ΣΤΑΥΡΟΥ Γ. ΙΟΥΛΙΔΗ

ΓΡΑΜΜΙΚΗ ΑΛΓΕΒΡΑ

ΑΛΓΕΒΡΙΚΕΣ ΔΟΜΕΣ

ΔΙΑΝΥΣΜΑΤΙΚΟΙ ΧΩΡΟΙ - ΠΙΝΑΚΕΣ

ΓΡΑΜΜΙΚΑ ΣΥΣΤΗΜΑΤΑ - ΙΔΙΟΜΕΓΕΘΗ

ΤΕΤΡΑΓΩΝΙΚΕΣ ΜΟΡΦΕΣ

ΣΗΜΕΙΑΚΟΙ ΧΩΡΟΙ - ΤΑΝΥΣΤΕΣ

ΕΚΔΟΣΕΙΣ ΖΗΤΗ
ΘΕΣΣΑΛΟΝΙΚΗ

Κάθε γνήσιο αντίτυπο υπογράφεται από το συγγραφέα

ISBN 960-431-437-8

Φωτοστοιχειοθεσία - Εκτύπωση **Π. ΖΗΤΗ & Σια ΟΕ**
18° χλμ. Θεσ/νίκης-Περαίας (στροφή Τριλόφου) • Τ.Θ. 170 57
Θεσσαλονίκη 542 10 • ☎ & Fax (0392) 72 222 (3 γραμμές)

Βιβλιοπωλείο **ΕΚΔΟΣΕΙΣ ΖΗΤΗ**
Αρμενοπούλου 27 • ☎ (031) 203 720
Θεσσαλονίκη 546 35 • Fax (031) 211 305
e-mail: ziti@hyper.gr

ΠΡΟΛΟΓΟΣ

Κύριος σκοπός του βιβλίου είναι να δώσει με σαφήνεια τη βασική δομή της Γραμμικής Άλγεβρας και του αντίστοιχου προς αυτήν Γεωμετρικού χώρου.

Επίσης δίνεται ιδιαίτερη προσοχή στη συνοχή των διαφόρων εννοιών και προτάσεων ώστε η όλη θεωρία να έχει ένα εννιαίο, συνεχές και πλήρως κατανοητό περιεχόμενο.

Το πρώτο τμήμα αρχίζει με μία σύντομη αναφορά στη θεωρία των αλγεβρικών δομών. Η γνώση των σωμάτων με άπειρο ή πεπερασμένο πλήθος στοιχείων και των αλγεβρικών δομών που προκύπτουν από έννοιες της μαθηματικής λογικής είναι απαραίτητη για τις εφαρμογές σε προβλήματα σύγχρονης τεχνολογίας. Η θεωρία των διανυσματικών χώρων αποτελεί το κύριο περιεχόμενο του πρώτου τμήματος.

Εδώ γίνεται η ανάπτυξη των βασικών στοιχείων των διανυσματικών χώρων, τα οποία είναι απαραίτητα για την πλήρη κατανόηση της παραπέρα θεωρίας. Οι έννοιες του διανυσματικού υπόχωρου και των γεννητόρων του, της γραμμικής εξάρτησης και ανεξαρτησίας, της βάσης, του εσωτερικού γινομένου, της γραμμικής απεικόνισης και των μετασχηματισμών είναι απαραίτητες για μία βασική κατανόηση της Γραμμικής Άλγεβρας.

Στο δεύτερο τμήμα γίνεται μία αρκετά μεγάλη ανάπτυξη της γενικής θεωρίας των πινάκων.

Συμμετρικοί, αντισυμμετρικοί, ερμιτιανοί, αντιερμιτιανοί, ορθοκανονικοί και ορθογώνιοι πίνακες είναι οι βασικοί πίνακες των εφαρμογών.

Οι ορίζουσες, οι σύνθετοι και οι αντίστροφοι πίνακες αποτελούν περιεχόμενο του τμήματος αυτού. Επίσης ο συνδυασμός των ιδιοτήτων των πινάκων με τις βάσεις και τις γραμμικές απεικονίσεις οδηγούν σε σημαντικά συμπεράσματα, όπως είναι ο μετασχηματισμός των βάσεων και ο βαθμός ενός πίνακα.

Στο τρίτο τμήμα αναπτύσσονται οι βασικοί μετασχηματισμοί των πινάκων. Ο προσδιορισμός υπολογιστικών μεθόδων υπολογισμού του αντιστρόφου, ενός γενικευμένου αντιστρόφου, της κανονικής, της διαγώνιας και της κλιμακωτής μορφής ενός πίνακα αποτελούν το κύριο περιεχόμενο της θεωρίας των βασικών μετασχηματισμών. Επίσης προκύπτουν σημαντικά συμπεράσματα από την ανάπτυξη της σχετικής θεωρίας.

Στο τέταρτο τμήμα αναπτύσσεται η θεωρία των γραμμικών συστημάτων. Προσδιορίζονται οι συνθήκες επιλυσιμότητας και οι βασικοί τρόποι επίλυσης αυτών.

Επίσης αναφέρονται μέθοδοι προσδιορισμού ενός διανυσματικού χώρου, της τομής και του αθροίσματος διανυσματικών χώρων με την επίλυση γραμμικών συστημάτων.

Τα χαρακτηριστικά μεγέθη και οι τετραγωνικές μορφές αποτελούν το περιεχόμενο του πέμπτου τμήματος.

Ο μετασχηματισμός ενός τετραγωνικού πίνακα στην τριγωνική και τη διαγώνια μορφή του είναι το κύριο περιεχόμενο της σχετικής θεωρίας και τα συμπεράσματα οδηγούν σε διάφορες εφαρμογές.

Τέλος γίνεται μία σύντομη ανάπτυξη της θεωρίας των τετραγωνικών μορφών, η οποία είναι απαραίτητη για τις εφαρμογές.

Οι σημειακοί χώροι αποτελούν το περιεχόμενο του έκτου τμήματος της θεωρίας. Αυτοί είναι γεωμετρικοί χώροι αντίστοιχοι των διανυσματικών. Οι έννοιες των συστημάτων αναφοράς και συντεταγμένων και οι ιδιότητες του βαρυκέντρου, της μεταφοράς και των μετασχηματισμών αποτελούν τα βασικά στοιχεία για την κατανόηση των σημειακών χώρων. Επίσης οι έννοιες του εξωτερικού, του μικτού και του διπλού εξωτερικού γινομένου είναι χρήσιμες στις εφαρμογές. Οι σημειακοί υπόχωροι δίνουν τη δυνατότητα μιας βασικής κατανόησης του γεωμετρικού χώρου, ο οποίος μας περιβάλλει.

