια παραγοντοποίηση και για το $1 \in \mathbb{N}$.] Τότε

- (i) $\mu\kappa\delta(a, b) = p_1^{\min(\alpha_1, \beta_1)} \dots p_n^{\min(\alpha_n, \beta_n)}$
- (ii) $\text{εκπ}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \dots p_n^{\max(\alpha_n, \beta_n)}$
- (iii) $\text{εκπ}(a, b) \cdot \mu\kappa\delta(a, b) = ab$

Απόδειξη. Το (i) και (ii) είναι άμεση συνέπεια της Παρατήρησης 9.14. Το (iii) προκύπτει από την σχέση $\alpha_i + \beta_i = \max(\alpha_i, \beta_i) + \min(\alpha_i, \beta_i)$. $\square$

Παραδείγματα 9.17. (i) Έστω $a = 2^5 3^4 5^0$ και $b = 2^1 3^6 5^2$. Τότε $\mu\kappa\delta(a, b) = 2^1 3^4 5^0$ και $\text{εκπ}(a, b) = 2^5 3^6 5^2$.

(ii) Έστω $a, b, t \in \mathbb{N}$. Θα δώσουμε μια τρίτη απόδειξη ότι $\mu\kappa\delta(ta, tb) = t\mu\kappa\delta(a, b)$ χρησιμοποιώντας την Πρόταση 9.16(i): Διατηρώντας τον συμβολισμό (και τις παραγοντοποιήσεις για τα a, b) στην πρόταση αυτή, υποθέτουμε ότι $t > 1$ και θεωρούμε μια παραγοντοποίηση $t = q_1^{\gamma_1} \dots q_m^{\gamma_m}$ όπου q_j πρώτοι και $\gamma_j \in \mathbb{N}$ για όλα τα j με $1 \leq j \leq m$. (Δεν υπάρχει κίνδυνος να δείξουμε αν $t = 1$.) Σε περίπτωση που $q_1 = p_i$ για κάποιο i με $1 \leq i \leq n$ παρατηρούμε ότι $\min(\gamma_1 + \alpha_i, \gamma_1 + \beta_i) = \gamma_1 + \min(\alpha_i, \beta_i)$. Διαφορετικά, αν $q_1 \notin \{p_1, \dots, p_n\}$, θέτουμε $q_1 = p_{n+1}$. Τότε, στις αντίστοιχες παραγοντοποιήσεις για τα ta, tb έχουμε $\alpha_{n+1} = \gamma_1 = \beta_{n+1}$, άρα $\min(\alpha_{n+1}, \beta_{n+1}) = \gamma_1$. Παρόμοια για τους υπόλοιπους πρώτους $q_2, \dots, q_m$.

9.2. Ισοτιμίες

Ορισμός. Έστω $n \in \mathbb{N}$. Λέμε ότι ο ακέραιος a είναι *ισότιμος modulo n* προς τον ακέραιο b , αν $n|(a - b)$. Στην περίπτωση αυτή γράφουμε $a \equiv b \pmod{n}$.

Σημείωση. Έστω $n \in \mathbb{N}$. Ορίζουμε μια διμελή σχέση R στο $\mathbb{Z}$ με $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a \equiv b \pmod{n}\}$. Τότε R είναι μια σχέση ισοδυναμίας στο $\mathbb{Z}$. Οι αντίστοιχες κλάσεις ισοδυναμίας (ως προς τη σχέση R) ονομάζονται *κλάσεις ισοτιμίας modulo n* . Σε περίπτωση που $a \equiv b \pmod{n}$ για κάποια $a, b \in \mathbb{Z}$, λέμε επίσης ότι *ακέραιοι a και b είναι ισότιμοι modulo n* .

Αν $x \in \mathbb{Z}$, η κλάση ισοτιμίας modulo n του x είναι το σύνολο

$$\begin{aligned} \bar{x} &= \{y \in \mathbb{Z} : y \equiv x \pmod{n}\} = \{y \in \mathbb{Z} : n|(y - x)\} \\ &= \{y \in \mathbb{Z} : y - x = kn, \text{ για κάποιο } k \in \mathbb{Z}\} = \{x + kn \in \mathbb{Z} : k \in \mathbb{Z}\}. \end{aligned}$$

Συμβολισμός. Το σύνολο των διακεκριμένων κλάσεων ισοτιμίας modulo n των ακεραίων συμβολίζεται με $\mathbb{Z}_n$.

Συνεχίζουμε με n θετικό ακέραιο και $x \in \mathbb{Z}$. Σύμφωνα με το θεώρημα διαίρεσης έχουμε ότι $x = qn + r$ όπου $q, r \in \mathbb{Z}$ και $0 \leq r < n$. Έπεται ότι $x \equiv r \pmod{n}$ και επομένως $\bar{x} = \bar{r}$. Συνοψίζοντας, αν $x \in \mathbb{Z}$, τότε $\bar{x} = \bar{r}$ για κάποιο $r \in \mathbb{Z}$ με $0 \leq r < n$. Υποθέτουμε τώρα ότι $\bar{s} = \bar{t}$ όπου $0 \leq s, t < n$ ($s, t \in \mathbb{Z}$). Έχουμε τότε ότι $s \equiv t \pmod{n}$ και επομένως $s - t = kn$ για κάποιο $k \in \mathbb{Z}$. Όμως $-n < s - t < n$. Συνάγουμε ότι $k = 0$ και $s = t$.

Έχουμε αποδείξει την εξής

Πρόταση 9.18. Το σύνολο $\{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ αποτελείται από όλες τις διακεκριμένες κλάσεις ισοτιμίας modulo n . (Έχουμε δηλαδή ότι $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$.)

Πρόταση 9.19. Έστω $n \in \mathbb{N}$ και $a, b, c, d \in \mathbb{Z}$. Έστω επίσης ότι $a \equiv b \pmod{n}$ και $c \equiv d \pmod{n}$. Τότε $a + c \equiv b + d \pmod{n}$ και $ac \equiv bd \pmod{n}$.

Απόδειξη. Δεχόμαστε την υπόθεση. Τότε $n|(a - b)$ και $n|(c - d)$. Άρα $n|((a - b) + (c - d))$ και επομένως $n|((a + c) - (b + d))$. Έπεται ότι $a + c \equiv b + d \pmod{n}$. Επιπλέον, $n|((a - b)c + (c - d)b)$. Άρα $n|(ac - bd)$ και επομένως $ac \equiv bd \pmod{n}$. $\square$

Πόρισμα 9.20. Έστω $a, b, c \in \mathbb{Z}$ και $n, m \in \mathbb{N}$. Έστω επίσης ότι $a \equiv b \pmod{n}$. Τότε $a + c \equiv b + c \pmod{n}$, $ac \equiv bc \pmod{n}$, και $a^m \equiv b^m \pmod{n}$.

Σημείωση. Βλέπουμε από την Πρόταση 9.19 ότι μπορούμε να πολλαπλασιάσουμε και να προσθέσουμε κατά μέλη δύο ισοτιμίες. Δεν μπορούμε όμως πάντα να διαιρέσουμε, για παράδειγμα, έχουμε ότι $22 \equiv 18 \pmod{4}$ ενώ δεν ισχύει ότι $11 \equiv 9 \pmod{4}$. Υπάρχουν όμως περιπτώσεις που μπορούμε να διαιρέσουμε:

Πρόταση 9.21. (i) Έστω $a, n \in \mathbb{Z}$ με $n \geq 1$ και $\mu\kappa\delta(a, n) = 1$. Έστω επίσης $x, y \in \mathbb{Z}$ με $xa \equiv ya \pmod{n}$. Τότε $x \equiv y \pmod{n}$.

(ii) Έστω p πρώτος και έστω $a \in \mathbb{Z}$ με $p \nmid a$. Αν $x, y \in \mathbb{Z}$ με $xa \equiv ya \pmod{p}$, τότε $x \equiv y \pmod{p}$.

Απόδειξη. (i) Δεχόμαστε την υπόθεση. Έστω ότι $xa \equiv ya \pmod{n}$. Τότε $n|(x - y)a$. Αφού $\mu\kappa\delta(a, n) = 1$, έπεται ότι $n|(x - y)$.

(ii) Έπεται από το (i), αφού $\mu\kappa\delta(a, p) = 1$ οποτεδήποτε $p \nmid a$ με p πρώτο. $\square$

Παραδείγματα 9.22. (i) Βρείτε το υπόλοιπο r , με $0 \leq r \leq 7$, που προκύπτει από την διαίρεση του 7^{41} διά 8.

Λύση. Από την ισοτιμία $7 \equiv -1 \pmod{8}$ λαμβάνουμε διαδοχικά $7^{41} \equiv (-1)^{41} \pmod{8}$ και $7^{41} \equiv -1 \pmod{8}$. Έπεται ότι $7^{41} = 8k - 1$ για κάποιο $k \in \mathbb{Z}$, και επομένως $7^{41} = 8(k - 1) + 7$, όπου $k - 1 \in \mathbb{Z}$.

(ii) Έστω $a \in \mathbb{Z}$. Δείξτε ότι είτε $a^2 \equiv 0 \pmod{4}$ ή $a^2 \equiv 1 \pmod{4}$.

Λύση. Από το θεώρημα διαίρεσης, έχουμε ότι ισχύει ακριβώς ένα από τα ακόλουθα για τον ακέραιο a : (a) $a \equiv 0 \pmod{4}$, (b) $a \equiv 1 \pmod{4}$, (c) $a \equiv 2 \pmod{4}$, και (d) $a \equiv 3 \pmod{4}$. Οι περιπτώσεις (a) και (c) δίνουν $a^2 \equiv 0 \pmod{4}$ και οι περιπτώσεις (b) και (d) δίνουν $a^2 \equiv 1 \pmod{4}$. Εναλλακτικά, θα μπορούσαμε να εξετάσουμε τις περιπτώσεις a άρτιος και a περιττός που αντιστοιχούν στα πιθανά υπόλοιπα της διαίρεσης του a διά 2.

(iii) Δείξτε ότι η μόνη τριάδα πρώτων της μορφής $(p, p+2, p+4)$ είναι η τριάδα $(3, 5, 7)$. [Υπόδειξη: Αν $p > 3$, τότε είτε $p \equiv 1$ ή $p \equiv 2 \pmod{3}$.]

Σημειώσεις και Σχόλια

1. Υπάρχουν πολλά θεωρήματα που αφορούν στην κατανομή των πρώτων αριθμών, η οποία δεν ακολουθεί κάποιο συγκεκριμένο νόμο. Το σπουδαιότερο είναι γνωστό ως “θεώρημα πρώτων αριθμών” και αποδείχθηκε ανεξάρτητα το 1896 από τους J. Hadamard και Ch.-J. de la Vallée-Poussin. Συμφωνα με το θεώρημα αυτό, αν ο θετικός πραγματικός αριθμός x είναι αρκετά μεγάλος, τότε $\pi(x)$ είναι κατά προσέγγιση $\frac{x}{\log_e x}$, όπου με $\pi(x)$ συμβολίζουμε το πλήθος των πρώτων αριθμών που είναι μικρότεροι από το x .

2. Εκτός από την εικασία του Goldbach που έχουμε συναντήσει στο Κεφάλαιο 2, μια άλλη διάσημη εικασία στην θεωρία αριθμών είναι η εικασία των “δίδυμων πρώτων” που λέει ότι υπάρχει άπειρο πλήθος δίδυμων πρώτων. [Αν p και $p+2$ είναι και οι δύο πρώτοι, τότε τους ονομάζουμε δίδυμους πρώτους, για παράδειγμα, 3 και 5, 5 και 7, 11 και 13, 71 και 73, 1997 και 1999 είναι όλοι δίδυμοι πρώτοι.]

3. Μια Διοφαντική εξίσωση είναι μια εξίσωση της μορφής $f(x_1, \dots, x_n) = 0$, όπου $f: \mathbb{Z}^n \rightarrow \mathbb{Z}$ είναι μια πολυωνυμική συνάρτηση που έχει ακέραιους συντελεστές. Μας ενδιαφέρουν οι ακέραιες λύσεις μιας εξίσωσης αυτής της μορφής. Οι περισσότερες Διοφαντικές εξισώσεις είναι πολύ δύσκολο να λυθούν. Ένα παράδειγμα Διοφαντικής εξίσωσης που μπορεί να λυθεί με στοιχειώδη τρόπο θα βρείτε στις Ασκήσεις που ακολουθούν.

Ασκήσεις

9.1 Έστω $a, b, c, d, s, t \in \mathbb{Z}$. Δείξτε τα πιο κάτω:

- (i) αν $a|b$ και $b|c$, τότε $a|c$
- (ii) αν $d|a$ και $d|b$, τότε $d|(sa + tb)$

9.2 Έστω n θετικός ακέραιος. Δείξτε ότι υπάρχουν n διαδοχικοί ακέραιοι οι οποίοι δεν περιέχουν μεταξύ τους πρώτο αριθμό. [Υπόδειξη: Θεωρούμε τους n ακέραιους $(n+1)!+2, (n+1)!+3, \dots, (n+1)!+(n+1)$.]

9.3 Δείξτε ότι, για κάθε $n \in \mathbb{N}$, ισχύει $\mu\kappa\delta(6n+8, 4n+5) = 1$.

9.4 Έστω $a, b, c \in \mathbb{Z}$. Αν $\mu\kappa\delta(a, b) = 1$ και $a|bc$, δείξτε ότι $a|c$.

9.5 Έστω $m, n \in \mathbb{Z}$ με $\mu\kappa\delta(m, n) = 1$. Έστω επίσης $a \in \mathbb{Z}$ με $m|a$ και $n|a$. Δείξτε ότι $mn|a$.

9.6 (i) Έστω $c, d \in \mathbb{Z}$ με $(c, d) \neq (0, 0)$. Αν $\mu\kappa\delta(c, d) = e$, δείξτε ότι $\mu\kappa\delta(c/e, d/e) = 1$.

(ii) Θεωρούμε την σχέση ισοδυναμίας R στην Άσκηση 5. Δείξτε ότι κάθε κλάση ισοδυναμίας (ως προς την σχέση R) περιέχει μοναδικό στοιχείο της μορφής (a, b) όπου $b > 0$ και $\mu\kappa\delta(a, b) = 1$.

9.7 Έστω $m, n \in \mathbb{Z}$ με $(m, n) \neq (0, 0)$. Έστω επίσης $d = \mu\kappa\delta(m, n)$. Γράφουμε $d = mx + ny$ όπου $x, y \in \mathbb{Z}$. Δείξτε ότι $\mu\kappa\delta(x, y) = 1$.

9.8 Βρείτε τον $\mu\kappa\delta(64, 24)$ και εκφράστε τον στην μορφή $64w + 24z$ όπου $w, z \in \mathbb{Z}$.

- 9.9 Έστω $a, b \in \mathbb{N}$. Έστω επίσης $c \in \mathbb{Z}$ τέτοιο ώστε $a|c$ και $b|c$. Δείξτε ότι $\text{εκπ}(a, b)|c$.
- 9.10 Έστω $a, b, m \in \mathbb{Z}$ με $m > 0$. Αν $a \equiv b \pmod{m}$, δείξτε ότι $\text{μκδ}(b, m) = \text{μκδ}(a, m)$.
- 9.11 Βρείτε το υπόλοιπο r , όπου $0 \leq r \leq 6$, που προκύπτει όταν διαιρέσουμε το 6^{184} διά 7.
- 9.12 Έστω $n \in \mathbb{N}$. Δείξτε ότι $\sqrt{n} \in \mathbb{Q}$ αν, και μόνο αν, n είναι τέλειο τετράγωνο. [Λέμε ότι ο φυσικός αριθμός n είναι τέλειο τετράγωνο αν $n = m^2$ για κάποιο $m \in \mathbb{Z}$.]
- 9.13 Έστω a, b θετικοί ακέραιοι όπου $\text{μκδ}(a, b) = 1$.
- (i) Αν το γινόμενο ab είναι τέλειο τετράγωνο, δείξτε ότι οι ακέραιοι a, b είναι επίσης τέλεια τετράγωνα.
 - (ii) Αν ab είναι n -οστη δύναμη (για κάποιο θετικό ακέραιο n), εξετάστε κατά πόσον οι ακέραιοι a και b είναι επίσης n -οστες δυνάμεις.
- 9.14 Έστω $x \in \mathbb{N}$. Δείξτε ότι $3|x$ αν, και μόνο αν, το άθροισμα των ψηφίων του x είναι πολλαπλάσιο του 3. Ισχύει το ίδιο αποτέλεσμα με το 9 στην θέση του 3;
- 9.15 Βρείτε τις λύσεις της εξίσωσης $4x^2 = y^3 + 1$ όπου x, y είναι και οι δύο μη-μηδενικοί ακέραιοι. [Υπόδειξη: Γράφουμε την εξίσωση στην μορφή $y^3 = (2x + 1)(2x - 1)$.]
- 9.16 Έστω p περιττός πρώτος. Αν $p = a^2 + b^2$ για κάποια $a, b \in \mathbb{Z}$, δείξτε ότι $p \equiv 1 \pmod{4}$.

10. Αριθμητική στο $\mathbb{Z}_n$

10.1. Πρόσθεση και πολλαπλασιασμός στο $\mathbb{Z}_n$

Η συνηθισμένη πρόσθεση και πολλαπλασιασμός ακεραίων είναι διμελείς πράξεις στο $\mathbb{Z}$. Έχουμε δηλαδή απεικονίσεις

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\rightarrow \mathbb{Z} : (a, b) \mapsto a + b, \text{ και} \\ \cdot : \mathbb{Z} \times \mathbb{Z} &\rightarrow \mathbb{Z} : (a, b) \mapsto ab, \text{ όπου } a, b \in \mathbb{Z}. \end{aligned}$$

Με τη βοήθεια αυτών ορίζουμε τις αντιστοιχίες

$$\begin{aligned} + : \mathbb{Z}_n \times \mathbb{Z}_n &\rightarrow \mathbb{Z}_n : (\bar{a}, \bar{b}) \mapsto \overline{a + b}, \text{ και} \\ \cdot : \mathbb{Z}_n \times \mathbb{Z}_n &\rightarrow \mathbb{Z}_n : (\bar{a}, \bar{b}) \mapsto \overline{ab}, \text{ όπου } a, b \in \mathbb{Z}. \end{aligned}$$

[Προσπαθούμε, δηλαδή, να ορίσουμε πρόσθεση (+) και πολλαπλασιασμό (·) στο $\mathbb{Z}_n$ με $\bar{a} + \bar{b} = \overline{a + b}$ και $\bar{a} \cdot \bar{b} = \overline{ab}$, όπου $a, b \in \mathbb{Z}$.]

Θα δείξουμε τώρα ότι οι αντιστοιχίες αυτές είναι στην πραγματικότητα απεικονίσεις, και επομένως διμελείς πράξεις στο $\mathbb{Z}_n$: Έστω $a, b, c, d \in \mathbb{Z}$ με $\bar{a} = \bar{c}$ και $\bar{b} = \bar{d}$ (αυτό ισχύει αν, και μόνο αν, $(\bar{a}, \bar{b}) = (\bar{c}, \bar{d})$ στο $\mathbb{Z}_n \times \mathbb{Z}_n$). Τότε $a \equiv c \pmod{n}$ και $b \equiv d \pmod{n}$. Από την Πρόταση 9.19, $a + b \equiv c + d \pmod{n}$ και $ab \equiv cd \pmod{n}$. Συμπεραίνουμε ότι $\overline{a + b} = \overline{c + d}$ και $\overline{ab} = \overline{cd}$ στο $\mathbb{Z}_n$ όπως ήταν το ζητούμενο.

Παράδειγμα 10.1. Στο $\mathbb{Z}_{10}$ έχουμε $\bar{4} + \bar{7} = \overline{11} = \bar{1}$ και $\bar{4} \cdot \bar{7} = \overline{28} = \bar{2}$.

Πρόταση 10.2. Έστω $a, b, c \in \mathbb{Z}$. Έστω επίσης $n \in \mathbb{N}$. Τότε στο $\mathbb{Z}_n$ ισχύουν:

- (i) $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$, (ii) $\bar{a} + \bar{0} = \bar{0} + \bar{a} = \bar{a}$, (iii) $\bar{a} + \overline{-a} = \bar{0} = \overline{-a} + \bar{a}$,
- (iv) $\bar{a} + \bar{b} = \bar{b} + \bar{a}$, (v) $(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$, (vi) $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$, (vii) $\bar{a} \cdot \bar{1} = \bar{a} = \bar{1} \cdot \bar{a}$,
- (viii) $\bar{a} \cdot (\bar{b} + \bar{c}) = (\bar{a} \cdot \bar{b}) + (\bar{a} \cdot \bar{c})$, (ix) $(\bar{a} + \bar{b}) \cdot \bar{c} = (\bar{a} \cdot \bar{c}) + (\bar{b} \cdot \bar{c})$.

Απόδειξη. Οι ιδιότητες αυτές προκύπτουν εύκολα από τους πιο πάνω ορισμούς και τις αντίστοιχες ιδιότητες στο $\mathbb{Z}$. Για παράδειγμα, η ιδιότητα (viii): Έχουμε, χρησιμοποιώντας την επιμεριστική ιδιότητα στο $\mathbb{Z}$, ότι $\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \overline{(b + c)} = \overline{a \cdot (b + c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$. □

Παρατηρήσεις 10.3. (i) Αν και η πρόσθεση και ο πολλαπλασιασμός στοιχείων του $\mathbb{Z}_n$ έχουν ιδιότητες που θυμίζουν την πρόσθεση και τον πολλαπλασιασμό ακεραίων, υπάρχουν επίσης και σημαντικές διαφορές : Για παράδειγμα, στο $\mathbb{Z}$ το γινόμενο δύο μη-μηδενικών στοιχείων είναι μη-μηδενικό. Στο $\mathbb{Z}_6$ όμως, έχουμε $\bar{2} \cdot \bar{3} = \bar{0}$. Επίσης, αν οι ακέραιοι a, b, c είναι τέτοιοι ώστε $ac = bc$ και $c \neq 0$, τότε $a = b$ (γράφουμε $ac - bc = (a - b)c$). Στο $\mathbb{Z}_6$ όμως έχουμε $\bar{1} \cdot \bar{3} = \bar{5} \cdot \bar{3}$ και $\bar{1} \neq \bar{5}$.

(ii) Οι ιδιότητες (i), (v) στην Πρόταση 10.2 μας λένε αντίστοιχα ότι η πρόσθεση και ο πολλαπλασιασμός στο $\mathbb{Z}_n$ ικανοποιούν την προσεταιριστική ιδιότητα.

Παράδειγμα. (Συγκρίνετε με την Άσκηση 10.5.) Έστω $n \in \mathbb{N}$ και $\bar{a} \in \mathbb{Z}_n$, όπου $a \in \mathbb{Z}$. Έχουμε τότε ότι $\{\bar{a} + \bar{c} : \bar{c} \in \mathbb{Z}_n\} = \mathbb{Z}_n$. Θέτοντας τώρα $n = 6$ και $\bar{a} = \bar{2}$ στο $\mathbb{Z}_6$, παρατηρούμε όμως ότι $\{\bar{2} \cdot \bar{c} : \bar{c} \in \mathbb{Z}_6\} = \{\bar{0}, \bar{2}, \bar{4}\} \neq \mathbb{Z}_6$.

10.2. Αντιστρέψιμα στοιχεία στο $\mathbb{Z}_n$

Έστω $n \in \mathbb{N}$. Θεωρούμε για παράδειγμα την εξίσωση $\bar{a} \cdot \bar{x} = \bar{c}$ στο $\mathbb{Z}_n$. Σε περίπτωση που υπάρχει $\bar{b} \in \mathbb{Z}_n$ τέτοιο ώστε $\bar{b} \cdot \bar{a} = \bar{1}$, μπορούμε εύκολα να λύσουμε την εξίσωση: Έχουμε, $\bar{a} \cdot \bar{x} = \bar{c} \Rightarrow \bar{b} \cdot (\bar{a} \cdot \bar{x}) = \bar{b} \cdot \bar{c} \Rightarrow (\bar{b} \cdot \bar{a}) \cdot \bar{x} = \bar{b} \cdot \bar{c} \Rightarrow \bar{1} \cdot \bar{x} = \bar{b} \cdot \bar{c} \Rightarrow \bar{x} = \bar{b} \cdot \bar{c}$.

Παρατηρούμε επίσης ότι $\bar{a} \cdot (\bar{b} \cdot \bar{c}) = \bar{a} \cdot (\bar{b} \cdot \bar{c}) = (\bar{a} \cdot \bar{b}) \cdot \bar{c} = \bar{1} \cdot \bar{c} = \bar{c}$ (αφού $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a} = \bar{1}$).

Όμως δεν μπορούμε πάντα να βρούμε τέτοια κλάση $\bar{b}$: Αν υπήρχε $\bar{b} \in \mathbb{Z}_6$ με $\bar{2} \cdot \bar{b} = \bar{1}$, θα είχαμε τότε ότι $\bar{2}\bar{b} = \bar{1}$ και επομένως $2b \equiv 1 \pmod{6}$. Η τελευταία σχέση είναι ισοδύναμη με $2b = 1 + 6k$ για κάποιο $k \in \mathbb{Z}$, που είναι άτοπο, αφού ένας άρτιος αριθμός δεν μπορεί να ισούται με ένα περιττό αριθμό.

Ορισμός. Ένα στοιχείο $\bar{a} \in \mathbb{Z}_n$ καλείται *αντιστρέψιμο* αν υπάρχει $\bar{b} \in \mathbb{Z}_n$ με την ιδιότητα $\bar{a} \cdot \bar{b} = \bar{1} (= \bar{b} \cdot \bar{a})$. Στην περίπτωση αυτή, το $\bar{b}$ καλείται *αντίστροφο* του $\bar{a}$.

Παραδείγματα. (i) Στο $\mathbb{Z}_6$, το $\bar{5}$ είναι αντιστρέψιμο αφού $\bar{5} \cdot \bar{5} = \bar{1}$, ενώ το $\bar{2}$ δεν είναι όπως έχουμε ήδη δει. Τα μόνα αντιστρέψιμα στοιχεία του $\mathbb{Z}_6$ είναι τα $\bar{1}, \bar{5}$. Στο $\mathbb{Z}_7$, το $\bar{2}$ είναι αντιστρέψιμο αφού $\bar{2} \cdot \bar{4} = \bar{1} (= \bar{4} \cdot \bar{2})$.

(ii) Στο $\mathbb{Z}_1$ προφανώς $\bar{0} = \bar{1}$, συνεπώς η κλάση $\bar{0}$ είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}_n$ (όπου $n \in \mathbb{N}$) μόνο στην περίπτωση που $n = 1$.

Λήμμα 10.4. Έστω $a, n \in \mathbb{Z}$ με $n \geq 1$. Αν $\bar{a} \in \mathbb{Z}_n$ είναι αντιστρέψιμο τότε υπάρχει μοναδικό $\bar{b} \in \mathbb{Z}_n$ τέτοιο ώστε $\bar{a} \cdot \bar{b} = \bar{1} (= \bar{b} \cdot \bar{a})$. [Συγκρίνετε με την Πρόταση 4.7]

Απόδειξη. Έστω $\bar{a} \in \mathbb{Z}_n$ αντιστρέψιμο. Έστω επίσης $\bar{b}_1, \bar{b}_2$ δύο αντίστροφες του $\bar{a}$ στο $\mathbb{Z}_n$. Τότε $\bar{a} \cdot \bar{b}_1 = \bar{1}$ και $\bar{b}_2 \cdot \bar{a} = \bar{1}$. Έπεται ότι $\bar{b}_2 = \bar{b}_2 \cdot \bar{1} = \bar{b}_2 \cdot (\bar{a} \cdot \bar{b}_1) = (\bar{b}_2 \cdot \bar{a}) \cdot \bar{b}_1 = \bar{1} \cdot \bar{b}_1 = \bar{b}_1$.

□

Πρόταση 10.5. Έστω $a, n \in \mathbb{Z}$ με $n \geq 1$. Το στοιχείο $\bar{a} \in \mathbb{Z}_n$ είναι αντιστρέψιμο αν, και μόνο αν, $\mu\kappa\delta(a, n) = 1$.

Απόδειξη. Υποθέτουμε πρώτα ότι $\bar{a} \in \mathbb{Z}_n$ είναι αντιστρέψιμο. Τότε υπάρχει $b \in \mathbb{Z}$ τέτοιο ώστε $\bar{a} \cdot \bar{b} = \bar{1}$ στο $\mathbb{Z}_n$, ή ισοδύναμα $ab \equiv 1 \pmod{n}$. Έπεται ότι $ab = kn + 1$ για κάποιο $k \in \mathbb{Z}$. Η τελευταία σχέση μας εξασφαλίζει ότι $\mu\kappa\delta(a, n) = 1$. Αντίστροφα, έστω ότι $\mu\kappa\delta(a, n) = 1$. Τότε $sa + tn = 1$ για κάποια $s, t \in \mathbb{Z}$. Επομένως στο $\mathbb{Z}_n$, $\bar{1} = \overline{sa + tn} = \overline{sa} + \overline{tn} = \bar{s} \cdot \bar{a} + \bar{t} \cdot \bar{n} = \bar{s} \cdot \bar{a} (= \bar{a} \cdot \bar{s})$ αφού $\bar{n} = \bar{0}$. Συνάγουμε ότι το $\bar{a}$ είναι αντιστρέψιμο. $\square$

Συμβολισμός. Έστω $n \geq 1$. Το σύνολο των αντιστρέψιμων στοιχείων του $\mathbb{Z}_n$ συμβολίζεται με $\mathbb{Z}_n^*$. Επίσης, αν $a \in \mathbb{Z}$ με $\mu\kappa\delta(a, n) = 1$, συμβολίζουμε με $(\bar{a})^{-1}$ το μοναδικό αντίστροφο του $\bar{a}$ στο $\mathbb{Z}_n$.

Παρατήρηση 10.6. Η απόδειξη της πιο πάνω πρότασης μας δίνει ένα πρακτικό τρόπο υπολογισμού του αντιστρόφου του $\bar{a}$ στο $\mathbb{Z}_n$, σε περίπτωση που αυτό υπάρχει. Διατηρώντας τον συμβολισμό στην απόδειξη, το αντίστροφο του $\bar{a}$ είναι το $\bar{s}$, όπου ο ακέραιος s μπορεί να εντοπιστεί χρησιμοποιώντας τον Ευκλείδειο αλγόριθμο και την αντίστροφη διαδικασία αντανάφρασης.

Η συνάρτηση του Euler. Συμβολίζουμε με $\phi(n)$ το πλήθος των στοιχείων του συνόλου $\mathbb{Z}_n^*$ για κάθε $n \in \mathbb{N}$. Τότε ορίζεται μια συνάρτηση $\phi: \mathbb{N} \rightarrow \mathbb{N}$ που ονομάζεται *συνάρτηση του Euler*.

Έστω $n \in \mathbb{N}$. Από την προηγούμενη πρόταση έχουμε τότε ότι $\phi(n)$ ισούται με το πλήθος των ακεραίων a με $0 \leq a \leq n - 1$ και $\mu\kappa\delta(a, n) = 1$.

Παράδειγμα 10.7. (i) Παρατηρούμε ότι $\phi(1) = 1$, $\phi(2) = 1$, $\phi(p) = p - 1$ αν p πρώτος, $\phi(4) = 2$, $\phi(6) = 2$, $\phi(10) = 4$.

(ii) Έστω $k, p \in \mathbb{N}$ με p πρώτο. Θα δείξουμε ότι $\phi(p^k) = p^k - p^{k-1}$: Οι θετικοί ακέραιοι $\leq p^k$ οι οποίοι δεν είναι σχετικά πρώτοι με το p^k είναι ακριβώς αυτοί οι οποίοι διαιρούνται από το p . Αυτοί είναι οι ακέραιοι rp όπου $1 \leq r \leq p^{k-1}$. Αφού υπάρχουν p^{k-1} τέτοιοι ακέραιοι, τότε υπάρχουν $p^k - p^{k-1}$ μη-αρνητικοί ακέραιοι $< p^k$ οι οποίοι είναι σχετικά πρώτοι με το p^k . Έπεται ότι $\phi(p^k) = p^k - p^{k-1}$.

Μικρό θεώρημα Fermat. Έστω p πρώτος και έστω $a \in \mathbb{Z}$ με $p \nmid a$. Τότε $\mu\kappa\delta(a, p) = 1$ και $\bar{a} \in \mathbb{Z}_p^*$. Θέτουμε $T = \{k \in \mathbb{N}: (\bar{a})^k = \bar{1}\}$. Τότε $T \neq \emptyset$. [Εξήγηση: Αφού $\mathbb{Z}_p^* (= \mathbb{Z}_p - \{\bar{0}\})$ είναι ένα πεπερασμένο σύνολο, οι δυνάμεις $(\bar{a})^l$, $l \in \mathbb{N}$, δεν μπορούν να είναι όλες διακεκριμένες, επομένως $(\bar{a})^s = (\bar{a})^t$ για κάποια $s, t \in \mathbb{N}$ με $s < t$. Πολλαπλασιάζοντας και τα δύο μέλη της πιο πάνω ισότητας με το $(\bar{v})^s$, όπου $\bar{v}$ είναι το μοναδικό αντίστροφο του $\bar{a}$ στο $\mathbb{Z}_p$, προκύπτει η ισότητα $\bar{1} = (\bar{a})^{t-s}$, όπου $t - s \in \mathbb{N}$.] Έστω $m (\in \mathbb{N})$ το ελάχιστο στοιχείο του T . Θέτουμε $S = \{(\bar{a})^l: l \in \mathbb{N}\}$. Έχουμε τότε ότι $|S| = m$ και $S = \{\bar{1}, \bar{a}, (\bar{a})^2, \dots, (\bar{a})^{m-1}\}$. [Εξήγηση: Σύμφωνα με το θεώρημα διαίρεσης, αφού $l, m \in \mathbb{N}$ έχουμε ότι $l = qm + r$ για κάποια $q, r \in \mathbb{N} \cup \{0\}$ με $r < m$ (αν $q \leq -1$ τότε, για $0 \leq r < m$, θα είχαμε $qm + r \leq -m + r < 0$). Επιπλέον, τα m στοιχεία $\bar{1} (= (\bar{a})^0 = (\bar{a})^m)$, $\bar{a}$, $\dots$, $(\bar{a})^{m-1}$ είναι διακεκριμένα αφού, αν $(\bar{a})^s = (\bar{a})^t$ με $0 \leq s < t < m$, θα είχαμε $\bar{1} = (\bar{a})^{t-s}$ με $1 \leq t - s < m$ που προφανώς αντιφάσκει με την επιλογή του m ως ελάχιστου στοιχείου του T .]

Ορίζουμε στο σύνολο $\mathbb{Z}_p^*$ την σχέση $R = \{(\bar{b}, \bar{c}) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*: (\bar{b})^{-1}\bar{c} \in S\}$. Τότε R είναι μια σχέση ισοδυναμίας (συγκρίνετε με την Άσκηση 6.7) και η αντίστοιχη κλάση ισοδυναμίας του στοιχείου $\bar{b} \in \mathbb{Z}_p^*$ είναι το υποσύνολο $\bar{b}S = \{\bar{b}(\bar{a})^k: 0 \leq k \leq m-1\}$ του $\mathbb{Z}_p^*$. Επιπλέον, ισχύει ότι $|\bar{b}S| = |S| = m$ για όλα τα $\bar{b} \in \mathbb{Z}_p^*$ (κοιτάξτε την Άσκηση 10.5(iii)). Οι κλάσεις ισοδυναμίας ως προς την πιο πάνω σχέση αποτελούν μια διαμέριση του συνόλου $\mathbb{Z}_p^*$ και, αφού $\mathbb{Z}_p^*$ είναι ένα πεπερασμένο σύνολο, υπάρχουν $\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n \in \mathbb{Z}_p^*$ (πεπερασμένο πλήθος) με $\cup_{i=1}^n \bar{b}_i S = \mathbb{Z}_p^*$ και $\bar{b}_i S \cap \bar{b}_j S = \emptyset$ οποτεδήποτε $1 \leq i < j \leq n$. Συμπεραίνουμε ότι $p-1 (= |\mathbb{Z}_p^*|) = nm$. Πιο ειδικά, $(\bar{a})^{p-1} = ((\bar{a})^m)^n = (\bar{1})^n = \bar{1}$. Όμως $(\bar{a})^{p-1} = \overline{a^{p-1}}$ σύμφωνα με τον πολλαπλασιασμό που έχουμε ορίσει στο $\mathbb{Z}_p$. Συνοψίζοντας έχουμε δείξει ότι αν $a \in \mathbb{Z}$ με $p \nmid a$ όπου p πρώτος, τότε $a^{p-1} \equiv 1 \pmod{p}$.

Θεώρημα 10.8. (Μικρό θεώρημα Fermat.) Αν $a \in \mathbb{Z}$ και p πρώτος, τότε $a^p \equiv a \pmod{p}$. Επιπλέον, αν $p \nmid a$, τότε $a^{p-1} \equiv 1 \pmod{p}$.

Απόδειξη. Έστω $a \in \mathbb{Z}$ και p πρώτος. Υποθέτουμε πρώτα ότι $p \nmid a$. Στην πιο πάνω συζήτηση έχουμε αποδείξει ότι $a^{p-1} \equiv 1 \pmod{p}$. Πολλαπλασιάζοντας με το a και τα δύο μέλη της τελευταίας ισοτιμίας και παρεμβάλλοντας το Πρόσμημα 9.20, προκύπτει ότι $a^p \equiv a \pmod{p}$. Αν $p|a$ τότε προφανώς $a \equiv 0 \pmod{p}$, και επομένως $a^p (\equiv 0) \equiv a \pmod{p}$. $\square$

Παράδειγμα 10.9. Δείξτε ότι $42^{47} + 47^{42}$ δεν είναι πρώτος αριθμός.

Λύση. Από το μικρό θεώρημα Fermat, με $p = 43$ και $a = 47$, παρατηρούμε ότι $47^{42} \equiv 1 \pmod{43}$. Επιπλέον, έχουμε ότι $42 \equiv -1 \pmod{43}$ και επομένως $42^{47} \equiv (-1)^{47} \pmod{43}$. Έπεται ότι $42^{47} \equiv -1 \pmod{43}$. Συνεπώς, $(42^{47} + 47^{42}) \equiv 0 \pmod{43}$, έχουμε δηλαδή ότι $43|(42^{47} + 47^{42})$. $\square$

10.3. Μια εφαρμογή — ο κώδικας ISBN-10

Σε κάθε βιβλίο αντιστοιχεί (μοναδικά) ο γνωστός αριθμός ISBN (International Standard Book Number — Διεθνής Πρότυπος Αριθμός Βιβλίου), ο οποίος αποτελεί την ‘ταυτότητα’ του βιβλίου και περιλαμβάνει πληροφορίες για το βιβλίο. Κοιτάξτε επίσης τις Σημειώσεις και Σχόλια στο τέλος του κεφαλαίου.

Ορισμός. Έστω $\mathbb{F}_q$ ένα πεπερασμένο σώμα (συγκρίνετε με την συζήτηση στην Παράγραφο 7.1) με ακριβώς q στοιχεία. [Μπορεί ναδειχθεί ότι τότε $q = p^k$ για κάποιο πρώτο p και κάποιο $k \in \mathbb{N}$.] Ένας q -αδικός κώδικας C μήκους n , όπου $n \in \mathbb{N}$, είναι ένα μη-κενό υποσύνολο του $(\mathbb{F}_q)^n$. Σε τέτοια περίπτωση λέμε επίσης ότι το σύνολο $\mathbb{F}_q$ είναι το αλφάβητο για τον κώδικα C . Τα στοιχεία του C ονομάζονται κωδικολέξεις. [Στο Κεφάλαιο 15 θα δείξουμε ότι το σύνολο $\mathbb{Z}_p$, όπου p πρώτος, είναι ένα σώμα ως προς την πρόσθεση και πολλαπλασιασμό που έχουμε ορίσει πάνω σε αυτό.]

Ο κώδικας ISBN-10 είναι ο 11-αδικός κώδικας C μήκους 10 που ορίζεται με $C = \{\bar{x}_1 \bar{x}_2 \dots \bar{x}_{10} \in (\mathbb{Z}_{11})^{10}: x_i \in \{0, 1, \dots, 10\} \subseteq \mathbb{Z} \ (1 \leq i \leq 10), x_i \neq 10 \ (1 \leq i \leq 9) \text{ και στο } \mathbb{Z}_{11} \text{ ισχύει}$

$\bar{x}_{10} = \bar{x}_1 + 2\bar{x}_2 + 3\bar{x}_3 + \dots + 9\bar{x}_9$. (Οι χαρακτήρες $\bar{x}_i$ που βρίσκονται στις πρώτες θέσεις δηλώνουν την γλώσσα στην οποία είναι γραμμένο το βιβλίο, οι χαρακτήρες που ακολουθούν δηλώνουν τον εκδοτικό οίκο ενώ οι υπόλοιποι χαρακτήρες εκτός από τον τελευταίο δίνονται από τον εκδότη για το συγκεκριμένο βιβλίο.) Ο τελευταίος χαρακτήρας υπολογίζεται από τους προηγούμενους χρησιμοποιώντας την σχέση $\bar{x}_{10} = \bar{x}_1 + 2\bar{x}_2 + 3\bar{x}_3 + \dots + 9\bar{x}_9$ στο $\mathbb{Z}_{11}$. Έχουμε επίσης τον περιορισμό ότι $x_i \in \{0, 1, 2, \dots, 9\}$ οποτεδήποτε $1 \leq i \leq 9$, όμως ο ακέραιος x_{10} μπορεί να πάρει και την τιμή 10. Επειδή ο ‘χαρακτήρας’ $\overline{10}$ είναι διψήφιος, τον συμβολίζουμε με “X”, για να αποφεύγουμε έτσι οποιαδήποτε σύγχυση. Επιπλέον, στην πραγματικότητα στα βιβλία, αντί του χαρακτήρα “ $\bar{a}$ ” σε μια κωδικολέξη (όπου $a \in \mathbb{Z}$, $0 \leq a \leq 9$), εμφανίζεται απλά ο χαρακτήρας “ a ”. Με τις ‘τροποποιήσεις’ αυτές πάνω σε μια κωδικολέξη του ISBN-10 κώδικα C προκύπτει ο γνωστός αριθμός ISBN-10. Για παράδειγμα ο αριθμός 055010206X ικανοποιεί όλες τις προϋποθέσεις για να είναι ένας αριθμός ISBN-10.

Ο κώδικας C , με τον τρόπο που σχεδιάστηκε, ανιχνεύει 1 λάθος. Πράγματι, υποθέτουμε ότι μας έχει σταλεί η κωδικολέξη $\mathbf{x} = \bar{x}_1\bar{x}_2\dots\bar{x}_{10}$ όμως εμείς λάβαμε το ‘διάνυσμα’ $\mathbf{a} = \bar{a}_1\bar{a}_2\dots\bar{a}_{10}$ το οποίο συμφωνεί σε όλους τους χαρακτήρες με την $\mathbf{x}$, εκτός από τον χαρακτήρα $\bar{x}_r$, στην θέση του οποίου έχουμε τον χαρακτήρα $\bar{a}_r = \bar{x}_r + \bar{e}$ για κάποιο $\bar{e} \in \mathbb{Z}_{11} - \{\bar{0}\}$. Από τον τρόπο που έχουμε ορίσει τον κώδικα C έχουμε τότε ότι $\sum_{i=1}^{10} \bar{i} \cdot \bar{x}_i = \bar{0}$ στο $\mathbb{Z}_{11}$ (αφού $-\bar{1} = \bar{10}$ στο $\mathbb{Z}_{11}$), ενώ για το διάνυσμα $\mathbf{a}$ έχουμε $\sum_{i=1}^{10} \bar{i} \cdot \bar{a}_i = (\sum_{i=1}^{10} \bar{i} \cdot \bar{x}_i) + (\bar{r} \cdot \bar{e}) = \bar{r} \cdot \bar{e}$. Όμως r είναι ένας θετικός ακέραιος με $1 \leq r \leq 10$, άρα $\bar{r} \neq \bar{0}$ στο $\mathbb{Z}_{11}$. Από την υπόθεση μας πιο πάνω έχουμε επίσης ότι $\bar{e} \neq \bar{0}$ στο $\mathbb{Z}_{11}$ και επομένως $\bar{r} \cdot \bar{e} \neq \bar{0}$ στο $\mathbb{Z}_{11}$ (κοιτάζτε την Άσκηση 10.2). Συνάγουμε ότι το διάνυσμα $\mathbf{a} = \bar{a}_1\bar{a}_2\dots\bar{a}_{10}$ δεν είναι κωδικολέξη, αφού $\sum_{i=1}^{10} \bar{i} \cdot \bar{a}_i \neq \bar{0}$ στο $\mathbb{Z}_{11}$. Με αυτό τον τρόπο ανιχνεύθηκε το λάθος.

Παρατηρήσεις. (1) Ο κώδικας C (δηλαδή ο ISBN-10 κώδικας) επιπλέον έχει την δυνατότητα να ανιχνεύει τον “αναγραμματισμό” δύο χαρακτήρων σε μια κωδικολέξη: Υποθέτουμε τώρα ότι μας έχουν στείλει την κωδικολέξη $\mathbf{x} = \bar{x}_1\bar{x}_2\dots\bar{x}_{10}$ και εμείς λάβαμε το διάνυσμα $\mathbf{b} = \bar{b}_1\bar{b}_2\dots\bar{b}_{10}$ του οποίου όλοι οι χαρακτήρες συμφωνούν με τους χαρακτήρες του $\mathbf{x}$, εκτός από τις θέσεις r, j ($1 \leq j, r \leq 10, r \neq j$) όπου οι χαρακτήρες έχουν αλλάξει θέση, δηλαδή $\bar{b}_r = \bar{x}_j$ και $\bar{b}_j = \bar{x}_r$. Υποθέτουμε επιπλέον ότι $\bar{x}_j \neq \bar{x}_r$ (ότι δηλαδή ο αναγραμματισμός πράγματι αλλοίωσε το αρχικό μήνυμα). Θα είχαμε τότε $\sum_{i=1}^{10} \bar{i} \cdot \bar{b}_i = \sum_{i=1}^{10} \bar{i} \cdot \bar{x}_i + (\bar{r} - \bar{j}) \cdot \bar{x}_j + (\bar{j} - \bar{r}) \cdot \bar{x}_r = (\bar{r} - \bar{j}) \cdot (\bar{x}_j - \bar{x}_r) \neq \bar{0}$ στο $\mathbb{Z}_{11}$. [Εξήγηση: Έχουμε $\bar{r} \neq \bar{j}$ και επομένως $\bar{r} - \bar{j} (= \bar{r} + (-\bar{j})) \neq \bar{0}$ στο $\mathbb{Z}_{11}$. Παρόμοια, $\bar{x}_j - \bar{x}_r \neq \bar{0}$ στο $\mathbb{Z}_{11}$.]

(2) Ο κώδικας C έχει επίσης την μερική δυνατότητα να διορθώνει λάθη: Υποθέτουμε ότι μας έχει σταλεί η κωδικολέξη $\mathbf{x} = \bar{x}_1\bar{x}_2\dots\bar{x}_{10}$ και εμείς λάβαμε το διάνυσμα $\mathbf{c} = \bar{c}_1\bar{c}_2\dots\bar{c}_{10}$ όπου $\bar{c}_r \neq \bar{x}_r$ για κάποιο r (με $1 \leq r \leq 10$) το οποίο όμως εμείς γνωρίζουμε, και $\bar{c}_i = \bar{x}_i$ για όλα τα $i \in \{1, 2, 3, \dots, 10\} - \{r\}$. Μπορούμε τότε να θέσουμε $\bar{c}_1 + 2\bar{c}_2 + \dots + (r-1)\bar{c}_{r-1} + \bar{r}\bar{x}_r + (r+1)\bar{c}_{r+1} + \dots + (10)\bar{c}_{10} = \bar{0}$ στο $\mathbb{Z}_{11}$ και να υπολογίσουμε την τιμή του χαρακτήρα $\bar{x}_r$ ο οποίος είχε αλλοιωθεί κατά την μετάδοση. Για παράδειγμα, αν $\mathbf{c} = 0\bar{2}0\bar{1}\bar{1}\bar{c}_6\bar{5}0\bar{2}\bar{7}$ όπου $\bar{c}_6 \neq \bar{x}_6$ μπορούμε να υπολογίσουμε το $\bar{x}_6$ ως εξής: $\bar{1} \cdot \bar{0} + \bar{2} \cdot \bar{2} + \bar{3} \cdot \bar{0} + \bar{4} \cdot \bar{1} + \bar{5} \cdot \bar{1} + \bar{6} \cdot \bar{x}_6 + \bar{7} \cdot \bar{5} + \bar{8} \cdot \bar{0} + \bar{9} \cdot \bar{2} + \bar{10} \cdot \bar{7} = \bar{0}$ στο $\mathbb{Z}_{11}$, από το οποίο προκύπτει η σχέση $\bar{6} \cdot \bar{x}_6 + \bar{4} = \bar{0}$. Τέλος παρατηρούμε ότι $(\bar{6})^{-1} = \bar{2}$ στο $\mathbb{Z}_{11}$, άρα $\bar{2}(\bar{6}\bar{x}_6) + (\bar{2})(\bar{4}) = \bar{0}$. Συνάγουμε ότι

$$\bar{x}_6 = \bar{2} \cdot (\bar{-4}) = \bar{-8} = \bar{3}.$$

(3) Αν $\bar{x}_1\bar{x}_2 \dots \bar{x}_{10}$ είναι μια κωδικολέξη του ISBN-10 κώδικα C , είναι προφανές ότι $x_{10} \equiv \sum_{i=1}^9 ix_i \pmod{11}$ — έχουμε δηλαδή ότι x_{10} είναι το υπόλοιπο της διαίρεσης του αθροίσματος $\sum_{i=1}^9 ix_i$ διά το 11.

(4) Το σύνολο $\mathbb{Z}_{10}$ φαινομενικά θα μπορούσε να ήταν ένα φυσιολογικό αλφάβητο για τον κώδικα ISBN-10, όμως δεν είχε επιλεγεί για τον σκοπό αυτό. Ο λόγος είναι ότι στο $\mathbb{Z}_{10}$ το γινόμενο δύο μη-μηδενικών στοιχείων δεν είναι υποχρεωτικά μη-μηδενικό, και έτσι ο κώδικας θα έχανε τις σημαντικές ιδιότητες που έχουμε περιγράψει πιο πάνω.

Σημειώσεις και Σχόλια

1. Από την 1^η Ιανουαρίου 2007 καθιερώθηκε το ISBN-13, που είναι πλέον ένας αριθμός με 13 ψηφία, έτσι ώστε να μπορεί να ανταποκριθεί στον αυξανόμενο αριθμό των εκδόσεων. Ο νέος κώδικας ISBN-13 δεν παρουσιάζει ιδιαίτερο ενδιαφέρον από μαθηματικής άποψης, για τον λόγο αυτό μελετάμε εδώ τον κώδικα ISBN-10.

2. Το κρυπτόςστημα RSA βασίζεται στην γενική αντίληψη ότι δεν υπάρχει γρήγορος τρόπος παραγοντοποίησης αριθμών που είναι το γινόμενο δύο ‘μεγάλων’ πρώτων αριθμών (αυτό φυσικά μπορεί σήμερα να αμφισβητηθεί ανάλογα με την πρόοδο που έχει επιτευχθεί στον τομέα της πληροφορικής). Το όνομα RSA προέρχεται από τους δημιουργούς του συστήματος Ron Rivest, Adi Shamir και Leonard Adleman. Η διαδικασία κρυπτογράφησης–αποκρυπτογράφησης χρησιμοποιώντας το σύστημα αυτό είναι η εξής:

(i) Επιλέγουμε δύο ‘μεγάλους’ πρώτους αριθμούς p και q με $p \neq q$.

(ii) Γράφουμε $n = pq$ και $m = (p-1)(q-1) (= \phi(n))$.

(iii) Επιλέγουμε ένα ακέραιο e με $1 \leq e < m$ σχετικά πρώτο με το m . [Επομένως το $\bar{e}$ είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}_m$.]

(iv) Βρίσκουμε αριθμό d με $1 \leq d < m$ τέτοιο ώστε $\bar{d} = (\bar{e})^{-1}$ στο $\mathbb{Z}_m$. [Μπορεί ναδειχθεί ότι τότε, για κάθε $x \in \mathbb{Z}$, ισχύει $x^{ed} \equiv x \pmod{n}$, κοιτάζτε την Άσκηση 10.8.]

Το ζεύγος (n, e) αποτελεί το δημόσιο κλειδί, όμως οι αριθμοί p, q, m, d διατηρούνται μυστικοί. Το ζεύγος (n, d) αποτελεί το ιδιωτικό κλειδί. Η κρυπτογράφηση γίνεται μέσω της συνάρτησης $f: \mathbb{Z}_n \rightarrow \mathbb{Z}_n: x \mapsto x^e$ ($x \in \mathbb{Z}_n$) και η αποκρυπτογράφηση μέσω της αντίστροφης συνάρτησης $g: \mathbb{Z}_n \rightarrow \mathbb{Z}_n: y \mapsto y^d$, ($y \in \mathbb{Z}_n$).

Ασκήσεις

10.1 Βρείτε όλες τις λύσεις στο $\mathbb{Z}_8$ για τις εξισώσεις

(i) $\bar{2}x = \bar{0}$, (ii) $\bar{3}x = \bar{0}$, (iii) $\bar{4}x = \bar{0}$, και (iv) $\bar{5}x = \bar{3}$.

10.2 Έστω p πρώτος. Αν $\bar{a}, \bar{b} \in \mathbb{Z}_p - \{\bar{0}\}$, δείξτε ότι $\bar{a} \cdot \bar{b} \neq \bar{0}$ στο $\mathbb{Z}_p$.

10.3 (i) Να υπολογίσετε (αν υπάρχει) το αντίστροφο του $\bar{5}$ (a) στο $\mathbb{Z}_6$, και (b) στο $\mathbb{Z}_7$.

(ii) Μπορείτε να βρείτε $a \in \mathbb{Z}$ τέτοιο ώστε η εξίσωση $\bar{a} \cdot \bar{5} = \bar{1}$ να ισχύει και στο $\mathbb{Z}_6$ και στο $\mathbb{Z}_7$;

10.4 Βρείτε, αν υπάρχει, το αντίστροφο του $\bar{56}$ στο $\mathbb{Z}_{121}$.

10.5 Έστω $n \in \mathbb{N}$ με $n > 1$. Έστω επίσης $a, b \in \mathbb{Z}$ με $\mu\kappa\delta(b, n) = 1$, και S τυχαίο μη-κενό υποσύνολο του $\mathbb{Z}_n$. Δείξτε τα πιο κάτω.

- (i) $\mathbb{Z}_n = \{\bar{a} + \bar{c} : \bar{c} \in \mathbb{Z}_n\}$,
(ii) $\mathbb{Z}_n = \{\bar{b} \cdot \bar{c} : \bar{c} \in \mathbb{Z}_n\}$,
(iii) Θέτουμε $\bar{b}S = \{\bar{b} \cdot \bar{d} : \bar{d} \in S\}$. Τότε η συνάρτηση $\phi: S \rightarrow \bar{b}S : \bar{x} \mapsto \bar{b} \cdot \bar{x}$, ($\bar{x} \in S$) είναι αμφιμονοσήμαντη.
- 10.6 Έστω $a, b, n \in \mathbb{Z}$ με $n > 1$. Δείξτε ότι υπάρχει $x \in \mathbb{Z}_n$ με $\bar{a}x = \bar{b}$ στο $\mathbb{Z}_n$ αν, και μόνο αν, $\mu\kappa\delta(a, n) | b$.
- 10.7 Δείξτε ότι $4^{555} + 555^4$ δεν είναι πρώτος αριθμός.
- 10.8 Έστω p, q πρώτοι με $p \neq q$. Θέτουμε $n = pq$ και $m = \phi(n)$. Έστω επίσης $e, d \in \mathbb{Z}$ με $1 \leq e, d < m$ τέτοιοι ώστε $ed \equiv 1 \pmod{m}$. Δείξτε ότι για κάθε $x \in \mathbb{Z}$ ισχύει $x^{ed} \equiv x \pmod{n}$. [Υπόδειξη: Δείξτε πρώτα ότι $m = (p-1)(q-1)$ και, χρησιμοποιώντας το μικρό θεώρημα Fermat ότι $x^{ed} \equiv x \pmod{p}$ οποτεδήποτε $x \in \mathbb{Z}$ με $p \nmid x$.]
- 10.9 (i) Εξετάστε κατά πόσον ο αριθμός 0131653326 είναι ένας αριθμός ISBN-10.
(ii) Συμπληρώστε το αριθμό ISBN-10 0131■91399.

11. Συμμετρίες στο επίπεδο

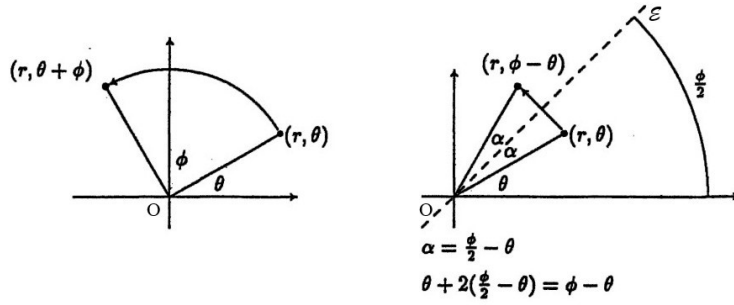
11.1. Ανακλάσεις και περιστροφές στον $\mathbb{R}^2$ (xy -επίπεδο)

Για τους σκοπούς της συζήτησης στην παράγραφο αυτή είναι βολικό να ταυτίσουμε το καρτεσιανό γινόμενο $\mathbb{R} \times \mathbb{R} (= \mathbb{R}^2)$ με το σύνολο $\mathbb{R}^{2 \times 1}$ των 2×1 πινάκων με συντελεστές από το $\mathbb{R}$, όπου $\mathbb{R}^2 \ni (x, y) \leftrightarrow \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^{2 \times 1}$. Έχουμε δηλαδή, $\mathbb{R}^2 = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} : x, y \in \mathbb{R} \right\}$.

Ένας $\mathbb{R}$ -ισομορφισμός $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ είναι μια αμφιμονοσήμαντη συνάρτηση $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$, η οποία επιπλέον ικανοποιεί $f(u+v) = f(u)+f(v)$ και $f(\lambda u) = \lambda f(u)$ για όλα τα $u, v \in \mathbb{R}^2$ και $\lambda \in \mathbb{R}$. (Έχουμε δηλαδή ότι ένας $\mathbb{R}$ -ισομορφισμός $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ είναι μια αμφιμονοσήμαντη $\mathbb{R}$ -γραμμική απεικόνιση από τον $\mathbb{R}$ -διανυσματικό χώρο $\mathbb{R}^2$ στον εαυτό του.) Συμβολίζουμε με $I_{\mathbb{R}}(\mathbb{R}^2)$ το σύνολο όλων των $\mathbb{R}$ -ισομορφισμών $\mathbb{R}^2 \rightarrow \mathbb{R}^2$.

Σημείωση 11.1. Συμβολίζουμε με $GL(2, \mathbb{R})$ το σύνολο των αντιστρέψιμων 2×2 πινάκων με συντελεστές από το $\mathbb{R}$. Έστω τώρα $A \in GL(2, \mathbb{R})$. Ορίζουμε $f_A: \mathbb{R}^2 \rightarrow \mathbb{R}^2 : \begin{bmatrix} x \\ y \end{bmatrix} \mapsto A \begin{bmatrix} x \\ y \end{bmatrix}$, (συνηθισμένος πολλαπλασιασμός πινάκων). Τότε $f_A \in I_{\mathbb{R}}(\mathbb{R}^2)$. Επιπλέον, η απεικόνιση $T: GL(2, \mathbb{R}) \rightarrow I_{\mathbb{R}}(\mathbb{R}^2): A \mapsto f_A$, ($A \in GL(2, \mathbb{R})$) είναι αμφιμονοσήμαντη. [Παρατηρούμε επίσης ότι, για $A, B \in GL(2, \mathbb{R})$ και $v = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \in \mathbb{R}^2$, έχουμε $f_{(AB)}(v) = (AB)v = A(Bv) = A(f_B(v)) = f_A(f_B(v)) = (f_A \circ f_B)(v)$.]

Η αντίστροφη απεικόνιση δίνεται με $T^{-1}: I_{\mathbb{R}}(\mathbb{R}^2) \rightarrow GL(2, \mathbb{R}) : f \mapsto \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix}$, ($f \in I_{\mathbb{R}}(\mathbb{R}^2)$), όπου $f\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$ και $f\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$. (Ελέγξτε ότι πράγματι $T^{-1}(f)$ είναι ένας αντιστρέψιμος πίνακας οποτεδήποτε $f \in I_{\mathbb{R}}(\mathbb{R}^2)$.)



Έστω $\theta, \phi \in \mathbb{R}$. Στο πιο πάνω σχήμα βλέπουμε τον τρόπο που δρουν οι μετασχηματισμοί rot_ϕ και ref_ϕ πάνω σε τυχαίο σημείο του $\mathbb{R}^2$, όπου

(i) $\text{rot}_\phi: \mathbb{R}^2 \rightarrow \mathbb{R}^2: \begin{bmatrix} r \cos \theta \\ r \sin \theta \end{bmatrix} \mapsto \begin{bmatrix} r \cos(\theta + \phi) \\ r \sin(\theta + \phi) \end{bmatrix}$ είναι μία περιστροφή γύρω από το $O(0, 0)$ κατά γωνία ϕ κατά την θετική φορά (αντίθετη προς την φορά του ρολογιού), και

(ii) $\text{ref}_\phi: \mathbb{R}^2 \rightarrow \mathbb{R}^2: \begin{bmatrix} r \cos \theta \\ r \sin \theta \end{bmatrix} \mapsto \begin{bmatrix} r \cos(\phi - \theta) \\ r \sin(\phi - \theta) \end{bmatrix}$ είναι μια ανάκλαση ως προς την ευθεία $\mathcal{E}$.

Ορίζουμε $A_\phi, B_\phi \in \text{GL}(2, \mathbb{R})$ με $A_\phi = \begin{bmatrix} \cos \phi & -\sin \phi \\ \sin \phi & \cos \phi \end{bmatrix}$ και $B_\phi = \begin{bmatrix} \cos \phi & \sin \phi \\ \sin \phi & -\cos \phi \end{bmatrix}$. Τότε $\det A_\phi = 1$ και $\det B_\phi = -1$. Θέτουμε $v = \begin{bmatrix} r \cos \theta \\ r \sin \theta \end{bmatrix} \in \mathbb{R}^2$ και παρατηρούμε, χρησιμοποιώντας τους τριγωνομετρικούς τύπους, ότι $\text{rot}_\phi(v) = A_\phi v$ και $\text{ref}_\phi(v) = B_\phi v$. Από τις παρατηρήσεις αυτές προκύπτει εύκολα ότι rot_ϕ και ref_ϕ ανήκουν στο σύνολο $I_{\mathbb{R}}(\mathbb{R}^2)$. Αυτό μας δείχνει ότι $f_{A_\phi} = \text{rot}_\phi$ και $f_{B_\phi} = \text{ref}_\phi$.

Εύκολα μπορούμε επίσης να δείξουμε ότι ισχύει το εξής αποτέλεσμα.

Πρόταση 11.2. Έστω $\alpha, \beta \in \mathbb{R}$. Έχουμε τότε

- (i) $\text{rot}_\alpha \circ \text{rot}_\beta = \text{rot}_{\alpha+\beta}$, (ii) $\text{ref}_\alpha \circ \text{ref}_\beta = \text{rot}_{\alpha-\beta}$,
 (iii) $\text{rot}_\alpha \circ \text{ref}_\beta = \text{ref}_{\alpha+\beta}$, (iv) $\text{ref}_\alpha \circ \text{rot}_\beta = \text{ref}_{\alpha-\beta}$.

Απόδειξη. Θα αποδείξουμε τα (ii) και (iii). Η απόδειξη των (i) και (iv) είναι παρόμοια.

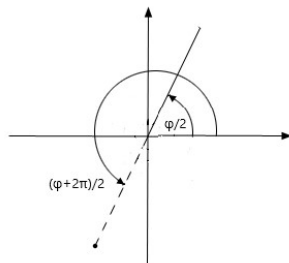
$$\begin{aligned} \text{(ii) Έχουμε, } (\text{ref}_\alpha \circ \text{ref}_\beta) \left(\begin{bmatrix} r \cos \theta \\ r \sin \theta \end{bmatrix} \right) &= \text{ref}_\alpha \left(\text{ref}_\beta \begin{bmatrix} r \cos \theta \\ r \sin \theta \end{bmatrix} \right) = \text{ref}_\alpha \left(\begin{bmatrix} r \cos(\beta - \theta) \\ r \sin(\beta - \theta) \end{bmatrix} \right) \\ &= \begin{bmatrix} r \cos(\alpha - (\beta - \theta)) \\ r \sin(\alpha - (\beta - \theta)) \end{bmatrix} = \begin{bmatrix} r \cos((\alpha - \beta) + \theta) \\ r \sin((\alpha - \beta) + \theta) \end{bmatrix}. \end{aligned}$$

$$\begin{aligned} \text{(iii) Έχουμε, } (\text{rot}_\alpha \circ \text{ref}_\beta) \left(\begin{bmatrix} r \cos \theta \\ r \sin \theta \end{bmatrix} \right) &= \text{rot}_\alpha \left(\text{ref}_\beta \begin{bmatrix} r \cos \theta \\ r \sin \theta \end{bmatrix} \right) = \text{rot}_\alpha \left(\begin{bmatrix} r \cos(\beta - \theta) \\ r \sin(\beta - \theta) \end{bmatrix} \right) \\ &= \begin{bmatrix} r \cos((\alpha + \beta) - \theta) \\ r \sin((\alpha + \beta) - \theta) \end{bmatrix}. \end{aligned}$$

□

Παρατήρηση 11.3. Έστω $\theta, \phi \in \mathbb{R}$.

(i) Προφανώς $\text{rot}_\phi = \text{rot}_{\phi+2\pi}$ και $\text{ref}_\phi = \text{ref}_{\phi+2\pi}$. Συνεπώς έχουμε $\text{rot}_{3\pi/2}\text{rot}_{3\pi/2} = \text{rot}_{3\pi} = \text{rot}_\pi$ και $\text{ref}_{\pi/2}\text{rot}_\pi = \text{ref}_{-\pi/2} = \text{ref}_{3\pi/2}$



(ii) Παρατηρούμε επίσης ότι $(\text{rot}_\phi)^{-1} = \text{rot}_{(-\phi)} = \text{rot}_{2\pi-\phi}$ και $(\text{ref}_\phi)^{-1} = \text{ref}_\phi$.

Ορισμός. Συμβολίζουμε με $O(\mathbb{R}^2)$ το σύνολο όλων των απεικονίσεων της μορφής rot_ϕ ή ref_ϕ με $0 \leq \phi < 2\pi$ όπως αυτές έχουν οριστεί πιο πάνω. Έχουμε, δηλαδή, ότι $O(\mathbb{R}^2) = \{\text{rot}_\phi: 0 \leq \phi < 2\pi\} \cup \{\text{ref}_\phi: 0 \leq \phi < 2\pi\}$.

Παρατήρηση 11.4. Προφανώς, $O(\mathbb{R}^2) \subseteq I_{\mathbb{R}}(\mathbb{R}^2)$. Μια άμεση συνέπεια της Πρότασης 11.2 είναι ότι η σύνθεση συναρτήσεων αποτελεί μια διμελή πράξη πάνω στο σύνολο $O(\mathbb{R}^2)$.

11.2. Ρίζες της μονάδας στο $\mathbb{C}$

Χρησιμοποιώντας τον ορισμό του πολλαπλασιασμού στο $\mathbb{C}$ και τους τριγωνομετρικούς τύπους εύκολα μπορούμε να αποδείξουμε την εξής

Πρόταση 11.5. (Γεωμετρική ερμηνεία πολλαπλασιασμού μιγαδικών.) Έστω $z, w \in \mathbb{C}$ με πολικές συντεταγμένες (r, θ) και (s, ψ) αντίστοιχα. Τότε οι πολικές συντεταγμένες του zw είναι (rs, ϕ) όπου $\phi = \begin{cases} \theta + \psi & \text{αν } \theta + \psi < 2\pi \\ \theta + \psi - 2\pi & \text{αν } \theta + \psi \geq 2\pi \end{cases}$. Πιο ειδικά, $|zw| = |z||w|$.

[Στην περίπτωση που τουλάχιστον ένα από τα z, w ισούται με 0, οι πιο πάνω πολικές συντεταγμένες για το zw , που επίσης ισούται με 0, δεν είναι μοναδικές όπως έχουμε δει.]

Παρατήρηση. Διατηρούμε την υπόθεση και τον συμβολισμό από την Πρόταση 11.5. Συμβολίζουμε επίσης με P_v το σημείο στο xy -επίπεδο που αντιστοιχεί στον μιγαδικό αριθμό v μέσω της ταύτισης που έχουμε κάνει. Στην ειδική περίπτωση που $w = \cos \psi + i \sin \psi$, όταν δηλαδή $s = 1$, παρατηρούμε ότι $P_{(zw)} = \text{rot}_\psi(P_z)$ — συγκρίνετε με την συζήτηση στην Παράγραφο 11.1. Με άλλα λόγια πολλαπλασιασμός με το w ‘αντιστοιχεί’ σε μια περιστροφή γύρω από το $O(0, 0)$ κατά γωνία ψ (κατά την θετική φορά). Ελέγξτε ότι $\text{ref}_\psi(P_z) = P_{(\bar{z}w)}$.

Θεώρημα 11.6. (De Moivre). Για κάθε $x \in \mathbb{R}$ και για κάθε $n \in \mathbb{N}$, ισχύει ότι $\cos(nx) + i \sin(nx) = (\cos x + i \sin x)^n$.

Απόδειξη. Θα χρησιμοποιήσουμε επαγωγή ως προς $n \geq 1$. Προφανώς το αποτέλεσμα ισχύει για $n = 1$. Για το επαγωγικό βήμα, έχουμε για $n \in \mathbb{N}$:

$$\begin{aligned} (\cos x + i \sin x)^{n+1} &= (\cos x + i \sin x)^n (\cos x + i \sin x) \\ &= (\cos(nx) + i \sin(nx))(\cos x + i \sin x) && \text{(επαγωγική υπόθεση)} \\ &= \cos(nx + x) + i \sin(nx + x) && \text{(τριγωνομετρικοί τύποι)} \\ &= \cos((n+1)x) + i \sin((n+1)x). \end{aligned}$$

□

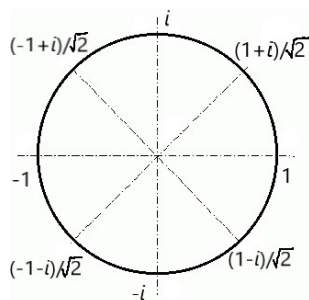
Ορισμός. Έστω $n \in \mathbb{N}$. Μια n -οστή ρίζα της μονάδας στο $\mathbb{C}$ είναι ένας μιγαδικός αριθμός z τέτοιος ώστε $z^n = 1$.

Η γεωμετρική ερμηνεία του πολλαπλασιασμού μιγαδικών αριθμών έχει ξεχωριστό ενδιαφέρον όταν οι μιγαδικοί αριθμοί z, w βρίσκονται πάνω στον μοναδιαίο κύκλο (όταν δηλαδή $|z| = 1 = |w|$). Δοσμένου $n \in \mathbb{N}$, θέτουμε $\theta = \frac{2\pi}{n}$ και $z = \cos \theta + i \sin \theta$. Παρατηρούμε ότι οι πολικές συντεταγμένες του z είναι $(1, \theta)$, οι πολικές συντεταγμένες του z^2 είναι $(1, 2\theta)$, ..., οι πολικές συντεταγμένες του z^{n-1} είναι $(1, (n-1)\theta)$, και οι πολικές συντεταγμένες του z^n είναι $(1, 0)$, (αφού $n\theta = 2\pi$). Στην πραγματικότητα μόλις έχουμε βρει όλες τις n -οστές ρίζες της μονάδας, όπως θα αποδείξουμε στην επόμενη πρόταση.

Πρόταση 11.7. Έστω $n \in \mathbb{N}$. Κάθε n -οστή ρίζα της μονάδας στο $\mathbb{C}$ ισούται με $\cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right)$ για κάποιο $k \in \{0, 1, 2, \dots, n-1\}$, και επομένως έχει μέτρο 1. Πιο ειδικά, υπάρχουν ακριβώς n διακεκριμένες n -οστές ρίζες της μονάδας στο $\mathbb{C}$.

Απόδειξη. Θέτουμε $z = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$. Από το θεώρημα De Moivre, $z^n = \left(\cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)\right)^n = \cos(2\pi) + i \sin(2\pi) = 1$. Συνεπώς z είναι μια n -οστή ρίζα της μονάδας. Αφού $z^n = 1$, έπεται ότι $(z^k)^n = z^{kn} = (z^n)^k = 1^k = 1$ για κάθε $k \in \{0, 1, 2, \dots, n-1\}$. Συμπεραίνουμε ότι z^k , όπου $k \in \{0, 1, 2, \dots, n-1\}$ είναι μια n -οστή ρίζα της μονάδας και έχουμε ήδη βρει n διακεκριμένες n -οστές ρίζες της μονάδας στο $\mathbb{C}$. Όμως δεν μπορεί να υπάρχουν άλλες n -οστές ρίζες της μονάδας στο $\mathbb{C}$ εκτός από αυτές. Για να το δούμε αυτό υποθέτουμε ότι $w \in \mathbb{C}$ με $w^n = 1$. Προφανώς $|w| = 1$ αφού $|w^n| = |w|^n$. Έχουμε δηλαδή ότι $w = \cos \theta + i \sin \theta$ για κάποιο $\theta \in \mathbb{R}$ και επομένως $w^n = \cos n\theta + i \sin n\theta (= 1)$. Έπεται ότι $n\theta = 2\pi l$ για κάποιο $l \in \mathbb{Z}$. Όμως $l = qn + r$ για κάποια $q, r \in \mathbb{Z}$ με $0 \leq r < n$. Έπεται ότι $w = \cos\left(\frac{2\pi l}{n}\right) + i \sin\left(\frac{2\pi l}{n}\right) = \cos\left(\frac{2\pi r}{n}\right) + i \sin\left(\frac{2\pi r}{n}\right) = z^r$. [Εναλλακτικά για το τελευταίο σημείο: Στο Κεφάλαιο 16 αποδεικνύουμε ότι ένα πολυώνυμο βαθμού n με ρητούς συντελεστές, όπως για παράδειγμα το $x^n - 1$, έχει το πολύ n ρίζες στο $\mathbb{C}$.] Τέλος, παρατηρούμε ότι $z^k = \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right)$ για κάθε $k \in \mathbb{N}$ (De Moivre). □

Συνεπώς, οι n -οστές ρίζες της μονάδας είναι συμμετρικά κατανεμημένες πάνω στον μοναδιαίο κύκλο. Στο Σχήμα 3 βλέπουμε την κατανομή των 8^{ων} ριζών της μονάδας πάνω στον μοναδιαίο κύκλο (εδώ, $\theta = \frac{2\pi}{8} = \frac{\pi}{4}$).



Σχήμα 3: 8^{ες} ρίζες της μονάδας

Παράδειγμα 11.8. Συμβολίζουμε με W το σύνολο των 8^{ων} ριζών της μονάδας στο $\mathbb{C}$. Θέτουμε $\zeta = \frac{1}{\sqrt{2}}(1+i) \in W$. Παρατηρούμε τότε ότι $W = \{\omega\zeta : \omega \in W\}$, αφού πολλαπλασιάζοντας το στοιχείο $\omega \in W$ με το ζ , αυτό έχει ως αποτέλεσμα να περιστραφεί το ω γύρω από το $O(0,0)$ κατά γωνία $\pi/4$. Όμως μια τέτοια περιστροφή απεικονίζει το σύνολο W στον εαυτό του.

Θεωρούμε τώρα το κανονικό οκτάγωνο Δ που είναι τοποθετημένο στο xy -επίπεδο έτσι ώστε οι κορυφές του να συμπίπτουν με τις θέσεις που έχουν οι 8^{ες} ρίζες της μονάδας. Πολλαπλασιάζοντας με το ζ έχει ως αποτέλεσμα κάθε κορυφή του Δ να απεικονιστεί στην ‘επόμενη’ κορυφή του Δ . Προκύπτει έτσι μια μετάθεση του συνόλου των κορυφών του Δ .

Ελέγξτε ότι η συνάρτηση $f: \mathbb{C} \rightarrow \mathbb{C} : z \mapsto z\zeta$ επίσης επάγει μια μετάθεση του συνόλου W των 8^{ων} ριζών της μονάδας (και επομένως του συνόλου των κορυφών του Δ). Ποια από τα στοιχεία του συνόλου $\text{Sym}(W)$ μπορούν να πραγματοποιηθούν μέσω μιας πεπερασμένης ακολουθίας μετασχηματισμών της μορφής $z \mapsto z\zeta$ και $z \mapsto \bar{z}$; [Συγκρίνετε με την Άσκηση 11.5.]

Ορισμός. Έστω $n \in \mathbb{N}$ και έστω $\omega \in \mathbb{C}$ μια n -οστή ρίζα της μονάδας στο $\mathbb{C}$. Θέτουμε $S = \{k \in \mathbb{N} : \omega^k = 1\}$. Τότε $S \neq \emptyset$, αφού $n \in S$. Έστω c το ελάχιστο στοιχείο του S (αρχή καλής διάταξης). Αν $c = n$, τότε ω καλείται μια *πρωταρχική* n -οστή ρίζα της μονάδας.

Παράδειγμα. Θέτουμε $\omega = i \in \mathbb{C}$. Τότε ω είναι μια 8^η ρίζα της μονάδας, όμως δεν είναι μια πρωταρχική 8^η ρίζα της μονάδας. Ελέγξτε ότι ω είναι μια πρωταρχική 4^η ρίζα της μονάδας.

11.3. Κινήσεις και συμμετρίες

Ορισμός. (i) Μια *κίνηση* είναι μια συνάρτηση $S: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ η οποία διατηρεί τις αποστάσεις. [Λέμε ότι η συνάρτηση $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ διατηρεί τις αποστάσεις αν ικανοποιεί $d(\mathbf{u}, \mathbf{v}) = d(f(\mathbf{u}), f(\mathbf{v}))$ για όλα τα $\mathbf{u}, \mathbf{v} \in \mathbb{R}^2$. Με $d(\mathbf{x}, \mathbf{y})$ συμβολίζουμε την γνωστή Ευκλείδεια απόσταση μεταξύ των σημείων $\mathbf{x}, \mathbf{y}$ του $\mathbb{R}^2$. Έχουμε δηλαδή ότι αν $\mathbf{x} = (x_1, x_2)$ και $\mathbf{y} = (y_1, y_2)$, τότε $d(\mathbf{x}, \mathbf{y}) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2}$.] Προφανώς οι κινήσεις είναι ενριπτικές συναρτήσεις.

(ii) Το υποσύνολο $\{\mathbf{e}_1, \mathbf{e}_2\}$ του $\mathbb{R}^2$, όπου $\mathbf{e}_1 = (1, 0)$ και $\mathbf{e}_2 = (0, 1)$, καλείται η *φυσιολογική* $\mathbb{R}$ -βάση του $\mathbb{R}^2$. Αν $\mathbf{x} = (x_1, x_2) \in \mathbb{R}^2$ ορίζουμε το *μήκος* $\|\mathbf{x}\|$ του $\mathbf{x}$ με $\|\mathbf{x}\| = \sqrt{x_1^2 + x_2^2}$.

Έπεται ότι $\|\lambda \mathbf{x}\| = |\lambda| \|\mathbf{x}\|$ για όλα τα $\lambda \in \mathbb{R}$. Επιπλέον, αν $\mathbf{a}, \mathbf{b} \in \mathbb{R}^2$ με $\mathbf{a} = (a_1, a_2)$, $\mathbf{b} = (b_1, b_2)$, έχουμε ότι $\|\mathbf{a} - \mathbf{b}\| (= \|(a_1 - b_1)\mathbf{e}_1 + (a_2 - b_2)\mathbf{e}_2\|) = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2} = d(\mathbf{a}, \mathbf{b})$.

