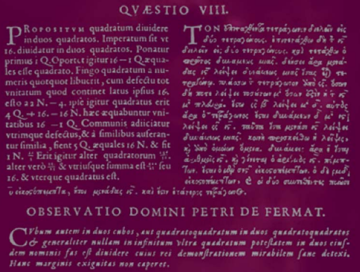
ΔΗΜΗΤΡΙΟΣ Μ. ΠΟΥΛΑΚΗΣ

ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Μια σύγχρονη θεώρηση της κλασσικής Θεωρίας Αριθμών


QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum a numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

ΕΚΔΟΣΕΙΣ ΖΗΤΗ
ΘΕΣΣΑΛΟΝΙΚΗ

Κάθε γνήσιο αντίτυπο υπογράφεται από το συγγραφέα

Εξώφυλλο:
Από την έκδοση των Αριθμητικών του Διοφάντου που επιμελήθηκε ο Samuel de Fermat (Τουλούζη, 1670). Φωτογραφία της σελίδας που περιέχει το πρόβλημα Β′ 8, όπου διακρίνεται το περίφημο σχόλιο (σήμερα πια, θεώρημα) του Pierre de Fermat: ''Είναι αδύνατο να διασπαστεί ένας κύβος σε δύο άλλους κύβους, μια τετάρτη δύναμη, ή γενικά μια οποιαδήποτε δύναμη ανώτερη της δευτέρας, σε δύο δυνάμεις της ίδιας τάξης με αυτήν· έχω βρει μια αληθινά θαυμάσια απόδειξη, αλλά το περιθώριο είναι πολύ στενό για να τη χωρέσει''. Χρειάστηκε να περάσουν 350 χρόνια ώσπου η εικασία αυτή να αποδειχθεί από τον Άγγλο μαθηματικό A. Wiles. (Η ανακοίνωση της απόδειξης έγινε στο Καίμπριτζ τον Ιούνιο του 1993· ένα κενό που περιείχε συμπληρώθηκε το φθινόπωρο του 1994 από τον Wiles και τον R. Taylor).

ISBN 960-431-429-7

Φωτοστοιχειοθεσία
Εκτύπωση

Π. ΖΗΤΗ & Σια ΟΕ
18ο χλμ Θεσ/νίκης-Περαίας
Τ.Θ. 4171 • Περαία Θεσσαλονίκης • Τ.Κ. 570 19
Τηλ.: 23920 72.222 (8 γραμ.) - Fax: 23920 72.229
e-mail: info@ziti.gr

Βιβλιοπωλείο

ΕΚΔΟΣΕΙΣ **ΖΗΤΗ**
Αρμενοπούλου 27 • 546 35 Θεσσαλονίκη
Τηλ. 2310 203.720, Fax 2310 211.305
e-mail: sales@ziti.gr

www.ziti.gr

ΠΡΟΛΟΓΟΣ

Η Θεωρία Αριθμών αποτελεί έναν από τους σημαντικούς κλάδους της Μαθηματικής Επιστήμης. Αυτό οφείλεται όχι μόνο στη μεγάλη ποικιλία των μεθόδων που χρησιμοποιεί και στα πολλά ανοικτά προβλήματα που περιέχει, αλλά και στις εφαρμογές της σε σύγχρονους κλάδους όπως π.χ. η Κρυπτογραφία, η Θεωρία Κωδίκων, η Θεωρία Αυτομάτων κ.λ.π..

Σκοπός αυτού του βιβλίου είναι να δώσει μία εισαγωγή στη στοιχειώδη Θεωρία Αριθμών. Η συγγραφή του έγινε με γνώμωνα την απλούστερη αλλά και πληρέστερη παρουσίαση της ύλης. Αυτή συνοδεύεται από ένα πλήθος παραδειγμάτων και άλυτων ασκήσεων, ποικίλης δυσκολίας. Για την κατανόησή του απαιτούνται γνώσεις Μαθηματικών προ-πανεπιστημιακού επιπέδου.

Στο πρώτο κεφάλαιο παρουσιάζεται μία αξιωματική θεμελίωση του συνόλου των φυσικών αριθμών και κατασκευάζονται τα σύνολα των ακεραίων και ρητών αριθμών. Στο δεύτερο κεφάλαιο περιγράφεται η βασική θεωρία διαιρετότητας των ακεραίων αριθμών. Το αντικείμενο του τρίτου κεφαλαίου είναι η μελέτη των αριθμητικών πολλαπλασιαστικών συναρτήσεων και ειδικώτερα ορισμένων σημαντικών συναρτήσεων όπως π.χ της συνάρτησης φ του Euler. Στο τέταρτο κεφάλαιο μελετώνται οι βασικές ιδιότητες των ισοτιμιών, οι γραμμικές ισοτιμίες και τα συστήματα αυτών. Στο πέμπτο κεφάλαιο μελετώνται οι πολυωνυμικές ισοτιμίες και αποτελέσματα αυτής της μελέτης χρησιμοποιούνται για να προσδιοριστούν οι φυσικοί n για τους οποίους υπάρχουν αρχικές ρίζες (modn). Το έκτο κεφάλαιο είναι αφιερωμένο στα τετραγωνικά υπόλοιπα και στο νόμο της τετραγωνικής αντιστροφής. Στο έβδομο κεφάλαιο εξετάζεται η παράσταση των ακεραίων από δυαδικές τετραγωνικές μορφές και αποδεικνύεται ότι κάθε φυσικός γράφεται ως άθροισμα τεσσάρων τετραγώνων. Μερικές σημαντικές διοφαντικές εξισώσεις μελετώνται στο όγδοο κεφάλαιο. Τέλος, στο τελευταίο κεφάλαιο παρουσιάζεται η στοιχειώδη θεωρία των συνεχών κλασμάτων.

Θεωρώ χρέος μου ν' απευθύνω θερμές ευχαριστίες στον καθηγητή κ. Συμεών Μποζαπαλίδη για την συμπαράσταση του και τις χρήσιμες συζητήσεις που είχα μαζί του, κατά την συγγραφή αυτού του βιβλίου. Επίσης ευχαριστώ θερμά τον κ. Νίκο Τζανάκη, καθηγητή του Πανεπιστημίου Κρήτης, για πολλές χρήσιμες υποδείξεις. Τέλος, ευχαριστώ τον μαθηματικό κ. Νίκο Καστάνη ο οποίος μου υπέδειξε το ιστορικό κείμενο που βρίσκεται στο εξώφυλλο.

Θεσσαλονίκη, 1996 *Δημήτριος Πουλάκης*

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1. Συστήματα Αριθμών

ΚΕΦΑΛΑΙΟ 2. Διαιρετότητα

ΚΕΦΑΛΑΙΟ 3. Αριθμητικές Συναρτήσεις

ΚΕΦΑΛΑΙΟ 4. Ισοτιμίες

ΚΕΦΑΛΑΙΟ 5. Πολυωνυμικές ισοτιμίες. Αρχικές ρίζες

ΚΕΦΑΛΑΙΟ 6. Τετραγωνικά υπόλοιπα

ΚΕΦΑΛΑΙΟ 7. Παράσταση ακεραίων από τετραγωνικές μορφές

ΚΕΦΑΛΑΙΟ 8. Διοφαντικές Εξισώσεις

ΚΕΦΑΛΑΙΟ 9. Συνεχή Κλάσματα

ΚΕΦΑΛΑΙΟ 1

Συστήματα Αριθμών

1. Εισαγωγή

Η Θεωρία Αριθμών αποτελεί έναν από τους αρχαιότερους κλάδους των Μαθηματικών. Αντικείμενο μελέτης της στοιχειώδους Θεωρίας Αριθμών είναι το σύνολο των φυσικών αριθμών $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, ή γενικότερα το σύνολο των ακεραίων αριθμών $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$. Γι' αυτή τη μελέτη είναι συχνά χρήσιμο να θεωρούμε το $\mathbb{Z}$ ως υποσύνολο ενός περιεκτικοτέρου συνόλου, όπως το συνόλο των ρητών αριθμών

$$\mathbb{Q} = \{x / \ x = a/b, \quad \text{με } a, b \in \mathbb{Z} \ \text{ και } \ b \neq 0\}.$$

Σκοπός αυτού του κεφαλαίου είναι να παρουσιάσει μία αξιωματική θεμελίωση των παραπάνω συνόλων και να περιγράψει τις βασικές ιδιότητες της διάταξης, της πρόσθεσης και του πολλαπλασιασμού σ' αυτά. Επίσης, εισάγονται στοιχειώδεις αλγεβρικές έννοιες, που είναι στενά συνδεδεμένες με ορισμένες από τις έννοιες που θα εξετάσουμε στα επόμενα κεφάλαια.

2. Φυσικοί αριθμοί

Έστω $\varphi : X \to Y$ μία απεικόνιση. Υπενθυμίζουμε ότι η φ καλείται *ένεση* αν για κάθε $x, y \in X$, με $x \neq y$, έχουμε $\varphi(x) \neq \varphi(y)$ και *έφεση* αν για κάθε $y \in Y$, υπάρχει $x \in X$, με $\varphi(x) = y$. Επίσης, η φ λέγεται *αμφίεση* αν είναι ταυτόχρονα ένεση και έφεση.

Μία αξιωματική θεμελίωση του συνόλου των φυσικών αριθμών, δόθηκε για πρώτη φορά το 1882, από τον G. Peano.