Έτσι οι ευθείες, τα επίπεδα, οι καμπύλες και οι επιφάνειες δευτέρου βαθμού, τα παραλληλεπίπεδα και τα παραλληλόγραμμα γίνονται πλήρως κατανοητά. Επίσης η παραλληλία και ο προσδιορισμός της τομής και του αθροίσματος των σημειακών υποχώρων είναι πολύ σημαντικά στοιχεία για τα υπολογιστικά προβλήματα.

Τέλος οι ιδιότητες των σημειακών απεικονίσεων και των ισομετριών οδηγούν στην κατανόηση των βασικών κινήσεων στο γεωμετρικό χώρο.

Στο έβδομο τμήμα της θεωρίας γίνεται μία σύντομη ανάπτυξη του τανυστικού λογισμού. Βασικός σκοπός της σχετικής θεωρίας είναι ο καθορισμός των συμβόλων και οι ορισμοί των τανυστών και των πράξεων που μπορούμε να κάνουμε με τους τανυστές.

Εδώ είναι απαραίτητη η πλήρης κατανόηση της έννοιας του τανυστικού χαρακτήρα ενός μεγέθους.

Όλη η θεωρία αναπτύσσεται με επεξηγηματικό τρόπο έτσι ώστε η σημασία της αφετηρίας των συμπερασμάτων να είναι σαφής.

ΠΕΡΙΕΧΟΜΕΝΑ

ΣΤ. ΣΗΜΕΙΑΚΟΙ ΧΩΡΟΙ

Ζ. ΣΤΟΙΧΕΙΑ ΤΑΝΥΣΤΙΚΟΥ ΛΟΓΙΣΜΟΥ

A

ΔΙΑΝΥΣΜΑΤΙΚΟΙ ΧΩΡΟΙ

1. Εισαγωγή

Θεωρούμε απαραίτητη την ανάπτυξη ορισμένων εννοιών για μια στοιχειώδη γνώση των βασικών αλγεβρικών δομών και για τη σύνδεση της Άλγεβρας με τη Γεωμετρία.

Μία **πράξη** επί ενός συνόλου G είναι μία απεικόνιση φ του καρτεσιανού γινομένου $G\times G$, επί του G. Το σύνολο G εφοδιασμένο με μία πράξη φ λέγεται **ομαδοειδές.**

Μία πράξη φ λέγεται **προσεταιριστική,** όταν είναι

$$\varphi(\varphi(x, y), z) = \varphi(x, \varphi(y, z))$$

Ένα σύνολο εφοδιασμένο με μία προσεταιριστική πράξη φ λέγεται **ημιομάδα.**

Ένα στοιχείο e λέγεται **ουδέτερο** ή **ταυτοτικό** ως προς μία πράξη φ, όταν είναι

$$\varphi(e, x) = \varphi(x, e) = x.$$

και τότε μία ημιομάδα G με ουδέτερο στοιχείο e λέγεται **μονοειδές.** Το ουδέτερο στοιχείο e είναι μοναδικό.

Ένα στοιχείο $\kappa\in G$ λέγεται απορροφητικό ως προς μία πράξη φ, όταν είναι

$$\varphi(x, k) = \varphi(k, x) = k.$$

Τότε το k είναι μοναδικό και διάφορο από το ουδέτερο στοιχείο e, δηλ. είναι $k\neq e$, διότι διαφορετικά προκύπτει $G=\{k\}$. Πράγματι, όταν είναι $e=\kappa$, τότε $\varphi(k, x) = k= \varphi(e, x) = x$ για κάθε $x\in G$. Τα x, y, και z είναι τυχαία στοιχεία του G.

Μία πράξη φ λέγεται **αντιμεταθετική** ή **αβελιανή,** όταν είναι $\varphi(x, y) = \varphi(y, x)$.

Θεωρούμε δύο στοιχεία x και y ενός μονοειδούς G με πράξη φ και ουδέτερο στοιχείο e. Λέμε ότι το y είναι **αντίστροφο** του x, όταν είναι

$$\varphi(x, y) = \varphi(y, x) = e$$

Το αντίστροφο στοιχείο y ενός στοιχείου x (αν υπάρχει) είναι μοναδικό. Πράγματι, αν z είναι ένα άλλο αντίστροφο του x, τότε έχουμε

$$y = \varphi(e, y) = \varphi(\varphi(z, x), y) = \varphi(z, \varphi(x, y)) = \varphi(z, e) = z.$$

Μία πράξη φ επί του G γράφεται συμβολικά με τους ακόλουθους τρεις τρόπους.

$$\varphi(x, y), \quad x\varphi y, \quad (x, y)\varphi$$

και ο συνηθέστερος είναι ο δεύτερος τρόπος. Επίσης μία πράξη φ συμβολίζεται συνήθως προσθετικά ή πολλαπλασιαστικά, δηλ. γράφουμε

$$\varphi(x, y) = x+y, \quad \varphi(x, y) = xy$$

αντίστοιχα. Χρησιμοποιούμε συνήθως τον προσθετικό συμβολισμό $+$, όταν η πράξη φ είναι αντιμεταθετική, και τον πολλαπλασιαστικό, όταν η φ δεν είναι αντιμεταθετική. Άλλος συνήθης συμβολισμός είναι ο κυκλίσκος $\circ$, τον οποίο εφαρμόζουμε συνήθως στη σύνθεση δύο συναρτήσεων f και g και γράφουμε $\varphi(f, g) = f \circ g$.

Όταν η πράξη συμβολίζεται προσθετικά (αντ. πλλαπλασιαστικά), τότε το ουδέτερο στοιχείο e συμβολίζεται συνήθως με το μηδέν 0 (αντ. τη μονάδα) και λέγεται **μηδενικό** (αντ**. μονάδα**). Επίσης η ταυτοτική απεικόνιση συμβολίζεται συνήθως με τη μονάδα.

Στην προσθετική (αντ. πολλαπλασιαστική) περίπτωση το αντίστροφο ενός στοιχείου x συμβολίζεται με $-x$ (αντ. x^{-1}) και λέγεται **αντίθετο** (αντ. **αντίστροφο**) του x.

Αν G είναι ένα μονοειδές, του οποίου κάθε στοιχείο x έχει αντίστροφο, τότε το G ονομάζεται **ομάδα.** Όταν η πράξη μιας ομάδας G είναι αντιμεταθετική, τότε η G λέγεται αντιμεταθετή ή **αβελιανή.**

Κάθε σύνολο, εφοδιασμένο με μία ή περισσότερες πράξεις λέγεται **αλγεβρική δομή.**

Άρα ένα σύνολο G εφοδιασμένο με μία πράξη αποτελεί ομάδα, όταν για τα τυχαία στοιχεία του x, y και z ισχύουν οι ιδιότητες

i. $(xy)z = x(yz)$

ii. $(\forall\, x \in G)\ (\exists\, e \in G)\colon xe = ex = x$ ή $x1 = 1x = x$

iii. $(\forall\, x \in \Gamma)\ (\exists\, x^{-1} \in G)\colon xx^{-1} = x^{-1}x = e.$

Η ομάδα G λέγεται αντιμεταθετική, όταν είναι $xy = yx$.