(iii) Μια *ορθοκανονική βάση* του $\mathbb{R}^2$ είναι μια $\mathbb{R}$ -βάση $\{\mathbf{w}_1, \mathbf{w}_2\}$ του $\mathbb{R}^2$ με τα διανύσματα $\mathbf{w}_1, \mathbf{w}_2$ να είναι κάθετα μεταξύ τους και να έχουν και τα δύο μήκος 1. Παρατηρώντας τις στήλες των πινάκων της μορφής A_ϕ, B_ϕ (κοιτάξτε την Παράγραφο 11.1) βλέπουμε αμέσως ότι κάθε στοιχείο του συνόλου $O(\mathbb{R}^2)$ απεικονίζει την φυσιολογική βάση του $\mathbb{R}^2$ σε μια ορθοκανονική βάση του $\mathbb{R}^2$.

Λήμμα 11.9. Κάθε στοιχείο του συνόλου $O(\mathbb{R}^2)$ είναι μια κίνηση.

Απόδειξη. Υποθέτουμε ότι $f \in O(\mathbb{R}^2)$ και ότι $\mathbf{u}, \mathbf{v} \in \mathbb{R}^2$ με $\mathbf{u} = (u_1, u_2)$ και $\mathbf{v} = (v_1, v_2)$. Αρκεί να δείξουμε ότι $\|f(\mathbf{u}) - f(\mathbf{v})\| = \|\mathbf{u} - \mathbf{v}\|$. Όπως έχουμε δει, το σύνολο $\{f(\mathbf{e}_1), f(\mathbf{e}_2)\}$ είναι μια ορθοκανονική $\mathbb{R}$ -βάση του $\mathbb{R}^2$. Έχουμε επίσης ότι $f(\mathbf{u} - \mathbf{v}) = f(\mathbf{u}) - f(\mathbf{v})$ αφού f είναι μια $\mathbb{R}$ -γραμμική απεικόνιση και επομένως $\|f(\mathbf{u}) - f(\mathbf{v})\| = \|f(\mathbf{u} - \mathbf{v})\|$. Συνοψίζοντας, $\|f(\mathbf{u}) - f(\mathbf{v})\|^2 = \|f(\mathbf{u} - \mathbf{v})\|^2 = \|f((u_1 - v_1)\mathbf{e}_1 + (u_2 - v_2)\mathbf{e}_2)\|^2 = \|(u_1 - v_1)f(\mathbf{e}_1) + (u_2 - v_2)f(\mathbf{e}_2)\|^2 = (u_1 - v_1)^2 + (u_2 - v_2)^2 = \|\mathbf{u} - \mathbf{v}\|^2$. (Για την προτελευταία ισότητα χρησιμοποιήσαμε το Πυθαγόρειο θεώρημα.) $\square$

Ορισμός. Ο πίνακας $P \in M_n(\mathbb{R})$ καλείται *ορθογώνιος* αν $PP^t = I_n = P^tP$. [Με $M_n(\mathbb{R})$ συμβολίζουμε το σύνολο των $n \times n$ πινάκων με συντελεστές από το $\mathbb{R}$, και με P^t τον ανάστροφο του P].

Πρόταση 11.10. Έστω $P \in M_2(\mathbb{R})$ ένας ορθογώνιος πίνακας. Τότε

(i) $\det(P) \in \{1, -1\}$.

(ii) Αν $\det(P) = 1$ (αντίστοιχα, $\det(P) = -1$), τότε υπάρχει $\phi \in \mathbb{R}$ με $0 \leq \phi < 2\pi$ τέτοιο ώστε $P = A_\phi$ (αντίστοιχα, $P = B_\phi$) με τους πίνακες A_ϕ και B_ϕ όπως έχουν οριστεί στην Παράγραφο 11.1.

Απόδειξη. Έστω $P \in M_2(\mathbb{R})$ ένας ορθογώνιος πίνακας. (i) Από ιδιότητες της ορίζουσας, $1 = \det(I_2) = \det(PP^t) = \det(P)\det(P^t) = (\det(P))^2$ αφού $\det(P) = \det(P^t)$. Έπεται ότι $\det(P) \in \{1, -1\}$.

(ii) Θέτουμε $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, όπου $a, b, c, d \in \mathbb{R}$. Αφού P είναι ορθογώνιος, έχουμε ότι $P^t = P^{-1}$ και επομένως $\begin{pmatrix} a & c \\ b & d \end{pmatrix} = (\det P) \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Αν $\det(P) = +1$, τότε $a = d$, $b = -c$, και $P = \begin{pmatrix} a & -c \\ c & a \end{pmatrix}$, όπου $a^2 + c^2 = 1$. Η τελευταία σχέση μας εξασφαλίζει ότι υπάρχει $\phi \in \mathbb{R}$ με $0 \leq \phi < 2\pi$ τέτοιο ώστε $a = \cos \phi$, $c = \sin \phi$, δηλαδή με $P = A_\phi$. Παρόμοια, αν $\det(P) = -1$, τότε $a = -d$, $b = c$ και $P = \begin{pmatrix} a & c \\ c & -a \end{pmatrix}$, όπου $-a^2 - c^2 = -1$ (ισοδύναμα, $a^2 + c^2 = 1$). Συνεπώς, $P = B_\phi$ για κάποιο $\phi \in \mathbb{R}$ με $0 \leq \phi < 2\pi$ στην περίπτωση αυτή. $\square$

Πρόταση 11.11. (i) Κάθε κίνηση $S: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ η οποία σταθεροποιεί το σημείο $O(0, 0)$ είναι στοιχείο του συνόλου $O(\mathbb{R}^2)$. (Πιο ειδικά οι κινήσεις οι οποίες σταθεροποιούν το σημείο $O(0, 0)$ είναι όλες αμφιμονοσήμαντες $\mathbb{R}$ -γραμμικές απεικονίσεις.)

(ii) Το σύνολο $O(\mathbb{R}^2)$ αποτελείται ακριβώς από τις κινήσεις $S: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ οι οποίες ικανοποιούν $S((0,0)) = (0,0)$.

Απόδειξη. (i) Θα δείξουμε πρώτα ότι οποιαδήποτε κίνηση $S_1: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ η οποία σταθεροποιεί το σημείο $(0,0) (= \mathbf{0})$ και επιπλέον σταθεροποιεί τα στοιχεία $\mathbf{e}_1, \mathbf{e}_2$ της φυσιολογικής βάσης του $\mathbb{R}^2$, ισούται υποχρεωτικά με την ταυτοτική απεικόνιση $i_{\mathbb{R}^2}$. Έστω $\mathbf{x} = (x_1, x_2) \in \mathbb{R}^2$. Θέτουμε $\mathbf{y} = S_1(\mathbf{x}) = (y_1, y_2)$. Αφού $S_1(\mathbf{0}) = \mathbf{0}$, έχουμε ότι $\|S_1(\mathbf{x})\| = \|S_1(\mathbf{x}) - \mathbf{0}\| = \|S_1(\mathbf{x}) - S_1(\mathbf{0})\| = \|\mathbf{x} - \mathbf{0}\| = \|\mathbf{x}\|$. Έπεται ότι $x_1^2 + x_2^2 = y_1^2 + y_2^2$. Έχουμε επίσης, $\|S_1(\mathbf{x}) - \mathbf{e}_1\| = \|S_1(\mathbf{x}) - S_1(\mathbf{e}_1)\| = \|\mathbf{x} - \mathbf{e}_1\|$, άρα $(y_1 - 1)^2 + y_2^2 = (x_1 - 1)^2 + x_2^2$. Από τις πιο πάνω σχέσεις προκύπτει ότι $2y_1 - 1 = 2x_1 - 1$ και επομένως $y_1 = x_1$. Με παρόμοιο συλλογισμό μπορούμε να δείξουμε ότι $y_2 = x_2$. [Συγκρίνετε επίσης με την Άσκηση 11.2.]

Έστω τώρα $S: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ μια κίνηση με $S(\mathbf{0}) = \mathbf{0}$. Υποθέτουμε ότι $S(\mathbf{e}_1) = \mathbf{u}_1$ και $S(\mathbf{e}_2) = \mathbf{u}_2$. Αφού κάθε κίνηση προφανώς απεικονίζει οποιοδήποτε τρίγωνο σε ίσο τρίγωνο, βλέπουμε ότι το σύνολο $\{\mathbf{u}_1, \mathbf{u}_2\}$ επίσης αποτελεί ορθοκανονική $\mathbb{R}$ -βάση του $\mathbb{R}^2$. Συμβολίζουμε με T την (μοναδική) $\mathbb{R}$ -γραμμική απεικόνιση από τον $\mathbb{R}^2$ στον $\mathbb{R}^2$ η οποία ικανοποιεί $T(\mathbf{e}_i) = \mathbf{u}_i$ για $i = 1, 2$. Τότε T είναι ένας $\mathbb{R}$ -ισομορφισμός, επομένως υπάρχει η αντίστροφη συνάρτηση T^{-1} . Παρατηρούμε επίσης ότι η συνάρτηση T είναι μια κίνηση. [Εξήγηση: Για $\mathbf{a} = (a_1, a_2)$ και $\mathbf{b} = (b_1, b_2) \in \mathbb{R}^2$ ισχύει, $\|T(\mathbf{a}) - T(\mathbf{b})\|^2 = \|T(\mathbf{a} - \mathbf{b})\|^2 = \|T((a_1 - b_1)\mathbf{e}_1 + (a_2 - b_2)\mathbf{e}_2)\|^2 = \|(a_1 - b_1)T(\mathbf{e}_1) + (a_2 - b_2)T(\mathbf{e}_2)\|^2 = \|(a_1 - b_1)\mathbf{u}_1 + (a_2 - b_2)\mathbf{u}_2\|^2 = (a_1 - b_1)^2 + (a_2 - b_2)^2 = \|\mathbf{a} - \mathbf{b}\|^2$. (Έχουμε χρησιμοποιήσει ότι $\{\mathbf{u}_1, \mathbf{u}_2\}$ είναι μια ορθοκανονική βάση).] Συμπεραίνουμε ότι η συνάρτηση $T^{-1} \circ S$ είναι μια κίνηση (αφού είναι σύνθεση κινήσεων) η οποία σταθεροποιεί τα σημεία $\mathbf{0}, \mathbf{e}_1$ και $\mathbf{e}_2$ (και επομένως $T^{-1} \circ S = i_{\mathbb{R}^2}$). Συνοψίζοντας, μέχρι τώρα έχουμε δείξει ότι $S = T$ όπου T είναι μια $\mathbb{R}$ -γραμμική απεικόνιση. Θέτοντας $\mathbf{u}_1 = (u_1, v_1)$ και $\mathbf{u}_2 = (u_2, v_2)$, εύκολα προκύπτει ότι $S = f_P$, όπου P είναι ο ορθογώνιος πίνακας $\begin{pmatrix} u_1 & u_2 \\ v_1 & v_2 \end{pmatrix}$. Παρεμβάλλουμε τέλος την Πρόταση 11.10.

(ii) Άμεση συνέπεια του τμήματος (i) πιο πάνω και του Λήμματος 11.9. □

Έστω τώρα Δ ένα γεωμετρικό σχήμα (για παράδειγμα ένας κύκλος ή ένα κανονικό n -γώνο) στον $\mathbb{R}^2$ (xy -επίπεδο) τοποθετημένο με τέτοιο τρόπο ώστε το κέντρο του να βρίσκεται στο σημείο $O(0,0)$. Αν $f \in O(\mathbb{R}^2)$, ορίζουμε $f(\Delta) = \{f(u): u \in \Delta\}$. Ορίζουμε επίσης $\Sigma(\Delta) = \{f \in O(\mathbb{R}^2): f(\Delta) = \Delta\}$. Τα στοιχεία του συνόλου $\Sigma(\Delta)$ καλούνται *συμμετρίες* του γεωμετρικού σχήματος Δ . Είναι εύκολο να δούμε ότι η σύνθεση συναρτήσεων αποτελεί μια διμελή πράξη στο σύνολο $\Sigma(\Delta)$. [Εξήγηση: Έστω $f, g \in \Sigma(\Delta)$. Από τον ορισμό του συνόλου $\Sigma(\Delta)$ έχουμε ότι $f, g \in O(\mathbb{R}^2)$ και επομένως $g \circ f \in O(\mathbb{R}^2)$ από την Παρατήρηση 11.4. Επιπλέον, έχουμε $\Delta = f(\Delta) = \{f(u): u \in \Delta\}$ και επομένως $(g \circ f)(\Delta) = \{(g \circ f)(u): u \in \Delta\} = \{g(f(u)): u \in \Delta\} = g(\Delta) = \Delta$.]

Σημείωση. (i) Με τον όρο *κέντρο* ενός κανονικού n -γώνου εννοούμε το κέντρο του μοναδικού περιγεγραμμένου κύκλου του κανονικού αυτού n -γώνου.

(ii) Διαισθητικά, συμμετρία ενός γεωμετρικού σχήματος είναι ένας ‘μετασχηματισμός’ (που διατηρεί τις αποστάσεις και σταθεροποιεί το σημείο $O(0,0)$) ο οποίος ‘μετακινεί’ το σχήμα με τέτοιο τρόπο ώστε η τελική του θέση να μην διακρίνεται από την αρχική, χωρίς να

αποκλείουμε όμως το ενδεχόμενο ξεχωριστά σημεία του γεωμετρικού σχήματος να έχουν μετακινηθεί σε νέα σημεία του σχήματος.

Πρόταση 11.12. Έστω Δ_n ($n \geq 3$) ένα κανονικό n -γωνο τοποθετημένο στο xy -επίπεδο έτσι ώστε το κέντρο του να βρίσκεται στο σημείο $O(0, 0)$ και η μια κορυφή του στο σημείο $Q(1, 0)$. Τότε κάθε στοιχείο του $\Sigma(\Delta_n)$ επάγει μια μετάθεση του συνόλου των κορυφών του Δ_n και, επιπλέον, καθορίζεται πλήρως από την δράση του πάνω στο σύνολο αυτό.

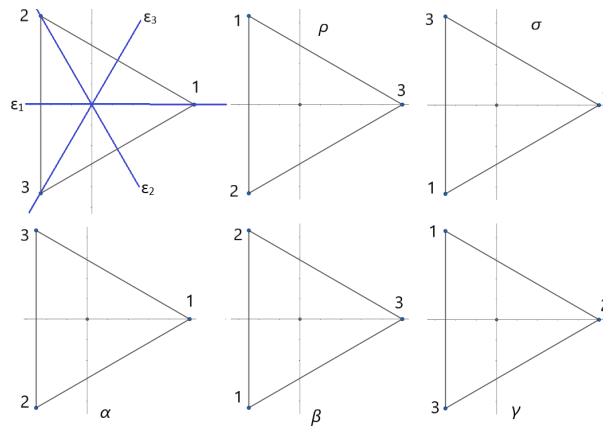
Απόδειξη. Έστω $f \in \Sigma(\Delta_n)$. Πιο ειδικά η f είναι μια $\mathbb{R}$ -γραμμική απεικόνιση η οποία διατηρεί τις αποστάσεις. Έστω επίσης $X = \{1, 2, \dots, n\}$ το σύνολο των κορυφών του Δ_n . Το σημείο $O(0, 0)$ βρίσκεται στο κέντρο του μοναδιαίου κύκλου που είναι ο μοναδικός περιγεγραμμένος κύκλος του Δ_n . Επομένως, τα μόνα σημεία του Δ_n που βρίσκονται σε απόσταση 1 από το σημείο $O(0, 0)$ είναι τα στοιχεία του συνόλου X , ενώ τα υπόλοιπα σημεία του Δ_n βρίσκονται σε απόσταση < 1 από το $O(0, 0)$. Συνεπώς, αν $\kappa \in X$ έχουμε ότι $1 = d(O, \kappa) = d(f(O), f(\kappa)) = d(O, f(\kappa))$ αφού $f(O) = O$. Έπεται ότι $f(\kappa) \in X$ για όλες τις $\kappa \in X$ και, αφού f είναι ενριπτική, έχουμε ότι $\{f(\kappa) : \kappa \in X\} = X$. Συνοψίζοντας, έχουμε δείξει μέχρι τώρα ότι κάθε $f \in \Sigma(\Delta_n)$ επάγει μια μετάθεση του συνόλου $X = \{1, 2, \dots, n\}$ των κορυφών του Δ_n .

Υποθέτουμε τώρα, χωρίς βλάβη της γενικότητας, ότι η κορυφή **1** βρίσκεται στο σημείο $Q(1, 0)$ και η κορυφή **2** στο σημείο $P(\cos(\frac{2\pi}{n}), \sin(\frac{2\pi}{n}))$. Υποθέτουμε επιπλέον ότι $g, h \in \Sigma(\Delta_n)$ με $g(\kappa) = h(\kappa)$ για όλες τις $\kappa \in X$. Όμως το σύνολο $\{(1, 0), (\cos(\frac{2\pi}{n}), \sin(\frac{2\pi}{n}))\}$ αποτελεί μια $\mathbb{R}$ -βάση του $\mathbb{R}^2$ οποτεδήποτε $n \geq 3$, και g, h είναι $\mathbb{R}$ -γραμμικές απεικονίσεις με $g((1, 0)) = h((1, 0))$ και $g((\cos(\frac{2\pi}{n}), \sin(\frac{2\pi}{n}))) = h((\cos(\frac{2\pi}{n}), \sin(\frac{2\pi}{n})))$. Συνάγουμε ότι $g = h$, και επομένως κάθε στοιχείο της $\Sigma(\Delta_n)$ καθορίζεται πλήρως από την δράση του πάνω στο σύνολο X . [Συγκρίνετε επίσης με την Άσκηση 11.2.] $\square$

Σχόλιο. Διατηρούμε τον συμβολισμό από την Πρόταση 11.12. Έστω επίσης $S: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ μια κίνηση τέτοια ώστε $S(\Delta_n) = \Delta_n$. Αφού S διατηρεί τις αποστάσεις, ο κύκλος με ακτίνα 1 και κέντρο το $S((0, 0))$ είναι ο (μοναδικός) περιγεγραμμένος κύκλος για το $\Delta_n (= S(\Delta_n))$. Έπεται ότι $S((0, 0)) = (0, 0)$. Παρεμβάλλοντας τώρα την Πρόταση 11.11 βλέπουμε ότι το σύνολο $\Sigma(\Delta_n)$ αποτελείται ακριβώς από τις κινήσεις $S: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ οι οποίες ικανοποιούν $S(\Delta_n) = \Delta_n$.

Παραδείγματα 11.13. (i) Κάθε στοιχείο του συνόλου $O(\mathbb{R}^2)$ είναι και μια συμμετρία του μοναδιαίου κύκλου.

(ii) Οι συμμετρίες του ισοπλεύρου τριγώνου Δ_3 :



Από την Πρόταση 11.12, κάθε στοιχείο του συνόλου $\Sigma(\Delta_3)$ επάγει μια μετάθεση του συνόλου των κορυφών του Δ_3 και, επιπλέον, καθορίζεται πλήρως από την δράση του πάνω στο σύνολο αυτό. Πιο συγκεκριμένα, έχουμε τις εξής συμμετρίες:

$$i = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \quad \rho = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \quad \sigma = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix},$$

$$\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \quad \beta = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \quad \gamma = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix},$$

όπου i , ρ και σ είναι περιστροφή γύρω από το $O(0,0)$ κατά γωνία 0° , 120° και 240° αντίστοιχα κατά την θετική φορά (αντίθετη προς την φορά των δεικτών του ρολογιού), και α , β και γ είναι ανάκλαση ως προς την ευθεία e_1 , e_2 και e_3 αντίστοιχα. Προφανώς, i ισούται με την ταυτοτική συνάρτηση. Εύκολα μπορούμε να δείξουμε τώρα ότι $\Sigma(\Delta_3) = \{i, \alpha, \beta, \gamma, \rho, \sigma\}$.

Σημειώσεις και Σχόλια

1. Η συμμετρία εμφανίζεται σε πολλούς τομείς των μαθηματικών όπως και σε πολλές άλλες μορφές τέχνης. Η γεωμετρική συμμετρία είναι ίσως η πιο εμφανής από όλες. Γι' αυτό οι ομάδες (κοιτάξτε το Κεφάλαιο 12) και η γεωμετρία είναι τόσο στενά συνδεδεμένες. Στην πραγματικότητα η συμμετρία είναι και ένας από τους πιο σημαντικούς λόγους ύπαρξης των ομάδων.

2. Οι μαθηματικοί και οι φυσικοί συχνά αναγνωρίζουν την ομορφιά αλλά και την σπουδαιότητα της συμμετρίας: Μια θεωρία που βασίζεται σε συμμετρικές αρχές είναι πιο πιθανό να περιγράψει με περισσότερη ακρίβεια την φύση, επειδή οι συμμετρίες είναι συχνά συνώνυμες με την απλότητα, την αρμονία και την εσωτερική συνέπεια. Η συμμετρία μας επιτρέπει να διακρίνουμε ποιες ποσότητες ή νόμοι παραμένουν σταθεροί κάτω από συγκεκριμένους μετασχηματισμούς (όπως περιστροφές, ανακλάσεις, και μεταφορές). Για παράδειγμα, αν ξέρουμε ότι ένα σύστημα έχει συμμετρία ως προς τις περιστροφές, μπορούμε να μειώσουμε τον αριθμό των μεταβλητών που πρέπει να λάβουμε υπόψη για την περιγραφή του.

3. Σημαντικές εφαρμογές της θεωρίας αναπαράστασεων αφορούν στις συμμετρίες. Τέτοιες εφαρμογές προκύπτουν επειδή σε κάθε φυσικό σύστημα αντιστοιχεί μία ομάδα συμμετρίας G , και ορισμένοι διανυσματικοί χώροι που συνδέονται με το σύστημα αποδεικνύεται ότι έχουν την δομή ενός $\mathbb{R}G$ -μοδίου. Για παράδειγμα, η παλμική κίνηση ενός μορίου διέπεται από διάφορες διαφορικές εξισώσεις, και η ομάδα συμμετρίας του μορίου δρα στον χώρο των λύσεων των εξισώσεων αυτών.

Ασκήσεις

11.1 Δείξτε ότι μια κίνηση $S: \mathbb{R}^2 \rightarrow \mathbb{R}^2$

- (i) απεικονίζει οποιοδήποτε τρίγωνο ABC σε ένα ίσο τρίγωνο
- (ii) διατηρεί τις γωνίες, και
- (iii) απεικονίζει ευθεία σε ευθεία

11.2 Αν οι κινήσεις $S_1, S_2: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ συμφωνούν πάνω σε 3 μη-συνευθειακά σημεία, εξετάστε κατά πόσον $S_1 = S_2$.

11.3 Να προσδιορίσετε τον μιγαδικό z_2 ο οποίος προκύπτει μετά από την περιστροφή του $z_1 = 2 + i$ γύρω από το $O(0, 0)$ κατά γωνία $\pi/6$.

11.4 Βρείτε το σύνολο των συμμετριών $\Sigma(\Delta)$ στην περίπτωση που το σχήμα Δ (το οποίο είναι τοποθετημένο στο xy -επίπεδο) είναι ένα

- (i) τετράγωνο με το κέντρο του να βρίσκεται στο σημείο $O(0, 0)$ και η μια κορυφή του στο σημείο $Q(1, 0)$, και
- (ii) ορθογώνιο με τις κορυφές του να βρίσκονται στα σημεία $Q_1(4, 3)$, $Q_2(-4, 3)$, $Q_3(-4, -3)$, $Q_4(4, -3)$.

11.5 Διατηρούμε τον συμβολισμό από το Παράδειγμα 11.8. Θέτουμε $G = \Sigma(\Delta) \cap \{\text{rot}_\phi: 0 \leq \phi < 2\pi\}$. Δείξτε ότι υπάρχει στοιχείο $g \in G$ το οποίο έχει και τις δύο ιδιότητες (i), (ii) πιο κάτω:

- (i) $G = \{g^k: 0 \leq k \leq 7\}$, όπου $g^0 = i_{\mathbb{R}^2}$ και $g^r = gg \dots g$ (r φορές) για $r \in \mathbb{N}$.
- (ii) Η συνάρτηση $\phi: G \rightarrow C_8: g^k \mapsto \zeta^k$ ($0 \leq k \leq 7$) είναι αμφιμονοσήμαντη και ικανοποιεί $\phi(f \circ h) = \phi(f)\phi(h)$ για όλα τα $f, h \in G$.

Υπάρχουν και άλλα στοιχεία στο σύνολο G που ικανοποιούν και τις δύο πιο πάνω ιδιότητες;

11.6 Έστω C_6 το σύνολο των 6^{ων} ριζών της μονάδας στο $\mathbb{C}$.

- (i) Βρείτε τα στοιχεία του C_6 .
- (ii) Ποιά από τα στοιχεία του C_6 είναι πρωταρχικές 6^{ες} ρίζες της μονάδας;

11.7 (i) Βρείτε $q, r \in \mathbb{Z}$ με $0 \leq r < 6$ τέτοια ώστε $131 = 6q + r$.

- (ii) Θέτουμε $w = \cos(2\pi/6) + i \sin(2\pi/6) \in C_6$ και $\pi \in S_6$ όπου $\pi = (1\ 2\ 3\ 4\ 5\ 6)$. Μπορείτε να βρείτε $s, t \in \mathbb{Z}$ με $0 \leq s, t < 6$ τέτοια ώστε $w^{131} = w^s$ και $\pi^{131} = \pi^t$; (Υπόδειξη: Να υπολογίσετε πρώτα τα w^6 και π^6 .)

11.8 Έστω $n \in \mathbb{N}$. Έστω επίσης C_n το σύνολο των n -οστών ριζών της μονάδας στο $\mathbb{C}$. Θέτουμε $w = \cos(2\pi/n) + i \sin(2\pi/n) \in C_n$. Δείξτε τα ακόλουθα.

- (i) $C_n = \{1, w, w^2, \dots, w^{n-1}\}$.
- (ii) Ο συνηθισμένος πολλαπλασιασμός στο $\mathbb{C}$ ορίζει μια διμελή πράξη στο C_n .
- (iii) Αν $u \in C_n$, τότε υπάρχει $v \in C_n$ τέτοιο ώστε $uv = 1 = vu$.
- (iv) Αν $x \in C_n$ είναι μια πρωταρχική n -οστή ρίζα της μονάδας, τότε $C_n = \{1, x, \dots, x^{n-1}\}$.

11.9 Έστω $n \in \mathbb{N}$. Θέτουμε $C_n = \{z \in \mathbb{C}: z^n = 1\}$. Θέτουμε επίσης $R_1 = \{(z, w) \in C_{12} \times C_{12}: zw^{-1} \in C_4\} (\subseteq C_{12} \times C_{12})$ και $R_2 = \{(z, w) \in C_{12} \times C_{12}: z^{-1}w \in C_4\} (\subseteq C_{12} \times C_{12})$. Δείξτε ότι R_1 και R_2 αποτελούν σχέσεις ισοδυναμίας πάνω στο σύνολο C_{12} και βρείτε, για την κάθε περίπτωση, την αντίστοιχη διαμέριση του συνόλου C_{12} .

11.10 Έστω $m, n \in \mathbb{N}$. Εξετάστε κατά πόσον υπάρχει $d \in \mathbb{N}$ με $C_m \cap C_n = C_d$.

12. Ομάδες

12.1. Ορισμοί, παραδείγματα, βασικές ιδιότητες

Ορισμός. Ομάδα είναι ένα ζεύγος $(G, *)$ που αποτελείται από ένα μη-κενό σύνολο G και μια διμελή πράξη $*$ πάνω σ' αυτό τέτοια ώστε

- (i) $f * (g * h) = (f * g) * h$ για όλα τα $f, g, h \in G$ (προσεταιρισμός)
- (ii) υπάρχει κάποιο στοιχείο $e \in G$ (ουδέτερο) με $g * e = g = e * g$ για όλα τα $g \in G$
- (iii) αν $g \in G$, τότε υπάρχει στοιχείο $\tilde{g} \in G$ (συμμετρικό του g) με $g * \tilde{g} = e = \tilde{g} * g$.

Σημείωση. Έστω $(G, *)$ ομάδα. Τότε υπάρχει μοναδικό ουδέτερο στοιχείο $e \in G$ και κάθε στοιχείο $g \in G$ έχει μοναδικό συμμετρικό στοιχείο (κοιτάξτε τις Προτάσεις 4.3 και 4.7).

Παραδείγματα 12.1.

- (i) Έστω X μη-κενό σύνολο. Τότε το ζεύγος $(\text{Sym}(X), \circ)$, όπου $\circ$ συμβολίζει την σύνθεση συναρτήσεων, αποτελεί ομάδα — συγκρίνετε με την συζήτηση στην Παράγραφο 4.2. [Σε τέτοια περίπτωση λέμε ότι $\text{Sym}(X)$ αποτελεί ομάδα ως προς την σύνθεση συναρτήσεων.]
- (ii) Το σύνολο $O(\mathbb{R}^2) (= \{\text{rot}_\phi: 0 \leq \phi < 2\pi\} \cup \{\text{ref}_\phi: 0 \leq \phi < 2\pi\})$ επίσης αποτελεί ομάδα ως προς την σύνθεση συναρτήσεων (είναι μια από τις *ορθογώνιες ομάδες*).
- (iii) $\mathbb{R}$ (αντίστοιχα, $\mathbb{C}$) αποτελεί ομάδα ως προς την συνηθισμένη πρόσθεση στο $\mathbb{R}$ (αντίστοιχα, στο $\mathbb{C}$).
- (iv) $\mathbb{R} - \{0\}$ (αντίστοιχα, $\mathbb{C} - \{0\}$) αποτελεί ομάδα ως προς τον συνηθισμένο πολλαπλασιασμό στο $\mathbb{R}$ (αντίστοιχα, στο $\mathbb{C}$).
- (v) Έστω $n \in \mathbb{N}$. Θέτουμε $C_n = \{z \in \mathbb{C}: z^n = 1\}$, το σύνολο των n -οστων ριζών της μονάδας στο $\mathbb{C}$. Τότε C_n αποτελεί ομάδα ως προς τον συνηθισμένο πολλαπλασιασμό στο $\mathbb{C}$. [Υπενθύμιση: $C_n = \{1, \omega, \omega^2, \dots, \omega^{n-1}\}$ όπου $\omega = \cos(\frac{2\pi}{n}) + i \sin(\frac{2\pi}{n}) \in \mathbb{C}$.]
- (vi) Έστω $n \in \mathbb{N}$ με $n > 1$. Τότε $(\mathbb{Z}_n, +)$ και $(\mathbb{Z}_n^*, \cdot)$, όπου $+$ και $\cdot$ είναι αντίστοιχα η πρόσθεση και ο πολλαπλασιασμός που έχουμε ορίσει στο σύνολο $\mathbb{Z}_n$, αποτελούν ομάδες.

- (vii) Συμβολίζουμε, ως συνήθως, με $M_n(\mathbb{R})$ το σύνολο $n \times n$ πινάκων με συντελεστές στο $\mathbb{R}$. Θέτουμε επίσης $GL(n, \mathbb{R}) = \{A \in M_n(\mathbb{R}) : A \text{ είναι αντιστρέψιμος}\}$. Τότε $GL(n, \mathbb{R})$ αποτελεί ομάδα ως προς τον συνηθισμένο πολλαπλασιασμό πινάκων. Η ομάδα αυτή καλείται η *γενική γραμμική ομάδα βαθμού n επί του $\mathbb{R}$* .
- (viii) Έστω Δ ένα γεωμετρικό σχήμα (για παράδειγμα ένας κύκλος ή ένα κανονικό n -γωνο) στον $\mathbb{R}^2$ (xy -επίπεδο) τοποθετημένο με τέτοιο τρόπο ώστε το κέντρο του να βρίσκεται στο σημείο $O(0, 0)$. [Υπενθύμιση: Αν $f \in O(\mathbb{R}^2)$, ορίζουμε $f(\Delta) = \{f(u) : u \in \Delta\}$. Ορίζουμε επίσης $\Sigma(\Delta) = \{f \in O(\mathbb{R}^2) : f(\Delta) = \Delta\}$.] Ελέγξτε ότι το σύνολο $\Sigma(\Delta)$ αποτελεί ομάδα ως προς την σύνθεση συναρτήσεων. Η ομάδα $\Sigma(\Delta)$ ονομάζεται η *ομάδα συμμετριών του σχήματος Δ* .

Σημείωση. Στο Παράδειγμα 12.1(vii) μπορούμε να αντικαταστήσουμε το $\mathbb{R}$ με $\mathbb{F}$, όπου $\mathbb{F}$ είναι οποιοδήποτε σώμα (κοιτάξτε στο Κεφάλαιο 15), ορίζοντας έτσι την ομάδα $GL(n, \mathbb{F})$. Για παράδειγμα $\mathbb{F} = \mathbb{C}$ ή $\mathbb{F} = \mathbb{Z}_p$. Σε όλες αυτές τις περιπτώσεις προκύπτει εύκολα από τις ιδιότητες της ορίζοντας ότι $GL(n, \mathbb{F}) = \{A \in M_n(\mathbb{F}) : \det(A) \neq 0\}$.

Ορισμός. Μια ομάδα $(G, *)$ ονομάζεται *αβελιανή* αν επιπλέον η διμελής πράξη $*$ είναι αντιμεταθετική, δηλαδή ισχύει $a * b = b * a$ για όλα τα $a, b \in G$.

Παράδειγμα 12.2. Οι ομάδες στα Παραδείγματα 12.1 (iii), (iv), (v) και (vi) είναι αβελιανές. Η $(\text{Sym}(X), \circ)$ δεν είναι αβελιανή οποτεδήποτε το σύνολο X περιέχει περισσότερα από 2 στοιχεία. Επιπλέον, η $GL(n, \mathbb{R})$ είναι αβελιανή αν, και μόνο αν, $n = 1$.

Συμβολισμός. Πιο κάτω, για σκοπούς απλοποίησης του συμβολισμού, θα γράφουμε ab αντί για $a * b$ και θα ονομάζουμε την έκφραση ab *γινόμενο των a και b* ($a, b \in G$). Επίσης για το ουδέτερο στοιχείο, αντί του e θα χρησιμοποιούμε το 1_G , το οποίο θα ονομάζουμε *μοναδιαίο* στοιχείο της ομάδας. Το συμμετρικό $\tilde{a}$ κάποιου στοιχείου $a \in G$ θα το συμβολίζουμε με a^{-1} και θα το ονομάζουμε *αντίστροφο* του a .

Προσθετικός συμβολισμός. Σε μερικές όμως περιπτώσεις, η διμελής πράξη πάνω στο σύνολο G ονομάζεται *πρόσθεση* και συμβολίζεται με $+$ (Παραδείγματα 12.1(iii), (vi)). Σε τέτοιες περιπτώσεις, αντί του $a * b$ χρησιμοποιείται το $a + b$, το ουδέτερο ονομάζεται *μηδενικό* και συμβολίζεται με 0_G , και το συμμετρικό κάποιου στοιχείου $a \in G$ ονομάζεται *αντίθετο* του a και συμβολίζεται με $-a$. [Θα χρησιμοποιούμε τον προσθετικό συμβολισμό σε περιπτώσεις που αυτός ταιριάζει περισσότερο.]

Σε αρκετές περιπτώσεις πιο κάτω, πάλι για συντομία, αντί να λέμε η ομάδα $(G, *)$ ή $(G, \cdot)$ ή $(G, +)$ θα λέμε η ομάδα G και θα υπονοούμε την πράξη.

Λήμμα 12.3. Έστω G ομάδα και $g, h \in G$. Έχουμε τότε ότι

$$(i) (g^{-1})^{-1} = g, \quad (ii) (gh)^{-1} = h^{-1}g^{-1}.$$

Απόδειξη. (i) Έχουμε, $gg^{-1} = 1_G = g^{-1}g$, άρα $(g^{-1})^{-1} = g$.

(ii) Από την Πρόταση 5.5 έχουμε, $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = g1_Gg^{-1} = gg^{-1} = 1_G$. Παρόμοια, $(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1}g)h = h^{-1}1_Gh = h^{-1}h = 1_G$. $\square$

Ορισμός. Η ομάδα G ονομάζεται *πεπερασμένης τάξης* n (συμβολισμός: $|G| = n$), αν το σύνολο G αποτελείται από ακριβώς n στοιχεία για κάποιο $n \in \mathbb{N}$. Διαφορετικά λέμε ότι η ομάδα G είναι *άπειρης τάξης*.

Παράδειγμα. Η ομάδα $(\mathbb{Z}, +)$, όπου $+$ είναι η συνηθισμένη πρόσθεση ακεραίων, είναι άπειρης τάξης. Οι ομάδες $(\mathbb{Z}_n, +)$ και $(\mathbb{Z}_n^*, \cdot)$ στο Παράδειγμα 12.1(vi) είναι και οι δύο πεπερασμένης τάξης και έχουν τάξη n και $\phi(n)$ αντίστοιχα. Έχουμε επίσης ότι $|C_n| = n$.

Ο επόμενος ορισμός στην πραγματικότητα γενικεύει τον ορισμό που είχαμε δώσει στο Παράδειγμα 4.8 για την ‘δύναμη’ μιας μετάθεσης.

Ορισμός. (Συγκρίνετε με την Πρόταση 5.5.) Έστω G ομάδα, $g \in G$ και $n \in \mathbb{Z}$. Θέτουμε

$$g^n = \begin{cases} gg \dots g \text{ (} n \text{ φορές)}, & \text{αν } n \in \mathbb{N}, \\ 1_G, & \text{αν } n = 0, \\ g^{-1}g^{-1} \dots g^{-1} \text{ (} -n \text{ φορές)}, & \text{αν } -n \in \mathbb{N}. \end{cases}$$

Πρόταση 12.4. Έστω G ομάδα. Για όλα τα $g \in G$ και για όλα τα $m, n \in \mathbb{Z}$ ισχύουν

$$g^m g^n = g^{m+n} \quad \text{και} \quad (g^m)^n = g^{mn}.$$

Απόδειξη. Προφανές αν $m = 0$ ή $n = 0$, άρα υποθέτουμε ότι $m \neq 0$ και $n \neq 0$. Θεωρούμε τις περιπτώσεις (i) $m > 0, n > 0$, (ii) $m > 0, n < 0$, (iii) $m < 0, n > 0$ και (iv) $m < 0, n < 0$. Το αποτέλεσμα προφανώς ισχύει στην περίπτωση (i). Έστω τώρα ότι $m > 0$ και $n < 0$. Θέτουμε $\nu = -n (\in \mathbb{N})$. Έχουμε τότε, $g^m g^n = g^m (g^{-1})^\nu = g^{m-\nu} = g^{m+n}$ (για την προτελευταία ισότητα εξετάζουμε ξεχωριστά τις περιπτώσεις $m > \nu, m = \nu, m < \nu$, και χρησιμοποιούμε τον πιο πάνω ορισμό). Επίσης, $(g^m)^n = ((g^m)^{-1})^\nu = ((g^{-1})^m)^\nu = (g^{-1})^{m\nu} = g^{-m\nu} = g^{mn}$. Με παρόμοιο τρόπο δείχνουμε τις περιπτώσεις (iii) και (iv). $\square$

Παράδειγμα. $(g^{-3})^4 = (g^{-1}g^{-1}g^{-1})^4 = (g^{-1})^{12} = g^{-12} = g^{(-3 \cdot 4)}$.

Ένας εύκολος τρόπος να κατασκευάσουμε νέες ομάδες από γνωστές ομάδες είναι ο εξής.

Έστω H, K ομάδες. Προσπαθούμε να ορίσουμε πάνω στο καρτεσιανό γινόμενο $H \times K$ μια διμελή πράξη ως εξής:

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2) \quad \text{όπου } h_1, h_2 \in H \text{ και } k_1, k_2 \in K.$$

Για να ελέγξουμε ότι πράγματι έχουμε ορίσει μια διμελή πράξη αρκεί να παρατηρήσουμε, αφού H, K είναι ομάδες, ότι $h_1 h_2 \in H$ και $k_1 k_2 \in K$ οποτεδήποτε $h_1, h_2 \in H$ και $k_1, k_2 \in K$.

Η πιο πάνω διμελής πράξη είναι προσεταιριστική: Για $1 \leq i \leq 3$, έστω $(h_i, k_i) \in H \times K$. Χρησιμοποιώντας τον προσεταιρισμό στις H, K έχουμε τότε $((h_1, k_1)(h_2, k_2))(h_3, k_3) = (h_1 h_2, k_1 k_2)(h_3, k_3) = ((h_1 h_2)h_3, (k_1 k_2)k_3) = (h_1(h_2 h_3), k_1(k_2 k_3)) = (h_1, k_1)(h_2 h_3, k_2 k_3) = (h_1, k_1)((h_2, k_2)(h_3, k_3))$.

Έχουμε επίσης ότι $(1_H, 1_K)$ είναι το ουδέτερο στοιχείο του συνόλου $H \times K$ ως προς την πράξη αυτή, ενώ το στοιχείο $(h^{-1}, k^{-1}) \in H \times K$ είναι το συμμετρικό του $(h, k) \in H \times K$. [H, K είναι ομάδες, άρα $h^{-1} \in H$ και $k^{-1} \in K$ οποτεδήποτε $h \in H$ και $k \in K$.]

Πρόταση 12.5. Έστω H, K ομάδες. Τότε το σύνολο $H \times K$ αποτελεί ομάδα ως προς την πιο πάνω ορισθείσα πράξη. (Η ομάδα αυτή καλείται το *εξωτερικό ευθύ γινόμενο* των ομάδων H και K .)

Παραδείγματα. (i) Θέτουμε $\omega = \cos\left(\frac{2\pi}{5}\right) + i \sin\left(\frac{2\pi}{5}\right)$. Τότε $C_5 \times \mathbb{Z}_6^* = \{(1, \bar{1}), (1, \bar{5}), (\omega, \bar{1}), (\omega, \bar{5}), (\omega^2, \bar{1}), (\omega^2, \bar{5}), (\omega^3, \bar{1}), (\omega^3, \bar{5}), (\omega^4, \bar{1}), (\omega^4, \bar{5})\}$.

(ii) Θέτουμε $H = (\mathbb{Z}_4, +)$ και $K = (\mathbb{Z}_8^*, \cdot)$. Το ουδέτερο στοιχείο της ομάδας $H \times K$ είναι το στοιχείο $(\bar{0}, \bar{1}) \in H \times K$ και το συμμετρικό του στοιχείου $(\bar{3}, \bar{5}) \in H \times K$ είναι το στοιχείο $(\bar{1}, \bar{5}) \in H \times K$. Έχουμε επίσης ότι $|H \times K| = 16$.

(iii) Το εξωτερικό ευθύ γινόμενο αβελιανών ομάδων είναι αβελιανή ομάδα.

12.2. Η συμμετρική ομάδα

Θέτουμε $X = \{1, 2, \dots, n\}$ όπου $n \in \mathbb{N}$. Τότε η ομάδα $\text{Sym}(X)$ (ως προς την σύνθεση συναρτήσεων) ονομάζεται η *συμμετρική ομάδα σε n σύμβολα*, ή η *συμμετρική ομάδα βαθμού n* και συμβολίζεται με S_n . Προφανώς, $|S_n| = n!$. Τα στοιχεία της S_n ονομάζονται *μεταθέσεις*.

Όπως έχουμε δει, μια μετάθεση $\pi \in S_n$ έχει μια παράσταση της μορφής

$$\pi = \begin{bmatrix} 1 & 2 & \dots & n \\ x_1 & x_2 & \dots & x_n \end{bmatrix} \text{ όπου } x_i = \pi(i), \text{ για όλα τα } i \text{ με } 1 \leq i \leq n.$$

Ορισμός. (Υπενθύμιση.) Έστω $\emptyset \neq \{a_1, \dots, a_k\} \subseteq \{1, 2, \dots, n\}$. Έστω επίσης η μετάθεση $\pi \in S_n$ όπου $\pi(a_1) = a_2, \pi(a_2) = a_3, \dots, \pi(a_{k-1}) = a_k, \pi(a_k) = a_1$ και $\pi(b) = b$ για $b \in \{1, 2, \dots, n\} - \{a_1, \dots, a_k\}$. Τότε π ονομάζεται *k -κύκλος*. Γράφουμε $\pi = (a_1 a_2 \dots a_k)$. Προφανώς $\pi^{-1} = (a_k a_{k-1} \dots a_1)$.

Παράδειγμα 12.6.

$$\pi = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix} = (1\ 2\ 3) \text{ είναι ένας 3-κύκλος στην } S_4.$$

Ορισμός. (Υπενθύμιση.) Δύο κύκλοι $(a_1 a_2 \dots a_k), (b_1 b_2 \dots b_l)$ ονομάζονται *ξένοι* μεταξύ τους αν $\{a_1, a_2, \dots, a_k\} \cap \{b_1, b_2, \dots, b_l\} = \emptyset$.

Παράδειγμα 12.7. Στην S_8 , οι κύκλοι $(1\ 3\ 5\ 7)$ και $(2\ 4\ 8)$ είναι ξένοι μεταξύ τους. Όπως έχουμε δει, κύκλοι ξένοι μεταξύ τους αντιμετατίθενται.

Παράδειγμα 12.8. Στην S_8 παρατηρούμε ότι

$$\begin{aligned} \pi &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 8 & 7 & 6 & 1 & 2 \end{bmatrix} = (1\ 3\ 5\ 7)(2\ 4\ 8) \\ &= (2\ 4\ 8)(1\ 3\ 5\ 7) = (2\ 4\ 8)(1\ 3\ 5\ 7)(6). \end{aligned}$$

Ορισμός. (i) Οι κύκλοι $\alpha_1, \alpha_2, \dots, \alpha_m$ (όπου $m > 2$) στην S_n καλούνται *ξένοι μεταξύ τους* αν είναι ξένοι μεταξύ τους *ανά δύο* (αν δηλαδή οποιοδήποτε δύο από αυτούς είναι ξένοι μεταξύ τους).

(ii) Έστω $\rho_1, \dots, \rho_m \in S_n$. Αναφερόμαστε τότε στην σύνθεση $\rho_1 \rho_2 \dots \rho_m$ ως ένα *γινόμενο μεταθέσεων*, συγκρίνεται με την Πρόταση 5.5.

Στην ειδική περίπτωση που $\rho_1, \dots, \rho_m$ είναι κύκλοι ξένοι μεταξύ τους στην S_n , αναφερόμαστε στην σύνθεση $\rho_1 \rho_2 \dots \rho_m$ ως ένα *γινόμενο κύκλων ξένων μεταξύ τους*. Στον ορισμό αυτό συμπεριλαμβάνουμε και την περίπτωση $m = 1$, όπου έχουμε δηλαδή ένα μόνο κύκλο.

Για παράδειγμα, στην S_{10} η σύνθεση $(2\ 5)(1\ 3\ 4)(6\ 7\ 8)(9)$ είναι ένα γινόμενο κύκλων ξένων μεταξύ τους.

Πρόταση 12.9. Αν $\pi \in S_n$, τότε π μπορεί να εκφραστεί ως γινόμενο κύκλων ξένων μεταξύ τους.

Απόδειξη. Θέτουμε $X = \{1, \dots, n\}$ και $R = \{(i, j) \in X \times X : j = \pi^k(i) \text{ για κάποιο } k \in \mathbb{Z}\}$. Τότε R είναι μια σχέση ισοδυναμίας στο X . Έστω τώρα $i \in X$. Παρατηρούμε ότι το σύνολο $S(i) = \{m \in \mathbb{N} : \pi^m(i) = i\}$ είναι μη-κενό, αφού τα στοιχεία $\pi^1(i), \pi^2(i), \pi^3(i), \dots$, δεν μπορούν να είναι όλα διαφορετικά μεταξύ τους. Έστω $k(i)$ το ελάχιστο στοιχείο του συνόλου $S(i)$. Έχουμε τότε ότι $\pi^{k(i)}(i) = i = \pi^{-k(i)}(i)$. Από το θεώρημα διαίρεσης, για $a \in \mathbb{Z}$ έχουμε $\pi^a = \pi^{qk(i)+r} (= (\pi^{k(i)})^q \pi^r)$ για κάποια $q, r \in \mathbb{Z}$ (τα οποία εξαρτώνται από το i), με $0 \leq r < k(i)$. Έπεται ότι $\pi^a(i) = \pi^r(i)$ όπου $0 \leq r < k(i)$. Επίσης, αν $\pi^r(i) = \pi^s(i)$ με $0 \leq r, s < k(i)$, τότε $r = s$ από την επιλογή του $k(i)$ ως ελαχίστου στοιχείου του $S(i)$. Συνεπώς, η κλάση ισοδυναμίας $\bar{i}$ του i ως προς την σχέση R είναι το υποσύνολο $\{i, \pi(i), \pi^2(i), \dots, \pi^{k(i)-1}(i)\}$ του X . Όμως $X = \bigcup_{i \in X} \bar{i}$. Θεωρώντας τώρα τις διακεκριμένες κλάσεις ισοδυναμίας συνάγουμε ότι π μπορεί να εκφραστεί ως γινόμενο κύκλων της μορφής $(i\ \pi(i)\ \pi^2(i)\ \dots\ \pi^{k(i)-1}(i))$, που είναι ξένοι μεταξύ τους αφού για $1 \leq u, v \leq n$, είτε $\bar{u} = \bar{v}$ είτε $\bar{u} \cap \bar{v} = \emptyset$. $\square$

Ορισμός. Μια παραγοντοποίηση της μετάθεσης $\pi \in S_n$ σε γινόμενο κύκλων ξένων μεταξύ τους καλείται *πλήρης* αν περιέχει ένα 1-κύκλο (i) για κάθε $i \in \{1, \dots, n\}$ που σταθεροποιείται από την π .

Αφού κύκλοι ξένοι μεταξύ τους αντιμετατίθενται, παίρνουμε το εξής πόρισμα.

Πόρισμα 12.10. Μια μετάθεση $\pi \in S_n$ έχει μοναδική πλήρη παραγοντοποίηση σε γινόμενο κύκλων ξένων μεταξύ τους, εκτός από την σειρά με την οποία εμφανίζονται οι παράγοντες.

Ορισμός. Έστω $n \in \mathbb{N}$. Αν οι θετικοί ακεραίοι $n_1, \dots, n_k$ ικανοποιούν $n_1 \geq n_2 \geq \dots \geq n_k (> 0)$ και $n = n_1 + \dots + n_k$, τότε λέμε ότι η πεπερασμένη ακολουθία $(n_1, n_2, \dots, n_k)$ είναι μια *διαμέριση* του n . Από το Πόρισμα 12.10 προκύπτει ότι σε κάθε $\pi \in S_n$ αντιστοιχεί μοναδική διαμέριση του n , που είναι γνωστή ως ο *τύπος κύκλων* της π .

Παράδειγμα 12.11. Έστω $\pi = (8\ 9)(1\ 2)(1\ 2\ 3\ 4)(4\ 5\ 6)(6\ 2)(7\ 9) \in S_{10}$. Μια πλήρης παραγοντοποίηση της π ως γινόμενο κύκλων ξένων μεταξύ τους δίνεται από την παράσταση $\pi = (1)(2)(3\ 4\ 5\ 6)(7\ 8\ 9)(10)$. Ο τύπος κύκλων της π είναι $(4, 3, 1, 1, 1)$.

Πρόταση 12.12. Έστω π ο k -κύκλος $(i_1\ i_2\ \dots\ i_k) \in S_n$ και έστω $\sigma \in S_n$. Τότε $\sigma\pi\sigma^{-1}$ είναι ο k -κύκλος $(\sigma(i_1)\ \sigma(i_2)\ \dots\ \sigma(i_k))$.

Απόδειξη. Αρκεί να δείξουμε ότι $\sigma\pi = (\sigma(i_1)\ \sigma(i_2)\ \dots\ \sigma(i_k))\sigma$. Θέτουμε $X = \{1, \dots, n\}$. Έστω $i \in X$. Υποθέτουμε πρώτα ότι $i \in X - \{i_1, \dots, i_k\}$. Τότε $\pi(i) = i$ και $\sigma(i) \notin \{\sigma(i_1), \dots, \sigma(i_k)\}$, αφού σ είναι αμφιμονοσήμαντη. Συνεπώς $\sigma\pi(i) = \sigma(i) = (\sigma(i_1)\ \sigma(i_2)\ \dots\ \sigma(i_k))\sigma(i)$. Έστω τώρα $i \in \{i_1, \dots, i_k\}$. Παρατηρούμε ότι $\sigma\pi(i_r)$ ισούται με $\sigma(i_{r+1})$ (αντίστοιχα, $\sigma(i_1)$) αν $1 \leq r < k$ (αντίστοιχα, αν $r = k$). Συγκρίνουμε τώρα με την εικόνα του i_r μέσω της $(\sigma(i_1)\ \sigma(i_2)\ \dots\ \sigma(i_k))\sigma$ στις περιπτώσεις $1 \leq r < k$ και $r = k$. $\square$

Πόρισμα 12.13. Έστω $\rho, \sigma \in S_n$. Τότε οι μεταθέσεις ρ και $\sigma\rho\sigma^{-1}$ έχουν τον ίδιο τύπο κύκλων.

Απόδειξη. Έστω $\rho, \sigma \in S_n$ και έστω $\rho = \alpha_1\alpha_2\ \dots\ \alpha_m$ μια πλήρης παραγοντοποίηση της ρ ως γινόμενο κύκλων ξένων μεταξύ τους, όπου α_i είναι ένας k_i -κύκλος για όλα τα i με $1 \leq i \leq m$. Όμως τότε $\sigma\rho\sigma^{-1} = \sigma\alpha_1\sigma^{-1}\sigma\alpha_2\sigma^{-1}\ \dots\ \sigma\alpha_m\sigma^{-1}$. Θέτοντας τώρα $\beta_i = \sigma\alpha_i\sigma^{-1}$ για $1 \leq i \leq m$, έχουμε ότι β_i είναι ένας k_i -κύκλος από την Πρόταση 12.12. Πάλι από την Πρόταση 12.12 οι κύκλοι β_i είναι ξένοι μεταξύ τους αφού σ είναι αμφιμονοσήμαντη. Συνάγουμε ότι $\beta_1\beta_2\ \dots\ \beta_m$ είναι μια πλήρης παραγοντοποίηση της $\sigma\rho\sigma^{-1}$ σε γινόμενο κύκλων ξένων μεταξύ τους και επομένως οι μεταθέσεις ρ και $\sigma\rho\sigma^{-1}$ έχουν τον ίδιο τύπο κύκλων. $\square$

Ορισμός. (Υπενθύμιση.) Ένας 2-κύκλος (δηλαδή ένας κύκλος της μορφής (a, b)) στην S_n όπου $n \geq 2$, ονομάζεται *αντιμετάθεση*.

Πρόταση 12.14. Έστω $n \geq 2$. Τότε μια μετάθεση $\pi \in S_n$ μπορεί να παρασταθεί ως γινόμενο αντιμεταθέσεων.

Απόδειξη. Για τυχαίο k -κύκλο $(a_1\ a_2\ \dots\ a_k)$, όπου $k > 1$, έχουμε

$$(a_1\ a_2\ \dots\ a_k) = (a_1\ a_k)\ \dots\ (a_1\ a_3)(a_1\ a_2).$$

Επίσης, για τον 1-κύκλο $(i) \in S_n$, όπου $1 \leq i \leq n$, έχουμε $(i) = (1\ 2)(1\ 2)$, αφού (i) ισούται με το μοναδιαίο στοιχείο της S_n . Το ζητούμενο είναι τώρα άμεση συνέπεια της Πρότασης 12.9. $\square$

Παράδειγμα 12.15. Η παράσταση μιας μετάθεσης ως γινόμενο αντιμεταθέσεων δεν είναι μοναδική. Για παράδειγμα στην S_3 έχουμε, $(1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(2\ 3) = (1\ 3)(2\ 3)(1\ 2)(1\ 3)$.

Ορισμός. Έστω $\pi \in S_n$. Θεωρούμε μια πλήρη παραγοντοποίηση της π σε γινόμενο κύκλων ξένων μεταξύ τους. Αν το πλήθος των κύκλων με άρτιο μήκος στην παραγοντοποίηση αυτή είναι άρτιος αριθμός (αντίστοιχα, περιττός αριθμός), τότε λέμε ότι η μετάθεση π είναι *άρτια* και ορίζουμε $\text{sgn}(\pi) = +1$ (αντίστοιχα, λέμε ότι η μετάθεση π είναι *περιττή* και ορίζουμε $\text{sgn}(\pi) = -1$).

Σημείωση 12.16. (i) Παρατηρούμε ότι ένας κύκλος άρτιου μήκους είναι μια περιττή μετάθεση, ενώ ένας κύκλος περιττού μήκους είναι μια άρτια μετάθεση. Πιο ειδικά, όλες οι αντιμεταθέσεις είναι περιττές μεταθέσεις. Έχουμε επίσης ότι το μοναδιαίο στοιχείο της S_n είναι μια άρτια μετάθεση.

(ii) Εξετάζουμε πως επηρεάζεται το $\text{sgn}(\pi)$, για μια μετάθεση $\pi \in S_n$, αν συνθέσουμε την μετάθεση αυτή με την αντιμετάθεση $\tau = (b\ c)$. Προφανώς αν κάποιος κύκλος περιέχει το σύμβολο b , μπορεί να γραφτεί στην μορφή $(b\ a_1\ a_2\ \dots\ a_k)$. Αν τώρα $b, c, a_1, \dots, a_k, d_1, \dots, d_l$ είναι διακεκριμένα στοιχεία του συνόλου $X = \{1, \dots, n\}$, εύκολα μπορούμε να ελέγξουμε ότι $(b\ c)(b\ a_1\ a_2\ \dots\ a_k)(c\ d_1\ d_2\ \dots\ d_l) = (b\ a_1\ a_2\ \dots\ a_k\ c\ d_1\ d_2\ \dots\ d_l)$ και $(b\ c)(b\ a_1\ a_2\ \dots\ a_k\ c\ d_1\ d_2\ \dots\ d_l) = (b\ a_1\ a_2\ \dots\ a_k)(c\ d_1\ d_2\ \dots\ d_l)$. Συμπεραίνουμε ότι $\text{sgn}(\tau\pi) = -\text{sgn}(\pi) (= \text{sgn}(\tau)\text{sgn}(\pi))$, ανεξάρτητα από το αν τα σύμβολα b, c εμφανίζονται σε διαφορετικούς κύκλους ή όχι σε μια πλήρη παραγοντοποίηση της π σε γινόμενο κύκλων ξένων μεταξύ τους. Επαγωγικά, βλέπουμε ότι συνθέτοντας την π με περιττό (αντίστοιχα, άρτιο) πλήθος αντιμεταθέσεων, αυτό έχει ως αποτέλεσμα το sgn να αλλάξει (αντίστοιχα, το sgn να μείνει αναλλοίωτο). Πιο ειδικά, θέτοντας $\pi = i_X$ στην πιο πάνω συζήτηση και παρεμβάλλοντας την Πρόταση 12.14, προκύπτει το εξής αποτέλεσμα.

Πρόταση 12.17. Έστω $n \geq 2$. Αν $\pi \in S_n$, το πλήθος των παραγόντων σε όλες τις παραστάσεις της π ως γινόμενο αντιμεταθέσεων είναι πάντοτε άρτιος ή πάντοτε περιττός αριθμός. Επιπλέον, αν $\pi = \tau_l \dots \tau_2 \tau_1$ (γινόμενο αντιμεταθέσεων), τότε $\text{sgn}(\pi) = (-1)^l$. Πιο ειδικά, $\text{sgn}(\rho\sigma) = \text{sgn}(\rho)\text{sgn}(\sigma)$ για όλες τις $\rho, \sigma \in S_n$.

Παράδειγμα 12.18. Στην S_5 έχουμε ότι $(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2) = (3\ 4)(1\ 3)(3\ 4)(1\ 3)(1\ 2)$ είναι μια περιττή μετάθεση και $(1\ 2\ 3\ 4\ 5) = (1\ 5)(1\ 4)(1\ 3)(1\ 2) = (1\ 5)(1\ 4)(1\ 3)(2\ 3)(1\ 3)(2\ 3)$ είναι μια άρτια μετάθεση.

12.3. Υποομάδες, κυκλική υποομάδα

Ορισμός. Ένα υποσύνολο H της ομάδας G ονομάζεται *υποομάδα* της G (συμβολισμός: $H \leq G$) αν ισχύουν

- (i) $1_G \in H$,
- (ii) $fh \in H$ οποτεδήποτε $f, h \in H$,
- (iii) $h^{-1} \in H$ οποτεδήποτε $h \in H$.

Παρατήρηση. Έστω G ομάδα και H υποσύνολο του συνόλου G . Παρατηρούμε τότε ότι $H \leq G$ αν, και μόνο αν, H αποτελεί η ίδια ομάδα ως προς την διμελή πράξη της G (κοιτάζτε την Άσκηση 12.8).

Πρόταση 12.19. Έστω H ένα μη-κενό υποσύνολο της ομάδας G . Τότε $H \leq G$ αν, και μόνο αν, $h_1 h_2^{-1} \in H$ οποτεδήποτε $h_1, h_2 \in H$.

Απόδειξη. Αν $H \leq G$, είναι προφανές ότι $h_1 h_2^{-1} \in H$ οποτεδήποτε $h_1, h_2 \in H$. Υποθέτουμε τώρα ότι H είναι ένα μη-κενό υποσύνολο της G με την ιδιότητα ότι $h_1 h_2^{-1} \in H$ οποτεδήποτε $h_1, h_2 \in H$. Αφού $H \neq \emptyset$, υπάρχει $h \in H$. Επομένως $1_G (= h h^{-1}) \in H$. Έστω τώρα f, g τυχαία στοιχεία του H . Τότε $g^{-1} (= 1_G g^{-1}) \in H$. Επιπλέον, $fg (= f(g^{-1})^{-1}) \in H$. $\square$

[**Προσθετικός συμβολισμός.** Το υποσύνολο B της ομάδας A είναι υποομάδα της (προσθετικής) ομάδας A αν ισχύουν

(i) $0_A \in B$, (ii) $a + b \in B$ οποτεδήποτε $a, b \in B$, (iii) $-a \in B$ οποτεδήποτε $a \in B$.]

Παραδείγματα 12.20. (i) Για κάθε ομάδα G , τα υποσύνολα G και $\{1_G\}$ αποτελούν υποομάδες της G .

(ii) Θέτουμε $SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) : \det A = 1\}$. Τότε $SL(n, \mathbb{R}) \leq GL(n, \mathbb{R})$.

Η $SL(n, \mathbb{R})$ καλείται ειδική γραμμική ομάδα βαθμού n επί του $\mathbb{R}$.

(iii) $P = \{f \in O(\mathbb{R}^2) : f = \text{rot}_\phi \text{ για κάποιο } \phi \text{ με } 0 \leq \phi < 2\pi\} \leq O(\mathbb{R}^2)$.

(iv) $(\mathbb{Q}, +) \leq (\mathbb{R}, +)$.

(v) $H = \{\alpha \in S_n : \alpha(1) = 1\} \leq S_n$.

(vi) $\{(1), (1\ 2\ 3), (1\ 3\ 2)\} \leq S_3$, $\{(1), (1\ 2)\} \leq S_3$.

(vii) Έστω $n \geq 2$. Θέτουμε $A_n = \{\pi \in S_n : \text{sgn}(\pi) = +1\} (= \{\pi \in S_n : \pi \text{ είναι άρτια}\})$. Τότε $A_n \leq S_n$. Η υποομάδα A_n της S_n καλείται η εναλλάσσουσα ομάδα σε n σύμβολα.

(viii) Αν $k, n \in \mathbb{N}$ με $k|n$, τότε $C_k \leq C_n$. [Ελέγξτε πρώτα ότι $C_k \subseteq C_n$ οποτεδήποτε $k|n$.]

(ix) Έστω G ομάδα και $g \in G$. Τότε το υποσύνολο $\{g^k : k \in \mathbb{Z}\}$ της G αποτελεί υποομάδα της G .

Αφήνουμε την απόδειξη της επόμενης πρότασης στις Ασκήσεις.

Πρόταση 12.21. Έστω $n \geq 5$. Τότε κάθε στοιχείο της A_n μπορεί να εκφραστεί ως γινόμενο 3-κύκλων.

Σημείωση 12.22. (i) Η τομή μιας (μη-κενής) οικογένειας υποομάδων μιας ομάδας G είναι επίσης υποομάδα της G . Δηλαδή αν $H_i \leq G$, $i \in I$ (σύνολο δεικτών), τότε $\bigcap_{i \in I} H_i \leq G$.

[Αν το σύνολο δεικτών I πιο πάνω είναι το κενό σύνολο, έχουμε $\bigcap_{i \in I} H_i = G$, όμως η περίπτωση αυτή δεν μας ενδιαφέρει στο βιβλίο αυτό.]

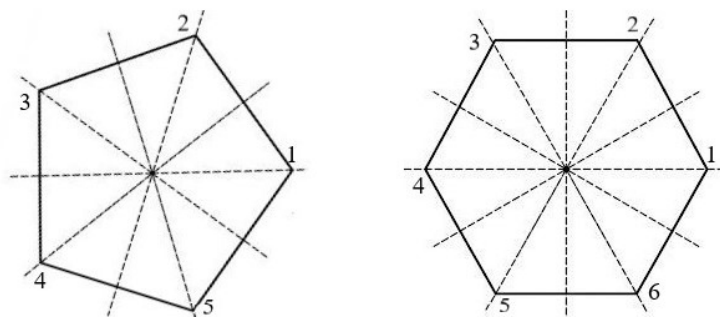
(ii) Η ένωση υποομάδων δεν είναι πάντα υποομάδα. Για παράδειγμα, στην S_3 έχουμε ότι $H_1 = \{(1), (1\ 2\ 3), (1\ 2\ 3)^2\}$ και $H_2 = \{(1), (1\ 2)\}$ είναι υποομάδες της S_3 , όμως $H_1 \cup H_2$ δεν είναι υποομάδα της S_3 .

Στο επόμενο παράδειγμα θα μελετήσουμε μια σημαντική υποομάδα της $O(\mathbb{R}^2)$.

Παράδειγμα 12.23. Έστω Δ_n ($n \geq 3$) ένα κανονικό n -γωνο τοποθετημένο στο xy -επίπεδο έτσι ώστε το κέντρο του να βρίσκεται στο σημείο $O(0,0)$ και μια από τις κορυφές του στο σημείο $Q(1,0)$. Από την Πρόταση 11.12, κάθε στοιχείο της $\Sigma(\Delta_n)$ επάγει μια μετάθεση του συνόλου $X = \{1, \dots, n\}$ των κορυφών του Δ_n και, επιπλέον, καθορίζεται πλήρως από τις εικόνες $f(1), \dots, f(n)$. Επιπλέον, $\Sigma(\Delta_n)$ αποτελεί ομάδα ως προς την σύνθεση συναρτήσεων από το Παράδειγμα 12.1(viii).

Θα δείξουμε ότι $|\Sigma(\Delta_n)| = 2n$. Θέτουμε $\Sigma_n = \{\text{rot}_{2\pi k/n} : 0 \leq k \leq n-1\} \cup \{\text{ref}_{2\pi k/n} : 0 \leq k \leq n-1\} \subseteq O(\mathbb{R}^2)$. Παρατηρούμε ότι $\Sigma_n \subseteq \Sigma(\Delta_n)$ και επομένως $|\Sigma(\Delta_n)| \geq 2n$ αφού το σύνολο Σ_n έχει ακριβώς $2n$ στοιχεία. Έστω τώρα $f \in \Sigma(\Delta_n)$. Τότε υπάρχουν n πιθανές εικόνες $f(1)$ για την κορυφή 1 του Δ_n αφού, όπως έχουμε δει πιο πάνω, f απεικονίζει κορυφή του Δ_n σε κορυφή του Δ_n . Αν η κορυφή 2 είναι ‘γειτονική’ προς την κορυφή 1 τότε και η κορυφή $f(2)$ θα είναι ‘γειτονική’ προς την κορυφή $f(1)$ αφού $d(1,2) = d(f(1), f(2))$. [Εξήγηση: Κάθε στοιχείο της $\Sigma(\Delta_n)$ απεικονίζει τρίγωνο σε ίσο τρίγωνο.] Συνεπώς, με δεδομένο ότι έχει καθοριστεί η εικόνα $f(1)$, υπάρχουν μόνο δύο πιθανές εικόνες $f(2)$ για την κορυφή 2 . Όμως, από την στιγμή που έχουν καθοριστεί οι εικόνες $f(1)$ και $f(2)$, οι ιδιότητες της f μας εξασφαλίζουν ότι καθορίζονται με μοναδικό τρόπο και οι υπόλοιπες εικόνες $f(3), \dots, f(n)$. Συνάγουμε ότι $|\Sigma(\Delta_n)| \leq 2n$ και επομένως $|\Sigma(\Delta_n)| = 2n$.

Ορισμός. Η ομάδα $\Sigma(\Delta_n)$ στο πιο πάνω παράδειγμα καλείται η *διεδρική ομάδα τάξης $2n$* και συμβολίζεται με D_{2n} . Έχουμε, δηλαδή, ότι $D_{2n} = \{\text{rot}_{2\pi k/n}, \text{ref}_{2\pi k/n} : 0 \leq k \leq n-1\}$.



Οι διεδρικές ομάδες D_{10} και D_{12}

Οι κυκλικές υποομάδες θα παίξουν σημαντικό ρόλο στην συνέχεια της συζήτησής μας.

Ορισμός 12.24. Έστω G ομάδα και $g \in G$. Συμβολίζουμε με $\langle g \rangle$ την τομή όλων των υποομάδων H της G με την ιδιότητα ότι $g \in H$. (Έχουμε τότε ότι $\langle g \rangle \leq G$ — κοιτάξτε την Σημείωση 12.22(i).) Η υποομάδα $\langle g \rangle$ της G καλείται η *κυκλική υποομάδα της G που παράγεται από το στοιχείο $g \in G$* .

Σημείωση 12.25. Παρεμβάλλοντας το Παράδειγμα 12.20(ix), είναι εύκολο να δείξουμε ότι $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$. Το υποσύνολο $\{g^k : k \in \mathbb{Z}\}$ αποτελεί υποομάδα της G η οποία περιέχει το στοιχείο $g \in G$. Έπεται, από τον ορισμό της $\langle g \rangle$, ότι $\langle g \rangle \subseteq \{g^k : k \in \mathbb{Z}\}$. Όμως οποιαδήποτε υποομάδα της G περιέχει το στοιχείο g υποχρεωτικά θα περιέχει και το σύνολο $\{g^k : k \in \mathbb{Z}\}$. Συνάγουμε ότι $\{g^k : k \in \mathbb{Z}\} \subseteq \langle g \rangle$ και επομένως $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$.

[**Προσθετικός συμβολισμός.** Έστω $(A, +)$ μια (προσθετική) ομάδα. Αν $a \in A$, έχουμε τότε ότι $\langle a \rangle = \{k \cdot a : k \in \mathbb{Z}\}$ όπου, για $k \in \mathbb{Z}$,

$$k \cdot a = \begin{cases} a + a + \dots + a \text{ (} k \text{ φορές)}, & \text{αν } k \in \mathbb{N}, \\ 0_A, & \text{αν } k = 0, \\ -a + -a + \dots + -a \text{ (} -k \text{ φορές)}, & \text{αν } -k \in \mathbb{N}. \end{cases}$$

Για παράδειγμα, στην $(\mathbb{Z}, +)$ έχουμε $\langle 1 \rangle = \{k \cdot 1 : k \in \mathbb{Z}\} = \mathbb{Z}$ (όπου $+$ είναι η συνηθισμένη πρόσθεση ακεραίων). Επίσης, $\langle 2 \rangle = \{k \cdot 2 : k \in \mathbb{Z}\} = \{r \in \mathbb{Z} : 2|r\} \neq \mathbb{Z}$. Ελέγξτε ότι στην ειδική αυτή περίπτωση το σύμβολο $k \cdot a$ (όπου $k, a \in \mathbb{Z}$) συμπίπτει με τον συνηθισμένο πολλαπλασιασμό ακεραίων.]

Έστω τώρα G ομάδα και $g \in G$. Θέτουμε $T = \{k \in \mathbb{N} : g^k = 1_G\}$. Υπάρχουν δύο περιπτώσεις για το σύνολο T :

(i) $T = \{k \in \mathbb{N} : g^k = 1_G\} = \emptyset$.

Τότε τα στοιχεία g^m , όπου $m \in \mathbb{Z}$, είναι όλα διακεκριμένα (αν $g^t = g^s$ όπου $s, t \in \mathbb{Z}$ με $s < t$, τότε προφανώς $t - s \in \mathbb{N}$ και $g^{t-s} = 1_G$). Έπεται ότι $\langle g \rangle$ είναι άπειρης τάξης σε αυτή την περίπτωση.

(ii) $T = \{k \in \mathbb{N} : g^k = 1_G\} \neq \emptyset$.

Έστω n το ελάχιστο στοιχείο του T (αρχή καλής διάταξης). Έστω επίσης $a \in \mathbb{Z}$. Σύμφωνα με το θεώρημα διαίρεσης, υπάρχουν $q, r \in \mathbb{Z}$ τέτοια ώστε $a = qn + r$ με $0 \leq r < n$. Έπεται ότι $g^a = g^{qn+r} = (g^n)^q g^r = (1_G)^q g^r = g^r$, όπου $0 \leq r < n$. Έχουμε επίσης ότι, αν $g^t = g^s$ με $0 \leq s < t < n$, τότε $g^{t-s} = 1_G$ με $1 \leq t - s \leq n - 1$, το οποίο προφανώς αντιφάσκει με την επιλογή του n . Επομένως, σ' αυτή την περίπτωση, $|\langle g \rangle| = n$ και $\langle g \rangle = \{1_G, g, g^2, \dots, g^{n-1}\}$.

Σημείωση. Προφανώς η περίπτωση (i) πιο πάνω δεν μπορεί να προκύψει σε περίπτωση που η ομάδα G είναι πεπερασμένης τάξης.

Παραδείγματα 12.26. (i) Στην $\mathbb{Z}_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ έχουμε ότι $\langle \bar{1} \rangle = \{\bar{1}\}$, $\langle \bar{3} \rangle = \{\bar{1}, \bar{3}\}$, $\langle \bar{5} \rangle = \{\bar{1}, \bar{5}\}$ και $\langle \bar{7} \rangle = \{\bar{1}, \bar{7}\}$.

(ii) Στην S_4 έχουμε ότι $\langle (1 \ 2 \ 3 \ 4) \rangle = \{(1 \ 2 \ 3 \ 4), (1 \ 3)(2 \ 4), (4 \ 3 \ 2 \ 1), (1)\} = \{\pi^1, \pi^2, \pi^3, \pi^0\}$, όπου $\pi = (1 \ 2 \ 3 \ 4)$. [Συγκρίνετε με την Άσκηση 12.7 και την συζήτηση πιο πάνω.]

Ορισμός. Έστω G ομάδα. Αν $G = \langle g \rangle$ για κάποιο $g \in G$, τότε λέμε ότι G είναι κυκλική και παράγεται από το στοιχείο $g \in G$.

Παραδείγματα 12.27. (i) $(\mathbb{Z}, +) = \langle 1 \rangle$ είναι κυκλική άπειρης τάξης.

(ii) $C_n = \langle \omega \rangle$, όπου $\omega = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right) \in \mathbb{C}$, είναι κυκλική τάξης n .

(iii) $(\mathbb{Z}_n, +) = \langle \bar{1} \rangle$ είναι κυκλική τάξης n .

(iv) S_3 δεν είναι κυκλική αφού $|\langle x \rangle| \in \{1, 2, 3\}$ για κάθε $x \in S_3$.

(v) $(\mathbb{Q}, +)$ δεν είναι κυκλική (άσκηση).

(vi) $(\mathbb{Z}_8^*, \cdot)$ δεν είναι κυκλική ενώ $(\mathbb{Z}_{10}^*, \cdot)$ είναι κυκλική.

(vii) $D_{2n} \cap \{f \in O(\mathbb{R}^2) : f = \text{rot}_\phi \text{ για κάποιο } \phi \text{ με } 0 \leq \phi < 2\pi\}$ είναι κυκλική τάξης n .

Ορισμός. Έστω G ομάδα και $g \in G$. Θέτουμε $T = \{k \in \mathbb{N} : g^k = 1_G\}$.

(i) Αν $T = \emptyset$, τότε λέμε ότι το στοιχείο g είναι άπειρης τάξης.

(ii) Αν $T \neq \emptyset$, τότε λέμε ότι το στοιχείο g έχει τάξη n , όπου n είναι το ελάχιστο στοιχείο του T (αρχή καλής διάταξης).

Συμβολισμός. Η τάξη του στοιχείου $g \in G$ συμβολίζεται με $o(g)$. [Εύκολα παρατηρούμε ότι η τάξη του στοιχείου $g \in G$ συμπίπτει με την τάξη της υποομάδας $\langle g \rangle$ της G .]

Παράδειγμα. (i) Έστω $\pi_1, \pi_2 \in S_6$ όπου $\pi_1 = (1\ 2\ 3)(4\ 5)$ και $\pi_2 = (3\ 4\ 5)(5\ 6)$. Τότε $o(\pi_1) = 6$ και $o(\pi_2) = 4$. (Παρατηρούμε ότι $\pi_2 = (3\ 4\ 5\ 6)$.)

(ii) Θέτουμε $\omega = \cos\left(\frac{2\pi}{6}\right) + i \sin\left(\frac{2\pi}{6}\right)$. Στην $C_6 = \langle \omega \rangle$, έχουμε ότι $o(\omega) = 6 = o(\omega^5)$, ενώ $o(\omega^2) = 3 = o(\omega^4)$ και $o(\omega^3) = 2$.

Παρατηρήσεις 12.28. (i) Το μοναδιαίο στοιχείο 1_G της ομάδας G είναι το μοναδικό στοιχείο της G που έχει τάξη 1. (Προφανώς $o(1_G) = 1$. Επίσης, αν $h \in G$ με $h^1 = 1_G$ τότε $h = 1_G$ αφού $h^1 = h$.)

(ii) Έστω G ομάδα και $g \in G$ όπου g έχει πεπερασμένη τάξη n . Αν $g^a = 1_G$ για κάποιο $a \in \mathbb{Z}$, τότε $n|a$. [Εξήγηση: Υπάρχουν $q, r \in \mathbb{Z}$ με $a = qn + r$ και $0 \leq r < n$. Όμως $1_G = g^a = g^{qn+r} = (g^n)^q g^r = g^r$ όπου $0 \leq r < n$ (έχουμε χρησιμοποιήσει ότι $o(g) = n$). Έπεται, από τον ορισμό της τάξης ενός στοιχείου, ότι $r = 0$ και επομένως $a = qn$.]

(iii) Αν η ομάδα G είναι κυκλική τότε προφανώς G είναι αβελιανή, όμως το αντίστροφο δεν ισχύει γενικά. Για παράδειγμα η ομάδα $C_2 \times C_2 = \{(1, 1), (1, -1), (-1, 1), (-1, -1)\}$ είναι αβελιανή (αφού είναι το εξωτερικό ευθύ γινόμενο αβελιανών ομάδων), δεν είναι όμως κυκλική αφού όλα τα στοιχεία της $C_2 \times C_2$ έχουν τάξη ≤ 2 .

Θεώρημα 12.29. Έστω G κυκλική ομάδα και $H \leq G$. Τότε H είναι επίσης κυκλική.