Τα Αξιώματα του Peano. Το σύστημα $\mathbb{N}$ των φυσικών αριθμών είναι ένα σύνολο $\mathbb{N}$, εφοδιασμένο με μία απεικόνιση $\sigma : \mathbb{N} \to \mathbb{N}$ και ένα στοιχείο $0 \in \mathbb{N}$, τέτοια, ώστε

(1) η απεικόνιση σ είναι ένεση,

(2) $0 \notin \sigma(\mathbb{N})$,

(3) αν $S \subseteq \mathbb{N}$ με τις ιδιότητες

α) $0 \in S$ και

β) $\sigma(n) \in S$ για κάθε $n \in S$,

τότε $S = \mathbb{N}$.

Η απεικόνιση σ καλείται *απεικόνιση διαδοχής* και το $\sigma(x)$ *διάδοχος* του x. Το αξίωμα (3) καλείται *Αρχή της Μαθηματικής Επαγωγής*. Απ' αυτό έπεται ότι το $\mathbb{N}$ είναι απλώς το σύνολο

$$\{0, \sigma(0), \sigma(\sigma(0)), \sigma(\sigma(\sigma(0))) \ldots\}.$$

Θέτοντας $\sigma(0) = 1$, $\sigma(1) = 2$, $\sigma(2) = 3$, ... επανερχόμαστε στη συνηθισμένη γραφή των φυσικών αριθμών. Επίσης, η Αρχή της Μαθηματικής Επαγωγής αποτελεί τη βάση μιας αποδεικτικής μεθόδου που καλείται *Μέθοδος της Μαθηματικής Επαγωγής* και εφαρμόζεται για την απόδειξη προτάσεων $P(n)$ που εξαρτώνται από το φυσικό n. Πιο συγκεκριμένα, θεωρούμε το σύνολο

$$S = \{n \in \mathbb{N} / P(n) \text{ αληθής}\}.$$

Αποδεικνύοντας ότι $0 \in S$ και ότι για κάθε $n \in S$ το $n+1 \in S$, η Αρχή της Μαθηματικής Επαγωγής δίνει $S = \mathbb{N}$. Επομένως, η πρόταση $P(n)$ είναι αληθής για κάθε $n \in \mathbb{N}$.

Στο σύνολο $\mathbb{N}$ ορίζεται μία πράξη, που καλείται *πρόσθεση* και συμβολίζεται με «+», με την βοήθεια των σχέσεων:

(1) $m+0 = m$ για κάθε $m \in \mathbb{N}$,

(2) $m+\sigma(n) = \sigma(m+n)$ για κάθε $n, m \in \mathbb{N}$.

Το αποτέλεσμα m+n της πρόσθεσης δύο φυσικών m και n καλείται *άθροισμά* τους. Ο ορισμός αυτός της πρόσθεσης καλείται *επαγωγικός* γιατί το άθροισμα των m και σ(n) ορίζεται με βάση τον ορισμό του αθροίσματος των n και m. Χρησιμοποιώντας λοιπόν τις σχέσεις (1) και (2) μπορούμε να υπολογίσουμε το αθροισμά δύο οποιωνδήποτε φυσικών αριθμών. Για παράδειγμα, ας υπολογίσουμε το άθροισμα των φυσικών 2 και 3. Είναι

$$3+2 = 3+\sigma(1) = \sigma(3+1) = \sigma(3+\sigma(0)) = \sigma(\sigma(3+0)) = \sigma(\sigma(3)) = \sigma(4) = 5,$$

όπως περιμέναμε.

Στο σύνολο $\mathbb{N}$ ορίζεται επαγωγικά και μία άλλη πράξη, που καλείται *πολλαπλασιασμός* και συμβολίζεται με «·», με την βοήθεια των σχέσεων:

(3) $m \cdot 0 = 0$ για κάθε $m \in \mathbb{N}$,

(4) $m \cdot \sigma(n) = m \cdot n + m$ για κάθε $n, m \in \mathbb{N}$.

Το αποτέλεσμα $m\cdot n$ του πολλαπλασιασμού δύο φυσικών m και n καλείται *γινόμενο* τους. Συνήθως το γινόμενο $m\cdot n$ συμβολίζεται πιο απλά mn. Για να πολλαπλασιάσουμε λοιπόν δύο φυσικούς χρησιμοποιούμε τις σχέσεις (3) και (4). Για παράδειγμα, έχουμε

$$3\cdot 2 = 3\cdot\sigma(1) = 3\cdot 1+3 = 3\cdot\sigma(0)+3 = (3\cdot 0+3)+3 = (0+3)+3 = 3+3.$$

Καθώς δείξαμε παραπάνω, $3+2 = 5$. Οπότε

$$3+3 = 3+\sigma(2) = \sigma(3+2) = \sigma(5) = 6.$$

Οι βασικότερες ιδιότητες της πρόσθεσης και του πολλαπλασιασμού δίνονται στη παρακάτω πρόταση.

ΠΡΟΤΑΣΗ 2.1. *Για κάθε* $x, y, z\in\mathbb{N}$ *ισχύουν τα παρακάτω:*

(α) $x+(y+z) = (x+y)+z$, $x(yz) = (xy)z$ *(προσεταιριστικος νόμος),*

(β) $x+y = y+x$, $xy = yx$ *(αντιμεταθετικός νόμος),*

(γ) $x(y+z) = xy+xz$ *(επιμεριστικός νόμος),*

(δ) $x+y = x+z \Rightarrow y = z$, $x \neq 0$ *και* $xy = xz \Rightarrow y = z$ *(νόμος διαγραφής).*

ΑΠΟΔΕΙΞΗ. (α) Έστω S το σύνολο των φυσικών k, που έχουν την ιδιότητα

$$x+(y+k) = (x+y)+k.$$

Καθώς

$$x+(y+0) = x+y = (x+y)+0,$$

έχουμε $0\in S$. Ας υποθέσουμε ότι $k\in S$. Οπότε

$$x+\big(y+\sigma(k)\big) = x+\sigma(y+k) = \sigma\big(x+(y+k)\big) = \sigma\big((x+y)+k\big) = (x+y)+\sigma(k).$$

Άρα $\sigma(k)\in S$. Επομένως, σύμφωνα με την Αρχή της Μαθηματικής Επαγωγής, έχουμε $S = \mathbb{N}$.

Συμβολίζουμε με T, το σύνολο των φυσικών k, που έχουν την ιδιότητα

$$x(yk) = (xy)k.$$

Καθώς

$$x(y0) = x0 = 0 = (xy)0,$$

έπεται $0\in T$. Ας υποθέσουμε ότι $k\in T$. Οπότε

$$x\big(y\sigma(k)\big) = x(yk+y) = x(yk)+xy = (xy)k+xy = (xy)\,\sigma(k) = (xy)\,(k+1) =$$

$$= (xy)\,\big(k+\sigma(0)\big) = (xy)\,\sigma(k),$$

δηλαδή $\sigma(k)\in T$. Συνεπώς $T = \mathbb{N}$.

Η απόδειξη των υπολοίπων ιδιοτήτων αφήνεται ως άσκηση.

ΠΡΟΤΑΣΗ 2.2. *Έστω* $m, n \in \mathbb{N}$. *Τότε*

(α) $m+n = 0 \Leftrightarrow m = 0$ *και* $n = 0$.

(β) $mn = 0 \Leftrightarrow m = 0$ *ή* $n = 0$.

ΑΠΟΔΕΙΞΗ. (α) Έστω $m+n = 0$. Αν $n \neq 0$, τότε υπάρχει $k \in \mathbb{N}$, με $\sigma(k) = n$, οπότε

$$\sigma(m+k) = m+\sigma(k) = m+n = 0.$$

Αυτό όμως είναι άτοπο, γιατί $0 \notin \sigma(\mathbb{N})$. Άρα $n = 0$. Ομοίως, έχουμε $m = 0$. Αντιστρόφως, αν $m = n = 0$, τότε $0+0 = 0$.

(β) Έστω $m = 0$ ή $n = 0$. Τότε, από τον ορισμό του πολλαπλασιασμού, παίρνουμε $mn = 0$. Αντιστρόφως, ας υποθέσουμε ότι $mn = 0$. Αν $n \neq 0$, τότε υπάρχει $k \in \mathbb{N}$, με $\sigma(k) = n$, οπότε

$$0 = mn = m\sigma(k) = mk+m.$$

Σύμφωνα με την (α), έχουμε $mk = 0$ και $m = 0$.

Έστω $m, n \in \mathbb{N}$. Λέμε ότι ο φυσικός m είναι *μικρότερος* του n και γράφουμε $m < n$, ή ο n *μεγαλύτερος* του m και γράφουμε $n > m$, αν υπάρχει $k \in \mathbb{N}$, με $k \neq 0$ έτσι, ώστε $n = m+k$. Ο φυσικός k, αν υπάρχει, είναι μοναδικός και συμβολίζεται με $n-m$. Πραγματικά, αν υπάρχουν $x, y \in \mathbb{N}$, με $n = m+x$ και $n = m+y$, τότε $m+x = m+y$. Οπότε η Πρόταση 2.1.(δ) συνεπάγεται $x = y$. Επίσης, αν ισχύει $m = n$ ή $m < n$, γράφουμε $m \leq n$ ή $n \geq m$.