Με τον προσθετικό συμβολισμό $+$, οι παραπάνω ιδιότητες γράφονται αντίστοιχα

i. $(x+y)+z = x+(y+z)$

ii. $(\forall\, x \in G)\ (\exists\, 0 \in G)\colon x+0 = 0+x = x$

iii. $(\forall\, x\in G)\,(\exists\mid -x\in G)$: $x+(-x)=(-x)+x=0$

iv. $x+y=y+x$

και η αντιμεταθετική ομάδα G λέγεται και προσθετική.

Αν A και B είναι υποσύνολα μιας ομάδας G, τότε ορίζεται το γινόμενο

$$AB=\{\alpha\beta\mid \alpha\in A,\ \beta\in B\}$$

και το άθροισμα $A+B=\{\alpha+\beta\mid \alpha\in A,\ \beta\in B\}$, όταν η πράξη είναι πολ/κή (αντ. προσθετική). Έτσι, για $x\in G$, έχουμε αντίστοιχα.

$$xA=\{x\alpha\mid \alpha\in A\},\quad x+A=\{x+\alpha\mid \alpha\in A\}.$$

Τότε το σύνολο xA (αντ. $x+A$) λέγεται αριστερή θήκη του A στο G. Αντίστοιχα ορίζεται η δεξιά θήκη Ax (αντ. $A+x$) του A στο G. Ο συμβολισμός είναι ο ίδιος με εκείνο της πράξης της G.

Ένα υποσύνολο H μιας ομάδας G εφοδιασμένο με την πράξη φ της ομάδας G λέγεται **υποομάδα** της G, όταν αποτελεί ομάδα ως προς την φ.

Ένα υποσύνολο H μιας ομάδας G είναι υποομάδα της ανν $xy\in H$ και $x^{-1}\in H$ για κάθε $x, y\in H$.

Το ταυτοτικό στοιχείο e και η ίδια η ομάδα G θεωρούνται υποομάδες της G. Αν αυτές είναι οι μοναδικές υποομάδες της G, τότε η G λέγεται **απλή.** Οι υπόλοιπες υποομάδες της G λέγονται γνήσιες.

Το πλήθος των στοιχείων μιας ομάδας G λέγεται **τάξη** της G. Ο μικρότερος θετικός ακέραιος k για τον οποίο είναι $x^{\kappa}=e$ λέγεται **τάξη** του στοιχείου $x\in G$, όπου e είναι το ουδέτερο στοιχείο της G και $x^{\kappa}=xx\ldots x$ kφορές.

Μία υποομάδα H της G λέγεται **κανονική** ή **αναλλοίωτη** ή **αυτοσυζυγής,** όταν είναι $xHx^{-1}=H$ για κάθε $x\in G$, δηλ. όταν $xyx^{-1}\in H$ για κάθε $y\in H$ και κάθε $x\in G$.

Αν H είναι υποομάδα μιας ομάδας G, τότε έχουμε $xH=H$ για κάθε $x\in H$.

Όταν μία πράξη είναι προσεταιριστική, τότε παραλείπουμε τις παρενθέσεις, διότι το νόημα της προσεταιριστικότητας είναι ότι μπορούμε να αρχίσουμε τις πράξεις από το τυχαίο σημείο μιας παράστασης.

Αν H είναι υποομάδα μιας ομάδας G, τότε το σύνολο των θηκών xH της H στην G, συμβολικά $G/H=\{xH\mid x\in G\}$ αποτελεί διαμερισμό της G, δηλ. είναι $G=\bigcup_{x\in G} xH$ και $xH\cap yH=\varnothing$ για $x\neq y$. Επίσης κάθε θήκη xH έχει το ίδιο πλήθος στοιχείων με την H. Αν $\pi(G)$, $\pi(H)$ και $\pi(G/H)$ είναι αντιστοίχως οι πληθικότητες των G, H και του πηλικοσυνόλου G/H, τότε έχουμε

$$\pi(G)=\pi(H)\,\pi(G/H)$$

και το πλήθος $\pi(G/H)$ των θηκών λέγεται **δείκτης** της H στην G. Άρα η τάξη

κάθε υποομάδος μιας πεπερασμένης ομάδας G διαιρεί την τάξη της G. Έτσι, όταν γνωρίζουμε τη τάξη της G, μπορούμε να υπολογίσουμε τις τάξεις των υποομάδων της π.χ. αν $\pi(G) = 12 = 1\cdot 2^2\cdot 3$, τότε η G μπορεί να έχει δύο γνήσιες υποομάδες με τάξεις 3 και 4. Το ίδιο ισχύει για τις δεξιές θήκες Hx. Αν η H είναι κανονική τότε έχουμε $xH = Hx$ για κάθε $x\in G$ και ορίζεται επί του πηλικοσυνόλου G/H μία δομή ομάδας με την πράξη $(xH)(yH) = xyH$. Η G/H λέγεται πηλικοομάδα της H στην G. Χρησιμοποιούμε συνήθως τον συμβολισμό $\bar{x} = xH$ για τις θήκες.

Αν G είναι μία πεπερασμένη ομάδα τάξεως $2k$ και H είναι υποομάδα τάξεως k, τότε η H είναι κανονική και η G/H είναι κυκλική τάξεως 2.

Εφαρμόζουμε τον πολ/κό συμβολισμό. Αντίστοιχα ισχύουν με τον προσθετικό συμβολισμό.

Θεωρούμε μία ομάδα G και ένα τυχαίο υποσύνολο A της G. Τότε το σύνολο $H(A)$ όλων των πεπερασμένων γινομένων της μορφής

$$\alpha_1^{\nu_1}\alpha_2^{\nu_2}\dots\alpha_\mu^{\nu_\mu}\ (\nu\geq 1)$$

όπου $\alpha_1, \alpha_2, \dots, \alpha_\mu\in A$ και $\nu_i\in Z$, αποτελεί μία υποομάδα της G και λέμε ότι η $H(A)$ **παράγεται** ή γεννιέται από το A.

Μία υποομάδα H της G λέγεται **κυκλική,** όταν παράγεται από ένα μοναδικό στοιχείο $x\in G$. Έτσι είναι $H = (x) = \{e, x, x^2, \dots, x^k, \dots\}$.