Απόδειξη. Υποθέτουμε ότι $H \leq G = \langle g \rangle$. Το αποτέλεσμα είναι προφανές αν $H = \{1_G\}$, επομένως υποθέτουμε ότι $H \neq \{1_G\}$. Τότε υπάρχει $t \in \mathbb{Z}$ τέτοιο ώστε $g^t \in H$ και $g^t \neq 1_G$ (προφανώς $t \neq 0$). Όμως $g^{-t} = (g^t)^{-1} \in H$ αφού H είναι υποομάδα. Άρα $S = \{k \in \mathbb{N} : g^k \in H\} \neq \emptyset$. Έστω $b \in \mathbb{N}$ το ελάχιστο στοιχείο του S (αρχή καλής διάταξης). Θα δείξουμε ότι $H = \langle g^b \rangle$. Έστω $h \in H$. Τότε $h = g^a$ για κάποιο $a \in \mathbb{Z}$ (αφού $h \in G = \langle g \rangle$). Σύμφωνα με το θεώρημα διαίρεσης υπάρχουν $q, r \in \mathbb{Z}$ τέτοια ώστε $a = qb + r$ και $0 \leq r < b$. Έχουμε τότε, $h = g^a = (g^b)^q g^r$, όπου $(g^b)^q \in \langle g^b \rangle \leq H$. Άρα $g^r = (g^b)^{-q} h \in H$. Όμως $0 \leq r < b$ όπου b είναι το ελάχιστο στοιχείο του S . Έπεται ότι $r = 0$ και επομένως $h = (g^b)^q \in \langle g^b \rangle$. Συνάγουμε ότι $H \subseteq \langle g^b \rangle$ (άρα $H = \langle g^b \rangle$ αφού προφανώς $\langle g^b \rangle \subseteq H$). □

Παράδειγμα 12.30. Θα βρούμε όλες τις υποομάδες της $(\mathbb{Z}, +)$. Η ομάδα αυτή είναι κυκλική (Παράδειγμα 12.27(ii)), επομένως όλες οι υποομάδες της είναι κυκλικές από το

Θεώρημα 12.29. Έπεται ότι H είναι υποομάδα της $(\mathbb{Z}, +)$ αν, και μόνο αν, $H = \{k \cdot m : k \in \mathbb{Z}\} (= \langle m \rangle)$ για κάποιο $m \in \mathbb{Z}$. [Στην περίπτωση που εξετάζουμε, η ‘έκφραση’ $k \cdot m$ είναι απλά το γινόμενο των δύο ακεραίων k και m ως προς τον συνηθισμένο πολλαπλασιασμό στο $\mathbb{Z}$.] Τέλος, για $m_1, m_2 \in \mathbb{Z}$, έχουμε ότι $\langle m_1 \rangle = \langle m_2 \rangle$ αν, και μόνο αν, $m_1 | m_2$ και $m_2 | m_1$, και το τελευταίο ισχύει αν, και μόνο αν, $m_1 = m_2$ ή $m_1 = -m_2$.

Πρόταση 12.31. Έστω G μια πεπερασμένη κυκλική ομάδα τάξης n . Έστω επίσης $d \in \mathbb{N}$ με $d | n$. Η ομάδα G περιέχει ακριβώς μια υποομάδα G_d τάξης d . Επιπλέον, $G_d = \{x \in G : x^d = 1_G\}$.

Απόδειξη. Υπάρχει $g \in G$ με $G = \langle g \rangle$. Τότε $o(g) = n$. Θεωρούμε το στοιχείο $g^{n/d}$ της G . Προφανώς $o(g^{n/d}) = d$ και επομένως $|\langle g^{n/d} \rangle| = d$. Αν τώρα H είναι τυχαία υποομάδα της G τάξης d , τότε H είναι κυκλική από το Θεώρημα 12.29, και επομένως $H = \langle y \rangle$ για κάποιο $y \in G$. Όμως $y = g^r$ για κάποιο $r \in \{0, 1, \dots, n-1\}$ και, αφού $o(y) = d$, έχουμε ότι $g^{rd} = 1_G$. Από την Παρατήρηση 12.28(ii) έχουμε ότι $n | rd$, άρα $rd = kn$ για κάποιο $k \in \mathbb{N} \cup \{0\}$. Έπεται ότι $r = k(\frac{n}{d})$, άρα $(n/d) | r$. Συμπεραίνουμε ότι $y = (g^{n/d})^k$. Συνεπώς $H \leq \langle g^{n/d} \rangle$ και αφού $|H| = |\langle g^{n/d} \rangle| = d$ προκύπτει ότι $H = \langle g^{n/d} \rangle (= G_d)$. Ο πιο πάνω συλλογισμός δείχνει ότι $x \in G$ ικανοποιεί $x^d = 1_G$ αν, και μόνο αν, x είναι δύναμη του $g^{n/d}$. Συνάγουμε ότι $G_d = \{x \in G : x^d = 1_G\}$. $\square$

Πρόταση 12.32. Έστω G ομάδα και $g \in G$ όπου g είναι πεπερασμένης τάξης n . Έστω επίσης $b \in \mathbb{Z}$. Τότε $\langle g^b \rangle = \langle g \rangle$ αν, και μόνο αν, $\mu\kappa\delta(b, n) = 1$.

Απόδειξη. Έστω G ομάδα και $g \in G$ με $o(g) = n$.

Υποθέτουμε πρώτα ότι $\langle g^b \rangle = \langle g \rangle$. Έχουμε τότε ότι $g \in \langle g^b \rangle$, συνεπώς $g^1 = g = (g^b)^t$ για κάποιο $t \in \mathbb{Z}$. Έπεται ότι $g^{1-bt} = 1_G$, άρα $n | (1 - bt)$ από την Παρατήρηση 12.28(ii). Συνάγουμε ότι $1 - bt = sn$ για κάποιο $s \in \mathbb{Z}$, και επομένως $\mu\kappa\delta(b, n) = 1$.

Έστω τώρα ότι $\mu\kappa\delta(b, n) = 1$. Τότε υπάρχουν $x, y \in \mathbb{Z}$ τέτοια ώστε $bx + ny = 1$. Συνεπώς $g = g^1 = (g^b)^x (g^n)^y = (g^b)^x$, αφού $g^n = 1_G$. Συνάγουμε ότι $\langle g \rangle \subseteq \langle g^b \rangle$. Προφανώς ισχύει επίσης ότι $\langle g^b \rangle \subseteq \langle g \rangle$. $\square$

Παράδειγμα 12.33. (i) Θεωρούμε την ομάδα $C_8 = \langle \omega \rangle$, όπου $\omega = \cos(\frac{2\pi}{8}) + i \sin(\frac{2\pi}{8}) \in \mathbb{C}$. Παρατηρούμε ότι $C_8 = \langle \omega^3 \rangle = \langle \omega^5 \rangle = \langle \omega^7 \rangle$, όμως $\langle \omega^2 \rangle = \{1, \omega^2, \omega^4, \omega^6\} \neq C_8$. Συγκρίνετε με την Άσκηση 11.8 — ποιες είναι οι πρωταρχικές $8^{\text{ες}}$ ρίζες της μονάδας στο $\mathbb{C}$;

(ii) Έστω $G = (\mathbb{Z}_5^*, \cdot)$. Τότε $G = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. Έχουμε ότι $G = \langle \bar{2} \rangle = \langle \bar{3} \rangle$ και επομένως G είναι κυκλική με το $\bar{2}$ να είναι ένα από τα στοιχεία που παράγουν την G . Όμως, στην $\mathbb{Z}_5^*$, έχουμε $\langle \bar{1} \rangle = \{\bar{1}\}$ και $\langle \bar{4} \rangle = \{\bar{1}, \bar{4}\}$. Ελέγξτε ότι $\bar{4} = (\bar{2})^2$ και $\bar{1} = (\bar{2})^4$, όπου $o(\bar{2}) = 4$, και συγκρίνετε με τους $\mu\kappa\delta(2, 4)$ και $\mu\kappa\delta(4, 4)$.

(iii) Έστω $G = (\mathbb{Z}_4, +)$. Τότε $G = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$. Έχουμε ότι $G = \langle \bar{1} \rangle = \langle \bar{3} \rangle$ όμως $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}\} \neq G$.

Σημειώσεις και Σχόλια

Η θεωρία ομάδων αποτελεί ενοποίηση και γενίκευση διαφόρων εννοιών που ήταν κοινές σε διάφορους σημαντικούς τομείς των μαθηματικών που μελετούνταν ουσιαστικά ταυτόχρονα. Οι τρεις κύριοι τομείς που οδήγησαν στην θεωρία ομάδων ήταν η γεωμετρία στις αρχές του 19ου αιώνα, η θεωρία αριθμών στα τέλη του 18ου αιώνα και η θεωρία των αλγεβρικών εξισώσεων στα τέλη του 18ου αιώνα. Η τελευταία ήταν αυτή που οδήγησε και στην μελέτη των μεταθέσεων.

(1) Στις αρχές του 19ου αιώνα η γεωμετρία άρχισε να χάνει τον ‘μετρικό’ της χαρακτήρα με την μελέτη της προβολικής και της μη-ευκλείδειας γεωμετρίας. Επίσης, δημιουργήθηκε η τάση για μελέτη της γεωμετρίας πιο αφαιρετικά σε n διαστάσεις. Την μη-ευκλείδεια γεωμετρία μελέτησαν, μεταξύ άλλων, οι Lambert, Gauss, Lobachevsky και Janos Bolyai. Ο Möbius το 1827, πολύ πριν καθιερωθεί ο ‘ορισμός’ της ομάδας, άρχισε να ταξινομεί τις γεωμετρίες χρησιμοποιώντας το γεγονός ότι μια συγκεκριμένη γεωμετρία μελετά ιδιότητες που παραμένουν αναλλοίωτες κάτω από μια συγκεκριμένη ομάδα. Ο Steiner το 1832 μελέτησε έννοιες της συνθετικής γεωμετρίας (γεωμετρίας χωρίς την χρήση συντεταγμένων) που τελικά θα γίνονταν μέρος της μελέτης των ομάδων μετασχηματισμών.

(2) Το 1761, ο Euler μελέτησε την αριθμητική modulo n . Στην πραγματικότητα το έργο του Euler αποτελεί ένα παράδειγμα μελέτης της διάσπασης μιας αβελιανής ομάδας σε σύμπλοκα μιας υποομάδας της. Επίσης, ο Euler απέδειξε στην ειδική αυτή περίπτωση ότι η τάξη μιας υποομάδας είναι διαιρετής της τάξης της (πεπερασμένης) ομάδας. Ο Gauss το 1801 ανέπτυξε το έργο του Euler παραπέρα και είχε σημαντική συνεισφορά στην αριθμητική modulo n , που ισοδυναμεί με θεωρία των αβελιανών ομάδων.

(3) Οι μεταθέσεις μελετήθηκαν για πρώτη φορά από τον Lagrange στο έργο του το 1770 για την θεωρία των αλγεβρικών εξισώσεων. Ο κύριος στόχος του ήταν να εξηγήσει γιατί οι εξισώσεις 3^{ου} και 4^{ου} βαθμού μπορούν να λυθούν αλγεβρικά. Αν και το έργο του περιέχει τα πρώτα στοιχεία της θεωρίας των ομάδων μεταθέσεων, δεν υπάρχει σε αυτό η έννοια της σύνθεσης μεταθέσεων. Η σύνθεση των μεταθέσεων εμφανίζεται στο έργο των Ruffini και Abbatì γύρω στο 1800. Το 1815, ο Cauchy καθιέρωσε τον λογισμό των μεταθέσεων, και αυτή η οπτική χρησιμοποιήθηκε από τον Abel στην απόδειξή του (1824) για την μη-επιλυσιμότητα της εξίσωσης 5^{ου} βαθμού. Θα μπορούσε κάποιος να ισχυριστεί ότι το 1830 ο Galois, μόλις 19 ετών τότε, ουσιαστικά ‘ίδρυσε’ την θεωρία ομάδων, επισυνάπτοντας σε κάθε πολυώνυμο μια ομάδα μεταθέσεων των ριζών του και αποδεικνύοντας έτσι ότι υπάρχει τύπος για τις ρίζες αν και μόνο αν η ομάδα αυτή έχει μια συγκεκριμένη ιδιότητα. Μελετώντας την δομή της ομάδας μεταθέσεων, πολύ πριν καν καθιερωθεί ο ‘ορισμός’ της ομάδας, ο Galois κατάφερε να επιλύσει ένα από τα πιο σημαντικά προβλήματα της εποχής του.

Ασκήσεις

12.1 Για $a, b \in \mathbb{Q}$ θέτουμε $a * b = (a + b) + (\frac{7}{8})$, όπου $+$ είναι η συνηθισμένη πρόσθεση ρητών. Εξετάστε κατά πόσον το ζεύγος $(\mathbb{Q}, *)$ αποτελεί ομάδα.

12.2 Συμπληρώστε τους συλλογισμούς στο Παράδειγμα 12.1.

12.3 Έστω G ομάδα. Αν $g^2 = 1_G$ για όλα τα $g \in G$, δείξτε ότι G είναι αβελιανή.

12.4 Έστω G ομάδα και $h \in G$. Δείξτε ότι $G = \{hg : g \in G\}$.

12.5 (i) Έστω $\mathbf{a} \in \mathbb{R}^2$ ένα σταθερό διάνυσμα. Θέτουμε $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2: \mathbf{x} \mapsto \mathbf{x} + \mathbf{a}$, ($\mathbf{x} \in \mathbb{R}^2$). Δείξτε ότι η συνάρτηση f (μια συνάρτηση αυτής της μορφής καλείται *μεταφορά*) είναι μια κίνηση.

(ii) Αν $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ είναι μια κίνηση, δείξτε ότι $T = T_1 \circ T_2$ όπου T_1 είναι μια μεταφορά και $T_2 \in O(\mathbb{R}^2)$.

(iii) Δείξτε ότι το σύνολο $K(\mathbb{R}^2)$ όλων των κινήσεων από τον $\mathbb{R}^2$ στον $\mathbb{R}^2$ αποτελεί ομάδα ως προς την σύνθεση συναρτήσεων.

12.6 Έστω p περιττός πρώτος.

(i) Έστω $a \in \mathbb{Z}$. Δείξτε ότι $a^2 \equiv 1 \pmod{p}$ αν, και μόνο αν, $a \equiv \pm 1 \pmod{p}$.

(ii) (Θεώρημα Wilson) Εξετάζοντας το γινόμενο των στοιχείων της $\mathbb{Z}_p^*$, δείξτε ότι $(p-1)! \equiv -1 \pmod{p}$.

12.7 Θέτουμε $X = \{1, \dots, n\}$. Αν $\rho = (i_1 \ i_2 \ \dots \ i_k) \in S_n$ είναι ένας k -κύκλος, δείξτε ότι το σύνολο $S = \{m \in \mathbb{N} : \rho^m = i_X\}$ είναι μη-κενό και βρείτε το ελάχιστο στοιχείο του.

12.8 Έστω G ομάδα και H υποσύνολο του συνόλου G . Αν H αποτελεί ομάδα ως προς την ίδια διμελή πράξη της G , δείξτε ότι $1_H = 1_G$ και ότι $(f^{-1})_H = (f^{-1})_G$ για όλα τα $f \in H$.

12.9 Έστω $n \geq 5$. Δείξτε ότι κάθε στοιχείο της A_n μπορεί να εκφραστεί ως γινόμενο 3-κύκλων.

12.10 Έστω H ένα μη-κενό υποσύνολο της πεπερασμένης ομάδας G . Δείξτε ότι $H \leq G$ αν, και μόνο αν, $h_1 h_2 \in H$ οποτεδήποτε $h_1, h_2 \in H$.

12.11 (a) Συμπληρώστε τους συλλογισμούς στα Παραδείγματα 12.20.

(b) Θέτουμε $T = \left\{ \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \in M_2(\mathbb{R}) : ab \neq 0 \right\}$. Εξετάστε κατά πόσον $T \leq GL(2, \mathbb{R})$.

(c) Θέτουμε $O(n, \mathbb{R}) = \{A \in M_n(\mathbb{R}) : A \text{ είναι ορθογώνιος}\}$. Εξετάστε κατά πόσον $O(n, \mathbb{R}) \leq GL(n, \mathbb{R})$.

12.12 Αν η ομάδα G είναι πεπερασμένης τάξης και έχει τάξη άρτιο αριθμό, δείξτε ότι G περιέχει τουλάχιστον ένα στοιχείο τάξης 2.

12.13 (i) Δείξτε ότι η ομάδα $(\mathbb{Q}, +)$ δεν είναι κυκλική.

(ii) Εξετάστε κατά πόσον η ομάδα $(\mathbb{Z}_7^*, \cdot)$ είναι κυκλική.

(iii) Βρείτε τις υποομάδες $\langle \omega^3 \rangle$ και $\langle \omega^5 \rangle$ της C_{12} , όπου $\omega = \cos\left(\frac{2\pi}{12}\right) + i \sin\left(\frac{2\pi}{12}\right) \in \mathbb{C}$.

12.14 Έστω G ομάδα και $a, b \in G$ όπου a, b είναι πεπερασμένης τάξης με $o(a) = m$ και $o(b) = n$. Υποθέτουμε επιπλέον ότι $ab = ba$ και ότι $\langle a \rangle \cap \langle b \rangle = \{1_G\}$. Δείξτε ότι $o(ab) = \text{εκπ}(m, n)$.

12.15 Έστω $G = \langle g \rangle$ κυκλική ομάδα πεπερασμένης τάξης n , και έστω $m \in \mathbb{Z}$. Θέτουμε $h = g^m$. Δείξτε ότι $|\langle h \rangle| = n/d$ όπου $d = \text{μκδ}(m, n)$.

12.16 Έστω $\rho, \sigma \in S_9$ όπου $\rho = (1 \ 2)(3 \ 4 \ 5 \ 6 \ 7 \ 8)(1 \ 3 \ 2)$ και $\sigma = (1 \ 9)(1 \ 5)(4 \ 5 \ 6 \ 7)(1 \ 2 \ 3)(1 \ 2 \ 3 \ 4)$.

(i) Για κάθε ένα από τα στοιχεία $\rho, \sigma, \rho\sigma$ της S_9 βρείτε μια πλήρη παραγοντοποίηση σε γινόμενο κύκλων ξένων μεταξύ τους και τον τύπο κύκλων του στοιχείου.

(ii) Να εκφράσετε τις ρ, σ ως γινόμενα αντιμεταθέσεων και να βρείτε τα $\text{sgn}(\rho)$ και $\text{sgn}(\sigma)$. Να υπολογίσετε επίσης τις τάξεις $o(\rho)$, $o(\sigma)$, $o(\rho\sigma)$ και $o(\sigma\rho\sigma^{-1})$.

(iii) Βρείτε το $\tau\sigma\tau^{-1}$ όπου $\tau = (2 \ 4 \ 6 \ 3)$.

(iv) Εξετάστε κατά πόσον υπάρχουν $\pi, \gamma \in S_9$ τέτοιες ώστε $\pi\sigma\pi^{-1} = (1 \ 2 \ 3)(4 \ 5 \ 6)$ και $\gamma\rho\gamma^{-1} = (1 \ 2)(3 \ 4 \ 5 \ 6 \ 7 \ 8)$.

12.17 Να υπολογίσετε την τάξη $o(g)$ για κάθε $g \in C_3 \times \mathbb{Z}_6^*$.

12.18 Βρείτε την τάξη της ομάδας $GL(2, \mathbb{Z}_p)$ όπου p πρώτος.

12.19 Το παιχνίδι με τα 15 συρόμενα τετράγωνα παίζεται σε ένα τετραγωνικό πλαίσιο 4×4 που περιλαμβάνει δεκαπέντε αριθμημένα τετράγωνα και μία κενή θέση. Ο παίκτης μπορεί να μετακινεί μόνο τα τετράγωνα που βρίσκονται δίπλα στην κενή θέση, σύροντάς τα ώστε να γλιστρούν στην θέση αυτή. Επιτρέπονται μόνο οριζόντιες ή κατακόρυφες κινήσεις — τα τετράγωνα δεν σηκώνονται ούτε αφαιρούνται από το πλαίσιο. Στόχος είναι η τελική διάταξη των αριθμών στην σωστή σειρά. Αποδείξτε ότι είναι αδύνατο να πραγματοποιηθεί μετάβαση από την αρχική διάταξη που φαίνεται στα αριστερά στην διάταξη που φαίνεται στα δεξιά, χρησιμοποιώντας μόνο τις επιτρεπτές κινήσεις.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

15	14	13	12
11	10	9	8
7	6	5	4
3	2	1	

13. Γεννήτριες και σχέσεις, ομομορφισμοί ομάδων

13.1. Γεννήτριες και σχέσεις

Δίνουμε τώρα μια επέκταση του Ορισμού 12.24.

Ορισμός. (i) Έστω S τυχαίο υποσύνολο της ομάδας G . Συμβολίζουμε με $\langle S \rangle$ την τομή όλων των υποομάδων της G οι οποίες περιέχουν το υποσύνολο S , δηλαδή $\langle S \rangle = \bigcap \{H : H \leq G \text{ και } S \subseteq H\}$. Είναι εύκολο να επαληθεύσουμε ότι αν $S \subseteq G$, τότε $\langle S \rangle$ είναι μια υποομάδα της G που περιέχει το υποσύνολο S , και καλείται η υποομάδα της G που παράγεται από το υποσύνολο S της G . Σε τέτοια περίπτωση λέμε επίσης ότι το υποσύνολο S της G αποτελεί ένα σύστημα γεννητριών της υποομάδας $\langle S \rangle$ της G .

(ii) Αν υπάρχει πεπερασμένο υποσύνολο T της ομάδας G με $G = \langle T \rangle$, τότε λέμε ότι G είναι πεπερασμένα παραγόμενη.

Παρατηρήσεις. (i) Αν $H \leq G$ και $S \subseteq H$, τότε $\langle S \rangle \subseteq H$. Προφανώς $\langle \emptyset \rangle = \{1_G\}$.

(ii) Στην ειδική περίπτωση $S = \{g\}$ για κάποιο $g \in G$, έχουμε $\langle \{g\} \rangle = \langle g \rangle = \{g^k : k \in \mathbb{Z}\}$.

(iii) Για κάθε $n \geq 2$ θέτουμε $T_2(n) = \{\pi \in S_n : \pi \text{ είναι ένας 2-κύκλος}\}$ και $T_3(n) = \{\pi \in S_n : \pi \text{ είναι ένας 3-κύκλος}\}$. Η Πρόταση 12.14 μας λέει τότε ότι $S_n = \langle T_2(n) \rangle$ για $n \geq 2$, ενώ η Πρόταση 12.21 μας λέει ότι $A_n = \langle T_3(n) \rangle$ για $n \geq 5$.

Πρόταση 13.1. Έστω S υποσύνολο της ομάδας G με $S \neq \emptyset$. Η υποομάδα $\langle S \rangle$ της G αποτελείται από όλα τα στοιχεία της μορφής $g = h_1^{\varepsilon_1} h_2^{\varepsilon_2} \dots h_k^{\varepsilon_k}$ όπου $h_i \in S$ ($i = 1, \dots, k$), $\varepsilon_i \in \{-1, 1\}$ και k τυχαίος θετικός ακέραιος.

Απόδειξη. Θέτουμε $H = \{h_1^{\varepsilon_1} h_2^{\varepsilon_2} \dots h_k^{\varepsilon_k} : h_i \in S, \varepsilon_i = \pm 1, k \in \mathbb{N}\}$. Θα δείξουμε πρώτα ότι $H \leq G$. Έστω $h \in S$. Θέτουμε $k = 2$, $h_1 = h = h_2$, $\varepsilon_1 = +1$, $\varepsilon_2 = -1$. Τότε $h_1^1 h_2^{-1} = hh^{-1} = 1_G$ και επομένως $1_G \in H$. (Με την ίδια ευκολία μπορούν ναδειχθούν και τα υπόλοιπα αξιώματα που πρέπει να ικανοποιούνται για να έχουμε $H \leq G$.) Προφανώς $S \subseteq H$, άρα $\langle S \rangle \subseteq H$. Όμως κάθε υποομάδα της G που περιέχει το υποσύνολο S πρέπει να περιέχει και την H , άρα $H \subseteq \langle S \rangle$. Συνάγουμε ότι $H = \langle S \rangle$. $\square$

Σημείωση 13.2. Έστω G ομάδα και $a, b \in G$. Θέτουμε $S = \{a, b\} (\subseteq G)$. Σύμφωνα με την Πρόταση 13.1, τα στοιχεία της υποομάδας $H = \langle S \rangle$ της G είναι ακριβώς τα στοιχεία της G που μπορούν να εκφραστούν ως γινόμενα δυνάμεων του a και του b , δηλαδή όλα τα στοιχεία της G που έχουν μορφή $a^{i_1} b^{j_1} a^{i_2} b^{j_2} \dots a^{i_n} b^{j_n}$ για κάποιο $n \in \mathbb{N}$, όπου $i_k, j_k \in \mathbb{Z}$ για

$1 \leq k \leq n$. [Για παράδειγμα $1_G = a^1 b^0 a^{-1} b^0$, $a = a^1 b^0$, $b = a^0 b^1$.] Σε τέτοια περίπτωση λέμε ότι H είναι η υποομάδα της G που παράγεται από τα στοιχεία a και b της G , και γράφουμε $H = \langle a, b \rangle$.

Παράδειγμα 13.3. (i) Έστω $\alpha, \beta \in S_4$ όπου $\alpha = (1\ 2\ 3\ 4)$ και $\beta = (2\ 4)$. Θα βρούμε την τάξη και τα στοιχεία της υποομάδας $\langle \alpha, \beta \rangle$ της S_4 . Παρατηρούμε ότι $o(\alpha) = 4$ και $o(\beta) = 2$. Έχουμε επίσης ότι $\alpha\beta = (1\ 2\ 3\ 4)(2\ 4) = (1\ 2)(3\ 4) = (2\ 4)(4\ 3\ 2\ 1) = \beta\alpha^{-1}$. Χρησιμοποιώντας πρώτα την σχέση $\alpha\beta = \beta\alpha^{-1}$ μπορούμε να δείξουμε ότι κάθε στοιχείο της $\langle \alpha, \beta \rangle$ είναι της μορφής $\alpha^i \beta^j$ για κάποια $i, j \in \mathbb{Z}$: Από την σχέση $\alpha\beta = \beta\alpha^{-1}$ προκύπτει, χρησιμοποιώντας επαγωγή στο i , ότι $\alpha^i \beta = \beta\alpha^{-i}$ για κάθε $i \in \mathbb{N}$. [Εξήγηση: Αν $\alpha^i \beta = \beta\alpha^{-i}$ για κάποιο $i \in \mathbb{N}$, τότε $\alpha^{i+1}\beta = \alpha\alpha^i\beta = \alpha(\beta\alpha^{-i}) = (\alpha\beta)\alpha^{-i} = \beta\alpha^{-1}\alpha^{-i} = \beta\alpha^{-(i+1)}$.] Έπεται επίσης ότι $\alpha^{-i}\beta = \beta\alpha^i$ για κάθε $i \in \mathbb{N}$.

Στην συνέχεια, χρησιμοποιώντας τις σχέσεις $\alpha^4 = (1)$ και $\beta^2 = (1)$ μπορούμε εύκολα να δείξουμε ότι κάθε στοιχείο της S_4 είναι της μορφής $\alpha^i \beta^j$ όπου $i, j \in \mathbb{Z}$ με $0 \leq i \leq 3$ και $0 \leq j \leq 1$. Πολλαπλασιάζοντας, βλέπουμε ότι τα στοιχεία $(1), \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta$ είναι διακεκριμένα, άρα $|\langle \alpha, \beta \rangle| = 8$.

(ii) Έστω $n \in \mathbb{N}$ με $n \geq 3$. Θέτουμε $G = D_{2n} = \{\text{rot}_{2\pi k/n}, \text{ref}_{2\pi k/n} : 0 \leq k \leq n-1\}$. Έχουμε τότε ότι $|G| = 2n$. Θέτουμε επίσης $a = \text{rot}_{2\pi/n}$, $b = \text{ref}_0$ (τότε $\{a, b\} \subseteq G$). Θα βρούμε τα στοιχεία της υποομάδας $\langle a, b \rangle$ της G και θα δείξουμε ότι $G = \langle a, b \rangle$. Παρατηρούμε πρώτα ότι $a^n = 1_G = b^2$. Επιπλέον, $ab = \text{rot}_{2\pi/n}\text{ref}_0 = \text{ref}_{2\pi/n} = \text{ref}_0\text{rot}_{-2\pi/n} = ba^{-1}$. Από την σχέση $ab = ba^{-1}$ προκύπτει, χρησιμοποιώντας επαγωγή στο i , ότι $a^i b = ba^{-i}$ για κάθε $i \in \mathbb{N}$. Από την σχέση $a^i b = ba^{-i}$ προκύπτει επίσης εύκολα ότι $a^{-i} b = ba^i$ για κάθε $i \in \mathbb{N}$. Συνεπώς, κάθε στοιχείο της υποομάδας $\langle a, b \rangle$ της G μπορεί να εκφραστεί στην μορφή $a^i b^j$ για κάποια $i, j \in \mathbb{Z}$. Χρησιμοποιώντας τώρα τις σχέσεις $a^n = 1_G$ και $b^2 = 1_G$, συμπεραίνουμε ότι κάθε στοιχείο της $\langle a, b \rangle$ είναι της μορφής $a^i b^j$ όπου $i, j \in \mathbb{Z}$ με $0 \leq i \leq n-1$ και $0 \leq j \leq 1$. Για να δείξουμε ότι $G = \langle a, b \rangle$, αρκεί να δείξουμε ότι τα $2n$ στοιχεία $a^i b^j$ ($0 \leq i \leq n-1$, $0 \leq j \leq 1$) είναι διακεκριμένα. Θέτουμε $S_1 = \{a^i : 0 \leq i \leq n-1\}$ και $S_2 = \{a^i b : 0 \leq i \leq n-1\}$. Προφανώς $|S_1| = n$, αφού $o(a) = n$. Η συνάρτηση $\phi: S_1 \rightarrow S_2 : x \mapsto xb$ ($x \in S_1$) είναι αμφιμονοσήμαντη, άρα έχουμε επίσης ότι $|S_2| = n$. Απομένει να δείξουμε ότι $S_1 \cap S_2 = \emptyset$. Για να το δείξουμε αυτό υποθέτουμε ότι $a^i = ba^j$ για κάποια i, j με $0 \leq i, j \leq n-1$, και επομένως $b = a^{i-j}$, που είναι άτοπο. [Εξήγηση: Έχουμε ότι b είναι μια ανάκλαση, άρα $\det(T^{-1}(b)) = -1$, ενώ a^{i-j} είναι μια περιστροφή, άρα $\det(T^{-1}(a^{i-j})) = 1$, με την συνάρτηση $T: \text{GL}(2, \mathbb{R}) \rightarrow I_{\mathbb{R}}(\mathbb{R}^2)$ όπως έχει ορισθεί στην Σημείωση 11.1.] Τέλος, είναι εύκολο να δούμε ότι οι τρεις σχέσεις $a^n = 1_G$, $b^2 = 1_G$ και $ab = ba^{-1}$ καθορίζουν πλήρως τον πίνακα πολλαπλασιασμού της G . [Εξήγηση: Το γινόμενο $(a^i)(a^j)$ (αντίστοιχα, $(a^i)(a^j b)$) ισούται με a^{i+j} (αντίστοιχα, $a^{i+j} b$), αντικαθιστούμε a^{i+j} με a^{i+j-n} αν $(i+j) \geq n$. Επιπλέον, χρησιμοποιώντας την σχέση $ba^j = a^{-j}b$ που έχουμε βρει πιο πάνω, προκύπτει ότι το γινόμενο $(a^i b)(a^j)$ (αντίστοιχα, $(a^i b)(a^j b)$) ισούται με $a^{i-j} b$ (αντίστοιχα, a^{i-j}), αντικαθιστούμε $a^{i-j} b$ με a^{i-j+n} αν $i < j$.]

Για παράδειγμα, $(ab)(a^2 b) = a(ba^2)b = a(a^{-2}b)b = (aa^{-2})(bb) = a^{-1} = a^{n-1}b$.

(iii) Παρατηρούμε ότι η υποομάδα $H_1 = \langle \alpha, \beta \rangle$ της S_4 στο τμήμα (i) του παραδείγματος και η υποομάδα $H_2 = \langle a, b \rangle$ της D_8 (ειδική περίπτωση $n = 4$ στο τμήμα (ii) του παρα-

δείγματος) είναι “ουσιαστικά οι ίδιες” (συγκρίνετε επίσης με την Πρόταση 11.12 και το Παράδειγμα 12.23). Η συνάρτηση $\phi: H_1 \rightarrow H_2: \alpha^i \beta^j \mapsto a^i b^j$ ($0 \leq i \leq 3, 0 \leq j \leq 1$) είναι μια αμφιμονοσήμαντη συνάρτηση η οποία “διατηρεί την δομή της ομάδας”. Οι όροι αυτοί μπορούν να γίνουν καλύτερα κατανοητοί στην επόμενη παράγραφο, όταν θα μελετήσουμε τέτοιου είδους συναρτήσεις με περισσότερη λεπτομέρεια.

Παράσταση ομάδας. Έστω G ομάδα και $S = \{g_1, \dots, g_n\}$ ένα υποσύνολο του G . Αν $G = \langle S \rangle$, τότε λέμε επίσης ότι τα στοιχεία $g_1, \dots, g_n$ παράγουν την G και γράφουμε πιο απλά ότι $G = \langle g_1, \dots, g_n \rangle$. Μια έκφραση η οποία είναι γινόμενο των g_i και των αντιστρώφων τους, καλείται λέξη στα g_i . Για παράδειγμα, η εκφράση $g_1 g_2^{-1} g_1$ είναι μια λέξη στα g_1 και g_2 .

Όπως στο πιο πάνω παράδειγμα, τα σύμβολα $g_1, \dots, g_n$ μπορούν να εμφανιστούν με οποιαδήποτε σειρά σε μια λέξη και επιτρέπεται να εμφανιστούν περισσότερες από μια φορά. Επίσης, δεν είναι απαραίτητο να χρησιμοποιήσουμε όλα τα σύμβολα σε μια λέξη.

Ορισμός. Έστω G ομάδα. Υποθέτουμε ότι G παράγεται από τα στοιχεία της $g_1, \dots, g_n$.

(i) Μια σχέση μεταξύ των $g_1, \dots, g_n$ είναι οποιαδήποτε εξίσωση (η οποία ισχύει στην G) της μορφής $w_1 = w_2$ η οποία εκφράζει το γεγονός ότι δύο λέξεις w_1 και w_2 στα g_i αποτελούν εκφράσεις για το ίδιο στοιχείο της G .

(ii) Ένα πλήρες σύνολο σχέσεων μεταξύ των $g_1, \dots, g_n$ είναι οποιοδήποτε σύνολο R σχέσεων (μεταξύ των $g_1, \dots, g_n$) το οποίο είναι αρκετά μεγάλο ώστε οποιαδήποτε σχέση μεταξύ των g_i να μπορεί να προκύψει ως λογική συνέπεια των σχέσεων στο R και των ιδιοτήτων (στον ορισμό) της ομάδας (κοιτάξτε το σχόλιο στο τέλος της Παραγράφου 13.1).

Παράδειγμα. Έστω $G = \langle g \rangle$ μια κυκλική ομάδα τάξης 5. Τότε $R = \{g^5 = gg^{-1} (= 1_G)\}$ (ή $R = \{g^6 = g\}$) αποτελεί ένα πλήρες σύνολο σχέσεων (ως προς την γεννήτρια g της ομάδας). [Το αποτέλεσμα αυτό είναι άμεση συνέπεια της Παρατήρησης 12.28(ii).]

Σημείωση. (i) Γενικά αν $G = \langle S \rangle$ όπου το υποσύνολο S της G έχει περισσότερα από ένα στοιχεία, το ερώτημα πότε δύο γινόμενα της μορφής $h_1^{\epsilon_1} h_2^{\epsilon_2} \dots h_k^{\epsilon_k}$ (όπου $h_i \in S, \epsilon_i \in \{-1, 1\}$ και k τυχαίος θετικός ακέραιος) συμπίπτουν (αποτελούν δηλαδή εκφράσεις για το ίδιο στοιχείο της G) είναι ένα από τα πιο δύσκολα προβλήματα της θεωρίας ομάδων και είναι γνωστό ως το “πρόβλημα της λέξης”

(ii) Αρκετά συχνά στην θεωρία ομάδων είναι χρήσιμο να προσδιορίσουμε μια ομάδα G μέσω ενός συστήματος γεννητριών και ενός πλήρους συνόλου σχέσεων μεταξύ των γεννητριών δίνοντας έτσι μια παράσταση για την ομάδα G . Για παράδειγμα η παράσταση $\langle a: a^n = 1 \rangle$, όπου $n \in \mathbb{N}$, προσδιορίζει την κυκλική ομάδα τάξης n (στην επόμενη παράγραφο θα δείξουμε ότι όλες οι κυκλικές ομάδες τάξης n είναι “ουσιαστικά ίδιες”). Ένα άλλο παράδειγμα, όπου $n \in \mathbb{Z}$ με $n \geq 3$, είναι η παράσταση $G = \langle a, b: a^n = 1_G, b^2 = 1_G, ab = ba^{-1} \rangle$ που προσδιορίζει την διεδρική ομάδα τάξης $2n$, συγκρίνετε με το Παράδειγμα 13.3(ii).

Υπάρχει όμως ένα αδύνατο σημείο στην μέχρι τώρα συζήτηση μας σχετικά με παραστάσεις. Στον ορισμό ενός πλήρους συνόλου σχέσεων μεταξύ των γεννητριών ο όρος “συνέπεια των σχέσεων στο σύνολο R και των ιδιοτήτων της ομάδας” δεν είναι αρκετά ακριβής (παρ’

όλο που μπορούμε να έχουμε μια πολύ καλή διαισθητική εικόνα για το τι σημαίνει από τα παραδείγματα που έχουμε μελετήσει). Υπάρχει αυστηρός ορισμός του πιο πάνω όρου όπως και του όρου “παράσταση ομάδας” ο οποίος εμπλέκει τις έννοιες της *ελεύθερης ομάδας* και της *κανονικής κλειστότητας* (κοιτάξτε, για παράδειγμα, το βιβλίο W. Ledermann, A. Weir “An Introduction to Group Theory”, Κεφάλαιο 9).

13.2. Ομομορφισμοί ομάδων

Παράδειγμα. Θεωρούμε τον πίνακα πρόσθεσης της $\mathbb{Z}_4$ και τον πίνακα πολλαπλασιασμού της $\mathbb{Z}_5^*$. (Πίνακες αυτής της μορφής καλούνται πίνακες Cayley των αντίστοιχων ομάδων.)

	+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$		$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	
		$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$			$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	
$(\mathbb{Z}_4, +)$		$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$(\mathbb{Z}_5^*, \cdot)$	$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
		$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$		$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
		$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$		$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Παρατηρούμε ότι οι δύο αυτοί πίνακες έχουν εκπληκτικές ομοιότητες: Έστω $\phi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_5^*$ η συνάρτηση που ορίζεται με $\phi(\bar{0}) = \bar{1}$, $\phi(\bar{1}) = \bar{2}$, $\phi(\bar{2}) = \bar{4}$ και $\phi(\bar{3}) = \bar{3}$. Αντικαθιστώντας τα σύμβολα στον πρώτο πίνακα με τις εικόνες τους μέσω της ϕ (και χρησιμοποιώντας την “σωστή σειρά” $\bar{1}, \bar{2}, \bar{4}, \bar{3}$), προκύπτει ο δεύτερος πίνακας. Πιο ειδικά, $\phi(a+b) = (\phi a) \cdot (\phi b)$ για όλα τα $a, b \in \mathbb{Z}_4$.

Ορισμός. Έστω $(G, \cdot)$ και $(H, *)$ δύο ομάδες (με πράξεις $\cdot$ και $*$ αντίστοιχα). Μια απεικόνιση $\phi : G \rightarrow H$ ονομάζεται *ομομορφισμός ομάδων* αν $\phi(g \cdot h) = (\phi g) * (\phi h)$ για όλα τα $g, h \in G$.

[Πιο κάτω θα επανέλθουμε στην προηγούμενη συνθήκη. Θα λέμε G, H αντί $(G, \cdot)$ και $(H, *)$ και αν $\phi : G \rightarrow H$ είναι ομομορφισμός ομάδων, θα γράφουμε $\phi(gh) = (\phi g)(\phi h)$ για $g, h \in G$ αφού δεν πρόκειται να δημιουργηθεί σύγχυση.]

Παράδειγμα 13.4. (i) $G = \text{GL}(2, \mathbb{R})$, $H = (\mathbb{R} - \{0\}, \cdot)$. Θέτουμε $\phi : G \rightarrow H : A \mapsto \det(A)$, $A \in \text{GL}(2, \mathbb{R})$. Αν $A_1, A_2 \in \text{GL}(2, \mathbb{R})$ έχουμε τότε: $\phi(A_1 A_2) = \det(A_1 A_2) = (\det A_1)(\det A_2) = (\phi A_1)(\phi A_2)$.

(ii) $G = (\mathbb{R}, +)$, $H = (\mathbb{R}^+, \cdot)$, όπου $\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$. [Ελέγξτε ότι H αποτελεί ομάδα.] Θέτουμε $\phi : G \rightarrow H : x \mapsto \exp(x)$, $x \in \mathbb{R}$. Αν $x_1, x_2 \in \mathbb{R}$ έχουμε: $\phi(x_1 + x_2) = \exp(x_1 + x_2) = (\exp x_1)(\exp x_2) = (\phi x_1)(\phi x_2)$.

(iii) $G = (\mathbb{R}, +)$, $H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R} \right\}$. [Ελέγξτε ότι H αποτελεί ομάδα ως προς τον συνηθισμένο πολλαπλασιασμό πινάκων.] Θέτουμε $\phi : G \rightarrow H : a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, $a \in \mathbb{R}$. Τότε $\phi(a+b) = (\phi a)(\phi b)$ για όλα τα $a, b \in G$. Επιπλέον, ϕ είναι αμφιμονοσήμαντη.

(iv) $G = (\mathbb{R}^+, \cdot)$, $H = (\mathbb{R}, +)$. Τότε $\phi: G \rightarrow H : x \mapsto \log x$ ($x \in \mathbb{R}^+$) είναι ένας ομομορφισμός ομάδων.

(v) Έστω $n > 1$. Τότε η συνάρτηση $\theta: \mathbb{Z} \rightarrow \mathbb{Z}_n : a \mapsto \bar{a}$, ($a \in \mathbb{Z}$) είναι ένας επιρριπτικός ομομορφισμός ομάδων.

Πρόταση 13.5. Έστω $\phi: G \rightarrow H$ ομομορφισμός ομάδων. Τότε $\phi(1_G) = 1_H$ και $\phi(g^{-1}) = (\phi g)^{-1}$ για κάθε $g \in G$.

Απόδειξη. Δεχόμαστε την υπόθεση. Έστω $g \in G$. Από τις σχέσεις $1_G^2 = 1_G$ και $g^{-1}g = 1_G$, έπεται ότι $\phi(1_G) = \phi(1_G 1_G) = (\phi 1_G)(\phi 1_G)$ και $\phi(1_G) = \phi(g^{-1}g) = (\phi g^{-1})(\phi g)$. Συνεπώς έχουμε ότι στην H ισχύει $1_H = (\phi 1_G)(\phi 1_G)^{-1} = (\phi 1_G)(\phi 1_G)(\phi 1_G)^{-1} = (\phi 1_G)$. Επίσης $(\phi g^{-1})(\phi g) = \phi(g^{-1}g) = \phi(1_G) = 1_H = \phi(gg^{-1}) = (\phi g)(\phi g^{-1})$. Συνάγουμε ότι $(\phi g)^{-1} = \phi(g^{-1})$. $\square$

Ορισμός. Έστω $\phi: G \rightarrow H$ ομομορφισμός ομάδων. Θέτουμε

(i) $\text{im } \phi = \{h \in H : h = \phi(g) \text{ για κάποιο } g \in G\} = \{\phi(g) : g \in G\}$, και

(ii) $\ker \phi = \{g \in G : \phi(g) = 1_H\}$.

Πρόταση 13.6. Αν $\phi: G \rightarrow H$ είναι ομομορφισμός ομάδων, τότε

(i) $\text{im } \phi \leq H$, (ii) ϕ είναι επιρριπτικός αν-ν $\text{im } \phi = H$, (iii) $\ker \phi \leq G$, και

(iv) ϕ είναι ενριπτικός αν-ν $\ker \phi = \{1_G\}$.

Απόδειξη. (i) Παρατηρούμε ότι $1_H = \phi(1_G) \in \text{im } \phi$. Έστω $h_1, h_2 \in \text{im } \phi$. Τότε $h_1 = \phi(g_1)$ και $h_2 = \phi(g_2)$ για κάποια $g_1, g_2 \in G$. Συνεπώς $h_1 h_2 = (\phi g_1)(\phi g_2) = \phi(g_1 g_2) \in \text{im } \phi$, αφού $g_1 g_2 \in G$. Επιπλέον, $h_1^{-1} = (\phi g_1)^{-1} = \phi(g_1^{-1}) \in \text{im } \phi$, αφού $g_1^{-1} \in G$.

(ii) Από τον ορισμό της επίρριψης.

(iii) Προφανώς $\ker \phi \subseteq G$ από τον ορισμό του συνόλου $\ker \phi$. Έχουμε, $\phi(1_G) = 1_H$ άρα $1_G \in \ker \phi$. Έστω $g_1, g_2 \in \ker \phi$. Τότε $\phi(g_1 g_2) = (\phi g_1)(\phi g_2) = 1_H 1_H = 1_H$ και $\phi(g_1^{-1}) = (\phi g_1)^{-1} = (1_H)^{-1} = 1_H$. Άρα $g_1 g_2 \in \ker \phi$ και $g_1^{-1} \in \ker \phi$.

(iv) Από την Πρόταση 13.5 έχουμε ότι $\{1_G\} \subseteq \ker \phi$. Έστω πρώτα ότι ϕ είναι ενριπτικός και ότι $g \in \ker \phi$. Τότε $\phi(g) = \phi(1_G) (= 1_H)$, και επομένως $g = 1_G$. Αντίστροφα, υποθέτουμε ότι $\ker \phi = \{1_G\}$. Αν τώρα $g_1, g_2 \in G$ με $\phi(g_1) = \phi(g_2)$ έχουμε, $1_H = (\phi g_1)(\phi g_2)^{-1} = (\phi g_1)(\phi g_2^{-1}) = \phi(g_1 g_2^{-1})$. Έπεται ότι $g_1 g_2^{-1} \in \ker \phi$ και επομένως $g_1 g_2^{-1} = 1_G$. Συμπεραίνουμε ότι $g_1 = g_2$, και επομένως ϕ είναι ενριπτικός. $\square$

Παράδειγμα 13.7. Έστω $n \geq 3$ και έστω $G = D_{2n}$. Τότε $|G| = 2n$ και $G = \langle a, b \rangle = \{a^i b^j : 0 \leq i \leq n-1 \text{ και } 0 \leq j \leq 1\}$ όπου $a = \text{rot}_{2\pi/n}$ και $b = \text{ref}_0$ (κοιτάζτε το Παράδειγμα 13.3(ii)). Έχουμε τότε ότι $a^n = 1_G$, $b^2 = 1_G$ και $ab = ba^{-1}$. Έστω επίσης H μια ομάδα η οποία περιέχει στοιχεία x, y τα οποία ικανοποιούν $x^n = 1_H$, $y^2 = 1_H$ και $xy = yx^{-1}$. Θα δείξουμε ότι η συνάρτηση $\theta: G \rightarrow H : a^i b^j \mapsto x^i y^j$, ($0 \leq i \leq n-1$, $0 \leq j \leq 1$) είναι ομομορφισμός. Υποθέτουμε ότι $0 \leq r \leq n-1$, $0 \leq s \leq 1$, $0 \leq t \leq n-1$ και $0 \leq u \leq 1$. Τότε $a^r b^s a^t b^u = a^i b^j$ για κάποια i, j με $0 \leq i \leq n-1$, $0 \leq j \leq 1$.

Επιπλέον, τα i και j προσδιορίζονται πλήρως χρησιμοποιώντας τις τρεις σχέσεις $a^n = 1_G$, $b^2 = 1_G$, $ab = ba^{-1}$ (κοιτάξτε και πάλι το Παράδειγμα 13.3(ii)). Αφού ισχύουν $x^n = 1_H$, $y^2 = 1_H$ και $xy = yx^{-1}$, προκύπτει εύκολα ότι $x^r y^s x^t y^u = x^i y^j$. Συνεπώς, $\theta(a^r b^s a^t b^u) = \theta(a^i b^j) = x^i y^j = x^r y^s x^t y^u = \theta(a^r b^s) \theta(a^t b^u)$. Συνάγουμε ότι θ είναι ομομορφισμός ομάδων. Παρατηρούμε επίσης ότι $\text{im } \theta = \langle x, y \rangle$, αφού κάθε στοιχείο της υποομάδας $\langle x, y \rangle$ της H μπορεί να εκφραστεί στην μορφή $x^i y^j$ ($0 \leq i \leq n-1$, $0 \leq j \leq 1$), όχι όμως υποχρεωτικά με μοναδικό τρόπο.

Ορισμός. Έστω G, H ομάδες.

- (i) Ένας ομομορφισμός ομάδων $\phi: G \rightarrow H$ ο οποίος είναι αμφιμονοσήμαντη συνάρτηση ονομάζεται *ισομορφισμός*.
- (ii) Σε περίπτωση που υπάρχει ισομορφισμός $\phi: G \rightarrow H$, λέμε ότι η ομάδα G είναι *ισομορφική* προς την ομάδα H (συμβολισμός: $G \cong H$).
- (iii) Ένας ισομορφισμός $\phi: G \rightarrow G$ ονομάζεται *αυτομορφισμός* της G . Το σύνολο των αυτομορφισμών της G συμβολίζεται με $\text{Aut}(G)$.

Παράδειγμα. Ο ομομορφισμός ϕ στο Παράδειγμα 13.4(iii) είναι ένας ισομορφισμός, δεν ισχύει όμως το ίδιο για τον ομομορφισμό θ στο Παράδειγμα 13.4(v).

Πρόταση 13.8. (i) Η σύνθεση δύο ομομορφισμών είναι επίσης ομομορφισμός.

(ii) Η σύνθεση δύο ισομορφισμών είναι επίσης ισομορφισμός.

(iii) Η αντίστροφη απεικόνιση ενός ισομορφισμού είναι επίσης ισομορφισμός.

Απόδειξη. (i) Έστω $\phi: G \rightarrow H$ και $\psi: H \rightarrow K$ ομομορφισμοί ομάδων. Έστω επίσης $g, h \in G$. Έχουμε, $(\psi \circ \phi)(gh) = \psi(\phi(gh)) = \psi((\phi g)(\phi h)) = \psi(\phi(g))\psi(\phi(h)) = ((\psi \circ \phi)(g))((\psi \circ \phi)(h))$.

(ii) Άμεση συνέπεια του (i) αφού η σύνθεση αμφιμονοσήμαντων συναρτήσεων είναι μια αμφιμονοσήμαντη συνάρτηση.

(iii) Υποθέτουμε τώρα ότι $\phi: G \rightarrow H$ είναι ισομορφισμός ομάδων. Η αντίστροφη απεικόνιση $\phi^{-1}: H \rightarrow G$ υπάρχει και είναι επίσης αμφιμονοσήμαντη. Θα δείξουμε ότι ϕ^{-1} είναι ομομορφισμός. Έστω $h_1, h_2 \in H$. Τότε $h_1 = \phi(g_1)$ και $h_2 = \phi(g_2)$ για κάποια $g_1, g_2 \in G$. Έχουμε επίσης, $\phi^{-1}(h_1 h_2) = \phi^{-1}((\phi g_1)(\phi g_2)) = \phi^{-1}(\phi(g_1 g_2)) = g_1 g_2 = (\phi^{-1} h_1)(\phi^{-1} h_2)$.

□

Παράδειγμα. Συγκρίνετε την Πρόταση 13.8(iii) με τα Παραδείγματα 13.4(ii) και (iv).

Σημείωση. Αν $\phi: G \rightarrow H$ είναι ένας ισομορφισμός ομάδων, τότε όλες οι ιδιότητες που αφορούν στην ομάδα G , μεταφέρονται μέσω του ισομορφισμού ϕ στην ομάδα H , και αντίστροφα. Έτσι, από “ομαδοθεωρητικής” πλευράς οι δύο ομάδες αυτές δεν διαφέρουν και συνήθως δεν κάνουμε διάκριση μεταξύ τους. Λέμε ότι οι δύο ομάδες είναι *ισομορφικές* ή ότι *ανήκουν στην ίδια ισομορφική κλάση*.

Παράδειγμα 13.9. Έστω $\phi: G \rightarrow H$ ομομορφισμός ομάδων και $K \leq G$. Τότε

- (i) Το σύνολο $\phi(K) (= \{\phi(g) : g \in K\})$ αποτελεί υποομάδα της H .
- (ii) Αν ϕ είναι ισομορφισμός και K είναι πεπερασμένης τάξης n , τότε και η $\phi(K)$ είναι πεπερασμένης τάξης n .

Σημείωση 13.10. Έστω G ομάδα. Τότε $\text{Aut}(G) \leq \text{Sym}(G)$. [Εξήγηση: Προφανώς $\text{Aut}(G) \subseteq \text{Sym}(G)$. Έχουμε επίσης ότι $i_G \in \text{Aut}(G)$. Το αποτέλεσμα είναι τώρα άμεση συνέπεια της Πρότασης 13.8.]

Ορισμός. Έστω G ομάδα. Η ομάδα $\text{Aut}(G)$ καλείται η ομάδα αυτομορφισμών της G .

Παραδείγματα 13.11. (i) Αν G είναι κυκλική ομάδα άπειρης τάξης, τότε $\text{Aut}(G) \cong C_2$.

(ii) Θέτουμε $\omega = \cos\left(\frac{2\pi}{5}\right) + i \sin\left(\frac{2\pi}{5}\right) \in \mathbb{C}$. Έστω τώρα $\phi: \mathbb{Z}_5 \rightarrow C_5 : \bar{k} \mapsto \omega^k$, ($0 \leq k \leq 4$). (Προφανώς ϕ είναι μια συνάρτηση από την $\mathbb{Z}_5$ στην C_5). Έστω επίσης $u, v \in \mathbb{Z}$ με $0 \leq u, v \leq 4$. Σύμφωνα με το θεώρημα διαίρεσης, υπάρχουν ακέραιοι q, r με $u+v = 5q+r$ και $0 \leq r \leq 4$. Συνεπώς, $\phi(\bar{u} + \bar{v}) = \phi(\overline{u+v}) = \phi(\bar{r}) = \omega^r = (\omega^5)^q \omega^r = \omega^{5q+r} = \omega^{u+v} = \omega^u \omega^v$. Όμως $\omega^u = \phi(\bar{u})$ και $\omega^v = \phi(\bar{v})$, επομένως έχουμε δείξει ότι $\phi(\bar{u} + \bar{v}) = \phi(\bar{u})\phi(\bar{v})$. Συνάγουμε ότι ϕ είναι ομομορφισμός ομάδων και επομένως ισομορφισμός, αφού προφανώς ϕ είναι μια αμφιμονοσήμαντη συνάρτηση.

(iii) Οι ομάδες H_1 και H_2 στο Παράδειγμα 13.3(iii) είναι ισομορφικές (συγκρίνετε με το Παράδειγμα 13.7).

Πρόταση 13.12. Έστω G κυκλική ομάδα.

- (i) Αν G είναι άπειρης τάξης, τότε $G \cong (\mathbb{Z}, +)$.
- (ii) Αν G είναι πεπερασμένης τάξης n , τότε $G \cong (\mathbb{Z}_n, +)$.

Απόδειξη. (i) Έστω πρώτα G κυκλική ομάδα άπειρης τάξης. Τότε $G = \langle g \rangle (= \{g^k : k \in \mathbb{Z}\})$ για κάποιο $g \in G$, όπου $S = \{r \in \mathbb{N} : g^r = 1_G\} = \emptyset$.

Θέτουμε $\phi: G \rightarrow \mathbb{Z} : g^k \mapsto k$, ($k \in \mathbb{Z}$). Η συνάρτηση $\phi: G \rightarrow \mathbb{Z}$ είναι καλά ορισμένη, αφού οι δυνάμεις g^k , όπου $k \in \mathbb{Z}$, είναι διακεκριμένες. Επιπλέον, αν $k_1, k_2 \in \mathbb{Z}$ έχουμε $\phi(g^{k_1}g^{k_2}) = \phi(g^{k_1+k_2}) = k_1 + k_2 = \phi(g^{k_1}) + \phi(g^{k_2})$, και επομένως ϕ είναι ομομορφισμός ομάδων. Προφανώς $\text{im } \phi = \mathbb{Z}$ και $\ker \phi = \{g^0\} = \{1_G\}$, άρα ϕ είναι αμφιμονοσήμαντη.

(ii) Έστω τώρα ότι G είναι κυκλική ομάδα (πεπερασμένης) τάξης n . Τότε υπάρχει $g \in G$ με $o(g) = n$ και $G = \langle g \rangle = \{1, g, \dots, g^{n-1}\}$. Θέτουμε $\phi: G \rightarrow \mathbb{Z}_n : g^k \mapsto \bar{k}$, ($0 \leq k \leq n-1$). Προφανώς ϕ είναι μια αμφιμονοσήμαντη συνάρτηση. Έστω τώρα $k_1, k_2 \in \mathbb{Z}$ με $0 \leq k_1, k_2 \leq n-1$. Τότε $k_1 + k_2 = qn + r$, όπου $q, r \in \mathbb{Z}$ και $0 \leq r < n$ από το θεώρημα διαίρεσης. Έπεται ότι $g^{k_1+k_2} = g^{qn+r} = (g^n)^q g^r = g^r$. Συνεπώς, $\phi(g^{k_1}g^{k_2}) = \phi(g^{k_1+k_2}) = \phi(g^r) = \bar{r} = \bar{q}n + \bar{r} = \overline{qn+r} = \overline{k_1+k_2} = \bar{k}_1 + \bar{k}_2 = \phi(g^{k_1}) + \phi(g^{k_2})$. Άρα ϕ είναι ομομορφισμός. $\square$

Σχόλια. (i) Στην απόδειξη της Πρότασης 13.12(ii) η γεννήτρια g της G ικανοποιεί την σχέση $g^n = 1_G$ ενώ η γεννήτρια $\bar{1} (= \phi(g))$ της $\mathbb{Z}_n$ ικανοποιεί την “ίδια” σχέση (προσθετικός συμβολισμός) $\bar{0} = n \cdot \bar{1}$. Συγκρίνετε με το Παράδειγμα 13.7.

(ii) Θεωρώντας την ειδική περίπτωση $n = 8$ στην Πρόταση 13.12(ii), παρατηρούμε ότι η συνάρτηση $\theta: G \rightarrow \mathbb{Z}_n : g^k \mapsto \bar{2}k$ ($0 \leq k \leq 7$) είναι ένας ομομορφισμός ομάδων όπου $\text{im } \phi = \langle \bar{2} \rangle$ και με την γεννήτρια $\bar{2}$ της $\text{im } \theta$ να ικανοποιεί την σχέση $\bar{0} = 8 \cdot \bar{2}$. Ο ομομορφισμός θ δεν είναι ενριπτικός ούτε επιρριπτικός.

Πρόταση 13.13. (Απόδειξη: Άσκηση.) Έστω $m, n \in \mathbb{N}$. Έχουμε τότε ότι $C_m \times C_n \cong C_{mn}$ αν, και μόνο αν, $\text{μκδ}(m, n) = 1$.

13.3. Θεώρημα Cayley

Στην συνέχεια θα δείξουμε ότι κάθε ομάδα G είναι ισομορφική με μια υποομάδα της $\text{Sym}(X)$ για κάποιο μη-κενό σύνολο X (θεώρημα Cayley).

Πρόταση 13.14. Έστω G ομάδα. Αν $g \in G$, θέτουμε $\theta_g: G \rightarrow G : x \mapsto gx$ ($x \in G$). Τότε $\theta_g \in \text{Sym}(G)$ για κάθε $g \in G$. Επιπλέον, η συνάρτηση $\phi: G \rightarrow \text{Sym}(G) : g \mapsto \theta_g$ ($g \in G$), είναι ομομορφισμός ομάδων.

Απόδειξη. Για $g \in G$, έχουμε: $\theta_g x = \theta_g y$ ($x, y \in G$) $\Rightarrow gx = gy \Rightarrow g^{-1}(gx) = g^{-1}(gy) \Rightarrow (g^{-1}g)x = (g^{-1}g)y \Rightarrow x = y$ (άρα θ_g είναι ενριπτική). Επίσης, αν $z \in G$, παρατηρούμε ότι $z = (gg^{-1})z = g(g^{-1}z) = \theta_g(g^{-1}z)$, όπου $g^{-1}z \in G$. Έπεται ότι θ_g είναι επιρριπτική. Συνάγουμε ότι $\theta_g \in \text{Sym}(G)$ για κάθε $g \in G$. Θα δείξουμε τώρα ότι η συνάρτηση $\phi: G \rightarrow \text{Sym}(G)$ που ορίζεται με $\phi(g) = \theta_g$ ($g \in G$) είναι ομομορφισμός ομάδων. Έστω $g, h, x \in G$. Έχουμε τότε, $\theta_{(gh)}(x) = (gh)x = g(hx) = g(\theta_h x) = \theta_g(\theta_h x) = (\theta_g \theta_h)(x)$. Συνεπώς, $\phi(gh) = \theta_{(gh)} = \theta_g \theta_h = (\phi g)(\phi h)$. $\square$

Ορισμός. Ο ομομορφισμός $\phi: G \rightarrow \text{Sym}(G)$ που δίνεται στην Πρόταση 13.14 καλείται η *αριστερή κανονική αναπαράσταση* της ομάδας G .

Ορισμός. Μια ομάδα ονομάζεται *ομάδα μεταθέσεων* όταν τα στοιχεία της είναι μεταθέσεις. Μια τέτοια ομάδα είναι μια υποομάδα της $\text{Sym}(X)$ για κάποιο μη-κενό σύνολο X .

Παράδειγμα 13.15. Η ομάδα του *Klein* (Klein's 4-group) είναι μια ομάδα μεταθέσεων σε τέσσερα σύμβολα και τάξης 4. Η ομάδα αυτή είναι η $V_4 = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ και είναι μια υποομάδα της S_4 .

Θα δείξουμε ότι πράγματι $V_4 \leq S_4$ και ότι $V_4 \cong C_2 \times C_2$: Προφανώς $V_4 \subseteq S_4$. Έχουμε επίσης ότι $(1) \in V_4$ και $\pi^{-1} = \pi$ για όλα τα $\pi \in V_4$. Θέτουμε $\rho, \sigma \in S_4$ με $\rho = (1\ 2)(3\ 4)$ και $\sigma = (1\ 3)(2\ 4)$. Τότε $\rho, \sigma \in V_4$ και $\rho\sigma = \sigma\rho = (1\ 4)(2\ 3) \in V_4$. Έπεται ότι $V_4 = \{\rho^i \sigma^j : 0 \leq i, j \leq 1\}$, όπου $\rho^2 = (1) = \sigma^2$ και $\rho\sigma = \sigma\rho$. Από τις σχέσεις που διέπουν τις γεννήτριες ρ, σ της V_4 , και την μορφή των στοιχείων της V_4 , προκύπτει εύκολα ότι το γινόμενο δύο στοιχείων της V_4 είναι στοιχείο της V_4 . Ελέγξτε ότι η συνάρτηση $\phi: V_4 \rightarrow C_2 \times C_2 : \rho^i \sigma^j \mapsto (1, -1)^i (-1, 1)^j$, ($0 \leq i, j \leq 1$) είναι ένας ισομορφισμός ομάδων.

Θεώρημα 13.16. (Cayley). Κάθε ομάδα G είναι ισομορφική με μια ομάδα μεταθέσεων. Πιο ειδικά, αν G είναι πεπερασμένης τάξης n , τότε G είναι ισομορφική με μια υποομάδα της S_n .

Απόδειξη. Έστω G ομάδα. Χρησιμοποιούμε τον συμβολισμό από την Πρόταση 13.14 για τις συναρτήσεις $\theta_g: G \rightarrow G$ και $\phi: G \rightarrow \text{Sym}(G)$. Παρατηρούμε ότι $\ker \phi = \{g \in G: \theta_g = i_G\} = \{1_G\}$. [Εξήγηση: Αν $g \in \ker \phi$, τότε $\phi(g) = \theta_g = i_G$, άρα $g = g1_G = \theta_g(1_G) = i_G(1_G) = 1_G$.] Συνεπώς ϕ είναι ένας ενριπτικός ομομορφισμός ομάδων (χρησιμοποιούμε την Πρόταση 13.14 και την Πρόταση 13.6(iv)). Άρα η συνάρτηση $\hat{\phi}: G \rightarrow \text{im} \phi: g \mapsto \theta_g$ ($g \in G$) είναι ισομορφισμός ομάδων (έχουμε ότι $\text{im} \phi \leq \text{Sym}(G)$ από την Πρόταση 13.6(i)). Συνάγουμε ότι $G \cong \text{im} \phi (\leq \text{Sym}(G))$.

Στην περίπτωση που $|G| = n$, προφανώς $\text{Sym}(G) \cong S_n$. □

Παράδειγμα 13.17. Θέλουμε να βρούμε την αριστερή κανονική αναπαράσταση της $G = C_4$. Έχουμε δει ότι $G = \langle \omega \rangle = \{1_G, \omega, \omega^2, \omega^3\}$ όπου $o(\omega) = 4$ (για παράδειγμα μπορούμε να θέσουμε $\omega = i \in \mathbb{C}$). Έστω $\phi: G \rightarrow \text{Sym}(G): g \mapsto \theta_g$ ($g \in G$) η αριστερή κανονική αναπαράσταση της G . Έχουμε τότε: $\theta_{1_G} = \phi(1_G) = (1_G)(\omega)(\omega^2)(\omega^3)$, $\theta_\omega = (1_G \ \omega \ \omega^2 \ \omega^3)$, $\theta_{\omega^2} = (1_G \ \omega^2)(\omega \ \omega^3)$, $\theta_{\omega^3} = (1_G \ \omega^3 \ \omega^2 \ \omega)$. Παρατηρούμε επίσης ότι $(\phi\omega^2)(\phi\omega^3) = \theta_{\omega^2}\theta_{\omega^3} = (1_G \ \omega^2)(\omega \ \omega^3)(1_G \ \omega^3 \ \omega^2 \ \omega) = (1_G \ \omega \ \omega^2 \ \omega^3) = \theta_\omega = \phi(\omega) = \phi(\omega^2\omega^3)$, αφού $\omega^4 = 1$.

Αν $n \in \mathbb{N}$, τότε S_n είναι ένα πεπερασμένο σύνολο, άρα περιέχει πεπερασμένο πλήθος υποσυνόλων (και υποομάδων). Επομένως, μια άμεση συνέπεια του θεωρήματος Cayley είναι το

Πόρισμα 13.18. Έστω $n \in \mathbb{N}$. Τότε υπάρχει, ως προς ισομορφισμό, πεπερασμένο πλήθος ομάδων με τάξη n .

Ασκήσεις

- 13.1 Θέτουμε $S = \{(1 \ 2), (1 \ 3)(4 \ 5)\} \subseteq S_5$ και $H = \langle S \rangle (\leq S_5)$. Βρείτε τα στοιχεία της H .
- 13.2 Έστω $n \in \mathbb{N}$ με $n > 2$. Για $1 \leq i \leq n-1$, θέτουμε $s_i = (i \ i+1) \in S_n$. Έστω επίσης ρ ο n -κύκλος $(1 \ 2 \dots n) \in S_n$. Δείξτε ότι (i) $S_n = \langle s_1, \dots, s_{n-1} \rangle$, και (ii) $S_n = \langle s_1, \rho \rangle$.
- 13.3 Έστω $G \leq (\mathbb{Q}, +)$, όπου $+$ είναι η συνηθισμένη πρόσθεση ρητών. Αν $G = \langle a, b \rangle$ για κάποια $a, b \in \mathbb{Q} - \{0\}$, δείξτε ότι G είναι άπειρη κυκλική.
- 13.4 Έστω $\phi: G \rightarrow H$ ομομορφισμός ομάδων και $g \in G$.
(i) Δείξτε ότι $\phi(g^k) = (\phi g)^k$ για όλα τα $k \in \mathbb{Z}$.
(ii) Αν, επιπλέον, ϕ είναι ενριπτικός, εξετάστε κατά πόσον τα στοιχεία g και $\phi(g)$ έχουν την ίδια τάξη.
- 13.5 Έστω $\phi: G \rightarrow H$ ομομορφισμός ομάδων. Έστω επίσης $g \in G$ όπου g πεπερασμένης τάξης. Δείξτε ότι $o(\phi(g)) \mid o(g)$.
- 13.6 Δείξτε ότι οι ομάδες $\mathbb{R} - \{0\}$ και $\mathbb{C} - \{0\}$ (ως προς τον συνηθισμένο πολλαπλασιασμό πραγματικών και μιγαδικών αντίστοιχα) δεν είναι ισομορφικές.
- 13.7 Εξετάστε κατά πόσον
(i) οι ομάδες $(\mathbb{Z}_4, +)$ και $(\mathbb{Z}_8^*, \cdot)$ είναι ισομορφικές, και
(ii) οι ομάδες $(\mathbb{Z}_4, +)$ και $(\mathbb{Z}_{10}^*, \cdot)$ είναι ισομορφικές.
- 13.8 Θέτουμε $\phi: S_{10} \rightarrow C_2: \sigma \mapsto \text{sgn}(\sigma)$, ($\sigma \in S_{10}$). Δείξτε ότι η συνάρτηση ϕ είναι ομομορφισμός ομάδων και βρείτε τα $\ker \phi$ και $\text{im} \phi$.
- 13.9 Βρείτε όλους τους ομομορφισμούς ομάδων $\phi: C_9 \rightarrow C_{13}$.

- 13.10 Έστω $m, n \in \mathbb{N}$. Δείξτε ότι $C_m \times C_n \cong C_{mn}$ αν, και μόνο αν, $\mu\kappa\delta(m, n) = 1$.
- 13.11 (i) Έστω G ομάδα. Δείξτε ότι $\phi : G \rightarrow G : x \mapsto x^{-1}$ ($x \in G$) είναι αυτομορφισμός της G αν, και μόνο αν, G είναι αβελιανή.
(ii) Αν K είναι κυκλική ομάδα άπειρης τάξης, δείξτε ότι $\text{Aut}(K) \cong C_2$.
- 13.12 (i) Δείξτε ότι $I_{\mathbb{R}}(\mathbb{R}^2)$ αποτελεί ομάδα ως προς την σύνθεση συναρτήσεων. [Κοιτάζτε στην Παράγραφο 11.1 για τον ορισμό του συνόλου $I_{\mathbb{R}}(\mathbb{R}^2)$.]
(ii) Βρείτε, αν υπάρχει, ένα ισομορφισμό ομάδων $\phi : I_{\mathbb{R}}(\mathbb{R}^2) \rightarrow \text{GL}(2, \mathbb{R})$ τέτοιο ώστε $\{\phi(f) : f \in O(\mathbb{R}^2)\} = O(2, \mathbb{R})$.
- 13.13 Δείξτε ότι υπάρχει ενριπτικός ομομορφισμός ομάδων $\psi : D_{2n} \rightarrow S_n$.
- 13.14 (i) Έστω $A, B \in \text{GL}(2, \mathbb{C})$ όπου $A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ και $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Θέτουμε $H = \langle A, B \rangle \leq \text{GL}(2, \mathbb{C})$. (Η ομάδα H είναι η ομάδα των τετρακτύων και συμβολίζεται με Q_8 .) Βρείτε την τάξη της H . [Υπόδειξη: Δείξτε ότι $A^4 = I_2$, $A^2 = B^2$, $B^{-1}AB = A^{-1}$.]
(ii) Δείξτε ότι οι ομάδες Q_8 και D_8 δεν είναι ισομορφικές.
- 13.15 Βρείτε την αριστερή κανονική αναπαράσταση της S_3 .

14. Κανονικές υποομάδες, θεωρήματα ομομορφισμών

14.1. Σύμπλοκα, θεώρημα Lagrange

Ορισμός. Έστω S, T μη-κενά υποσύνολα της ομάδας G . Ορίζουμε

(i) $ST = \{st: s \in S, t \in T\}$, και (ii) $T_{(-1)} = \{t^{-1}: t \in T\}$.

Παρατήρηση 14.1. Έστω G ομάδα. Παρατηρούμε ότι

(i) αν $\emptyset \neq T \subseteq G$ και $W = T_{(-1)}$, τότε $W_{(-1)} = T$, και

(ii) αν $H \leq G$, τότε $H_{(-1)} = H$.

Παράδειγμα. Έστω $G = S_3 = \{(1), (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$. Θέτουμε $S = \{(1), (1\ 2\ 3)\}$, $T = \{(1), (1\ 3\ 2)\}$, $U = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ και $V = \{(1\ 2), (1\ 3)\}$. Ελέγξτε ότι $ST = \{(1), (1\ 3\ 2), (1\ 2\ 3)\}$, $S_{(-1)} = T$, $U_{(-1)} = U$, $U \leq G$ και ότι $V_{(-1)} = V$ όμως V δεν αποτελεί υποομάδα της G .

Λήμμα 14.2. Έστω S, T, U μη-κενά υποσύνολα της ομάδας G . Τότε $(ST)U = S(TU)$.

Απόδειξη. Έχουμε, $(ST)U = \{(st)u: s \in S, t \in T, u \in U\} = \{s(tu): s \in S, t \in T, u \in U\} = S(TU)$. $\square$

Έστω τώρα H υποομάδα της ομάδας G και $g \in G$. Αν $K = \{g\}$, τότε αντί $KH = \{g\}H$ γράφουμε απλά gH , και λέμε ότι gH είναι ένα αριστερό σύμπλοκο της H στην G . Παρόμοια, λέμε ότι το υποσύνολο $Hg (= H\{g\} = HK)$ της G είναι ένα δεξιό σύμπλοκο της H στην G . Έχουμε, δηλαδή, για $H \leq G$ και $g \in G$, ότι $Hg = \{hg: h \in H\}$ και $gH = \{gh: h \in H\}$.

Παράδειγμα 14.3. Θέτουμε $G = S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ και $H = \langle (1\ 2) \rangle \leq G$. Τότε $H = \{(1), (1\ 2)\}$. Παρατηρούμε ότι

$$H(1\ 2) = \{(1), (1\ 2)\} = H(1) (= H),$$

$$H(1\ 3) = \{(1\ 3), (1\ 2)(1\ 3)\} = \{(1\ 3), (1\ 3\ 2)\} = H(1\ 3\ 2), \text{ αφού } (1\ 2)(1\ 3\ 2) = (1\ 3),$$

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

Παρατηρούμε επίσης ότι τα δεξιά σύμπλοκα της H στην G αποτελούν μια διαμέριση της G .

Παρατήρηση 14.4. Έστω G ομάδα και $H \leq G$. Για $b \in G$, θέτουμε $X = Hb$. Τότε $X_{(-1)} = \{(hb)^{-1}: h \in H\} = \{b^{-1}h^{-1}: h \in H\} = \{b^{-1}h: h \in H\} = b^{-1}H$. Έχουμε χρησιμοποιήσει ότι $H_{(-1)} = \{h^{-1}: h \in H\} = H$, αφού $H \leq G$.

Πρόταση 14.5. Έστω G ομάδα και $H \leq G$. Τότε η συνάρτηση $\alpha: \mathcal{R} \rightarrow \mathcal{L}: X \mapsto X_{(-1)}$, $X \in \mathcal{R}$, όπου $\mathcal{R}$ (αντίστοιχα, $\mathcal{L}$) είναι η οικογένεια των δεξιών (αντίστοιχα, αριστερών) συμπλόκων της H στην G , είναι αμφιμονοσήμαντη.

Απόδειξη. Δεχόμαστε την υπόθεση. Έστω $T, S \in \mathcal{R}$ με $\alpha(T) = \alpha(S)$. Έχουμε τότε (Παρατήρηση 14.1(i)) ότι $T = (\alpha T)_{(-1)} = (\alpha S)_{(-1)} = S$, άρα η συνάρτηση α είναι ενριπτική. Έστω τώρα $Y \in \mathcal{L}$. Τότε $Y = cH$ για κάποιο $c \in G$. Όμως $c^{-1} \in G$ αφού G είναι ομάδα και, επιπλέον, η Παρατήρηση 14.4 μας εξασφαλίζει ότι $Y = cH = \alpha(Hc^{-1})$, όπου $Hc^{-1} \in \mathcal{R}$. Συνάγουμε ότι α είναι επιρριπτική και επομένως αμφιμονοσήμαντη. $\square$

Σημείωση. Μέσω της πιο πάνω πρότασης μπορούμε να μεταφέρουμε πληροφορίες που έχουμε σχετικά με δεξιά σύμπλοκα σε αντίστοιχες πληροφορίες σχετικά με αριστερά σύμπλοκα.

Παράδειγμα 14.6. (i) Έστω $G = S_3$ και $H = \langle (1\ 2) \rangle \leq G$. Τα αριστερά σύμπλοκα της H στην G είναι:

$$\begin{aligned} (1) \quad H &= \{(1), (1\ 2)\} = (1\ 2)H = H = (H(1))_{(-1)} = (H(1\ 2))_{(-1)} \\ (1\ 3)H &= \{(1\ 3), (1\ 2\ 3)\} = (1\ 2\ 3)H = (H(1\ 3))_{(-1)} = (H(1\ 3\ 2))_{(-1)} \\ (2\ 3)H &= \{(2\ 3), (1\ 3\ 2)\} = (1\ 3\ 2)H = (H(2\ 3))_{(-1)} = (H(1\ 2\ 3))_{(-1)}. \end{aligned}$$

Παρατηρούμε ότι τα αριστερά σύμπλοκα της H στην G αποτελούν μια διαμέριση της G (συγκρίνετε με το Παράδειγμα 14.3 και την Πρόταση 14.5). Επίσης, το αριστερό σύμπλοκο $(1\ 2\ 3)H$ της G δεν ισούται με οποιοδήποτε δεξιό σύμπλοκο της H στην G .

(ii) Διατηρούμε τον συμβολισμό από το Παράδειγμα 13.3(ii). Υπάρχουν ακριβώς δύο δεξιά σύμπλοκα στην D_{2n} για την υποομάδα της $\langle a \rangle$: τα $\langle a \rangle$ και $\langle a \rangle b$.

Πιο κάτω θα δείξουμε ότι για τυχαία ομάδα G και $H \leq G$ τα δεξιά σύμπλοκα (αντίστοιχα, αριστερά σύμπλοκα) της H στην G αποτελούν μια διαμέριση της G .

Πρόταση 14.7. Έστω G ομάδα. Έστω επίσης $H \leq G$ και $g \in G$. Τότε υπάρχει αμφιμονοσήμαντη απεικόνιση $\alpha: H \rightarrow Hg$.

Απόδειξη. Θέτουμε $\alpha: H \rightarrow Hg: h \mapsto hg$ ($h \in H$). Αν $h_1g = h_2g$ με $h_1, h_2 \in H$, τότε $(h_1g)g^{-1} = (h_2g)g^{-1}$ και επομένως $h_1 = h_2$. Άρα α είναι ενριπτική. Αν τώρα $x \in Hg$, τότε $x = hg$ ($= \alpha(h)$) για κάποιο $h \in H$, συνεπώς α είναι επιρριπτική. $\square$

Πρόταση 14.8. Έστω G ομάδα, $H \leq G$ και $g, f \in G$. Οι πιο κάτω προτάσεις είναι ισοδύναμες.

$$(i) \quad Hg = Hf, \quad (ii) \quad f \in Hg, \quad (iii) \quad fg^{-1} \in H.$$

Απόδειξη. Υποθέτουμε ότι $H \leq G$ και $g, f \in G$.

$$(i) \Rightarrow (ii): \text{ Έστω ότι } Hg = Hf. \text{ Τότε } f = 1_G f \in Hf = Hg. [H \leq G, \text{ άρα } 1_G \in H.]$$

(ii) $\Rightarrow$ (iii): Έστω ότι $f \in Hg$. Τότε $f = hg$ για κάποιο $h \in H$. Συνεπώς $fg^{-1} = h \in H$.