ΠΡΟΤΑΣΗ 2.3. *(Νόμος της τριχοτομίας) Για κάθε ζεύγος* $m, n \in \mathbb{N}$ *ισχύει μόνο μία από τις εξής σχέσεις:*

$$m < n, \ m = n, \ m > n.$$

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς παρατηρούμε ότι το πολύ μία από τις παραπάνω σχέσεις ισχύει. Πραγματικά, ας υποθέσουμε ότι $m < n$ και $m = n$. Τότε υπάρχει $k \in \mathbb{N}$, με $k \neq 0$ ώστε $n = m+k$. Καθώς $n = m$ και $n = m+k$, ο νόμος της διαγραφής δίνει $k = 0$, που δεν αληθεύει. Ας υποθέσουμε στη συνέχεια, ότι $m < n$ και $m > n$. Τότε υπάρχουν $k, l \in \mathbb{N}$, με $k \neq 0$ και $l \neq 0$ έτσι, ώστε $n = m+k$ και $m = n+l$, οπότε

$$n = m+k = (n+l)+k = n+(l+k) \Rightarrow l+k = 0$$

και σύμφωνα με την Πρόταση 2.2, έχουμε $k = l = 0$, που είναι άτοπο.

Μένει να δείξουμε ότι τουλάχιστον μία από τις παραπάνω σχέσεις αληθεύει. Αν $m = 0$, τότε $m \leq n$. Ας υποθέσουμε ότι $m \neq 0$. Θεωρούμε το σύνολο

$$S(m) = \{k \in \mathbb{N} / \ m < k \ \text{ή} \ m = k \ \text{ή} \ m > k\}.$$

Επειδή $m+0 = m$, έχουμε $m > 0$ και επομένως $0 \in S(m)$. Έστω $k \in S(m)$. Θα δείξουμε ότι $\sigma(k) \in S(m)$. Καθώς $k \in S(m)$, μία από τις σχέσεις

$$m < k, m = k, m > k,$$

αληθεύει. Αν $m < k$, τότε υπάρχει $x \in \mathbb{N}$, με $x \neq 0$ έτσι, ώστε $m+x = k$. Είναι

$$m+\sigma(x) = \sigma(m+x) = \sigma(k),$$

απ' όπου $m < \sigma(k)$. Αν $m = k$, τότε $m+1 = \sigma(m) = \sigma(k)$ και επομένως $m < \sigma(k)$. Τέλος, ας υποθέσουμε ότι $m > k$. Τότε υπάρχει $x \in \mathbb{N}$, με $x \neq 0$ έτσι, ώστε $k+x = m$. Είναι

$$\sigma(k)+x = \sigma(k+x) = \sigma(m) = m+1.$$

Καθώς $x \neq 0$, υπάρχει $r \in \mathbb{N}$ ώστε $x = \sigma(r)$. Επομένως

$$(\sigma(k)+r)+1 = \sigma(k)+(r+1) = \sigma(k)+\sigma(r) = \sigma(k)+x = m+1,$$

απ' όπου, σύμφωνα με την Πρόταση 2.1.(δ), παίρνουμε $\sigma(k)+r = m$. Συνεπώς έχουμε $\sigma(k) = m$ ή $\sigma(k) < m$. Άρα $\sigma(k) \in S(m)$. Έτσι, σύμφωνα με την Αρχή της Μαθηματικής Επαγωγής, έχουμε $S(m) = \mathbb{N}$.

Μερικές βασικές ιδότητες των σχέσεων «<» και «≤» δίνονται στις ασκήσεις 1, 2 και 3. Η παρακάτω πρόταση, θα χρησιμοποιηθεί πολλές φορές στα επόμενα.

ΠΡΟΤΑΣΗ 2.4. *(Αρχή της καλής διάταξης) Έστω S ένα μη κενό υποσύνολο του $\mathbb{N}$. Τότε το S έχει ένα μοναδικό ελάχιστο στοιχείο, δηλαδή, ένα στοιχείο $\alpha \in S$ τέτοιο, ώστε $\alpha \leq x$, για κάθε $x \in S$.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι το S δεν έχει ελάχιστο στοιχείο. Θεωρούμε το σύνολο:

$$M = \{n \in \mathbb{N} \,/\, m \geq n, \text{ για κάθε } m \in S\}.$$

Προφανώς $0 \in M$. Υποθέτουμε ότι $k \in M$. Τότε $m \geq k$, για κάθε $m \in S$. Αν $k \in S$, τότε το k είναι ελάχιστο στοιχείο του S, άτοπο. Άρα $k \notin S$ και επομένως $m > k$, για κάθε $m \in S$. Συνεπώς $m \geq k+1$, για κάθε $m \in S$. Δηλαδή $k+1 \in M$. Σύμφωνα λοιπόν με την Αρχή της Μαθηματικής Επαγωγής, έχουμε $M = \mathbb{N}$. Ειδικότερα, αν m είναι τυχόν στοιχείο του S, ισχύει $m \geq m+1$, άτοπο. Συνεπώς, το S έχει ελάχιστο στοιχείο. Αν το S έχει δύο ελάχιστα στοιχεία a και b, τότε $a \geq b$ και $a \leq b$, οπότε η Πρόταση 2.3 δίνει $a = b$.

Στη συνέχεια θα δώσουμε δύο χρήσιμες παραλλαγές της Αρχής της Μαθηματικής Επαγωγής. Συμβολίζουμε με $\mathbb{N}(m)$ το σύνολο των φυσικών n με $n \geq m$.

ΠΡΟΤΑΣΗ 2.5. *Έστω* S *ένα μη κενό υποσύνολο του* $\mathbb{N}$ *και* n_0 *το ελάχιστο στοιχείο του. Αν για κάθε* $n \in S$, *το* $n+1 \in S$, *τότε* $S = \mathbb{N}(n_0)$.

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι $S \neq \mathbb{N}(n_0)$. Σύμφωνα με την Πρόταση 2.4, το σύνολο $\mathbb{N}(n_0)-S$ έχει ελάχιστο στοιχείο και ας είναι αυτο το m. Καθώς $n_0 \in S$, έχουμε $m > n_0$. Επομένως $m-1 \notin \mathbb{N}(n_0)-S$ και $m-1 \geq n_0$. Άρα $m-1 \in S$. Από την υπόθεση μας παίρνουμε $m \in S$ που είναι άτοπο. Συνεπώς $S = \mathbb{N}(n_0)$.

Παράδειγμα 2.1. Θα δείξουμε ότι για $n \geq 4$ ισχύει $(3/2)^n > n+1$. Για $n = 4$ έχουμε $(3/2)^4 = 81/16 > 5 = 4+1$. Υποθέτουμε ότι για $n = k$ η ανισότητα αληθεύει. Έχουμε

$$\left(\frac{3}{2}\right)^{k+1} > \frac{3}{2}(k+1) \geq k+1+\frac{5}{2} > k+2.$$

Δηλαδή η ανισότητα αληθεύει για $n = k+1$. Επομένως, σύμφωνα με την Πρόταση 2.5, η ανισότητα αληθεύει για κάθε $n \geq 4$. Επίσης, παρατηρούμε ότι για $n \leq 3$ η ανισότητα δεν ισχύει.

ΠΡΟΤΑΣΗ 2.6. *Έστω* S *ένα μη κενό υποσύνολο του* $\mathbb{N}$ *και* n_0 *το ελάχιστο στοιχείο του. Ας υποθέσουμε ότι το* S *έχει την εξής ιδιότητα:*

$$\text{για κάθε } n \in \mathbb{N} \text{ με } n_0+1, \ldots, n-1 \in S \Rightarrow n \in S.$$

Τότε $S = \mathbb{N}(n_0)$.

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι $S \neq \mathbb{N}(n_0)$. Σύμφωνα με την Πρόταση 2.4, το σύνολο $\mathbb{N}(n_0)-S$ έχει ελάχιστο στοιχείο και ας είναι αυτο το m. Επειδή $n_0 \in S$, έχουμε $m > n_0$. Επομένως $m-1 \notin \mathbb{N}(n_0)-S$ και $m-1 \geq n_0$, άρα $n \in S$ για κάθε φυσικό n, με $n_0 \leq n \leq m-1$. Από την υπόθεση μας παίρνουμε $m \in S$, άτοπο. Συνεπώς $S = \mathbb{N}(n_0)$.

Παράδειγμα 2.2. Η ακολουθία του Fibonacci F_n ορίζεται ως εξής:

$$F_1 = F_2 = 1 \text{ και } F_{n+1} = F_n+F_{n-1}, \quad \text{για κάθε } n \geq 2.$$

Θα δείξουμε ότι $F_n < (7/4)^n$ για κάθε $n \geq 1$. Η ανισότητα ισχύει για $n = 1, 2$. Υποθέτουμε ότι $F_m < (7/4)^m$, για κάθε φυσικό m, με $2 \leq m < n$. Οπότε

$$F_n = F_{n-1}+F_{n-2} < (7/4)^{n-1}+(7/4)^{n-2} = (7/4)^{n-2}\,(11/4) < (7/4)^n.$$

Έτσι, σύμφωνα με την Πρόταση 2.6, έχουμε $F_n < (7/4)^n$ για κάθε $n \geq 1$.