Για μια κυκλική ομάδα $H=(x)$ διακρίνουμε τις παρακάτω δύο περιπτώσεις.

i. Όταν $\mu\neq\nu \Rightarrow x^\mu\neq x^\nu$. Αν Z είναι το σύνολο των ακεραίων, τότε η απεικόνιση

$$f:H\to Z,\ f(x^\nu) = \nu$$

είναι αμφιμονότιμη επί του Z και άρα η H περιέχει άπειρο πλήθος στοιχείων, δηλ. είναι απείρου τάξεως.

ii. Υποθέτουμε ότι υπάρχουν θετικοί ακέραιοι μ, ν ώστε να είναι

$$\mu\neq\nu \Rightarrow x^\mu = x^\nu.$$

Τότε το σύνολο $A = \{\nu\in N \mid (\exists\, \mu\in\mathbb{N}),\ x^\mu = x^\nu,\ \mu\neq\nu\}\neq\varnothing$ έχει ελάχιστο στοιχείο $\kappa\in N$ ως υποσύνολο του συνόλου των φυσικών αριθμών $N = \{1, 2, \dots\}$.

Έτσι το σύνολο $B = \{\nu\in N \mid x^{k+\nu} = x^k\}\neq\varnothing$ και άρα έχει ελάχιστο ένα στοιχείο λ. Άρα έχουμε $x^k = x^{k+\lambda}$ και είναι $x^\lambda = x^0 = e$, διότι το αντίστροφο του $x^k = xx\dots x$ είναι το $x^{-k} = x^{-1}x^{-1}\dots x^{-1}$ k φορές. Έτσι τα στοιχεία $x^0 = e, x, x^2, \dots, x^{\lambda-1}$ είναι διάφορα μεταξύ τους. Πράγματι, αν

$$\mu\neq\nu \Rightarrow x^\mu = x^\nu \quad \text{για} \quad \mu, \nu\leq\lambda$$

τότε, αν $\mu>\nu$, έχουμε $x^{\mu-\nu} = e$ και είναι $\mu-\nu<\lambda$, το οποίο αντιφάσκει στο γεγονός ότι το λ είναι ελάχιστο στοιχείο για το οποίο έχουμε $x^\lambda = e$.

Για $\mu>\lambda$ είναι $\mu = s\lambda+\upsilon$, όπου $0\le\upsilon<\lambda$, και άρα $x^{\mu} = x^{\upsilon}$. Έτσι η H είναι σε αμφιμονότιμη αντιστοιχία με το σύνολο $\{0, 1, \ldots, \lambda-1\}$ και άρα περιέχει λ στοιχεία, δηλ. είναι $H = \{x^0=e, x, x^2, \ldots, x^{\lambda-1}\}$, όπου λ είναι η τάξη του x.

Θεωρούμε δύο ομάδες G_1, G_2 και ας είναι e_1, e_2 τα ουδέτερα στοιχεία και H_1, H_2 δύο υποομάδες αυτών αντιστοίχως.

Μία απεικόνιση $f: G_1\to G_2$ λέγεται **ομομορφισμός,** όταν αυτή διατηρεί τις πράξεις, δηλ. όταν $f(x, y) = f(x)f(y)$. Τότε έχουμε

$$f(e_1) = e_2 \quad \text{και} \quad (f(x))^{-1} = f(x^{-1}).$$

Αν $\varphi: G_1\to G_2$ είναι ομομορφισμός, τότε η εικόνα

$$f(H_1) = \{f(x)\in G_2 \mid x\in H_1\}$$

και η αντίστροφη εικόνα $f^{-1}(H_2) = \{x\in G_1 \mid f(x)\in H_2\}$, είναι υποομάδες των G_2 και G_1 αντιστοίχως. Το σύνολο $f^{-1}(e_2) = \{x\in G_1 \mid f(x) = e_2\}$ είναι κανονική υποομάδα της G_1 και ονομάζεται **πυρήνας** της f.

Ένας ομομορφισμός $f: G_1\to G_2$ λέγεται **μονομορφισμός** ή **βουτιά,** όταν είναι ενριπτική απεικόνιση, **επιμορφισμός,** όταν είναι επί απεικόνιση και **ισομορφισμός,** όταν η f είναι αμφιμονότιμη απεικόνιση επί του G_2. Όταν η f είναι ισομορφισμός μπορούμε να ταυτίσουμε αλγεβρικά τις ομάδες G_1 και G_2. Για κάθε ισομορφισμό f, η αντίστροφη απεικόνιση f^{-1} είναι επίσης ισομορφισμός.

Ένας ομομορφισμός $f: G\to G$ λέγεται **ενδομορφισμός** και **αυτομορφισμός,** όταν είναι ισομορφισμός.

Αν H είναι κανονική υποομάδα μιας ομάδας G, τότε ορίζεται η απεικόνιση

$$f: G \to G/H \ , \quad f(x) = xH = \overline{x}$$

η οποία είναι επιμορφισμός και λέγεται **κανονικός** ή **φυσικός** ομομορφισμός. Το ουδέτερο στοιχείο της πηλικοομάδας G/H είναι το H. Άρα ο πυρήνας της f είναι το H, διότι έχουμε $f(x) = H = xH$ για κάθε $x\in H$.

Αν $f: G_1\to G_2$ είναι επιμορφισμός με πυρήνα $f^{-1}(e_2)$, τότε η απεικόνιση

$$\overline{f}: G_1/ f^{-1}(e_2) \to G_2 \ , \quad \overline{f}(\overline{x}) = f(x)$$

είναι ισομορφισμός επί την G_2.

Οι παραπάνω έννοιες (ομομομορφισμού, ισομορφισμού κ.λπ.) ισχύουν για κάθε άλγεβρική δομή.

Το σύνολο N των φυσικών αριθμών αποτελεί αντιμεταθετικό μονοειδές ως προς τον πολ/σμό με ουδέτερο στοιχείο τη μονάδα 1 που είναι το μοναδικό αντιστρεπτό στοιχείο του.

Το σύνολο $N_0 = \{0\}\cup N$ είναι αντιμεταθετικό μονοειδές ως προς την πρόσθεση με ουδέτερο στοιχείο το μηδέν 0.

Ας είναι G ένα μονοειδές με πράξη φ, ουδέτερο στοιχείο e και $x \in G$. Τότε υπάρχει μοναδικός ομομορφισμός $f: N_0 \to G$ τέτοιος, ώστε να είναι $f(1) = x$ και $f(x) = x\varphi x\varphi x \ldots \varphi x$ k φορές. Είναι $f(0) = e$. Έτσι έχουμε

$$f(k+\mu) = f(k)\, \varphi f(\mu),$$

δηλ. είναι $\underbrace{x\varphi x \ldots \varphi x}_{k+\mu \text{ φορές}} = \underbrace{(x\varphi x\varphi \ldots \varphi x)}_{k \text{ φορές}}\, \varphi\, \underbrace{(x\varphi \ldots \varphi x)}_{\mu \text{ φορές}}$.