(iii) $\Rightarrow$ (i): Έστω ότι $fg^{-1} \in H$. Τότε $fg^{-1} = k$ για κάποιο $k \in H$. Άρα $f = kg \in Hg$. Αν τώρα $l \in H$, τότε $lf = l(kg) = (lk)g \in Hg$ αφού $l, k \in H$ και $H \leq G$. Έπεται ότι $Hf \subseteq Hg$. Παρόμοια δείχνουμε ότι $Hg \subseteq Hf$. (Χρησιμοποιούμε ότι $(fg^{-1})^{-1} (= gf^{-1}) \in H$ οποτεδήποτε $fg^{-1} \in H$.) $\square$

Πόρισμα 14.9. Έστω G ομάδα και $H \leq G$.

(i) Αν $f, g \in G$, τότε είτε $Hg = Hf$, είτε $(Hg) \cap (Hf) = \emptyset$.

(ii) Η συλλογή των δεξιών συμπλόκων της H στην G αποτελεί μια διαμέριση της G .

Απόδειξη. Έστω ότι $H \leq G$. Έστω επίσης $f, g \in G$.

(i) Υποθέτουμε ότι $(Hg) \cap (Hf) \neq \emptyset$. Έστω $c \in (Hg) \cap (Hf)$. Τότε $c \in Hg$ και $c \in Hf$. Σύμφωνα με την Πρόταση 14.8, έχουμε τότε $Hg = Hc$ και $Hf = Hc$. Άρα $Hg = Hf$.

(ii) Προφανώς $g \in Hg$. Συνεπώς κάθε στοιχείο της G ανήκει σε τουλάχιστον ένα από τα δεξιά σύμπλοκα. Το ζητούμενο είναι τώρα άμεση συνέπεια του (i). $\square$

Παρατήρηση 14.10. Εύκολα μπορούμε να αποδείξουμε αντίστοιχα αποτελέσματα για αριστερά σύμπλοκα. Για παράδειγμα, αν G είναι ομάδα και $H \leq G$, τότε για $f, g \in G$ ισχύει: $gH = fH$ αν-ν $f^{-1}g \in H$ αν-ν $g \in fH$.

Ορισμός. Έστω $H \leq G$. Ο δείκτης της H στην G (συμβολισμός: $[G:H]$) είναι το πλήθος των (διακεκριμένων) δεξιών συμπλόκων της H στην G . (Λόγω της Πρότασης 14.5, ο δείκτης $[G:H]$ ισούται επίσης με το πλήθος των (διακεκριμένων) αριστερών συμπλόκων της H στην G .)

Θεώρημα 14.11. (Lagrange). Έστω G μια ομάδα πεπερασμένης τάξης και $H \leq G$. Τότε $|H| \mid |G|$.

Απόδειξη. Δεχόμαστε την υπόθεση. Αφού G είναι πεπερασμένη, ο δείκτης $[G:H]$ είναι πεπερασμένος και επομένως υπάρχει πεπερασμένο υποσύνολο $\{g_1, \dots, g_k\}$ της G τέτοιο ώστε (i) $Hg_i \cap Hg_j = \emptyset$ αν $i \neq j$ ($1 \leq i, j \leq k$) και (ii) $G = \cup_{i=1}^k Hg_i$. [Εξήγηση: Η συλλογή των δεξιών συμπλόκων της H στην G αποτελεί μια διαμέριση της G .] Συνάγουμε ότι $|G| = |Hg_1| + \dots + |Hg_k| = k|H|$. (Χρησιμοποιούμε την Πρόταση 14.7.) $\square$

Ορισμός. Λέμε ότι το υποσύνολο $\{g_1, \dots, g_k\}$ της G στην απόδειξη του Θεωρήματος 14.11 αποτελεί ένα σύστημα δεξιών αντιπροσώπων της H στην G . Παρόμοια μπορούμε να ορίσουμε ένα σύστημα αριστερών αντιπροσώπων της H στην G .

Παρατήρηση. Έστω G ομάδα και $H \leq G$ με $[G:H] = n$. Αν $\{t_1, \dots, t_n\}$ είναι ένα σύστημα αριστερών αντιπροσώπων της H στην G , τότε το υποσύνολο $\{t_1^{-1}, \dots, t_n^{-1}\}$ της G αποτελεί ένα σύστημα δεξιών αντιπροσώπων της H στην G .

Παράδειγμα. Έστω $G = S_3$ και $H = \langle (1\ 2) \rangle \leq G$. Το υποσύνολο $\{(1), (1\ 3\ 2), (2\ 3)\}$ (αντίστοιχα, $\{(1), (1\ 2\ 3), (2\ 3)\}$) της G αποτελεί ένα σύστημα δεξιών (αντίστοιχα, αριστερών) αντιπροσώπων της H στην G . (Συγκρίνετε με τα Παραδείγματα 14.3 και 14.6.)

Πόρισμα 14.12. Έστω G ομάδα με $|G| = p$ όπου p πρώτος. Τότε G είναι κυκλική.

Απόδειξη. Δεχόμαστε την υπόθεση. Έστω $g \in G - \{1_G\}$, ($p \geq 2$, άρα υπάρχει τέτοιο g). Θέτουμε $H = \langle g \rangle$. Από το θεώρημα Lagrange, $|H| \mid |G|$, άρα $|H| \in \{1, p\}$. Όμως $|H| \geq 2$ αφού 1_G και g είναι στοιχεία της H με $g \neq 1_G$. Συνάγουμε ότι $|H| = p$ και επομένως $G = H = \langle g \rangle$. $\square$

Πόρισμα 14.13. Έστω G ομάδα πεπερασμένης τάξης και $g \in G$. Τότε $o(g) \mid |G|$.

Απόδειξη. Δεχόμαστε την υπόθεση. Έχουμε τότε $o(g) = |\langle g \rangle| (= r, \text{ όπου } r \text{ είναι ένας (πεπερασμένος) θετικός ακέραιος})$. Όμως $|\langle g \rangle| \mid |G|$ (Lagrange). $\square$

Πόρισμα 14.14. Διατηρούμε την υπόθεση και συμβολισμό από την Πρόταση 12.31. Τότε οι υποομάδες G_d της G , όπου $d \in \mathbb{N}$ με $d \mid n$, είναι όλες οι υποομάδες της G .

Παράδειγμα. Έστω $n \in \mathbb{N}$. Όπως έχουμε δει $C_k \leq C_n$ οποτεδήποτε $k \in \mathbb{N}$ με $k \mid n$. Στην πραγματικότητα σε τέτοια περίπτωση C_k είναι η μοναδική υποομάδα της C_n τάξης k . [Αν $H \leq C_n$ με $|H| = k$ και $H \neq C_k$, τότε θα υπήρχαν τουλάχιστον $k + 1$ διακεκριμένες k -οστες ρίζες της μονάδας στο $\mathbb{C}$ που είναι άτοπο, αφού από το Πόρισμα 14.13 κάθε στοιχείο της ομάδας H είναι μια k -οστη ρίζα της μονάδας.] Επιπλέον, αν $T \leq C_n$ τότε $|T| = r$ για κάποιο $r \mid n$, επομένως $x^r = 1_T$ για όλα τα $x \in T$. Έπεται ότι $T \leq C_r$, και αφού $|T| = r$ τότε $T = C_r$. Αφού κάθε κυκλική υποομάδα τάξης n είναι ισομορφική προς την C_n , η πιο πάνω συζήτηση αποτελεί εναλλακτική απόδειξη για το Θεώρημα 12.29 και Πρόταση 12.31.

Υπενθύμιση. Έχουμε ορίσει την συνάρτηση ϕ του Euler με $\phi: \mathbb{N} \rightarrow \mathbb{N}$ όπου $\phi(1) = 1$ και $\phi(n) = |\{k: 1 \leq k < n \text{ και } \mu\kappa\delta(k, n) = 1\}|$ αν $n > 1$.

Παραδείγματα 14.15. (i) Η ομάδα S_4 δεν μπορεί να έχει υποομάδα τάξης 5.

(ii) Αν $|G| = 9$ και $g \in G$, τότε $o(g) \in \{1, 3, 9\}$.

(iii) Έστω G ομάδα και H, K πεπερασμένες υποομάδες της G με $\mu\kappa\delta(|H|, |K|) = 1$. Τότε $H \cap K = \{1_G\}$. [Υπόδειξη: $H \cap K \leq H$ και $H \cap K \leq K$.]

(iv) Αν $|G| = 105$ και $H \leq G$ με $|H| \geq 36$, τότε $H = G$.

(v) (Μικρό θεώρημα του Fermat.) Αν p είναι πρώτος και $a \in \mathbb{Z}$, τότε $a^p \equiv a \pmod{p}$. [Υπόδειξη: Θέτουμε $G = (\mathbb{Z}_p^*, \cdot)$. Τότε $|G| = p - 1$. Θεωρούμε τις περιπτώσεις $\bar{a} = \bar{0}$ και $\bar{a} \neq \bar{0}$ στο $\mathbb{Z}_p$.]

(vi) Έστω $a, m \in \mathbb{Z}$ με $m > 1$. Αν $\mu\kappa\delta(a, m) = 1$, δείξτε ότι $a^{\phi(m)} \equiv 1 \pmod{m}$. [Υπόδειξη: $|\mathbb{Z}_m^*| = \phi(m)$.]

14.2. Κανονικές υποομάδες, ομάδα πηλίκου

Ορισμός. Μια υποομάδα N της ομάδας G ονομάζεται *κανονική υποομάδα* της G (συμβολισμός: $N \triangleleft G$) αν για κάθε $g \in G$ και για κάθε $n \in N$ έχουμε $g^{-1}ng \in N$.

Παράδειγμα 14.16. Έστω $G = S_3$ και H, K αντίστοιχα τα υποσύνολα $\{(1), (1\ 2)\}$ και $\{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ της G . Προφανώς H, K αποτελούν υποομάδες της G . Παρατηρούμε ότι $(1\ 3)^{-1}(1\ 2)(1\ 3) = (1\ 3)(1\ 2)(1\ 3) = (2\ 3)$ και επομένως H δεν είναι κανονική υποομάδα της G . Ελέγξτε ότι $K \triangleleft G$.

Πρόταση 14.17. Έστω G ομάδα και $N \leq G$. Τότε $N \triangleleft G$ αν, και μόνο αν, $gN = Ng$ για όλα τα $g \in G$.

Απόδειξη. Υποθέτουμε πρώτα ότι $N \triangleleft G$ και ότι $g \in G$. Αν $x \in gN$, τότε $x = gn_1$ για κάποιο $n_1 \in N$. Όμως $gn_1 = (gn_1g^{-1})g = ((g^{-1})^{-1}n_1g^{-1})g \in Ng$. Έπεται ότι $gN \subseteq Ng$. Αν $x \in Ng$, τότε υπάρχει $n_2 \in N$ τέτοιο ώστε $x = g(g^{-1}n_2g)$. Όμως $g^{-1}n_2g \in N$. Άρα $Ng \subseteq gN$.

Υποθέτουμε τώρα ότι $N \leq G$ και ότι $Ng = gN$ για όλα τα $g \in G$. Έστω $n \in N$ και $h \in G$. Αφού $Nh = hN$, έπεται ότι $nh = hn_3$ για κάποιο $n_3 \in N$. Συνεπώς $h^{-1}nh = n_3 \in N$. $\square$

Πρόταση 14.18. Αν $N \triangleleft G$ και $g_1, g_2 \in G$, τότε $(g_1N)(g_2N) = (g_1g_2)N$. [Έχουμε, δηλαδή, ότι το γινόμενο των υποσυνόλων g_1N και g_2N της G έχει ακριβώς τα ίδια στοιχεία με το αριστερό σύμπλοκο $(g_1g_2)N$.]

Απόδειξη. Υποθέτουμε ότι $N \triangleleft G$ και ότι $g_1, g_2 \in G$. Έστω επίσης $x \in (g_1N)(g_2N)$. Τότε $x = g_1n_1g_2n_2$ για κάποια $n_1, n_2 \in N$. Όμως $n_1g_2 = g_2n_3$ για κάποιο $n_3 \in N$ αφού $Ng_2 = g_2N$ (Πρόταση 14.17). Άρα $x = (g_1g_2)(n_3n_2) \in (g_1g_2)N$. Έπεται ότι $(g_1N)(g_2N) \subseteq (g_1g_2)N$. Επιπλέον, αν $y \in (g_1g_2)N$, τότε $y = (g_11_G)(g_2n)$ για κάποιο $n \in N$. Αφού $1_G \in N$, έπεται ότι $y \in (g_1N)(g_2N)$. Συνάγουμε ότι $(g_1g_2)N \subseteq (g_1N)(g_2N)$ και επομένως $(g_1N)(g_2N) = (g_1g_2)N$. $\square$

Παράδειγμα 14.19. Συνεχίζουμε με τον συμβολισμό του Παραδείγματος 14.16. Παρατηρούμε ότι $((1\ 2)H)((1\ 3)H) = \{(1\ 3), (1\ 2\ 3), (1\ 3\ 2), (2\ 3)\} \neq ((1\ 2)(1\ 3))H$. Έχουμε επίσης $(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\} \neq \{(1\ 3), (1\ 3\ 2)\} = H(1\ 3)$.

Ορισμός. Έστω $N \triangleleft G$. Θέτουμε $G/N = \{gN : g \in G\}$. [Έχουμε δηλαδή ότι G/N είναι το σύνολο των διακεκριμένων συμπλόκων της N στην G . (Αφού $N \triangleleft G$ έχουμε ότι $Ng = gN$ για όλα τα $g \in G$.)]

Πρόταση 14.20. Έστω $N \triangleleft G$. Το σύνολο G/N αποτελεί, με πράξη τον πολλαπλασιασμό υποσυνόλων, μια ομάδα.

Απόδειξη. Άμεση συνέπεια της Πρότασης 14.18 και των αντίστοιχων ιδιοτήτων στην ομάδα G . Είναι εύκολο ναδειχθεί ότι 1_GN είναι το μοναδιαίο στοιχείο της G/N , ότι $(gN)^{-1} = g^{-1}N$ για κάθε $g \in G$, όπως επίσης και ο προσεταιρισμός ο οποίος κληρονομείται από τον προσεταιρισμό στην ομάδα G (Λήμμα 14.2). $\square$

Ορισμός. Έστω G ομάδα και $N \triangleleft G$. Η ομάδα G/N (ως προς τον πολλαπλασιασμό υποσυνόλων) καλείται η ομάδα πηλίκο της G διά N .

Πόρισμα 14.21. Έστω G ομάδα πεπερασμένης τάξης και $N \triangleleft G$. Τότε $|G/N| = |G|/|N|$.

[Προσθετικός συμβολισμός.] Έστω A προσθετική ομάδα και $B \leq A$.

$B \triangleleft A$ σημαίνει: $(-a) + b + a \in B$ για κάθε $a \in A$ και για κάθε $b \in B$.

Το αντίστοιχο αριστερό σύμπλοκο του $a \in A$: $a + B = \{a + b : b \in B\}$.

Πρόσθεση στην ομάδα πηλίκου A/B : $(a_1 + B) + (a_2 + B) = (a_1 + a_2) + B$, $(a_1, a_2 \in A)$.

Αν, επιπλέον, A είναι αβελιανή, τότε $B \triangleleft A$ για κάθε υποομάδα B της A . Επομένως, σε τέτοια περίπτωση, η ομάδα A/B πάντα υπάρχει οποτεδήποτε $B \leq A$.]

Παραδείγματα 14.22. (i) Έστω G ομάδα και $H \leq G$ με $[G : H] = 2$. Τότε $H \triangleleft G$.

(ii) Έστω $G = S_3$ και $H = \langle (1\ 2\ 3) \rangle = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$. Προφανώς $[G : H] = 2$, άρα $H \triangleleft G$ από το (i). Έχουμε επίσης ότι η ομάδα G/H έχει τάξη 2 και $G/H = \{(1)H, (1\ 2)H\} = \{1_G H, \alpha H\}$ όπου $\alpha = (1\ 2)$. Παρατηρούμε ότι $(1_G H)(\alpha H) = \alpha H$ και ότι $(\alpha H)(\alpha H) = \alpha^2 H = 1_G H$.

(iii) Έστω $n \geq 2$. Έχουμε τότε ότι $S_n = A_n \cup (1\ 2)A_n$ όπου το σύμπλοκο $(1\ 2)A_n$ είναι ακριβώς το σύνολο των περιττών μεταθέσεων στην S_n . [Υπόδειξη: Αν $\pi \in S_n$ είναι περιττή μετάθεση, τότε $\pi = (1\ 2)(1\ 2)\pi$, όπου $(1\ 2)\pi$ είναι άρτια μετάθεση.] Έπεται ότι $[S_n : A_n] = 2$ και $|A_n| = \frac{1}{2}(n!)$. Επιπλέον, $A_n \triangleleft S_n$.

(iv) Αν $\theta : G \rightarrow H$ είναι ομομορφισμός ομάδων, τότε $\ker \theta \triangleleft G$.

Ορισμός. Έστω G ομάδα. Θέτουμε $R = \{(a, b) \in G \times G : b = g^{-1}ag \text{ για κάποιο } g \in G\}$. [Είναι εύκολο να δείξουμε ότι R είναι μια σχέση ισοδυναμίας στο σύνολο G .]

(i) Οι κλάσεις ισοδυναμίας ως προς την σχέση R καλούνται κλάσεις συζυγίας της G . Έχουμε λοιπόν ότι η κλάση συζυγίας της G που περιέχει το στοιχείο $x \in G$ είναι το υποσύνολο $x^G = \{g^{-1}xg : g \in G\} (= \{gxg^{-1} : g \in G\})$ της G .

(ii) Δυο στοιχεία a, b της G ονομάζονται συζυγή αν υπάρχει $g \in G$ τέτοιο ώστε $b = g^{-1}ag$ (δηλαδή αν $(a, b) \in R$, όπου R είναι η πιο πάνω διμελής σχέση στην G).

Παράδειγμα 14.23. Υπάρχουν ακριβώς 3 (διακεκριμένες) κλάσεις συζυγίας στην S_3 οι οποίες είναι σε αμφιμονοσήμαντη αντιστοιχία με τους τύπους κύκλων των μεταθέσεων στην S_3 . Οι κλάσεις αυτές είναι οι $\{(1)\}$, $\{(1\ 2), (2\ 3), (1\ 3)\}$ και $\{(1\ 2\ 3), (1\ 3\ 2)\}$.

Η πιο κάτω πρόταση είναι άμεση συνέπεια των ορισμών της κανονικής υποομάδας και της κλάσης συζυγίας.

Πρόταση 14.24. Έστω $N \leq G$. Έχουμε τότε ότι $N \triangleleft G$ αν, και μόνο αν, N αποτελείται από την ένωση κλάσεων συζυγίας της G .

Παράδειγμα 14.25. (i) Οι μόνες κανονικές υποομάδες της ομάδας S_3 είναι οι $\{(1)\}$, $\langle (1\ 2\ 3) \rangle (= A_3)$ και S_3 . [Χρησιμοποιούμε το θεώρημα Lagrange και την Πρόταση 14.24.]

(ii) Ελέγξτε ότι $V_4 \triangleleft S_4$ και ότι $V_4 \triangleleft A_4$. Βρείτε ένα σύστημα δεξιών αντιπροσώπων (a) της V_4 στην A_4 , και (b) της V_4 στην S_4 .

Ορισμός. Μια ομάδα $G \neq \{1_G\}$ καλείται απλή, αν οι υποομάδες της $\{1_G\}$ και G είναι οι *μόνες* κανονικές της υποομάδες.

Οι απλές ομάδες είναι τα “δομικά στοιχεία” από τα οποία μπορούν να κατασκευαστούν πιο γενικές ομάδες. Μια χαλαρή αντιστοιχία είναι με τους πρώτους αριθμούς: όπως κάθε ακέραιος αριθμός μπορεί να αναλυθεί σε γινόμενο πρώτων, έτσι και κάθε πεπερασμένη ομάδα μπορεί — μέσω μιας κατάλληλης ακολουθίας κανονικών υποομάδων — να “αναλυθεί” σε απλές ομάδες. Ωστόσο, η αντιστοιχία αυτή είναι σημαντικά πιο περίπλοκη. Στους ακεραίους η παραγοντοποίηση σε πρώτους είναι ουσιαστικά μοναδική. Στις ομάδες, αντίθετα, η “ανάλυση” περνά μέσα από συνθέσεις και πηλίκα, και η δομή που προκύπτει δεν είναι ένα απλό γινόμενο αλλά μια πιο σύνθετη κατασκευή (θεωρία επεκτάσεων).

Παράδειγμα 14.26. (i) Αν $n \geq 3$, τότε $\{(1)\} \neq A_n \triangleleft S_n$. Επομένως S_n δεν είναι απλή.

(ii) $\{(1)\} \triangleleft \{(1), (1\ 2)(3\ 4)\} \triangleleft V_4 (= \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}) \triangleleft A_4$, όμως η υποομάδα $\{(1), (1\ 2)(3\ 4)\}$ της A_4 δεν είναι κανονική στην A_4 . Συμπεραίνουμε ότι (a) A_4 δεν είναι απλή αφού $V_4 \triangleleft A_4$, (b) η σχέση της κανονικότητας δεν είναι μεταβατική.

(iii) Η ομάδα C_p , όπου p πρώτος, είναι απλή.

Πρόταση 14.27. Έστω $n \geq 5$ και έστω $H \triangleleft A_n$. Τότε ισχύουν:

(i) Αν H περιέχει κάποιο 3-κύκλο, τότε $H = A_n$.

(ii) Αν H περιέχει την μετάθεση α , όπου α μπορεί να εκφραστεί ως το γινόμενο δύο αντιμεταθέσεων ξένων μεταξύ τους, τότε $H = A_n$.

Απόδειξη. (i) Έστω ότι $H \triangleleft A_n$ και ότι H περιέχει ένα 3-κύκλο. Έστω $(a\ b\ c) \in H$. Αν x, y, z είναι διακεκριμένα στοιχεία του $\{1, \dots, n\}$ και $\theta \in S_n$ ικανοποιεί $\theta(a) = x$, $\theta(b) = y$, $\theta(c) = z$, έχουμε τότε $\theta(a\ b\ c)\theta^{-1} = (x\ y\ z)$. Αν θ είναι άρτια, $(x\ y\ z) \in H$ αφού $H \triangleleft A_n$. Αν θ είναι περιττή θέτουμε $\pi = (e\ f)$ όπου $1 \leq e, f \leq n$ και $\{e, f\} \cap \{a, b, c\} = \emptyset$. Έχουμε τότε ότι $\theta\pi$ είναι άρτια και $(\theta\pi)(a\ b\ c)(\theta\pi)^{-1} = \theta\pi(a\ b\ c)\pi^{-1}\theta^{-1} = \theta(e\ f)(a\ b\ c)(e\ f)\theta^{-1} = (x\ y\ z)$. Έπεται ότι $(x\ y\ z) \in H$ και επομένως H περιέχει όλους τους 3-κύκλους. Το ζητούμενο είναι τώρα άμεση συνέπεια της Πρότασης 12.21.

(ii) Έστω ότι $H \triangleleft A_n$ και ότι $\alpha = (a_1\ a_2)(a_3\ a_4) \in H$ όπου a_1, a_2, a_3, a_4 είναι διακεκριμένα. Αφού $n \geq 5$, υπάρχει $e \in \{1, 2, \dots, n\} - \{a_1, a_2, a_3, a_4\}$. Θέτουμε $\pi = (a_1\ a_2\ e)$. Τότε $\pi \in A_n$ και $\pi\alpha\pi^{-1} = (a_2\ e)(a_3\ a_4)$, $\pi\alpha\pi^{-1}\alpha^{-1} = (a_2\ e)(a_3\ a_4)(a_1\ a_2)(a_3\ a_4) = (a_1\ e\ a_2)$. Συνεπώς H περιέχει ένα 3-κύκλο και το αποτέλεσμα είναι άμεση συνέπεια του τμήματος (i) πιο πάνω. $\square$

Θεώρημα 14.28. Η ομάδα A_n είναι απλή για $n \geq 5$.

Απόδειξη. Έστω $H \triangleleft A_n$ με $H \neq \{(1)\}$ και έστω $\pi \in H - \{(1)\}$. Υποθέτουμε χωρίς βλάβη της γενικότητας ότι $\pi = \pi_1\pi_2 \dots \pi_r$ όπου $\pi_1, \dots, \pi_r$ είναι κύκλοι ξένοι μεταξύ τους και, επιπλέον, π_i είναι ένας k_i -κύκλος με $k_i \geq 2$ ($1 \leq i \leq r$) και $k_i \geq k_{i+1}$ ($1 \leq i \leq r-1$). Παραμβάλλοντας την Πρόταση 14.27, το ζητούμενο είναι άμεση συνέπεια των παρατηρήσεων (i)–(iv) πιο κάτω:

- (i) $\pi_1 = (a_1 \dots a_m)$ με $m > 3$. Αν $\sigma = (a_1 a_2 a_3)$, τότε $\sigma\pi\sigma^{-1}\pi^{-1} = (a_1 a_2 a_4)$.
- (ii) $\pi_1 = (a_1 a_2 a_3)$ και $\pi_2 = (a_4 a_5 a_6)$. Αν $\tau = (a_2 a_3 a_4)$, τότε $\tau\pi\tau^{-1}\pi^{-1} = (a_1 a_2 a_3 a_4 a_5)$.
- (iii) $\pi_1 = (a_1 a_2 a_3)$ και $\pi_2, \dots, \pi_r$ είναι 2-κύκλοι. Τότε $\pi^2 = (a_1 a_3 a_2)$.
- (iv) $\pi_1 = (a_1 a_2)$ και $\pi_2 = (a_3 a_4)$. Αν $\rho = (a_2 a_3 a_4)$, τότε $\pi^{-1}\rho\pi\rho^{-1} = (a_1 a_4)(a_2 a_3)$. $\square$

Στα αποτελέσματα της επόμενης παραγράφου θα συνδέσουμε διάφορες έννοιες που έχουμε συναντήσει μέχρι τώρα στο κεφάλαιο αυτό.

14.3. Θεωρήματα ομομορφισμών

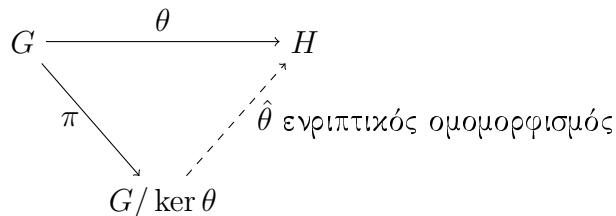
Θεώρημα 14.29. Έστω $\theta: G \rightarrow H$ ομομορφισμός ομάδων. Τότε $G/\ker \theta \cong \text{im}\theta$.

Απόδειξη. Δεχόμαστε την υπόθεση. Θέτουμε $K = \ker \theta$. Έχουμε δει στο Παράδειγμα 14.22(iv) ότι $K \triangleleft G$, άρα μπορούμε να ορίσουμε την ομάδα G/K . Θέτουμε $\hat{\theta}: G/K \rightarrow H : gK \mapsto \theta(g)$, ($g \in G$). Τότε $\hat{\theta}$ είναι καλά ορισμένη και ενριπτική αφού, οποτεδήποτε $g_1, g_2 \in G$, έχουμε $\hat{\theta}(g_1K) = \hat{\theta}(g_2K)$ αν-ν $\theta(g_1) = \theta(g_2)$ αν-ν $1_H = \theta(g_1^{-1}g_2)$ αν-ν $g_1^{-1}g_2 \in K$ αν-ν $g_1K = g_2K$. Παρατηρούμε επίσης ότι $\hat{\theta}$ είναι ομομορφισμός ομάδων αφού $\hat{\theta}((g_1K)(g_2K)) = \hat{\theta}((g_1g_2)K) = \theta(g_1g_2) = \theta(g_1)\theta(g_2) = \hat{\theta}(g_1K)\hat{\theta}(g_2K)$. Επιπλέον, έχουμε ότι $\text{im}\hat{\theta} = \text{im}\theta$. Για να το δούμε αυτό παρατηρούμε ότι $x \in \text{im}\theta$ αν-ν $x = \theta(g)$ για κάποιο $g \in G$ και το τελευταίο ισχύει αν, και μόνο αν, $x = \hat{\theta}(gK)$ για κάποιο $g \in G$ ή, ισοδύναμα, $x \in \text{im}\hat{\theta}$. Συνάγουμε ότι $G/\ker \theta \cong \text{im}\theta$. $\square$

Παραδείγματα 14.30. (i) Έστω $n \in \mathbb{N}$. Θέτουμε $\pi: \mathbb{Z} \rightarrow \mathbb{Z}_n: k \mapsto \bar{k}$ ($k \in \mathbb{Z}$). Τότε π είναι επιρριπτικός ομομορφισμός ομάδων με $\ker \pi = n\mathbb{Z} = \{nr: r \in \mathbb{Z}\}$. Έπεται ότι $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

(ii) Γενικεύοντας το τμήμα (i), έστω G ομάδα και $N \triangleleft G$. Η απεικόνιση $\pi: G \rightarrow G/N : g \mapsto gN$ ($g \in G$) είναι ένας επιρριπτικός ομομορφισμός με $\ker \pi = N$ και ονομάζεται ο **φυσιολογικός ομομορφισμός** της G στην G/N .

Στο πιο κάτω (μεταθετικό) διάγραμμα βλέπουμε την κύρια ιδέα στην απόδειξη του Θεωρήματος 14.29.



(iii) Συμβολίζουμε με $\mathbb{Q}^*$ την πολλαπλασιαστική ομάδα των μη-μηδενικών ρητών και ορίζουμε $\theta: \mathbb{Z} \rightarrow \mathbb{Q}^*$ με $\theta(x) = \begin{cases} 1, & (x \text{ άρτιος}), \\ -1, & (x \text{ περιττός}) \end{cases}$. Έχουμε τότε $\ker \theta = 2\mathbb{Z}$ και

$\text{im}\theta = C_2 = \{-1, 1\}$. Παρατηρούμε ότι $\mathbb{Z}/\ker\theta (= \mathbb{Z}/2\mathbb{Z})$ και $\text{im}\theta$ είναι και οι δύο κυκλικές ομάδες τάξης 2.

(iv) Έστω $\mathbb{R}^*$ η πολλαπλασιαστική ομάδα των μη-μηδενικών πραγματικών. Μπορείτε να βρείτε επιρριπτικό ομομορφισμό ομάδων $\phi: \text{GL}(n, \mathbb{R}) \rightarrow \mathbb{R}^*$ με $\ker\phi = \text{SL}(n, \mathbb{R})$;

Θεώρημα 14.31. Έστω G ομάδα, $H \leq G$ και $N \triangleleft G$. Τότε $HN/N \cong H/H \cap N$.

Απόδειξη. Δεχόμαστε την υπόθεση. Τότε $HN \leq G$ από την Άσκηση 14.15. Προφανώς $N \triangleleft HN$, αφού $N \triangleleft G$, $HN \leq G$ και $N \leq HN$. Θέτουμε $\phi: H \rightarrow HN/N : h \mapsto hN$, $h \in H$. (Προφανώς $hN \in HN/N$, αφού $(hn)N = hN$ για όλα τα $n \in N$.) Αν $h_1, h_2 \in H$, τότε $\phi(h_1h_2) = (h_1h_2)N = (h_1N)(h_2N) = (\phi h_1)(\phi h_2)$, άρα ϕ είναι ομομορφισμός. Επιπλέον, $\text{im}\phi = \{hN : h \in H\} = \{(hk)N : h \in H, k \in N\} = HN/N$ και $\ker\phi = \{h \in H : hN = N\} = \{h \in H : h \in N\} = H \cap N$. Από το Θεώρημα 14.29 έχουμε, $H/H \cap N = H/\ker\phi \cong \text{im}\phi = HN/N$. $\square$

Πόρισμα 14.32. Έστω G ομάδα, $H \leq G$ και $N \triangleleft G$. Τότε $H \cap N \triangleleft H$.

Παράδειγμα. Έστω οι υποομάδες H, N της $\mathbb{Q}^*$ όπου $H = \langle \frac{1}{2} \rangle$ και $N = \{-1, 1\}$. Αφού $\mathbb{Q}^*$ είναι αβελιανή, κάθε υποομάδα της είναι κανονική. Έχουμε $H = \{(\frac{1}{2})^r : r \in \mathbb{Z}\}$, συνεπώς $HN = \{(\frac{1}{2})^r : r \in \mathbb{Z}\} \cup \{- (\frac{1}{2})^r : r \in \mathbb{Z}\}$. Ένα στοιχείο της HN/N είναι ένα σύμπλοκο της μορφής $xN = \{x, -x\}$ όπου $x \in HN$. Έπεται ότι τα στοιχεία της HN/N είναι ακριβώς τα σύμπλοκα $\{(\frac{1}{2})^r, -(\frac{1}{2})^r\}$, όπου $r \in \mathbb{Z}$. Όμως $\{(\frac{1}{2})^r, -(\frac{1}{2})^r\} = (\frac{1}{2})^r N = ((\frac{1}{2})N)^r$ για κάθε $r \in \mathbb{Z}$, άρα $HN/N = \langle (\frac{1}{2})N \rangle$. Παρατηρούμε επίσης ότι $(\frac{1}{2})^r \notin N$ για $r \neq 0$, επομένως HN/N είναι κυκλική άπειρης τάξης. Έχουμε επίσης $H \cap N = \{1\}$, άρα $H/H \cap N \cong H$. Όμως H είναι μια κυκλική ομάδα άπειρης τάξης και με αυτό τον τρόπο έχουμε επαληθεύσει ότι $H/H \cap N \cong HN/N$.

Θεώρημα 14.33. (Θεώρημα αντιστοιχίας) Έστω G, H ομάδες και $\theta: G \rightarrow H$ ένας επιρριπτικός ομομορφισμός. Συμβολίζουμε το σύνολο των υποομάδων της H με $S(H)$ και το σύνολο των υποομάδων της G που περιέχουν το $\ker\theta$ με $S_\theta(G)$. Ορίζουμε $\gamma: S_\theta(G) \rightarrow S(H) : K \mapsto \theta(K) = \{\theta k : k \in K\}$, ($K \in S_\theta(G)$). Τότε γ είναι μια αμφιμονοσήμαντη συνάρτηση. Επιπλέον, αν $K \in S_\theta(G)$, τότε $K \triangleleft G$, αν, και μόνο αν, $\gamma(K) \triangleleft H (= \theta(G) = \gamma(G))$.

Απόδειξη. Δεχόμαστε την υπόθεση. Θα δείξουμε πρώτα ότι γ είναι ενριπτική. Έστω $K_1, K_2 \in S_\theta(G)$ με $\gamma(K_1) = \gamma(K_2)$. Έστω επίσης $k \in K_1$. Τότε $\theta(k) \in \gamma(K_1) = \gamma(K_2)$. Έπεται ότι υπάρχει $l \in K_2$ με $\theta(k) = \theta(l)$. Συνεπώς $\theta(kl^{-1}) = 1_H$, και επομένως $kl^{-1} \in \ker\theta \subseteq K_2$. Αφού $l \in K_2$, συμπεραίνουμε ότι $k \in K_2$, επομένως $K_1 \subseteq K_2$. Επίσης $K_2 \subseteq K_1$ αφού μπορούμε να ανταλλάξουμε τους ρόλους των K_1, K_2 .

Θα δείξουμε τώρα ότι γ είναι επιρριπτική. Έστω $L \in S(H)$. Θέτουμε $K = \{g \in G : \theta(g) \in L\}$. Προφανώς $\ker\theta \subseteq K$ (αφού 1_H είναι στοιχείο της υποομάδας L) και $\theta(K) = L$ (αφού θ είναι επίρριψη). Αρχεί να δείξουμε ότι K είναι υποομάδα της G . Έχουμε ότι $\theta(1_G) = 1_H \in L$, άρα $1_G \in K$. Έστω τώρα $x, y \in K$. Τότε $\theta(x), \theta(y), \theta(y^{-1}) = (\theta y)^{-1}$ είναι όλα στοιχεία της L . Άρα και το $\theta(xy^{-1}) = \theta(x)\theta(y^{-1}) \in L$, επομένως $xy^{-1} \in K$. Συνάγουμε ότι $K \leq G$, άρα $K \in S_\theta(G)$. Έχουμε επίσης $L = \gamma(K)$, άρα γ είναι επίρριψη.

Για να τελειώσουμε την απόδειξη είναι αρκετό να δείξουμε, για $M \in S_\theta(G)$, $J \in S(H)$, ότι (i) $M \triangleleft G \Rightarrow \gamma(M) \triangleleft H$ και (ii) $J \triangleleft H \Rightarrow \gamma^{-1}(J) \triangleleft G$ (όπου $\gamma^{-1}(J)$ ισούται με την αντίστροφη εικόνα $\theta^{-1}(J) = \{g \in G: \theta(g) \in J\}$). Για να αποδείξουμε το τμήμα (i) υποθέτουμε ότι $M \in S_\theta(G)$, $M \triangleleft G$ και ότι $l \in \gamma(M)$, $h \in H$. Υπάρχουν τότε $x \in G$ και $y \in M$ με $h = \theta(x)$ και $l = \theta(y)$. Συνεπώς $h^{-1}lh = (\theta x)^{-1}(\theta y)(\theta x) = \theta(x^{-1}yx) \in \gamma(M)$, αφού $x^{-1}yx \in M$ ($M \triangleleft G$). Άρα $\gamma(M) \triangleleft H$. Για το τμήμα (ii) υποθέτουμε ότι $g \in G$ και $t \in \gamma^{-1}(J)$. Τότε $\theta(t) \in J$ και, αφού $J \triangleleft H$, έχουμε ότι $\theta(g^{-1}tg) = (\theta g)^{-1}(\theta t)(\theta g) \in J$. Συνεπώς $g^{-1}tg \in \gamma^{-1}(J)$, άρα $\gamma^{-1}(J) \triangleleft G$. $\square$

Πόρισμα 14.34. Έστω G ομάδα και $N \triangleleft G$. Τότε

- (i) Κάθε υποομάδα της G/N είναι της μορφής K/N , όπου K είναι υποομάδα της G η οποία περιέχει την N . Επιπλέον, $K/N \triangleleft G/N$ αν, και μόνο αν, $K \triangleleft G$.
- (ii) Αν $H_1/N = H/N$, όπου H_1, H είναι υποομάδες της G που περιέχουν την N , τότε $H_1 = H$.

Πόρισμα 14.35. Έστω $\theta: G \rightarrow K$ ένας επιρριπτικός ομομορφισμός ομάδων. Έστω επίσης $S \leq K$ με $[K : S] = n$ (πεπερασμένος δείκτης). Θέτουμε $H = \{g \in G: \theta(g) \in S\}$. Τότε $[G : H] = n$. (Από την απόδειξη του Θεωρήματος 14.33 ξέρουμε ότι $H \leq G$.)

Απόδειξη. Δεχόμαστε την υπόθεση. Έστω $Sk_1, \dots, Sk_n$, όπου $k_i \in K$, τα διακεκριμένα δεξιά σύμπλοκα της S στην K . Αφού θ είναι επιρριπτική, υπάρχουν $g_1, \dots, g_n \in G$ με $\theta(g_i) = k_i$, $1 \leq i \leq n$. Θα δείξουμε ότι $Hg_1, \dots, Hg_n$ είναι τα διακεκριμένα δεξιά σύμπλοκα της H στην G . Υποθέτουμε πρώτα ότι $Hg_i = Hg_j$, όπου $1 \leq i, j \leq n$. Έχουμε τότε ότι $g_i g_j^{-1} \in H$. Έπεται ότι $(\theta g_i)(\theta g_j)^{-1} = \theta(g_i g_j^{-1}) \in S$, δηλαδή $k_i k_j^{-1} \in S$. Συμπεραίνουμε ότι $Sk_i = Sk_j$ και επομένως $i = j$. Έστω τώρα $g \in G$. Τότε $\theta(g) \in K$, συνεπώς $\theta(g) \in Sk_i$ για κάποιο i με $1 \leq i \leq n$. Έπεται ότι $\theta(g) = sk_i$ με $s \in S$. Θέτουμε $x = gg_i^{-1}$. Τότε $\theta(x) = (\theta g)(\theta g_i)^{-1} = sk_i k_i^{-1} = s \in S$. Συνεπώς $gg_i^{-1} = x \in H$. Αυτό σημαίνει ότι $g \in Hg_i$. (Έχουμε δείξει ότι τα $Hg_1, \dots, Hg_n$ είναι διακεκριμένα και κάθε στοιχείο $g \in G$ ανήκει σε κάποιο από αυτά τα δεξιά σύμπλοκα.) $\square$

Παράδειγμα. Έστω $\theta: G \rightarrow K$ επιρριπτικός ομομορφισμός ομάδων, όπου K είναι κυκλική τάξης 10. Θα δείξουμε ότι G έχει κανονικές υποομάδες με δείκτη 2, 5, και 10:

Έστω $K = \langle x \rangle$, όπου $x \in K$. Τότε $K_1 = \{1_K\}$, $K_2 = \langle x^5 \rangle$, $K_3 = \langle x^2 \rangle$ είναι κανονικές υποομάδες της K με δείκτη 10, 5, 2 αντίστοιχα. Έπεται ότι οι αντίστροφες εικόνες τους μέσω του ομομορφισμού θ είναι κανονικές υποομάδες της G με δείκτη 10, 5, 2 αντίστοιχα. (Χρησιμοποιούμε το Θεώρημα 14.33 και το Πόρισμα 14.35)

Θεώρημα 14.36. Έστω G ομάδα και $N \triangleleft G$. Αν στην ομάδα πηλίκο G/N υπάρχει μια κανονική υποομάδα M/N , $M \supseteq N$, τότε $M \triangleleft G$ και $G/M \cong (G/N)/(M/N)$.

Απόδειξη. Έστω $\pi: G \rightarrow G/N$, ο φυσιολογικός ομομορφισμός της G στην G/N . Έστω επίσης $\rho: G/N \rightarrow (G/N)/(M/N)$ ο φυσιολογικός ομομορφισμός της G/N στην $(G/N)/(M/N)$. Θέτουμε $\theta = \rho \circ \pi$. Τότε $\theta: G \rightarrow (G/N)/(M/N)$ είναι ένας επιρριπτικός

ομομορφισμός. Συνεπώς $G/\ker\theta \cong (G/N)/(M/N)$. Θα δείξουμε ότι $M = \ker\theta$. Παρατηρούμε ότι το μοναδιαίο στοιχείο της $(G/N)/(M/N)$ είναι το M/N . Συνεπώς $\ker\theta = \{g \in G : (gN)(M/N) = M/N\}$. Όμως $(gN)(M/N) = M/N$ αν-ν $gN \in M/N$ αν-ν $gN = mN$ για κάποιο $m \in M$, και το τελευταίο ισχύει αν-ν $m^{-1}g \in N \subseteq M$ (όπου $m \in M$). Συνάγουμε ότι $g \in \ker\theta$ αν-ν $g \in M$ όπως ήταν το ζητούμενο. $\square$

Ασκήσεις

- 14.1 (i) Έστω G ομάδα και $H \leq G$. Θεωρούμε την διμελή σχέση R στην G όπου $R = \{(a, b) \in G \times G : ab^{-1} \in H\}$. Δείξτε ότι R είναι μια σχέση ισοδυναμίας στην G . Ποιά είναι η αντίστοιχη διαμέριση της G ;
- (ii) Βρείτε τις αντίστοιχες κλάσεις ισοδυναμίας στην περίπτωση που $G = C_{12}$ και $H = C_4$. (Συγκρίνετε με την Άσκηση 11.9.)
- 14.2 (i) Έστω $x, y \in S_n$. Δείξτε ότι x και y είναι συζυγή αν, και μόνο αν, x και y έχουν τον ίδιο τύπο κύκλων.
- (ii) Βρείτε ένα αντιπρόσωπο από κάθε κλάση συζυγίας της S_4 και όλες τις κανονικές υποομάδες της S_4 .
- 14.3 Συμπληρώστε τους συλλογισμούς στα Παραδείγματα 14.22, 14.25 και 14.30.
- 14.4 Έστω G ομάδα και $H \leq G$ με $[G : H] = 2$. Αν $g \in G$, δείξτε ότι $g^2 \in H$.
- 14.5 (Θεώρημα Cauchy.) Έστω G μια πεπερασμένη ομάδα και p πρώτος αριθμός με $p \mid |G|$. Τότε G περιέχει στοιχείο τάξης p .
- [Υπόδειξη: Θέτουμε $L = \{(g_1, g_2, \dots, g_p) : g_1 g_2 \dots g_p = 1_G\} \subseteq G^p$. Ορίζουμε $\pi \in \text{Sym}(L)$ με $\pi(g_1, g_2, \dots, g_p) = (g_2, \dots, g_p, g_1)$. (Δείξτε ότι πράγματι π είναι στοιχείο του συνόλου $\text{Sym}(L)$.) Βρίσκουμε τώρα μια πλήρη παραγοντοποίηση της π στο L ως γινόμενο κύκλων ξένων μεταξύ τους. Δείξτε τα πιο κάτω:
- (i) Αν $g^p = 1_G$ για κάποιο $g \in G$, τότε $(g, g, \dots, g) \in L$ και το στοιχείο αυτό σταθεροποιείται από την π .
- (ii) Όλα τα υπόλοιπα στοιχεία του L περιέχονται σε p -κύκλους στην πιο πάνω παραγοντοποίηση της π .
- (iii) Το σύνολο L έχει ακριβώς $|G|^{p-1}$ στοιχεία.]
- 14.6 Έστω $a, c \in O(\mathbb{R}^2)$ όπου $a = \text{rot}_{\pi/3}$ και $c = \text{ref}_{\pi/3}$.
- (i) Δείξτε ότι $\{a, c\} \subseteq D_{12}$ και ότι $\langle a \rangle \triangleleft \langle a, c \rangle$.
- (ii) Δείξτε ότι $D_{12} = \langle a, c \rangle$ και βρείτε τα σύμπλοκα της $\langle a \rangle$ στην D_{12} .
- (iii) Μπορείτε να βρείτε $x, y \in \langle a, c \rangle$ τέτοια ώστε $o(x) = 2$, $o(y) = 2$ και $\langle a, c \rangle = \langle x, y \rangle$;
- 14.7 Έστω $\alpha, \beta \in S_6$ όπου $\alpha = (1\ 2\ 3\ 4\ 5\ 6)$ και $\beta = (2\ 6)(3\ 5)$. Θέτουμε $H_1 = \langle \alpha, \beta \rangle$ και $H_2 = \langle \alpha^2, \beta \rangle$.
- (i) Εκφράστε τα γινόμενα α^6 , β^2 , $\alpha\beta$, $\beta\alpha^{-1}$ ως γινόμενα κύκλων ξένων μεταξύ τους. Βρείτε επίσης τα σύμπλοκα της $\langle a \rangle$ στην H_1 .
- (ii) Δείξτε ότι $D_{12} \cong H_1$.
- (iii) Δείξτε ότι υπάρχει επιρριπτικός ομομορφισμός ομάδων $\phi : D_{12} \rightarrow H_2$. Είναι οι ομάδες D_{12} και H_2 ισομορφικές;
- 14.8 Έστω G ομάδα και $x, y \in G$. Δείξτε τα πιο κάτω
- (i) $x, x^{-1}, y^{-1}xy$ έχουν την ίδια τάξη, και
- (ii) xy, yx έχουν την ίδια τάξη.

- 14.9 Βρείτε, ως προς ισομορφισμό, όλες τις ομάδες G με $1 \leq |G| \leq 7$ και $|G| = 10$.
- 14.10 Δείξτε ότι $D_{12} \cong D_6 \times C_2$.
- 14.11 Έστω $G = \langle x, y \rangle$ (όπου $x, y \in G$). Αν $x^6 = 1_G$, $y^2 = 1_G$, $xy = yx^{-1}$ και $x^k \neq 1_G$ αν $k \in \{1, 2, 3, 4, 5\}$, δείξτε ότι $G \cong D_{12}$.
- 14.12 Έστω $G \leq S_n$ και ότι G δεν περιέχεται στην A_n . Δείξτε ότι $G \cap A_n \triangleleft G$ και ότι $[G : G \cap A_n] = 2$.
- 14.13 Αν H είναι μια πεπερασμένη υποομάδα μιας πολλαπλασιαστικής ομάδας των μη-μηδενικών μιγαδικών αριθμών, δείξτε ότι H είναι κυκλική.
- 14.14 Έστω G ομάδα και H, K υποομάδες της G . Δείξτε ότι $HK \leq G$ αν και μόνο αν $HK = KH$.
- 14.15 Έστω G ομάδα και $H \leq G$, $K \triangleleft G$. Δείξτε τα πιο κάτω:
(i) $HK \leq G$, (ii) $HK = \langle H \cup K \rangle = KH$, και (iii) αν $H \triangleleft G$, τότε $HK \triangleleft G$.
- 14.16 Έστω $G = \langle a \rangle$, όπου $o(a) = 12$ και $K = \langle b \rangle$, όπου $o(b) = 4$. Δείξτε ότι $\theta: G \rightarrow K : a^i \mapsto b^i$ ($0 \leq i \leq 11$) είναι ένας επιρριπτικός ομομορφισμός, και για κάθε υποομάδα K_1 της K βρείτε υποομάδα G_1 της G που περιέχει το $\ker \theta$ με $\theta(G_1) = K_1$.
- 14.17 Έστω G ομάδα. Αν $H \leq G$ και M, N κανονικές υποομάδες της G με $H \cap M = H \cap N$, δείξτε ότι $HN/N \cong HM/M$.

15. Δακτύλιοι και σώματα

15.1. Ορισμοί, παραδείγματα, βασικές ιδιότητες

Ορισμός. Δακτύλιος είναι μια (διατεταγμένη) τριάδα $(R, +, \cdot)$ που αποτελείται από ένα μη-κενό σύνολο R που είναι εφοδιασμένο με δύο διμελείς πράξεις, πρόσθεση $+: R \times R \rightarrow R: (r, r') \mapsto r + r'$, και πολλαπλασιασμό $\cdot: R \times R \rightarrow R: (r, r') \mapsto rr'$, έτσι ώστε:

- (i) $(R, +)$ αποτελεί μια αβελιανή ομάδα,
- (ii) $a(bc) = (ab)c$ για όλα τα $a, b, c \in R$, και
- (iii) $(a + b)c = ac + bc$ και $c(a + b) = ca + cb$ για όλα τα $a, b, c \in R$.

Σημείωση. (i) Από την Πρόταση 4.3, το ουδέτερο στοιχείο του R ως προς την πρόσθεση είναι μοναδικό. Το συμβολίζουμε με 0_R . Επίσης, από την Πρόταση 4.7, αν $r \in R$, τότε r έχει μοναδικό συμμετρικό ως προς την πρόσθεση, το οποίο ονομάζουμε *αντίθετο* του r και συμβολίζουμε με $-r$. (Έχουμε δηλαδή $r + -r = 0_R = -r + r$.)

(ii) Ειδικές περιπτώσεις της Πρότασης 5.5: Σε ένα δακτύλιο R , το άθροισμα $a_1 + \dots + a_n$ και το γινόμενο $a_1 \dots a_n$ οποιουδήποτε πεπερασμένου πλήθους στοιχείων $a_1, \dots, a_n \in R$ είναι ανεξάρτητο από το που τοποθετούνται οι παρενθέσεις.

(iii) Πιο κάτω, για συντομία, θα χρησιμοποιούμε την ορολογία “ο δακτύλιος R ” και θα υπονοούμε τις πράξεις.

Παραδείγματα 15.1. (i) Τα σύνολα $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ και $2\mathbb{Z} (= \{2k: k \in \mathbb{Z}\})$, ως προς την συνηθισμένη πρόσθεση και πολλαπλασιασμό, είναι δακτύλιοι. Δεν συμβαίνει όμως το ίδιο με το σύνολο $\mathbb{N}$. Επίσης το σύνολο $\mathbb{Z}_n$, ως προς την πρόσθεση και πολλαπλασιασμό που έχουμε ορίσει πάνω σε αυτό, είναι ένας δακτύλιος για κάθε $n \in \mathbb{N}$.

(ii) Έστω S ένα μη-κενό σύνολο. Στο $\mathcal{P}(S)$, το δυναμοσύνολο του S , ορίζουμε $\oplus$ και $\odot$ με $A \oplus B = (A \cup B) - (A \cap B)$ και $A \odot B = A \cap B$. Τότε η τριάδα $(\mathcal{P}(S), \oplus, \odot)$ αποτελεί δακτύλιο (κοιτάξτε την Άσκηση 15.1) ο οποίος καλείται δακτύλιος Boole. Αν ορίσουμε $\boxplus$ με $A \boxplus B = A \cup B$, είναι η τριάδα $(\mathcal{P}(S), \boxplus, \odot)$ ένας δακτύλιος;

(iii) Συμβολίζουμε με $\text{End}(\mathbb{R}^{n \times 1})$ το σύνολο όλων των συναρτήσεων $f: \mathbb{R}^{n \times 1} \rightarrow \mathbb{R}^{n \times 1}$ οι οποίες ικανοποιούν $f(u + v) = f(u) + f(v)$ και $f(\lambda u) = \lambda f(u)$ για όλα τα $u, v \in \mathbb{R}^{n \times 1}$ και όλα τα $\lambda \in \mathbb{R}$. Για $g, h \in \text{End}(\mathbb{R}^{n \times 1})$ ορίζουμε $g + h$ με $(g + h)(u) = g(u) + h(u)$ για όλα τα $u \in \mathbb{R}^{n \times 1}$, και $g \cdot h = g \circ h$ (σύνθεση συναρτήσεων). Δείξτε ότι $+, \cdot$ όπως τις έχουμε ορίσει αποτελούν διμελείς πράξεις στο σύνολο $\text{End}(\mathbb{R}^{n \times 1})$ και εξετάστε κατά πόσον η τριάδα $(\text{End}(\mathbb{R}^{n \times 1}), +, \cdot)$ αποτελεί δακτύλιο.

(iv) Στο σύνολο $\mathbb{R}^3$ ορίζουμε $\mathbf{x} \wedge \mathbf{y} = (x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1)$ και $\mathbf{x} + \mathbf{y} = (x_1 + y_1, x_2 + y_2, x_3 + y_3)$ όπου $\mathbf{x}, \mathbf{y} \in \mathbb{R}^3$ με $\mathbf{x} = (x_1, x_2, x_3)$ και $\mathbf{y} = (y_1, y_2, y_3)$. Τότε η τριάδα $(\mathbb{R}^3, +, \wedge)$ δεν αποτελεί δακτύλιο αφού $\wedge$ δεν ικανοποιεί την προσεταιριστική ιδιότητα $(\mathbf{i} \wedge (\mathbf{i} \wedge \mathbf{j})) \neq (\mathbf{i} \wedge \mathbf{i}) \wedge \mathbf{j}$. Εδώ έχουμε μια άλγεβρα Lie που είναι ένα παράδειγμα ενός “μη-προσεταιριστικού δακτυλίου”.

Λήμμα 15.2. Έστω R δακτύλιος. Τότε για κάθε $r \in R$ ισχύει ότι $0_R \cdot r = 0_R = r \cdot 0_R$.

Απόδειξη. Έστω $r \in R$. Η επιμεριστική ιδιότητα δίνει $0_R r = (0_R + 0_R)r = 0_R r + 0_R r$. Προσθέτοντας το αντίθετο του $0_R r$ και στα δύο μέλη της πιο πάνω ισότητας, προκύπτει ότι $0_R = 0_R r$. (Παρόμοια για το $r 0_R = 0_R$.) $\square$

Ορισμός. Ένας δακτύλιος R ονομάζεται 1-δακτύλιος αν υπάρχει στοιχείο $1_R \in R$ με $1_R \neq 0_R$ τέτοιο ώστε $a 1_R = a = 1_R a$ για όλα τα $a \in R$. Το στοιχείο 1_R ονομάζεται τότε ουδέτερο ως προς τον πολλαπλασιασμό ή μοναδιαίο στοιχείο του R . [Αν R είναι ένας 1-δακτύλιος, τότε το ουδέτερο στοιχείο ως προς τον πολλαπλασιασμό στον R είναι μοναδικό (κοιτάζτε την Πρόταση 4.3).]

Πρόταση 15.3. Έστω R ένας 1-δακτύλιος. Τότε

- (i) Για κάθε στοιχείο $r \in R$ ισχύει ότι $-r = (-1_R) \cdot r$.
- (ii) Για κάθε $r \in R$ ισχύει ότι $(-1_R)(-r) = r$ (πιο ειδικά, $(-1_R)(-1_R) = 1_R$).

Απόδειξη.

(i) Αν $r \in R$, έχουμε ότι $0_R \cdot r = 0_R = (1_R + (-1_R)) \cdot r = r + (-1_R)r$. Προσθέτουμε τώρα $-r$ και στα δυο μέλη της εξίσωσης.

(ii) Αν $r \in R$, έχουμε ότι $0_R = 0_R(-r) = (-1_R + 1_R)(-r) = (-1_R)(-r) + (-r)$. $\square$

Ορισμός. Έστω R ένας 1-δακτύλιος. Αν για κάθε $a \in R - \{0_R\}$ υπάρχει $b \in R$ τέτοιο ώστε $ab = 1_R = ba$, τότε R καλείται δακτύλιος διαίρεσης.

Ορισμός. Ένας δακτύλιος R ονομάζεται μεταθετικός αν $ab = ba$ για όλα τα $a, b \in R$.

Ορισμός. Σώμα είναι ένας μεταθετικός δακτύλιος διαίρεσης.

Παραδείγματα 15.4. (i) Οι δακτύλιοι $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (ως προς τη συνηθισμένη πρόσθεση και πολλαπλασιασμό) είναι μεταθετικοί 1-δακτύλιοι. Επιπλέον, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ είναι σώματα, όμως $\mathbb{Z}$ δεν είναι σώμα (για παράδειγμα δεν υπάρχει ακέραιος a τέτοιος ώστε $2a = 1$). Ο δακτύλιος $2\mathbb{Z}$ είναι μεταθετικός αλλά δεν είναι ένας 1-δακτύλιος αφού δεν υπάρχει άρτιος ακέραιος e που να ικανοποιεί $ae = a$ για όλα τα $a \in 2\mathbb{Z}$.

(ii) Ο δακτύλιος $\mathbb{Z}_n$ ($n > 1$), ως προς την πρόσθεση και πολλαπλασιασμό που έχουμε ορίσει, είναι ένας μεταθετικός 1-δακτύλιος.

(iii) **Δακτύλιοι πινάκων.** Έστω R ένας 1-δακτύλιος. Συμβολίζουμε με $M_n(R)$ το σύνολο των $n \times n$ πινάκων με συντελεστές από τον R . Τότε $M_n(R)$ αποτελεί 1-δακτύλιο ως προς την συνηθισμένη πρόσθεση και πολλαπλασιασμό πινάκων. [Αν $A, B \in M_n(R)$ όπου $A = (a_{ij})$ και $B = (b_{ij})$, τότε $A + B = C = (c_{ij})$ όπου $c_{ij} = a_{ij} + b_{ij}$ και $AB = D = (d_{ij})$ όπου $d_{ij} = \sum_{k=1}^n a_{ik}b_{kj}$.]

Ακόμη και στην περίπτωση που ο δακτύλιος R είναι μεταθετικός, ο δακτύλιος $M_n(R)$ δεν είναι μεταθετικός όταν $n > 1$. [Εξήγηση: Έστω $E_{ij} \in M_n(R)$ ο πίνακας του οποίου όλοι οι συντελεστές ισούνται με 0_R εκτός από τον (i, j) -συντελεστή που ισούται με 1_R . Τότε $E_{12}E_{21} = E_{11}$ και $E_{21}E_{12} = E_{22}$.]

Ορισμός. Έστω R ένας 1-δακτύλιος. Ένα στοιχείο $u \in R$ ονομάζεται *αντιστρέψιμο* αν υπάρχει $v \in R$ με $uv = 1_R = vu$. Σε τέτοια περίπτωση λέμε ότι v είναι ένα *αντίστροφο* του u . Το σύνολο των αντιστρέψιμων στοιχείων του R συμβολίζεται με R^* .

[Σημείωση στον πιο πάνω ορισμό. (i) Από την Πρόταση 4.7, αν το στοιχείο $u \in R$ είναι αντιστρέψιμο, τότε u έχει μοναδικό αντίστροφο στον R . Σε τέτοια περίπτωση συμβολίζουμε το αντίστροφο του u με u^{-1} .

(ii) Στην περίπτωση που $R = \mathbb{Z}_n$ ($n > 1$), ο ορισμός του R^* και ο ορισμός του αντιστρέψιμου στοιχείου του R που έχουμε μόλις δώσει συμπίπτει αντίστοιχα με τον ορισμό του $\mathbb{Z}_n^*$ και τον ορισμό του αντιστρέψιμου στοιχείου του $\mathbb{Z}_n$ που έχουμε δώσει στο Κεφάλαιο 10.]

Παρατήρηση 15.5. (i) Σώμα είναι ένας μεταθετικός 1-δακτύλιος στον οποίο κάθε μη-μηδενικό στοιχείο είναι αντιστρέψιμο.

(ii) Σε ένα σώμα υπάρχουν τουλάχιστον δύο στοιχεία, τα στοιχεία $0 (= 0_F)$ και $1 (= 1_F)$ όπου $0 \neq 1$. Το 0 είναι το ουδέτερο ως προς την πρόσθεση και το 1 είναι το ουδέτερο ως προς τον πολλαπλασιασμό.

Ορισμός. Έστω R μεταθετικός 1-δακτύλιος. Λέμε ότι R είναι *ακέραια περιοχή* αν το γινόμενο δύο μη-μηδενικών στοιχείων του R είναι και πάλι ένα μη-μηδενικό στοιχείο.

Παράδειγμα. (i) Ο δακτύλιος $\mathbb{Z}$ είναι ακέραια περιοχή.

(ii) Κάθε σώμα F είναι ακέραια περιοχή. [Εξήγηση: Έστω $a, b \in F$ με $ab = 0_F$. Αν $b \neq 0_F$, τότε υπάρχει $c \in F$ με $bc = 1_F$. Έχουμε τότε $0_F = 0_Fc = (ab)c = a(bc) = a1_F = a$.]

Το αντίστροφο δεν ισχύει γενικά αφού υπάρχουν ακέραιες περιοχές που δεν είναι σώματα (για παράδειγμα ο δακτύλιος $\mathbb{Z}$ είναι ακέραια περιοχή αλλά δεν είναι σώμα).

(iii) Ο δακτύλιος $\mathbb{Z}_6$ δεν είναι ακέραια περιοχή αφού $\bar{2} \neq \bar{0}$ και $\bar{3} \neq \bar{0}$, ενώ $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$.

Πρόταση 15.6. Έστω $n \in \mathbb{N}$. Ο δακτύλιος $\mathbb{Z}_n$ είναι σώμα αν, και μόνο αν, n είναι πρώτος.

Απόδειξη. Έστω $n \in \mathbb{N}$. Υποθέτουμε πρώτα ότι ο δακτύλιος $\mathbb{Z}_n$ είναι σώμα. Προχωρούμε με απαγωγή σε άτοπο και υποθέτουμε ότι ο φυσικός n δεν είναι πρώτος. Τότε είτε $n = 1$ ή $n = kl$ όπου $k, l \in \mathbb{N}$ με $1 < k, l < n$. Όμως $n \neq 1$ αφού $\mathbb{Z}_1$ δεν είναι σώμα όπως έχουμε δει (έχουμε ότι $\bar{0} = \bar{1}$ στο $\mathbb{Z}_1$). Επομένως $n = kl$ με k, l όπως πιο πάνω. Έπεται

ότι $\bar{k}\bar{l} = \bar{n} = \bar{0}$ στο $\mathbb{Z}_n$ με $\bar{k} \neq \bar{0}$ και $\bar{l} \neq \bar{0}$, που είναι άτοπο αφού κάθε σώμα είναι ακέραια περιοχή. Συνάγουμε ότι n είναι πρώτος. Έστω τώρα ότι n είναι πρώτος (πιο ειδικά $n > 1$). Τότε $\mathbb{Z}_n^* = \{\bar{1}, \bar{2}, \dots, \overline{n-1}\}$ αφού $\mu\kappa\delta(a, n) = 1$ για όλα τα $a \in \mathbb{Z}$ με $1 \leq a \leq n-1$. Έπεται ότι κάθε μη-μηδενικό στοιχείο του μεταθετικού 1-δακτυλίου $\mathbb{Z}_n$ είναι αντιστρέψιμο. Συμπεραίνουμε ότι $\mathbb{Z}_n$ είναι σώμα. $\square$

Ορισμός. Έστω R δακτύλιος. Ένας υποδακτύλιος του R είναι ένα υποσύνολο S του R το οποίο αποτελεί δακτύλιο ως προς την ίδια πρόσθεση και τον ίδιο πολλαπλασιασμό του R .

Πρόταση 15.7. Έστω S ένα μη-κενό υποσύνολο του δακτυλίου R . Υποθέτουμε επιπλέον ότι $a + b, ab, -a \in S$ οποτεδήποτε $a, b \in S$. Τότε S είναι υποδακτύλιος του R .

Απόδειξη. Η υπόθεση που έχουμε κάνει μας εξασφαλίζει ότι η πρόσθεση και ο πολλαπλασιασμός του R αποτελούν διμελείς πράξεις στο S . Έστω $t \in S$, ($S \neq \emptyset$). Τότε $-t \in S$ και $t + (-t) \in S$ από την υπόθεση μας, και επομένως $0_R \in S$. Οι υπόλοιπες ιδιότητες κληρονομούνται από τον R . $\square$

Παράδειγμα 15.8. (i) Για $m \in \mathbb{Z}$ θέτουμε $m\mathbb{Z} = \{mk : k \in \mathbb{Z}\}$. Τότε $m\mathbb{Z}$ αποτελεί υποδακτύλιο του $\mathbb{Z}$.

(ii) Δείξτε ότι κάθε υποδακτύλιος του δακτυλίου $\mathbb{Z}$ των ακεραίων είναι της μορφής $m\mathbb{Z}$ για κάποιο $m \in \mathbb{Z}$. (Υπόδειξη: Αν S είναι υποδακτύλιος του $\mathbb{Z}$, τότε $(S, +)$ αποτελεί κυκλική υποομάδα της $(\mathbb{Z}, +)$.)

Άσκηση. Θέτουμε $\omega = i\sqrt{5} \in \mathbb{C}$. Θέτουμε επίσης $R = \{z \in \mathbb{C} : z = a + b\omega \text{ για κάποια } a, b \in \mathbb{Z}\}$. Δείξτε ότι (i) R είναι υποδακτύλιος του $\mathbb{C}$, και (ii) ο δακτύλιος R είναι ακέραια περιοχή. Βρείτε επίσης τα στοιχεία του R^* .

Ορισμός. Έστω F σώμα.

- (i) Ένα υπόσωμα του F είναι ένα υποσύνολο K του F το οποίο αποτελεί σώμα ως προς την ίδια πρόσθεση και τον ίδιο πολλαπλασιασμό του F .
- (ii) Αν L είναι υπόσωμα του F , τότε λέμε επίσης ότι F είναι μια επέκταση του σώματος L .

Παρατήρηση 15.9. (i) Έστω S υποδακτύλιος του δακτυλίου R . Τότε $0_S = 0_R$. Επιπλέον, αν $a \in S$, τότε $(-a)_S = (-a)_R$.

(ii) Έστω T υπόσωμα του σώματος F . Έχουμε τότε ότι $1_T = 1_F$ και ότι, για $a \in T - \{0_F\}$, $(a^{-1})_T = (a^{-1})_F$.

(iii) Έστω F σώμα και K ένα υπόσωμα του F . Τότε $(K, +)$ είναι υποομάδα της $(F, +)$ και $(K^*, \cdot)$ είναι υποομάδα της $(F^*, \cdot)$. [Προφανώς $K^* \subseteq F^*$ αφού $0_F = 0_K$ από το (i) πιο πάνω.]

Άσκηση. Εξετάστε κατά πόσον $S = \{z \in \mathbb{C} : z = a + ib \text{ για κάποια } a, b \in \mathbb{Q}\}$ αποτελεί υπόσωμα του $\mathbb{C}$.

Ορισμός. Έστω R μια ακέραια περιοχή.

(i) Μια *Ευκλείδεια συνάρτηση* στην R είναι μια συνάρτηση $\delta: R - \{0_R\} \rightarrow \mathbb{N} \cup \{0\}$ η οποία ικανοποιεί

(a) $\delta(ab) \geq \delta(a)$ οποτεδήποτε $a, b \in R - \{0_R\}$, και

(b) αν $a, b \in R$ με $b \neq 0_R$, τότε υπάρχουν $q, r \in R$ με $a = qb + r$ και είτε $r = 0$, είτε $\delta(r) < \delta(b)$.

(ii) R καλείται *Ευκλείδεια περιοχή* (ΕΠ), αν υπάρχει μια Ευκλείδεια συνάρτηση στην R .

Παράδειγμα. Η ακέραια περιοχή $\mathbb{Z}$ είναι Ευκλείδεια περιοχή. Θέτουμε $\delta(a) = |a|$ αν $a \in \mathbb{Z} - \{0\}$. Αν $b \neq 0$ τότε $\delta(ab) = |ab| = |a||b| = \delta(a)\delta(b) \geq \delta(a)$, αφού $\delta(b) \geq 1$. Για το (b) υποθέτουμε ότι $b \in \mathbb{Z} - \{0\}$. Αν $b > 0$, το θεώρημα διαίρεσης μας εξασφαλίζει ότι υπάρχουν $q, r \in \mathbb{Z}$ με $a = qb + r$ και είτε $r = 0$ ή $0 < r < b$ (όμως $\delta(r) < \delta(b)$ αν $0 < r < b$). Αν $b < 0$ τότε (θεώρημα διαίρεσης με $-b > 0$) υπάρχουν $q', r' \in \mathbb{Z}$ με $a = q'(-b) + r'$ όπου είτε $r' = 0$ ή $0 < r' < -b$ (όμως αν $0 < r' < -b$ έχουμε $\delta(r') = r' < -b = |b| = \delta(b)$).

15.2. Ομομορφισμοί δακτυλίων

Ορισμός. Έστω R, S δακτύλιοι. Μια συνάρτηση $\phi: R \rightarrow S$ καλείται *ομομορφισμός δακτυλίων* αν, για όλα τα $r, s \in R$, ισχύουν

(i) $\phi(r + s) = \phi(r) + \phi(s)$, και (ii) $\phi(rs) = \phi(r)\phi(s)$.

[Σημειώστε ότι η πρόσθεση και ο πολλαπλασιασμός στην αριστερή πλευρά αυτών των εξισώσεων είναι οι πράξεις στον δακτύλιο R , ενώ αυτές στα δεξιά είναι οι πράξεις στον S .]

Ένας ομομορφισμός δακτυλίων που επιπλέον είναι μια αμφιμονοσήμαντη συνάρτηση ονομάζεται *ισομορφισμός δακτυλίων*. Αν υπάρχει ισομορφισμός από τον δακτύλιο R στον δακτύλιο S , τότε λέμε ότι οι δακτύλιοι R και S είναι *ισομορφικοί* (συμβολισμός: $R \cong S$). Σε τέτοια περίπτωση οι R και S έχουν την ίδια δομή ως δακτύλιοι.

Παρατήρηση 15.10. Έστω $\phi: R \rightarrow S$ ομομορφισμός δακτυλίων. Τότε ϕ αποτελεί ομομορφισμό ομάδων $(R, +) \rightarrow (S, +)$. Έπεται ότι $\phi(0_R) = 0_S$ και $\phi(-r) = -\phi(r)$ για όλα τα $r \in R$ (Πρόταση 13.5).

Παράδειγμα 15.11. (i) Έστω $\phi: \mathbb{Z} \rightarrow \mathbb{Z}$ ένας ομομορφισμός δακτυλίων. Τότε $\phi(1) = n$ για κάποιο $n \in \mathbb{Z}$. Έπεται ότι $\phi(m) = mn$ για κάθε $m \in \mathbb{Z}$ (συγκρίνετε με την Άσκηση 12.4(i)). Όμως $n = \phi(1) = \phi(1^2) = \phi(1)\phi(1) = n^2$. Συνάγουμε ότι $n \in \{0, 1\}$, και επομένως $\theta_0: m \mapsto 0$, ($m \in \mathbb{Z}$) και $\theta_1: m \mapsto m$, ($m \in \mathbb{Z}$), είναι οι μόνοι ομομορφισμοί δακτυλίων $\mathbb{Z} \rightarrow \mathbb{Z}$. (Ελέγξτε ότι πράγματι θ_0, θ_1 είναι ομομορφισμοί δακτυλίων $\mathbb{Z} \rightarrow \mathbb{Z}$.)

(ii) Έστω R, S 1-δακτύλιοι και $\phi: R \rightarrow S$ ομομορφισμός δακτυλίων. Αν ϕ είναι επιρριπτικός, τότε $\phi(1_R) = 1_S$. [Εξήγηση: Αφού ϕ είναι επιρριπτικός, υπάρχει $r \in R$ με $\phi(r) = 1_S$. Έχουμε τότε, $1_S = \phi(r) = \phi(r1_R) = \phi(r)\phi(1_R) = 1_S\phi(1_R) = \phi(1_R)$.] Πιο ειδικά, αν R, S είναι σώματα και $\phi: R \rightarrow S$ ένας ισομορφισμός δακτυλίων, τότε $\phi(1_R) = 1_S$.

Σημείωση. (i) Αν $\phi: R \rightarrow S$ και $\psi: S \rightarrow T$ είναι ομομορφισμοί δακτυλίων, τότε το ίδιο συμβαίνει με την σύνθεση τους $\psi \circ \phi: R \rightarrow T$.

- (ii) Αν $\phi: R \rightarrow S$ είναι ισομορφισμός δακτυλίων, τότε $\phi^{-1}: S \rightarrow R$ είναι επίσης ισομορφισμός δακτυλίων.
- (iii) Έστω R δακτύλιος. Η ταυτοτική απεικόνιση $i_R: R \rightarrow R$ αποτελεί ισομορφισμό δακτυλίων.

Άσκηση. Εξετάστε κατά πόσον η συνάρτηση $\phi: \mathbb{C} \rightarrow \mathbb{C} : z \mapsto \bar{z}$, ($z \in \mathbb{C}$), είναι ένας ισομορφισμός δακτυλίων.

Ορισμός. Έστω $\phi: R \rightarrow S$ ομομορφισμός δακτυλίων. Ορίζουμε την *εικόνα* του ϕ με $\text{im}\phi = \{\phi(r) : r \in R\}$ και τον *πυρήνα* του ϕ με $\ker\phi = \{r \in R : \phi(r) = 0_S\}$.

Πρόταση 15.12. Έστω $\phi: R \rightarrow S$ ομομορφισμός δακτυλίων. Τότε

- (i) $\text{im}\phi$ είναι υποδακτύλιος του S , και
- (ii) $\ker\phi$ είναι υποδακτύλιος του R με την επιπλέον ιδιότητα ότι $rs, sr \in \ker\phi$ οποτεδήποτε $r \in R$ και $s \in \ker\phi$.

Απόδειξη. Για το (i) είναι αρκετό να δείξουμε ότι $s_1s_2 \in \text{im}\phi$ οποτεδήποτε $s_1, s_2 \in \text{im}\phi$, και για το (ii) είναι αρκετό να δείξουμε ότι $rs, sr \in \ker\phi$ οποτεδήποτε $r \in R$ και $s \in \ker\phi$. [Εξήγηση. Χρησιμοποιούμε την Παρατήρηση 15.10, την Πρόταση 13.6 και την Πρόταση 15.7 και επίσης ότι $\ker\phi \subseteq R$.] □

Παράδειγμα 15.13. (i) Η συνάρτηση $\pi: \mathbb{Z} \rightarrow \mathbb{Z}_n : a \mapsto \bar{a}$ ($a \in \mathbb{Z}$) είναι ένας επιρριπτικός ομομορφισμός δακτυλίων με $\ker\pi = n\mathbb{Z}$.

(ii) Θέτουμε $\phi: \mathbb{R} \rightarrow \mathbb{C} : x \mapsto x + i0$ ($x \in \mathbb{R}$). Τότε ϕ είναι ένας ενριπτικός ομομορφισμός δακτυλίων και $\text{im}\phi = \{x + i0 : x \in \mathbb{R}\}$ είναι ένα υπόσωμα του $\mathbb{C}$ ισομορφικό με το $\mathbb{R}$ (ως δακτύλιο).

Παρατήρηση 15.14. Αν S και R είναι δύο δακτύλιοι και $\phi: S \rightarrow R$ ένας ενριπτικός ομομορφισμός δακτυλίων, τότε $\text{im}\phi$ είναι ένας υποδακτύλιος του R ισομορφικός προς τον S . Συνήθως ταυτίζουμε τους δακτύλιους S και $\text{im}\phi$ και θεωρούμε τον S ως υποδακτύλιο του R . [Ταυτίζουμε το στοιχείο s με το στοιχείο $\phi(s)$, $s \in S$. Αν $s \in S$ και $r \in R - S$, “ $s+r$ ” σημαίνει “ $\phi(s)+r$ ”, “ sr ” σημαίνει “ $\phi(s)r$ ” και “ rs ” σημαίνει “ $r\phi(s)$ ”. Δεν υπάρχει περίπτωση να δημιουργηθεί σύγχυση ακριβώς διότι η συνάρτηση ϕ έχει και τις δύο πιο πάνω ιδιότητες, είναι δηλαδή ένας ενριπτικός ομομορφισμός.]

Παράδειγμα. Σε αρκετές περιπτώσεις είναι βολικό να ταυτίσουμε το σώμα $\mathbb{R}$ με το υπόσωμα $\{x + i0 : x \in \mathbb{R}\}$ του $\mathbb{C}$ και να θεωρήσουμε έτσι το $\mathbb{R}$ ως υπόσωμα του $\mathbb{C}$ (συγκρίνετε με το Παράδειγμα 15.13(ii)).

Σημειώσεις και Σχόλια

Η μελέτη ενός δακτυλίου παρέχει μια γενίκευση της αριθμητικής των ακεραίων. Το κίνητρο για την γενίκευση της αριθμητικής προήλθε κυρίως από τις προσπάθειες απόδειξης του τελευταίου θεωρήματος του Fermat. Σύμφωνα με αυτό το θεώρημα, που πιστεύεται ότι διατυπώθηκε στα τέλη της δεκαετίας του 1630 και αποδείχθηκε μόλις την δεκαετία του 1990, η εξίσωση $x^n + y^n = z^n$ δεν έχει λύση για θετικούς ακεραίους x, y, z όταν $n > 2$.

Το έργο του Euler (1753) για την περίπτωση $n = 3$ του θεωρήματος αυτού περιλάμβανε την επέκταση της συνηθισμένης αριθμητικής των ακεραίων σε αριθμούς της μορφής $a + b\sqrt{-3}$, όπου a, b είναι ακέραιοι. Επίσης, γύρω στο 1801 ο Gauss απέδειξε ότι οι αριθμοί της μορφής $a + b\sqrt{-1}$, όπου a και b είναι ακέραιοι, μπορούν να παρασταθούν μοναδικά ως γινόμενο 'πρώτων' αριθμών της μορφής $a + b\sqrt{-1}$, με ανάλογο τρόπο με τη μοναδική παραγοντοποίηση ενός ακεραίου σε γινόμενο πρώτων αριθμών.

Μέχρι αυτό το σημείο βρισκόμαστε ακόμα στο πλαίσιο της θεωρίας αριθμών. Ήταν το έργο του Kummer και αργότερα του Dedekind που οδήγησε στην έννοια του ιδεώδους. Ο Dedekind εισήγαγε επίσης τους όρους σώμα και μόδιο, αν και ο αρχικός ορισμός του μοδίου ήταν πιο περιορισμένος από τον σημερινό.

Ασκήσεις

15.1 Συμπληρώστε τους συλλογισμούς στο Παράδειγμα 15.1(ii).

15.2 Ποιοί από τους πιο κάτω δακτυλίους είναι σώματα;

(i) $\mathbb{Q}$, (ii) $\mathbb{R}$, (iii) $\mathbb{Z}$, (iv) $M_n(\mathbb{R})$, $n > 1$.

15.3 Δείξτε ότι το σύνολο $\{3k : k \in \mathbb{Z}\}$ αποτελεί δακτύλιο ως προς τη συνηθισμένη πρόσθεση και πολλαπλασιασμό ακεραίων. Είναι ο δακτύλιος αυτός 1-δακτύλιος;

15.4 Έστω R ένας 1-δακτύλιος.