3. Σχέσεις ισοδυναμίας

Έστω Σ ένα μη κενό σύνολο. Ένα υποσύνολο S του $\Sigma \times \Sigma$ καλείται *σχέση ισοδυναμίας,* αν έχει τις εξής ιδιότητες:

(1) $(x, x) \in S$ για κάθε $x \in \Sigma$ (ανακλαστική),

(2) αν $(x, y) \in S \Rightarrow (y, x) \in S$ (συμμετρική),

(3) αν $(x, y) \in S$ και $(y, z) \in S \Rightarrow (x, z) \in S$ (μεταβατική).

Συνήθως αντί $(x, y) \in S$, γράφουμε $x \equiv y\ (S)$. Δύο στοιχεία που συνδέονται με την σχέση ισοδυναμίας S λέγονται *ισοδύναμα* ως προς την σχέση S.

Παράδειγμα 3.1. Έστω E το σύνολο των τριγώνων του επιπέδου. Θεωρούμε την σχέση:

$$x \equiv y\ (S) \Leftrightarrow \text{το } x \text{ είναι όμοιο προς το } y.$$

Η σχέση S είναι μία σχέση ισοδυναμίας. Πράγματι, έχουμε:

(i) Κάθε τρίγωνο είναι όμοια με τον εαυτό του. Άρα $x \equiv x\ (S)$ για κάθε $x \in E$.

(ii) Αν $x \equiv y\ (S) \Rightarrow$ το x είναι όμοιο προς το y. Τότε όμως και το y είναι όμοιο προς το x. Οπότε $y \equiv x\ (S)$.

(iii) Έστω $x \equiv y\ (S)$ και $y \equiv z\ (S)$. Τότε το x είναι όμοιο προς το y και το y όμοιο προς το z. Επομένως, το x είναι όμοιο προς το z. Συνεπώς $x \equiv z\ (S)$.

Ας θεωρήσουμε τώρα την εξής σχέση:

$$x \equiv y\ (P) \Leftrightarrow \text{το } x \text{ έχει μία πλευρά κοινή με το } y.$$

Αυτή η σχέση δεν είναι μία σχέση ισοδυναμία στο σύνολο E, γιατί δεν ισχύει η μεταβατικότητα.

Καλούμε *κλάση ισοδυναμίας* ενός στοιχείου $a \in \Sigma$ και τη συμβολίζουμε με $[a]$ το σύνολο

$$[a] = \{x \in \Sigma / \ x \equiv a\ (S)\}.$$

Καλούμε *σύνολο πηλίκο* του Σ με την S και το συμβολίζουμε με Σ/S, το σύνολο που έχει για στοιχεία τις κλάσεις ισοδυναμίας της S.

ΠΡΟΤΑΣΗ 3.1. *Αν* $[x] \cap [y] \neq \varnothing$, *τότε* $[x] = [y]$.

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε $[x] \cap [y] \neq \varnothing$. Αν $z \in [x] \cap [y]$, τότε $z \in [x]$ και $z \in [y]$. Επομένως $z \equiv x\ (S)$ και $z \equiv y\ (S)$. Η συμμετρική ιδιότητα δίνει $x \equiv z\ (S)$. Άρα $x \equiv z\ (S)$ και $z \equiv y\ (S)$. Οπότε, από τη μεταβατική ιδιότητα έπεται $x \equiv y\ (S)$.

Έστω $a \in [x]$. Τότε $a \equiv x\ (S)$. Καθώς $x \equiv y\ (S)$, παίρνουμε $a \equiv y\ (S)$ και επομένως $a \in [y]$. Άρα $[x] \subseteq [y]$. Με τον ίδιο τρόπο αποδεικνύεται ότι ισχύει

$[y] \subseteq [x]$. Συνεπώς $[x] = [y]$.

Επομένως, οι κλάσεις ισοδυναμίας των στοιχείων του Σ (ως προς την ισοδυναμία S) έχουν τις εξής ιδιότητες:

(α) $[x] \neq \varnothing$ για κάθε $x \in \Sigma$,

(β) $\bigcup\limits_{x \in \Sigma} [x] = \Sigma$,

(γ) $[x] \neq [y] \Rightarrow [x] \cap [y] = \varnothing$.

Μία συλλογή υποσυνόλων του Σ που έχει τις ιδιότητες (α), (β) και (γ) καλείται *διαμέριση* του Σ. Έτσι, βλέπουμε ότι μία σχέση ισοδυναμίας στο Σ, ορίζει μία διαμέριση του Σ. Αντιστρόφως, αν $\{U_a\}_{a \in A}$ είναι μία διαμέριση του Σ, τότε η σχέση R που ορίζεται ως εξής:

$$x \equiv y \ (R) \Leftrightarrow x \text{ και } y \text{ βρίσκονται στο ίδιο σύνολο } U_a$$

είναι μία σχέση ισοδυναμίας που οι κλάσεις ισοδυναμίας της είναι τα σύνολα U_a (βλ. άσκηση 8). Μπορούμε λοιπόν να ορίσουμε τόσες σχέσεις ισοδυναμίας επί ενός συνόλου, όσοι ακριβώς είναι οι τρόποι με τους οποίους μπορούμε να το διαμερίσουμε.

ΠΡΟΤΑΣΗ 3.2. *Έστω S μία σχέση ισοδυναμίας επί του Σ. Τότε για κάθε $x, y \in \Sigma$ έχουμε*

$$x \equiv y \ (S) \Leftrightarrow [x] = [y].$$

ΑΠΟΔΕΙΞΗ. Αν $x \equiv y \ (S)$, τότε $y \in [x]$ και επομένως $[x] \cap [y] \neq \varnothing$. Άρα, σύμφωνα με την Πρόταση 3.1, έχουμε $[x] = [y]$. Αντιστρόφως, αν $[x] = [y]$, τότε $y \in [x]$. Άρα $x \equiv y \ (S)$.

Παράδειγμα 3.2. Θεωρούμε μία απεικόνιση $\varphi : X \to Y$. Ορίζουμε μία σχέση R στο X ως εξής:

$$x \equiv y \ (R) \Leftrightarrow \varphi(x) = \varphi(y).$$

Εύκολα διαπιστώνουμε ότι η R είναι μία σχέση ισοδυναμίας. Οι κλάσεις ισοδυναμίας της R είναι:

$$[x] = \{z \in X / \ \varphi(z) = \varphi(x)\},$$

επομένως, το σύνολο πηλίκο X/R αποτελείται από τα σύνολα:

$$R(y) = \{z \in X / \ \varphi(z) = y\}, \ \ y \in \varphi(X).$$

4. Ακέραιοι αριθμοί

Έστω $m, n \in \mathbb{N}$ και ας θεωρήσουμε την εξίσωση

$$m+x = n.$$

Παρατηρούμε ότι αυτή η εξίσωση δεν έχει πάντα λύση στο $\mathbb{N}$. Δηλαδή, δεν υπάρχει πάντα $x \in \mathbb{N}$ ώστε $m+x = n$. Για παράδειγμα, αν υποθέσουμε ότι υπάρχει φυσικός x που επαληθεύει την εξίσωση $3+x = 1$, τότε ο νόμος της διαγραφής (Πρόταση 2.1) δίνει $2+x = 0$, οπότε, σύμφωνα με την Πρόταση 2.2, έχουμε $2 = 0$, άτοπο. Άρα η εξίσωση $3+x = 1$ δεν έχει λύση.

Σκοπός μας σ' αυτή την παραγράφο είναι να δώσουμε, με τη βοήθεια του $\mathbb{N}$, μία κατασκευή ενός συνόλου πιό "μεγάλου" από το $\mathbb{N}$, του συνόλου των ακεραίων αριθμών, μεσα στο οποίο η παραπάνω εξίσωση θα έχει λύση. Θεωρούμε λοιπόν το καρτεσιανό γινόμενο $\mathbb{N}\times\mathbb{N}$ και ορίζουμε την εξής σχέση σ' αυτό:

$$(a, b) \sim (c, d) \Leftrightarrow a+d = b+c.$$

Εύκολα διαπιστώνουμε ότι η σχέση $\sim$ είναι μία σχέση ισοδυναμίας. Ορίζουμε το σύνολο $\mathbb{Z}$ των ακεραίων ως το σύνολο πηλίκο του $\mathbb{N}\times\mathbb{N}$ με την σχέση $\sim$. Στο σύνολο $\mathbb{Z}$ ο ρίζουμε τις εξής πράξεις:

$[(a, b)]+[(c, d)] = [(a+c, b+d)]$ (πρόσθεση)

$[(a, b)]\,[(c, d)] = [(ac+bd, ad+bc)]$ (πολλαπλασιασμός).

Θα δείξουμε ότι τα αποτελέσματα των παραπάνω πράξεων, δεν εξαρτώνται από τους αντιπροσώπους των κλάσεων που χρησιμοποιήσαμε, παρά μόνο από τις κλάσεις. Έστω $[(a, b)] = [(a', b')]$ και $[(c, d)] = [(c', d')]$. Τότε $(a, b) \sim (a', b')$ και $(c, d) \sim (c', d')$, απ' όπου

$$a+b' = b+a' \text{ και } c+d' = d+c'.$$

Προσθέτοντας κατά μέλη παίρνουμε

$$a+b'+c+d' = b+a'+d+c',$$

οπότε $(a+c, b+d) \sim (a'+c', b'+d')$ και επομένως $[(a+c, b+d)] = [(a'+c', b'+d')]$. Στη συνέχεια, προσθέτοντας κατά μέλη τις ισότητες

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

παίρνουμε, ύστερα από απλοποίηση,

$$ac+bd+a'd'+b'c' = a'c'+b'd'+ad+bc.$$

Άρα $(ac+bd, ad+bc) \sim (a'c'+b'd', a'd'+b'c')$ και επομένως

$$[(ac+bd, ad+bc)] = [(a'c'+b'd', a'd'+b'c')].$$

Δείξαμε λοιπόν ότι οι παραπάνω πράξεις είναι καλά ορισμένες.