Άρα, αν η πράξη της G είναι προσθετική, τότε έχουμε

$$f(k) = kx = x+\ldots+x \quad k \text{ φορές},$$

$f(0) = 0x=0$, $(k+\mu)x = kx+\mu x$, $f(1) = 1x = x$, $k(\mu x) = (k\mu)x$.

Όταν η πράξη της G είναι πολ/κή, τότε έχουμε

$$f(k) = x^k, \quad f(k+\mu) = x^{k+\mu} = f(k)f(\mu) = x^k x^\mu, \quad f(0) = x^0 = 1 \quad \text{και} \quad (x^k)^\mu = x^{k\mu}.$$

Το σύνολο Z των ακεραίων είναι αντιμεταθετικό μονοειδές ως προς τον πολ/μό με απορροφητικό στοιχείο το μηδέν 0. Επίσης το Z είναι αντιμεταθετική ομάδα, ως προς την πρόσθεση με ουδέτερο στοιχείο το μηδενικό 0 και είναι $-k = (-1)k = k(-1)$ για κάθε $k \in Z$, όπου $-k$ είναι το αντίθετο του k.

Αν x είναι αντιστρεπτό στοιχείο μιας ομάδας G, τότε υπάρχει μοναδικός ομομορφισμός $h: Z \to G$ με $h(1) = x$ και περιορισμό $h \mid N = f: N \to G$.

Άρα για κάθε μη-αρνητικό ακέραιο k ισχύουν τα παραπάνω.

Αν η πράξη της G είναι προσθετική, τότε έχουμε

$$h(-k) = -kx = (-x)+(-x)+ \ldots + (-x) = (-1)kx,$$

όπου $-kx$ είναι το αντίθετο του kx, και $h(-1) = (-1)x = -x$.

Όταν η πράξη του G συμβολίζεται πολ/κά, τότε είναι

$$h(-k) = x^{-k} = x^{-1}x^{-1} \ldots x^{-1} \quad k \text{ φορές} \quad \text{και} \quad h(-1) = x^{-1},$$

όπου x^{-k} είναι το αντίστροφο του x^k.

Θεωρούμε ένα σύνολο X. Τότε το σύνολο $X^X = \{f \mid f: X \to X\}$ όλων των απεικονίσεων του X στο X αποτελεί ένα μονοειδές με πράξη τη σύνθεση των συναρτήσεων, διότι η σύνθεση είναι προσεταιριστική, δηλ. είναι

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

Το ουδέτερο στοιχείο είναι η ταυτοτική συνάρτηση

$$1: X \to X, \quad 1(x) = x$$

Ονομάζουμε **μετάθεση** των στοιχείων του συνόλου X κάθε αμφιμονότιμη απεικόνιση $f: X \to X$ του X επί του X. Τότε το σύνολο

$$S(X) = \{f \mid f: X \to X)$$

των μεταθέσεων του X αποτελεί ομάδα με πράξη τη σύνθεση των απεικονίσεων, η οποία λέγεται **συμμετρική** και αποτελείται από m! στοιχεία, όταν το X έχει m στοιχεία. Κάθε υποομάδα της S(X) λέγεται ομάδα μετασχηματισμών του X.

Ας είναι $X = \{x_1,\ldots, x_m\}$. Θεωρούμε το τμήμα των φυσικών αριθμών

$$N_m = \{k\in N \mid k\le m\} = \{1, 2, \ldots, m\}$$

μήκους m. Τότε μπορούμε να κατασκευάσουμε ένα ισομορφισμό

$$F: S(N_m) \to S(X)$$

και έτσι να ταυτίσουμε αλγεβρικά τις ομάδες $S(N_m)$ και S(X). Θεωρούμε την απεικόνιση

$$\varphi: N_m\to X,\ \varphi(k)=x_k \ \text{για}\ k=1, 2, \ldots, m.$$

Η φ είναι αμφιμονότιμη επί του X. Ας συμβολίσουμε τη συμμετρική ομάδα $S(N_m)$ με S(m). Τότε ορίζεται ο ισομορφισμός

$$F(\varphi) : S(m) \to S(X),\quad F(\varphi)\,(h) = \varphi\circ h\circ\varphi^{-1} = \overline{h}.$$

Η F(φ) γράφεται συμβολικά με F_φ, δηλ. η φ τοποθετείται ως δείκτης στο F. Έτσι έχουμε

$$F_\varphi(h\circ g) = f\circ h\circ g\circ\varphi^{-1} = (\varphi\circ h\circ\varphi^{-1})\circ(\varphi\circ g\circ\varphi^{-1}) = F_\varphi(h)\circ F_\varphi(g)$$

δηλ. η F_φ είναι ομομορφισμός.

Η $\varphi^{-1}\circ\rho\circ\varphi\in S(m)$ για κάθε $\rho\in S(X)$ και είναι $F_\varphi(\varphi^{-1}\circ\rho\circ\varphi) = \rho$. Άρα η F_φ είναι επί.

Τέλος η F_φ είναι ενριπτική, διότι έχουμε

$$F_\varphi(h) = F_\varphi(g) \Rightarrow \varphi\circ h\circ\varphi^{-1} = \varphi\circ g\circ\varphi^{-1} \Rightarrow h=g.$$

Έτσι, στο λογισμό, μπορούμε κάθε φορά να θεωρούμε την ομάδα S(m) αντί της S(X).

Η εφαρμογή μιας μετάθεσης επί ενός συνόλου διατηρεί τα στοιχεία του συνόλου αλλάζοντας τη σειρά διαδοχής τους.