(i) Δείξτε ότι $(R^*, \cdot)$ αποτελεί ομάδα.

(ii) Εξετάστε κατά πόσον $T = \{(r, s) \in R \times R : s = ru \text{ για κάποιο } u \in R^*\}$ αποτελεί σχέση ισοδυναμίας στο R .

15.5 (i) Έστω S υποδακτύλιος του δακτυλίου R . Δείξτε ότι $0_S = 0_R$. Επιπλέον, αν $a \in S$, τότε $(-a)_S = (-a)_R$.

(ii) Έστω T υπόσωμα του σώματος F . Δείξτε ότι $1_T = 1_F$ και ότι, για $a \in T - \{0_F\}$, ισχύει $(a^{-1})_T = (a^{-1})_F$.

15.6 Έστω S ένα μη-κενό υποσύνολο του δακτυλίου R . Υποθέστε επίσης ότι $a + (-b), ab \in S$ οποτεδήποτε $a, b \in S$. Δείξτε ότι S είναι υποδακτύλιος του R .

15.7 Συμπληρώστε τους συλλογισμούς στο Παράδειγμα 15.8(i).

15.8 Θέτουμε $\omega = i\sqrt{5} \in \mathbb{C}$. Θέτουμε επίσης $R = \{z \in \mathbb{C} : z = a + b\omega \text{ για κάποια } a, b \in \mathbb{Z}\}$. Δείξτε ότι (i) R είναι υποδακτύλιος του $\mathbb{C}$, και (ii) ο δακτύλιος R είναι αθέριος περιοχή.

(iii) Βρείτε τα στοιχεία του R^* .

15.9 Έστω F σώμα. Έστω επίσης T ένα υποσύνολο του F το οποίο περιέχει τουλάχιστον δύο στοιχεία και ικανοποιεί και τις τρεις ιδιότητες (i), (ii) και (iii) πιο κάτω :

(i) Αν $a, b \in T$, τότε $a + b \in T$ και $ab \in T$.

(ii) Αν $a \in T$ τότε $-a \in T$

(iii) Αν $a \in T$ και $a \neq 0_F$, τότε $a^{-1} \in T$.

Δείξτε ότι T αποτελεί υπόσωμα του F .

15.10 Εξετάστε κατά πόσον $S = \{z \in \mathbb{C} : z = a + ib \text{ για κάποια } a, b \in \mathbb{Q}\}$ αποτελεί υπόσωμα του $\mathbb{C}$.

15.11 Εξετάστε κατά πόσον $L = \{x \in \mathbb{R} : x = \alpha + \beta\sqrt{7} \text{ για κάποια } \alpha, \beta \in \mathbb{Q}\}$ αποτελεί υπόσωμα του $\mathbb{R}$.

15.12 Έστω F σώμα. Δείξτε ότι η τομή οποιασδήποτε (μη-κενής) οικογένειας υποσωμάτων του F είναι επίσης υπόσωμα του F .

15.13 Έστω R, S αθέριες περιοχές.

(i) Αν $\phi : R \rightarrow S$ είναι ένας ομομορφισμός δακτυλίων με $\phi(1_R) \neq 0_S$, δείξτε ότι $\phi(1_R) = 1_S$.

(ii) Αν R είναι υποδακτύλιος του S , δείξτε ότι $1_R = 1_S$.

- 15.14 (i) Έστω $\phi: R \rightarrow S$ ομομορφισμός δακτυλίων. Αν ϕ είναι ενριπτικός, δείξτε ότι οι δακτύλιοι $\text{im}\phi$ και R είναι ισομορφικοί.
- (ii) Έστω F, K σώματα και $\psi: F \rightarrow K$ ένας ενριπτικός ομομορφισμός δακτυλίων. Δείξτε ότι $\psi(1_F) = 1_K$ και ότι $\text{im}\psi$ είναι ένα υπόσωμα του K ισομορφικό προς το F (ως δακτύλιοι).

16. Δακτύλιοι πολυωνύμων

16.1. Ορισμοί, βασικές ιδιότητες

Για ολόκληρη την Παράγραφο 16.1, με R θα συμβολίζουμε ένα μεταθετικό 1-δακτύλιο. Επίσης, θα γράφουμε $0, 1$ αντί για $0_R, 1_R$ για σκοπούς απλοποίησης.

Ορισμός. Ένα πολυώνυμο επί του R είναι μια άπειρη ακολουθία $\sigma = (c_0, c_1, c_2, \dots)$, όπου $c_i \in R$ για όλα τα i , με την ιδιότητα ότι υπάρχει ακέραιος n τέτοιος ώστε $c_i = 0$ για όλα τα $i > n$.

Σημείωση. Έστω $\tau = (d_0, d_1, d_2, \dots)$ ακόμη ένα πολυώνυμο επί του R . Έπεται ότι $\sigma = \tau$ αν, και μόνο αν, $c_i = d_i$, για όλα τα i . [Παρατηρούμε ότι σ, τ είναι στην πραγματικότητα συναρτήσεις $\mathbb{N} \cup \{0\} \rightarrow R$ με $\sigma(i) = c_i$ και $\tau(i) = d_i$ για όλα τα $i \geq 0$.]

Συμβολισμός. Το σύνολο των πολυωνύμων επί του R συμβολίζεται με $R[x]$.

Ορισμός. Ορίζουμε πρόσθεση και πολλαπλασιασμό στο σύνολο $R[x]$ ως εξής.

$$(c_0, c_1, \dots) + (d_0, d_1, \dots) = (c_0 + d_0, c_1 + d_1, \dots), \text{ και} \\ (c_0, c_1, \dots)(d_0, d_1, \dots) = (e_0, e_1, \dots)$$

όπου $e_0 = c_0 d_0$, $e_1 = c_0 d_1 + c_1 d_0$ και πιο γενικά $e_k = \sum c_i d_j$ όπου το άθροισμα εκτελείται πάνω σε όλους τους δείκτες i, j με $i + j = k$. [Παρατήρηση. Αν $c_i = 0$ για όλα τα $i > l$ και $d_j = 0$ για όλα τα $j > m$ τότε $e_k = 0$ για όλα τα $k > l + m$.]

Θεώρημα 16.1. Έστω R ένας μεταθετικός 1-δακτύλιος. Τότε $R[x]$ είναι ένας μεταθετικός 1-δακτύλιος ως προς την πρόσθεση και πολλαπλασιασμό που έχουμε ορίσει πιο πάνω.

Απόδειξη. Ελέγχουμε ότι ισχύουν οι ιδιότητες. Για παράδειγμα το μηδενικό στοιχείο του $R[x]$ είναι το $(0, 0, \dots, 0, \dots)$ και το μοναδιαίο είναι το $(1, 0, 0, \dots, 0, \dots)$. $\square$

Ορισμός. Ο δακτύλιος $R[x]$ ονομάζεται ο δακτύλιος πολυωνύμων επί του R .

Σημείωση. (i) Θεωρούμε την απεικόνιση $\varepsilon: R \rightarrow R[x]: r \mapsto (r, 0, 0, \dots, 0, \dots)$, ($r \in R$). Τότε ε είναι ένας ενριπτικός ομομορφισμός δακτυλίων. Έπεται ότι ο δακτύλιος R είναι ισομορφικός προς τον υποδακτύλιο $R' = \{(r, 0, 0, \dots, 0, \dots): r \in R\} (= \text{im } \varepsilon)$ του $R[x]$.

Συνήθως ταυτίζουμε τον R' με τον R , και το στοιχείο $(r, 0, 0, \dots, 0, \dots)$ με το r , και θεωρούμε τον R ως υποδακτύλιο του $R[x]$. Παρατηρούμε ότι $(r, 0, 0, \dots, 0, \dots)(c_0, c_1, \dots, c_j, \dots) = (rc_0, rc_1, \dots, rc_j, \dots)$ — συνήθως γράφουμε $r(c_0, c_1, \dots, c_j, \dots) = (rc_0, rc_1, \dots, rc_j, \dots)$.

(ii) Θέτουμε $x = (0, 1, 0, 0, \dots) \in R[x]$. Έπεται ότι $x^2 = (0, 0, 1, 0, 0, \dots)$ και ότι x^i συμπίπτει με την ακολουθία που έχει 0 παντού εκτός από την i -θέση (σημειώστε ότι εδώ αρχίζουμε με την 0-θέση) στην οποία υπάρχει το στοιχείο 1. Επανακάμπτει δηλαδή ο συνηθισμένος συμβολισμός

$$\begin{aligned}(c_0, c_1, \dots, c_n, 0, 0, \dots) &= (c_0, 0, 0, \dots) + (0, c_1, 0, \dots) + \dots + (0, \dots, 0, c_n, 0, \dots) \\ &= c_0(1, 0, 0, \dots) + c_1(0, 1, 0, \dots) + \dots + c_n(0, \dots, 0, 1, 0, \dots) \\ &= c_0 + c_1x + c_2x^2 + \dots + c_nx^n = f(x).\end{aligned}$$

Έχουμε λοιπόν ότι το x δεν είναι τίποτα άλλο από απλά ένα στοιχείο του δακτύλιου $R[x]$ και δεν πρόκειται για μια μεταβλητή. (Στο (iii) πιο κάτω θα δούμε μέσα σε ποιά πλαίσια μπορεί να του αποδοθεί ο ρόλος του ως μεταβλητή.)

(iii) Έστω $a \in R$. Θέτουμε $\text{ev}_a: R[x] \rightarrow R: f(x) = r_0 + r_1x + \dots + r_nx^n \mapsto r_0 + r_1a + \dots + r_na^n$ ($f(x) \in R[x]$). Εύκολα μπορεί ναδειχθεί ότι η απεικόνιση ev_a είναι ένας ομομορφισμός δακτυλίων και ονομάζεται *αποτίμηση* στο a . Αν συμβολίσουμε το στοιχείο $r_0 + r_1a + \dots + r_na^n$ του R με $f(a)$, βλέπουμε ότι κάθε πολυώνυμο $f(x) \in R[x]$ ορίζει μια πολυωνυμική συνάρτηση $f: R \rightarrow R: a \mapsto f(a) (= \text{ev}_a(f))$.

Μια χρήσιμη παρατήρηση είναι ότι το πολυώνυμο $f(x) = x^p - x \in \mathbb{Z}_p[x]$ (p πρώτος), που προφανώς δεν ισούται με το μηδενικό πολυώνυμο του $\mathbb{Z}_p[x]$, έχει την ιδιότητα ότι $\text{ev}_\alpha(f(x)) = \bar{0}$ για όλα τα $\alpha \in \mathbb{Z}_p$.

(iv) Πιο γενικά, αν R είναι υποδακτύλιος του μεταθετικού δακτύλιου D και $a \in D$, τότε η συνάρτηση $\text{ev}_a: R[x] \rightarrow D: f(x) = r_0 + r_1x + \dots + r_nx^n \mapsto r_0 + r_1a + \dots + r_na^n$, ($f(x) \in R[x]$) είναι επίσης ομομορφισμός δακτυλίων.

Έστω τώρα $f(x) = c_0 + c_1x + c_2x^2 + \dots + c_nx^n \in R[x]$. Αν το πολυώνυμο $f(x)$ δεν είναι μηδενικό (δηλαδή δεν ισούται με το $(0, 0, \dots, 0, \dots)$), ο επικεφαλής συντελεστής του ορίζεται να είναι ο c_n όπου n είναι ο μεγαλύτερος δείκτης με $c_n \neq 0$. Σε τέτοια περίπτωση ο δείκτης n ονομάζεται *βαθμός* του πολυωνύμου $f(x)$ και συμβολίζεται με $\deg(f)$.

Ένα πολυώνυμο ονομάζεται *μονικό* όταν ο επικεφαλής συντελεστής του είναι το 1. Ένα σταθερό πολυώνυμο είναι ένα πολυώνυμο $(a_0, a_1, a_2, \dots)$ όπου $a_i = 0$ για $i > 0$. Με άλλα λόγια, τα σταθερά πολυώνυμα είναι το μηδενικό πολυώνυμο και τα πολυώνυμα βαθμού 0.

Από τον ορισμό, ο σταθερός όρος του πολυωνύμου $f(x)g(x)$, όπου $f(x), g(x) \in R[x]$, ισούται με το γινόμενο των σταθερών όρων των $f(x), g(x)$.

Παραδείγματα 16.2. (i) $R[x]$ ουδέποτε είναι δακτύλιος διαίρεσης. [Αν $f(x) \in R[x]$, ο σταθερός όρος του πολυωνύμου $xf(x)$ είναι το 0, άρα $xf(x) \neq 1$.]

(ii) Παρατηρούμε ότι $(\bar{2}x + \bar{1})^2 = \bar{1}$ στον δακτύλιο $\mathbb{Z}_4[x]$. Συνεπώς ο τύπος $\deg(fg) = \deg(f) + \deg(g)$ δεν ισχύει γενικά.

(iii) Έστω ότι R είναι μια ακέραια περιοχή. Αν $f(x), g(x) \in R[x]$ είναι μη-μηδενικά πολυώνυμα, τότε ο επικεφαλής συντελεστής του $f(x)g(x)$ είναι το γινόμενο των επικεφαλής συντελεστών των $f(x)$ και $g(x)$. Συνεπώς, αν f, g είναι μη-μηδενικά πολυώνυμα του $R[x]$ όπου R είναι ακέραια περιοχή, τότε το πολυώνυμο fg είναι μη-μηδενικό και $\deg(fg) = \deg(f) + \deg(g)$. Έπεται ότι $R[x]$ είναι επίσης ακέραια περιοχή.

Εύκολα μπορούμε να αποδείξουμε το ακόλουθο αποτέλεσμα.

Πρόταση 16.3. Έστω R, S μεταθετικοί 1-δακτύλιοι. Αν $\sigma : R \rightarrow S$ είναι ένας ομομορφισμός δακτυλίων με $\sigma(1_R) = 1_S$, τότε η απεικόνιση $\sigma^* : R[x] \rightarrow S[x] : \sum r_i x^i \mapsto \sum \sigma(r_i) x^i$ είναι επίσης ένας ομομορφισμός δακτυλίων ο οποίος ικανοποιεί $\sigma^*(1_{R[x]}) = 1_{S[x]}$ για όλα τα $i \geq 0$. [Ο ομομορφισμός σ^* καλείται ο ομομορφισμός πολυωνυμικών δακτυλίων ο οποίος επάγεται από τον σ .]

16.2. Πολυωνυμικοί δακτύλιοι πάνω σε σώματα

Θεώρημα 16.4. Έστω F σώμα και $f(x), g(x) \in F[x]$ όπου $g(x) \neq 0$. Τότε υπάρχουν μοναδικά πολυώνυμα $q(x), r(x) \in F[x]$ τέτοια ώστε $f(x) = q(x)g(x) + r(x)$ και όπου είτε $r(x) = 0$ ή $\deg(r) < \deg(g)$.

Απόδειξη. Θα αποδείξουμε πρώτα την ύπαρξη τέτοιων πολυωνύμων $q(x), r(x) \in F[x]$. Θέτουμε $S = \{f(x) - m(x)g(x) : m(x) \in F[x]\}$. Προφανώς το σύνολο S περιέχει μη-μηδενικά πολυώνυμα αφού $g(x) \neq 0$. Αν τώρα $0 (= 0_{F[x]}) \in S$ τότε $f(x) = m_1(x)g(x)$ για κάποιο $m_1(x) \in F[x]$, και στην περίπτωση αυτή μπορούμε να θέσουμε $q(x) = m_1(x)$ και $r(x) = 0$. Επομένως υποθέτουμε ότι $0 \notin S$ (έχουμε επίσης τότε ότι $\deg(g(x)) \geq 1$). Το σύνολο $T = \{k \in \mathbb{N} \cup \{0\} : k = \deg(h(x)) \text{ για κάποιο } h(x) \in S\}$ είναι μη-κενό και επομένως περιέχει ελάχιστο στοιχείο, έστω το l . Τότε υπάρχει πολυώνυμο $r(x) \in S$ με $\deg(r(x)) = l$. Από το ορισμό του συνόλου S έχουμε ότι $r(x) = f(x) - q(x)g(x)$ για κάποιο $q(x) \in F[x]$, με $r(x) \neq 0$ αφού $0 \notin S$.

Ισχυρισμός. Ισχύει ότι $\deg(r(x)) < \deg(g(x))$.

Απόδειξη ισχυρισμού. Υποθέτουμε ότι $l = \deg(r(x)) \geq \deg(g(x)) = m$. Έχουμε τότε ότι $r(x) = r_0 + r_1x + \dots + r_lx^l$ (όπου $r_l \neq 0$) και $g(x) = g_0 + g_1x + \dots + g_mx^m$ (όπου $g_m \neq 0$), με $l \geq m$. Θέτουμε $s(x) = r(x) - g_m^{-1}r_lx^{l-m}g(x)$. [Αν $l = m$, ορίζουμε $x^{l-m} = 1$.] Έπεται ότι $s(x) = f(x) - (q(x) + g_m^{-1}r_lx^{l-m})g(x)$ ανήκει στο σύνολο S (και επομένως $s(x) \neq 0$ από την υπόθεση μας). Όμως $\deg(s(x)) < \deg(r(x))$, που προφανώς αντιφάσκει με την επιλογή του $r(x)$.

Συνοψίζοντας, μέχρι το σημείο αυτό έχουμε δείξει ότι υπάρχουν πολυώνυμα $q(x), r(x) \in F[x]$ με $f(x) = q(x)g(x) + r(x)$ όπου είτε $r(x) = 0$ ή $\deg(r(x)) < \deg(g(x))$.

Έστω τώρα $\hat{q}(x), \hat{r}(x) \in F[x]$ με $f(x) = \hat{q}(x)g(x) + \hat{r}(x)$ όπου $\hat{r}(x) = 0$ ή $\deg(\hat{r}) < \deg(g)$. Έχουμε τότε ότι $r(x) - \hat{r}(x) = (\hat{q}(x) - q(x))g(x)$. Αν $r(x) - \hat{r}(x) \neq 0$, τότε $\hat{q}(x) - q(x) \neq 0$ και επομένως $\deg(r(x) - \hat{r}(x)) \geq \deg(g(x))$ που είναι άτοπο. Συνάγουμε ότι $\hat{r}(x) = r(x)$ και $\hat{q}(x) = q(x)$. □

Πόρισμα. Έστω F σώμα. Τότε ο δακτύλιος $F[x]$ είναι Ευκλείδεια περιοχή.

Ορισμός. Έστω ότι το σώμα K είναι μια επέκταση του σώματος F . Έστω επίσης ότι $f(x) = c_0 + c_1x + \dots + c_nx^n \in F[x]$. Λέμε ότι $\alpha \in K$ είναι μια *θέση μηδενισμού* του $f(x)$ στο K αν $\text{ev}_\alpha(f) (= c_0 + c_1\alpha + \dots + c_n\alpha^n) = 0_K (= 0_F)$.

Παράδειγμα. Έστω $f(x) = x^2 + 1 \in \mathbb{R}[x]$. Παρατηρούμε ότι $f(x)$ δεν έχει θέσεις μηδενισμού στο $\mathbb{R}$ ενώ έχει ακριβώς δύο θέσεις μηδενισμού στο $\mathbb{C}$ (θεωρώντας το σώμα $\mathbb{C}$ ως επέκταση του σώματος $\mathbb{R}$).

Άσκηση. Έστω F σώμα και $f(x) \in F[x]$ ένα μη-μηδενικό πολυώνυμο με $\deg(f) = n > 0$. Δείξτε τα πιο κάτω.

- (i) Αν $\alpha \in F$ είναι μια θέση μηδενισμού του $f(x)$ στο F , τότε $f(x) = (x - \alpha)q(x)$ για κάποιο $q(x) \in F[x]$.
- (ii) Το σώμα F περιέχει το πολύ n θέσεις μηδενισμού του $f(x)$. (Επιπλέον, αν το σώμα K είναι επέκταση του σώματος F , τότε το K περιέχει το πολύ n θέσεις μηδενισμού του $f(x)$.)

Ορισμός. Έστω F σώμα και $q_1(x), q_2(x) \in F[x]$. Λέμε ότι $q_1(x)$ διαιρεί το $q_2(x)$, και γράφουμε $q_1(x)|q_2(x)$, αν $q_2(x) = q_1(x)s(x)$ για κάποιο $s(x) \in F[x]$.

Ορισμός. Έστω $f(x), g(x) \in F[x]$. Ένας *μέγιστος κοινός διαρέτης* (μκδ) των $f(x)$ και $g(x)$ είναι ένα πολυώνυμο $d(x) \in F[x]$ τέτοιο ώστε

- (i) $d(x)|f(x)$ και $d(x)|g(x)$,
- (ii) αν $c(x) \in F[x]$ με $c(x)|f(x)$ και $c(x)|g(x)$, τότε $c(x)|d(x)$,
- (iii) το πολυώνυμο $d(x)$ είναι μονικό.

Προφανώς αν υπάρχει μκδ των $f(x)$ και $g(x)$ τότε είναι μοναδικός (και συμβολίζεται με $\mu\kappa\delta(f, g)$). [Αν $d_1(x), d_2(x) \in F[x] - \{0\}$ με $d_1(x)|d_2(x)$ και $d_2(x)|d_1(x)$, τότε $d_2(x) = \alpha d_1(x)$ για κάποιο $\alpha \in F^*$.]

Οι δακτύλιοι $\mathbb{Z}$ και $\mathbb{F}[x]$, όπου $\mathbb{F}$ σώμα, είναι και οι δύο Ευκλείδειες περιοχές και δεν είναι καθόλου τυχαίο ότι μοιράζονται παρόμοιες ιδιότητες (κοιτάξτε τα αποτελέσματα που ακολουθούν) και άλλες, όπως για παράδειγμα την ύπαρξη αλγορίθμου (Ευκλείδειος αλγόριθμος) που υπολογίζει τον μκδ και τον εκφράζει ως γραμμικό συνδυασμό.

Θεώρημα 16.5. Έστω $f(x), g(x) \in F[x]$ με $g(x) \neq 0$. Τότε υπάρχει ο $\mu\kappa\delta(f, g)$. Επιπλέον αν $d(x) = \mu\kappa\delta(f, g)$, τότε $d(x) = a(x)f(x) + b(x)g(x)$ για κάποια $a(x), b(x) \in F[x]$.

Απόδειξη. Θέτουμε $I = \{s(x)f(x) + t(x)g(x) : s(x), t(x) \in F[x]\}$. Τότε $f(x), g(x) \in I$ και, αφού $g(x) \neq 0$, το σύνολο $S = \{k \in \mathbb{N} \cup \{0\} : \deg(h(x)) = k \text{ για κάποιο } h(x) \in I\}$ είναι μη-κενό. Έστω l το ελάχιστο στοιχείο του S . Τότε υπάρχει $d(x) \in I$, όπου $d(x)$ είναι μονικό, με $\deg(d(x)) = l$. Από τον ορισμό του συνόλου I έχουμε ότι $d(x) = a(x)f(x) + b(x)g(x)$ για κάποια $a(x), b(x) \in F[x]$. Θα δείξουμε ότι $d(x) = \mu\kappa\delta(f(x), g(x))$. Προφανώς τα (ii) και (iii) στον ορισμό του μκδ ισχύουν. Συνεπώς αρκεί να δείξουμε ότι $d(x)|f(x)$ και $d(x)|g(x)$. Θα δείξουμε ότι $d(x)|m(x)$ για όλα τα $m(x) \in I$. Υποθέτουμε λοιπόν ότι

$m(x) = s(x)f(x) + t(x)g(x) \in I$. Χρησιμοποιώντας το θεώρημα διαίρεσης, λαμβάνουμε $m(x) = q(x)d(x) + r(x)$ όπου $q(x), r(x) \in F[x]$ και είτε $r(x) = 0$ ή $\deg(r(x)) < \deg(d(x))$. Όμως $r(x) = m(x) - q(x)d(x) = s(x)f(x) + t(x)g(x) - q(x)(a(x)f(x) + b(x)g(x)) = (s(x) - q(x)a(x))f(x) + (t(x) - q(x)b(x))g(x) \in I$. Συνάγουμε ότι $r(x) = 0$ και επομένως $d(x)|m(x)$. $\square$

Οι αποδείξεις των δύο πιο κάτω προτάσεων είναι σχεδόν πανομοιότυπες με τις αποδείξεις των αντίστοιχων αποτελεσμάτων στο $\mathbb{Z}$, και τις αφήνουμε ως άσκηση.

Πρόταση 16.6. Έστω F σώμα και $f(x), g(x) \in F[x]$. Έχουμε τότε ότι $\mu\chi\delta(f(x), g(x)) = 1$ αν, και μόνο αν, $a(x)f(x) + b(x)g(x) = 1$ για κάποια $a(x), b(x) \in F[x]$.

Απόδειξη. Παρεμβάλλοντας το Θεώρημα 16.5, είναι αρκετό να δείξουμε ότι $\mu\chi\delta(f, g) = 1$ αν $a(x)f(x) + b(x)g(x) = 1$ για κάποια $a(x), b(x) \in F[x]$. Προφανώς το πολυώνυμο 1 είναι μονικό και διαιρεί τα $f(x)$ και $g(x)$. Αν τώρα $m(x) \in F[x]$ με $m(x)|f(x)$ και $m(x)|g(x)$, τότε $m(x)|(a(x)f(x) + b(x)g(x))$. $\square$

Πρόταση 16.7. Έστω F σώμα και έστω $q(x), f(x), g(x) \in F[x]$. Αν $\mu\chi\delta(q(x), f(x)) = 1$ και $q(x)|f(x)g(x)$, τότε $q(x)|g(x)$.

Απόδειξη. Από την Πρόταση 16.6, έχουμε ότι $a(x)f(x) + b(x)q(x) = 1$ για κάποια $a(x), b(x) \in F[x]$. Συνεπώς, $a(x)f(x)g(x) + b(x)q(x)g(x) = g(x)$. Αφού $q(x)|b(x)q(x)g(x)$ και, από την υπόθεση, $q(x)|f(x)g(x)$, τότε $q(x)$ διαιρεί το αριστερό μέλος (και επομένως και το δεξιό μέλος) της τελευταίας ισότητας. $\square$

Ορισμός. Έστω ότι το σώμα K είναι μια επέκταση του σώματος F . Ένα πολυώνυμο $f(x) \in F[x]$ καλείται *ανάγωγο επί του K* αν $\deg(f) \geq 1$ και, επιπλέον, από την σχέση $f(x) = g(x)h(x)$ με $g(x), h(x) \in K[x]$ προκύπτει ότι ένα από τα $g(x), h(x)$ είναι σταθερό πολυώνυμο.

Παράδειγμα 16.8. Έστω $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Τότε το πολυώνυμο $f(x)$ είναι ανάγωγο επί του $\mathbb{Q}$, όμως δεν είναι ανάγωγο επί του $\mathbb{R}$ αφού $f(x) = (x + \sqrt{2})(x - \sqrt{2})$ στον $\mathbb{R}[x]$.

Πόρισμα 16.9. Έστω F σώμα και έστω $p(x), a_1(x), \dots, a_n(x) \in F[x]$, με $p(x)$ ανάγωγο επί του F . Αν $p(x)|a_1(x) \dots a_n(x)$, τότε $p(x)|a_i(x)$ για κάποιο i με $1 \leq i \leq n$.

Ανάλογη απόδειξη με την πιο κάτω θα μπορούσαμε να είχαμε δώσει και για το θεμελιώδες θεώρημα της αριθμητικής.

Θεώρημα 16.10. Έστω F σώμα. Κάθε μη-σταθερό πολυώνυμο $f(x) \in F[x]$ διαθέτει μια παραγοντοποίηση $\alpha p_1(x)p_2(x) \dots p_r(x)$ όπου $\alpha \in F^*$ είναι ο επικεφαλής συντελεστής του $f(x)$, και $p_i \in F[x]$ ($1 \leq i \leq r$) είναι (όχι απαραίτητα διαφορετικά) μονικά ανάγωγα πολυώνυμα επί του F . Η παραγοντοποίηση αυτή είναι μοναδική αν δεν ληφθεί υπόψη η σειρά με την οποία εμφανίζονται οι παράγοντες.

Απόδειξη. Έστω $f(x) \in F[x]$ με $\deg(f(x)) \geq 1$. Θα δείξουμε πρώτα ότι υπάρχει τέτοια παραγοντοποίηση για το $f(x)$ χρησιμοποιώντας επαγωγή στον βαθμό του $f(x)$. Αν $\deg(f(x)) = 1$, τότε $f(x) = \alpha x + \beta$ με $\alpha \neq 0_F$ και επομένως έχουμε $f(x) = \alpha(x + \alpha^{-1}\beta)$, όπου προφανώς το πολυώνυμο $x + \alpha^{-1}\beta \in F[x]$ είναι ανάγωγο. Υποθέτουμε τώρα ότι $\deg(f(x)) > 1$ και ότι το αποτέλεσμα ισχύει για όλα τα $c(x) \in F[x]$ με $1 \leq \deg(c(x)) < \deg(f(x))$. Αν το $f(x)$ είναι ανάγωγο δεν έχουμε κάτι να δείξουμε, επομένως υποθέτουμε ότι το $f(x)$ δεν είναι ανάγωγο. Έπεται ότι $f(x) = a(x)b(x)$ με $a(x), b(x) \in F[x]$ και $1 \leq \deg(a(x)), \deg(b(x)) < \deg(f(x))$. Από την επαγωγική υπόθεση τα $a(x)$ και $b(x)$ μπορούν να εκφραστούν ως γινόμενα που έχουν την πιο πάνω μορφή, και επομένως και το $f(x)$.

Θα χρησιμοποιήσουμε επαγωγή για να αποδείξουμε και την μοναδικότητα: Αν $\deg(f(x)) = 1$ προφανώς η έκφραση $f(x) = \alpha(x + \alpha^{-1}\beta)$ που έχουμε βρει προηγουμένως είναι μοναδική. Υποθέτουμε τώρα ότι $\deg(f(x)) > 1$ και ότι το αποτέλεσμα ισχύει για πολυώνυμα με (θετικό) βαθμό $< \deg(f(x))$. Έστω επίσης ότι $f(x) = \alpha p_1(x)p_2(x) \dots p_r(x) = \alpha q_1(x)q_2(x) \dots q_k(x)$ όπου $\alpha \in F^*$ είναι ο επικεφαλής συντελεστής του $f(x)$ και $p_i(x), q_j(x) \in F[x]$ ($1 \leq i \leq r$, $1 \leq j \leq k$) είναι μονικά ανάγωγα πολυώνυμα επί του F . Αφού $p_1(x)|f(x)$, έχουμε ότι $p_1(x)|q_1(x)q_2(x) \dots q_k(x)$ και επομένως $p_1(x)|q_i(x)$ για κάποιο i με $1 \leq i \leq k$ από το Πρόρισμα 16.9. Αφού τα $p_1(x)$ και $q_i(x)$ είναι μονικά και ανάγωγα παίρνουμε ότι $p_1(x) = q_i(x)$. Μετά από μια πιθανή αναδιάταξη των $q_j(x)$ μπορούμε να υποθέσουμε ότι $p_1(x) = q_1(x)$. Έπεται ότι $\alpha p_2(x) \dots p_r(x) = \alpha q_2(x) \dots q_k(x) = g(x)$, όπου $g(x) (= \frac{f(x)}{p_1(x)}) \in F[x]$ και $\deg(g(x)) < \deg(f(x))$. Αν $\deg(g(x)) = 0$ τότε $g(x) = \alpha$ και η απόδειξη τελειώνει. Αν $\deg(g(x)) \geq 1$, από την επαγωγική υπόθεση, έχουμε ότι $r = k$ και, επιπλέον, μετά από μια πιθανή αναδιάταξη των $q_j(x)$, ότι $p_i(x) = q_i(x)$ για $2 \leq i \leq r$. $\square$

Αν F είναι ένα σώμα και $f(x) \in F[x]$ ένα πολυώνυμο βαθμού $n > 0$, τότε $f(x)$ μπορεί να έχει ή να μην έχει θέσεις μηδενισμού στο F . Αν $F = \mathbb{C}$, τότε ισχύει το πιο κάτω θεώρημα.

Θεώρημα 16.11 (Θεμελιώδες Θεώρημα της Άλγεβρας). Αν $f(x) \in \mathbb{C}[x]$ είναι ένα πολυώνυμο βαθμού $n > 0$, τότε $f(x)$ έχει τουλάχιστον μια θέση μηδενισμού στο $\mathbb{C}$.

Η πρώτη απόδειξη του θεωρήματος αυτού οφείλεται στον Gauss, όμως η πιο απλή απόδειξη είναι μέσω της θεωρίας μιγαδικών συναρτήσεων. Άλλες αποδείξεις στηρίζονται στην θεωρία Galois.

Πόρισμα 16.12. Έστω $f(x) \in \mathbb{R}[x]$ ένα ανάγωγο πολυώνυμο επί του $\mathbb{R}$. Τότε $\deg f \in \{1, 2\}$.

Ασκήσεις

16.1 Θέτουμε $\phi: \mathbb{C} \rightarrow \mathbb{C}: z \mapsto \bar{z}$ και $g: \mathbb{C} \rightarrow \mathbb{C}: z \mapsto 2 + 3z + 4z^2 + 5z^3$ ($z \in \mathbb{C}$).

- (i) Εξετάστε κατά πόσον η συνάρτηση ϕ είναι ισομορφισμός δακτυλίων.
- (ii) Δείξτε ότι ισχύει για $w \in \mathbb{C}$: $g(w) = 0$ αν-ν $g(\bar{w}) = 0$.
- (iii) Έστω $f(x) \in \mathbb{R}[x]$ και $w \in \mathbb{C}$. Εξετάστε κατά πόσον ισχύει: $\text{ev}_w(f(x)) = 0$ αν-ν $\text{ev}_{\bar{w}}(f(x)) = 0$.

- 16.2 Έστω F σώμα και $p(x), h_1(x), h_2(x), f(x), g(x) \in F[x]$ με $g(x) \neq 0$. Δείξτε τα πιο κάτω:
- (i) Αν $p(x)$ είναι ανάγωγο και $p(x)|h_1(x)h_2(x)$ τότε $p(x)|h_1(x)$ ή $p(x)|h_2(x)$.
 - (ii) Γράφουμε $f(x) = q(x)g(x) + r(x)$ όπου $q(x), r(x) \in F[x]$ και $r(x) = 0$ ή $\deg(r) < \deg(g)$ σύμφωνα με το Θεώρημα 16.4. Δείξτε ότι $\mu\kappa\delta(f(x), g(x)) = \mu\kappa\delta(g(x), r(x))$.
- 16.3 Έστω F σώμα. Δείξτε ότι $F[x]$ είναι Ευκλείδεια περιοχή.
- 16.4 Έστω F σώμα και $f(x) \in F[x]$ ένα μη-μηδενικό πολυώνυμο με $\deg(f) = n > 0$. Δείξτε τα πιο κάτω:
- (i) Αν $\alpha \in F$ και $\text{ev}_\alpha(f(x)) = 0_F$, τότε $f(x) = (x - \alpha)q(x)$ για κάποιο $q(x) \in F[x]$.
 - (ii) Το σώμα F περιέχει το πολύ n θέσεις μηδενισμού του $f(x)$.
 - (iii) Έστω $g(x) \in F[x]$ επίσης μη-μηδενικό πολυώνυμο με $\deg(g) \leq n$. Αν $\text{ev}_{\alpha_i}(g(x)) = \text{ev}_{\alpha_i}(f(x))$ για $1 \leq i \leq n+1$, όπου $\alpha_1, \dots, \alpha_{n+1}$ είναι διακεκριμένα στοιχεία του F , τότε $f(x) = g(x)$.
- 16.5 Έστω $f(x) \in \mathbb{R}[x]$ ένα ανάγωγο πολυώνυμο επί του $\mathbb{R}$. Δείξτε ότι $\deg f \in \{1, 2\}$.
- 16.6 Τα υπόλοιπα της διαίρεσης του πολυωνύμου $f(x) \in \mathbb{R}[x]$ διά $x - 3$ και $x - 1$ ισούνται με 6 και 4 αντίστοιχα. Βρείτε το υπόλοιπο της διαίρεσης του $f(x)$ διά $x^2 - 4x + 3$.
- 16.7 Αν $a, b, c \in \mathbb{R}$ με a, b, c διακεκριμένα. Δείξτε ότι $\frac{(d-b)(d-c)}{(a-b)(a-c)} + \frac{(d-c)(d-a)}{(b-c)(b-a)} + \frac{(d-a)(d-b)}{(c-a)(c-b)} - 1 = 0$ για όλα τα $d \in \mathbb{R}$.
- 16.8 Έστω $f(x) \in \mathbb{R}[x]$ βαθμού 100 τέτοιο ώστε $f(-1) = f(1), f(-2) = f(2), \dots, f(-50) = f(50)$. Εξετάστε κατά πόσον ισχύει ότι $f(-a) = f(a)$ για κάθε $a \in \mathbb{R}$.

17. Ιδεώδη, επεκτάσεις σωμάτων

17.1. Ιδεώδη, Δακτύλιος πηλίκου

Ορισμός. Ένα μη-κενό υποσύνολο I ενός δακτυλίου R καλείται ιδεώδες του R αν

(i) $a + (-b) \in I$, (ii) $ar \in I$, και (iii) $ra \in I$

για όλα τα $a, b \in I$ και όλα τα $r \in R$.

Το ιδεώδες I του R καλείται γνήσιο αν $I \neq R$.

Παρατήρηση 17.1. Έστω I ιδεώδες του δακτυλίου R . Τότε $0_R \in I$. Επίσης $-x \in I$ και $x + y \in I$ οποιοδήποτε $x, y \in I$. Έπεται ότι $(I, +)$ είναι υποομάδα της $(R, +)$ και ότι I είναι ένας υποδακτύλιος του R .

Παράδειγμα. (i) Σε ένα δακτύλιο R , τα υποσύνολα $\{0_R\}$ και R είναι ιδεώδη του R .

(ii) Αν $n \in \mathbb{N}$, τότε $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ είναι ιδεώδες του $\mathbb{Z}$. Υπάρχουν ιδεώδη του δακτυλίου $\mathbb{Z}$ που δεν είναι αυτής της μορφής;

(iii) Το υποσύνολο $\{(x^2 + 1)g(x) : g(x) \in \mathbb{R}[x]\}$ του $\mathbb{R}[x]$ είναι ιδεώδες του $\mathbb{R}[x]$.

(iv) Αν $\phi : R \rightarrow S$ είναι ένας ομομορφισμός δακτυλίων τότε $\ker \phi$ είναι ιδεώδες του R (κοιτάξτε την Πρόταση 15.12).

Ασκήσεις. (i) Έστω R δακτύλιος. Δείξτε ότι η τομή οποιασδήποτε (μη-κενής) οικογένειας ιδεωδών του R είναι επίσης ιδεώδες του R .

(ii) Έστω I, J ιδεώδη του δακτυλίου R . Θέτουμε $I + J = \{a + b : a \in I, b \in J\}$. Δείξτε ότι $I + J$ είναι ιδεώδες του R .

Ορισμός. Έστω R δακτύλιος, I ιδεώδες του R και $r, s \in R$. Λέμε ότι το r είναι *ισότιμο* προς το s modulo I , (συμβολισμός: $r \equiv s \pmod{I}$), αν (και μόνο αν) $r - s (= r + (-s)) \in I$.

Πρόταση 17.2. Έστω ότι R είναι δακτύλιος και I ιδεώδες του R . Η σχέση ισοτιμίας modulo I που έχουμε ορίσει πιο πάνω είναι μια σχέση ισοδυναμίας στον R .

Απόδειξη. (i) $r \equiv r \pmod{I}$ για όλα τα $r \in R$ αφού $r - r = 0_R \in I$.

(ii) Αν $r, s \in R$ με $r \equiv s \pmod{I}$ τότε $r - s \in I$ και επομένως $s \equiv r \pmod{I}$, αφού $s - r (= -(r - s)) \in I$.

(iii) Αν $r, s, t \in R$ με $r \equiv s \pmod{I}$ και $s \equiv t \pmod{I}$, τότε $r - s, s - t \in I$ και επομένως $r - t (= (r - s) + (s - t)) \in I$. $\square$

Παρατήρηση 17.3. (i) Αν R είναι δακτύλιος και I ιδεώδες του R τότε η οικογένεια των κλάσεων ισοδυναμίας που αντιστοιχούν στην πιο πάνω σχέση ισοδυναμίας (ισοτιμία modulo I) αποτελούν μια διαμέριση του συνόλου R .

(ii) Αν $\bar{r}$ είναι η κλάση ισοδυναμίας του $r \in R$ ως προς την πιο πάνω σχέση, τότε $\bar{r} = \{s \in R: s \equiv r \pmod{I}\} = \{s \in R: s - r \in I\} = \{r + x: x \in I\}$.

Παράδειγμα. (i) Έστω $n \in \mathbb{N}$, $R = \mathbb{Z}$ και $I = n\mathbb{Z} (= \{r \in \mathbb{Z}: n|r\})$. Τότε $a \equiv b \pmod{n\mathbb{Z}}$ (όπου $a, b \in \mathbb{Z}$) αν, και μόνο αν, $n|(a - b)$ (αν-ν $a \equiv b \pmod{n}$). Επιπλέον, αν $r \in \mathbb{Z}$, τότε η κλάση ισοδυναμίας του r ως προς την σχέση “ $\equiv \pmod{I}$ ” είναι ακριβώς η κλάση ισοτιμίας του r modulo n .

(ii) Έστω $R = \mathbb{R}[x]$, I ιδεώδες του R και $g(x), f(x) \in \mathbb{R}[x]$. Παρατηρούμε τότε ότι $g(x) - f(x) \in I$ αν, και μόνο αν, $g(x) = f(x) + s(x)$ για κάποιο $s(x) \in I$.

Ορισμός. Έστω R δακτύλιος, I ιδεώδες του R και $a \in R$. Θέτουμε $a + I = \{a + x: x \in I\}$. Θέτουμε επίσης $R/I = \{r + I: r \in R\}$.

Σημείωση στον πιο πάνω ορισμό:

(i) Βλέπουμε ότι $r + I = \bar{r}$, όπου $\bar{r}$ είναι η κλάση ισοδυναμίας του $r \in R$ ως προς την σχέση ισοδυναμίας “ $\equiv \pmod{I}$ ” που έχουμε ορίσει πιο πάνω. Έχουμε επίσης ότι τα στοιχεία του συνόλου R/I είναι ακριβώς οι (διακεκριμένες) κλάσεις ισοδυναμίας ως προς την σχέση αυτή.

(ii) Έστω $r, s \in R$. Παρατηρούμε τότε ότι $r + I = s + I$ αν-ν $r \in s + I$ αν-ν $r - s \in I$ αν-ν $r \equiv s \pmod{I}$. (Μπορεί δηλαδή να έχουμε $r + I = s + I$ με $r \neq s$.)

Στην συνέχεια θα μιμηθούμε τον τρόπο που ορίσαμε $+$, $\cdot$ στο σύνολο $\mathbb{Z}_n$ για να ορίσουμε διμελείς πράξεις $+$, $\cdot$ στο σύνολο R/I έτσι ώστε $(R/I, +, \cdot)$ να είναι δακτύλιος.

Ορισμός. Έστω I ιδεώδες του δακτυλίου R . Στο σύνολο R/I προσπαθούμε να ορίσουμε δύο διμελείς πράξεις, πρόσθεση και πολλαπλασιασμό (χρησιμοποιώντας τα ίδια σύμβολα $+$, $\cdot$) ως εξής: Για $a, b \in R$,

$$(a + I) + (b + I) = (a + b) + I,$$

$$(a + I)(b + I) = ab + I.$$

(Προσπαθούμε να ορίσουμε δηλαδή $\bar{a} + \bar{b} = \overline{a + b}$ και $\bar{a} \cdot \bar{b} = \overline{ab}$.)

Πρέπει να βεβαιωθούμε ότι οι ‘αντιστοιχίες’ $+$, $\cdot$ που έχουμε ορίσει πιο πάνω είναι ‘καλά ορισμένες’, ότι δηλαδή πράγματι αποτελούν διμελείς πράξεις πάνω στο σύνολο R/I :

Έστω ότι $a + I = a' + I$ και $b + I = b' + I$, όπου $a, a', b, b' \in R$. Τότε $a - a' \in I$, $b - b' \in I$ και επομένως $(a + b) - (a' + b') = (a - a') + (b - b') \in I$. Συνεπώς $(a + b) + I = (a' + b') + I$.

Έχουμε επίσης ότι $a = a' + c$ και $b = b' + d$ για κάποια $c, d \in I$, και επομένως $ab = (a' + c)(b' + d) = a'b' + a'd + cb' + cd$. Επειδή I είναι ιδεώδες του R και $c, d \in I$ έχουμε $a'd, cb', cd \in I$, συνεπώς $ab - a'b' \in I$. Συνάγουμε ότι $ab + I = a'b' + I$.

Πρόταση 17.4. Έστω I ιδεώδες του δακτυλίου R . Το σύνολο R/I αποτελεί δακτύλιο ως προς την πρόσθεση (+) και πολλαπλασιασμό ($\cdot$) που έχουμε ορίσει πιο πάνω.

Απόδειξη. Ελέγχουμε ότι ισχύουν ιδιότητες. Για παράδειγμα αν $r, s, t \in R$, τότε $\bar{r} + (\bar{s} + \bar{t}) = \bar{r} + \overline{(s+t)} = \overline{r+(s+t)} = \overline{(r+s)+t} = \overline{(r+s)} + \bar{t} = (\bar{r} + \bar{s}) + \bar{t}$. Με παρόμοιο τρόπο μπορούμε να δείξουμε ότι ισχύουν και οι υπόλοιπες ιδιότητες χρησιμοποιώντας τους ορισμούς των +, $\cdot$ και τις αντίστοιχες ιδιότητες του δακτυλίου R . $\square$

Σημείωση 17.5. (i) Το μηδενικό στοιχείο του R/I είναι το $0_R + I (= I)$.

(ii) Αν R είναι ένας μεταθετικός 1-δακτύλιος και I είναι ένα γνήσιο ιδεώδες του R τότε R/I είναι επίσης ένας μεταθετικός 1-δακτύλιος με μοναδιαίο στοιχείο το $1_R + I$.

Ορισμός. Ο δακτύλιος R/I που μόλις έχουμε κατασκευάσει καλείται ο **δακτύλιος πηλίκο** του δακτυλίου R ως προς το ιδεώδες I .

Σημείωση 17.6. Έστω I ιδεώδες του δακτυλίου R . Όπως έχουμε δει (Παρατήρηση 17.1), $(I, +)$ είναι υποομάδα της $(R, +)$ και αφού $(R, +)$ είναι μια αβελιανή ομάδα έχουμε ότι $(I, +) \triangleleft (R, +)$. Συνεπώς μπορεί να οριστεί η αντίστοιχη ομάδα πηλίκο, τα στοιχεία της οποίας είναι τα σύμπλοκα της υποομάδας I στην ομάδα R (προσθετικός συμβολισμός) και τα οποία προφανώς συμπίπτουν με τις κλάσεις $r + I$ που έχουμε ορίσει αμέσως πιο πάνω. Σύμφωνα όμως με τον ορισμό μας, έχουμε ότι και τα στοιχεία του δακτυλίου πηλίκο R/I είναι ακριβώς οι κλάσεις $r + I$. Επιπλέον, η πρόσθεση που έχουμε ορίσει στον δακτύλιο πηλίκο R/I συμπίπτει με την πρόσθεση ('άθροισμα' υποσυνόλων) που έχουμε ορίσει στην αντίστοιχη ομάδα πηλίκο — συγκρίνετε με την Πρόταση 14.18 (προσθετικός συμβολισμός).

Παραδείγματα 17.7. (i) Έστω I ιδεώδες του δακτυλίου R . Η φυσιολογική απεικόνιση $\pi: R \rightarrow R/I: r \mapsto r + I$, ($r \in R$) είναι ένας επιρριπτικός ομομορφισμός δακτυλίων.

(ii) Θέτουμε $p(x) = x^2 + 1 \in \mathbb{R}[x]$ και $I = \{p(x)f(x): f(x) \in \mathbb{R}[x]\}$. Όπως έχουμε δει, το I είναι ένα ιδεώδες του δακτυλίου $\mathbb{R}[x]$. Στον δακτύλιο πηλίκο $\mathbb{R}[x]/I$, κάθε στοιχείο είναι της μορφής $(a + bx) + I$, όπου $a, b \in \mathbb{R}$. (Υπόδειξη: Χρησιμοποιούμε το Θεώρημα 16.4.) Επίσης αν $(a + bx) + I = (a' + b'x) + I$ (όπου $a, a', b, b' \in \mathbb{R}$), τότε $a = a'$ και $b = b'$. (Υπόδειξη: $(a + bx) + -(a' + b'x) \in I$.) Αν $a, b, c, d \in \mathbb{R}$, το γινόμενο των στοιχείων $(a + bx) + I$ και $(c + dx) + I$ στον δακτύλιο $\mathbb{R}[x]/I$ δίνεται με $((a + bx) + I)((c + dx) + I) = (a + bx)(c + dx) + I = (ac + (bc + ad)x + bdx^2) + I$. Αφού $x^2 + 1 (= x^2 - (-1)) \in I$, έχουμε ότι $x^2 + I = -1 + I$. Έτσι προκύπτει ότι $((a + bx) + I)((c + dx) + I) = ((ac - bd) + (bc + ad)x) + I$. Συγκρίνετε με την πρόσθεση και τον πολλαπλασιασμό μιγαδικών αριθμών, και ελέγξτε επίσης ότι:

(a) Αν $a, b \in \mathbb{R}$ (όπου $a \neq 0$ ή $b \neq 0$), τότε το στοιχείο $(a + bx) + I$ είναι αντιστρέψιμο στον $\mathbb{R}[x]/I$ με αντίστροφο το στοιχείο $(c + dx) + I$, όπου $c = a/(a^2 + b^2)$ και $d = -b/(a^2 + b^2)$. Έπεται ότι ο μεταθετικός 1-δακτύλιος $\mathbb{R}[x]/I$ (προφανώς το I είναι γνήσιο ιδεώδες του $\mathbb{R}[x]$) είναι στην πραγματικότητα ένα σώμα. Το πολυώνυμο $x^2 + 1 \in \mathbb{R}[x]$ είναι ανάγωγο επί του $\mathbb{R}$ — συγκρίνετε με την Άσκηση 17.3.

(b) Η συνάρτηση $\phi: \mathbb{R}[x]/I \rightarrow \mathbb{C}: (a + bx) + I \mapsto a + ib$ ($a, b \in \mathbb{R}$) είναι ένας ισομορφισμός δακτυλίων. [Παρατήρηση: $\phi(x + I) = i$ (όπου $i^2 = -1$).]

Θεώρημα 17.8. Έστω $\theta: R \rightarrow S$ ένας ομομορφισμός δακτυλίων. Τότε $R/\ker \theta \cong \text{im} \theta$.

Απόδειξη. Ξεχνώντας προσωρινά την πολλαπλασιαστική δομή των δακτυλίων R και S , η απόδειξη του Θεωρήματος 14.29 μας εξασφαλίζει ότι η συνάρτηση $\hat{\theta}: R/\ker \theta \rightarrow \text{im} \theta : r + \ker \theta \mapsto \theta(r)$, ($r \in R$) είναι μια καλά ορισμένη συνάρτηση και επιπλέον $\hat{\theta}$ είναι ένας ισομορφισμός ομάδων $(R/\ker \theta, +) \rightarrow (\text{im} \theta, +)$. [Εξήγηση: Η συνάρτηση θ μπορεί να θεωρηθεί ως ένας ομομορφισμός ομάδων $(R, +) \rightarrow (S, +)$. Συγκρίνετε επίσης με την Σημείωση 17.6.] Για $r \in R$, θέτουμε $\bar{r} = r + \ker \theta$. Αν $r_1, r_2 \in R$, έχουμε τότε: $\hat{\theta}(\bar{r}_1 \cdot \bar{r}_2) = \hat{\theta}(\overline{r_1 r_2}) = \theta(r_1 r_2) = (\theta r_1)(\theta r_2) = (\hat{\theta} \bar{r}_1)(\hat{\theta} \bar{r}_2)$. Από την πιο πάνω συζήτηση, έχουμε επίσης ότι $\hat{\theta}(\bar{r}_1 + \bar{r}_2) = \hat{\theta}(\bar{r}_1) + \hat{\theta}(\bar{r}_2)$. $\square$

Παραδείγματα 17.9. (i) Ορίζουμε $\theta: \mathbb{Z} \rightarrow \mathbb{Z}_n : a \mapsto \bar{a}$ ($a \in \mathbb{Z}$). Τότε θ είναι ένας επιρριπτικός ομομορφισμός δακτυλίων με $\ker \theta = n\mathbb{Z}$. Συνεπώς $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$, όπως αναμενόταν.

(ii) Θα βρούμε ένα επιρριπτικό ομομορφισμό δακτυλίων $\theta: \mathbb{R}[x] \rightarrow \mathbb{C}$ με $\ker \theta = \{(x^2 + 1)f(x) : f(x) \in \mathbb{R}[x]\}$, συγκρίνετε με το Παράδειγμα 17.7(ii) και το Θεώρημα 17.8.

Θεωρούμε την συνάρτηση αποτίμησης $\text{ev}_c: \mathbb{R}[x] \rightarrow \mathbb{C}$ (όπου $c = i \in \mathbb{C}$). Θέτουμε $I = \{(x^2 + 1)f(x) : f(x) \in \mathbb{R}[x]\}$. Προφανώς $I \subseteq \ker \text{ev}_c$. Έστω τώρα $g(x) \in \ker \text{ev}_c$. Τότε $g(x) = (x^2 + 1)q(x) + r(x)$ για κάποια $q(x), r(x) \in \mathbb{R}[x]$, όπου $r(x) = \alpha_0 + \alpha_1 x$ για κάποια $\alpha_0, \alpha_1 \in \mathbb{R}$. Έπεται ότι $0 = \text{ev}_c(g) = \text{ev}_c(x^2 + 1)\text{ev}_c(q) + (\alpha_0 + \alpha_1 c) = \alpha_0 + \alpha_1 c$, και επομένως τα α_0 και α_1 είναι και τα δύο ίσα με μηδέν. Συμπεραίνουμε ότι $g \in I$, άρα $I = \ker \text{ev}_c$. Έστω τώρα $\beta_0 + \beta_1 i \in \mathbb{C}$ (με $\beta_0, \beta_1 \in \mathbb{R}$). Παρατηρούμε τότε ότι $\beta_0 + \beta_1 i = \text{ev}_c(\beta_0 + \beta_1 x)$, όπου $\beta_0 + \beta_1 x \in \mathbb{R}[x]$.

Ορισμός. Έστω R δακτύλιος και $\{a_1, \dots, a_n\}$ ένα πεπερασμένο υποσύνολο του R . Το ιδεώδες του R που παράγεται από τα $a_1, \dots, a_n$ (συμβολισμός: $\langle a_1, \dots, a_n \rangle$) ορίζεται ως η τομή όλων των ιδεωδών του R που περιέχουν το υποσύνολο $\{a_1, \dots, a_n\}$. (Προφανώς ο ίδιος ο δακτύλιος R είναι ένα ιδεώδες του R που περιέχει το υποσύνολο αυτό.)

Παρατήρηση. Έστω R δακτύλιος και $\{a_1, \dots, a_n\} \subseteq R$. Τότε $\{a_1, \dots, a_n\} \subseteq \langle a_1, \dots, a_n \rangle$. Επίσης, αν J είναι ιδεώδες του R με $\{a_1, \dots, a_n\} \subseteq J$, τότε $\langle a_1, \dots, a_n \rangle \subseteq J$.

Πρόταση 17.10. Έστω R μεταθετικός 1-δακτύλιος και $\{a_1, \dots, a_n\} \subseteq R$. Τότε $\langle a_1, \dots, a_n \rangle = \{r_1 a_1 + r_2 a_2 + \dots + r_n a_n : r_1, \dots, r_n \in R\}$.

Απόδειξη. Δεχόμαστε την υπόθεση. Θέτουμε $I = \{r_1 a_1 + r_2 a_2 + \dots + r_n a_n : r_1, \dots, r_n \in R\}$ ($\subseteq R$). Θα δείξουμε πρώτα ότι I είναι ιδεώδες του R και ότι $\{a_1, \dots, a_n\} \subseteq I$.

Έστω $a, b \in I$. Τότε $a = x_1 a_1 + \dots + x_n a_n$ και $b = y_1 a_1 + \dots + y_n a_n$ για κάποια $x_i, y_i \in R$. Έπεται ότι $-b = (-y_1) a_1 + \dots + (-y_n) a_n \in I$. Συνεπώς $a + (-b) = (x_1 + (-y_1)) a_1 + \dots + (x_n + (-y_n)) a_n \in I$. (Εξήγηση: $(x_i + (-y_i)) \in R$, $1 \leq i \leq n$.) Αν $r \in R$, τότε $ar = ra = r(x_1 a_1 + \dots + x_n a_n) = (rx_1) a_1 + \dots + (rx_n) a_n \in I$, αφού $rx_i \in R$ για $1 \leq i \leq n$. Συνάγουμε ότι I είναι ιδεώδες του R .

[Σημείωση: Για να δείξουμε ότι $a + -b \in I$ και $ar (= ra) \in I$ έχουμε χρησιμοποιήσει διάφορες ιδιότητες που ισχύουν στον δακτύλιο R , για παράδειγμα την επιμεριστική ιδιότητα.]

Αν τώρα $1 \leq i \leq n$, έχουμε $a_i = 0_R a_1 + \dots + 0_R a_{i-1} + 1_R a_i + 0_R a_{i+1} + \dots + 0_R a_n \in I$, και επομένως $\{a_1, \dots, a_n\} \subseteq I$. Αφού I είναι ιδεώδες του R με $\{a_1, \dots, a_n\} \subseteq I$, έπεται ότι $\langle a_1, \dots, a_n \rangle \subseteq I$. Συνεπώς, για να τελειώσουμε την απόδειξη είναι αρκετό να δείξουμε ότι οποιοδήποτε ιδεώδες του R το οποίο περιέχει το σύνολο $\{a_1, \dots, a_n\}$ υποχρεωτικά περιέχει και το I . (Πιο ειδικά, θα έχουμε τότε $\langle a_1, \dots, a_n \rangle \supseteq I$.) Υποθέτουμε λοιπόν ότι J είναι ένα ιδεώδες του R με $\{a_1, \dots, a_n\} \subseteq J$. Για οποιαδήποτε $x_1, \dots, x_n \in R$ έχουμε ότι $x_i a_i \in J$, και επομένως $x_1 a_1 + \dots + x_n a_n \in J$. Συνάγουμε ότι $I \subseteq J$ (άρα $I \subseteq \langle a_1, \dots, a_n \rangle$). $\square$

17.2. Περιοχές κυρίων ιδεωδών, Ευκλείδειες περιοχές

Ορισμός. Έστω R μεταθετικός 1-δακτύλιος. Ένα ιδεώδες J του R ονομάζεται *κύριο* αν $J = \langle a \rangle (= \{ra : r \in R\})$ για κάποιο $a \in R$. (Έχουμε δηλαδή ότι το ιδεώδες J είναι κύριο αν μπορεί να παραχθεί από ένα στοιχείο.)

Παράδειγμα 17.11. (i) Το ιδεώδες $I = \langle 12, 30 \rangle$ του $\mathbb{Z}$ είναι ένα κύριο ιδεώδες αφού $I = \langle 6 \rangle$ (συγκρίνετε με την απόδειξη του Θεωρήματος 9.6).

(ii) Το ιδεώδες $I = \langle 2, x \rangle$ του $\mathbb{Z}[x]$ δεν είναι κύριο.

Ορισμός. Μια περιοχή κυρίων ιδεωδών (ΠΚΙ) είναι μια ακέραια περιοχή με την ιδιότητα ότι κάθε ιδεώδες της είναι κύριο.

Παράδειγμα. (i) Ο δακτύλιος $\mathbb{Z}$ είναι περιοχή κυρίων ιδεωδών.

(ii) Ο δακτύλιος $\mathbb{Z}[x]$ είναι μια ακέραια περιοχή (Παραδείγματα 16.2(iii)), όμως δεν αποτελεί περιοχή κυρίων ιδεωδών αφού υπάρχουν ιδεώδη στον $\mathbb{Z}[x]$ που δεν είναι κύρια (Παράδειγμα 17.11(ii)).

Θεώρημα 17.12. Κάθε Ευκλείδεια περιοχή είναι περιοχή κυρίων ιδεωδών.

Απόδειξη. Έστω R μια Ευκλείδεια περιοχή. Υποθέτουμε ότι I είναι ιδεώδες της R . Αν $I = \{0_R\}$, τότε $I = \langle 0_R \rangle$ και I είναι κύριο ιδεώδες. Έστω τώρα ότι I περιέχει μη-μηδενικά στοιχεία. Τότε το σύνολο $S = \{\delta(a) : a \in I - \{0_R\}\} (\subseteq \mathbb{N} \cup \{0\})$ είναι ένα μη-κενό, κάτω φραγμένο υποσύνολο των ακεραίων. Έστω s το ελάχιστο στοιχείο του S (αρχή καλής διάταξης — παραλλαγή). Τότε υπάρχει $b \in I - \{0_R\}$ τέτοιο ώστε $\delta(b) = s$. Θα δείξουμε ότι $I = \langle b \rangle$. Προφανώς $\langle b \rangle \subseteq I$. Έστω τώρα $a \in I$. Τότε $a = qb + r$ για κάποια $q, r \in R$ όπου είτε $r = 0$, είτε $\delta(r) < \delta(b)$. Όμως $r = a - (qb) \in I$. Έπεται ότι $r = 0$ (μπορούμε εύκολα να αποκλείσουμε την περίπτωση ($r \neq 0$ και) $\delta(r) < \delta(b)$ από την επιλογή του b). Άρα $a = qb \in \langle b \rangle$. Συνάγουμε ότι $I \subseteq \langle b \rangle$ και επομένως $I = \langle b \rangle$. $\square$

Πόρισμα 17.13. Αν F είναι σώμα, τότε ο δακτύλιος πολυωνύμων $F[x]$ είναι μια περιοχή κυρίων ιδεωδών.

Παράδειγμα. Διατηρώντας τον συμβολισμό και την υπόθεση του Θεωρήματος 16.5 (και της απόδειξης του), θέτουμε $I = \{s(x)f(x) + t(x)g(x) : s(x), t(x) \in F[x]\}$. Τότε I είναι ένα (μη-μηδενικό) ιδεώδες του $F[x]$ και επομένως υπάρχει μονικό $e(x) \in I$ τέτοιο ώστε $I =$

$\langle e(x) \rangle$. Κάθε στοιχείο του I είναι γραμμικός συνδυασμός των $f(x)$ και $g(x)$ και επομένως το ίδιο συμβαίνει με το $e(x)$. Συνεπώς, $e(x) = \mu\kappa\delta(f(x), g(x))$ αφού ικανοποιούνται τα (i), (ii) και (iii) στον ορισμό του $\mu\kappa\delta$. Επιπλέον, κοιτάζετε την απόδειξη του Θεωρήματος 16.5, έχουμε ότι $e(x)$ είναι το μοναδικό μονικό πολυώνυμο ελάχιστου βαθμού στο I .

Παρατήρηση 17.14. Έστω R μεταθετικός 1-δακτύλιος, $a, b \in R$ και $u \in R^*$. Τότε ισχύουν:

- (i) $\langle a \rangle \subseteq \langle b \rangle$ αν, και μόνο αν, $a = cb$ για κάποιο $c \in R$.
- (ii) Αν ένα ιδεώδες I του R περιέχει το u τότε $I = R$.
- (iii) Αν $r \in R$, τότε $\langle r \rangle = \langle ur \rangle$.
- (iv) Στην περίπτωση που R είναι ακέραια περιοχή έχουμε ότι $\langle a \rangle = \langle b \rangle$ αν, και μόνο αν, $a = vb$ για κάποιο $v \in R^*$. (Πιο ειδικά $\langle a \rangle = R$ αν, και μόνο αν, $a \in R^*$, αφού προφανώς $\langle 1_R \rangle = R$.)

Ορισμός. Έστω R μια ακέραια περιοχή.

(1) Ένα στοιχείο $p \in R$ καλείται *ανάγωγο* αν $p \notin (R^* \cup \{0_R\})$ και, οποτεδήποτε $p = ab$ με $a, b \in R$, έχουμε ότι είτε $a \in R^*$ είτε $b \in R^*$.

(2) R καλείται *περιοχή μοναδικής παραγοντοποίησης* (ΠΜΠ) αν ισχύουν

- (i) κάθε στοιχείο του R που δεν ανήκει στο σύνολο $R^* \cup \{0_R\}$ μπορεί να εκφραστεί ως γινόμενο αναγώγων, και
- (ii) αν $p_1 \dots p_m = q_1 \dots q_n$, όπου p_i και q_j είναι ανάγωγα στοιχεία του R , τότε $m = n$ και (μετά από πιθανή αλλαγή της διάταξης) $p_i = u_i q_i$ με $u_i \in R^*$ ($1 \leq i \leq n$).

Σημείωση 17.15. (i) Αν p είναι ανάγωγο στοιχείο της ακέραιας περιοχής R και $u \in R^*$, τότε pu είναι επίσης ανάγωγο στοιχείο της R (κοιτάζετε την Άσκηση 17.4).

(ii) Το Θεμελιώδες Θεώρημα της Αριθμητικής μας λέει ότι $\mathbb{Z}$ είναι (ΠΜΠ). Σύμφωνα με τον ορισμό μας, τα ανάγωγα στοιχεία του $\mathbb{Z}$ είναι της μορφής $\pm p$ όπου p είναι πρώτος. (Στο πλαίσιο αυτής της συζήτησης, οι παραγοντοποιήσεις $2 \cdot 3$ και $(-2)(-3)$ του ακεραίου 6 είναι “ουσιαστικά ίδιες” — υπενθυμίζουμε ότι $\mathbb{Z}^* = \{1, -1\}$.)

(iii) Έστω F ένα σώμα. Έχουμε δει ότι τότε $F[x]$ είναι μια ακέραια περιοχή. Τα αντιστρέψιμα στοιχεία του $F[x]$ είναι τα μη-μηδενικά σταθερά πολυώνυμα. Τα ανάγωγα στοιχεία του $F[x]$ είναι τα γνωστά μας ανάγωγα πολυώνυμα επί του F (δηλαδή τα μη-μηδενικά πολυώνυμα $p(x) \in F[x]$ όπου $\deg(p) \geq 1$ και οποτεδήποτε $p(x) = f(x)g(x)$ με $f(x), g(x) \in F[x]$ προκύπτει ότι ένα από τα $f(x), g(x)$ είναι σταθερό πολυώνυμο).

Παράδειγμα. Θέτουμε $\omega = i\sqrt{5} \in \mathbb{C}$. Θέτουμε επίσης $R = \{a + b\omega : a, b \in \mathbb{Z}\}$. Στην Άσκηση 15.8 έχουμε δει ότι R είναι μια ακέραια περιοχή και ότι $R^* = \{1, -1\}$. Εύκολα μπορούμε να δείξουμε ότι τα στοιχεία $2, 3, 1 + \omega, 1 - \omega$ του R είναι ανάγωγα. Θεωρώντας τώρα την εξίσωση $6 = 2 \cdot 3 = (1 + \omega)(1 - \omega)$, συμπεραίνουμε ότι R δεν είναι περιοχή μοναδικής παραγοντοποίησης. [Για να δείξουμε ότι το 2 είναι ανάγωγο στοιχείο του R υποθέτουμε ότι

$2 = (a+b\omega)(x+y\omega)$, όπου $a, b, x, y \in \mathbb{Z}$. Έπεται ότι $4 = (a^2+5b^2)(x^2+5y^2)$ και επομένως $b = y = 0$. Συνάγουμε ότι $a = \pm 1$ ή ± 2 και $x = \pm 1$ ή $x = \pm 1$, άρα ο ένας από τους δύο παράγοντες ανήκει στο $R^* = \{1, -1\}$. Με παρόμοιο τρόπο δείχνουμε ότι και τα υπόλοιπα στοιχεία $3, 1+\omega, 1-\omega$ είναι ανάγωγα.]

Σημείωση 17.16. (i) Στην πραγματικότητα μπορεί να αποδειχθεί ότι $(\text{ΕΠ}) \Rightarrow (\text{ΠΚΙ}) \Rightarrow (\text{ΠΜΠ})$.

(ii) $\mathbb{Z}[x]$ είναι (ΠΜΠ) (προκύπτει από το Λήμμα του Gauss), όμως $\mathbb{Z}[x]$ δεν είναι (ΠΚΙ) αφού το ιδεώδες $I = \langle 2, x \rangle$ του $\mathbb{Z}[x]$ δεν είναι κύριο (Παράδειγμα 17.11(ii)).

(iii) Παράδειγμα (ΠΚΙ) που δεν είναι (ΕΠ): $R = \{a+b\sqrt{-19} : \text{είτε } a, b \in \mathbb{Z} \text{ είτε } a-\frac{1}{2}, b-\frac{1}{2} \in \mathbb{Z}\}$. (T.S. Motzkin, Bulletin of the AMS, volume 55.)

Παράδειγμα 17.17. Θα δείξουμε ότι ο υποδακτύλιος $R = \{a+ib : a, b \in \mathbb{Z}\}$ του $\mathbb{C}$ είναι μια Ευκλείδεια περιοχή με Ευκλείδεια συνάρτηση $\delta(a+ib) = a^2+b^2$. Παρατηρούμε πρώτα ότι R είναι μια ακέραια περιοχή (γιατί;). Επίσης, αν $z = a+ib$, τότε $\delta(z) = z\bar{z} = |z|^2$. Έστω τώρα $z_1, z_2 \in R - \{0\}$. Έχουμε τότε, $\delta(z_1 z_2) = (z_1 z_2)(\overline{z_1 z_2}) = z_1 z_2 \bar{z}_1 \bar{z}_2 = z_1 \bar{z}_1 z_2 \bar{z}_2 = \delta(z_1)\delta(z_2) \geq \delta(z_1)$, αφού $\delta(z_2) \geq 1$. Έστω τώρα $z, w \in R$ με $w \neq 0$. Θεωρούμε το στοιχείο zw^{-1} ως στοιχείο του $\mathbb{C}$. Όμως $w\bar{w} = |w|^2 = \delta(w) (\geq 1 \text{ αφού } w \neq 0)$. Συνεπώς $w^{-1} = \bar{w}/\delta(w)$ όπου $\delta(w) \in \mathbb{N}$. Έπεται ότι $zw^{-1} = \frac{1}{r}z\bar{w}$ για κάποιο $r \in \mathbb{N}$ και επομένως $zw^{-1} = x+iy$ για κάποια $x, y \in \mathbb{Q}$. Γράφουμε $x = c+u$ και $y = d+v$ όπου $c, d \in \mathbb{Z}$ και $u, v \in \mathbb{Q}$ με $|u|, |v| \leq \frac{1}{2}$. [Επιλέγουμε δηλαδή “τους πιο κοντινούς ακέραιους” στα x και y — σε ορισμένες περιπτώσεις έχουμε περισσότερες από μία επιλογές.] Προκύπτει τότε ότι $z = w(c+id) + w(u+iv)$. Όμως $w(u+iv) \in R$ αφού $w(u+iv) = z - w(c+id)$. Επιπλέον, έχουμε ότι είτε $w(u+iv) = 0$ (αυτό ισχύει αν, και μόνο αν, $u = v = 0$ αφού $w \neq 0$) είτε $\delta(w(u+iv)) = |w(u+iv)|^2 = |w|^2|u+iv|^2 = \delta(w)(u^2+v^2) < \delta(w)$, αφού $(u^2+v^2) \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1$, δείχνοντας έτσι ότι R είναι μια (ΕΠ).

Παράδειγμα 17.18. Έστω $R = \{a+ib : a, b \in \mathbb{Z}\}$. Θέτουμε επίσης $\delta(a+ib) = a^2+b^2$. Θα βρούμε $q, r \in R$ με $\delta(r) < \delta(8+i)$ τέτοια ώστε $10+11i = q(8+i) + r$. Χρησιμοποιούμε τον συλλογισμό στο Παράδειγμα 17.17. Έχουμε τότε

$$\frac{10+11i}{8+i} = \frac{10+11i}{8+i} \cdot \frac{8-i}{8-i} = \frac{91+78i}{65} = (1+i) + \left(\frac{26}{65} + \frac{13}{65}i\right) = (1+i) + \left(\frac{2}{5} + \frac{1}{5}i\right).$$

Έπεται ότι $10+11i = (1+i)(8+i) + (3+2i)$. Θέτουμε $q = 1+i, r = 3+2i$. Τότε $q, r \in R$ και $\delta(r) = 3^2+2^2 = 13 < 65 = \delta(8+i)$.

Σχόλιο. Στο Κεφάλαιο 1 (κοιτάξτε στις Σημειώσεις και Σχόλια) συναντήσαμε το “θεώρημα των δύο τετραγώνων” του Fermat. Στην Άσκηση 9.16 αποδείξαμε την μια κατεύθυνση του θεωρήματος αυτού. Για να αποδειχθεί η αντίστροφη κατεύθυνση, σημαντικό ρόλο παίζει το γεγονός ότι ο δακτύλιος $R = \{a+ib : a, b \in \mathbb{Z}\}$ είναι μια ΕΠ όπως έχουμε δείξει στο Παράδειγμα 17.17.

17.3. Μεγιστικά ιδεώδη, επεκτάσεις σωμάτων

Πρόταση 17.19. Έστω F σώμα και $I = \langle f(x) \rangle$ όπου $f(x) \in F[x]$ με $\deg(f(x)) = n > 0$. Κάθε στοιχείο του $F[x]/I$ εκφράζεται με μοναδικό τρόπο στην μορφή $(\alpha_0 + \alpha_1 x + \alpha_2 x^2 +$

$\dots + \alpha_{n-1}x^{n-1}) + I$, όπου $\alpha_0, \alpha_1, \dots, \alpha_{n-1} \in F$.

Απόδειξη. Δεχόμαστε την υπόθεση. Έστω $g(x) \in F[x]$. Σύμφωνα με το θεώρημα διαίρεσης, $g(x) = q(x)f(x) + r(x)$ όπου $q(x), r(x) \in F[x]$ και είτε $r(x) = 0$, είτε $\deg(r) < n = \deg(f)$. Προφανώς $g(x) + I = r(x) + I$ αφού $g(x) - r(x) \in I$. Έστω τώρα ότι $(\alpha_0 + \alpha_1x + \dots + \alpha_{n-1}x^{n-1}) + I = (\beta_0 + \beta_1x + \dots + \beta_{n-1}x^{n-1}) + I$ ($\alpha_i, \beta_j \in F$). Έχουμε τότε ότι $h(x) \in I$, όπου $h(x) = (\alpha_0 - \beta_0) + (\alpha_1 - \beta_1)x + \dots + (\alpha_{n-1} - \beta_{n-1})x^{n-1} \in F[x]$. Αν $h(x)$ δεν είναι το μηδενικό πολυώνυμο θα είχαμε τότε $\deg(h) \geq n = \deg(f)$, (αφού $h(x) \in \langle f(x) \rangle$), που είναι άτοπο. Συνάγουμε ότι $h(x) = 0$ και επομένως $\alpha_i = \beta_i$, για $i = 0, 1, \dots, n-1$. $\square$

Ορισμός. Ένα ιδεώδες I του δακτυλίου R καλείται **μεγιστικό ιδεώδες** του R αν είναι γνήσιο και, επιπλέον, δεν υπάρχει ιδεώδες J του R με $I \subsetneq J \subsetneq R$.

Θεώρημα 17.20. Έστω R μεταθετικός 1-δακτύλιος και M ιδεώδες του R . Τότε R/M είναι σώμα αν, και μόνο αν, M είναι μεγιστικό ιδεώδες του R .

Απόδειξη. Υποθέτουμε ότι R είναι μεταθετικός 1-δακτύλιος και M ιδεώδες του R . Προφανώς έχουμε τότε ότι R/M είναι ένας μεταθετικός δακτύλιος.

Έστω πρώτα ότι R/M είναι σώμα. Τότε M είναι γνήσιο ιδεώδες αφού R/M περιέχει τουλάχιστον δύο στοιχεία. Υποθέτουμε τώρα ότι N είναι ιδεώδες του R με $M \subsetneq N$ και ότι $a \in N - M$. Έχουμε τότε $a + M \neq 0_R + M$ και επομένως $a + M \in (R/M)^*$. Έπεται ότι υπάρχει $b \in R$ με $(a + M)(b + M) = 1_R + M$ (προφανώς $1_R + M$ είναι το μοναδιαίο στοιχείο του R/M). Όμως $(a + M)(b + M) = ab + M$, άρα $ab + M = 1_R + M$. Συνεπώς $ab - 1_R = m$ για κάποιο $m \in M$ ($\subseteq N$). Άρα $1_R = ab - m \in N$, αφού $ab \in N$ (N είναι ιδεώδες, $a \in N$ και $b \in R$). Συνάγουμε ότι $N = R$.

Έστω τώρα ότι M είναι μεγιστικό ιδεώδες του R . Προφανώς $1_R \notin M$ (το ιδεώδες M είναι γνήσιο). Αφού $1_R + M \neq 0_R + M$ έχουμε ότι ο μεταθετικός δακτύλιος R/M είναι ένας 1-δακτύλιος με μοναδιαίο στοιχείο το $1_R + M$. Υποθέτουμε επίσης ότι $a \in R - M$. Αρκεί να δείξουμε ότι $a + M \in (R/M)^*$. Προφανώς M περιέχεται γνήσια στο ιδεώδες $M + \langle a \rangle$. Αφού M είναι μεγιστικό, έχουμε ότι $M + \langle a \rangle = R$ και επομένως $1_R = m + ra$ για κάποια $m \in M$ και $r \in R$ (R είναι ένας 1-δακτύλιος). Έπεται ότι $1_R + M = ra + M$. Όμως $ra + M = (r + M)(a + M) = (a + M)(r + M)$ αφού R/M είναι μεταθετικός δακτύλιος. Συνάγουμε ότι $a + M \in (R/M)^*$ και επομένως R/M είναι σώμα. $\square$

Πρόταση 17.21. Έστω ότι R είναι (ΠΚΙ) και ότι $a \in R - \{0_R\}$. Τότε $\langle a \rangle$ είναι μεγιστικό ιδεώδες του R αν, και μόνο αν, a είναι ανάγωγο στοιχείο του R .

Απόδειξη. Δεχόμαστε την υπόθεση.

Υποθέτουμε πρώτα ότι $\langle a \rangle$ είναι μεγιστικό ιδεώδες του R . Προφανώς $a \notin R^*$ αφού $\langle a \rangle \neq R$ (Παρατήρηση 17.14(iv) — το ιδεώδες $\langle a \rangle$ είναι γνήσιο). Έστω τώρα ότι $a = bc$ για κάποια $b, c \in R$. Τότε $\langle a \rangle \subseteq \langle b \rangle$. Αν $b \notin R^*$, τότε $\langle b \rangle$ είναι γνήσιο ιδεώδες του R και $\langle a \rangle = \langle b \rangle$ αφού το ιδεώδες $\langle a \rangle$ είναι μεγιστικό. Συνεπώς $a = bu$ για κάποιο $u \in R^*$. Έπεται ότι

$bu = a = bc$, άρα $b(u - c) = 0_R$. Όμως $b \neq 0_R$ αφού $a \neq 0_R$. Συνάγουμε ότι $u - c = 0_R$ αφού R είναι ακέραια περιοχή. (Άρα $c = u \in R^*$.)

Υποθέτουμε τώρα ότι a είναι ανάγωγο στοιχείο του R . Πιο ειδικά $a \notin R^*$ και επομένως $\langle a \rangle$ είναι γνήσιο ιδεώδες του R . Έστω J ιδεώδες του R με $\langle a \rangle \subsetneq J \subseteq R$. Τότε $J = \langle d \rangle$ για κάποιο $d \in R$ αφού R είναι (ΠΚΙ). Έπεται ότι $a = rd$ για κάποιο $r \in R - R^*$. Αφού a είναι ανάγωγο, έχουμε ότι $d \in R^*$. Συνάγουμε ότι $\langle d \rangle = R$ (επομένως $\langle a \rangle$ είναι μεγιστικό). $\square$

Ορισμός. Ένα ιδεώδες I ενός δακτυλίου R καλείται πρώτο αν είναι γνήσιο και, επιπλέον, από $ab \in I$ (όπου $a, b \in R$) προκύπτει ότι είτε $a \in I$, είτε $b \in I$.