Εύκολα αποδεικνύεται ότι για κάθε $x, y, z \in \mathbb{Z}$ ισχύουν τα παρακάτω:

(1) $x+(y+z) = (x+y)+z$, $x(yz) = (xy)z$ (προσεταιριστικος νόμος),

(2) $x+y = y+x$, $xy = yx$ (αντιμεταθετικός νόμος),

(3) $x(y+z) = xy+xz$ (επιμεριστικός νόμος),

Οι κλάσεις $[(0, 0)]$ και $[(1, 0)]$ είναι ουδέτερα στοιχεία για την πρόσθεση και τον πολλαπλασιασμό αντίστοιχα. Δηλαδή

$$[(a, b)]+[(0, 0)] = [(a, b)] \quad \text{και} \quad [(a, b)][(1, 0)] = [(a, b)],$$

για κάθε $[(a, b)] \in \mathbb{Z}$. Επίσης, για κάθε $[(a, b)] \in \mathbb{Z}$ έχουμε

$$[(a, b)]+[(b, a)] = [(a+b, a+b)] = [(0, 0)].$$

και γράφουμε $[(b, a)] = -[(a, b)]$. Το $[(b, a)]$ καλείται *αντίθετο* του $[(a, b)]$. Άλλες ιδιότητες της πρόσθεσης και του πολλαπλασιασμού δίνονται στις ασκήσεις 9, και 10. Τέλος, αν $a, b \in \mathbb{Z}$ η εξίσωση

$$a+x = b$$

έχει μοναδική λύση στο $\mathbb{Z}$. Πραγματικά, προσθέτοντας και στα δύο μέλη το $-a$, παίρνουμε $x = b+(-a)$.

Έστω $[(a, b)], [(c, d)] \in \mathbb{Z}$. Λέμε ότι η κλάση $[(a, b)]$ είναι *μικρότερη* από την $[(c, d)]$ και γραφουμε $[(a, b)] < [(c, d)]$, ή ότι η $[(c, d)]$ είναι *μεγαλύτερη* της $[(a, b)]$ και γράφουμε $[(c, d)] > [(a, b)]$, αν ισχύει $a+d < b+c$. Αυτός ο ορισμός δεν εξαρτάται από τους αντιπροσώπους των κλάσεων, παρά μόνο από τις κλάσεις. Πραγματικά, αν $(a, b) \sim (a', b')$ και $(c, d) \sim (c', d')$, τότε

$$a+b' = b+a' \quad \text{και} \quad c+d' = d+c'.$$

Προσθέτοντας κατά μέλη παίρνουμε

$$a+b'+c'+d = b+a'+d'+c.$$

Καθώς $a+d < b+c$, υπάρχει $k \in \mathbb{N}$ με $k \neq 0$ ώστε $a+d+k = b+c$. Άντικαθιστούμε το $b+c$ με το ίσο του στη παραπάνω ισότητα και απλοποιώντας παίρνουμε

$$b'+c' = a'+d'+k.$$

Δηλαδή $b'+c' < a'+d'$ και επομένως $[(a', b')] < [(c', d')]$. Επίσης, αν $x, y \in \mathbb{Z}$ με $x = y$ ή $x < y$ γράφουμε $x \leq y$ ή $y \geq x$. Μερικές βασικές ιδιότητες των σχέσεων «<» και «≤» δίνονται στις ασκήσεις 11, 12, 13 και 14. Ένας ακέραιος x καλείται *θετικός* αν $x > 0$ και *αρνητικός* αν $x < 0$.

Έστω $x = [(a, b)]$ ένα στοιχείο του $\mathbb{Z}$. Σύμφωνα με τον νόμο της τριχοτομίας (Πρόταση 2.3) ισχύει μόνο μία από τις σχέσεις

$$a < b, \quad a = b, \quad a > b.$$

Αν $a < b$, τότε υπάρχει $k \in \mathbb{N}$, με $k \neq 0$ έτσι, ώστε $a+k = b$. Οπότε

$$[(a, b)] = [(a, a+k)] = [(0, k)].$$

Ομοίως, αν $a > b$ υπάρχει $n \in \mathbb{N}$, με $n \neq 0$ έτσι, ώστε $b+n = a$ και επομένως

$$[(a, b)] = [(a+n, a)] = [(n, 0)].$$

Συμπερασματικά λοιπόν, αν $a < b$ τότε $x = [(0, k)]$ με $k \neq 0$, αν $a = b$ τότε $x = [(0, 0)]$ και αν $a > b$ τότε $x = [(n, 0)]$ με $n \neq 0$. Παρατηρούμε επίσης ότι αυτές οι κλάσεις είναι ανά δύο άνισες. Συνεπώς, τα διακεκριμμένα στοιχεία του $\mathbb{Z}$ είναι οι κλάσεις $[(0, 0)]$, $[(n, 0)]$ και $[(0, n)]$, με $n \neq 0$. Στη συνέχεια θεωρούμε την απεικόνιση $\varphi : \mathbb{N} \to \mathbb{Z}$ που ορίζεται από

$$\varphi(n) = [(n, 0)], \text{ για κάθε } n \in \mathbb{N}.$$

Αν $\varphi(n) = \varphi(m)$, τότε $[(n, 0)] = [(m, 0)]$ και επομένως $n = m$. Δηλαδή, η απεικόνιση φ είναι ένεση. Επίσης, εύκολα αποδεικνύονται τα εξής:

(1) $\varphi(n+m) = \varphi(n)+\varphi(m)$, για κάθε $m, n \in \mathbb{N}$,

(2) $\varphi(nm) = \varphi(n)\,\varphi(m)$, για κάθε $m, n \in \mathbb{N}$,

(3) $n < m \Rightarrow \varphi(n) < \varphi(m)$.

Βλέπουμε λοιπόν ότι η ένεση φ αντιστοιχεί ανισότητες, αθροίσματα και γινόμενα μεταξύ των συνόλων $\mathbb{N}$ και $\varphi(\mathbb{N}) = \{[(n,0)]/ n \in \mathbb{N}]$ επακριβώς και αμοιβαία. Έτσι, στη πράξη θα ταυτίζουμε τον φυσικό n με την κλάση $[(n, 0)]$ και θα θεωρούμε το $\mathbb{N}$ ως υποσύνολο του $\mathbb{Z}$. Απλοποιώντας την γραφή για τα στοιχεία του $\mathbb{Z}$ σημειώνουμε $-n, 0, n$ αντί $[(0, n)]$, $[(0, 0)]$, $[(n, 0)]$ αντίστοιχα και κατ' αυτό τον τρόπο παίρνουμε την συνηθισμένη γραφή των ακεραίων. Τέλος, παρατηρούμε ότι το σύνολο των θετικών ακεραίων αποτελείται από τους ακέραιους 1, 2, 3, … ενώ το σύνολο των αρνητικών από τους –1, –2, –3, … όπως άλλωστε περιμέναμε.

5. Ρητοί αριθμοί

Η εξίσωση

$$ax = b,$$

όπου $a, b \in \mathbb{Z}$ και $a \neq 0$ δεν έχει πάντα λύση στο $\mathbb{Z}$. Π.χ. η εξίσωση $3x = 2$. Σ' αυτή την παράγραφο περιγράφουμε, με την βοήθεια του $\mathbb{Z}$, την κατασκευή ενός συνόλου πιό "μεγάλου" από το $\mathbb{Z}$, του συνόλου των ρητών αριθμών, μεσα στο οποίο η παραπάνω εξίσωση θα έχει λύση. Έστω $\mathbb{Z}^*$ το σύνολο των μη μηδενικών ακεραίων. Ορίζουμε την εξής σχέση επί του $\mathbb{Z}\times\mathbb{Z}^*$:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Εύκολα αποδεικνύεται ότι η σχέση $\sim$ είναι μία σχέση ισοδυναμίας. Ορίζουμε το σύνολο $\mathbb{Q}$ των ρητών ως το σύνολο πηλίκο του $\mathbb{Z}\times\mathbb{Z}^*$ με την $\sim$. Στο σύνολο $\mathbb{Q}$ η πρόσθεση και ο πολλαπλασιασμός ορίζονται ως εξής:

$$[(a, b)]+[(c, d)] = [(ad+bc, bd)] \qquad (\text{πρόσθεση})$$

$$[(a, b)][(c, d)] = [(ac, bd)] \qquad (\text{πολλαπλασιασμός}).$$

Οι παραπάνω πράξεις είναι καλά ορισμένες. Δηλαδή, το άθροισμα και το γινόμενο δύο κλάσεων δεν εξαρτώνται από τους αντιπροσώπους που χρησιμοποιήθηκαν για να τις περιγράψουν, αλλά μόνο από τις κλάσεις. Εύκολα βλέπουμε ότι η πρόσθεση και ο πολλαπλασιασμός ικανοποιούν τους νόμους του προσεταιρισμού και της αντιμεταθετικότητας. Επίσης, ο πολλαπλασμός είναι επιμεριστικός ως πρός την πρόσθεση. Οι κλασεις $[(0, 0)]$ και $[(1, 1)]$ είναι ουδέτερα στοιχεία για την πρόσθεση και τον πολλαπλασιασμό αντιστοιχα. Για κάθε $[(a, b)]\in\mathbb{Q}$ έχουμε $[(a, b)]+[(-a, b)] = [(0, 0)]$. Το στοιχείο $[(-a, b)]$ καλείται *αντίθετο* του $[(a, b)]$ και συμβολίζεται με $-[(a, b)]$. Επίσης, για κάθε $[(a, b)]\in\mathbb{Q}$ με $a \neq 0$, ισχύει $[(a, b)]\,[(b, a)] = [(1, 1)]$. Το στοιχείο $[(b, a)]$ καλείται *αντίστροφο* του $[(a, b)]$ και συμβολίζεται με $[(a, b)]^{-1}$. Τέλος, η εξίσωση

$$ax = b,$$

όπου $a, b\in\mathbb{Q}$ με $a \neq 0$, έχει μοναδική λύση στο $\mathbb{Q}$. Πραγματικά, αν πολλαπλασιάσουμε και τα δύο μέλη με a^{-1}, παίρνουμε $x = a^{-1}b$.

Έστω $[(a, b)], [(c, d)]\in\mathbb{Q}$. Λέμε ότι η κλάση $[(a, b)]$ είναι *μικρότερη* από την $[(c, d)]$ και γραφουμε $[(a, b)] < [(c, d)]$, ή ότι η $[(c, d)]$ είναι *μεγαλύτερη* της $[(a, b)]$ και γράφουμε $[(c, d)] > [(a, b)]$, αν ισχύει $abd^2 < b^2cd$. Αυτός ο ορισμός εξαρτάται μόνο από τις κλάσεις και όχι από τους αντιπροσώπους τους. Επίσης, αν $x, y\in\mathbb{Q}$ με $x = y$ ή $x < y$ γράφουμε $x \leq y$ ή $y \geq x$.

Θεωρούμε την απεικόνιση $\psi : \mathbb{Z} \to \mathbb{Q}$ που ορίζεται από

$$\psi(a) = [(a, 1)]$$

για κάθε $a\in\mathbb{Z}$. Αν $\psi(a) = \psi(b)$, τότε $[(a, 1)] = [(b, 1)]$ και επομένως $a = b$. Συνεπώς, η απεικόνιση ψ είναι ένεση. Επίσης, η ψ έχει τις εξής ιδιότητες:

(1) $\psi(a+b) = \psi(a)+\psi(b)$, για κάθε $a, b\in\mathbb{Z}$,

(2) $\psi(ab) = \psi(a)\,\psi(b)$, για κάθε $a, b\in\mathbb{Z}$,

(3) $a < b \Rightarrow \psi(a) < \psi(b)$.

Δηλαδή, η ένεση ψ αντιστοιχεί ανισότητες, αθροίσματα και γινόμενα μεταξύ των συνόλων $\mathbb{Z}$ και $\psi(\mathbb{Z})$ επακριβώς και αμοιβαία. Έτσι, θα ταυτίζουμε τον ακέραιο a με την κλάση $[(a, 1)]$ και θα θεωρούμε το $\mathbb{Z}$ ως υποσύνολο του $\mathbb{Q}$. Απλοποιώντας την γραφή για τα στοιχεία του $\mathbb{Q}$ θα γράφουμε

$$\frac{a}{b} \ \text{ή}\ a/b \ \text{αντί}\ [(a, b)].$$

Έτσι παίρνουμε τον συνηθισμένο συμβολισμό για τους ρητούς αριθμούς.

Ενας ρητός a/b καλείται *θετικός* αν $a/b > 0$ και *αρνητικός* αν $a/b < 0$. Παρατηρούμε ότι ο a/b είναι θετικός, αν οι ακέραιοι a και b είναι ταυτόχρονα θετικοί ή αρνητικοί και αρνητικός αν μόνο ένας από τους a και b είναι αρνητικός. Αν $x\in\mathbb{Q}$, η απόλυτη τιμή του x ορίζεται ως εξής:

$$|x| = x \text{ αν } x \geq 0 \text{ και } |x| = -x \text{ αν } x < 0.$$

Ισχύουν οι ιδιότητες:

(1) $|x| \geq x$ και $|x| = |-x|$, για κάθε $x\in\mathbb{Q}$.

(2) $|xy| = |x||y|$, για κάθε $x, y\in\mathbb{Q}$.

(3) $|x+y| \leq |x|+|y|$, για κάθε $x, y\in\mathbb{Q}$.

Για κάθε $x\in\mathbb{Q}$, με $x \neq 0$, ορίζουμε το *πρόσημο* του x ως εξής:

$$\operatorname{sgn}x = 1 \text{ αν } x > 0 \text{ και } \operatorname{sgn}x = -1 \text{ αν } x < 0.$$

6. Ομάδες, Δακτύλιοι, Σώματα

Σ' αυτή την παράγραφο μελετάμε στοιχειωδώς μερικές αλγεβρικές δομές, που θα μας βοηθήσουν στην καλύτερη κατανόηση ορισμένων από τις έννοιες της Θεωρίας Αριθμών που θα εξετάσουμε.

Έστω E ένα μη κενό σύνολο. Καλούμε *(διμελή) πράξη* επί του E μία απεικόνιση $E\times E \to E$. Π.χ. η πρόσθεση και ο πολλαπλασιασμός είναι πράξεις επί του $\mathbb{Z}$. Μία πράξη έχει σπουδαιότητα μόνον όταν έχει κάποιες γενικές ιδιότητες. Τα σύνολα $\mathbb{Z}$ και $\mathbb{Q}$ μας υποβάλλουν αμέσως την ιδέα να μελετήσουμε γενικά σύνολα στα οποία έχουν οριστεί πράξεις, που έχουν μερικές τουλάχιστον από τις ιδιότητές της πρόσθεσης και του πολλαπλασιασμού στο $\mathbb{Z}$ και $\mathbb{Q}$.

Ένα ζεύγος $(G,*)$, όπου G είναι ένα μη κενό σύνολο και $*$ μία πράξη

$$* : G\times G \to G,\ (x, y) \to x*y$$

καλείται *ομάδα,* αν η πράξη $*$ έχει τις εξής ιδιότητες:

(α) $x*(y*z) = (x*y)*z$, για κάθε $x, y, z\in G$ (προσεταιριστικός νόμος),

(β) υπάρχει $e\in G$ τέτοιο, ώστε για κάθε $x\in G$ να ισχύει

$$x*e = x = e*x,$$

(γ) για κάθε $x\in G$, υπάρχει $x'\in G$ τέτοιο, ώστε

$$x*x' = e = x'*x.$$

Το e είναι το μοναδικό στοιχείο που έχει την ιδιότητα (β). Πραγματικά, αν υποθέσουμε ότι k είναι ένα άλλο στοιχείο του G τέτοιο, ώστε

$$x*k = x = k*x, \text{ για κάθε } x\in G,$$

παίρνουμε

$$e*k = e \quad \text{και} \quad e*k = k.$$

Άρα $k = e$. Το e καλείται *ουδέτερο στοιχείο* της G.

Για κάθε $x\in G$, το στοιχείο x' είναι μοναδικό. Πραγματικά, αν υποθέσουμε ότι x'' είναι ένα άλλο στοιχείο του G έτσι, ώστε

$$x*x''= e = x''*x,$$

έχουμε

$$x' = x'*e = x'*(x*x'') = (x'*x)*x'' = e*x'' = x''.$$

Το στοιχείο x' καλείται *συμμετρικό* του x.

Αν επί πλέον η πράξη $*$ είναι αντιμεταθετική, δηλαδή, έχει την ιδιότητα

$$x*y = y*x, \quad \text{για κάθε } x, y\in G,$$

τότε η ομάδα G καλείται *αντιμεταθετική* ή *αβελιανή* .

Παράδειγμα 6.1. Τα σύνολα $\mathbb{Z}$ και $\mathbb{Q}$ με πράξη την πρόσθεση αποτελούν αβελιανές ομάδες.

Παράδειγμα 6.2. Το σύνολο $\mathbb{Q}^* = \mathbb{Q}-\{0\}$ με πράξη τον πολλαπλασιασμό αποτελεί αβελιανή ομάδα.

Παράδειγμα 6.3. Το σύνολο των θετικών ακεραίων $\mathbb{Q}^+$ με πράξη τον πολλαπλασιασμό αποτελεί αβελιανή ομάδα.

Παράδειγμα 6.4. Το σύνολο

$$S = \{2^m 3^n / \, m, n\in \mathbb{Z}\}$$

με τον συνήθη πολλαπλασιασμό είναι αβελιανή ομάδα.