Μία μετάθεση $f\in S(m)$ γράφεται συνήθως με τους ακόλουθους δύο τρόπους.

$$f = \begin{pmatrix} 1 & 2 & \ldots & m \\ f(1) & f(2) & \ldots & f(m) \end{pmatrix},\quad f= f(1)\, f(2)\, \ldots\, f(m)$$

Τότε το αντίστροφο f^{-1} της f είναι

$$f^{-1} = \begin{pmatrix} f(1) & f(2) & \ldots & f(m) \\ 1 & 2 & \ldots & m \end{pmatrix} = \begin{pmatrix} 1 & 2 & \ldots & m \\ f^{-1}(1) & f^{-1}(2) & \ldots & f^{-1}(m) \end{pmatrix} = f^{-1}(1)\, f^{-1}(2)\, \ldots\, f^{-1}(m)$$

Η ταυτοτική μετάθεση 1 είναι

$$1 = \begin{pmatrix} 1 & 2 \dots m \\ 1 & 2 \dots m \end{pmatrix} = 1\ 2 \dots m$$

και αν $g = g(1)g(2) \dots g(m)$, τότε η σύνθεση $g\circ f$ είναι

$$g\circ f = \begin{pmatrix} 1 & 2 & \dots & m \\ f(1) & f(2) & \dots & f(m) \end{pmatrix}\begin{pmatrix} 1 & 2 & \dots & m \\ g(1) & g(2) & \dots & g(m) \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & \dots & m \\ f(1) & f(2) & \dots & f(m) \end{pmatrix}\begin{pmatrix} f(1) & f(2) & \dots & f(m) \\ (g\circ f)(1) & (g\circ f)(2) & \dots & (g\circ f)(m) \end{pmatrix}$$

Μία μετάθεση f λέγεται **άρτια** (αντ. περιττή), όταν χρειάζεται άρτιο (αντ. περιττό) πλήθος διαδοχικών εναλλαγών των θέσεων των στοιχείων της έτσι, ώστε να πάρει τελικά τη φυσική σειρά της $1\ 2 \dots m$. Τοτε ορίζεται το **σημείο** $\varepsilon(f)$ της f και είναι $\varepsilon(f) = 1$, όταν η f είναι άρτια, και $\varepsilon(f) = -1$, αν η f είναι περιττή.

Το σύνολο $\{-1, 1\}$ με πράξη το συνήθη πολ/μό αποτελεί κυκλική ομάδα με γεννήτορα το -1 και η απεικόνιση $\varepsilon : S(X) \to \{1, -1\}$ που ορίζεται με

$$\varepsilon(\varphi) = \begin{cases} 1 & \text{αν } \varphi \text{ άρτια} \\ -1 & \text{αν } \varphi \text{ περιττή} \end{cases}$$

είναι επιμορφισμός. Έτσι έχουμε $\varepsilon(\varphi\circ g) = \varepsilon(\varphi)\,\varepsilon(g)$ και είναι $\varepsilon(1_X) = 1$ και $\varepsilon(\varphi) = \varepsilon(\varphi^{-1})$.

Το πλήθος των αρτίων μεταθέσεων είναι $\frac{m!}{2}$ και αυτές αποτελούν υποομάδα της $S(X)$.

Το πλήθος των περιττών μεταθέσεων είναι επίσης $\frac{m!}{2}$, αλλά αυτές δεν αποτελούν υποομάδα της $S(X)$.

Π.χ. θεωρούμε τη συμμετρική ομάδα $S(4)$, της οποίας η τάξη είναι $4! = 1\cdot2\cdot3\cdot4 = 24$. Το ουδέτερο στοιχείο 1 είναι η μετάθεση

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = 1234.$$

Το αντίστροφο της $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = 2413$ είναι

$$f^{-1} = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = 3142.$$

Είναι

$$f\circ f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}\begin{pmatrix} 3 & 1 & 4 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Για να πάρει η $f = 2413$ τη φυσική σειρά 1234 έχουμε τους ακόλουθους βηματισμούς.

i. Για το 4 έχουμε τις δύο εναλλαγές (4, 1) και (4, 3) σε (1, 4) και (3, 4). Έτσι είναι 2134.

ii. Για το 3 δεν απαιτείται εναλλαγή.

iii. Για το 2 έχουμε μία εναλλαγή του ζεύγους (2, 1) σε (1, 2).

Άρα έχουμε συνολικά τρεις διαδοχικές εναλλαγές, δηλ. η f είναι περιττή με σημείο ε(f)=–1.

Θεωρούμε μία ομάδα G, τη συμμετρική της S(G) και μία απεικόνιση $F: G \to S(G)$ ώστε $F(g): G \to G$ να ορίζεται με $F(g)(h) = gh$ για κάθε $g, h \in G$. Τότε F(g) είναι μία μετάθεση του G και η F είναι μονομορφισμός. Επειδή η F(G) είναι υποομάδα της S(G) και η $F : G \to F(G)$ ισομορφισμός, η G μπορεί να θεωρηθεί ως υποομάδα της S(G).

Ας είναι $Aut(G) = \{f \mid f : G \to G\}$ το σύνολο των αυτομορφισμών μιας ομάδας G. Τότε το Aut(G) αποτελεί ομάδα με πράξη τη σύνθεση των αυτομορφισμών, η οποία είναι υποομάδα της S(G) και άρα μία ομάδα μετασχηματισμών του G. Ορίζουμε μία συνάρτηση

$$F : G \to Aut(G), \quad x \to F(x)$$

με τη συνάρτηση

$$F(x) : G \to G, \quad F(x)(y) = xyx^{-1}$$

Η απεικόνιση F(x) είναι αυτομορφισμός, ο οποίος ονομάζεται **εσωτερικός.** Το σύνολο όλων των εσωτερικών αυτομορφισμών μιας ομάδας G, συμβολικά $E_\sigma(G)$, είναι κανονική υποομάδα της Aut(G). Προκύπτει ότι η F είναι ομομορφισμός.

Μία ομάδα G λέγεται **πλήρης,** όταν κάθε αυτομορφισμός της είναι εσωτερικός. Τότε ο ομομορφισμός $F : G \to Aut(G)$ είναι ισομορφισμός επί την A(G). Όλες οι συμμετρικές ομάδες S(X) είναι πλήρεις εκτός από τις S(n) για n=2 και n=6.

Αν H είναι μία κανονική υποομάδα της G, τότε έχουμε

$$F(x)H = xHx^{-1} = H$$

και λέμε ότι η H είναι ολικά σταθερή ως προς κάθε εσωτερικό αυτομορφισμό της G.

Αν H είναι μία τυχαία υποομάδα της G, τότε το σύνολο xHx^{-1} είναι υποομάδα της G για κάθε $x \in G$.

Δύο υποομάδες H_1 και H_2 μιας ομάδας G λέγονται **συζυγείς,** συμβολικά $H_1 \sim H_2$, όταν υπάρχει κάποιο $x \in G$ ώστε να είναι $H_2 = xH_1x^{-1}$. Η $\sim$ είναι μία σχέση ισοδυναμίας επί του συνόλου των υποομάδων της G. Το πλήθος των διαφορετικών συζυγών υποομάδων της G προς μία υποομάδα H είναι ίσο με το πλήθος των αριστερών θηκών gG_H της υποομάδος

$$G_H = \{g \in G \mid gHg^{-1} = H\} \quad \text{της} \quad G.$$

Η απεικόνιση

$$F(x) : H_1 \to H_2 , \quad F_x(y) = xyx^{-1}$$

είναι ισομορφισμός. Έτσι μπορούμε να ταυτίσουμε αλγεβρικά συζυγείς υποομάδες.