Άσκηση. Έστω R μεταθετικός 1-δακτύλιος. Δείξτε τα πιο κάτω.

- (i) Αν I είναι γνήσιο ιδεώδες του R , τότε R/I είναι ακέραια περιοχή αν, και μόνο αν, I είναι πρώτο ιδεώδες.
- (ii) Κάθε μεγιστικό ιδεώδες του R είναι και πρώτο ιδεώδες.

Για να κατασκευάσουμε τους μιγαδικούς από τους πραγματικούς αριθμούς ‘προσαρτούμε’ στους πραγματικούς ένα στοιχείο i που ικανοποιεί $i^2 + 1 = 0$. (Συγκρίνετε με τα Παραδείγματα 17.7(ii) και 17.9(ii).) Πιο κάτω γενικεύουμε την κατασκευή αυτή.

Θεώρημα 17.22. Έστω F σώμα και $p(x) \in F[x]$ ένα ανάγωγο πολυώνυμο στο $F[x]$. Τότε ο δακτύλιος πηλίκο $E = F[x]/\langle p(x) \rangle$ είναι ένα σώμα το οποίο περιέχει (ένα ισομορφικό αντίγραφο με) το F και μια θέση μηδενισμού του $p(x)$.

Απόδειξη. Δεχόμαστε την υπόθεση. Τώρα $F[x]$ είναι (ΠΚΙ), επομένως η Πρόταση 17.21 μας εξασφαλίζει ότι $\langle p(x) \rangle$ είναι μεγιστικό ιδεώδες του $F[x]$. Συνεπώς $E = F[x]/\langle p(x) \rangle$ είναι σώμα. [Χρησιμοποιούμε το Θεώρημα 17.20 — προφανώς $F[x]$ είναι ένας μεταθετικός 1-δακτύλιος.] Θέτουμε $I = \langle p(x) \rangle$ και $F' = \{c + I : c \in F\} \subseteq E$. Εύκολα παρατηρούμε ότι F' είναι ένα υπόσωμα του E και ότι η απεικόνιση $c \mapsto c + I$ από το F στο F' είναι ένας ισομορφισμός δακτυλίων (άσκηση). Μέσω του ισομορφισμού αυτού ταυτίζουμε το σώμα F με το F' και με αυτό τον τρόπο θεωρούμε το F ως υπόσωμα του E (συγκρίνετε με την Παρατήρηση 15.14 και το Παράδειγμα 15.13(ii)). Γράφουμε $p(y) = c_0 + c_1y + \dots + c_ny^n \in F[y]$, όπου $c_i \in F$ και $n \geq 1$ (p είναι ανάγωγο πολυώνυμο). Θέτουμε $\alpha = x + I \in E$. Έχουμε τότε (χρησιμοποιώντας την ταύτιση: $F \ni c \leftrightarrow c + I \in F'$):

$$\begin{aligned} \text{ev}_\alpha(p) &= c_0 + c_1\alpha + \dots + c_n\alpha^n = (c_0 + I) + (c_1 + I)\alpha + \dots + (c_n + I)\alpha^n \\ &= (c_0 + I) + (c_1 + I)(x + I) + \dots + (c_n + I)(x + I)^n \\ &= (c_0 + I) + (c_1x + I) + \dots + (c_nx^n + I) = (c_0 + c_1x + \dots + c_nx^n) + I \\ &= p(x) + I = I = 0_E. \end{aligned}$$

Συνάγουμε ότι α είναι μια θέση μηδενισμού στο E για το πολυώνυμο $p(y) \in F[y]$ ($\subseteq E[y]$). $\square$

Σημείωση 17.23. Διατηρούμε τον συμβολισμό από το Θεώρημα 17.22 όπου έχουμε δείξει ότι υπάρχει κάποιο σώμα E και ένας ενριπτικός ομομορφισμός $\psi: F \rightarrow E$ τ.ω. το

πολυώνυμο $\psi^*(p)$ έχει μια θέση μηδενισμού $\alpha (= x + \langle p(x) \rangle)$ στο E . [Ως συνήθως, με ψ^* συμβολίζουμε τον ομομορφισμό δακτυλίων $F[y] \rightarrow E[y]$ που επάγεται από τον ψ (κοιτάζτε την Πρόταση 16.3).] Έστω S ένα σύνολο το οποίο είναι όμοιο προς το $E - \text{im} \psi$ (υπάρχει δηλαδή αμφιμονοσήμαντη συνάρτηση από το S στο συμπλήρωμα του $\text{im} \psi$ στο E), και το οποίο είναι ξένο προς το F . Θέτουμε $E' = F \cup S$. Τότε η συνάρτηση ψ μπορεί να επεκταθεί σε μια αμφιμονοσήμαντη συνάρτηση από το E' στο E , την οποία επίσης συμβολίζουμε με ψ . Στην συνέχεια θα μετατρέψουμε το σύνολο E' σε ένα σώμα το οποίο περιέχει το F ως υπόσωμα. Για να το πετύχουμε αυτό ορίζουμε, για $x, y \in E'$, πρόσθεση και πολλαπλασιασμό ως εξής: $x + y = \psi^{-1}(\psi(x) + \psi(y))$ και $xy = \psi^{-1}(\psi(x)\psi(y))$, όπου οι πράξεις στα δεξιά μέλη είναι οι πράξεις στο σώμα E . Περιορίζοντας τις νέες πράξεις στο F , παρατηρούμε ότι συμπίπτουν με τις δοσμένες πράξεις στο αρχικό σώμα F . Επιπλέον, θέτοντας $\xi = \psi^{-1}(\alpha)$ παρατηρούμε ότι $\text{ev}_\xi(p) = 0$. [Εξήγηση: $0 = \text{ev}_\alpha \psi^*(p) = \psi(\text{ev}_\xi(p))$.] Συνοψίζοντας, με μια προσαρμογή της απόδειξης του Θεωρήματος 17.22, έχουμε δείξει ότι πράγματι υπάρχει ένα σώμα E' το οποίο περιέχει το F ως υπόσωμα (και όχι απλά περιέχει ένα ισομορφικό αντίγραφο του F ως υπόσωμα) και μια θέση μηδενισμού του ανάγωγου (επί του F) πολυωνύμου $p(x) \in F[x]$.

Παρατήρηση 17.24. Συνεχίζουμε με την υπόθεση (και συμβολισμό) του Θεωρήματος 17.22 και με παρόμοιο συλλογισμό όπως στην απόδειξη του θεωρήματος αυτού μπορούμε να δείξουμε (με $\alpha = x + I$), ότι $\text{ev}_\alpha(g) = g(x) + I \in E$ για κάθε $g(y) \in F[y] (\subseteq E[y])$. Συγκρίνοντας τώρα με την Πρόταση 17.19 παρατηρούμε ότι κάθε στοιχείο του $E = F[x]/\langle p(x) \rangle$ εκφράζεται με μοναδικό τρόπο στην μορφή $d_0 + d_1\alpha + d_2\alpha^2 + \dots + d_{n-1}\alpha^{n-1} (= (d_0 + d_1x + d_2x^2 + \dots + d_{n-1}x^{n-1}) + I)$, όπου $d_0, d_1, \dots, d_{n-1} \in F$. Η πρόσθεση και ο πολλαπλασιασμός στο E δίνονται από τους συνηθισμένους κανόνες της αριθμητικής με τον επιπλέον περιορισμό ότι $\text{ev}_\alpha(p) = 0$. Στην περίπτωση που F είναι ένα πεπερασμένο σώμα με ακριβώς q στοιχεία, έχουμε ότι E περιέχει ακριβώς q^n στοιχεία (όπου $n = \deg(p)$).

Παράδειγμα 17.25. (i) Η κατασκευή του $\mathbb{C} (= \mathbb{R}[x]/\langle x^2 + 1 \rangle)$: Κάθε μιγαδικός αριθμός εκφράζεται μοναδικά στην μορφή $d_0 + d_1i$ ($d_0, d_1 \in \mathbb{R}$) όπου $i^2 = -1$. [Θέτουμε $p(y) = y^2 + 1 \in \mathbb{R}[y]$, τότε $\text{ev}_i(p) = i^2 + 1 = 0$, όπου $i = x + \langle p(x) \rangle$.]

(ii) Θα κατασκευάσουμε ένα πεπερασμένο σώμα με ακριβώς τέσσερα στοιχεία: Ξεκινούμε με το σώμα $F = \mathbb{Z}_2 = \{0, 1\}$. Το πολυώνυμο $p(x) = 1 + x + x^2 \in F[x]$ είναι ανάγωγο επί του F αφού η μόνη πιθανή παραγοντοποίηση θα ήταν σε δύο παράγοντες βαθμού 1 και αυτό θα σήμαινε ότι το σώμα F περιέχει θέση μηδενισμού του $p(x)$. Όμως $0^2 + 0 + 1 \neq 0$ και $1^2 + 1 + 1 \neq 0$. Θέτουμε $E = F[x]/\langle p(x) \rangle$ και $\alpha = x + \langle p(x) \rangle$. Έχουμε τότε ότι $1 + \alpha + \alpha^2 (= \text{ev}_\alpha(p)) = 0$ και ότι $E = \{d_0 + d_1\alpha : d_0, d_1 \in F\} = \{0, 1, \alpha, 1 + \alpha\}$ (χρησιμοποιούμε τα 17.22 και 17.24). Το σώμα E έχει ακριβώς 4 στοιχεία. Παρατηρούμε επίσης ότι για κάθε $x \in E$ ισχύει $x + x = x(1 + 1) = x \cdot 0 = 0$, άρα $x = -x$. Θέτοντας $\beta = 1 + \alpha = \alpha^2$, παίρνουμε τους ακόλουθους πίνακες πρόσθεσης και πολλαπλασιασμού στο σώμα E :

+	0	1	α	β	·	0	1	α	β
0	0	1	α	β	0	0	0	0	0
1	1	0	β	α	1	0	1	α	β
α	α	β	0	1	α	0	α	β	1
β	β	α	1	0	β	0	β	1	α

[Για παράδειγμα, $\beta\beta = (1 + \alpha)(1 + \alpha) = (1 + \alpha + \alpha^2) + \alpha = 0 + \alpha = \alpha$.]

Σημείωση. Αν p είναι πρώτος και $n \in \mathbb{N}$, τότε ένα πεπερασμένο σώμα με ακριβώς p^n στοιχεία μπορεί να κατασκευαστεί με τον ίδιο τρόπο αν υπάρχει ανάγωγος πολυώνυμο βαθμού n στον δακτύλιο $\mathbb{Z}_p[x]$. Στην πραγματικότητα μπορούμε να δείξουμε ότι αυτό είναι πάντα δυνατό.

Θεώρημα 17.26. (Galois). Για οποιονδήποτε πρώτο p και οποιονδήποτε θετικό ακέραιο n , υπάρχει ένα ανάγωγος πολυώνυμο βαθμού n στον $\mathbb{Z}_p[x]$ και επομένως ένα πεπερασμένο σώμα με ακριβώς p^n στοιχεία.

Ασκήσεις

- 17.1 (i) Έστω R δακτύλιος. Δείξτε ότι η τομή οποιασδήποτε (μη-κενής) οικογένειας ιδεωδών του R είναι επίσης ιδεώδες του R .
(ii) Έστω R δακτύλιος και I, J ιδεώδη του R . Θέτουμε $I + J = \{a + b : a \in I, b \in J\}$. Δείξτε ότι $I + J$ είναι ιδεώδες του R .
- 17.2 Έστω R μεταθετικός 1-δακτύλιος. Δείξτε ότι R είναι σώμα αν, και μόνο αν, τα μόνα ιδεώδη του R είναι το $\{0_R\}$ και το R .
- 17.3 Έστω F σώμα και $s(x), p(x) \in F[x]$ όπου $p(x)$ είναι ανάγωγος επί του F . Θέτουμε $I = \{p(x)f(x) : f(x) \in F[x]\}$. Αν $p(x) \nmid s(x)$, δείξτε ότι $s(x) + I$ είναι αντιστρέψιμο στοιχείο του δακτυλίου πηλίκο $F[x]/I$.
- 17.4 Αν p είναι ανάγωγος στοιχείο της ακέραιας περιοχής R και $u \in R^*$, δείξτε ότι pu είναι επίσης ανάγωγος στοιχείο της R .
- 17.5 Θέτουμε $R = \{a + ib : a, b \in \mathbb{Z}\}$. Βρείτε $(q_j, r_j) \in R \times R$ με $|r_j|^2 < 4$ τ.ω. $3 + 5i = 2q_j + r_j$ για $1 \leq j \leq 4$.
- 17.6 Δείξτε ότι το ιδεώδες $\langle 2, x \rangle$ του δακτυλίου $\mathbb{Z}[x]$ δεν είναι κύριο.
- 17.7 Έστω R μεταθετικός 1-δακτύλιος. Δείξτε τα πιο κάτω.
(i) Αν I είναι γνήσιο ιδεώδες του R , τότε R/I είναι ακέραια περιοχή αν, και μόνο αν, I είναι πρώτο ιδεώδες.
(ii) Κάθε μεγιστικό ιδεώδες του R είναι και πρώτο ιδεώδες.
- 17.8 Κατασκευάστε σώματα F_1, F_2 με ακριβώς 8 και 9 στοιχεία αντίστοιχα.

Λύσεις ασκήσεων

1.1 Τα (i), (iii) και (iv) είναι προτάσεις ενώ το (ii) δεν είναι πρόταση.

1.2 Η λύση για τα (iv), (v), (vii) προκύπτει από τους πιο κάτω αληθοπίνακες:

p	q	$\sim p$	$\sim q$	$p \wedge q$	$\sim(p \wedge q)$	$(\sim p) \vee (\sim q)$	$p \vee q$	$\sim(p \vee q)$	$(\sim p) \wedge (\sim q)$
α	α	ψ	ψ	α	ψ	ψ	α	ψ	ψ
α	ψ	ψ	α	ψ	α	α	α	ψ	ψ
ψ	α	α	ψ	ψ	α	α	α	ψ	ψ
ψ	ψ	α	α	ψ	α	α	ψ	α	α

p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$
α	α	α	α	α	α	α	α
α	α	ψ	α	α	α	ψ	α
α	ψ	α	α	α	ψ	α	α
α	ψ	ψ	ψ	ψ	ψ	ψ	ψ
ψ	α	α	α	ψ	ψ	α	ψ
ψ	α	ψ	α	ψ	ψ	ψ	ψ
ψ	ψ	α	α	ψ	ψ	α	ψ
ψ	ψ	ψ	ψ	ψ	ψ	ψ	ψ

Για το (viii): Υποθέτουμε πρώτα ότι $p \leftrightarrow q$ είναι αληθής. Αν p είναι αληθής, τότε q είναι αληθής και οι προτάσεις $p \rightarrow q$, $q \rightarrow p$ είναι και οι δύο αληθείς. Παρόμοια, αν p είναι ψευδής, τότε q είναι επίσης ψευδής και πάλι οι προτάσεις $p \rightarrow q$, $q \rightarrow p$ είναι και οι δύο αληθείς.

Έστω τώρα ότι $p \leftrightarrow q$ είναι ψευδής με την p αληθή. Τότε q είναι ψευδής και η πρόταση $p \rightarrow q$ είναι ψευδής δείχνοντας έτσι ότι η πρόταση $((p \rightarrow q) \wedge (q \rightarrow p))$ είναι ψευδής. Χρησιμοποιούμε παρόμοιο συλλογισμό για την περίπτωση που $p \leftrightarrow q$ είναι ψευδής με την p να είναι ψευδή.

1.3 Γράφουμε $\sqrt{3} = m/n$ (όπου m είναι ακέραιος και n φυσικός με τους m, n να έχουν το 1 ως τον μόνο κοινό θετικό διαιρέτη). Έχουμε τότε ότι $3n^2 = m^2$ και επομένως m είναι πολλαπλάσιο του 3. [Εξήγηση: Προφανώς, το m^2 είναι πολλαπλάσιο του 3. Αν m δεν είναι πολλαπλάσιο του 3, τότε $m = 3k + 1$ ή $m = 3k + 2$ για κάποιο ακέραιο k (περισσότερα για το σημείο αυτό στο Κεφάλαιο 9). Αν $m = 3k + 1$, τότε $m^2 = 9k^2 + 6k + 1 = 1 + 3(2k + 3k^2)$, άρα m^2 δεν είναι πολλαπλάσιο του 3 που είναι άτοπο. Παρόμοια για την περίπτωση που $m = 3k + 2$.] Γράφοντας τώρα $m = 3k$ όπου k είναι ακέραιος προκύπτει ότι $3n^2 = 9k^2$ ή, ισοδύναμα, $n^2 = 3k^2$. Έχουμε δείξει ότι και ο ακέραιος n^2 , και επομένως ο ακέραιος n , είναι πολλαπλάσιο του 3 που είναι άτοπο.

1.4 Έστω ότι υπάρχουν ρητοί r, s με $\sqrt{3} = r + s\sqrt{2}$. Υπολογίζοντας το τετράγωνο για κάθε ένα από τα μέλη της εξίσωσης αυτής παίρνουμε $3 = r^2 + 2s^2 + 2\sqrt{2}rs$. Αν $rs \neq 0$, τότε από την τελευταία εξίσωση βλέπουμε ότι $\sqrt{2}$ μπορεί να εκφραστεί στην μορφή a/b όπου a ακέραιος και b φυσικός, που είναι άτοπο (έχουμε δείξει ότι $\sqrt{2}$ είναι άρρητος). Συνεπώς υποθέτουμε ότι $rs = 0$. Αν $s = 0$, έχουμε τότε ότι $3 = r^2$ που είναι άτοπο (Άσκηση 1.3). Απομένει λοιπόν να εξετάσουμε την περίπτωση που $rs = 0$ με $s \neq 0$. Έχουμε τότε ότι $r = 0$ και επομένως $3 = 2s^2$. Γράφοντας $s = \frac{m}{n}$ (όπου m ακέραιος, n φυσικός, με τους

m, n να μην έχουν άλλους κοινούς θετικούς διαιρέτες εκτός από το 1) προκύπτει ότι $3n^2 = 2m^2$. Αυτό μας οδηγεί στο συμπέρασμα ότι m, n είναι και οι δύο άρτιοι που και πάλι είναι άτοπο. [Εξήγηση: ο αριθμός $3n^2$ είναι άρτιος και επομένως και ο n^2 είναι άρτιος αφού το γινόμενο δύο περιττών αριθμών είναι περιττός.]

1.5 Θέτουμε $a = m/n$ και $a' = m'/n'$ (όπου m, m' ακέραιοι και n, n' φυσικοί). Υποθέτουμε επιπλέον ότι b είναι άρρητος.

(i) Έχουμε τότε ότι $a + a' = \frac{mn' + nm'}{nn'}$, όπου $mn' + nm'$ είναι ακέραιος και nn' φυσικός. Άρα $a + a'$ είναι ρητός

(ii) Έχουμε $aa' = mm'/nn'$, όπου mm' ακέραιος, nn' φυσικός. Άρα aa' είναι ρητός.

(iii) Έστω ότι $a + b$ είναι ρητός. Τότε $a + b = c/d$ (c ακέραιος, d φυσικός). Έπεται (από το (i)) ότι $b = (c/d) - a = c/d + (-a)$ είναι ρητός (αφού προφανώς $-a$ είναι ρητός οποτεδήποτε a είναι ρητός), που είναι άτοπο.

(iv) Υποθέτουμε ότι $a \neq 0$ και ότι ab είναι ρητός. Αφού $a \neq 0$, έχουμε ότι $m \neq 0$ και επομένως ο ρητός αριθμός n/m ικανοποιεί $(n/m)a = 1$. Έπεται ότι $b = 1 \cdot b = ((n/m)a)b = (n/m)(ab)$ είναι ρητός (από το (ii)), αφού n/m και ab είναι και οι δύο ρητοί, που είναι άτοπο.

1.6 Η λύση για το (iii) προκύπτει από τον πιο κάτω αληθοπίνακα.

p	q	r	$p \vee q$	$q \vee r$	$(p \vee q) \vee r$	$p \vee (q \vee r)$
α	α	α	α	α	α	α
α	α	ψ	α	α	α	α
α	ψ	α	α	α	α	α
α	ψ	ψ	α	ψ	α	α
ψ	α	α	α	α	α	α
ψ	α	ψ	α	α	α	α
ψ	ψ	α	ψ	α	α	α
ψ	ψ	ψ	ψ	ψ	ψ	ψ

(i) Δεν ισχύει. Θεωρούμε την περίπτωση που r είναι ψευδής και οι p, q είναι και οι δύο αληθείς.

(ii) Δεν ισχύει. Θεωρούμε την περίπτωση που p είναι αληθής και q ψευδής.

(iv) Ισχύει. Υποθέτουμε πρώτα ότι $(p \wedge q) \wedge r$ είναι αληθής. Έπεται ότι $p \wedge q$ και r είναι και οι δύο αληθείς και επομένως p, q, r είναι όλες αληθείς. Συμπεραίνουμε ότι η πρόταση $p \wedge (q \wedge r)$ είναι επίσης αληθής. Με παρόμοιο συλλογισμό δείχνουμε ότι $(p \wedge q) \wedge r$ είναι αληθής οποτεδήποτε $p \wedge (q \wedge r)$ είναι αληθής.

1.7 (i) (a), (ii) (b), (iii) (b), (iv) (d), (v) (a)

1.8 Όχι ($n = 11 : 2^{11} - 1 = 2047 = 23 \cdot 89$)

2.1 (i) $\emptyset$, (ii) $\{1\}$, (iii) $\{1, -1\}$, (iv) $\{1, 3, 7\}$.

[Υπόδειξη για το (iv): $\frac{n+9}{n+1} = 1 + \frac{8}{n+1}$, χρειαζόμαστε το $n+1$ να είναι διαιρέτης του 8.]

2.2 $\{-2, -1, 0, 1, 2\}$

2.3 (i) 0, 1, 1, 2

(ii) 8, 1, 2

2.4 $A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c), (3, a), (3, b), (3, c)\}$

$A \times A = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$

2.5 (i) Ισχύει: Προφανώς $A \times B = B \times A$ οποτεδήποτε $A = B$. Έστω τώρα ότι $A \times B = B \times A$ με $A \neq B$. Υποθέτουμε, χωρίς βλάβη της γενικότητας, ότι $x \in B - A$. Αν a είναι οποιοδήποτε στοιχείο του A , τότε $(a, x) \in A \times B$, όμως $(a, x) \notin B \times A$.

(ii) Δεν ισχύει: Θέτουμε $A = \{1, 2\} = B$ και $S = \{(1, 1), (2, 2)\} \subseteq A \times B$. Παρατηρούμε ότι δεν υπάρχουν $C \subseteq A$ και $D \subseteq B$ με $S = C \times D$.

2.6 (i) $x \in (A \cup B)' \Leftrightarrow x \notin A \cup B \Leftrightarrow x \notin A$ και $x \notin B \Leftrightarrow x \in A' \text{ και } x \in B' \Leftrightarrow x \in A' \cap B'$.

(ii) $x \in (A \cap B)' \Leftrightarrow x \notin A \cap B \Leftrightarrow x \notin A$ ή $x \notin B \Leftrightarrow x \in A' \text{ ή } x \in B' \Leftrightarrow x \in A' \cup B'$.

(iii) $x \in C - (A \cup B) \Leftrightarrow x \in C \cap (A \cup B)' \Leftrightarrow x \in C \cap (A' \cap B') \Leftrightarrow x \in (C \cap A') \cap (C \cap B') \Leftrightarrow x \in (C - A) \cap (C - B)$.

(iv) Θέτουμε $A = \{x: a(x)\}$, $B = \{x: b(x)\}$, $C = \{x: c(x)\}$. Τότε, χρησιμοποιώντας το Θεώρημα 1.2(vii), έχουμε $A \cap (B \cup C) = \{x: a(x) \wedge (b(x) \vee c(x))\} = \{x: (a(x) \wedge b(x)) \vee (a(x) \wedge c(x))\} = \{x: x \in A \cap B \text{ ή } x \in A \cap C\} = (A \cap B) \cup (A \cap C)$,

(v) $x \in C - (A \cap B) \Leftrightarrow x \in C \cap (A \cap B)' \Leftrightarrow x \in C \cap (A' \cup B') \Leftrightarrow x \in (C \cap A') \cup (C \cap B') \Leftrightarrow x \in (C - A) \cup (C - B)$.

(vi) $x \in B - (B - A) \Leftrightarrow x \in B \cap (B - A)' \Leftrightarrow x \in B \cap (B' \cup A) \Leftrightarrow x \in (B \cap B') \cup (B \cap A) \Leftrightarrow x \in \emptyset \cup (B \cap A) (= B \cap A = A \cap B)$.

2.7 (i)–(v): Ισχύουν όλα.

[Για το (v): $x \in (A \cup B) \times C \Leftrightarrow x = (d, c)$ για κάποιο $d \in A \cup B$ και κάποιο $c \in C \Leftrightarrow x = (a, c)$ ή $x = (b, c)$, (όπου $a \in A$, $b \in B$, $c \in C$) $\Leftrightarrow x \in (A \times C)$ ή $x \in (B \times C) \Leftrightarrow x \in (A \times C) \cup (B \times C)$]

2.8 (i) $\exists_{x \in \mathbb{Z}} \forall_{y \in \mathbb{Z}} (x \geq y)$.

Άρνηση: $\forall_{x \in \mathbb{Z}} \exists_{y \in \mathbb{Z}} (x < y)$, που είναι αληθές.

(ii) $\forall_{n \in \mathbb{Z}} \exists_{m_1, m_2 \in \mathbb{Z}} (2n = (2m_1 + 1) + (2m_2 + 1))$, που είναι αληθές.

Άρνηση: $\exists_{n \in \mathbb{Z}} \forall_{m_1, m_2 \in \mathbb{Z}} (2n \neq (2m_1 + 1) + (2m_2 + 1))$

2.9 (i) Το τετράγωνο οποιουδήποτε φυσικού αριθμού είναι φυσικός αριθμός. (Αληθές.)

(ii) Το άθροισμα των τετραγώνων οποιωνδήποτε δύο ακεραίων ισούται με το τετράγωνο κάποιου ακεραίου. (Ψευδής.)

(iii) Το άθροισμα των τετραγώνων οποιωνδήποτε τριών πραγματικών αριθμών ισούται με οκτώ φορές κάποιο πραγματικό αριθμό. (Αληθές.)

3.1 f είναι 1-1: Αν $2n_1 - 1 = 2n_2 - 1$ όπου $n_1, n_2 \in \mathbb{N}$, τότε $n_1 = n_2$.

f είναι επί: Αν $y \in Y$, τότε $x = \frac{1}{2}(y + 1) \in \mathbb{N}$ και $f(x) = 2(\frac{1}{2}(y + 1)) - 1 = y$. Θέτουμε $g: Y \rightarrow \mathbb{N} : y \mapsto \frac{1}{2}(y + 1)$, ($y \in Y$). Τότε $g \circ f = i_{\mathbb{N}}$ και $f \circ g = i_Y$, συνεπώς $g = f^{-1}$.

3.2 Είναι το γράφημα της συνάρτησης $f: \mathbb{R} \rightarrow \mathbb{Z} : x \mapsto \begin{cases} 1, & \text{αν } x \in \mathbb{N}, \\ 0, & \text{αν } x \in \mathbb{R} - \mathbb{N}. \end{cases}$

3.3 (i) Ναι (ii) Όχι (iii) 3^4 (iv) 4

3.4 (i) (a) g, h είναι 1-1, όχι όμως η f .

(b) f, g, h δεν είναι επί: Παρατηρούμε ότι $3 \in \mathbb{N}$, όμως δεν υπάρχουν $x, y \in \mathbb{N}$ με $f(x) = 3, g(y) = 3$. Επίσης $1 \in \mathbb{N}$, και $h(x) = 2x + 1 > 1$ για όλα τα $x \in \mathbb{N}$.

(ii) $h \circ (g \circ f) = (h \circ g) \circ f = \phi$, όπου $\phi: \mathbb{N} \rightarrow \mathbb{N}: n \mapsto \begin{cases} 5, & (n > 100), \\ 11, & (n \leq 100), \end{cases}$ (όπου $n \in \mathbb{N}$).

3.5 Έστω Y_1 και Y_2 τα σύνολα των άρτιων και περιττών φυσικών αριθμών αντίστοιχα. Τότε $f: Y_1 \rightarrow Y_2: x \mapsto x - 1$ ($x \in Y_1$), είναι αμφιμονοσήμαντη.

3.6 (i) Όχι (ii) Ναι (iii) Όχι (iv) 15

3.7 (i) $f: \mathbb{N} \rightarrow \mathbb{N}: x \mapsto x + 1$, ($x \in \mathbb{N}$). (Τότε $f(x) \geq 2$ για όλα τα $x \in \mathbb{N}$.)

(ii) Θέτουμε $f(x) = \begin{cases} 1, & \text{αν } x = 1, \\ 1, & \text{αν } x = 2, \\ x - 1, & \text{αν } x \geq 3. \end{cases}$

(iii) Θέτουμε $f(x) = \begin{cases} 2, & \text{αν } x = 1, \\ 1, & \text{αν } x = 2, \\ x, & \text{αν } x \geq 3, \end{cases}$ και $g(x) = \begin{cases} 3, & \text{αν } x = 2, \\ 2, & \text{αν } x = 3, \\ x, & \text{αν } x \in \mathbb{N} - \{2, 3\}. \end{cases}$

Τότε $(g \circ f)(2) = 1$ και $(f \circ g)(2) = 3$.

3.8 (i) Κοιτάξτε την Πρόταση 3.6(i).

(ii) Υποθέτουμε ότι $g \circ f$ είναι 1-1. Έστω τώρα ότι $f(x_1) = f(x_2)$, όπου $x_1, x_2 \in X$. Αφού g είναι συνάρτηση, έχουμε ότι $g(f(x_1)) = g(f(x_2))$. Άρα $(g \circ f)(x_1) = (g \circ f)(x_2)$ από τον ορισμό της σύνθεσης συναρτήσεων. Τέλος, η υπόθεση μας ότι $g \circ f$ είναι 1-1 μας εξασφαλίζει ότι $x_1 = x_2$.

(iii) Υποθέτουμε ότι f και g είναι και οι δύο επί. Έστω τώρα $z \in Z$. Αφού g είναι επί, υπάρχει $y \in Y$ τέτοιο ώστε $z = g(y)$. Αφού f είναι επί, υπάρχει $x \in X$ τέτοιο ώστε $y = f(x)$. Συνάγουμε ότι υπάρχει $x \in X$ τέτοιο ώστε $z = g(y) = g(f(x)) = (g \circ f)(x)$ και επομένως η $g \circ f$ είναι επί.

(iv) Υποθέτουμε ότι η $g \circ f$ είναι επί. Έστω $z \in Z$. Τότε $z = (g \circ f)(x)$ για κάποιο $x \in X$ αφού $g \circ f$ είναι επί. Έπεται ότι $z = g(f(x))$ όπου $f(x) \in Y$. Συμπεραίνουμε ότι g είναι επί.

Τελευταίο μέρος: Θέτουμε $X = \{1, 2\}$, $Y = \{\alpha, \beta, \gamma\}$ και $Z = \{d, e\}$. Θέτουμε επίσης $f: X \rightarrow Y$ όπου $f(1) = \alpha$, $f(2) = \beta$ και $g: Y \rightarrow Z$ όπου $g(\alpha) = d$, $g(\beta) = g(\gamma) = e$. Τότε g δεν είναι 1-1, όμως $g \circ f$ είναι 1-1.

3.9 (i) $y \in f(A \cup B) \Leftrightarrow y = f(x)$ για κάποιο $x \in A \cup B \Leftrightarrow y = f(x)$ για κάποιο $x \in X$, όπου $(x \in A \text{ ή } x \in B) \Leftrightarrow y \in f(A) \text{ ή } y \in f(B) \Leftrightarrow y \in f(A) \cup f(B)$.

(ii) $y \in f(A \cap B) \Rightarrow y = f(x)$ για κάποιο $x \in A \cap B \Rightarrow y = f(x)$ για κάποιο $x \in X$, όπου $(x \in A \text{ και } x \in B) \Rightarrow y \in f(A) \text{ και } y \in f(B) \Rightarrow y \in f(A) \cap f(B)$.

Παρατήρηση. Θεωρούμε την συνάρτηση $f: \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\}: 1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 1, 4 \mapsto 2$. Θέτουμε $A = \{1, 2\}$ και $B = \{3, 4\}$. Τότε $f(A \cap B) = f(\emptyset) = \emptyset$ και $f(A) \cap f(B) = \{1, 2\}$.

(iii) $x \in f^{-1}(\Gamma \cup \Delta) \Leftrightarrow f(x) \in \Gamma \cup \Delta \Leftrightarrow f(x) \in \Gamma \text{ ή } f(x) \in \Delta \Leftrightarrow x \in f^{-1}(\Gamma) \text{ ή } x \in f^{-1}(\Delta) \Leftrightarrow x \in f^{-1}(\Gamma) \cup f^{-1}(\Delta)$.

(iv) $x \in f^{-1}(\Gamma \cap \Delta) \Leftrightarrow f(x) \in \Gamma \cap \Delta \Leftrightarrow f(x) \in \Gamma \text{ και } f(x) \in \Delta \Leftrightarrow x \in f^{-1}(\Gamma) \text{ και } x \in f^{-1}(\Delta) \Leftrightarrow x \in f^{-1}(\Gamma) \cap f^{-1}(\Delta)$.

(v) $x \in f^{-1}(Y - \Gamma) \Leftrightarrow f(x) \in Y - \Gamma \Leftrightarrow f(x) \notin \Gamma \Leftrightarrow x \notin f^{-1}(\Gamma) \Leftrightarrow x \in X - f^{-1}(\Gamma)$.

(vi) $y \in f(f^{-1}(\Gamma)) \Rightarrow y = f(x)$ για κάποιο $x \in f^{-1}(\Gamma) \Rightarrow y = f(x)$ όπου $f(x) \in \Gamma \Rightarrow y \in \Gamma$.

(vii) $x \in A \Rightarrow f(x) \in f(A) \Rightarrow x \in f^{-1}(f(A))$.

(viii) Υποθέτουμε ότι f είναι 1-1 και ότι $y \in f(A) \cap f(B)$. Τότε $y = f(x_1)$ για κάποιο $x_1 \in A$ (αφού $y \in f(A)$) και $y = f(x_2)$ για κάποιο $x_2 \in B$ (αφού $y \in f(B)$). Από $f(x_1) = y = f(x_2)$, όπου $x_1, x_2 \in X$, παίρνουμε ότι $x_1 = x_2$ από την υπόθεση ότι f είναι 1-1. Συνάγουμε ότι $x_1 \in A \cap B$ και επομένως $y = f(x_1) \in f(A \cap B)$. Έχουμε δείξει ότι $f(A) \cap f(B) \subseteq f(A \cap B)$ οπότεδήποτε f είναι 1-1. Συγκρίνετε τέλος με την Άσκηση 3.9(ii).

3.10 Θέτουμε $X = \{x_1, x_2\}$ και $Y = \{y_1, y_2, y_3\}$. Θέτουμε επίσης $f: X \rightarrow Y$ όπου $f(x_1) = y_1, f(x_2) = y_2$ και $g: Y \rightarrow X$ όπου $g(y_1) = x_1, g(y_2) = x_2$ και $g(y_3) = x_2$.

4.1 Θα χρησιμοποιήσουμε **μόνο** ότι η πρόσθεση και πολλαπλασιασμός στο $\mathbb{Z}$ ικανοποιούν την προσεταιριστική και αντιμεταθετική ιδιότητα και ότι ισχύει επίσης η επιμεριστική ιδιότητα ως προς τις δύο αυτές διμελείς πράξεις.

Λήμμα 1. Έστω $x, y, z, w \in \mathbb{Z}$. Τότε $(x + y) + (z + w) = (x + z) + (y + w)$.

Απόδειξη. Χρησιμοποιώντας εδώ ότι η συνηθισμένη πρόσθεση στο $\mathbb{Z}$ είναι αντιμεταθετική και προσεταιριστική, παίρνουμε $(x + y) + (z + w) = x + (y + (z + w)) = x + ((y + z) + w) = x + ((z + y) + w) = x + (z + (y + w)) = (x + z) + (y + w)$. $\square$

Παρατηρούμε ότι: $(a \circ b) \circ c = ((a + b) + ab) \circ c = (((a + b) + ab) + c) + ((a + b) + ab)c = (((a + b) + ab) + c) + ((a + b)c + (ab)c) = ((a + b) + (ab + c)) + ((ac + bc) + a(bc)) = ((a + b) + (c + ab)) + ((bc + ac) + a(bc)) = (((a + b) + c) + ab) + (bc + (ac + a(bc))) = ((a + (b + c)) + ab) + (bc + (ac + a(bc))),$

ενώ $a \circ (b \circ c) = a \circ ((b + c) + bc) = (a + ((b + c) + bc)) + a((b + c) + bc) = (a + ((b + c) + bc)) + (a(b + c) + a(bc)) = ((a + (b + c)) + bc) + ((ab + ac) + a(bc)) = ((a + (b + c)) + bc) + ((ab + (ac + a(bc)))$.

Θέτοντας $x = a + (b + c)$, $y = ab$, $z = bc$ και $w = ac + a(bc)$, το αποτέλεσμα είναι τώρα άμεση συνέπεια του Λήμματος 1.

4.2 (i) Έστω $A, B, C \subseteq X$. Τότε, $A \Delta B = (A \cup B) - (A \cap B) = (B \cup A) - (B \cap A) = B \Delta A$.

(ii) Ελέγξτε πρώτα ότι ισχύει το εξής αποτέλεσμα.

Λήμμα 2. Πάνω στο σύνολο $\{0, 1\}$ ορίζουμε την διμελή πράξη $\oplus$ ως εξής: $0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1$ και $1 \oplus 1 = 0$. Τότε η διμελής πράξη $\oplus$ είναι προσεταιριστική.

[Στην πραγματικότητα, στο Λήμμα 2 έχουμε ορίσει πρόσθεση modulo 2. Στο Κεφάλαιο 10 θα δούμε πως η έννοια αυτή γενικεύεται.]

Ορισμός. Αν S είναι υποσύνολο του καθολικού συνόλου X , ορίζουμε την *χαρακτηριστική του συνάρτηση* $\chi_S: X \rightarrow \{0, 1\}$, με $\chi_S(t) = \begin{cases} 1, & \text{αν } t \in S, \\ 0, & \text{αν } t \in X - S. \end{cases}$

Έχουμε τότε, για οποιαδήποτε υποσύνολα U, V του X , ότι $U = V$ αν-ν $\chi_U = \chi_V$ (αν-ν $\chi_U(t) = \chi_V(t)$ για όλα τα $t \in X$). Επιπλέον, $\chi_{U \Delta V}(t) = \chi_U(t) \oplus \chi_V(t)$ για όλα τα $t \in X$. [Εξετάζουμε τις περιπτώσεις: (i) $t \in U$ και $t \in V$, (ii) $t \in U$ και $t \notin V$, (iii) $t \notin U$ και $t \in V$, (iv) $t \notin U$ και $t \notin V$.]

Έστω τώρα $A, B, C \subseteq X$. Από τα πιο πάνω, για κάθε $t \in X$, έχουμε $\chi_{(A \Delta B) \Delta C}(t) = \chi_{(A \Delta B)}(t) \oplus \chi_C(t) = (\chi_A(t) \oplus \chi_B(t)) \oplus \chi_C(t) = \chi_A(t) \oplus (\chi_B(t) \oplus \chi_C(t)) = \chi_A(t) \oplus \chi_{B \Delta C}(t) = \chi_{A \Delta (B \Delta C)}(t)$. Συνάγουμε ότι $\chi_{(A \Delta B) \Delta C}(t) = \chi_{A \Delta (B \Delta C)}(t)$ για όλα τα $t \in X$, και επομένως $(A \Delta B) \Delta C = A \Delta (B \Delta C)$.

[Σημείωση. Χρησιμοποιώντας τις ιδιότητες της ένωσης και τομής υποσυνόλων στην Πρόταση 2.5, μπορούμε να δώσουμε μια διαφορετική απόδειξη για την προσεταιριστική ιδιότητα.]

Τελευταίο μέρος: Το κενό σύνολο είναι ουδέτερο στοιχείο ως προς την πράξη αυτή.

4.3 Θέτουμε $S = \mathbb{N} \cup \{0\}$ και ορίζουμε $a * b = |a - b|$ για $a, b \in S$.

4.4 (i) Αν $x, y \in \mathbb{Z}$ με $x > 0$ και $y > 0$, τότε $x + y \in \mathbb{Z}$ με $x + y > 0$. Δεν υπάρχει ουδέτερο στοιχείο στο S ως προς την πράξη αυτή.

(ii) (a) Ναι, αφού το άθροισμα δύο μη-αρνητικών ακεραίων είναι ένας μη-αρνητικός ακέραιος.

(b) Όχι, αφού $-1 \in \{x \in \mathbb{Z} : x \geq -1\}$, όμως $-1 + -1 = -2 \notin \{x \in \mathbb{Z} : x \geq -1\}$.

4.5 $\pi_1 = (1 \ 2 \ 3)$, $\pi_2 = (3 \ 4 \ 5)$, $\pi_1^{-1} = (3 \ 2 \ 1)$, $\pi_2^{-1} = (5 \ 4 \ 3)$, $\pi_1 \circ \pi_2 = (1 \ 2 \ 3 \ 4 \ 5)$, $\pi_2 \circ \pi_1 = (1 \ 2 \ 4 \ 5 \ 3)$, $\pi_1^{-1} \circ \pi_2^{-1} = (\pi_2 \pi_1)^{-1} = (3 \ 5 \ 4 \ 2 \ 1)$, $\pi_2^{-1} \circ \pi_1^{-1} = (\pi_1 \pi_2)^{-1} = (5 \ 4 \ 3 \ 2 \ 1)$, $\pi_1 \circ (1 \ 2 \ 4) = (1 \ 2 \ 3)(1 \ 2 \ 4) = (1 \ 3)(2 \ 4)$.

5.1 Ο συλλογισμός καταρρέει ήδη από την περίπτωση $k = 2$: Η ευθεία l (αντίστοιχα, l') διέρχεται από τα σημεία M_1, M_2 (αντίστοιχα, M_2, M_3). Το M_2 είναι πράγματι κοινό σημείο για τις l και l' , όμως οι ευθείες αυτές μπορεί να μην έχουν άλλα κοινά σημεία ($M_2 = M_k$, αφού $k = 2$). Έχουμε δηλαδή ότι δεν ισχύει: $p(2)$ αληθής $\Rightarrow p(3)$ αληθής.

5.2 (i) Θέτουμε $p(n) : 1 + 3 + 5 + \dots + (2n - 1) = n^2$. Προφανώς $p(1)$ είναι αληθής. Υποθέτουμε ότι $p(k)$ είναι αληθής, όπου $k \in \mathbb{N}$. Έχουμε τότε, $1 + 3 + \dots + (2k - 1) + (2k + 1) = k^2 + (2k + 1) = (k + 1)^2$. Συνάγουμε ότι $p(k + 1)$ είναι αληθής, και επομένως $p(n)$ είναι αληθής για όλα τα $n \in \mathbb{N}$ από την **(PI)**.

(ii) Θέτουμε $p(n) : 1^2 + 2^2 + \dots + n^2 = \frac{1}{6}n(n + 1)(2n + 1)$. Παρατηρούμε πρώτα ότι $p(1)$ είναι αληθής. Υποθέτουμε ότι $p(k)$ είναι αληθής για κάποιο $k \in \mathbb{N}$. Τότε $1^2 + 2^2 + \dots + k^2 + (k + 1)^2 = \frac{1}{6}k(k + 1)(2k + 1) + (k + 1)^2 = (k + 1)(\frac{1}{6}k(2k + 1) + (k + 1)) = \frac{1}{6}(k + 1)(2k^2 + 7k + 6) = \frac{1}{6}(k + 1)(k + 2)(2k + 3) = \frac{1}{6}(k + 1)(k + 2)(2(k + 1) + 1)$. Το αποτέλεσμα είναι άμεση συνέπεια της **(PI)**.

(iii) Θέτουμε $p(n) : 1 \cdot 2 + 2 \cdot 3 + \dots + n(n + 1) = \frac{1}{3}n(n + 1)(n + 2)$. Τότε $p(1)$ είναι αληθής. Επιπλέον, αν $p(k)$ είναι αληθής, όπου $k \in \mathbb{N}$, έχουμε $1 \cdot 2 + 2 \cdot 3 + \dots + k(k + 1) + (k + 1)(k + 2) = \frac{1}{3}k(k + 1)(k + 2) + (k + 1)(k + 2) = \frac{1}{3}(k + 1)(k + 2)(k + 3)$. Έχουμε, δηλαδή, ότι $p(k + 1)$ είναι αληθής. Χρησιμοποιούμε, τέλος, την **(PI)**.

(iv) Θέτουμε $p(n) : \frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \dots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$. Παρατηρούμε πρώτα ότι $p(1)$ είναι αληθής. Αν τώρα $p(k)$ είναι αληθής για κάποιο $k \in \mathbb{N}$ έχουμε, $\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \dots + \frac{1}{(2k-1)(2k+1)} + \frac{1}{(2k+1)(2k+3)} = \frac{k}{2k+1} + \frac{1}{(2k+1)(2k+3)} = \frac{2k^2 + 3k + 1}{(2k+1)(2k+3)} = \frac{(2k+1)(k+1)}{(2k+1)(2k+3)} = \frac{k+1}{2k+3}$, άρα $p(k + 1)$ είναι αληθής. Χρησιμοποιούμε και πάλι την **(PI)**.

5.3 Έστω, για κάθε $n \in \mathbb{N}$, η πρόταση $p(n) : \text{Για τον ακέραιο } n, \text{ υπάρχει } a_n \in \mathbb{Z} \text{ με } 10^n = 9a_n + 1$. Έχουμε, $10^1 = 9(1) + 1$, συνεπώς $p(1)$ είναι αληθής (θέτουμε $a_1 = 1$). Υποθέτουμε τώρα ότι $p(k)$ είναι αληθής για κάποιο $k \in \mathbb{N}$. (Έχουμε υποθέσει δηλαδή ότι, για το συγκεκριμένο k , υπάρχει ακέραιος a_k με $10^k = 9a_k + 1$.) Έπεται ότι $10^{k+1} = 10(10^k) = 10(9a_k + 1) = 9 \cdot 10 \cdot a_k + 9 + 1 = 9(10a_k + 1) + 1$. Θέτουμε $a_{k+1} = 10a_k + 1$. Τότε $a_{k+1} \in \mathbb{Z}$ αφού $a_k \in \mathbb{Z}$ και, επιπλέον, $10^{k+1} = 9a_{k+1} + 1$. Συνοψίζοντας, έχουμε δείξει ότι για κάθε $k \in \mathbb{N}$ ισχύει: $p(k + 1)$ είναι αληθής οποτεδήποτε $p(k)$ είναι αληθής. Η **(PI)** μας εξασφαλίζει ότι $p(n)$ είναι αληθής για όλα τα $n \in \mathbb{N}$ (και επομένως για όλα τα $n \in \mathbb{Z}$ με $n > 0$).

5.4 Έστω, για κάθε $n \in \mathbb{N}$, η πρόταση $p(n) : 2^n > n^3$. Παρατηρούμε πρώτα ότι $2^{10} = 1024 > 1000 = 10^3$, άρα $p(10)$ είναι αληθής. Υποθέτουμε τώρα ότι $p(k)$ είναι αληθής για κάποιο $k \in \mathbb{N}$ με $k \geq 10$. Έχουμε τότε, $2^{k+1} (= 2(2^k)) > 2k^3 = (k + 1)^3 + k^3 - 3k^2 - 3k - 1 > (k + 1)^3 + k^3 - 3k^2 - 3k - 4 = (k + 1)^3 + (k - 4)(k^2 + k + 1) > (k + 1)^3$, αφού $k \geq 10$. Έχουμε δείξει ότι για όλα τα $k \in \mathbb{N}$ με $k \geq 10$ ισχύει: $p(k)$ αληθής $\Rightarrow p(k + 1)$ αληθής. Χρησιμοποιούμε, τέλος, την κατάλληλη γενίκευση της **(PI)**.

5.5 (i) **(I₁) $\Rightarrow$ (W)**. Υποθέτουμε ότι ισχύει το **(I₁)**. Έστω τώρα ότι T είναι ένα μη-κενό υποσύνολο του $\mathbb{N}$. Θέλουμε να δείξουμε ότι το T έχει ελάχιστο στοιχείο. Προχωρούμε με απαγωγή σε άτοπο και υποθέτουμε

ότι T δεν έχει ελάχιστο στοιχείο. Έπεται ότι $1 \notin T$ (διαφορετικά το 1 θα ήταν το ελάχιστο στοιχείο του T). Θέτουμε $S = \{a \in \mathbb{N} : a < t \text{ για όλα τα } t \in T\}$. Έχουμε δει ότι $1 \in S$. Έστω τώρα $a \in \mathbb{N}$ τέτοιο ώστε $x \in S$ για όλους τους φυσικούς x με $1 \leq x \leq a$. Έπεται ότι $a+1 \notin T$ (αν $a+1$ ήταν στοιχείο του T , τότε $a+1$ θα ήταν το ελάχιστο στοιχείο του T). Αυτός ο συλλογισμός δείχνει ότι $a+1 \in S$ αν για τον φυσικό a ισχύει ότι $x \in S$ για όλους τους ακέραιους x με $1 \leq x \leq a$. Υπενθυμίζουμε επίσης ότι $1 \in S$. Το αξίωμα (I_1) μας εξασφαλίζει τώρα ότι $S = \mathbb{N}$. Άρα $T = \emptyset$ (άτοπο).

(ii) $(W) \Rightarrow (I_1)$. Υποθέτουμε ότι ισχύει η (W) . Έστω τώρα V ένα υποσύνολο του $\mathbb{N}$ με τις ιδιότητες (I) $1 \in V$ και (II) (για όλα τα $a \in \mathbb{N}$), αν $x \in V$ για κάθε φυσικό x με $1 \leq x \leq a$, τότε $a+1 \in V$. Ο σκοπός μας είναι να δείξουμε ότι $V = \mathbb{N}$, και για να το πετύχουμε αυτό προχωρούμε με απαγωγή σε άτοπο. Θέτουμε $T = \mathbb{N} - V$ και υποθέτουμε ότι $T \neq \emptyset$. Η αρχή της καλής διάταξης μας εξασφαλίζει ότι T έχει ελάχιστο στοιχείο, έστω το b ($b \in T \subseteq \mathbb{N}$). Όμως $b \neq 1$ (άρα $b > 1$) αφού έχουμε υποθέσει ότι $1 \in V$. Έπεται ότι $b-1 \in \mathbb{N}$ και $b-1 \notin T$. Συνεπώς $b-1 \in V$. Στην πραγματικότητα αυτός ο συλλογισμός δείχνει ότι $x \in V$ για όλους τους φυσικούς x με $1 \leq x \leq b-1$ (έχουμε δείξει ότι $b-1 \geq 1$). Από την ιδιότητα (II) του συνόλου V συμπεραίνουμε ότι $b \in V$ (άτοπο, αφού $b \in T = \mathbb{N} - V$). Συνάγουμε ότι $T = \emptyset$ και επομένως $V = \mathbb{N}$.

5.6 Υποθέτουμε ότι $a, r \in \mathbb{R}$ με $r \neq 1$. Έστω, για κάθε $n \in \mathbb{N}$, η πρόταση $p(n) : \sum_{j=0}^n ar^j = \frac{a(1-r^{n+1})}{(1-r)}$. Τότε $p(1)$ είναι αληθής αφού $a + ar = a(1+r) = \frac{a(1-r^2)}{1-r}$. [Έχουμε ότι $1-r^2 = (1+r)(1-r)$.] Υποθέτουμε τώρα ότι $k \in \mathbb{N}$ και ότι $p(k)$ είναι αληθής. [Υποθέτουμε δηλαδή ότι $\sum_{j=0}^k ar^j = \frac{a(1-r^{k+1})}{(1-r)}$.] Τότε $\sum_{j=0}^{k+1} ar^j = (\sum_{j=0}^k ar^j) + ar^{k+1} = \frac{a(1-r^{k+1})}{(1-r)} + \frac{a(1-r)r^{k+1}}{(1-r)} = \frac{a - ar^{k+1} + ar^{k+1} - ar^{k+2}}{(1-r)} = \frac{a(1-r^{k+2})}{(1-r)}$. Έχουμε δείξει ότι $p(k+1)$ είναι αληθής οποτεδήποτε $p(k)$ είναι αληθής. Η (PI) μας εξασφαλίζει ότι $p(n)$ είναι αληθής για όλα τα $n \in \mathbb{N}$.

5.7 (i) Θεωρούμε, για κάθε $n \in \mathbb{N}$, την πρόταση $p(n) : 5^n - 3^n + 2n = 4r$ για κάποιο $r \in \mathbb{Z}$ (το οποίο εξαρτάται από το n). Τότε $p(1)$ είναι αληθής αφού $5 - 3 + 2 = 4$. Υποθέτουμε τώρα ότι $p(k)$ είναι αληθής για κάποιο $k \in \mathbb{N}$. Όμως τότε, $5^{k+1} - 3^{k+1} + 2(k+1) - (5^k - 3^k + 2k) = 4 \cdot 5^k - 2(3^k - 1)$, που είναι πολλαπλάσιο του 4, αφού $3^k - 1$ είναι άρτιος. Έπεται ότι $p(k+1)$ είναι αληθής. Χρησιμοποιούμε τέλος την (PI) .

(ii) Για κάθε $n \in \mathbb{N}$, έστω $p(n)$ η πρόταση στην Άσκηση 5.7(ii). Προφανώς $p(1)$ είναι αληθής. Έστω τώρα $k \in \mathbb{N}$. Υποθέτουμε ότι $p(k)$ είναι αληθής. Στο σχήμα μας με τις k ευθείες, επισυνάπτουμε την $(k+1)$ -οστή ευθεία, σύμφωνα με τους περιορισμούς που έχουμε, και παρατηρούμε ότι τα σημεία τομής έχουν αυξηθεί ακριβώς κατά k . Συνεπώς έχουμε τώρα ακριβώς $\frac{1}{2}k(k-1) + k = \frac{1}{2}k(k+1)$ σημεία τομής. Έπεται ότι $p(k+1)$ είναι αληθής. Χρησιμοποιούμε και πάλι την (PI) .

5.8 Παρατηρούμε πρώτα ότι $14 = 8 \cdot 1 + 3 \cdot 2$, άρα $p(14)$ είναι αληθής. Έστω τώρα $m \in \mathbb{N}$ με $m \geq 14$. Υποθέτουμε ότι $p(m)$ είναι αληθής, δηλαδή ότι $m = 8k + 3l$ για κάποια $k, l \in \mathbb{N} \cup \{0\}$.

Ισχυρισμός: Έχουμε ότι είτε $k \geq 1$ ή $l \geq 5$.

Απόδειξη ισχυρισμού: Αν $k < 1$ και $l < 5$, τότε $8k + 3l \leq 12$.

Χρησιμοποιώντας τις σχέσεις, $8k + 3l + 1 = 8(k-1) + 3(l+3)$ σε περίπτωση που $k \geq 1$, και $8k + 3l + 1 = 8(k+2) + 3(l-5)$ σε περίπτωση που $l \geq 5$, συνάγουμε ότι $p(m+1)$ είναι αληθής. Χρησιμοποιούμε τέλος την κατάλληλη γενίκευση της (PI) .

6.1 R_1 δεν είναι σχέση ισοδυναμίας, αφού $(1, 3) \in R_1$ όμως $(3, 1) \notin R_1$.

R_2 είναι μια σχέση ισοδυναμίας.

6.2 (i) Όχι [Έχουμε ότι $(2, 0), (0, -2) \in R_1$, όμως $(2, -2) \notin R_1$.]

(ii) Όχι [Έχουμε ότι $0 \in \mathbb{Z}$ και $(0, 0) \notin R_2$.]

(iii) Ναι [(a) Έχουμε ότι $(a, a) \in R_3$ για όλα τα $a \in \mathbb{Z}$ αφού $2|(a - a)$ και $3|(a - a)$.

(b) Αν $(a, b) \in R_3$, τότε $2|(a - b)$ και $3|(a - b)$. Άρα $2|(b - a)$ και $3|(b - a)$, και επομένως $(b, a) \in R_3$.

(c) Αν (a, b) και $(b, c) \in R_3$, τότε $2|((a - b) + (b - c))$ και $3|((a - b) + (b - c))$. Άρα $2|(a - c)$ και $3|(a - c)$, και επομένως $(a, c) \in R_3$.]

Για $c \in \mathbb{Z}$, παρατηρούμε ότι $(2|c$ και $3|c)$ αν-ν $6|c$. Συνεπώς $\bar{c} = \{6k + c : k \in \mathbb{Z}\}$. Παρατηρούμε επίσης ότι η συλλογή $\Delta = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ αποτελεί διαμέριση του $\mathbb{Z}$.

(iv) Όχι [Έχουμε ότι $(2, 3) \in R_4$, όμως $(3, 2) \notin R_4$.]

(v) Όχι [Έχουμε ότι $0 \in \mathbb{Z}$ όμως $(0, 0) \notin R_5$.]

(vi) Όχι [Έχουμε ότι $(4, 6), (6, 9) \in R_6$, όμως $(4, 9) \notin R_6$.]

6.3 Όχι [Παρατηρούμε ότι $\emptyset, A \in \mathcal{P}(A)$ και $\emptyset \neq A$, αφού A είναι μη-κενό. Προφανώς $(\emptyset, A) \in R$, όμως $(A, \emptyset) \notin R$.]

6.4 (i) Έστω $(r, s) \in S$. Έχουμε ότι $rs = sr$, άρα $(r, s) \sim (r, s)$.

(ii) Έστω ότι $(r, s) \sim (t, u)$, όπου $(r, s), (t, u) \in S$. Τότε $ru = st$ και επομένως $ts = ur$. Έπεται ότι $(t, u) \sim (r, s)$.

(iii) Έστω ότι $(r, s) \sim (t, u)$ και $(t, u) \sim (v, w)$, όπου $(r, s), (t, u), (v, w) \in S$. Τότε $ru = st$ και $tw = uv$. Έπεται ότι $ruw (= stw) = suv$, άρα $(rw - sv)u = 0$, όπου $u \neq 0$. Συμπεραίνουμε ότι $rw = sv$ και επομένως $(r, s) \sim (v, w)$.

6.5 (i) Έστω $(a, b) \in \mathbb{R}^2 - \{(0, 0)\}$. Θέτοντας $\lambda = 1 (> 0)$, βλέπουμε ότι $(a, b) \sim (a, b)$.

(ii) Έστω $(a, b), (c, d) \in \mathbb{R}^2 - \{(0, 0)\}$ με $(a, b) \sim (c, d)$. Τότε $a = \lambda c$ και $b = \lambda d$ για κάποιο $\lambda \in \mathbb{R}$ με $\lambda > 0$. Όμως $1/\lambda \in \mathbb{R}$ με $1/\lambda > 0$ και, επιπλέον, $c = (1/\lambda)a$ και $d = (1/\lambda)b$. Έπεται ότι $(c, d) \sim (a, b)$.

(iii) Έστω $(a, b), (c, d), (e, f) \in \mathbb{R}^2 - \{(0, 0)\}$ με $(a, b) \sim (c, d)$ και $(c, d) \sim (e, f)$. Υπάρχουν $\lambda, \mu \in \mathbb{R}$ με $\lambda > 0, \mu > 0$ τέτοια ώστε $a = \lambda c, b = \lambda d, c = \mu e, d = \mu f$. Όμως $\lambda\mu \in \mathbb{R}$ με $\lambda\mu > 0$ και, επιπλέον, ισχύουν $a = (\lambda\mu)e$ και $b = (\lambda\mu)f$.

Ο μοναδιαίος κύκλος είναι ένα παράδειγμα γεωμετρικού τόπου στο xy -επίπεδο το οποίο ικανοποιεί τις προϋποθέσεις.

6.6 (i) Αν $a \in \mathbb{R}$, τότε $a - a = 0 \in \mathbb{Q}$ και επομένως $a \sim a$.

(ii) Αν $a, b \in \mathbb{R}$ με $a \sim b$ τότε $b - a \in \mathbb{Q}$. Έπεται ότι $(a - b) = -(b - a) \in \mathbb{Q}$ και επομένως $b \sim a$.

(iii) Έστω $a, b, c \in \mathbb{R}$ με $a \sim b$ και $b \sim c$. Τότε $b - a$ και $c - b \in \mathbb{Q}$, και επομένως $c - a = (c - b) + (b - a) \in \mathbb{Q}$. Έπεται ότι $a \sim c$.

Τελευταίο μέρος: Παρατηρούμε πρώτα ότι $\bar{a} \subseteq \mathbb{R} - \mathbb{Q}$ οποτεδήποτε $a \in \mathbb{R} - \mathbb{Q}$, και ότι $\bar{c} = \mathbb{Q}$ για όλα τα $c \in \mathbb{Q}$. Η συλλογή $\{\bar{a}\}_{a \in \mathbb{R} - \mathbb{Q}}$ αποτελεί μια διαμέριση του συνόλου $\mathbb{R} - \mathbb{Q}$. [Δύο σύνολα από την συλλογή αυτή είτε συμπίπτουν είτε είναι ξένα μεταξύ τους. Επιπλέον, η ένωση των συνόλων της συλλογής αυτής μας δίνει ολόκληρο το $\mathbb{R} - \mathbb{Q}$.]

6.7 Η σχέση R_1 είναι μια σχέση ισοδυναμίας. Οι αντίστοιχες κλάσεις ισοδυναμίας είναι: $\bar{1} = \{(1), (1 \ 2)\} = (1 \ 2), (\bar{1} \ 3) = \{(1 \ 3), (1 \ 2 \ 3)\} = (1 \ 2 \ 3)$ και $(\bar{2} \ 3) = \{(2 \ 3), (1 \ 3 \ 2)\} = (1 \ 3 \ 2)$.

Η σχέση R_2 δεν αποτελεί σχέση ισοδυναμίας: Για παράδειγμα $(\alpha, \alpha) \notin R_2$ οποτεδήποτε $\alpha \in S_3$ αφού $\alpha^{-1}\alpha = (1) \notin H_2$.

6.8 (i) Είναι μια σχέση ισοδυναμίας: Παρατηρούμε πρώτα ότι $R_1 \cap R_2 \subseteq S \times S$ αφού R_1, R_2 είναι διμελείς σχέσεις στο S . Μεταβατική ιδιότητα: Έστω $(a, b), (b, c) \in R_1 \cap R_2$. Τότε, για $i = 1, 2$, $(a, c) \in R_i$ αφού $(a, b), (b, c) \in R_i$, και R_i είναι σχέση ισοδυναμίας. Έπεται ότι $(a, c) \in R_1 \cap R_2$. Παρόμοιος συλλογισμός για τις άλλες δύο ιδιότητες.

(ii) Δεν είναι σχέση ισοδυναμίας: Θεωρούμε για παράδειγμα τις σχέσεις $R_1 = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : 2|(x - y)\}$ και $R_2 = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : 3|(x - y)\}$. Έχουμε τότε ότι $(1, 3)$ και $(3, 6)$ ανήκουν στο σύνολο $R_1 \cup R_2$ όμως $(1, 6) \notin R_1 \cup R_2$.

7.6 (i) (Απόδειξη προσεταιριστικής ιδιότητας του πολλαπλασιασμού μιγαδικών αριθμών.) Έστω $z_1, z_2, z_3 \in \mathbb{C}$ με $z_1 = x_1 + iy_1$, $z_2 = x_2 + iy_2$, $z_3 = x_3 + iy_3$, $(x_i, y_i \in \mathbb{R})$. Έχουμε τότε:

$$z_1(z_2 z_3) = (x_1 + iy_1)((x_2 + iy_2)(x_3 + iy_3)) = (x_1 + iy_1)((x_2 x_3 - y_2 y_3) + i(x_2 y_3 + y_2 x_3)) = (x_1(x_2 x_3 - y_2 y_3) - y_1(x_2 y_3 + y_2 x_3)) + i(x_1(x_2 y_3 + y_2 x_3) + y_1(x_2 x_3 - y_2 y_3)), \text{ και}$$

$$(z_1 z_2) z_3 = ((x_1 + iy_1)(x_2 + iy_2))(x_3 + iy_3) = ((x_1 x_2 - y_1 y_2) + i(x_1 y_2 + y_1 x_2))(x_3 + iy_3) = ((x_1 x_2 - y_1 y_2)x_3 - (x_1 y_2 + y_1 x_2)y_3) + i((x_1 x_2 - y_1 y_2)y_3 + (x_1 y_2 + y_1 x_2)x_3).$$

Χρησιμοποιώντας τις ιδιότητες της πρόσθεσης και του πολλαπλασιασμού πραγματικών αριθμών (όπως επιμεριστική ιδιότητα, $\cdot$ είναι αντιμεταθετικός, $+$ είναι προσεταιριστική), βλέπουμε ότι οι δύο εκφράσεις είναι ίσες.

(Παρόμοια μπορούμε να δείξουμε ότι η πρόσθεση στο $\mathbb{C}$ ικανοποιεί την προσεταιριστική ιδιότητα.)

(ii) (a) Έστω $z = x + iy \in \mathbb{C}$, (όπου $x, y \in \mathbb{R}$). Θέτουμε $z' = -x + i(-y) \in \mathbb{C}$. Τότε $z + z' = 0$, από τον ορισμό της πρόσθεσης στο $\mathbb{C}$. Αν τώρα $z + z_1 = 0$ για κάποιο $z_1 \in \mathbb{C}$, έχουμε ότι $z' + (z + z_1) = z' + 0 = z'$ και επομένως $(z' + z) + z_1 = z'$. Όμως $z' + z = 0$, άρα $z_1 = z'$.

(b) Θέτουμε $e = 1 + i0 \in \mathbb{C}$. Τότε $ze = z$ για όλα τα $z \in \mathbb{C}$, από τον ορισμό του πολλαπλασιασμού στο $\mathbb{C}$ (θέτουμε, για παράδειγμα, $z = x + iy$). Υποθέτουμε τώρα ότι $ze' = z$ για όλα τα $z \in \mathbb{C}$. Όμως τότε $ee' = e$ όπου $ee' = e'e = e'$.

(c) Έστω $z = x + iy \in \mathbb{C}$ με $(x, y) \neq (0, 0)$. Θέτοντας $w = (\frac{x}{x^2+y^2}) + i(\frac{-y}{x^2+y^2})$ παρατηρούμε ότι $zw = 1 (= wz)$. Έστω τώρα $w' \in \mathbb{C}$ με $zw' = 1$. Τότε $w(zw') = w(1) = w$. Όμως $w(zw') = (wz)w' = 1w' = w'$.

7.7 (i) Έστω $z_1, z_2, z_3 \in \mathbb{C}$.

Αυτοπαθής: $z_1 - z_1 = 0 \in \mathbb{R}$.

Συμμετρική: Αν $(z_1, z_2) \in R_1$, τότε $z_1 - z_2 \in \mathbb{R}$, και επομένως $z_2 - z_1 (= -(z_1 - z_2)) \in \mathbb{R}$.

Μεταβατική: Έστω ότι $(z_1, z_2), (z_2, z_3) \in R_1$. Τότε $z_1 - z_2, z_2 - z_3 \in \mathbb{R}$ και επομένως $z_1 - z_3 = (z_1 - z_2) + (z_2 - z_3) \in \mathbb{R}$.

(ii) $\bar{a} = \mathbb{R}$, (iii) $\{i\beta : \beta \in \mathbb{R}\}$, (iv) Ευθείες στο xy -επίπεδο παράλληλες με τον x -άξονα.

8.1 Θέτουμε $f: A \rightarrow B : (r, \theta) \mapsto r \cos \theta + i r \sin \theta$, ($r \in \mathbb{R}$ με $r > 0$, και $0 \leq \theta < 2\pi$).

Η συνάρτηση f είναι αμφιμονοσήμαντη.

8.2 Προφανώς τα σύνολα $(\mathbb{N} \times \mathbb{N}) \times (\mathbb{Z} \times \mathbb{Q})$ και $\mathbb{N} \times \mathbb{N} \times \mathbb{Z} \times \mathbb{Q}$ είναι όμοια. Τα σύνολα $\mathbb{N}$, $\mathbb{Z}$ και $\mathbb{Q}$ είναι αριθμήσιμα (κοιτάξτε το Παράδειγμα 8.9 και το Πόρισμα 8.13). Παρεμβάλλοντας το Πόρισμα 8.12 βλέπουμε πρώτα ότι τα σύνολα $\mathbb{N} \times \mathbb{N}$ και $\mathbb{Z} \times \mathbb{Q}$ είναι και τα δύο αριθμήσιμα, και επομένως και το σύνολο $(\mathbb{N} \times \mathbb{N}) \times (\mathbb{Z} \times \mathbb{Q})$ είναι επίσης αριθμήσιμο.

8.3 Θέτουμε $C = B - A$. Τότε $A \cup B = A \cup C$, όπου τα σύνολα A και C είναι ξένα μεταξύ τους. Υποθέτουμε ότι $A \sim \mathbb{N}$ και ότι $f: A \rightarrow \mathbb{N}$ είναι μια αμφιμονοσήμαντη συνάρτηση. Αν $C = \emptyset$, τότε $A \cup B = A$ και η

συνάρτηση f είναι μια αμφιμονοσήμαντη συνάρτηση από το $A \cup B$ στο $\mathbb{N}$. Υποθέτουμε επομένως για το υπόλοιπο της λύσης ότι $C \neq \emptyset$.

(i) Αν B είναι πεπερασμένο, τότε C είναι επίσης πεπερασμένο και αφού, από την υπόθεση μας $C \neq \emptyset$, έχουμε ότι $C = \{c_1, \dots, c_m\}$ για κάποιο $m \in \mathbb{N}$. Παρατηρούμε τότε ότι η συνάρτηση $h: A \cup B \rightarrow \mathbb{N}$:

$$h(x) = \begin{cases} i, & \text{αν } x = c_i \in C, (1 \leq i \leq m), \\ m + f(x), & \text{αν } x \in A, \end{cases} \quad \text{είναι αμφιμονοσήμαντη.}$$

(ii) Έχουμε ήδη καλύψει την περίπτωση που C είναι πεπερασμένο στο τμήμα (i), επομένως μπορούμε να υποθέσουμε ότι C είναι άπειρο. Έχουμε τότε ότι $C \sim \mathbb{N}$. [Εξήγηση: Το σύνολο C είναι προφανώς αριθμήσιμο αφού οποιαδήποτε ένριψη από το B στο $\mathbb{N}$ όταν περιοριστεί στο C εξακολουθεί να είναι μια ένριψη (κοιτάζτε το Θεώρημα 8.4). Τώρα C δεν είναι πεπερασμένο και επομένως είναι αριθμήσιμα άπειρο.] Έστω

$g: C \rightarrow \mathbb{N}$ μια αμφιμονοσήμαντη συνάρτηση. Ορίζουμε $h: A \cup B \rightarrow \mathbb{N}$ με $h(x) = \begin{cases} 2f(x) - 1, & \text{αν } x \in A, \\ 2g(x), & \text{αν } x \in C. \end{cases}$

Η συνάρτηση h είναι αμφιμονοσήμαντη.

8.4 8.1(i): Η ταυτοτική συνάρτηση i_A είναι αμφιμονοσήμαντη.

8.1(ii): Αν $f: A \rightarrow B$ είναι αμφιμονοσήμαντη τότε f είναι αντιστρέψιμη και $f^{-1}: B \rightarrow A$ είναι αμφιμονοσήμαντη.

8.1(iii): Αν $f: A \rightarrow B$ και $g: B \rightarrow C$ είναι αμφιμονοσήμαντες, τότε και $g \circ f: A \rightarrow C$ είναι αμφιμονοσήμαντη.

8.10: Σημείωση: Αν $\{B_1, \dots, B_m\}$, όπου $m \in \mathbb{N}$ με $m > 1$, είναι μια πεπερασμένη συλλογή υποσυνόλων ενός καθολικού συνόλου τότε, σύμφωνα με τους ορισμούς που έχουμε δώσει, τα σύνολα $\bigcup_{i=1}^m B_i$ και $(\bigcup_{i=1}^{m-1} B_i) \cup B_m$ είναι ίσα.

Έστω τώρα $n \in \mathbb{N}$, και έστω $(A_i)_{i=1}^n$ μια (πεπερασμένη) συλλογή αριθμήσιμων συνόλων. Για κάθε $k \in \mathbb{N}$ με $1 \leq k \leq n$, θεωρούμε την πρόταση $p(k)$: “η ένωση $\bigcup_{i=1}^k A_i$ είναι ένα αριθμήσιμο σύνολο”. Προφανώς $p(1)$ είναι αληθής. Υποθέτουμε τώρα ότι $p(k)$ είναι αληθής για κάποιο $k \in \mathbb{N}$ με $1 \leq k < n$. Με άλλα λόγια έχουμε υποθέσει ότι $\bigcup_{i=1}^k A_i$ είναι ένα αριθμήσιμο σύνολο, όπου $1 \leq k < n$. Από την Πρόταση 8.8, η ένωση $(\bigcup_{i=1}^k A_i) \cup A_{k+1}$ είναι ένα αριθμήσιμο σύνολο. Όμως $\bigcup_{i=1}^{k+1} A_i = (\bigcup_{i=1}^k A_i) \cup A_{k+1}$. Έχουμε δείξει ότι αν $p(k)$ είναι αληθής, όπου $k \in \mathbb{N}$ με $1 \leq k < n$, τότε $p(k+1)$ είναι αληθής. Συνάγουμε ότι η πρόταση $p(n)$ είναι αληθής.

8.5 (i) Έστω $k \in \mathbb{Z}$. Θέτουμε $f(k) = \begin{cases} 2k, & \text{αν } k \leq 0, \\ 1 - 2k, & \text{αν } k > 0. \end{cases}$

(ii) Χρησιμοποιώντας την συνάρτηση f από το (i), ορίζουμε $g: \mathbb{R} \rightarrow \mathbb{R} - \mathbb{N}$ με $g(x) = \begin{cases} x, & \text{αν } x \in \mathbb{R} - \mathbb{Z}, \\ f(x), & \text{αν } x \in \mathbb{Z}. \end{cases}$

Τότε η συνάρτηση g είναι αμφιμονοσήμαντη: Προφανώς g είναι επιρριπτική αφού $\mathbb{R} - \mathbb{N} = (\mathbb{R} - \mathbb{Z}) \cup (\mathbb{Z} - \mathbb{N})$. Έστω τώρα ότι $g(x_1) = g(x_2)$ όπου $x_1, x_2 \in \mathbb{R}$. Αν $g(x_1) \in \mathbb{R} - \mathbb{Z}$, τότε $x_1, x_2 \in \mathbb{R} - \mathbb{Z}$ αφού $g(y) \in \mathbb{Z}$ για όλα τα $y \in \mathbb{Z}$. Έπεται ότι $x_1 = g(x_1) = g(x_2) = x_2$. Αν $g(x_1) \in \mathbb{Z}$, τότε $x_1, x_2 \in \mathbb{Z}$, αφού $g(y) \in \mathbb{R} - \mathbb{Z}$ οποτεδήποτε $y \in \mathbb{R} - \mathbb{Z}$. Έπεται ότι $f(x_1) = g(x_1) = g(x_2) = f(x_2)$ και επομένως $x_1 = x_2$, αφού f είναι ενριπτική.

8.6 Ορισμός. Αν $m \in \mathbb{N}$ και $(a_i)_{i=1}^m (= (a_i))$ μια (πεπερασμένη) ακολουθία ακεραίων, ορίζουμε $h((a_i)) = |a_1| + |a_2| + \dots + |a_m| + m \in \mathbb{N}$.

Έστω τώρα T το σύνολο όλων των πεπερασμένων ακολουθιών ακέραιων αριθμών. Προφανώς, για κάθε $n \in \mathbb{N}$, το υποσύνολο $T(n)$ του T που ορίζεται με $T(n) = \{(a_i) \in T : h((a_i)) = n\}$ είναι πεπερασμένο. Επιπλέον, έχουμε ότι $T = \bigcup_{n \in \mathbb{N}} T(n)$. Το αποτέλεσμα είναι τώρα άμεση συνέπεια της Πρότασης 8.14.

8.7 (i) Η συνάρτηση $g: \mathbb{N} \times \mathbb{N} \rightarrow S : (a, b) \mapsto \sqrt{2^a 3^b}$, ($a, b \in \mathbb{N}$) είναι επιρριπτική. Από το Θεώρημα 8.11 υπάρχει επίρριψη $f: \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$. Συνεπώς η συνάρτηση $g \circ f: \mathbb{N} \rightarrow S$ είναι επιρριπτική. Το αποτέλεσμα είναι τώρα άμεση συνέπεια του Θεωρήματος 8.4.

(ii) Παρατηρούμε ότι $T = T_1 \cup T_2$ όπου $T_1 = \{x \in \mathbb{R} : x = \sqrt{2^\alpha 3^\beta 5^\gamma} \text{ για κάποια } \alpha, \beta, \gamma \in \mathbb{N}\}$ και $T_2 = \{x \in \mathbb{R} : x = -\sqrt{2^\alpha 3^\beta 5^\gamma} \text{ για κάποια } \alpha, \beta, \gamma \in \mathbb{N}\}$. Τα σύνολα T_1, T_2 είναι αριθμήσιμα με παρόμοιο συλλογισμό όπως στο (i). Επομένως το σύνολο T είναι αριθμήσιμο (Πρόταση 8.8).

8.8 Έστω, για κάθε $n \in \mathbb{N}$, η πρόταση $p(n)$: “υπάρχουν μοναδικά ορισμένα στοιχεία $a_1, \dots, a_n \in A$ τέτοια ώστε $a_1 = x_A$ (όπου το x_A είναι το στοιχείο που έχει επιλεγεί από το ίδιο το σύνολο A), και για κάθε $k = 2, \dots, n$ το στοιχείο a_k είναι το στοιχείο που έχει επιλεγεί από το σύνολο $A - \{a_1, \dots, a_{k-1}\}$ ”. Προφανώς η πρόταση $p(1)$ είναι αληθής. Υποθέτουμε τώρα ότι η πρόταση $p(m)$ είναι αληθής για κάποιο $m \in \mathbb{N}$. Έστω a_{m+1} το στοιχείο που έχει επιλεγεί από το σύνολο $A - \{a_1, \dots, a_m\}$. [Προφανώς το σύνολο $A - \{a_1, \dots, a_m\}$ είναι μη-κενό αφού A είναι άπειρο.] Αφού τα $a_1, \dots, a_m$ έχουν προσδιοριστεί με μοναδικό τρόπο, το ίδιο συμβαίνει και με το στοιχείο a_{m+1} . Έχουμε δείξει ότι $p(m+1)$ είναι αληθής οπότεδήποτε $p(m)$ είναι αληθής. Έπεται ότι $p(n)$ είναι αληθής για όλα τα $n \in \mathbb{N}$. Πιο ειδικά, τα στοιχεία $a_1, \dots, a_n$ είναι διακεκριμένα για κάθε $n \in \mathbb{N}$ και, επιπλέον, το σύνολο $B = \{a_i : i \in \mathbb{N}\}$ είναι ένα αριθμήσιμο άπειρο υποσύνολο του A .