Συχνά συμβολίζουμε την πράξη $*$ μιας ομάδας $(G,*)$ σαν πολλαπλασιασμό. Τότε η ομάδα G καλείται *πολλαπλασιαστική*. Σ' αυτή την περίπτωση γράφουμε xy αντί $x*y$ και καλούμε το στοιχείο xy *γινόμενο* των x και y. Το ουδέτερο στοιχείο καλείται *μονάδα* και συμβολίζεται με 1. Επίσης, το συμμετρικό ενός στοιχείου x καλείται *αντίστροφο* του x και συμβολίζεται με x^{-1}. Όταν η ομάδα G είναι αβελιανή, συχνά συμβολίζουμε την πράξη $*$ και σαν πρόσθεση. Τότε η ομάδα G καλείται *προσθετική,* οπότε γράφουμε $x+y$ αντί $x*y$ και καλούμε το στοιχείο $x+y$ *άθροισμα* των x και y. Το ουδέτερο στοιχείο καλείται *μηδέν* και σημειώνεται με 0. Τέλος, το συμμετρικό ενός στοιχείου x καλείται *αντίθετο* του x και συμβολίζεται με $-x$.

Μερικές στοιχειώδεις ιδιότητες των ομάδων δίνονται παρακάτω.

ΠΡΟΤΑΣΗ 6.1. *Έστω* $(G,\cdot)$ *μία ομάδα. Τότε*

(α) $ax = bx \Rightarrow a = b$,

(β) $xa = xb \Rightarrow a = b$,

(γ) $(ab)^{-1} = b^{-1}a^{-1}$, *για κάθε* $a, b \in G$,

(δ) $(a^{-1})^{-1} = a$, *για κάθε* $a \in G$.

ΑΠΟΔΕΙΞΗ. (α) Πολλαπλασιάζοντας τη σχέση $ax = bx$ από δεξιά με x^{-1} έχουμε

$$(ax)x^{-1} = (bx)x^{-1},$$

απ' όπου

$$a(xx^{-1}) = b(xx^{-1})$$

και επομένως $a1 = b1$, δηλαδή $a = b$. Η απόδειξη της (β) είναι όμοια.

(γ) Έχουμε

$$(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a((bb^{-1})a^{-1} = a(1a^{-1}) = aa^{-1} = 1.$$

Ομοίως παίρνουμε $(b^{-1}a^{-1})(ab) = 1$. Συνεπώς $(ab)^{-1} = b^{-1}a^{-1}$.

δ) Είναι

$$(a^{-1})a = 1 \quad \text{και} \quad a(a^{-1}) = 1.$$

Άρα $(a^{-1})^{-1} = a$.

Ένας *δακτύλιος* είναι μία τριάδα $(A, +, \cdot)$, που αποτελείται από ένα μη κενό σύνολο A και από δύο πράξεις, μία πρόσθεση

$$A\times A \to A,\ (x, y) \to x+y$$

και ένα πολλαπλασιασμό

$$A\times A \to A,\ (x, y) \to xy$$

έτσι, ώστε να ισχύουν τα εξής:

(α) το ζεύγος $(G, +)$ είναι αβελιανή ομάδα,

(β) $x(yz) = (xy)z$, για κάθε $x, y, z\in A$,

(γ) υπάρχει μονάδα, δηλαδή υπάρχει ένα στοιχείο 1 του A τέτοιο, ώστε

$$1x = x = x1, \quad \text{για κάθε } x\in A,$$

(δ) $x(y+z) = xy+xz$ και $(y+z)x = yx+zx$, για κάθε $x, y, z\in A$.

Αποδεικνύεται, όπως και στην περίπτωση των ομάδων, ότι το στοιχείο 1 είναι μοναδικό. Χρησιμοποιώντας τα παραπάνω αξιώματα μπορούμε να πάρουμε διάφορες στοιχειώδεις ιδιότητες των δακτυλίων. Για παράδειγμα, θ' αποδείξουμε τα εξής:

$$0x = 0 = x0 \quad \text{και} \quad (-1)x = -x = x(-1).$$

Είναι

$$0x+x = 0x+1x = (0+1)x = 1x = x = 0+x,$$

οπότε η Πρόταση 6.1(α) δίνει $0x = 0$. Ομοίως παίρνουμε $x0 = 0$. Για τη δεύτερη σχέση έχουμε

$$(-1)x+x = (-1)x+1x = [(-1)+1]x = 0x = 0.$$

Επειδή κάθε στοιχείο του A έχει μοναδικό αντίθετο, έπεται ότι $(-1)x = -x$. Ομοίως αποδεικνύεται ότι $-x = x(-1)$.

Στην περίπτωση όπου $0 = 1$, $A = \{0\}$. Πραγματικά, αν $x \in A$ έχουμε

$$x = 1x = 0x = 0,$$

και κατά συνέπεια $A = \{0\}$.

Αν ισχύει

$$xy = yx, \text{ για κάθε } x, y \in A \text{ (αντιμεταθετικός νόμος)},$$

τότε ο δακτύλιος A καλείται *αντιμεταθετικός*.

Παράδειγμα 6.5. Τα σύνολα $\mathbb{Z}$ και $\mathbb{Q}$ με πράξεις την πρόσθεση και τον πολλαπλασιασμό αποτελούν αντιμεταθετικούς δακτυλίους.

Παράδειγμα 6.6. Το σύνολο $\mathbb{Q}\times\mathbb{Q}$ με πρόσθεση

$$(a_1, a_2)+(b_1, b_2) = (a_1+b_1, a_2+b_2)$$

και πολλαπλασιασμό

$$(a_1, a_2)\,(b_1, b_2) = (a_1b_1, a_2b_2)$$

αποτελεί δακτύλιο. Το μηδέν και η μονάδα είναι τα ζεύγη $(0, 0)$ και $(1, 1)$ αντιστοίχως. Το αντίθετο ενός στοιχείου (a_1, a_2) είναι το $(-a_1, -a_2)$.

Αν ο δακτύλιος A έχει μη μηδενικά στοιχεία x, y με $xy = 0$, τότε τα στοιχεία αυτά καλούνται *διαιρέτες του μηδενός.* Ένας αντιμεταθετικός δακτύλιος $A \neq \{0\}$, χωρίς διαιρέτες του μηδενός, καλείται *πεδίο ακεραιότητας.* Για παράδειγμα, οι δακτύλιοι $\mathbb{Z}$ και $\mathbb{Q}$ είναι πεδία ακεραιότητας. Αντίθετα στο δακτύλιο $\mathbb{Q}\times\mathbb{Q}$ έχουμε

$$(1, 0)\,(0, 1) = (0, 0).$$

Επομένως, ο δακτύλιος $\mathbb{Q}\times\mathbb{Q}$ έχει διαιρέτες του μηδενός και κατά συνέπεια δεν είναι πεδίο ακεραιότητας.

Έστω A ένας δακτύλιος και a ένα στοιχείο του. Το a καλείται *αντιστρέψιμο,* αν υπάρχει $a' \in A$ τέτοιο, ώστε

$$aa' = 1 = a'a.$$

Τότε το a' είναι μονοσήμαντα ορισμένο και καλείται *αντίστροφο* του a. Το συμβολίζουμε με a^{-1}. Για παράδειγμα, τα αντιστρέψιμα στοιχεία του $\mathbb{Z}$ είναι τα ± 1. Παρατηρούμε ότι το σύνολο των αντιστρεψίμων στοιχείων του A αποτελεί ομάδα, με πράξη τον πολλαπλασιασμό. Αν x είναι ένα αντιστρέψιμο στοιχείο ενός δακτυλίου A, τότε το x δεν είναι διαιρέτης του μηδενός. Πραγματικά, αν το x ήταν διαιρέτης του μηδενός, θα υπήρχε $y \in A$ με $y \neq 0$ τέτοιο, ώστε $xy = 0$ και επομένως

$$0 = x^{-1}(xy) = (x^{-1}x)y = y,$$

άτοπο.

Ένας αντιμεταθετικός δακτύλιος $A \neq \{0\}$ καλείται *σώμα* αν κάθε μη μηδενικό στοιχείο του είναι αντιστρέψιμο. Για παράδειγμα, ο δακτύλιος $\mathbb{Q}$ είναι σώμα ενώ οι δακτύλιοι $\mathbb{Z}$ και $\mathbb{Q}\times\mathbb{Q}$ δεν είναι σώματα. Παρατηρούμε ότι ένα σώμα δεν έχει διαιρέτες του μηδενός.

Έστω A ένας δακτύλιος και $x \in A$. Τότε ορίζουμε το στοιχείο x^n, για κάθε $n \in \mathbb{N}$, ως εξής:

$$x^0 = 1 \quad \text{και} \quad x^n = xx^{n-1} \quad \text{για } n > 0.$$

Αποδεικνύονται επαγωγικά οι παρακάτω κανόνες:

$$x^n x^m = x^{n+m} \quad \text{και} \quad (x^n)^m = x^{nm}.$$

Επίσης, ορίζουμε το nx ως εξής:

$$0x = 0, \quad nx = x+(n-1)x, \quad (-nx) = n(-x) \quad \text{για } n > 0.$$

Αποδεικνύονται με επαγωγή οι ακόλουθοι κανόνες:

$$mx+nx = (m+n)x \quad \text{και} \quad m(nx) = (mn)x.$$

Έστω $n, k \in \mathbb{N}$, με $0 \leq k \leq n$. Θέτουμε

$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

όπου $0! = 1 = 1!$ και $n! = 1\cdot 2\cdot 3 \ldots (n-1)n$ για κάθε φυσικό $n > 1$.