Ας είναι x και y στοιχεία μιας ομάδας G. Τότε το x λέγεται **συζυγές** του y, συμβολικά $x \sim y$, όταν είναι $y = zxz^{-1}$ για κάποιο $z \in G$. Η σχέση $x \sim y$ είναι μία σχέση ισοδυναμίας επί του G και διαμερίζει το G σε ξένες κλάσεις που λέγονται **κλάσεις συζυγίας.**

Ένα σύνολο A εφοδιασμένο με δύο πράξεις, οι οποίες συμβολίζονται συνήθως προσθετικά και πολ/κά αντίστοιχα, ονομάζεται **δακτύλιος,** όταν ισχύουν τα ακόλουθα

i. Το A αποτελεί αντιμεταθετική ομάδα ως προς την πρόσθεση.

ii. Το A είναι ημιομάδα ως προς τον πολ/μό .

iii. Ο πολ/μός είναι επιμεριστικός ως προς την πρόσθεση, δηλ. είναι

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

Ένας δακτύλιος A λέγεται **αντιμεταθετικός,** όταν είναι $xy=yx$ για κάθε $x, y \in A$ και **μοναδιαίος,** όταν έχει ουδέτερο στοιχείο, συμβολικά 1, ως προς τον πολ/μό. Στα επόμενα θα θεωρούμε ότι ο δακτύλιος είναι μοναδιαίος. Το ουδέτερο στοιχείο της πρόσθεσης, θα συμβολίζεται με 0 και θα λέγεται μηδέν. Ισχύουν οι ιδιότητες

$$0x = x0 = 0, \quad -x = (-1)x = x(-1), \quad -xy = (-x)y = x(-y), \quad (-x)(-y) = xy, \quad (-1)(-1) = 1$$

όπου $-x$ συμβολίζει το αντίθετο του x, δηλ. είναι $x-x=0$. Είναι πάντα $0 \neq 1$, διότι είναι $A=\{0\}$ για $0=1$. Πράγματι όταν $0=1$, είναι $x=x1=x0=0$.

Ένα υποσύνολο B ενός δακτυλίου A λέγεται **υποδακτύλιος** του A, όταν είναι εφοδιασμένο με τις πράξεις του A ως προς τις οποίες αποτελεί δακτύλιο.

Έαν υποσύνολο J ενός δακτυλίου A λέγεται **αριστερό** (αντ. **δεξιό**) **ιδεώδες** του A, όταν είναι υποομάδα της προσθετικής ομάδας του A και $ax \in J$ (αντ. $xa \in J$) για κάθε $a \in A$ και $x \in J$.

Το J λέγεται ιδεώδες του A όταν είναι συγχρόνως αριστερό και δεξιό ιδεώδες του.

Για κάθε δακτύλιο A, οι δακτύλιοι $\{0\}$ και A είναι ιδεώδη του A. Αν $x \in A$, το σύνολο $xA = \{xa \mid a \in A\}$ (αντ. Ax) είναι δεξιό (αντ. αριστερό) ιδεώδες του A. Όταν είναι $xA=Ax$, τότε το xA είναι ιδεώδες του A, λέγεται **κύριο ιδεώδες,** συμβολίζεται με (x) και λέμε ότι το (x) παράγεται από το x. Είναι $(x) = A$ ανν το x είναι αντιστρεπτό στοιχείο του A, δηλ. υπάρχει το αντίστροφο x^{-1} του x και $x^{-1} \in A$.

Ένα ιδεώδες J ενός δακτυλίου A είναι υποδακτύλιος του A και επιπλέον είναι κανονική υποομάδα της προσθετικής δομής του A. Η σχέση

$$x \equiv y(J), \quad \text{όταν} \quad x-y \in J$$

όπου $x, y \in A$ είναι μία σχέση ισοδυναμίας συμβιβαστή με την προσθετική και την πολ/κή δομή του A, δηλ. είναι

$$x_1 \equiv x_2(J),\ y_1 \equiv y_2(J) \Rightarrow (x_1+y_1) \equiv (x_2+y_2)(J),\ x_1y_1 \equiv x_2y_2(J),$$

Έτσι μπορούμε να ορίσουμε μία προσθετική και μία πολ/ κή πράξη επί του πηλικοσυνόλου

$$A / J = \{\overline{\alpha} = \alpha + J \mid \alpha \in A\}$$

όπως παρακάτω

$$\overline{\alpha} \dot{+} \overline{\beta} = (\alpha+J) \dot{+} (\beta+J) = (\alpha+\beta)+J = \overline{\alpha+\beta}$$

$$\overline{\alpha} \cdot \overline{\beta} = (\alpha+J)\cdot(\beta+J) = \alpha\beta+J = \overline{\alpha\beta}$$

Συνήθως παραλείπουμε τις τελείες, όταν δεν υπάρχει ασάφεια. Ως προς τις παραπάνω πράξεις, το σύνολο A/J αποτελεί δακτύλιο, ο οποίος ονομάζεται **πηλικοδακτύλιος** του A δια του J.

Θεωρούμε δύο δακτυλίους A και B, τους υποδακτυλίους A_1 και B_1 αυτών αντιστοίχως και ένα ιδεώδες J του B. Μία απεικόνιση $\varphi : A \to B$ λέγεται **ομομορφισμός,** όταν η φ διατηρεί τις πράξεις των δακτυλίων, δηλ. όταν είναι $\varphi(x+y) = \varphi(x)+\varphi(y)$ και $\varphi(xy) = \varphi(x)\varphi(y)$.

Ένας ομομορφισμός λέγεται επιμορφισμός (αντ. μονομορφισμός, ισομορφισμός), όταν η φ είναι επιρριπτική (αντ. ενριπτική, αμφιμονότιμη) απεικόνιση.

Ένας ομομορφισμός (αντ. ισομορφισμός) $\varphi : A \to A$ λέγεται ενδομορφισμός (αντ. αυτομορφισμός) του A.

Όταν $\varphi : A \to B$ είναι ομομορφισμός, τότε ισχύουν οι ακόλουθες ιδιότητες:

α. $\varphi(0) = 0,\ \varphi(-x) = -\varphi(x),\ \varphi(1) = 1.$

β. Ο πυρήνας $\varphi^{-1}(0) = \{x \in A \mid \varphi(x) = 0\}$ του φ είναι ιδεώδες του A.