8.9 Έστω $f : A_1 \rightarrow A_2$ και $g : B_1 \rightarrow B_2$ αμφιμονοσήμαντες συναρτήσεις. Θέτουμε $h : A_1 \times B_1 \rightarrow A_2 \times B_2 : (x, y) \mapsto (f(x), g(y))$, ($x \in A_1, y \in B_1$). Η συνάρτηση h είναι αμφιμονοσήμαντη: Αν $h((x_1, y_1)) = h((x_2, y_2))$, όπου $x_1, x_2 \in A_1$ και $y_1, y_2 \in B_1$, τότε $((f(x_1), g(y_1)) = (f(x_2), g(y_2))$ και επομένως $f(x_1) = f(x_2)$ και $g(y_1) = g(y_2)$ από τον ορισμό του καρτεσιανού γινομένου. Έπεται ότι $x_1 = x_2$ και $y_1 = y_2$ (και επομένως $(x_1, y_1) = (x_2, y_2)$) αφού οι συναρτήσεις f και g είναι και οι δύο ενριπτικές. Αν τώρα $(z, w) \in A_2 \times B_2$, τότε $z \in A_2$ και $w \in B_2$ και επομένως $z = f(x)$ και $w = g(y)$ για κάποια $x \in A_1$ και $y \in B_1$ αφού οι συναρτήσεις f και g είναι και οι δύο επιρριπτικές. Έπεται ότι $(z, w) = h((x, y))$.

8.10 Παρατηρούμε πρώτα ότι L είναι ένα μη-κενό υποσύνολο του δυναμοσυνόλου $\mathcal{P}(S)$. Τα μεγιστικά στοιχεία του L είναι ακριβώς όλα τα υποσύνολα του S που είναι της μορφής $S - \{t\}$ για κάποιο $t \in S$.

9.1 (i) Αν $a|b$ και $b|c$, τότε υπάρχουν $k, l \in \mathbb{Z}$ με $c = kb$ και $b = la$. Συνεπώς, $c = k(la) = (kl)a$, όπου $kl \in \mathbb{Z}$.

(ii) Αν $d|a$ και $d|b$, τότε υπάρχουν $e, f \in \mathbb{Z}$ με $a = ed$ και $b = fd$. Έχουμε τότε ότι $sa + tb = s(ed) + t(fd) = (se)d + (tf)d = (se + tf)d$, όπου $se + tf \in \mathbb{Z}$.

9.2 Παρατηρούμε ότι $2|((n+1)! + 2), 3|((n+1)! + 3), \dots, (n+1)|((n+1)! + (n+1))$. Συνεπώς κανένας από αυτούς τους πιο πάνω ακέραιους είναι πρώτος.

9.3 Έστω $n \in \mathbb{N}$. Χρησιμοποιώντας αλγοριθμική διαίρεση λαμβάνουμε διαδοχικά: $6n + 8 = 1(4n + 5) + (2n + 3)$, $4n + 5 = 1(2n + 3) + (2n + 2)$ και $2n + 3 = 1(2n + 2) + 1$. Έπεται ότι $\mu\chi\delta(6n + 8, 4n + 5) = \mu\chi\delta(4n + 5, 2n + 3) = \mu\chi\delta(2n + 3, 2n + 2) = 1$.

9.4 Έστω $a, b, c \in \mathbb{Z}$ με $\mu\chi\delta(a, b) = 1$ και $a|bc$. Τότε υπάρχουν $s, t \in \mathbb{Z}$ με $sa + tb = 1$. Άρα $sac + tbc = c$ όπου $bc = ra$ για κάποιο $r \in \mathbb{Z}$. Έπεται ότι $(sc + tr)a = c$ όπου $sc + tr \in \mathbb{Z}$.

9.5 Έστω $m, n, a \in \mathbb{Z}$ με $\mu\chi\delta(m, n) = 1$, $m|a$ και $n|a$. Τότε $sm + tn = 1$ για κάποια $s, t \in \mathbb{Z}$. Επομένως $sma + tna = a$, όπου $a = qm = rn$ για κάποια $q, r \in \mathbb{Z}$. Συμπεραίνουμε ότι $(sr + tq)(mn) = a$, όπου $sr + tq \in \mathbb{Z}$.

9.6 (i) Προφανώς $c/e, d/e \in \mathbb{Z}$ αφού $e|c$ και $e|d$. Από το Θεώρημα 9.6 έχουμε ότι $e = wc + zd$ για κάποια $w, z \in \mathbb{Z}$. Συνεπώς, $1 = w(c/e) + z(d/e)$. Το Λήμμα 9.8 μας εξασφαλίζει τώρα ότι $\mu\chi\delta(c/e, d/e) = 1$.

(ii) Έστω $(c, d) \in S$ με $d > 0$. Θέτουμε $e = \mu\chi\delta(c, d)$. Τότε $c = c'e$ και $d = d'e$ για κάποια $c', d' \in \mathbb{Z}$. Από το (i) έχουμε ότι $\mu\chi\delta(c', d') = 1$. Επιπλέον ισχύει $(c, d) \sim (c', d')$, όπου $d' > 0$. Αν $d < 0$, παρατηρούμε ότι $(c, d) \sim (-c', -d')$, όπου $-d' > 0$ και $\mu\chi\delta(-c', -d') = \mu\chi\delta(c, d) = 1$. Υποθέτουμε τώρα ότι $(a, b) \sim (a', b')$ όπου $b > 0$, $b' > 0$ και $\mu\chi\delta(a, b) = 1 = \mu\chi\delta(a', b')$. Έχουμε τότε ότι $ab' = ba'$. Έπεται ότι $b|b'$ και $b'|b$ (Άσκηση 9.4). Έπεται ότι $b = b'$ (αφού $b > 0$ και $b' > 0$). Συνάγουμε ότι $0 = ab' - ba' = ab - ba' = b(a - a')$ και επομένως $a = a'$ επίσης.

9.7 Αφού $d|m$ και $d|n$, έχουμε ότι $m/d, n/d \in \mathbb{Z}$. Όμως $1 = (\frac{m}{d})x + (\frac{n}{d})y$. Χρησιμοποιούμε το Λήμμα 9.8.

9.8 Χρησιμοποιώντας το θεώρημα διαίρεσης λαμβάνουμε διαδοχικά : $64 = 2(24) + 16$, $24 = 1(16) + 8$, $16 = 2(8) + 0$. Έπεται ότι $\mu\chi\delta(64, 24) = \mu\chi\delta(24, 16) = \mu\chi\delta(16, 8) = 8$. Έχουμε επίσης ότι $8 = 24 - 16 = 24 - (64 - 2(24)) = -1(64) + 3(24)$.

9.9 Θέτουμε $e = \epsilon\kappa\pi(a, b)$. Τότε $e \in \mathbb{N}$, και $c = qe + r$ για κάποια $q, r \in \mathbb{Z}$ με $0 \leq r < e$. Όμως $a|c$ και $a|e$, άρα $a|r$. Παρόμοια $b|r$. Συνάγουμε ότι $r = 0$, αφού η περίπτωση $r > 0$ αποκλείεται από τον ορισμό του $\epsilon\kappa\pi$.

9.10 Θέτουμε $c = \mu\chi\delta(b, m)$. Αφού $a \equiv b \pmod{m}$, έχουμε ότι $m|(a - b)$ ή, ισοδύναμα, $a = b + qm$ για κάποιο $q \in \mathbb{Z}$. Από τα πιο πάνω έχουμε ότι $c > 0$ και, επιπλέον, $c|a$ και $c|b$. Έστω τώρα $x \in \mathbb{Z}$ με $x|a$ και $x|m$. Τότε $x|b$ επίσης, και επομένως $x|\mu\chi\delta(b, m)$. Συνάγουμε ότι $c = \mu\chi\delta(a, m)$.

9.11 Από την ισοτιμία $6 \equiv -1 \pmod{7}$ λαμβάνουμε $6^{184} \equiv (-1)^{184} \pmod{7}$, άρα $6^{184} \equiv 1 \pmod{7}$. Έπεται ότι $6^{184} = 7k + 1$ για κάποιο $k \in \mathbb{Z}$. Θέτουμε $r = 1$.

9.12 Έστω $a \in \mathbb{Z}$ και p πρώτος. Αν $p|a^2$, τότε $p|a$. [Εξήγηση: Υποθέτουμε ότι $p \nmid a$. Τότε $\mu\chi\delta(a, p) = 1$ και $1 = sa + tp$ για κάποια $s, t \in \mathbb{Z}$. Συνεπώς $a = sa^2 + tpa$ όπου $p|sa^2$ και $p|tpa$, που είναι άτοπο. Εναλλακτικά θα μπορούσαμε να παρατηρήσουμε ότι μια παραγοντοποίηση σε γινόμενο πρώτων για το a^2 προκύπτει εύκολα από την αντίστοιχη παραγοντοποίηση για το a , και να χρησιμοποιήσουμε την μοναδικότητα της παραγοντοποίησης αυτής.]

Υποθέτουμε πρώτα ότι $n = m^2$ για κάποιο $m \in \mathbb{Z}$. Τότε $\sqrt{n} = |m| \in \mathbb{Z} \subseteq \mathbb{Q}$. Έστω τώρα ότι $\sqrt{n} \in \mathbb{Q}$. Τότε υπάρχουν $r, s \in \mathbb{Z}$ με $s \geq 1$ και $\mu\chi\delta(r, s) = 1$ τέτοιοι ώστε $\sqrt{n} = r/s$ (χρησιμοποιούμε την Άσκηση 9.6(ii)). Συνάγουμε ότι $s = 1$ και $n = r^2$. [Εξήγηση: Αν $s > 1$, τότε $p|s$ για κάποιο πρώτο p και επομένως $p|r^2$, αφού $r^2 = ns^2$. Άρα $p|r$ επίσης, που είναι άτοπο.]

9.13 (i) Υποθέτουμε ότι $ab > 1$, αφού το αποτέλεσμα είναι προφανές για $a = 1 = b$. Έστω ότι $ab = c^2$ για κάποιο $c \in \mathbb{N}$. Έχουμε τότε ότι στην παραγοντοποίηση $ab = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_n^{\gamma_n}$, όπου p_i είναι πρώτοι και $\gamma_i \in \mathbb{N}$ (συγκρίνετε με την Παρατήρηση 9.14), όλοι οι φυσικοί γ_i είναι άρτιοι. Επιπλέον, στις αντίστοιχες παραγοντοποιήσεις για τα a και b δεν υπάρχουν κοινοί πρώτοι αφού $\mu\chi\delta(a, b) = 1$.

(ii) Παρόμοια με το τμήμα (i): Αν $ab = c^n$, τότε τα γ_i είναι πολλαπλάσια του n .

9.14 Προφανώς $10^0 = 1 \equiv 1 \pmod{3}$ και $10 \equiv 1 \pmod{3}$. Έπεται ότι $10^k \equiv 1 \pmod{3}$ για κάθε $k \in \mathbb{N} \cup \{0\}$. Έστω τώρα $x \in \mathbb{N}$. Τότε $x = a_0 10^0 + a_1 10^1 + a_2 10^2 + \dots + a_r 10^r$ για κάποια $r, a_0, \dots, a_r \in \mathbb{N} \cup \{0\}$, με $0 \leq a_i \leq 9$ για $1 \leq i \leq r$, και $a_r \neq 0$. [Έχουμε δηλαδή $x = a_r a_{r-1} \dots a_0$.] Όμως $a_i 10^i \equiv a_i \pmod{3}$ για $i = 0, 1, \dots, r$. Συνάγουμε ότι $x \equiv a_0 + a_1 + \dots + a_r \pmod{3}$. Επομένως $3|x$ αν-ν $x \equiv 0 \pmod{3}$ αν-ν $a_0 + a_1 + \dots + a_r \equiv 0 \pmod{3}$ αν-ν $3|(a_0 + a_1 + \dots + a_r)$.

[Παρόμοια, $10^k \equiv 1 \pmod{9}$ για όλα τα $k \in \mathbb{N} \cup \{0\}$. Συνεπώς $x \equiv a_0 + a_1 + \dots + a_r \pmod{9}$, και $9|x$ αν-ν $9|(a_0 + a_1 + \dots + a_r)$.]

9.15 Γράφουμε την εξίσωση στη μορφή $y^3 = (2x+1)(2x-1)$. Αφού x είναι ακέραιος, οι παράγοντες $2x+1$, $2x-1$ είναι περιττοί ακέραιοι. Επίσης $\mu\kappa\delta(2x+1, 2x-1)$ διαιρεί το 2 που είναι η διαφορά τους. Συνεπώς $\mu\kappa\delta(2x+1, 2x-1) = 1$ (αφού δεν μπορεί να είναι το 2). Έχουμε δηλαδή ότι $2x+1$, $2x-1$ είναι σχετικά πρώτοι και το γινόμενο τους είναι κύβος. Έπεται ότι $2x+1$, $2x-1$ είναι και οι δύο κύβοι (Άσκηση 9.13). Όμως από την λίστα των κύβων $\dots, -8, -1, 0, 1, 8, 27, \dots$ είναι φανερό ότι οι μόνοι δύο κύβοι που έχουν διαφορά 2 είναι οι 1 και -1 . Συνάγουμε ότι $x = 0$, και επομένως δεν υπάρχουν λύσεις της εξίσωσης με x και y και τα δύο μη-μηδενικά.

9.16 Δεχόμαστε την υπόθεση. Τότε οι ακέραιοι a, b δεν μπορούν να είναι και οι δύο περιττοί και επίσης δεν μπορούν να είναι και οι δύο άρτιοι. Υποθέτουμε χβγ ότι a είναι άρτιος και b περιττός. Τότε $a = 2m$ και $b = 2n+1$ για κάποια $m, n \in \mathbb{Z}$. Συνεπώς, $p = a^2 + b^2 = 4m^2 + 4n^2 + 4n + 1 \equiv 1 \pmod{4}$.

10.1 (i) $\{\bar{0}, \bar{4}\}$, (ii) $\{\bar{0}\}$, (iii) $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$, (iv) $\{\bar{7}\}$

Παρατήρηση: Τα στοιχεία $\bar{3}$ και $\bar{5}$ είναι αντιστρέψιμα στο $\mathbb{Z}_8$.

10.2 Έστω ότι $\bar{a} \cdot \bar{b} = \bar{0}$ στο $\mathbb{Z}_p$ με $\bar{a}, \bar{b} \in \mathbb{Z}_p^*$. Τότε $(\bar{a})^{-1}(\bar{a} \cdot \bar{b}) = (\bar{a})^{-1} \cdot \bar{0} = \bar{0}$ και επομένως $\bar{b} (= ((\bar{a})^{-1} \cdot \bar{a}) \cdot \bar{b}) = \bar{0}$, που είναι άτοπο.

10.3 (i) (a) $\bar{5}$, (b) $\bar{3}$

(ii) Θα δείξουμε ότι ο ακέραιος a ικανοποιεί $\bar{a} \cdot \bar{5} = \bar{1}$ και στο $\mathbb{Z}_6$ και στο $\mathbb{Z}_7$ αν-ν $a = 17 + 42r$ για κάποιο $r \in \mathbb{Z}$.

($\Rightarrow$) Υποθέτουμε ότι $\bar{a} \cdot \bar{5} = \bar{1}$ και στο $\mathbb{Z}_6$ και στο $\mathbb{Z}_7$. Έπεται ότι $\bar{a} = \bar{5}$ στο $\mathbb{Z}_6$ και $\bar{a} = \bar{3}$ στο $\mathbb{Z}_7$ (από το (i), και την μοναδικότητα του αντιστρόφου). Έπεται ότι $6|(a-5)$ και $7|(a-3)$ και επομένως υπάρχουν $q_1, q_2 \in \mathbb{Z}$ με $a-5 = 6q_1$ και $a-3 = 7q_2$. Έχουμε τότε $7a-35 = 42q_1$ και $6a-18 = 42q_2$, από το οποίο προκύπτει ότι $a-17 = 42(q_1 - q_2) = 42r$ για κάποιο $r \in \mathbb{Z}$.

($\Leftarrow$) Έστω τώρα ότι $a = 17 + 42r$ όπου $r \in \mathbb{Z}$. Τότε $\bar{a} = \bar{17}$ και στο $\mathbb{Z}_6$ και στο $\mathbb{Z}_7$. Συνάγουμε ότι $\bar{a} = \bar{5}$ στο $\mathbb{Z}_6$ και $\bar{a} = \bar{3}$ στο $\mathbb{Z}_7$ και επομένως $\bar{a} \cdot \bar{5} = \bar{1}$ και στο $\mathbb{Z}_6$ και στο $\mathbb{Z}_7$.

10.4 Χρησιμοποιώντας τον Ευκλείδειο αλγόριθμο λαμβάνουμε διαδοχικά $121 = 2(56) + 9$, $56 = 6(9) + 2$, $9 = 4(2) + 1$ και $2 = 2(1) + 0$. Συνεπώς $\mu\kappa\delta(121, 56) = 1$ και το $\bar{56}$ είναι αντιστρέψιμο στο $\mathbb{Z}_{121}$. Μέσω της διαδικασίας αντανάφρεσης λαμβάνουμε επίσης, $1 = 9 - 4(2) = 9 - 4(56 - 6(9)) = 25(9) - 4(56) = 25(121 - 2(56)) - 4(56) = 25(121) + -54(56)$. Έπεται ότι $\bar{1} = \bar{-54} \cdot \bar{56} = \bar{67} \cdot \bar{56} (= \bar{56} \cdot \bar{67})$ στο $\mathbb{Z}_{121}$ και επομένως $(\bar{56})^{-1} = \bar{67}$ στο $\mathbb{Z}_{121}$.

10.5 (i) Προφανώς $\{\bar{a} + \bar{c} : \bar{c} \in \mathbb{Z}_n\} \subseteq \mathbb{Z}_n$. Έστω τώρα $\bar{x} \in \mathbb{Z}_n$. Τότε $\bar{x} = (\bar{a} + \bar{-a}) + \bar{x} = \bar{a} + (\bar{-a} + \bar{x}) = \bar{a} + \bar{(-a+x)} \in \{\bar{a} + \bar{c} : \bar{c} \in \mathbb{Z}_n\}$, αφού $\bar{-a+x} \in \mathbb{Z}_n$.

(ii) Προφανώς $\{\bar{b} \cdot \bar{c} : \bar{c} \in \mathbb{Z}_n\} \subseteq \mathbb{Z}_n$. Η υπόθεση ότι $\mu\kappa\delta(b, n) = 1$ μας εξασφαλίζει ότι υπάρχει $\bar{v} \in \mathbb{Z}_n$ με $\bar{v} \cdot \bar{b} = \bar{1} (= \bar{b} \cdot \bar{v})$. Έστω $\bar{x} \in \mathbb{Z}_n$. Τότε $\bar{x} = (\bar{b} \cdot \bar{v}) \cdot \bar{x} = \bar{b} \cdot (\bar{v} \cdot \bar{x}) \in \{\bar{b} \cdot \bar{c} : \bar{c} \in \mathbb{Z}_n\}$.

(iii) ϕ ενριπτική: $\phi(\bar{x}_1) = \phi(\bar{x}_2)$ (με $\bar{x}_1, \bar{x}_2 \in S$) $\Rightarrow \bar{b} \cdot \bar{x}_1 = \bar{b} \cdot \bar{x}_2 \Rightarrow \bar{v} \cdot (\bar{b} \cdot \bar{x}_1) = \bar{v} \cdot (\bar{b} \cdot \bar{x}_2) \Rightarrow (\bar{v} \cdot \bar{b}) \cdot \bar{x}_1 = (\bar{v} \cdot \bar{b}) \cdot \bar{x}_2 \Rightarrow \bar{1} \cdot \bar{x}_1 = \bar{1} \cdot \bar{x}_2 \Rightarrow \bar{x}_1 = \bar{x}_2$.

ϕ επιριπτική: $\bar{y} \in \bar{b}S \Rightarrow \bar{y} = \bar{b} \cdot \bar{d}$ για κάποιο $\bar{d} \in S \Rightarrow \bar{y} = \phi(\bar{d})$.

10.6 Γράφουμε $d = \mu\kappa\delta(a, n)$. Υποθέτουμε πρώτα ότι υπάρχει $\bar{y} \in \mathbb{Z}_n$ με $\bar{a} \cdot \bar{y} = \bar{b}$ στο $\mathbb{Z}_n$. Τότε $ay = qn + b$ για κάποιο $q \in \mathbb{Z}$. Από $d|a$ και $d|n$, έπεται ότι $d|b$.

Υποθέτουμε τώρα ότι $d|b$, έστω $b = kd$ με $k \in \mathbb{Z}$. Όμως υπάρχουν $s, t \in \mathbb{Z}$ με $d = sa + tn$, έχουμε δηλαδή $b = kd = k(sa + tn)$. Συνάγουμε ότι $aks = b - ktn \equiv b \pmod{n}$. Με άλλα λόγια $x = \overline{ks}$ είναι μια λύση της εξίσωσης.

10.7 Θα δείξουμε ότι $17|(4^{555} + 555^4)$. Έχουμε $555 = 32(17) + 11 = 34(16) + 11$. Από μικρό θεώρημα Fermat, $4^{16} \equiv 1 \pmod{17}$. Συνεπώς $4^{555} = (4^{16})^{34} 4^{11} \equiv 4^{11} = (4^2)^5 4 \equiv (-1)^5 4 = -4 \pmod{17}$. Έχουμε επίσης, $555^4 \equiv 11^4 \equiv (-6)^4 = 36^2 \equiv 2^2 = 4 \pmod{17}$.

10.8 Θέτουμε $n = pq$ και $A = \{i \in \mathbb{N}: 1 \leq i < n\}$. Θέτουμε επίσης $B = \{k \in A: p|k\}$ και $C = \{k \in A: q|k\}$. Έχουμε τότε ότι $B \cap C = \emptyset$, διότι $\text{εκπ}(p, q) = n (= pq)$. Συνεπώς, $\phi(n) = |A| - |B| - |C| = (pq - 1) - (q - 1) - (p - 1) = pq - p - q + 1 = (p - 1)(q - 1) = m$. Αφού $ed \equiv 1 \pmod{m}$, υπάρχει $t \in \mathbb{Z}$ τέτοιο ώστε $ed = 1 + tm = 1 + t(p - 1)(q - 1)$. Έστω τώρα $x \in \mathbb{Z}$. Αν $x \equiv 0 \pmod{p}$, είναι προφανές ότι $x^{ed} \equiv x \pmod{p}$. Υποθέτουμε τώρα ότι $p \nmid x$. Από το μικρό θεώρημα Fermat, $x^{p-1} \equiv 1 \pmod{p}$. Συνεπώς, $x^{ed} = x^{1+t(p-1)(q-1)} = x(x^{p-1})^{t(q-1)} \equiv x \pmod{p}$. Άρα, $x^{ed} \equiv x \pmod{p}$ για όλα τα $x \in \mathbb{Z}$. Με παρόμοιο συλλογισμό μπορούμε να δείξουμε ότι $x^{ed} \equiv x \pmod{q}$ για όλα τα $x \in \mathbb{Z}$. Έπεται ότι $p|(x^{ed} - x)$ και $q|(x^{ed} - x)$ και, αφού $\text{μκδ}(p, q) = 1$, έχουμε ότι $pq|(x^{ed} - x)$.

11.3 Συγκρίνετε με την Πρόταση 11.5: Έχουμε, $z_2 = z_1(\cos(\frac{\pi}{6}) + i \sin(\frac{\pi}{6})) = z_1(\frac{\sqrt{3}}{2} + i(\frac{1}{2})) = (2 + i)(\frac{\sqrt{3}}{2} + \frac{1}{2}i) = (\sqrt{3} - \frac{1}{2}) + i(1 + \frac{\sqrt{3}}{2})$.

11.4 (i) Θέτουμε $G = \{\text{rot}_0 (= i_{\mathbb{R}^2}), \text{rot}_{(\pi/2)}, \text{rot}_{\pi}, \text{rot}_{(3\pi/2)}\} \cup \{\text{ref}_0, \text{ref}_{(\pi/2)}, \text{ref}_{\pi}, \text{ref}_{(3\pi/2)}\}$. Παρατηρούμε πρώτα ότι $G \subseteq \Sigma(\Delta)$ και επομένως $|\Sigma(\Delta)| \geq 8$, αφού το σύνολο G έχει ακριβώς 8 στοιχεία.

Έστω τώρα $f \in \Sigma(\Delta)$. Τότε υπάρχουν 4 πιθανές εικόνες $f(\mathbf{1})$ για την κορυφή $\mathbf{1}$ του Δ αφού η f απεικονίζει κορυφή του Δ σε κορυφή του Δ . Αν η κορυφή $\mathbf{2}$ είναι ‘γειτονική’ προς την κορυφή $\mathbf{1}$ τότε και η κορυφή $f(\mathbf{2})$ θα είναι ‘γειτονική’ προς την $f(\mathbf{1})$ αφού $d(\mathbf{1}, \mathbf{2}) = d(f(\mathbf{1}), f(\mathbf{2}))$. [Εύκολα βλέπουμε ότι για οποιαδήποτε κορυφή του Δ , η ‘απέναντι’ κορυφή είναι σε απόσταση 2 ενώ οι ‘γειτονικές’ κορυφές είναι σε απόσταση $\sqrt{2}$.] Συνεπώς, με δεδομένο ότι έχει καθοριστεί η εικόνα $f(\mathbf{1})$, υπάρχουν μόνο δύο πιθανές εικόνες $f(\mathbf{2})$ για την κορυφή $\mathbf{2}$. Όμως, από την στιγμή που έχουν καθοριστεί οι εικόνες $f(\mathbf{1})$ και $f(\mathbf{2})$, οι ιδιότητες της f μας εξασφαλίζουν ότι καθορίζονται με μοναδικό τρόπο και οι υπόλοιπες εικόνες $f(\mathbf{3})$ και $f(\mathbf{4})$. Συνάγουμε ότι $|\Sigma(\Delta)| \leq 8$ και επομένως $|\Sigma(\Delta)| = 8$ και $G = \Sigma(\Delta)$.

(ii) Με παρόμοιο συλλογισμό όπως στο τμήμα (i), βρίσκουμε ότι $\Sigma(\Delta) = \{\text{rot}_0, \text{rot}_{\pi}, \text{ref}_0, \text{ref}_{\pi}\}$. [Υπόδειξη: Οι κορυφές του ορθογωνίου βρίσκονται πάνω σε ένα κύκλο με κέντρο το $O(0, 0)$ και ακτίνα 5. Επιπλέον, σταθεροποιώντας οποιαδήποτε από τις κορυφές του ορθογωνίου, παρατηρούμε ότι οι υπόλοιπες 3 κορυφές βρίσκονται σε απόσταση 6, 8 και 10 από την κορυφή αυτή. Συνεπώς, αν ξέρουμε την εικόνα μιας από τις κορυφές, τότε οι εικόνες των υπόλοιπων κορυφών καθορίζονται με μοναδικό τρόπο.]

11.5 Παρατηρούμε πρώτα ότι $|G| = 8$ και επομένως $G = \{\text{rot}_{(\pi k/4)}: 0 \leq k \leq 7\}$. [Εξήγηση: Από την Πρόταση 11.10 ξέρουμε ότι κάθε στοιχείο του συνόλου G επάγει μια μετάθεση του συνόλου των κορυφών του Δ . Επιπλέον, η δράση οποιαδήποτε περιστροφής γύρω από το σημείο $O(0, 0)$ καθορίζεται πλήρως από την εικόνα οποιασδήποτε από τις κορυφές του Δ . Θέτοντας $g = \text{rot}_{(\pi k/4)}$ βλέπουμε ότι $G = \{g^k: 0 \leq k \leq 7\}$.

Έστω τώρα $f, h \in G$. Τότε $f = g^i$ και $h = g^j$ για κάποια $i, j \in \mathbb{Z}$ με $0 \leq i, j \leq 7$. Έχουμε τότε από το θεώρημα διαίρεσης, ότι $i + j = 8l + r$ για κάποια $l, r \in \mathbb{Z}$ με $0 \leq r \leq 7$. Συνεπώς $\phi(f \circ h) = \phi(g^i \circ g^j) = \phi(g^{i+j}) = \phi(g^r) = \zeta^r = \zeta^{8l+r} = \zeta^{i+j} = \zeta^i \zeta^j = \phi(g^i) \phi(g^j) = \phi(f) \phi(h)$.

Τα υπόλοιπα στοιχεία του συνόλου G που μπορούν να παίξουν τον ρόλο του g πιο πάνω είναι τα g^3, g^5 και g^7 .

11.6 (i) Θέτουμε $\omega = \cos(\frac{2\pi}{6}) + i \sin(\frac{2\pi}{6}) (= \frac{1}{2} + \frac{1}{2}\sqrt{3}i)$. Τότε $\omega^6 = 1$ και $C_6 = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5\}$. [Συγκρίνετε με την Πρόταση 11.7.]

(ii) $T = \{\omega, \omega^5\}$ είναι το σύνολο των πρωταρχικών 6^{ων} ριζών της μονάδας. [Παρατηρούμε ότι $1 = (\omega^2)^3 = (\omega^3)^2 = (\omega^4)^3$.]

11.7 Από το θεώρημα διαίρεσης, $131 = (21)(6) + 5$. Τώρα $\omega^6 = 1$ και $\pi^6 = (1)$, η ταυτοτική απεικόνιση. Έπεται ότι $\omega^{131} = (\omega^6)^{21}\omega^5 = \omega^5$ και $\pi^{131} = (\pi^6)^{21}\pi^5 = \pi^5$. Θέτουμε $s = t = 5$.

11.8 (i) Κοιτάζτε την Πρόταση 11.7.

(ii) Έστω $z, u \in C_n$. Τότε $z^n = 1 = u^n$. Χρησιμοποιώντας την αντιμεταθετική ιδιότητα του πολλαπλασιασμού στο $\mathbb{C}$, έχουμε $(zu)^n = z^n u^n = 1$. Άρα $zu \in C_n$.

(iii) Από την Άσκηση 7.6, αφού $u \neq 0$, υπάρχει $v \in \mathbb{C}$ με $uv = 1 = vu$. Για να δείξουμε ότι $v \in C_n$, αρκεί να παρατηρήσουμε ότι $1 = (uv)^n = u^n v^n = v^n$ (χρησιμοποιούμε και πάλι ότι ο πολλαπλασιασμός στο $\mathbb{C}$ είναι αντιμεταθετικός, μαζί με την υπόθεση μας ότι $u^n = 1$).

(iv) Έστω x μια πρωταρχική n -οστή ρίζα της μονάδας και $k \in \{1, 2, \dots, n\}$. Προφανώς $x^n = 1$. Έχουμε τότε $(x^k)^n = x^{kn} = (x^n)^k = 1$. Συνεπώς $\{1, x, \dots, x^{n-1}\} \subseteq C_n$. Αφού το σύνολο C_n έχει ακριβώς n στοιχεία, αρκεί να δείξουμε ότι τα στοιχεία $x, \dots, x^{n-1}, x^n (= 1)$ είναι διακεκριμένα. Υποθέτουμε ότι $x^r = x^s$ με $1 \leq s < r \leq n$. Συμβολίζουμε με v το μοναδικό στοιχείο του $\mathbb{C}$ με $xv = 1 (= vx)$, κοιτάζτε την Άσκηση 7.6. Έχουμε τότε ότι $1 = (xv)^s = x^s v^s = x^r v^s = x^{r-s} x^s v^s = x^{r-s} (xv)^s = x^{r-s}$ όπου $1 \leq r - s < n$, που προφανώς αντιφάσκει με την υπόθεση μας ότι x είναι μια πρωταρχική n -οστή ρίζα της μονάδας.

11.9 Έστω $(z, w) \in C_{12} \times C_{12}$. Παρατηρούμε ότι $(z, w) \in R_1$ αν-ν $zw^{-1} \in C_4$ αν-ν $(zw^{-1})^{-1} \in C_4$ (Άσκηση 11.8(iii)) αν-ν $wz^{-1} \in C_4$ αν-ν $z^{-1}w \in C_4$ αν-ν $(z, w) \in R_2$. Έχουμε δηλαδή ότι $R_1 = R_2$ (για να το δείξουμε αυτό έχουμε χρησιμοποιήσει επίσης ότι ο πολλαπλασιασμός μιγαδικών αριθμών ικανοποιεί την αντιμεταθετική ιδιότητα). Για την συνέχεια θέτουμε $R = R_1 (= R_2)$.

Έστω τώρα $a, b, c \in C_{12}$. Έχουμε τότε

(1) $aa^{-1} = 1 \in C_4$, άρα $(a, a) \in R$.

(2) $(a, b) \in R \Rightarrow ab^{-1} \in C_4 \Rightarrow (ab^{-1})^{-1} \in C_4$ (Άσκηση 11.8(iii)) $\Rightarrow ba^{-1} \in C_4 \Rightarrow (b, a) \in R$.

(3) $(a, b) \in R$ και $(b, c) \in R \Rightarrow ab^{-1}, bc^{-1} \in C_4 \Rightarrow ac^{-1} (= ab^{-1}bc^{-1}) \in C_4$ (Άσκηση 11.8(iii)) $\Rightarrow (a, c) \in R$.

Θέτουμε $\omega = \cos(\frac{2\pi}{12}) + i \sin(\frac{2\pi}{12}) \in \mathbb{C}$. Οι διακεκριμένες κλάσεις ισοδυναμίας ως προς την σχέση R είναι τα υποσύνολα $\{1, \omega^3, \omega^6, \omega^9\}$, $\{\omega, \omega^4, \omega^7, \omega^{10}\}$ και $\{\omega^2, \omega^5, \omega^8, \omega^{11}\}$ του C_{12} .

11.8 Θέτουμε $d = \mu\chi\delta(m, n)$. Αν $z^d = 1$ όπου $z \in \mathbb{C}$, τότε $z^m = 1 = z^n$ και επομένως $C_d \subseteq C_m \cap C_n$. Έστω τώρα $z \in \mathbb{C}$ με $z \in C_m \cap C_n$. Τότε $d = sm + tn$ για κάποια $s, t \in \mathbb{Z}$, και επομένως $z^d = (z^m)^s (z^n)^t = 1$. Συνάγουμε ότι ισχύει επίσης $C_m \cap C_n \subseteq C_d$, άρα $C_m \cap C_n = C_d$.

12.2 (i) και (ii): Κοιτάζτε αντίστοιχα την Παράγραφο 4.2 και την Παράγραφο 11.1 (Πρόταση 11.2 και Παρατήρηση 11.3).

(iii), (iv): Προκύπτουν εύκολα από τις ιδιότητες της πρόσθεσης και πολλαπλασιασμού στα $\mathbb{R}$ και $\mathbb{C}$.

(v) Κοιτάζτε την Παράγραφο 11.2 (χρησιμοποιούμε εδώ ότι ο πολλαπλασιασμός στο $\mathbb{C}$ είναι προσεταιριστικός).

(vi) Κοιτάζτε τις Προτάσεις 10.2 και 10.5. Για να δείξουμε ότι ο πολλαπλασιασμός που έχουμε ορίσει στο $\mathbb{Z}_n$ αποτελεί διμελή πράξη στο $\mathbb{Z}_n^*$: Έστω $\bar{a}, \bar{b} \in \mathbb{Z}_n^*$. Από τον ορισμό του συνόλου $\mathbb{Z}_n^*$, υπάρχουν $\bar{u}, \bar{v} \in \mathbb{Z}_n$ με $\bar{a} \cdot \bar{u} = \bar{1} (= \bar{u} \cdot \bar{a})$ και $\bar{b} \cdot \bar{v} = \bar{1} (= \bar{v} \cdot \bar{b})$. Τώρα $\bar{v} \cdot \bar{u} (= \bar{v}\bar{u}) \in \mathbb{Z}_n$ και $(\bar{v} \cdot \bar{u}) \cdot (\bar{a} \cdot \bar{b}) = \bar{v} \cdot (\bar{u} \cdot \bar{a}) \cdot \bar{b} = (\bar{v} \cdot \bar{1}) \cdot \bar{b} =$

$\bar{v} \cdot \bar{b} = \bar{1} (= (\bar{a} \cdot \bar{b}) \cdot (\bar{v} \cdot \bar{u}))$. Συνάγουμε ότι $\bar{a} \cdot \bar{b} \in \mathbb{Z}_n^*$. [Χρησιμοποιήσαμε εδώ ότι ο πολλαπλασιασμός στο $\mathbb{Z}_n$ ικανοποιεί την προσεταιριστική ιδιότητα, όπως επίσης και την Πρόταση 5.5.]

(vii) Ο πολλαπλασιασμός πινάκων είναι διμελής πράξη στο σύνολο $GL(n, \mathbb{R})$: Αν $A, B \in GL(n, \mathbb{R})$ τότε $\det(A) \neq 0$ και $\det(B) \neq 0$, συνεπώς $\det(AB) = \det(A)\det(B) \neq 0$. Άρα $AB \in GL(n, \mathbb{R})$. [Χρησιμοποιήσαμε ότι $P \in M_n(\mathbb{R})$ είναι αντιστρέψιμος αν-ν $\det(P) \neq 0$]. Εναλλακτικά, θα μπορούσαμε να χρησιμοποιήσουμε παρόμοιο συλλογισμό με αυτό που δώσαμε για το τμήμα (vi) της άσκησης. Ο ταυτοτικός πίνακας είναι το ουδέτερο στοιχείο της $GL(n, \mathbb{R})$

Από τον ορισμό του αντίστροφου πίνακα, ο αντίστροφος του $A \in GL(n, \mathbb{R})$ αποτελεί συμμετρικό στοιχείο του A στην $GL(n, \mathbb{R})$. Τέλος, από το μάθημα της γραμμικής άλγεβρας, ξέρουμε ότι ο πολλαπλασιασμός πινάκων ικανοποιεί την προσεταιριστική ιδιότητα.

(viii) Έστω $f, g \in \Sigma(\Delta)$. Τότε $f \circ g \in O(\mathbb{R}^2)$, από το (ii) αφού $f, g \in O(\mathbb{R}^2)$, και $(f \circ g)(\Delta) = \{(f \circ g)(u) : u \in \Delta\} = \{f(g(u)) : u \in \Delta\}$. Όμως $\{g(u) : u \in \Delta\} = g(\Delta) = \Delta$, αφού $g \in \Sigma(\Delta)$. Συνεπώς, $(f \circ g)(\Delta) = \{f(v) : v \in \Delta\} = \Delta$, αφού $f \in \Sigma(\Delta)$. Άρα $(f \circ g) \in \Sigma(\Delta)$. Η ταυτοτική απεικόνιση $i_{\mathbb{R}^2} \in \Sigma(\Delta)$ είναι το ουδέτερο στοιχείο της $\Sigma(\Delta)$. Η f είναι μια αμφιμονοσήμαντη συνάρτηση και η αντίστροφή της, έστω $h : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, επίσης ανήκει στην $O(\mathbb{R}^2)$, συγκρίνετε με το τμήμα (ii). Επιπλέον, $h(\Delta) = h(f(\Delta)) = h(\{f(u) : u \in \Delta\}) = \{h(f(u)) : u \in \Delta\} = \{(h \circ f)(u) : u \in \Delta\} = \{i_{\mathbb{R}^2}(u) : u \in \Delta\} = \Delta$, και επομένως $h \in \Sigma(\Delta)$. Χρησιμοποιούμε, τέλος, ότι η σύνθεση συναρτήσεων είναι προσεταιριστική.

12.3 Έστω $a, b \in G$. Τότε $ba \in G$ και $(ba)^2 = 1_G$. Άρα, $ab = (ab)1_G = (ab)(ba)(ba) = a(b^2)aba = a1_Gaba = a^2ba = 1_Gba = ba$ (χρησιμοποιούμε την Πρόταση 5.5).

12.4 Προφανώς $\{hg : g \in G\} \subseteq G$ αφού G είναι ομάδα και $h \in G$. Έστω τώρα $f \in G$. Έχουμε ότι $h^{-1} \in G$ και επομένως $h^{-1}f \in G$. Άρα $f = 1_G f = (hh^{-1})f = h(h^{-1}f) \in \{hg : g \in G\}$. Συνάγουμε ότι $G \subseteq \{hg : g \in G\}$.

12.5 (i) Αν $\mathbf{x}, \mathbf{y} \in \mathbb{R}^2$ τότε $\|f(\mathbf{x}) - f(\mathbf{y})\| = \|(\mathbf{x} + \mathbf{a}) - (\mathbf{y} + \mathbf{a})\| = \|\mathbf{x} - \mathbf{y}\|$.

(ii) Έστω T μια κίνηση με $T(\mathbf{0}) = \mathbf{w} (\in \mathbb{R}^2)$. Θέτουμε $S : \mathbb{R}^2 \rightarrow \mathbb{R}^2 : \mathbf{x} \mapsto \mathbf{x} - \mathbf{w}$, ($\mathbf{x} \in \mathbb{R}^2$). Τότε $S \circ T$ είναι μια κίνηση αφού, για όλα τα $\mathbf{x}, \mathbf{y} \in \mathbb{R}^2$ έχουμε $\|(S \circ T)(\mathbf{x}) - (S \circ T)(\mathbf{y})\| = \|S(T(\mathbf{x})) - S(T(\mathbf{y}))\| = \|T(\mathbf{x}) - T(\mathbf{y})\| = \|\mathbf{x} - \mathbf{y}\|$, χρησιμοποιώντας διαδοχικά ότι S είναι μια κίνηση και μετά ότι T είναι μια κίνηση. Επιπλέον, $(S \circ T)(\mathbf{0}) = \mathbf{0}$ και επομένως $S \circ T \in O(\mathbb{R}^2)$, από την Πρόταση 11.11. Η συνάρτηση S είναι προφανώς αμφιμονοσήμαντη, με αντίστροφή συνάρτηση $S^{-1} : \mathbb{R}^2 \rightarrow \mathbb{R}^2 : \mathbf{x} \mapsto \mathbf{x} + \mathbf{w}$ ($\mathbf{x} \in \mathbb{R}^2$), η οποία επίσης είναι μεταφορά. Θέτουμε $T_1 = S^{-1}$ και $T_2 = S \circ T$.

(iii) Παρατηρούμε πρώτα ότι $i_{\mathbb{R}^2} \in K(\mathbb{R}^2)$. Με συλλογισμό όπως στο τμήμα (ii) βλέπουμε ότι η σύνθεση δύο κινήσεων είναι μια κίνηση. Επίσης από το τμήμα (ii) βλέπουμε ότι κάθε κίνηση είναι αμφιμονοσήμαντη συνάρτηση (αφού κάθε μεταφορά και κάθε στοιχείο της $O(\mathbb{R}^2)$ είναι αμφιμονοσήμαντες συναρτήσεις) και επομένως υπάρχει η αντίστροφή συνάρτηση, η οποία επίσης είναι μια κίνηση. [Εξήγηση: Αν T είναι μια κίνηση, και $\mathbf{x}, \mathbf{y} \in \mathbb{R}^2$ έχουμε $\|\mathbf{x} - \mathbf{y}\| = \|(TT^{-1})(\mathbf{x}) - (TT^{-1})(\mathbf{y})\| = \|T(T^{-1}(\mathbf{x})) - T(T^{-1}(\mathbf{y}))\| = \|T^{-1}(\mathbf{x}) - T^{-1}(\mathbf{y})\|$.]

12.6 (i) Αν $a \equiv \pm 1 \pmod{p}$, τότε $a^2 \equiv 1 \pmod{p}$ από την Πρόταση 9.19.

Έχουμε επίσης, $a^2 \equiv 1 \pmod{p} \Rightarrow p|(a^2 - 1) \Rightarrow p|(a - 1)(a + 1) \Rightarrow p|(a - 1)$ ή $p|(a + 1) \Rightarrow a \equiv 1 \pmod{p}$ ή $a \equiv -1 \pmod{p}$.

(ii) Προφανώς το αποτέλεσμα ισχύει στην περίπτωση $p = 3$. Υποθέτουμε τώρα ότι p είναι πρώτος με $p > 3$. Από το (i), τα μόνα στοιχεία της $\mathbb{Z}_p^* (= \{\bar{1}, \bar{2}, \dots, \overline{p-1}\})$ που ικανοποιούν $g = g^{-1}$ (ή, ισοδύναμα, $g^2 = \bar{1}$) είναι τα $\bar{1}$ και $\overline{p-1} (= \overline{-1})$, όπου $\bar{1} \neq \overline{p-1}$ στο $\mathbb{Z}_p$ (αφού $p > 3$). [Χρησιμοποιήσαμε εδώ ότι $\overline{u^2} = (\bar{u})^2$ στο $\mathbb{Z}_p$ οποιεδήποτε $u \in \mathbb{Z}$.] Έπεται ότι τα υπόλοιπα $p - 3$ στοιχεία της $\mathbb{Z}_p^*$ (δηλαδή τα στοιχεία του συνόλου $\mathbb{Z}_p^* - \{\bar{1}, \overline{p-1}\}$) προκύπτουν ως ζεύγη $\{g, g^{-1}\}$ με $g \neq g^{-1}$ (παρατηρούμε ότι $p - 3$

είναι άρτιος). Συνεπώς το γινόμενο των στοιχείων του συνόλου $\mathbb{Z}_p^* - \{\bar{1}, \overline{p-1}\}$ ισούται με $\bar{1}$ στο $\mathbb{Z}_p$ (χρησιμοποιούμε ότι ο πολλαπλασιασμός στο $\mathbb{Z}_p$ είναι αντιμεταθετικός και προσεταιριστικός). Συνάγουμε ότι $(p-1)! = \bar{1} \cdot \overline{(p-1)} = \overline{(p-1)} = -\bar{1}$ στο $\mathbb{Z}_p$ (ή, ισοδύναμα, $(p-1)! \equiv -1 \pmod{p}$).

12.7 Παρατηρούμε πρώτα ότι $k \in S$. Έστω t το ελάχιστο στοιχείο του S (αρχή καλής διάταξης). Προφανώς $1 \leq t \leq k$. Υποθέτουμε ότι $1 \leq t < k$. Τότε $2 \leq 1+t \leq k$ και $\rho^t(i_1) = i_{1+t} \neq i_1$, αφού τα σύμβολα $i_1, i_2, \dots, i_k$ είναι διακεκριμένα. Έπεται ότι $\rho^t \neq i_X$ που προφανώς αντιφάσκει με την επιλογή του t ως ελάχιστου στοιχείου του S . Συνάγουμε ότι $t = k$.

12.8 Έστω ότι H αποτελεί ομάδα ως προς την ίδια πράξη της G . Πιο ειδικά $H \neq \emptyset$. Έχουμε ότι $1_H = 1_{H1_H}$. Όμως $1_H \in G$, επομένως υπάρχει $a \in G$ με $1_H a = 1_G (= a 1_H)$. Συνεπώς, $1_G = 1_H a = (1_H 1_H) a = 1_H (1_H a) = 1_H 1_G = 1_H$. Έστω τώρα $h \in H$. Υπάρχει $h_1 \in H (\subseteq G)$ (το μοναδικό αντίστροφο του h στην H), τέτοιο ώστε $h h_1 = 1_H = h_1 h$. Έπεται ότι $h h_1 = 1_G = h_1 h$, έχουμε δηλαδή ότι h_1 είναι επίσης το μοναδικό αντίστροφο του στοιχείου $h \in H$, θεωρώντας τώρα το h ως στοιχείο της G . Συνάγουμε ότι $(h^{-1})_H = h_1 = (h^{-1})_G$.

12.9 Αρκεί να δείξουμε ότι το γινόμενο δύο αντιμεταθέσεων είναι γινόμενο 3-κύκλων. Θέτουμε $X = \{1, 2, \dots, n\}$. Έστω a, a_1, a_2 διακεκριμένα στοιχεία του συνόλου X . Τότε $(a_1 a_2)(a_1 a_2) = (1) = (a a_1 a_2)^3$ και $(a a_1)(a_1 a_2) = (a a_1 a_2)$. Παρατηρούμε επίσης ότι $(a_1 a_2) = (a a_1)(a a_2)(a a_1)$. Υποθέτουμε τώρα ότι $\{b_1, b_2\} \subseteq X$ με $\{b_1, b_2\} \cap \{a_1, a_2\} = \emptyset$. Αφού $n \geq 5$, υπάρχει $c \in X - \{a_1, a_2, b_1, b_2\}$. Έχουμε τότε, $(b_1 b_2)(a_1 a_2) = (c b_1)(c b_2)(c b_1)(c a_1)(c a_2)(c a_1) = ((c b_1)(c b_2))((c b_1)(c a_1))((c a_2)(c a_1)) = (c b_2 b_1)(c a_1 b_1)(c a_1 a_2)$.

12.10 Έστω $\emptyset \neq H \subseteq G$, όπου G ομάδα πεπερασμένης τάξης.

Αν $H \leq G$, τότε προφανώς $h_1 h_2 \in H$ για όλα τα $h_1, h_2 \in H$.

Αντίστροφα, υποθέτουμε ότι $h_1 h_2 \in H$ οποτεδήποτε $h_1, h_2 \in H$. Υπάρχει στοιχείο $a \in H$ (αφού $H \neq \emptyset$). Τότε τα στοιχεία $a^1 (= a)$, a^2 , a^3 , ... (που ανήκουν όλα στο υποσύνολο H από την ιδιότητα του συνόλου H) δεν μπορούν να είναι όλα διαφορετικά μεταξύ τους αφού H είναι ένα πεπερασμένο σύνολο (G είναι πεπερασμένης τάξης). Έπεται ότι $a^t = a^s$ για κάποια $s, t \in \mathbb{N}$ με $s < t$. Συνεπώς $a^{t-s} = 1_G$. [Εξήγηση: G είναι ομάδα με $a \in G$, άρα $(a^{-1})^s (= a^{-s}) \in G$.] Τώρα $t-s \in \mathbb{N}$ και επομένως $a^{t-s} \in H$, πάλι από την ιδιότητα του υποσυνόλου H . Συνάγουμε ότι $1_G \in H$, έχουμε δηλαδή ότι το a^0 επίσης ανήκει στο σύνολο H . Θέτουμε $r = t-s (\in \mathbb{N})$. Τότε $r-1 \in \mathbb{N} \cup \{0\}$ και επομένως $a^{r-1} \in H$. Παρατηρούμε όμως ότι $a a^{r-1} = a^1 a^{r-1} = a^r = 1_G = a^{r-1} a$. Έχουμε δείξει ότι $a^{-1} (= a^{r-1}) \in H$. Τέλος, από την υπόθεση μας, η διμελής πράξη στην G (η οποία είναι προσεταιριστική) αποτελεί επίσης διμελή πράξη πάνω στο υποσύνολο H . Συμπεραίνουμε ότι $H \leq G$.

Παρατήρηση. Θέτοντας $\mathbb{Z}^+ = \{x \in \mathbb{Z}: x > 0\}$, παρατηρούμε ότι η συνηθισμένη πρόσθεση (+) των ακεραίων είναι μια διμελής πράξη πάνω στο σύνολο $\mathbb{Z}^+$, όμως $(\mathbb{Z}^+, +)$ δεν αποτελεί υποομάδα της $(\mathbb{Z}, +)$.

12.11 (a) (i) Άμεση συνέπεια του ορισμού της υποομάδας.

(ii) Προφανώς $SL(n, \mathbb{R}) \subseteq GL(n, \mathbb{R})$ αφού $\det C \neq 0$ για όλα τα $C \in SL(n, \mathbb{R})$. Ο πίνακας I_n είναι το μοναδιαίο στοιχείο της $GL(n, \mathbb{R})$ και $I_n \in SL(n, \mathbb{R})$ αφού $\det(I_n) = 1$. Έστω $A, B \in SL(n, \mathbb{R})$. Τότε $AB \in SL(n, \mathbb{R})$ αφού $\det(AB) = \det(A) \cdot \det(B) = 1 \cdot 1 = 1$. Επίσης $A^{-1} \in SL(n, \mathbb{R})$ αφού $\det(A^{-1}) = 1/\det(A) = 1$.

(iii) Άμεση συνέπεια της Πρότασης 11.2 και της Παρατήρησης 11.3.

(iv) Παρατηρούμε πρώτα ότι $0 \in \mathbb{Q} (\subseteq \mathbb{R})$. Επίσης, αν $a, b \in \mathbb{Q}$ τότε προφανώς $a+b \in \mathbb{Q}$ και $-a \in \mathbb{Q}$.

(v) Προφανώς $H \subseteq S_n$ και $(1) \in H$. Έστω $\alpha, \beta \in H$. Τότε $\alpha(1) = 1$ και $\beta(1) = 1$, συνεπώς $(\alpha \circ \beta)(1) = \alpha(\beta(1)) = \alpha(1) = 1$ και $\alpha^{-1}(1) = \alpha^{-1}(\alpha(1)) = (\alpha^{-1} \circ \alpha)(1) = (1)$. Έπεται ότι $\alpha\beta \in H$ και $\alpha^{-1} \in H$.

(vi) Παρατηρούμε ότι $(1 \ 2 \ 3)^{-1} = (1 \ 3 \ 2)$ και $(1 \ 2)^{-1} = (1 \ 2)$. Η κλειστότητα προκύπτει εύκολα. (Τα υποσύνολα τα οποία εξετάζουμε προφανώς είναι υποσύνολα της S_3 .)

(vii) Παρατηρούμε ότι $A_n \subseteq S_n$ και $(1) \in A_n$. Έστω $\alpha, \beta \in A_n$. Τότε $\text{sgn}(\alpha\beta) = \text{sgn}(\alpha)\text{sgn}(\beta) = (+1)(+1) = +1$. Έπεται ότι $\alpha\beta \in A_n$. Επίσης $+1 = \text{sgn}((1)) = \text{sgn}(\alpha\alpha^{-1}) = \text{sgn}(\alpha)\text{sgn}(\alpha^{-1}) = \text{sgn}(\alpha^{-1})$. Άρα $\alpha^{-1} \in A_n$.

(viii) Έχουμε ότι $n = kl$ για κάποιο $l \in \mathbb{N}$. Αν $x \in C_k$ τότε $x^n = (x^k)^l = 1$, και επομένως $x \in C_n$. Χρησιμοποιούμε τώρα την Παρατήρηση κάτω από τον ορισμό της υποομάδας, και το Παράδειγμα 12.1(v).

(ix) Θέτουμε $H = \{g^k : k \in \mathbb{Z}\}$. Παρατηρούμε πρώτα ότι $H \subseteq G$. Επίσης $1_G \in H$, αφού $1_G = g^0$ και $0 \in \mathbb{Z}$. Έστω τώρα $a, b \in H$. Έχουμε επομένως ότι $a = g^{k_1}$ και $b = g^{k_2}$ για κάποια $k_1, k_2 \in \mathbb{Z}$. Τότε, $k_1 + k_2 \in \mathbb{Z}$, $-k_1 \in \mathbb{Z}$ και, επιπλέον, $ab = g^{k_1}g^{k_2} = g^{k_1+k_2}$ και $a^{-1} = (g^{k_1})^{-1} = g^{-k_1}$. Άρα $ab \in H$ και $a^{-1} \in H$.

(b) Προφανώς $T \subseteq \text{GL}(2, \mathbb{R})$ αφού $\det P \neq 0$ οποτεδήποτε $P \in T$. Παρατηρούμε πρώτα ότι $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in T$. Έστω τώρα $A, B \in T$. Τότε $A = \begin{pmatrix} a & c \\ 0 & b \end{pmatrix}$ και $B = \begin{pmatrix} a' & c' \\ 0 & b' \end{pmatrix}$ όπου $a, b, c, a', b', c' \in \mathbb{R}$ με $ab \neq 0$ και $a'b' \neq 0$. Συνεπώς $AB = \begin{pmatrix} aa' & ac' + cb' \\ 0 & bb' \end{pmatrix} \in T$ αφού $(aa')(bb') = (ab)(a'b') \neq 0$. Επίσης $A^{-1} = \frac{1}{(ab)} \begin{pmatrix} b & -c \\ 0 & a \end{pmatrix} \in T$, (αφού $ba \neq 0$). Έπεται ότι $AB \in T$ και $A^{-1} \in T$. Συνάγουμε ότι $T \leq \text{GL}(2, \mathbb{R})$.

(c) Παρατηρούμε ότι $O(n, \mathbb{R}) \subseteq \text{GL}(n, \mathbb{R})$ αφού όλα τα στοιχεία του συνόλου $O(n, \mathbb{R})$ είναι αντιστρέψιμοι πίνακες. Προφανώς $I_n \in O(n, \mathbb{R})$. Έστω τώρα $A, B \in O(n, \mathbb{R})$. Τότε $AA^t = I_n = A^tA$ και $BB^t = I_n = B^tB$. Συνεπώς $(AB)(AB)^t = AB(B^tA^t) = A(BB^t)A^t = AA^t = I_n = B^t(A^tA)B = (B^tA^t)(AB) = (AB)^t(AB)$. Άρα $AB \in O(n, \mathbb{R})$. Έχουμε επίσης, $A^t(A^t)^t = I_n = (A^t)^tA^t$ και επομένως $A^{-1} (= A^t) \in O(n, \mathbb{R})$. Συνάγουμε ότι $O(n, \mathbb{R}) \leq \text{GL}(n, \mathbb{R})$.

12.12 Υποθέτουμε ότι G είναι ομάδα πεπερασμένης τάξης με τάξη άρτιο αριθμό και, επιπλέον, ότι G δεν περιέχει στοιχείο τάξης 2. Τότε $g \neq g^{-1}$ για όλα τα $g \in G - \{1_G\}$. [Εξήγηση: Αν $g \in G - \{1_G\}$ με $g = g^{-1}$, τότε $g^2 = 1_G$ με $g^1 \neq 1_G$ και επομένως $\text{o}(g) = 2$.] Έπεται ότι τα στοιχεία της G είναι το 1_G και ζεύγη της μορφής $\{g, g^{-1}\}$ όπου $g \neq g^{-1}$. Αφού G είναι πεπερασμένη, συμπεραίνουμε ότι $|G| = 1 + 2k$ για κάποιο $k \in \mathbb{N}$, που είναι άτοπο.

12.13 (i) Έστω ότι υπάρχει $q \in \mathbb{Q}$ με $\mathbb{Q} = \langle q \rangle$. Προφανώς $q \neq 0$. Όμως $q/2 \in \mathbb{Q}$, άρα $q/2 = rq$ για κάποιο $r \in \mathbb{Z}$. [Σημείωση: Έχουμε ότι $r \cdot q = rq$ (πολλαπλασιασμός ρητών στην περίπτωση μας εδώ) — συγκρίνετε με τον ορισμό του συμβόλου $r \cdot q$ στην Παράγραφο 12.3.] Πολλαπλασιάζοντας (συνηθισμένους πολλαπλασιασμός στο $\mathbb{Q}$) και τα δύο μέλη της εξίσωσης $q/2 = rq$ με το $q^{-1} (\in \mathbb{Q})$, παίρνουμε $1/2 = r$ με $r \in \mathbb{Z}$, που είναι άτοπο.

(ii) $\mathbb{Z}_7^* = \langle \bar{3} \rangle = \{\bar{3}, \bar{2}, \bar{6}, \bar{4}, \bar{5}, \bar{1}\}$, άρα $(\mathbb{Z}_7^*, \cdot)$ είναι κυκλική.

(iii) Έχουμε ότι $C_{12} = \langle \omega \rangle$. Παρατηρούμε ότι $\langle \omega^3 \rangle = \{1, \omega^3, (\omega^3)^2, (\omega^3)^3\} = \{1, \omega^3, \omega^6, \omega^9\}$ και $\langle \omega^5 \rangle = \langle \omega \rangle = C_{12}$ (συγκρίνετε με την συζήτηση στην σελίδα 110).

12.14 Θέτουμε $r = \text{εκπ}(m, n)$. Τότε $m|r$ και $n|r$. Από τον ορισμό, $(ab)^r = (ab)(ab) \dots (ab)$, r φορές. Όμως $ab = ba$, άρα $(ab)^r = a^r b^r = 1_G$ (υπάρχουν $k, l \in \mathbb{N}$ με $r = km = ln$). Έπεται ότι $\text{o}(ab) \leq r$. Έστω τώρα $t \in \mathbb{N}$ με $(ab)^t = 1_G$. Παρεμβάλλοντας την υπόθεση μας ότι $ab = ba$, βλέπουμε ότι $a^t b^t = 1_G$. Επομένως $a^t = b^{-t} \in \langle a \rangle \cap \langle b \rangle = \{1_G\}$. Έχουμε δηλαδή ότι $a^t = 1_G$ και $b^{-t} = 1_G$. Επομένως, $b^t = (b^{-t})^{-1} = (1_G)^{-1} = 1_G$. Από την Παρατήρηση 12.28(ii), έχουμε ότι $m|t$ και $n|t$. Συνεπώς $t \geq r$. Συνάγουμε ότι $\text{o}(ab) \geq r$, και επομένως $\text{o}(ab) = r$.

12.15 Για $k \in \mathbb{N}$ ισχύει, $(g^m)^k = 1_G$ αν-ν $n|mk$ αν-ν $(\frac{n}{d}) | (\frac{m}{d})k$ αν-ν $(\frac{n}{d}) | k$, αφού $\mu\kappa\delta(\frac{n}{d}, \frac{m}{d}) = 1$. Έχουμε, δηλαδή, ότι $(g^m)^k = 1_G$ αν, και μόνο αν, k είναι ακέραιο πολλαπλάσιο του $\frac{n}{d}$. Συνάγουμε ότι $o(g^m) = \frac{n}{d}$.

12.16 (i) $\rho = (1\ 4\ 5\ 6\ 7\ 8\ 3)(2)(9)$, $\sigma = (1\ 3\ 9)(2\ 5\ 6\ 7\ 4)(8)$, $\rho\sigma = (1)(2\ 6\ 8\ 3\ 9\ 4)(5\ 7)$. Τύποι κύκλων: $(7, 1, 1)$, $(5, 3, 1)$, $(6, 2, 1)$ αντίστοιχα.

(ii) Έχουμε ότι $\rho = (1\ 4\ 5\ 6\ 7\ 8\ 3) = (1\ 3)(1\ 8)(1\ 7)(1\ 6)(1\ 5)(1\ 4)$, $\sigma = (1\ 3\ 9)(2\ 5\ 6\ 7\ 4) = (1\ 9)(1\ 3)(2\ 4)(2\ 7)(2\ 6)(2\ 5)$ και $\rho\sigma = (2\ 6\ 8\ 3\ 9\ 4)(5\ 7)$. Παρατηρούμε ότι $\text{sgn}(\rho) = +1 = \text{sgn}(\sigma)$. Έχουμε επίσης ότι $o(\rho) = 7 = o(\sigma\rho\sigma^{-1})$ από την Άσκηση 12.7, και $o(\sigma) = \text{εκπ}(3, 5) = 15$ και $o(\rho\sigma) = \text{εκπ}(2, 6) = 6$, από την Άσκηση 12.14. [Παρατήρηση: Αφού ρ είναι ένας 7-κύκλος τότε, από την Πρόταση 12.12, και η $\sigma\rho\sigma^{-1}$ είναι επίσης ένας 7-κύκλος.]

(iii) $\tau\sigma\tau^{-1} = \tau(1\ 3\ 9)\tau^{-1}\tau(2\ 5\ 6\ 7\ 4)\tau^{-1} = (1\ 2\ 9)(4\ 5\ 3\ 7\ 6)$

(iv) Δεν υπάρχει τέτοιο π αφού οι μεταθέσεις σ και $(1\ 2\ 3)(4\ 5\ 6)$ δεν έχουν τον ίδιο τύπο κύκλων.

Έστω ότι υπάρχει $\gamma \in S_9$ με $\gamma\rho\sigma\gamma^{-1} = (1\ 2)(3\ 4\ 5\ 6\ 7\ 8)$. Αφού οι κύκλοι $(2\ 6\ 8\ 3\ 9\ 4)$ και $(5\ 7)$ είναι ξένοι μεταξύ τους, θα είχαμε τότε $\gamma(1\ 2\ 6\ 8\ 3\ 9\ 4)(5\ 7)\gamma^{-1} = \gamma(5\ 7)(2\ 6\ 8\ 3\ 9\ 4)\gamma^{-1} = \gamma(5\ 7)\gamma^{-1}\gamma(2\ 6\ 8\ 3\ 9\ 4)\gamma^{-1} = (\gamma(5)\ \gamma(7))(\gamma(2)\ \gamma(6)\ \gamma(8)\ \gamma(3)\ \gamma(9)\ \gamma(4))$. Ελέγξτε, για παράδειγμα, ότι $\gamma = (1\ 9\ 7\ 2\ 3\ 6\ 4\ 8\ 5)$ ικανοποιεί την σχέση αυτή.

12.17 Έστω $\alpha \in \{\omega, \omega^2\} \subseteq C_3$ όπου $\omega = \cos(2\pi/3) + i\sin(2\pi/3)$. Έχουμε τότε ότι $o(1, \bar{1}) = 1$, $o(1, \bar{5}) = 2$, $o(\alpha, \bar{1}) = 3$ και $o(\alpha, \bar{5}) = 6$. [Εξήγηση για το $o(\alpha, \bar{5})$: Παρατηρούμε πρώτα ότι $(\alpha, \bar{5})^6 = (\alpha^6, (\bar{5})^6) = (1, \bar{1}) = 1_G$, όπου $G = C_3 \times \mathbb{Z}_5^*$. Άρα $o(\alpha, \bar{5}) \leq 6$. Έστω τώρα ότι $(\alpha, \bar{5})^r = (1, \bar{1})$ για κάποιο $r \in \mathbb{N}$. Τότε $(\alpha^r, (\bar{5})^r) = (1, \bar{1})$ και επομένως $\alpha^r = 1$ και $(\bar{5})^r = \bar{1}$. Από την Παρατήρηση 12.28(ii), έχουμε ότι $3|r$ και $2|r$ αφού $o(\alpha) = 3$ και $o(\bar{5}) = 2$. Έπεται ότι $6|r$ αφού $\mu\kappa\delta(2, 3) = 1$ (Άσκηση 9.5(ii)). Συνάγουμε ότι $r \geq 6$ και επομένως $o(\alpha, \bar{5}) = 6$.]

12.19 Χρωματίζοντας τα τετράγωνα μαύρα και άσπρα εναλλάξ, όπως σε μια σκακιέρα, το χρώμα της κενής θέσης αλλάζει σε κάθε βήμα. Αφού οι κενές θέσεις συμπίπτουν στις δύο διατάξεις που εξετάζουμε, και επομένως το χρώμα της κενής θέσης παραμένει το ίδιο, για να είναι δυνατή η συγκεκριμένη μετάβαση πρέπει υποχρεωτικά να εμπλέκει μια άρτια μετάθεση (αφού θα είναι σύνθεση άρτιου πλήθους αντιμεταθέσεων) του συνόλου $X = \{1, 2, 3, \dots, 15\}$.

13.1 Θέτουμε $a = (1\ 2)$ και $b = (1\ 3)(4\ 5)$. Παρατηρούμε ότι $o(a) = 2 = o(b)$. Έχουμε επίσης ότι $ab = (1\ 3\ 2)(4\ 5)$ και επομένως $o(ab) = 6$, δίνοντας έτσι την σχέση $ababab = bababa$. Ελέγχοντας ότι τα πιο κάτω 12 γινόμενα μας δίνουν διακεκριμένες μεταθέσεις στην S_5 , συνάγουμε ότι $H = \{(1), a, ab, aba, abab, ababa, ababab, b, ba, bab, baba, babab\}$.

13.2 (i) Χρησιμοποιούμε τις Προτάσεις 12.12 και 12.14: Θεωρούμε την αντιμετάθεση $(i\ j) \in S_n$, όπου $0 \leq i < j \leq n$. Τότε $(i\ j) = (j-1\ j) \dots (i+1\ i+2)(i\ i+1)(i+1\ i+2) \dots (j-1\ j)$. [Για παράδειγμα στην S_8 , έχουμε $(2\ 7) = (6\ 7)(5\ 6)(4\ 5)(3\ 4)(2\ 3)(3\ 4)(4\ 5)(5\ 6)(6\ 7)$.]

13.4 (i) Παρατηρούμε πρώτα ότι $\phi(g^k) = (\phi g)^k$ ισχύει για $k = 0$ και $k = 1$. [Εξήγηση: Για $k = 0$: $\phi(g^0) = \phi(1_G) = 1_H = (\phi g)^0$. Για $k = 1$: $\phi(g^k) = \phi(g) = (\phi g)^1$.] Έστω τώρα $m \geq 1$. Υποθέτουμε ότι $\phi(g^m) = (\phi g)^m$. Έχουμε τότε $\phi(g^{m+1}) = \phi(g^m g) = \phi(g^m)\phi(g) = (\phi g)^m(\phi g) = (\phi g)^{m+1}$. Από το αξίωμα της επαγωγής έχουμε ότι $\phi(g^k) = (\phi g)^k$ για όλα τα $k \in \mathbb{N}$.

Έστω τώρα $k \in \mathbb{Z}$ με $k < 0$. Τότε $k = -r$ για κάποιο $r \in \mathbb{N}$. Έχουμε τότε $\phi(g^k) = \phi(g^{-r}) = \phi((g^{-1})^r) = (\phi(g^{-1}))^r = ((\phi g)^{-1})^r = (\phi g)^{-r} = (\phi g)^k$, (έχουμε χρησιμοποιήσει την Πρόταση 13.5). Συνάγουμε ότι $\phi(g^k) = (\phi g)^k$ για όλα τα $k \in \mathbb{Z}$.

(ii) Έστω $k \in \mathbb{N}$. Παρατηρούμε, αφού ϕ είναι ενριπτικός, ότι $g^k = 1_G$ αν-ν $\phi(g^k) = \phi(1_G) (= 1_H)$ αν-ν $(\phi g)^k = 1_H$. Θέτουμε $S_1 = \{k \in \mathbb{N} : g^k = 1_G\}$ και $S_2 = \{k \in \mathbb{N} : (\phi g)^k = 1_H\}$. Τότε $S_1 = S_2$. Πιο

ειδικά, $S_1 \neq \emptyset$ αν-ν $S_2 \neq \emptyset$, και σε τέτοια περίπτωση τα σύνολα S_1 και S_2 έχουν το ίδιο ελάχιστο στοιχείο. (Έχουμε επίσης ότι $S_1 = \emptyset$ αν-ν $S_2 = \emptyset$). Συνάγουμε ότι τα στοιχεία g και $\phi(g)$ έχουν την ίδια τάξη.

13.6 Η ομάδα $(\mathbb{R} - \{0\}, \cdot)$ δεν περιέχει στοιχεία τάξης 4. [Εξήγηση: Αν $x^4 = 1$ με $x \in \mathbb{R}$, τότε $x \in \{1, -1\}$. Όμως, $o(1) = 1$ και $o(-1) = 2$.] Από την άλλη, η ομάδα $(\mathbb{C} - \{0\}, \cdot)$ περιέχει ακριβώς 2 στοιχεία τάξης 4 (τα i και $-i$). Συγκρίνετε τώρα με την Άσκηση 13.4.

13.7 (i) Δεν είναι ισομορφικές, αφού η $\mathbb{Z}_4$ περιέχει στοιχείο τάξης 4 (το $\bar{1}$), όχι όμως η $\mathbb{Z}_8^*$ (συγκρίνετε με την Άσκηση 12.4(ii)).

(ii) Παρατηρούμε ότι και οι δύο ομάδες είναι κυκλικές τάξης 4. [Έχουμε ότι $\mathbb{Z}_4 = \langle \bar{1} \rangle$ και $\mathbb{Z}_{10}^* = \langle \bar{3} \rangle$.] Είναι τώρα άμεση συνέπεια της Πρότασης 13.12 ότι οι δύο ομάδες είναι ισομορφικές.

13.8 Έστω $\pi, \rho \in S_{10}$. Τότε $\phi(\pi\rho) = \text{sgn}(\pi\rho) = \text{sgn}(\pi)\text{sgn}(\rho) = (\phi\pi)(\phi\rho)$. Έχουμε επίσης ότι $\ker \phi = A_{10}$ και $\text{im } \phi = C_2$.

13.9 Έστω $g \in C_9$ και $h \in C_{13}$ με $o(g) = 9$ και $o(h) = 13$. Τότε $C_9 = \langle g \rangle$, $C_{13} = \langle h \rangle$ και $\phi(g) = h^k$ για κάποιο $k \in \mathbb{Z}$ με $0 \leq k \leq 12$. Έχουμε τότε, $1 = \phi(1) = \phi(g^9) = (\phi g)^9 = (h^k)^9 = h^{9k}$. Έπεται ότι $13|9k$ και επομένως $13|k$ (όπου $0 \leq k \leq 12$), αφού $\text{μκδ}(9, 13) = 1$. Συνάγουμε ότι $k = 0$ και ϕ είναι ο τετριμμένος ομομορφισμός που απεικονίζει όλα τα στοιχεία της C_9 στο 1.

13.10 Θα δείξουμε το εξής αποτέλεσμα: Έστω H, K κυκλικές ομάδες (πεπερασμένης) τάξης m και n αντίστοιχα. Τότε η ομάδα $H \times K$ είναι κυκλική αν-ν $\text{μκδ}(m, n) = 1$. [Συγκρίνετε με την Πρόταση 13.12 — προφανώς $|H \times K| = mn$.]

Υποθέτουμε ότι $H = \langle a \rangle$ και $K = \langle b \rangle$ όπου $a \in H$ με $o(a) = m$ και $b \in K$ με $o(b) = n$.

($\Rightarrow$) Έστω ότι $\text{μκδ}(m, n) = d > 1$. Έστω επίσης $(u, v) \in H \times K$. Τότε $u = a^i$ και $v = b^j$ για κάποια $i, j \in \mathbb{Z}$, και επομένως $u^m = (a^i)^m = 1_H$ και $v^n = (b^j)^n = 1_K$. Επιπλέον $d|m$, $d|n$ και $(u, v)^{mn/d} = (u^{mn/d}, v^{mn/d}) = ((u^m)^{n/d}, (v^n)^{m/d}) = (1_H, 1_K)$. Έπεται ότι $o((u, v)) \leq \frac{mn}{d} < mn$ και επομένως $H \times K$ δεν είναι κυκλική.

($\Leftarrow$) Έστω τώρα ότι $\text{μκδ}(m, n) = 1$. Αρχεί να δείξουμε ότι $o((a, b)) = mn$ (προφανώς $(a, b) \in H \times K$). Παρατηρούμε πρώτα ότι $(a, b)^{mn} = (a^{mn}, b^{mn}) = ((a^m)^n, (b^n)^m) = (1_H, 1_K)$. Επομένως $o((a, b)) | mn$, από την Παρατήρηση 12.28(ii). Θέτουμε $r = o((a, b))$. Έχουμε τότε ότι $(a, b)^r = (1_H, 1_K)$, άρα $(a^r, b^r) = (1_H, 1_K)$. Συνεπώς, $a^r = 1_H$ και $b^r = 1_K$. Έπεται ότι $m|r$ και $n|r$ (πάλι από την Παρατήρηση 12.28(ii)) και, αφού $\text{μκδ}(m, n) = 1$, έχουμε ότι $mn|r$. Συνάγουμε ότι $o((a, b)) = mn$ και επομένως η ομάδα $H \times K$ είναι κυκλική.

13.11 (i) Έστω πρώτα ότι G είναι αβελιανή και ότι $x, y \in G$. Τότε, $\phi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = (\phi x)(\phi y)$ και επομένως ϕ είναι ομομορφισμός. Η συνάρτηση ϕ είναι ενριπτική αφού $\phi(x) = \phi(y) \Rightarrow x^{-1} = y^{-1} \Rightarrow (x^{-1})^{-1} = (y^{-1})^{-1} \Rightarrow x = y$. Είναι επίσης επιρριπτική αφού, για κάθε $y \in G$, έχουμε $y = (y^{-1})^{-1} = \phi(y^{-1})$, όπου $y^{-1} \in G$ (έχουμε ότι G είναι ομάδα και $y \in G$).

Έστω τώρα ότι $\phi \in \text{Aut}(G)$. Αν $x, y \in G$, τότε $x = \phi(x^{-1})$ και $y = \phi(y^{-1})$, όπου $x^{-1}, y^{-1} \in G$. Συνεπώς, $xy = (\phi x^{-1})(\phi y^{-1}) = \phi(x^{-1}y^{-1}) = \phi((yx)^{-1}) = yx$. Άρα G είναι αβελιανή.

(ii) Έστω $K = \langle g \rangle$ κυκλική άπειρης τάξης (όπου $g \in G$), και $\phi \in \text{Aut}(K)$. Τότε $g (= g^1) = \phi(g^s)$ για κάποιο $s \in \mathbb{Z}$, αφού ϕ είναι επιρριπτική και $G = \{g^r : r \in \mathbb{Z}\}$. Έχουμε επίσης ότι $\phi(g) = g^t$ για κάποιο $t \in \mathbb{Z}$. Έπεται ότι $g^1 = \phi(g^s) = (\phi g)^s = (g^t)^s = g^{ts}$. Επομένως $ts = 1$ και $t \in \{-1, 1\}$, αφού οι δυνάμεις g^r , όπου $r \in \mathbb{Z}$, είναι διακεκριμένες από την υπόθεση μας. Και οι δύο αυτές επιλογές για το t μας δίνουν αυτομορφισμούς της G :

$t = 1 : \phi(g^r) = (\phi g)^r = g^r$, η ταυτοτική απεικόνιση από την G στην G ,

$t = -1 : \phi(g^r) = (\phi g)^r = (g^{-1})^r = g^{-r} = (g^r)^{-1}$, είναι πράγματι αυτομορφισμός της G από το τμήμα (i) της άσκησης.

Συμπεραίνουμε ότι $|\text{Aut}(K)| = 2$ και επομένως $\text{Aut}(K) \cong C_2$, αφού $\text{Aut}(K) = \{i, \alpha\}$ με $\alpha = \alpha^{-1}$.

13.12 [Υπενθύμιση. Έστω $f: V \rightarrow W$ ένας $\mathbb{R}$ -ισομορφισμός $\mathbb{R}$ -διανυσματικών χώρων. Έστω επίσης $w_1, w_2 \in W$ και $\lambda \in \mathbb{R}$. Τότε $w_1 = f(v_1)$ και $w_2 = f(v_2)$ για κάποια $v_1, v_2 \in V$. Θέτουμε $g = f^{-1}$. Τότε $g(w_1 + w_2) = g(f(v_1) + f(v_2)) = g(f(v_1 + v_2)) = (g \circ f)(v_1 + v_2) = v_1 + v_2 = f^{-1}(w_1) + f^{-1}(w_2) = g(w_1) + g(w_2)$. Επιπλέον, $g(\lambda w_1) = g(\lambda f(v_1)) = g(f(\lambda v_1)) = (g \circ f)(\lambda v_1) = \lambda v_1 = \lambda f^{-1}(w_1) = \lambda g(w_1)$. Αυτό δείχνει ότι $f^{-1}: W \rightarrow V$ είναι επίσης $\mathbb{R}$ -ισομορφισμός.]

(i) Από μαθήματα γραμμικής άλγεβρας, η σύνθεση δύο $\mathbb{R}$ -ισομορφισμών και η αντίστροφη απεικόνιση ενός $\mathbb{R}$ -ισομορφισμού από το $\mathbb{R}^2$ στο $\mathbb{R}^2$ είναι στοιχεία του $I_{\mathbb{R}}(\mathbb{R}^2)$. Έχουμε επίσης ότι $i_{\mathbb{R}^2} \in I_{\mathbb{R}}(\mathbb{R}^2)$ και $i_{\mathbb{R}^2}$ είναι το ουδέτερο στοιχείο της ομάδας αυτής. (Ο προσεταιρισμός ισχύει στην σύνθεση συναρτήσεων.)

(ii) Έστω $\hat{e} = (e_1, e_2)$ η φυσιολογική διατεταγμένη $\mathbb{R}$ -βάση $((1, 0), (0, 1))$ του $\mathbb{R}^2$. Αν $f \in I_{\mathbb{R}}(\mathbb{R}^2)$, θέτουμε $[f]_{\hat{e}} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(\mathbb{R})$, όπου $f(e_1) = a_{11}e_1 + a_{21}e_2$ και $f(e_2) = a_{12}e_1 + a_{22}e_2$. Έχουμε τότε ότι $[f]_{\hat{e}} \in \text{GL}(2, \mathbb{R})$ για κάθε $f \in I_{\mathbb{R}}(\mathbb{R}^2)$ αφού, στην περίπτωση που f είναι $\mathbb{R}$ -ισομορφισμός, τα διανύσματα $f(e_1), f(e_2)$ είναι $\mathbb{R}$ -γραμμικά ανεξάρτητα. Θέτουμε $\psi: I_{\mathbb{R}}(\mathbb{R}^2) \rightarrow \text{GL}(2, \mathbb{R}) : f \mapsto [f]_{\hat{e}}$, ($f \in I_{\mathbb{R}}(\mathbb{R}^2)$). Και πάλι από τα μαθήματα γραμμικής άλγεβρας έχουμε ότι $\psi(g \circ f) = [g]_{\hat{e}}[f]_{\hat{e}}$, και επομένως ψ είναι ομομορφισμός ομάδων. Επιπλέον η συνάρτηση ψ είναι αμφιμονοσήμαντη. Από την Πρόταση 11.10, συγκρίνετε επίσης με την Άσκηση 12.11(c), έχουμε ότι η ομάδα $O(2, \mathbb{R})$ αποτελείται ακριβώς από όλους τους πίνακες της μορφής A_{ϕ}, B_{ϕ} όπου $\phi \in \mathbb{R}$ με $0 \leq \phi < 2\pi$. Όμως, με ϕ όπως προηγούμενως, έχουμε ότι $\text{rot}_{\phi}, \text{ref}_{\phi} \in I_{\mathbb{R}}(\mathbb{R}^2)$ όπου $\psi(\text{rot}_{\phi}) = A_{\phi}$ και $\psi(\text{ref}_{\phi}) = B_{\phi}$.