ΠΡΟΤΑΣΗ 6.2. (*Διώνυμο του Newton*) *Έστω* A *ένας δακτύλιος και* x, $y \in A$ *με* $xy = yx$. *Τότε για κάθε φυσικό* $n \geq 1$ *ισχύει*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

ΑΠΟΔΕΙΞΗ. Θα χρησιμοποιήσουμε την μέθοδο της Μαθηματικής Επαγωγής. Για $n=1$ διαπιστώνουμε εύκολα ότι η πρόταση ισχύει. Υποθέτουμε ότι η πρόταση ισχύει για $n = m$. Έχουμε

$$(x+y)^{m+1} = (x+y)^m(x+y) = \left\{\binom{m}{0}x^m + \ldots + \binom{m}{k}x^{m-k}y^k + \ldots + \binom{m}{m}y^m\right\}(x+y) =$$

$$= \binom{m}{0}x^{m+1} + \left\{\binom{m}{0} + \binom{m}{1}\right\}x^m y + \ldots +$$

$$+ \left\{\binom{m}{k-1} + \binom{m}{k}\right\}x^{(m+1)-k}y^k + \ldots + \binom{m}{m}y^{m+1}$$

Είναι

$$\binom{m}{0} = 1 = \binom{m+1}{0} \quad \text{και} \quad \binom{m}{m} = 1 = \binom{m+1}{m+1}.$$

Επίσης, για $0 < k < m$ έχουμε

$$\binom{m}{k-1} + \binom{m}{k} = \frac{m!}{(m-k+1)!\,(k-1)!} + \frac{m!}{(m-k)!k!} = \frac{m!}{(m-k)!\,(k-1)!}\left(\frac{1}{m-k+1} + \frac{1}{k}\right) =$$

$$= \frac{(m+1)!}{k!\,(m-k+1)!} = \binom{m+1}{k}.$$

Επομένως

$$(x+y)^{m+1} = \sum_{k=0}^{m+1} \binom{m+1}{k} x^{(m+1)-k}y^k.$$

Άρα η πρόταση ισχύει για $n = m+1$ και συνεπώς για κάθε φυσικό ≥ 1.

Τέλος, παρατηρούμε ότι επειδή οι αριθμοί $\binom{n}{k}$ παρουσιάζονται ως συντελεστές του διώνυμου $(x+y)^n$, έχουμε $\binom{n}{k} \in \mathbb{N}$.

7. Ασκήσεις

1. Έστω $m, n, k \in \mathbb{N}$. Τότε ισχύουν τα εξής:

(α) $m < n$ και $n < k \Rightarrow m < k$,

(β) $m < n \Leftrightarrow m+k < n+k$.

2. Έστω $m, n, k \in \mathbb{N}$, με $k \neq 0$. Τότε ισχύουν τα εξής:

(α) $m = n \Leftrightarrow mk = nk$,

(β) $m < n \Leftrightarrow m+k < n+k$.

3. Έστω $m, n, k \in \mathbb{N}$. Τότε ισχύουν τα εξής:

(α) $m \leq m$ (ανάκλαση),

(β) $m \leq n$ και $n \leq m \Rightarrow n = m$ (αντισυμμετρία),

(γ) $m \leq n$ και $n \leq k \Rightarrow m \leq k$ (μετάβαση).

4. (Ανισότητα του Bernoulli) Έστω x πραγματικός αριθμός με $0 < x < 1$. N' αποδειχθεί, χρησιμοποιώντας τη μέθοδο της Μαθηματικής Επαγωγής, ότι για κάθε φυσικό $n \geq 2$, ισχύει:

$$(1-x)^n > 1-nx.$$

5. Έστω n ένας φυσικός ≥ 1.

(α) Ένας φυσικός της μορφής

$$T_n = 1+2+ \dots +n$$

καλείται *τριγωνικός*. Να δειχθεί ότι

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

(β) Ένας φυσικός της μορφής

$$C_n = 1+3+5+ \dots +(2n-1)$$

καλείται *τετραγωνικός*. Να δειχθεί ότι

$$C_n = n^2.$$

(γ) Ένας φυσικός της μορφής

$$P_n = 1+4+ \dots +(3n-2)$$

ονομάζεται *πενταγωνικός*. Να δειχθεί ότι

$$P_n = \frac{1}{2} n(3n-1).$$

6. *Πυραμιδικός αριθμός ρίζας* n καλείται το άθροισμα των n πρώτων τριγωνικών αριθμών:

$$\Pi_n = 1+3+6+ \dots + \frac{1}{2} n(n+1).$$

Να δειχθεί ότι

$$\Pi_n = \frac{1}{6} n(n+1)(n+2).$$

7. Έστω Σ σύνολο και A ένα υποσύνολο του. Ορίζουμε μία σχέση S στο Σ ως εξής:

$$x \equiv y \ (S) \ \Leftrightarrow \ x = y \ \text{ ή } \ x, y \in A.$$

Να δειχθεί ότι η S είναι μία σχέση ισοδυναμίας και να προσδιοριστούν οι κλάσεις ισοδυναμίας των στοιχείων του Σ.

8. Έστω $\{U_a\}_{a\in A}$ μία διαμέριση του Σ. Δείξτε ότι η σχέση που ορίζεται ως εξής:

$$x \equiv y\ (R) \iff x \text{ και } y \text{ βρίσκονται στο ίδιο σύνολο } U_a$$

είναι μία σχέση ισοδυναμίας στο Σ που οι κλάσεις της είναι τα σύνολα U_a.

9. Έστω $x, y\in\mathbb{Z}$. Να δειχθεί
(α) $x0 = 0$
(β) $xy = 0 \Rightarrow x = 0$ ή $y = 0$.

10. Έστω $x, y, z\in\mathbb{Z}$. Να δειχθεί
(α) $x+y = x+z \Rightarrow y = z$,
(β) αν $x \neq 0$ και $xy = xz \Rightarrow y = z$.

11. Έστω $a, b\in\mathbb{Z}$. Να δειχθεί ότι $a < b$, αν και μόνον αν, υπάρχει $k\in\mathbb{N}$, με $k \neq 0$ ώστε $a+k = b$.

12. Έστω $a, b\in\mathbb{Z}$. Τότε ισχύει μόνο μία από τις εξής σχέσεις:

$$a < b,\ \ a = b,\ \ a > b.$$

13. Έστω $a, b, c\in\mathbb{Z}$. Τότε ισχύουν τα εξής:
(α) αν $a < b$ και $b < c$, τότε $a < c$,
(β) αν $a < b$, τότε $a+c < b+c$,
(γ) αν $a < b$ και $c \neq 0$, τότε $ac < bc$ αν $c > 0$ και $ac > bc$ αν $c < 0$.

14. Έστω $a\in\mathbb{Z}$ και A το σύνολο των ακεραίων που είναι $\geq a$. Τότε, κάθε μη κενό υποσύνολο S του A περιέχει ένα ελάχιστο στοιχείο, δηλαδή, υπάρχει $\varepsilon\in S$ τέτοιο, ώστε $\varepsilon \leq x$, για κάθε $x\in S$.

15. Έστω $G = \mathbb{Q}-\{1/2\}$. Ορίζουμε μία πράξη επί του G ως εξής:

$$x*y = x+2xy+y, \quad \text{για κάθε } x, y\in G.$$

Να δειχθεί ότι το ζεύγος $(G,*)$ είναι ομάδα.

16. Έστω X ένα μη κενό σύνολο. Συμβολίζουμε με $S(X)$ το σύνολο των αμφιέσεων του X στο X. Να δειχθεί ότι το σύνολο $S(X)$ με πράξη την σύνθεση απεικονίσεων αποτελεί ομάδα.

17. Σε κάθε δακτύλιο A ισχύει

$$(-x)y = x(-y) = -xy,$$

για κάθε $x, y\in A$.

18. Έστω K ένα σώμα τέτοιο, ώστε

$$-x = x^{-1},$$

για κάθε $x\in K-\{0\}$. Να δειχθεί ότι $K = \{0,1\}$.

19. Να δειχθεί ότι το σύνολο

$$A = \left\{ \frac{a}{2^n} \in \mathbb{Q} / \ a\in \mathbb{Z} \ \ \text{και} \ \ n\in \mathbb{Z} \right\}$$

εφοδιασμένο με τις συνηθισμένες πράξεις της πρόσθεσης και του πολλαπλασιασμού αποτελεί δακτύλιο. Να βρεθούν τα αντιστρέψιμα στοιχεία του.

20. Να δειχθεί ότι το σύνολο

$$\mathbb{Z}[\sqrt{3}] = \{a+b\sqrt{3} \ / \ \ a, b\in \mathbb{Z}\}$$

εφοδιασμένο με τις συνηθισμένες πράξεις της πρόσθεσης και του πολλαπλασιασμού αποτελεί δακτύλιο.

21. Έστω $(A, +, \cdot)$ ένας δακτύλιος. Στο σύνολο $\mathbb{Z}\times A$ ορίζουμε τις εξής πράξεις:

$$(m, a)\oplus(n, b) = (m+n, a+b)$$

$$(m, a)\otimes(n, b) = (mn, na+mb+ab).$$

Να δειχθεί ότι η τριάδα $(\mathbb{Z}\times A, \oplus, \otimes)$ αποτελεί δακτύλιο.