13.13 Για κάθε $f \in D_{2n}$, ορίζουμε $\hat{f}: X \rightarrow X$ με $\hat{f}(\kappa) = f(\kappa)$, ($\kappa \in X$). Από το Παράδειγμα 12.23, έχουμε ότι $\hat{f}$ είναι καλά ορισμένη και ότι $\hat{f}$ είναι μια μετάθεση του X . Προφανώς, $\text{Sym}(X) \cong S_n$. Θέτουμε $\chi: D_{2n} \rightarrow \text{Sym}(X) : f \mapsto \hat{f}$, ($f \in D_{2n}$). Έστω τώρα $f, g \in D_{2n}$. Τότε $\chi(g \circ f) = h$ για κάποιο $h \in \text{Sym}(X)$. Αν $\kappa \in X$, τότε $h(\kappa) = (g \circ f)(\kappa) = g(f(\kappa))$, άρα $h(\kappa) = \hat{g}(\hat{f}(\kappa)) = (\hat{g} \circ \hat{f})(\kappa)$. Συμπεραίνουμε ότι $\chi(g \circ f) = \hat{g} \circ \hat{f} = (\chi g) \circ (\chi f)$, άρα χ είναι ομομορφισμός ομάδων. Επιπλέον, αν $\chi(f) = \chi(g)$, έχουμε ότι $f(\kappa) = g(\kappa)$ για κάθε $\kappa \in X$ και επομένως $f = g$ και πάλι από το Παράδειγμα 12.23. Έπεται ότι ο ομομορφισμός ομάδων χ είναι ενριπτικός.

13.14 Χρησιμοποιώντας την τρίτη σχέση, βλέπουμε ότι κάθε στοιχείο της H μπορεί να εκφραστεί στην μορφή $A^i B^j$ για κάποια $i, j \in \mathbb{Z}$. Χρησιμοποιώντας τώρα τις πρώτες δύο σχέσεις, προκύπτει ότι είναι αρκετό να περιοριστούμε στις τιμές $0 \leq i \leq 3$ και $0 \leq j \leq 1$. Συνεπώς $|H| \leq 8$. Αφού όμως οι πίνακες $A^i B^j$ ($0 \leq i \leq 3, 0 \leq j \leq 1$) είναι διακεκριμένοι, συνάγουμε ότι $|H| = 8$.

Παρατηρούμε ότι H έχει ακριβώς 1 στοιχείο τάξης 2 ενώ η D_8 έχει ακριβώς 5 στοιχεία τάξης 2. [Το στοιχείο $A^2 \left(= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right)$ είναι το μόνο στοιχείο της υποομάδας $\langle A \rangle$ της H που έχει τάξη 2. Έστω τώρα $C \in \{A^i B : 0 \leq i \leq 3\}$. Τότε $C^2 = A^i B A^i B = A^i A^{-i} B B = B^2 = A^2$, και επομένως $\text{o}(C) \neq 2$. Στην πραγματικότητα $\text{o}(C) = 4$, αφού $C^4 = I_2$ και $\text{o}(C) \notin \{1, 2\}$.] Επομένως $Q_8 \not\cong D_8$.

13.15 Θέτουμε $S_3 = \{\alpha_i : 1 \leq i \leq 6\}$, όπου $\alpha_1 = (1)$, $\alpha_2 = (1\ 2)$, $\alpha_3 = (1\ 3)$, $\alpha_4 = (2\ 3)$, $\alpha_5 = (1\ 2\ 3)$ και $\alpha_6 = (1\ 3\ 2)$. Έστω επίσης ϕ η αριστερή κανονική αναπαράσταση της S_3 . Τότε

$$\begin{aligned} \phi(\alpha_1) &= (\alpha_1)(\alpha_2)(\alpha_3)(\alpha_4)(\alpha_5)(\alpha_6), & \phi(\alpha_2) &= (\alpha_1\ \alpha_2)(\alpha_3\ \alpha_6)(\alpha_4\ \alpha_5), \\ \phi(\alpha_3) &= (\alpha_1\ \alpha_3)(\alpha_2\ \alpha_5)(\alpha_4\ \alpha_6), & \phi(\alpha_4) &= (\alpha_1\ \alpha_4)(\alpha_2\ \alpha_6)(\alpha_3\ \alpha_5), \\ \phi(\alpha_5) &= (\alpha_1\ \alpha_5\ \alpha_6)(\alpha_2\ \alpha_3\ \alpha_4), & \phi(\alpha_6) &= (\alpha_1\ \alpha_6\ \alpha_5)(\alpha_2\ \alpha_4\ \alpha_3). \end{aligned}$$

14.1 (i) Έστω $a, b, c \in G$. Έχουμε τότε

$$(1) aa^{-1} = 1_G \in H, \text{ άρα } (a, a) \in R.$$

$$(2) (a, b) \in R \Rightarrow ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} \in H \text{ (αφού } H \leq G) \Rightarrow ba^{-1} \in H \Rightarrow (b, a) \in R.$$

$$(3) (a, b) \in R \text{ και } (b, c) \in R \Rightarrow ab^{-1}, bc^{-1} \in H \Rightarrow ac^{-1} (= ab^{-1}bc^{-1}) \in H \text{ (αφού } H \leq G) \Rightarrow (a, c) \in R.$$

Αν $x \in G$, τότε $\bar{x} = \{y \in G: (y, x) \in R\} = \{y \in G: yx^{-1} \in H\} = \{y \in G: y \in Hx\}$. [Για την τελευταία ισότητα έχουμε χρησιμοποιήσει την Πρόταση 14.8.] Επομένως οι αντίστοιχες κλάσεις ισοδυναμίας είναι ακριβώς τα δεξιά σύμπλοκα της H στην G .

(ii) Θέτουμε $G = C_{12}$ και $H = C_4$. Προφανώς $H \leq G$. Έχουμε επίσης ότι $G = \langle \omega \rangle$ και $H = \langle \omega^3 \rangle = \{1, \omega^3, \omega^6, \omega^9\}$ όπου $\omega = \cos(\frac{2\pi}{12}) + i \sin(\frac{2\pi}{12}) \in \mathbb{C}$. [Ελέγξτε ότι $o(\omega) = 12$ και $o(\omega^3) = 4$.] Οι αντίστοιχες κλάσεις ισοδυναμίας είναι τα δεξιά σύμπλοκα της H στην G (που στην περίπτωση αυτή συμπίπτουν με τα αριστερά σύμπλοκα της H στην G αφού G είναι αβελιανή):

$$\begin{aligned} H1 &= \{1, \omega^3, \omega^6, \omega^9\} = H\omega^3 = H\omega^6 = H\omega^9, \\ H\omega &= \{\omega, \omega^4, \omega^7, \omega^{10}\} = H\omega^4 = H\omega^7 = H\omega^{10} \\ H\omega^2 &= \{\omega^2, \omega^5, \omega^8, \omega^{11}\} = H\omega^5 = H\omega^8 = H\omega^{11}. \end{aligned}$$

14.2 (i) Από το Πρόσχημα 12.13, αν $x, y \in S_n$ είναι συζυγή, τότε x, y έχουν τον ίδιο τύπο κύκλων.

Υποθέτουμε τώρα ότι $x, y \in S_n$ και x, y έχουν τον ίδιο τύπο κύκλων. Έστω $\pi_1 \dots \pi_r$ και $\rho_1 \dots \rho_r$ οι πλήρεις παραγοντοποιήσεις των x, y ως γινόμενα κύκλων ξένων μεταξύ τους, όπου μήκος $\pi_i \geq \text{μήκος } \pi_{i+1}$ και μήκος $\rho_i \geq \text{μήκος } \rho_{i+1}$ για όλα τα i με $1 \leq i \leq r$. Έχουμε τότε, για κάθε i , ότι ο κύκλος π_i έχει το ίδιο μήκος με τον κύκλο ρ_i (δηλαδή π_i είναι ένας $k(i)$ -κύκλος αν-ν ρ_i είναι ένας $k(i)$ -κύκλος). Συνοψίζοντας, έχουμε διευθετήσει της πλήρεις παραγοντοποιήσεις για τις μεταθέσεις x, y στην μορφή $x = (a_1 \dots a_{k(1)}) \dots (c_1 \dots c_{k(r)})$ και $y = (a'_1 \dots a'_{k(1)}) \dots (c'_1 \dots c'_{k(r)})$. Παρατηρούμε ότι υπάρχει $g \in S_n$ με $g(a_1) = a'_1, \dots, g(c_{k(r)}) = c'_{k(r)}$, και επομένως $gxg^{-1} = g(a_1 \dots a_{k(1)})g^{-1} \dots g(c_1 \dots c_{k(r)})g^{-1} = (g(a_1) \dots g(a_{k(1)})) \dots (g(c_1) \dots g(c_{k(r)})) = y$.

(ii) Από το τμήμα (i), στην S_4 έχουμε τις εξής κλάσεις συζυγίας (ακριβώς μια για κάθε τύπο κύκλων)

$$\begin{array}{c} \text{αντιπρόσωπος} \\ \text{πλήθος στοιχείων} \end{array} \quad \left| \begin{array}{c} (1 \ 2 \ 3 \ 4) \\ 6 \end{array} \right| \left| \begin{array}{c} (1 \ 2 \ 3)(4) \\ 8 \end{array} \right| \left| \begin{array}{c} (1 \ 2)(3 \ 4) \\ 3 \end{array} \right| \left| \begin{array}{c} (1 \ 2)(3)(4) \\ 6 \end{array} \right| \left| \begin{array}{c} (1)(2)(3)(4) \\ 1 \end{array} \right|$$

Παρατηρούμε πρώτα ότι οι υποομάδες $\{1\}$, V_4 , A_4 και S_4 της S_4 είναι όλες κανονικές υποομάδες, αφού αποτελούνται όλες από την ένωση κλάσεων συζυγίας. Έστω τώρα N μια τυχαία κανονική υποομάδα της S_4 . Τότε $(1) \in N$, $|N| \mid 24$ και N είναι ένωση κλάσεων συζυγίας. Όμως τα μόνα αθροίσματα από τον κατάλογο αριθμών 1, 3, 6, 6, 8 τα οποία περιέχουν το 1 και είναι διαιρέτες του 24 είναι τα εξής: 1, 1 + 3, 1 + 3 + 8, 1 + 3 + 6 + 6 + 8. Συνάγουμε ότι $\{1\}$, V_4 , A_4 , S_4 είναι οι μόνες κανονικές υποομάδες της S_4 .

14.3 (14.22)(i) Έστω G ομάδα και $H \leq G$ με $[G: H] = 2$. Αν $g \in H$, τότε $gH = H = Hg$. Αν $g \in G - H$, τότε $G = H \cup Hg = H \cup gH$ με $H \cap Hg = \emptyset$ και $H \cap gH = \emptyset$ (υπάρχουν ακριβώς 2 διακεκριμένα δεξιά και 2 διακεκριμένα αριστερά σύμπλοκα της H στην G). Έπεται ότι $Hg = G - H = gH$. Έχουμε δείξει ότι $Hg = gH$ για όλα τα $g \in G$. Το αποτέλεσμα είναι άμεση συνέπεια της Πρότασης 14.17.

(14.22)(iii) Έστω $n \geq 2$. Θέτουμε $P = \{\pi \in S_n: \pi \text{ είναι περιττή}\}$. Αν $\sigma \in P$, τότε $\sigma = (1 \ 2)(1 \ 2)\sigma \in (1 \ 2)A_n$, αφού $(1 \ 2)\sigma \in A_n$. Έπεται ότι $P \subseteq (1 \ 2)A_n$. Προφανώς $(1 \ 2)A_n \subseteq P$.

(14.22)(iv) Από την Πρόταση 13.6, ξέρουμε ότι $\ker \theta \leq G$. Έστω τώρα $g \in G$ και $h \in \ker \theta$. Έχουμε τότε $\phi(g^{-1}hg) = \phi(g^{-1})\phi(h)\phi(g) = (\phi g)^{-1}1_H\phi(g) = 1_H$. Άρα $g^{-1}hg \in \ker \theta$.

(14.25)(ii) Παρατηρούμε ότι $V_4 \subseteq A_4 \subseteq S_4$. Έστω τώρα $\pi \in V_4$. Έχουμε τότε ότι $g^{-1}\pi g \in V_4$ οποτεδήποτε $g \in S_4$ (και επομένως οποτεδήποτε $g \in A_4$) από την Άσκηση 14.2.

(a) Το σύνολο $\{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ (αντίστοιχα, $\{(1), (1\ 2)\}$) αποτελεί ένα σύστημα δεξιών αντιπροσώπων της V_4 στην A_4 (αντίστοιχα, της A_4 στην S_4). Έπεται ότι το υποσύνολο $\{(1), (1\ 2), (1\ 2\ 3), (1\ 2\ 3)(1\ 2) (= (1\ 3)), (1\ 3\ 2), (1\ 3\ 2)(1\ 2) (= (2\ 3))\}$ της S_4 αποτελεί ένα σύστημα δεξιών αντιπροσώπων της V_4 στην S_4 .

(14.30)(iv) Θέτουμε $\phi: \text{GL}(n, \mathbb{R}) \rightarrow \mathbb{R}^*: m \mapsto \det(m)$, $m \in \text{GL}(n, \mathbb{R})$. [Η συνάρτηση ϕ είναι καλά ορισμένη αφού κάθε αντιστρέψιμος τετραγωνικός πίνακας με συντελεστές από το $\mathbb{R}$ έχει μη-μηδενική ορίζουσα, η οποία είναι ένας πραγματικός αριθμός.]

Έστω τώρα $m_1, m_2 \in \text{GL}(n, \mathbb{R})$. Τότε $\phi(m_1 m_2) = \det(m_1 m_2) = (\det m_1)(\det m_2) = (\phi m_1)(\phi m_2)$, συνεπώς ϕ είναι ομομορφισμός ομάδων. Τώρα αν $\alpha \in \mathbb{R}^*$ τότε $\alpha = \phi(m_\alpha)$ όπου m_α είναι ο διαγώνιος πίνακας $D(\alpha, 1, \dots, 1)$. Προφανώς ο πίνακας m_α είναι αντιστρέψιμος, αφού $\det(m_\alpha) = \alpha (\neq 0)$. Επομένως ϕ είναι επιρριπτικός. Τέλος, παρατηρούμε ότι $\ker \phi = \{m \in \text{GL}(n, \mathbb{R}): \phi(m) = 1\} = \{m \in \text{GL}(n, \mathbb{R}): \det(m) = 1\} = \text{SL}(n, \mathbb{R})$.

14.4 Από την υπόθεση, $H \triangleleft G$ και επομένως $K = G/H$ είναι μια ομάδα τάξης 2. Έπεται ότι, $h^2 = 1_K$ για όλα τα $h \in K$. Πιο ειδικά, $(gH)^2 = 1_K (= 1_G H)$. Όμως $(gH)^2 = g^2 H$, άρα $g^2 H = 1_G H$. Συνάγουμε ότι $g^2 \in H$.

14.5 Παρατηρούμε πρώτα ότι $(g_1, \dots, g_p) \in L \Rightarrow g_1 g_2 \dots g_p = 1_G \Rightarrow g_2 \dots g_p = g_1^{-1} \Rightarrow g_2 \dots g_p g_1 = 1_G \Rightarrow (g_2, \dots, g_p, g_1) \in L \Rightarrow \pi(g_1, \dots, g_p) \in L$. Συνεπώς π είναι πράγματι μια συνάρτηση από το L στο L . Επιπλέον, αν $(x_1, \dots, x_p) \in L$, τότε $(x_p, x_1, \dots, x_{p-1}) \in L$ αφού $x_1 \dots x_{p-1} = x_p^{-1}$. Όμως $(x_1, \dots, x_p) = \pi(x_p, x_1, \dots, x_{p-1})$ άρα π είναι επιρριπτική, και αφού L είναι πεπερασμένο σύνολο συμπεραίνουμε ότι π είναι αμφιμονοσήμαντη. Έχουμε δηλαδή ότι $\pi \in \text{Sym}(L)$. Επιπλέον, ο $(\pi)|_p$ θεωρώντας την π ως στοιχείο της ομάδας $\text{Sym}(L)$, αφού $\pi^p = i_L$.

(i), (ii): Αν $g^p = 1_G$, όπου $g \in G$, τότε προφανώς $(g, g, \dots, g) \in L$ και το στοιχείο αυτό σταθεροποιείται από την L . Αντίστροφα, αν $x = (x_1, \dots, x_p) \in L$ και $\pi(x) = x$, έχουμε ότι $(x_1, x_2, \dots, x_{p-1}, x_p) = (x_2, x_3, \dots, x_p, x_1)$, συνεπώς $x_1 = x_2 = x_3 = \dots = x_{p-1} = x_p = h$ για κάποιο $h \in G$ (έχουμε, δηλαδή, $x = (h, h, \dots, h)$ όπου $h^p = 1_G$). Συμπεραίνουμε, αφού p είναι πρώτος, ότι τα στοιχεία του συνόλου L που σταθεροποιούνται από την π είναι το $(1_G, 1_G, \dots, 1_G)$ και όλα τα στοιχεία της μορφής $(g, g, \dots, g)$ με $o(g) = p$. Θεωρώντας τώρα μια πλήρη παραγοντοποίηση της π ως γινόμενο κύκλων ξένων μεταξύ τους και παρεμβάλλοντας την Άσκηση 12.14 συμπεραίνουμε, αφού $o(\pi)|_p$, ότι τα υπόλοιπα στοιχεία του συνόλου L (αν υπάρχουν τέτοια) περιέχονται σε p -κύκλους. [Σημείωση: Στην ειδική περίπτωση που $|G| = 2 = p$, τότε G είναι κυκλική, άρα $G = \langle g \rangle$ για κάποιο $g \in G$ με $o(g) = 2$. Έχουμε τότε ότι $L = \{(1_G, 1_G), (g, g)\}$ και $\pi = i_L$.]

(iii) Για να βρούμε το πλήθος των p -άδων του συνόλου G^p που ανήκουν στο σύνολο L παρατηρούμε ότι σε κάθε μια από τις πρώτες $p-1$ θέσεις μιας τέτοιας p -άδας μπορούμε να τοποθετήσουμε τυχαίο στοιχείο της G , όμως από την στιγμή που έχει γίνει η επιλογή για τις πρώτες $p-1$ θέσεις, η τελευταία θέση καθορίζεται με μοναδικό τρόπο. Συνεπώς $|L| = |G|^{p-1}$. Έστω τώρα s το πλήθος των στοιχείων του L που σταθεροποιούνται από την π . Τότε $s \geq 1$, αφού $(1_G, 1_G, \dots, 1_G) \in L$.

Έχουμε επίσης ότι $|L| (= |G|^{p-1}) = s + kp$ για κάποιο $k \in \mathbb{N} \cup \{0\}$, από το τμήμα (ii), αφού τα υπόλοιπα στοιχεία του L περιέχονται σε p -κύκλους. Όμως $p \nmid |G|$ και επομένως $p \nmid |L|$. Συνάγουμε ότι $p|s$ και επομένως $s \geq p$ αφού $s \geq 1$. Από το τμήμα (ii), προκύπτει τώρα άμεσα ότι υπάρχει $g \in G$ με $o(g) = p$.

14.6 (i) Έχουμε ότι $\{a, c\} \subseteq D_{12}$ αφού και το a και το c αποτελούν συμμετρίες του κανονικού εξαγώνου. Παρατηρούμε επίσης ότι $ac = \text{rot}_{\pi/3} \text{ref}_{\pi/3} = \text{ref}_{2\pi/3} = \text{ref}_{\pi/3} \text{rot}_{-\pi/3} = ca^{-1}$. Έπεται ότι $a^k c = ca^{-k}$ για κάθε $k \in \mathbb{Z}$. Έχουμε επίσης ότι $o(a) = 6$ και $o(c) = 2$, επομένως κάθε στοιχείο της $\langle a, c \rangle$ μπορεί να εκφραστεί στην μορφή $a^i c^j$ όπου $0 \leq i \leq 5$ και $0 \leq j \leq 1$. Αν τώρα $m, i \in \mathbb{Z}$ με $0 \leq m, i \leq 5$,

έχουμε $(a^i)^{-1}a^ma^i = a^m$ και $(a^ic)^{-1}a^m(a^ic) = c^{-1}a^{-i}a^ma^ic = c^{-1}a^mc = ca^mc = a^{-m}c^2 = a^{-m} \in \langle a \rangle$. Συνάγουμε ότι $\langle a \rangle \triangleleft \langle a, c \rangle$.

(ii) Από το Παράδειγμα 13.3(ii), έχουμε ότι $D_{12} = \langle \text{rot}_{\pi/3}, \text{ref}_0 \rangle$. Έχουμε επίσης ότι $\{\text{rot}_{\pi/3}, \text{ref}_{\pi/3}\} \subseteq D_{12}$ και επομένως $\langle \text{rot}_{\pi/3}, \text{ref}_{\pi/3} \rangle \leq D_{12}$. Από την άλλη $\{\text{rot}_{\pi/3}, \text{ref}_0\} \subseteq \langle \text{rot}_{\pi/3}, \text{ref}_{\pi/3} \rangle$, αφού $\text{ref}_0 = \text{ref}_{\pi/3} \circ \text{rot}_{\pi/3} \in \langle \text{rot}_{\pi/3}, \text{ref}_{\pi/3} \rangle$. Συνάγουμε ότι $D_{12} (= \langle \text{rot}_{\pi/3}, \text{ref}_0 \rangle) \leq \langle \text{rot}_{\pi/3}, \text{ref}_{\pi/3} \rangle$ και επομένως $D_{12} = \langle \text{rot}_{\pi/3}, \text{ref}_{\pi/3} \rangle$.

Έχουμε ότι $|D_{12}| = 12$ (κοιτάζτε το Παράδειγμα 12.23 και τον ορισμό που το ακολουθεί). Προφανώς $\langle a \rangle = \{a^k : 0 \leq k \leq 5\}$, άρα $|\langle a \rangle| = 6 (= o(a))$. Συνεπώς υπάρχουν ακριβώς δύο σύμπλοκα της $\langle a \rangle$ στην D_{12} . Παρατηρούμε επίσης ότι $c \notin \langle a \rangle$, συγκρίνετε με την συζήτηση στο Παράδειγμα 13.3(ii). Έπεται ότι $D_{12} = \langle a \rangle \cup \langle a \rangle c = \langle a \rangle \cup c\langle a \rangle$. [Βλέπουμε για ακόμη μια φορά ότι $\langle a \rangle \triangleleft D_{12}$ αφού $[D_{12} : \langle a \rangle] = 2$.]

(iii) Θέτουμε $x = \text{ref}_{\pi/3}$ και $y = \text{ref}_0$. Τότε $\{x, y\} \subseteq D_{12}$ και επομένως $\langle x, y \rangle \leq D_{12}$. Από την άλλη, $xy = \text{ref}_{\pi/3} \circ \text{ref}_0 = \text{rot}_{\pi/3}$ και επομένως $\{\text{rot}_{\pi/3}, \text{ref}_0\} \subseteq \langle x, y \rangle$. Έπεται ότι $D_{12} \leq \langle x, y \rangle$.

14.7 Θέτουμε $X = \{1, 2, 3, 4, 5, 6\}$. Παρατηρούμε ότι $o(\alpha) = 6$, $o(\beta) = 2$ άρα $\alpha^6 = i_X = \beta^2$. Έχουμε επίσης ότι $\alpha\beta = (1 \ 2 \ 3 \ 4 \ 5 \ 6)(2 \ 6)(3 \ 5) = (1 \ 2)(3 \ 6)(4 \ 5)$ και $\beta\alpha^{-1} = (2 \ 6)(3 \ 5)(6 \ 5 \ 4 \ 3 \ 2 \ 1) = (1 \ 2)(3 \ 6)(4 \ 5) = \alpha\beta$.

Ισχυρισμός. Ισχύει ότι $|H_1| = 12$ και $H_1 = \{\alpha^i\beta^j : 0 \leq i \leq 5, 0 \leq j \leq 1\}$.

Απόδειξη ισχυρισμού. Παρατηρούμε πρώτα ότι για $1 \leq i \leq 5$ έχουμε $\alpha^i(1) = i+1$ και επομένως $\beta \notin \langle \alpha \rangle = \{i_X, \alpha, \alpha^2, \dots, \alpha^5\}$. Συνεπώς, υπάρχουν τουλάχιστον δύο διακεκριμένα δεξιά σύμπλοκα της $\langle \alpha \rangle$ στην H_1 , τα $\langle \alpha \rangle$ και $\langle \alpha \rangle\beta$. Έπεται ότι $|H_1| \geq 12$. Χρησιμοποιώντας τώρα την σχέση $\alpha\beta = \beta\alpha^{-1}$, βλέπουμε ότι $\beta\alpha^r = \alpha^{-r}\beta$ για όλα τα $r \in \mathbb{Z}$ (συγκρίνετε με το Παράδειγμα 13.3). Συμπεραίνουμε ότι κάθε στοιχείο της H_1 μπορεί να εκφραστεί στην μορφή $\alpha^l\beta^m$, για κάποια $l, m \in \mathbb{Z}$. Από τις σχέσεις $\alpha^6 = i_X = \beta^2$, προκύπτει ότι $H_1 = \{\alpha^i\beta^j : 0 \leq i \leq 5, 0 \leq j \leq 1\}$ και επομένως $|H_1| \leq 12$. Συνάγουμε ότι $|H_1| = 12$ και ότι τα στοιχεία $\alpha^i\beta^j$ της S_6 , όπου $0 \leq i \leq 5$ και $0 \leq j \leq 1$, πρέπει υποχρεωτικά να είναι διακεκριμένα (χάτι που μπορούμε να επαληθεύσουμε υπολογίζοντας τα 12 αυτά γινόμενα μεταθέσεων). Άμεση συνέπεια της πιο πάνω συζήτησης είναι ότι $H_1 = \langle \alpha \rangle \cup \langle \alpha \rangle\beta = \langle \alpha \rangle \cup \beta\langle \alpha \rangle$.

(ii) Διατηρούμε τον συμβολισμό από το Παράδειγμα 13.3(ii), και ορίζουμε $\phi : D_{12} \rightarrow H_1 : a^ib^j \mapsto \alpha^i\beta^j$ ($0 \leq i \leq 5, 0 \leq j \leq 1$). Από τα πιο πάνω, η συνάρτηση ϕ είναι αμφιμονοσήμαντη. Επιπλέον, ϕ είναι ομομορφισμός ομάδων. [Εξήγηση: Στην H_1 ισχύουν οι σχέσεις $\alpha^6 = i_X, \beta^2 = i_X$ και $\alpha\beta = \beta\alpha^{-1}$, συγκρίνετε τώρα με το Παράδειγμα 13.7.]

Ερώτηση: Υπάρχει κάποια σχέση μεταξύ του ομομορφισμού ϕ που έχουμε ορίσει εδώ με τον ενριπτικό ομομορφισμό ομάδων χ στην λύση της Άσκησης 13.13;

(iii) Υπόδειξη: Ελέγξτε, χρησιμοποιώντας την σχέση $\beta(\alpha^2)^r = (\alpha^2)^{-r}\beta$ για όλα τα $r \in \mathbb{Z}$, ότι $H_2 = \{i_X, \alpha^2, \alpha^4, \beta, \alpha^2\beta, \alpha^4\beta\}$ και ότι η συνάρτηση $\theta : D_{12} \rightarrow H_2 : a^ib^j \mapsto (\alpha^2)^i\beta^j$, ($0 \leq i \leq 5, 0 \leq j \leq 1$) είναι ένας επιρριπτικός ομομορφισμός ομάδων. [Για το τελευταίο ελέγξτε, θέτοντας $x = \alpha^2, y = \beta$, ότι ισχύουν οι σχέσεις $x^6 = i_X, y^2 = i_X$ και $xy = yx^{-1}$. Συγκρίνετε και πάλι με το Παράδειγμα 13.7.]

14.8 (i) Έστω $k \in \mathbb{N}$. Παρατηρούμε πρώτα ότι $x^k = 1_G$ αν-ν $(x^k)^{-1} = 1_G$ αν-ν $x^{-k} = 1_G$ αν-ν $(x^{-1})^k = 1_G$. Έχουμε επίσης, $(y^{-1}xy)^k = y^{-1}x^ky$, αφού $(y^{-1}xy)^k = (y^{-1}xy)(y^{-1}xy) \dots (y^{-1}xy)$, k φορές. Έπεται ότι $x^k = 1_G$ αν-ν $y^{-1}x^ky = 1_G$ αν-ν $(y^{-1}xy)^k = 1_G$. [Εναλλακτικά, ελέγξτε ότι η συνάρτηση $\phi : G \rightarrow G : g \mapsto y^{-1}gy$, ($g \in G$) είναι ένας αυτομορφισμός της G .]

(ii) Από το τμήμα (i), τα στοιχεία yx και $y^{-1}(yx)y (= xy)$ έχουν την ίδια τάξη.

14.9 Αν $|G| = 1$, τότε $G \cong C_1$. Επιπλέον, αν $|G| = p$ όπου p πρώτος, τότε $G \cong C_p$ (κοιτάζτε το Πρόγραμμα 14.12 και την Πρόταση 13.12). Απομένει να εξετάσουμε τις περιπτώσεις $|G| \in \{4, 6, 10\}$.

Περίπτωση $|G| = 4$: Αν G είναι κυκλική, τότε $G \cong C_4 (\cong (\mathbb{Z}_4, +))$. Έστω τώρα ότι G δεν είναι κυκλική. Αφού στην G δεν υπάρχει στοιχείο τάξης 4, το θεώρημα Lagrange μας εξασφαλίζει ότι $g^2 = 1_G$ για όλα

τα $g \in G$, και επομένως η ομάδα G είναι αβελιανή (Άσκηση 12.3). Έστω $a, b \in G - \{1_G\}$ με $a \neq b$. Τότε $o(a) = 2$ και $[G : \langle a \rangle] = 2$. Τώρα $b \notin \langle a \rangle = \{1_G, a\}$, συνεπώς $G = \langle a \rangle \cup \langle a \rangle b = \{1_G, a, b, ab\} (= \langle a, b \rangle)$, όπου $ab = ba$ και $o(a) = 2 = o(b)$. Παρατηρούμε ότι υπάρχει τέτοια ομάδα G , αφού η ομάδα Klein πληροί όλες τις πιο πάνω προϋποθέσεις. Τέλος, ελέγξτε ότι η συνάρτηση $\phi: C_2 \times C_2 \rightarrow G : (1, -1)^i (-1, 1)^j \mapsto a^i b^j$, ($0 \leq i, j \leq 1$) είναι ισομορφισμός ομάδων, συγκρίνετε με το Παράδειγμα 13.7. (Θέτοντας $\rho = (1, -1)$ και $\sigma = (-1, 1)$ παρατηρούμε ότι οι σχέσεις $\rho^2 = (1, 1) = \sigma^2$ και $\rho\sigma = \sigma\rho$ καθορίζουν πλήρως τον πίνακα πολλαπλασιασμού της $C_2 \times C_2$.) Συνάγουμε ότι $G \cong C_2 \times C_2$ αν G δεν είναι κυκλική.

Περίπτωση $|G| = 6$: Αν G είναι κυκλική, τότε $G \cong C_6$. Έστω τώρα ότι G δεν είναι κυκλική. Αφού $2|6$ και $3|6$, το θεώρημα Cauchy μας εξασφαλίζει ότι υπάρχουν $a, b \in G$ με $o(a) = 3$ και $o(b) = 2$. Έχουμε τότε ότι $\langle a \rangle \cap \langle b \rangle = \{1_G\}$ από το θεώρημα Lagrange, αφού η τάξη της υποομάδας $\langle a \rangle \cap \langle b \rangle$ της G διαιρεί και το 2 και το 3, και επομένως τον $\mu\delta(2, 3)$. Έπεται ότι $b \notin \langle a \rangle$, και επομένως $G = \langle a \rangle \cup \langle a \rangle b$, με $\langle a \rangle \cap \langle a \rangle b = \emptyset$ και $\langle a \rangle \triangleleft G$. Επιπλέον, ισχύει ότι $ab \neq ba$. [Εξήγηση για τον τελευταίο ισχυρισμό: Αν $ab = ba$, παρεμβάλλοντας την Άσκηση 12.14, θα είχαμε ότι $o(ab) = \text{εκπ}(3, 2) = 6$ και επομένως $G (= \langle ab \rangle)$ είναι κυκλική, που είναι άτοπο.]

Σχόλιο: Η ομάδα S_3 (με $a = (1\ 2\ 3)$, $b = (2\ 3)$) πληροί όλες τις πιο πάνω προϋποθέσεις.

Τώρα $b^{-1}ab \in \langle a \rangle$ αφού $\langle a \rangle \triangleleft G$. Έπεται ότι $b^{-1}ab = a^{-1} (= a^2)$. [Εξήγηση: Έχουμε ότι $b^{-1}ab = a^i$ για κάποιο $i \in \{0, 1, 2\}$. Αν $i = 0$, τότε $b^{-1}ab = 1_G$ ή, ισοδύναμα, $a = 1_G$ που είναι άτοπο. Παρόμοια από $b^{-1}ab = a$ προκύπτει ότι $ab = ba$, που πάλι είναι άτοπο.] Τέλος, θέτοντας $\rho = \text{rot}_{2\pi/3}$ και $\sigma = \text{ref}_0$, ελέγξτε ότι η συνάρτηση $\theta: D_6 \rightarrow G : \rho^i \sigma^j \mapsto a^i b^j$, ($0 \leq i \leq 2$, $0 \leq j \leq 1$) είναι ισομορφισμός ομάδων. Συνάγουμε ότι $G \cong D_6$ στην περίπτωση που η ομάδα G δεν είναι κυκλική.

Περίπτωση $|G| = 10$: Από το θεώρημα Cauchy υπάρχουν στοιχεία $a, b \in G$ με $o(a) = 5$ και $o(b) = 2$. Έχουμε τότε ότι $[G : \langle a \rangle] = 2$ και επομένως $\langle a \rangle \triangleleft G$. Επίσης $b \notin \langle a \rangle$ αφού $o(b) \nmid 5$, άρα $G = \langle a \rangle \cup \langle a \rangle b$ και $G = \langle a, b \rangle$. Αφού $\langle a \rangle \triangleleft G$ έχουμε ότι $b^{-1}ab \in \langle a \rangle$ και, αφού $o(a) = o(bab^{-1})$, έχουμε ότι $b^{-1}ab = a^r$ για κάποιο $r \in \mathbb{N}$ με $1 \leq r \leq 4$. Όμως $a = b^2ab^2 = b^{-2}ab^2 = b^{-1}b^{-1}abb = b^{-1}a^r b = (b^{-1}ab)^r = (a^r)^r = a^{r^2}$. Συμπεραίνουμε ότι $a^{r^2-1} = 1_G$ και επομένως $5|(r+1)(r-1)$. Συνοψίζοντας, έχουμε ότι $b^{-1}ab = a^r$ για κάποιο $r \in \mathbb{N}$ με $1 \leq r \leq 4$ και όπου $5|(r+1)$ ή $5|(r-1)$.

Περίπτωση $5|(r-1)$: Τότε $r = 1$ και ισχύει $ab = ba$. Όμως $ab \in G$ και $o(ab) = 10$ (Άσκηση Άσκηση 12.14). Συνεπώς $G \cong C_{10}$ στην περίπτωση αυτή.

Περίπτωση $5|(r+1)$: Τότε $r = 4$ και $b^{-1}ab = a^4 (= a^{-1})$ ή, ισοδύναμα, $ab = ba^{-1}$. Μπορούμε τώρα να δείξουμε ότι $G \cong D_{10}$ (συγκρίνετε με το Παράδειγμα 13.7).

14.14 Έστω πρώτα ότι $HK \leq G$. Αν $x \in HK$, τότε $x^{-1} \in HK$, άρα $x^{-1} = hk$ για κάποια $h \in H$ και $k \in K$. Συνεπώς, $x = (x^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$ (αφού $k^{-1} \in K$, $h^{-1} \in H$). Άρα $HK \subseteq KH$. Με παρόμοιο τρόπο δείχνουμε ότι $KH \subseteq HK$.

Έστω τώρα ότι $HK = KH$. Θα χρησιμοποιήσουμε την Πρόταση 12.19. Παρατηρούμε πρώτα ότι $1_G (= 1_G 1_G) \in HK$, άρα $HK \neq \emptyset$. Υποθέτουμε ότι $a, b \in HK$. Τότε $a = h_1 k_1$ και $b = h_2 k_2$ για κάποια $h_1, h_2 \in H$ και $k_1, k_2 \in K$. Έπεται ότι $ab^{-1} = (h_1 k_1)(h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1} = (h_1 h_3) k_3 \in HK$. (Αφού $HK = KH$, έχουμε ότι $k_1 k_2^{-1} h_2^{-1} = h_3 k_3$ για κάποια $h_3 \in H$ και $k_3 \in K$.)

14.15 (i) Έστω G ομάδα, $H \leq G$ και $K \triangleleft G$. Προφανώς $1_G (= 1_G 1_G) \in HK$ (έχουμε ότι $1_G \in H \cap K$ αφού H, K είναι υποομάδες της G). Συνεπώς HK είναι ένα μη-κενό υποσύνολο της G . Έστω τώρα $x, y \in HK$. Τότε $x = h_1 k_1$ και $y = h_2 k_2$ για κάποια $h_1, h_2 \in H$ και $k_1, k_2 \in K$. Έχουμε, $xy^{-1} = (h_1 k_1)(h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1} = h_1 h_2^{-1} (h_2 k_1 k_2^{-1} h_2^{-1}) \in HK$. Χρησιμοποιούμε τέλος την Πρόταση 12.19.

(ii) Από την Άσκηση 14.14, έχουμε ότι $HK = KH$. Από την Πρόταση 13.1, θέτοντας $S = H \cup K$, βλέπουμε ότι $hk \in \langle H \cup K \rangle$ για όλα τα $h \in H$ και $k \in K$ και επομένως $HK \subseteq \langle H \cup K \rangle$ (αφού $HK = \{hk : h \in H, k \in K\}$ από τον ορισμό του γινομένου υποσυνόλων. Για να δείξουμε ότι $\langle H \cup K \rangle \subseteq HK$ αρκεί να παρατηρήσουμε ότι $HK \leq G$ με $H \subseteq HK$ και $K \subseteq HK$ (και επομένως $H \cup K \subseteq HK$).

(iii) Αν $h \in H$, $k \in K$ και $g \in G$, τότε $g^{-1}hkg = g^{-1}hgg^{-1}kg \in HK$.

14.16 Προφανώς η συνάρτηση θ είναι επιρριπτική. Έστω τώρα $i, j \in \mathbb{Z}$ με $0 \leq i, j \leq 11$. Τότε $a^i a^j = a^r$ για κάποιο $r \in \mathbb{Z}$ με $0 \leq r \leq 11$ και μπορούμε να βρούμε αυτό το r χρησιμοποιώντας μόνο την σχέση $a^{12} = 1_G$. Έπεται ότι $b^i b^j = b^r$ αφού στην ομάδα K ισχύει η σχέση $b^{12} = 1_K$. Συνεπώς, $\theta(a^i a^j) = \theta(a^r) = b^r = b^i b^j = \theta(a^i) \theta(a^j)$ δείχνοντας έτσι ότι θ είναι ομομορφισμός. Από σχετικά αποτελέσματα έχουμε ότι $\{1_K\}, \langle b^2 \rangle (= \{1, b^2\})$ και $\langle b \rangle (= K)$ είναι όλες οι υποομάδες της K . Παρατηρούμε επίσης ότι $\ker \theta = \{x \in G : \theta(x) = 1_K\} = \{1_G, a^4, a^8\} = \langle a^4 \rangle$ και, επιπλέον, ότι $\theta(\langle a^4 \rangle) = \{1_K\}$, $\theta(\langle a^2 \rangle) = \langle b^2 \rangle$ και $\theta(\langle a \rangle) = \langle b \rangle$. Συγκρίνετε με το Θεώρημα 14.33 και το Πρόσχημα 14.35. [Σχόλιο: Θεωρούμε την υποομάδα $\langle a^3 \rangle (= \{1_G, a^3, a^6, a^9\})$ της G . Παρατηρούμε ότι $\theta(\langle a^3 \rangle) = \langle b \rangle$, όμως η $\langle a^3 \rangle$ δεν περιέχει το $\ker \theta$.]

14.17 Από το Θεώρημα 14.31 έχουμε, $HN/N \cong H/H \cap N = H/H \cap M \cong HM/M$.

[Η Άσκηση 14.15 μας εξασφαλίζει ότι HN και HM είναι πράγματι ομάδες.]

15.1 Ορισμός. Αν W είναι υποσύνολο του καθολικού συνόλου S , ορίζουμε την *χαρακτηριστική του συνάρτηση* $\chi_W : S \rightarrow \mathbb{Z}_2$, με $\chi_W(t) = \begin{cases} \bar{1}, & \text{αν } t \in W, \\ \bar{0}, & \text{αν } t \in S - W. \end{cases}$

Έχουμε τότε, για οποιαδήποτε υποσύνολα U, V του S , ότι $U = V$ αν-ν $\chi_U = \chi_V$ (αν-ν $\chi_U(t) = \chi_V(t)$ για όλα τα $t \in S$). Επιπλέον, ως προς την πρόσθεση (+) και πολλαπλασιασμό ($\cdot$) στο $\mathbb{Z}_2$, έχουμε ότι $\chi_{U \oplus V}(t) = \chi_U(t) + \chi_V(t)$ και $\chi_{U \odot V}(t) = \chi_U(t) \cdot \chi_V(t)$ για όλα τα $t \in S$. Από τις ιδιότητες του δακτύλιου $(\mathbb{Z}_2, +, \cdot)$ προκύπτουν οι αντίστοιχες ιδιότητες για την τριάδα $(\mathcal{P}(S), \oplus, \odot)$. Για παράδειγμα, για την προσεταιριστική ιδιότητα ως προς την ‘πρόσθεση’ $\oplus$:

Έστω $A, B, C \subseteq S$. Από τα πιο πάνω, για κάθε $t \in S$ έχουμε, χρησιμοποιώντας ότι η πρόσθεση που έχουμε ορίσει στο $\mathbb{Z}_2$ ικανοποιεί την προσεταιριστική ιδιότητα, ότι $\chi_{(A \oplus B) \oplus C}(t) = \chi_{(A \oplus B)}(t) + \chi_C(t) = (\chi_A(t) + \chi_B(t)) + \chi_C(t) = \chi_A(t) + (\chi_B(t) + \chi_C(t)) = \chi_A(t) + \chi_{B \oplus C}(t) = \chi_{A \oplus (B \oplus C)}(t)$. Συνάγουμε ότι $\chi_{(A \oplus B) \oplus C}(t) = \chi_{A \oplus (B \oplus C)}(t)$ για όλα τα $t \in S$, και επομένως $(A \oplus B) \oplus C = A \oplus (B \oplus C)$.

Η τριάδα $(\mathcal{P}(S), \boxplus, \odot)$ δεν αποτελεί δακτύλιο αφού γενικά δεν υπάρχουν τα συμμετρικά στοιχεία ως προς την ‘πρόσθεση’ $\boxplus$. (Το κενό σύνολο αποτελεί ουδέτερο στοιχείο ως προς την $\boxplus$.)

15.2 Οι δακτύλιοι $\mathbb{Q}, \mathbb{R}$ είναι σώματα, όχι όμως οι δακτύλιοι $\mathbb{Z}$ και $M_n(\mathbb{R}), n > 1$.

15.3 Παρατηρούμε πρώτα ότι το σύνολο $3\mathbb{Z}$ αποτελεί αβελιανή ομάδα ως προς την συνηθισμένη πρόσθεση ακεραίων. [Το άθροισμα δύο πολλαπλασίων του 3 είναι πολλαπλάσιο του 3. Επίσης, $0 \in 3\mathbb{Z}$ και αν $m \in 3\mathbb{Z}$ τότε $m = 3k$ για κάποιο $k \in \mathbb{Z}$. Όμως τότε $3(-k) \in 3\mathbb{Z}$ και $3k + 3(-k) = 3(k + -k) = 0$.] Επιπλέον, τα (ii) και (iii) στον ορισμό του δακτύλιου κληρονομούνται από τον δακτύλιο $\mathbb{Z}$ (ως προς την συνηθισμένη πρόσθεση και πολλαπλασιασμό).

15.4 (i) Έστω $r, s \in R^*$. Τότε υπάρχουν τα $r^{-1}, s^{-1} \in R^*$ όπου $rr^{-1} = 1_R = r^{-1}r$ και $s^{-1}s = 1_R = ss^{-1}$. Έπεται ότι $(s^{-1}r^{-1})(rs) = 1_R = (rs)(s^{-1}r^{-1})$ και επομένως $rs \in R^*$. Προφανώς $1_R \in R^*$ αφού $1_R 1_R = 1_R$. Ο προσεταιρισμός κληρονομείται από τον R .

(ii) Παρατηρούμε ότι $r = r1_R$ για όλα τα $r \in R$ και επομένως $(r, r) \in T$. Αν $(r, s) \in T$, όπου $r, s \in R$, τότε $s = ru$ για κάποιο $u \in R^*$ και επομένως $r = su^{-1}$ όπου $u^{-1} \in R^*$. Τέλος, υποθέτουμε ότι $(r, s), (s, t) \in T$. Τότε $s = ru$ και $t = sv$ για κάποια $u, v \in R^*$. Συνεπώς $t = sv = (ru)v = r(uv)$, όπου $uv \in R^*$.

15.5 (i) Έχουμε ότι $0_S + 0_S = 0_S$ στο S , όμως $S \subseteq R$ και S, R έχουν την ίδια πρόσθεση. Έπεται ότι η σχέση $0_S + 0_S = 0_S$ ισχύει στο R . Προσθέτοντας το αντίθετο του 0_S στον R και στα δύο μέλη της τελευταίας

ισότητάς, προκύπτει ότι $0_S = 0_R$. Έστω $a \in S$. Έχουμε τότε ότι $a + (-a)_S = 0_S (= 0_R) = (-a)_S + a$. Έπεται ότι $(-a)_S = (-a)_R$ από την μοναδικότητα του αντίθετου στοιχείου.

(ii) Από το (i) ξέρουμε ότι $0_T = 0_F$, αφού T είναι υποδακτύλιος του F . Έπεται ότι $1_T \neq 0_F (= 0_T)$ (αφού T είναι 1-δακτύλιος) και επομένως υπάρχει το $(1_T^{-1})_F$. Η σχέση $1_T 1_T = 1_T$ ισχύει και στο σώμα F . Πολλαπλασιάζοντας και τα δύο μέλη της τελευταίας ισότητας με το $(1_T^{-1})_F$ προκύπτει ότι $1_T = 1_F$. Έστω τώρα $a \in T - \{0_F\}$. Τότε $a \in T - \{0_T\}$ και επομένως υπάρχει το $(a^{-1})_T \in T (\subseteq F)$ όπου $(a^{-1})_T a = 1_T (= 1_F) = a(a^{-1})_T$. Από την μοναδικότητα του αντίστροφου στο F προκύπτει ότι $(a^{-1})_T = (a^{-1})_F$.

15.6 Έστω $t \in S$. Τότε $t + (-t) \in S$ και επομένως $0_R \in S$. Έχουμε επίσης ότι $-t = 0_R + (-t) \in S$. Επιπλέον, αν $s \in S$, τότε $s + t = s + (-(-t)) \in S$. Το αποτέλεσμα είναι τώρα άμεση συνέπεια της Πρότασης 15.7.

15.7 Χρησιμοποιούμε την Άσκηση 15.6. Προφανώς $m\mathbb{Z} \neq \emptyset$. Έστω $a, b \in m\mathbb{Z}$. Τότε $a = mk_1$ και $b = mk_2$ για κάποια $k_1, k_2 \in \mathbb{Z}$. Συνεπώς $a + (-b) = mk_1 + m(-k_2) = m(k_1 - k_2) \in m\mathbb{Z}$ αφού $k_1 - k_2 \in \mathbb{Z}$. Επίσης, $ab = (mk_1)(mk_2) = m(mk_1 k_2) \in m\mathbb{Z}$ αφού $mk_1 k_2 \in \mathbb{Z}$.

15.8 (i) Προφανώς $R \neq \emptyset$. Έστω $z_1, z_2 \in R$. Τότε $z_1 = a_1 + b_1\omega$ και $z_2 = a_2 + b_2\omega$ για κάποια $a_i, b_j \in \mathbb{Z}$. Έχουμε τότε ότι $z_1 + (-z_2) = (a_1 - a_2) + (b_1 - b_2)\omega \in R$, αφού $a_1 - a_2, b_1 - b_2 \in \mathbb{Z}$. Επιπλέον, $z_1 z_2 = (a_1 a_2 + b_1 b_2 \omega^2) + (a_1 b_2 + b_1 a_2)\omega = (a_1 a_2 - 5b_1 b_2) + (a_1 b_2 + b_1 a_2)\omega \in R$. Χρησιμοποιούμε τώρα την Άσκηση 15.6.

(ii) Έχουμε ότι R είναι υποδακτύλιος του σώματος $\mathbb{C}$ και, επιπλέον, $1 \in R$.

(iii) Έστω ότι $a + b\omega \in R^*$, όπου $a, b \in \mathbb{Z}$. Τότε υπάρχουν $x, y \in \mathbb{Z}$ με $(a + b\omega)(x + y\omega) = 1$. Έπεται ότι $1 = |(a + b\omega)(x + y\omega)| = |a + b\omega||x + y\omega|$. Όμως $|a + b\omega|^2 = |a + b\sqrt{5}i|^2 = a^2 + 5b^2$, και $|x + y\omega|^2 = x^2 + 5y^2$. Έχουμε δηλαδή $(a^2 + 5b^2)(x^2 + 5y^2) = 1$, όπου $a^2 + 5b^2, x^2 + 5y^2 \in \mathbb{N}$. Έπεται ότι $a^2 + 5b^2 = 1$ με $a, b \in \mathbb{Z}$. Συνάγουμε ότι $R^* = \{1, -1\}$, αφού $a \in \{1, -1\}$ και $b = 0$.

15.9 Το σύνολο T αποτελεί υποδακτύλιο του F (Πρόταση 15.7) και επομένως T είναι ένας μεταθετικός δακτύλιος (ως προς τις ίδιες πράξεις του σώματος F). Επιπλέον έχουμε ότι $0_T = 0_F$ από την Παρατήρηση 15.9. Έστω τώρα $a \in T$ με $a \neq 0_F$ (το σύνολο T περιέχει τουλάχιστον δύο στοιχεία). Από το (iii) έχουμε ότι $a^{-1} \in T$, άρα από το (i) προκύπτει ότι $1_F = aa^{-1} \in T$. Έπεται ότι T είναι ένας 1-δακτύλιος αφού το 1_F είναι προφανώς ένα ουδέτερο στοιχείο του T ως προς το πολλαπλασιασμό και $1_F \neq 0_F (= 0_T)$. Τέλος, η ιδιότητα (iii) μας εξασφαλίζει ότι κάθε μη-μηδενικό στοιχείο του T είναι αντιστρέψιμο.

15.10 Προφανώς $1 + 0i \in S \subseteq \mathbb{C}$. Χρησιμοποιώντας τις ιδιότητες του σώματος $\mathbb{C}$ και την Άσκηση 15.6 βλέπουμε ότι S είναι ένας μεταθετικός 1-δακτύλιος ως προς την πρόσθεση και πολλαπλασιασμό στο $\mathbb{C}$. Έστω τώρα $z \in S - \{0\}$. Τότε $z = a + ib$ για κάποια $a, b \in \mathbb{Q}$ με $(a, b) \neq (0, 0)$. Θέτουμε $w = \frac{1}{a^2 + b^2}(a - ib)$. Τότε $w \in S$ και $zw = 1 = wz$.

15.12 Έστω $A_\lambda, \lambda \in \Lambda$ (όπου Λ σύνολο δεικτών) μια οικογένεια υποσωμάτων του F . Χρησιμοποιούμε την Άσκηση 15.9 και παρατηρούμε πρώτα ότι $\{0_F, 1_F\} \subseteq \bigcap_{\lambda \in \Lambda} A_\lambda$. Έστω τώρα $a, b \in \bigcap_{\lambda \in \Lambda} A_\lambda$. Τότε $a, b \in A_\lambda$ για όλα τα $\lambda \in \Lambda$ και επομένως $a + b, ab, -a \in A_\lambda$ για όλα τα $\lambda \in \Lambda$ αφού A_λ αποτελεί υπόσωμα του F . Έπεται ότι $a + b, ab, -a \in \bigcap_{\lambda \in \Lambda} A_\lambda$. Επιπλέον, αν $a \neq 0_F$, τότε $a^{-1} \in A_\lambda$ για όλα τα $\lambda \in \Lambda$ (χρησιμοποιήσαμε και πάλι εδώ την Παρατήρηση 15.9) και επομένως $a^{-1} \in \bigcap_{\lambda \in \Lambda} A_\lambda$.

Σημείωση. Με παρόμοιο τρόπο, χρησιμοποιώντας τώρα την Πρόταση 15.7, μπορούμε να δείξουμε ότι η τομή μιας οικογένειας υποδακτυλίων ενός δακτυλίου R είναι υποδακτύλιος του R .

15.13 Από τον ορισμό της αθέραιας περιοχής έχουμε, πιο ειδικά, ότι R, S είναι μεταθετικοί 1-δακτύλιοι.

(i) Έχουμε ότι $\phi(1_R) = \phi(1_R 1_R) = (\phi 1_R)(\phi 1_R)$. Συνεπώς, $0_S = (\phi 1_R)(\phi 1_R) - (\phi 1_R) = (\phi 1_R)((\phi 1_R) - 1_S)$. Όμως $(\phi 1_R) \neq 0_S$ και S είναι αθέραια περιοχή. Έπεται ότι $\phi(1_R) = 1_S$.

(ii) Θεωρούμε τον ομομορφισμό δακτυλίων $\phi: R \rightarrow S: r \mapsto r$ ($r \in R$). Τότε $\phi(1_R) \neq 0_S$ αφού $1_R \neq 0_R (= 0_S)$. Παρεμβάλλοντας το (i), συνάγουμε ότι $1_R = \phi(1_R) = 1_S$. [Εναλλακτικά, παρατηρούμε ότι $0_S = 1_R - 1_R = 1_R 1_R - 1_R 1_S = 1_R(1_R - 1_S)$.]

15.14 (i) Η συνάρτηση $\hat{\phi}: R \rightarrow \text{im } \phi: r \mapsto \phi(r)$ είναι αμφιμονοσήμαντη και, επιπλέον, ένας ομομορφισμός δακτυλίων από τις ιδιότητες της ϕ .

(ii) Παρατηρούμε πρώτα ότι $\psi(1_F) \neq 0_K$, αφού ψ είναι ενριπτικός ενώ επίσης ισχύουν $\psi(0_F) = 0_K$ και $0_F \neq 1_F$. Η Άσκηση 15.13(i) μας εξασφαλίζει ότι $\psi(1_F) = 1_K$, αφού κάθε σώμα είναι αθέραια περιοχή. Έπεται ότι $\{0_K, 1_K\} \subseteq \text{im } \psi (\subseteq K)$. Συνεπώς, για να δείξουμε ότι $\text{im } \psi$ αποτελεί υπόσωμα του K αρκεί να δείξουμε ότι ισχύει το (iii) στην Άσκηση 15.9. (Τα (i) και (ii) ισχύουν αφού $\text{im } \psi$ είναι υποδακτύλιος του K από την Πρόταση 15.12.) Έστω λοιπόν $a \in \text{im } \psi$ με $a \neq 0_K$. Τότε $a = \psi(r)$ για κάποιο $r \in F$ με $r \neq 0_F$ (ψ είναι ενριπτικός). Από τις ιδιότητες ενός σώματος, υπάρχει $r^{-1} \in F$ με $1_F = rr^{-1}$. Έπεται ότι $1_K = \psi(1_F) = \psi(rr^{-1}) = (\psi r)(\psi r^{-1}) = (\psi r^{-1})(\psi r)$. Συνάγουμε ότι το στοιχείο $a (= \psi(r))$ του $\text{im } \psi$ είναι αντιστρέψιμο στο $\text{im } \psi$, αφού $\psi(r^{-1}) (= a^{-1}) \in \text{im } \psi$. Για να δείξουμε ότι $\text{im } \psi \cong F$, χρησιμοποιούμε το τμήμα (i) της άσκησης.

16.1 (i) Προφανώς η συνάρτηση ϕ είναι αμφιμονοσήμαντη. Έστω τώρα $z, w \in \mathbb{C}$. Τότε $\phi(z + w) = \overline{z + w} = \overline{z} + \overline{w} = \phi(z) + \phi(w)$, και $\phi(zw) = \overline{zw} = \overline{z} \overline{w} = \phi(z)\phi(w)$. Συνεπώς ϕ είναι επίσης ομομορφισμός δακτυλίων.

(ii) Έστω $w \in \mathbb{C}$. Έχουμε τότε: $g(w) = 0 \Leftrightarrow \overline{g(w)} = \overline{0} (= 0) \Leftrightarrow 2 + 3\overline{w} + 4\overline{w^2} + 5\overline{w^3} = 0 \Leftrightarrow g(\overline{w}) = 0$.

(iii) Έστω $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{R}[x]$. Με παρόμοιο συλλογισμό όπως στο τμήμα (ii): $\text{ev}_w((f(x))) = 0 \Leftrightarrow \overline{\text{ev}_w((f(x)))} = \overline{0} (= 0) \Leftrightarrow a_0 + a_1\overline{w} + \dots + a_n\overline{w^n} = 0 \Leftrightarrow a_0 + a_1\overline{w} + \dots + a_n(\overline{w})^n = 0 \Leftrightarrow \text{ev}_{\overline{w}}((f(x))) = 0$.

16.2 (ii) Υπάρχει ο $\text{μκδ}(f, g)$ αφού $g \neq 0$. Έστω $d = \text{μκδ}(f, g)$. Έχουμε τότε:

(a) το πολυώνυμο $d \in F[x]$ είναι μονικό,

(b) $d|f$ και $d|g$, επομένως $d|r$ αφού $r = f - qg$, και

(c) αν $m \in F[x]$ με $m|g$ και $m|r$, τότε $m|f$ επίσης (αφού $f = qg + r$) και επομένως $m|d$, (αφού $d = \text{μκδ}(f, g)$).

16.3 Προφανώς ο δακτύλιος $F[x]$ είναι αθέραια περιοχή αφού F είναι σώμα. Θέτουμε $\delta: F[x] - \{0\} \rightarrow \mathbb{N} \cup \{0\}: f(x) \mapsto \deg(f)$, ($f(x) \neq 0$). Έστω $f, g \in F[x] - \{0\}$. Έχουμε τότε ότι $\delta(g) \geq 0$ και, επιπλέον, $\delta(fg) = \deg(fg) = \deg(f) + \deg(g) \geq \deg(f) = \delta(f)$. Το αποτέλεσμα είναι τώρα άμεση συνέπεια του Θεωρήματος 16.4.

16.4 (i) Έστω $\alpha \in F$ μια θέση μηδενισμού του $f(x)$. Τότε $x - \alpha \in F[x] - \{0\}$. Από το θεώρημα διαίρεσης υπάρχουν $q(x), r(x) \in F[x]$ με $f(x) = q(x)(x - \alpha) + r(x)$ όπου είτε $r(x) = 0$ ή $\deg(r) < \deg(x - \alpha) = 1$. Έπεται ότι $r(x)$ είναι ένα σταθερό πολυώνυμο, έστω $r(x) = \beta$ όπου $\beta \in F$. Συνεπώς, $0_F = \text{ev}_\alpha(f) = \text{ev}_\alpha((x - \alpha)q(x) + \beta) = \text{ev}_\alpha((x - \alpha)q(x)) + \text{ev}_\alpha(\beta) = \text{ev}_\alpha(x - \alpha)\text{ev}_\alpha(q(x)) + \text{ev}_\alpha(\beta) = 0_F \text{ev}_\alpha(q(x)) + \beta = \beta$. Συνάγουμε ότι $\beta = 0_F$ και επομένως $f(x) = (x - \alpha)q(x)$.

(ii) Προχωρούμε με επαγωγή στο $n = \deg(f)$.

Αν $n = 1$, τότε $f(x) = \gamma + \delta x$ ($\gamma, \delta \in F$ με $\delta \neq 0_F$). Αν $\alpha \in F$ είναι μια θέση μηδενισμού του $f(x)$, τότε $0_F = \gamma + \delta\alpha$ ή, ισοδύναμα, $\alpha = -\gamma\delta^{-1}$ (μοναδική λύση).

Έστω τώρα ότι $n > 1$. Αν $f(x)$ δεν έχει θέσεις μηδενισμού, η απόδειξη τελειώνει, αφού $0 \leq n$. Υποθέτουμε λοιπόν ότι $\alpha \in F$ είναι μια θέση μηδενισμού του $f(x)$. Από το (i) προκύπτει ότι $f(x) = (x - \alpha)q(x)$ για

κάποιο $q(x) \in F[x]$ με $\deg(q) = n - 1 (\geq 1)$. Αν τώρα $\beta \in F$ (όπου $\beta \neq \alpha$) είναι μια άλλη θέση μηδενισμού του $f(x)$, έχουμε ότι $0_F = \text{ev}_\beta(f(x)) = \text{ev}_\beta((x - \alpha)q(x)) = \text{ev}_\beta(x - \alpha)\text{ev}_\beta(q(x)) = (\beta - \alpha)\text{ev}_\beta(q(x))$, όπου $\beta - \alpha \neq 0_F$. Συμπεραίνουμε, αφού F είναι ακέραια περιοχή, ότι οποιαδήποτε άλλη θέση μηδενισμού του $f(x)$ εκτός (πιθανά) από την α , είναι θέση μηδενισμού του $q(x)$. Από την επαγωγική υπόθεση, $q(x)$ έχει το πολύ $\deg(q) = n - 1$ θέσεις μηδενισμού στο F . Συνάγουμε ότι $f(x)$ έχει το πολύ n θέσεις μηδενισμού στο F .

(iii) Θέτουμε $h(x) = f(x) - g(x) \in F[x]$. Τότε $\text{ev}_{\alpha_i}(h(x)) = \text{ev}_{\alpha_i}(f(x)) - \text{ev}_{\alpha_i}(g(x)) = 0_F$. Έπεται ότι $\alpha_1, \dots, \alpha_{n+1}$ είναι $n + 1$ διακεκριμένες θέσεις μηδενισμού του $h(x) \in F[x]$, όπου είτε $h(x)$ είναι ένα σταθερό πολυώνυμο ή $1 \leq \deg(h) \leq n$. Χρησιμοποιούμε το τμήμα (ii) της άσκησης για το 2^ο ενδεχόμενο.

16.5 Έστω $f(x) \in \mathbb{R}[x]$ ένα ανάγωγο πολυώνυμο επί του $\mathbb{R}$. Από το θεμελιώδες θεώρημα της άλγεβρας (και την Άσκηση 16.4(i)), βλέπουμε ότι το $f(x)$ μπορεί να εκφραστεί ως γινόμενο πολυωνύμων του $\mathbb{C}[x]$ βαθμού 1. Επιπλέον, από την Άσκηση 16.1(iii), οι μη-πραγματικές θέσεις μηδενισμού του $f(x)$ στο $\mathbb{C}$ (αν υπάρχουν τέτοιες) προκύπτουν ως ζεύγη μιγαδικών αριθμών $\{w, \bar{w}\}$ όπου $w \in \mathbb{C} - \mathbb{R}$. Συνεπώς, στον δακτύλιο $\mathbb{C}[x]$, έχουμε (αν $w \in \mathbb{C} - \mathbb{R}$) ότι $(x - w)|f(x)$ αν-ν $(x - \bar{w})|f(x)$ αν-ν $(x - w)(x - \bar{w})|f(x)$, αφού $\text{mcd}(x - w, x - \bar{w}) = 1$. Όμως $(x - w)(x - \bar{w}) = x^2 - (w + \bar{w})x + w\bar{w} \in \mathbb{R}[x]$, αφού $w + \bar{w}, w\bar{w} \in \mathbb{R}$. Συνοψίζοντας, υπάρχουν δύο ενδεχόμενα για το ανάγωγο (επί του $\mathbb{R}$) πολυώνυμο $f(x) \in \mathbb{R}[x]$.

(i) Υπάρχει $\alpha \in \mathbb{R}$ με $\text{ev}_\alpha(f) = 0$. Τότε $f = \beta(x - \alpha)$ για κάποιο $\beta \in \mathbb{R}$, άρα $\deg(f) = 1$.

(ii) Δεν υπάρχει $\alpha \in \mathbb{R}$ με $\text{ev}_\alpha(f) = 0$. Τότε υπάρχει $w \in \mathbb{C} - \mathbb{R}$ με $\text{ev}_w(f) = 0 = \text{ev}_{\bar{w}}(f)$. Άρα $f(x) = \beta(x^2 - (w + \bar{w})x + w\bar{w})$ για κάποιο $\beta \in \mathbb{R}$, και $\deg(f) = 2$.

16.6 Έχουμε, $f(x) = (x^2 - 4x + 3)q(x) + (ax + b)$, όπου $a, b \in \mathbb{R}$. Από την υπόθεση, $\text{ev}_3(f) = f(3) = 6$ και $f(1) = 4$. Έπεται ότι $a = 1, b = 3$.

16.7 Θεωρούμε το πολυώνυμο $f(x) = \frac{(x-b)(x-c)}{(a-b)(a-c)} + \frac{(x-c)(x-a)}{(b-c)(b-a)} + \frac{(x-a)(x-b)}{(c-a)(c-b)} - 1 \in \mathbb{R}[x]$. Τότε $f(x) = 0$ ή $f(x)$ είναι πολυώνυμο βαθμού το πολύ 2. Αν $f(x)$ είναι μη-μηδενικό, τότε έχει το πολύ 2 ρίζες, όμως παρατηρούμε ότι a, b, c είναι τρεις διαφορετικές ρίζες του $f(x)$. Άρα $f(x) = 0$ και επομένως $f(d) = 0$ για όλα τα $d \in \mathbb{R}$.

16.8 Θεωρούμε το πολυώνυμο $g(x) = f(x) - f(-x) \in \mathbb{R}[x]$. Τότε $g(x)$ είναι βαθμού το πολύ 99 όμως έχει τουλάχιστον 100 θέσεις μηδενισμού.

17.1 (i) Έστω $(I_\lambda)_{\lambda \in \Lambda}$, όπου Λ είναι ένα σύνολο δεικτών, μια οικογένεια ιδεωδών του R . Έστω επίσης $r \in R$ και $a, b \in (\cap_{\lambda \in \Lambda} I_\lambda)$. Παρατηρούμε ότι, για κάθε $\lambda \in \Lambda$, ισχύουν (a) $0_R \in I_\lambda$, (b), $a - b \in I_\lambda$ και (c) $ra, ar \in I_\lambda$.

(ii) Παρατηρούμε ότι $0_R = 0_R + 0_R \in I + J$, αφού $0_R \in I$ και $0_R \in J$. Έστω τώρα $x_1, x_2 \in I + J$ και $r \in R$. Τότε $x_i = a_i + b_i$ ($i = 1, 2$) όπου $a_i \in I, b_i \in J$. Επομένως, $x_1 - x_2 = (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in I + J$, αφού $a_1 - a_2 \in I$ και $b_1 - b_2 \in J$. Επιπλέον, $rx_1 = r(a_1 + b_1) = ra_1 + rb_1 \in I + J$, αφού $ra_1 \in I$ και $rb_1 \in J$. Παρόμοια, $x_1r \in I + J$.

17.2 Έστω R μεταθετικός 1-δακτύλιος. Υποθέτουμε πρώτα ότι R είναι σώμα. Αν $I \neq \{0_R\}$ είναι ιδεώδες του R , τότε υπάρχει $r \in R^* \cap I$, αφού κάθε μη-μηδενικό στοιχείο του R είναι αντιστρέψιμο. Έπεται ότι $1_R = r^{-1}r \in I$, αφού $r^{-1} \in R$ και $r \in I$. Συνάγουμε ότι $I = R$ στην περίπτωση αυτή. Υποθέτουμε τώρα ότι $\{0_R\}, R$ είναι τα μόνα ιδεώδη του R . Αρκεί να δείξουμε ότι $R^* = R - \{0_R\}$ για να δείξουμε ότι R είναι σώμα. Έστω $a \in R - \{0_R\}$. Τότε $\langle a \rangle = R$, αφού προφανώς $\langle a \rangle \neq \{0_R\}$. Έπεται ότι $1_R \in \langle a \rangle$. Συνάγουμε ότι $1_R = ta (= at)$ για κάποιο $t \in R$.

17.3 Έχουμε ότι $\mu\kappa\delta(p(x), s(x)) = 1$ και επομένως $1 = a(x)p(x) + b(x)s(x)$ για κάποια $a(x), b(x) \in F[x]$. Έπεται ότι $\bar{1} = \overline{a(x)p(x) + b(x)s(x)}$ στον δακτύλιο πηλίκο $F[x]/I$, όπου $\overline{p(x)} = \bar{0}$. Συνάγουμε ότι $\bar{1} = \overline{b(x)s(x)} (= \overline{s(x)b(x)})$.

17.4 Έστω p ανάγωγο στοιχείο της αθέραιας περιοχής R και $u \in R^*$. Έστω επίσης $q = pu \in R$. Θα δείξουμε ότι q είναι ανάγωγο στοιχείο της R . Παρατηρούμε πρώτα ότι $q \neq 0_R$ αφού $q = pu$ με $p \neq 0_R$ (p είναι ανάγωγο) και $u \neq 0_R$ (u είναι αντιστρέψιμο). Επίσης $q \notin R^*$. [Εξήγηση: Αν $q \in R^*$, θα είχαμε ότι $p (= qu^{-1}) \in R^*$ ως γινόμενο στοιχείων του R^* .] Έστω τώρα $q = ab$ με $a, b \in R$. Έχουμε τότε $pu = ab$ ή, ισοδύναμα, $p = (ab)u^{-1} = a(bu^{-1})$. Αφού p είναι ανάγωγο συμπεραίνουμε ότι είτε $a \in R^*$ ή $bu^{-1} \in R^*$. Όμως $bu^{-1} \in R^*$ αν-ν $b \in R^*$, αφού $u, u^{-1} \in R^*$.

17.5 Έχουμε, $3 + 5i (= 2(\frac{3}{2} + \frac{5}{2}i) = 2((1 + 2i) + (\frac{1}{2} + \frac{1}{2}i))) = 2(1 + 2i) + (1 + i) = 2(2 + 2i) + (-1 + i) = 2(1 + 3i) + (1 - i) = 2(2 + 3i) + (-1 - i)$. [Έστω $z = 3 + 5i$. Χρησιμοποιούμε ότι $z = 2w + r$ με $|r| < 2$ αν-ν $z/2 = w + r/2$ με $|r/2| < 1$. Για ποια $a + bi$ (με $a, b \in \mathbb{Z}$) ισχύει ότι $|z/2 - (a + bi)| < 1$;

17.6 Θέτουμε $I = \langle 2, x \rangle \subseteq \mathbb{Z}[x]$. Ο δακτύλιος $\mathbb{Z}[x]$ είναι ένας μεταθετικός 1-δακτύλιος και επομένως, σύμφωνα με την Πρόταση 17.10, $I = \{2a(x) + xb(x) : a(x), b(x) \in \mathbb{Z}[x]\}$. Έπεται ότι I αποτελείται ακριβώς από τα πολυώνυμα του $\mathbb{Z}[x]$ που έχουν άρτιο σταθερό όρο. Πιο ειδικά, τα σταθερά πολυώνυμα $1, -1$ του $\mathbb{Z}[x]$ δεν ανήκουν στο I . Έστω τώρα ότι $I = \langle d(x) \rangle$ για κάποιο $d(x) \in \mathbb{Z}[x]$. Αφού $2 \in I$, υπάρχει $f(x) \in \mathbb{Z}[x]$ με $2 = f(x)d(x)$. Συμπεραίνουμε ότι $d(x) = c$ για κάποιο $c \in \mathbb{Z}$. [Εξήγηση: $\mathbb{Z}[x]$ είναι αθέραια περιοχή και επομένως $\deg(f) + \deg(d) = 0$. Έπεται ότι τα $f(x), d(x)$ είναι σταθερά πολυώνυμα.] Από $c|2$ και $c \notin \{-1, 1\}$, προκύπτει ότι $c \in \{2, -2\}$. Συνάγουμε ότι $x = 2g(x)$ για κάποιο $g(x) \in \mathbb{Z}[x]$, που είναι άτοπο.

17.7 Έστω R μεταθετικός 1-δακτύλιος.

(i) Έστω I γνήσιο ιδεώδες του R . Τότε ο δακτύλιος πηλίκο R/I είναι ένας μεταθετικός 1-δακτύλιος.

Υποθέτουμε πρώτα ότι R/I είναι αθέραια περιοχή. Έστω επίσης $a, b \in R$ με $ab \in I$. Έχουμε τότε ότι στον R/I ισχύει $0_R + I (= I) = ab + I = (a + I)(b + I)$. Η υπόθεση μας ότι R/I είναι αθέραια περιοχή μας εξασφαλίζει ότι είτε $a + I = 0_{R/I} (= 0_R + I)$ είτε $b + I = 0_R + I$. Όμως $a + I = I$ αν-ν $a \in I$ και $b + I = I$ αν-ν $b \in I$. Συμπεραίνουμε ότι I είναι πρώτο ιδεώδες.

Υποθέτουμε τώρα ότι το ιδεώδες I είναι πρώτο. Τότε R/I είναι ένας μεταθετικός 1-δακτύλιος, και για να δείξουμε ότι R/I είναι αθέραια περιοχή, αρκεί να δείξουμε ότι το γινόμενο δύο μη-μηδενικών στοιχείων του R/I είναι μη-μηδενικό. Έστω $c, d \in R$ με $(c + I)(d + I) = 0_{R/I} (= 0_R + I)$. Έπεται ότι $cd + I = 0_R + I$ και επομένως $cd \in I$. Συνεπώς, αφού I είναι πρώτο ιδεώδες, έχουμε ότι είτε $c \in I$ ή $d \in I$. Όμως $c \in I$ αν-ν $c + I = 0_R + I (= 0_{R/I})$ και $d \in I$ αν-ν $d + I = 0_R + I$. Συνάγουμε ότι R/I είναι αθέραια περιοχή.

(ii) Έστω M μεγιστικό ιδεώδες του R (πιο ειδικά M είναι γνήσιο ιδεώδες του R). Το Θεώρημα 17.20 μας εξασφαλίζει ότι R/M είναι σώμα. Έπεται ότι R/M είναι αθέραια περιοχή. Χρησιμοποιούμε τέλος το τμήμα (i) της άσκησης.

17.8 (i) Το πολυώνυμο $x^3 + x + 1$ (αντίστοιχα, $x^3 + x^2 + 1$) είναι ανάγωγο επί του $\mathbb{Z}_2$, αφού είναι βαθμού 3 και δεν έχει θέση μηδενισμού στο $\mathbb{Z}_2$. Θέτουμε $F_1 = \mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$ (αντίστοιχα, $F'_1 = \mathbb{Z}_2[x]/\langle x^3 + x^2 + 1 \rangle$). Τότε το F_1 (αντίστοιχα, το F'_1) είναι ένα σώμα με ακριβώς 8 στοιχεία (χαιτάζτε τις Προτάσεις 17.19, 17.21 και το Θεώρημα 17.20). Τα 8 διακεκριμένα στοιχεία του F_1 δίνονται με $(\alpha_0 + \alpha_1 x + \alpha_2 x^2) + \langle x^3 + x + 1 \rangle$, όπου $(\alpha_0, \alpha_1, \alpha_2) \in (\mathbb{Z}_2)^3$.

(ii) Το πολυώνυμο $x^2 + 1 \in \mathbb{Z}_3[x]$ είναι ανάγωγο επί του $\mathbb{Z}_3$ αφού είναι βαθμού 2 και δεν έχει θέση μηδενισμού στο $\mathbb{Z}_3$. Τότε $F_2 = \mathbb{Z}_3[x]/\langle x^2 + 1 \rangle$ είναι ένα σώμα με ακριβώς 9 στοιχεία.

Βιβλιογραφία

- [1] Allenby R.B.J.T., *Rings, Fields and Groups*, Butterworth-Heinemann, 1991.
- [2] Baumslag B., Chandler B., *Group Theory*, McGraw Hill, 1968.
- [3] Cameron P.J., *Sets, Logic and Categories*, Springer, 1999.
- [4] Cameron P.J., *Introduction to Algebra*, 2nd Edition, Oxford University Press, 2008.
- [5] Devlin K., *Sets, Functions and Logic: An Introduction to Abstract Mathematics*, Chapman Hall/CRC Mathematics Series, 2003.
- [6] Grimaldi R.P., *Discrete and Combinatorial Mathematics: an Applied Introduction*, Addison-Wesley, 1989.
- [7] Halmos P.R., *Naive Set Theory*, Springer-Verlag, 1974.
- [8] Herstein I. N., *Topics in Algebra*, John Wiley & Sons, 1991.
- [9] Herstein I. N., *Abstract Algebra*, Wiley, 1996.
- [10] Hewitt E., Stromberg K., *Real and Abstract Analysis*, Springer, 1975.
- [11] James G., Liebeck M., *Representations and Characters of Groups*, Cambridge University Press, 2001.
- [12] Jordan C.R. and Jordan D.A., *Groups*, Elsevier Science, Butterworth-Heinemann, 1994.
- [13] Klein F., *Elementary Mathematics from a Higher Standpoint. I: Arithmetic, Algebra, Analysis. II: Geometry. III: Precision Mathematics and Approximation Mathematics*, Springer, 2016.
- [14] Lang S., *Undergraduate Algebra*, Springer, 2010.
- [15] Ledermann W., Weir A., *An Introduction to Group Theory*, Longman, 1996.
- [16] Liebeck M., *A Concise Introduction to Pure Mathematics*, 4th Edition, Routledge, 2015.
- [17] Merzlyak A., Polons'kyi V., Yiakir M., *Algebra in-depth study, grade 8*, on-line textbook, <https://pidruchnyk.com.ua/860-poglyblyeno-algebra-dlya-8-klasu-2016-merzlyak.html> (in Ukrainian).
- [18] Ore O., *Invitation to Number Theory*, AMS, 2016.
- [19] Rotman J.J., *An Introduction to the Theory of Groups*, Springer-Verlag, 1995.
- [20] Rotman J.J., *Galois Theory*, Springer-Verlag, 1998.

- [21] Rotman J.J., *Advanced Modern Algebra*, Prentice Hall, 2002.
- [22] Smith G., *Introductory Mathematics: Algebra and Analysis*, Springer, 1998.
- [23] Velleman D.J., *How to Prove It*, Cambridge University Press, 2006.
- [24] Ανδρεαδάκης Σ.Α., *Μαθήματα επί της Θεωρίας Ομάδων*, Αθήνα, 1986.
- [25] Βάρσος Δ., *Στοιχεία Αλγεβρικής θεωρίας Κωδίκων*, Σοφία, 2005.
- [26] Βάρσος Δ., Δεριζιώτης Δ., Μαλιάκας Μ., Παπασταυρίδης Σ., Ράπτης Ε., Ταλέλλη Ο., *Μια Εισαγωγή στην Άλγεβρα*, Σοφία, 2003.