γ. Η εικόνα $\varphi(A_1)$ είναι υποδακτύλιος του B και η αντίστροφη εικόνα $\varphi^{-1}(B_1)$ είναι υποδακτύλιος του A και περιέχει τον πυρήνα.

δ. Η αντίστροφη εικόνα $\varphi^{-1}(J)$ είναι ιδεώδες του A.
Ένα ιδεώδες J ενός δακτυλίου A λέγεται **μεγιστοποιημένο** ή **σχετικά μέγιστο,** όταν δεν περιέχεται σε κανένα άλλο ιδεώδες του A.

Ένας δακτύλιος K λέγεται **σώμα,** όταν είναι $K \neq \{0\}$ και κάθε στοιχείο του $K-\{0\}$ έχει πολ/κό αντίστροφο, δηλ. για κάθε $x \in K-\{0\}$ υπάρχει μοναδικό $x^{-1} \in K-$

$\{0\}$ ώστε να είναι $xx^{-1} = x^{-1}x=1$.

Ένας υποδακτύλιος F ενός σώματος K, ο οποίος είναι σώμα ως προς τις πράξεις του K, λέγεται **υπόσωμα** του K και το K σώμα επέκτασης του F.

Ένα πηλικοδακτύλιος A/J είναι σώμα ανν το ιδεώδες J του A είναι μεγιστοποιημένο.

Ένα σώμα K λέγεται **αλγεβρικώς κλειστό,** όταν κάθε πολυώνυμο με συντελεστές στο K έχει όλες τις ρίζες του στο K.

Τα σώματα διακρίνονται στις ακόλουθες δύο κατηγορίες.

α. Σώματα **χαρακτηριστικής μηδέν,** τα οποία περιέχουν άπειρα στοιχεία. Από τα σώματα αυτά, τα πιο γνωστά είναι το σώμα R των πραγματικών αριθμών και το σώμα C των μιγαδικών αριθμών. Τα σώματα R και C αποτελούν τη βάση επί της οποίας γίνεται όλη η παραπέρα ανάπτυξη της θεωρίας.

Το σώμα R είναι το σύνολο όλων των πραγματικών αριθμών εφοδιασμένο με τις γνωστές πράξεις της πρόσθεσης και του πολλαπλασιασμού.

Το σώμα C των μιγαδικών αριθμών είναι το καρτεσιανό γινόμενο $R \times R$ με πράξεις που ορίζονται όπως παρακάτω

$$(\alpha, \beta)+(\gamma, \delta) = (\alpha+\gamma, \beta+\delta), \quad (\alpha, \beta)(\gamma, \delta) = (\alpha\gamma-\beta\delta, \alpha\delta+\beta\gamma)$$

Η απεικόνιση

$$\varphi : R \to C, \quad \varphi(\alpha) = (\alpha, 0)$$

είναι μονομορφισμός (βουτιά) και έτσι μπορούμε να ταυτίσουμε αλγεβρικά το R με την εικόνα $\varphi(R)$, δηλ. κάθε πραγματικός αριθμός α ταυτίζεται με το ζεύγος $(\alpha, 0)$. Με την έννοια αυτή το σώμα R θεωρείται υπόσωμα του C.

Κάθε μιγαδικός αριθμός $z = (\alpha, \beta)$ γράφεται με τη μορφή

$$z = (1, 0)\alpha+(0, 1)\beta = \alpha+i\beta,$$

όπου τα ζεύγη $(1, 0)$ και $(0, 1)$ είναι αντίστοιχα η πραγματική μονάδα 1 και η φανταστική μονάδα i.

Είναι

$$(\alpha, \beta)(1, 0) = (1, 0)(\alpha, \beta) = (\alpha, \beta) \quad \text{και} \quad i^2 = (0, 1)(0, 1) = (-1, 0) = -(1, 0) = -1$$

και έτσι γράφουμε $i = \sqrt{-1}$ στο C.

Ο συζυγής ενός μιγαδικού αριθμού $z = (\alpha, \beta) = \alpha+i\beta$ είναι ο αριθμός

$$\overline{z} = (\alpha, -\beta) = \alpha-i\beta.$$

Είναι $z=0$ ανν $\alpha=0$ και $\beta=0$.

Για τους συζυγείς $\overline{z}_1 = \alpha-i\beta$ και $\overline{z}_2=\gamma-i\delta$ δύο μιγαδικών αριθμών

$$z_1 = \alpha+i\beta \quad \text{και} \quad z_2 = \gamma+i\delta$$

ισχύουν οι ιδιότητες

$$\overline{z_1+z_2} = \overline{z}_1+\overline{z}_2,\ \overline{z_1\cdot z_2} = \overline{z}_1\cdot\overline{z}_2 \quad \text{και} \quad \left(\overline{\frac{z_1}{z_2}}\right)=\frac{\overline{z}_1}{\overline{z}_2}$$

Για κάθε $z = \alpha+i\beta$ το αντίστροφό του είναι $z^{-1} = \left(\frac{\alpha}{|z|^2}, \frac{-\beta}{|z|^2}\right)$, όπου είναι $|z|^2 = z\overline{z} = \alpha^2+\beta^2$.

Ένας μιγαδικός αριθμός z είναι πραγματικός (αντ. φανταστικός) ανν

$$z = \overline{z} \quad (\text{αντ. } z = -\overline{z}).$$

Το σώμα C είναι αλγεβρικά κλειστό, ενώ το σώμα R δεν είναι αλγεβρικά κλειστό. Είναι γνωστή η περίπτωση ενός τριωνύμου με συντελεστές στο R και αρνητική διακρίνουσα. Τότε το τριώνυμο έχει μιγαδικές συζυγείς ρίζες.

Το σώμα Q των ρητών αριθμών είναι υπόσωμα του R και το μικρότερο υπόσωμα του C.

Κάθε άπειρο σώμα K (χαρακτηριστικής 0) περιέχει ένα υπόσωμα F ισομορφικό προς το σώμα Q των ρητών αριθμών. Έτσι το Q μπορεί να θεωρηθεί αλγεβρικά ως υπόσωμα του K και με διαδοχικές επεκτάσεις να προσδιορίσουμε τα στοιχεία του K.

β. Σώματα χαρακτηριστικής p, όπου $p>1$ είναι **πρώτος** αριθμός, δηλ. ο p είναι ακέραιος αριθμός με μοναδικό διαιρέτη το ίδιο το p. Αυτά τα σώματα έχουν πεπερασμένο πλήθος στοιχείων, δηλ. είναι πεπερασμένα σώματα.

Αμέσως παρακάτω κάνουμε μία σύντομη αλλά βασική κατασκευή αυτών των σωμάτων.

Το σύνολο των ακεραίων Z εφοδιασμένο με τις γνωστές πράξεις της πρόσθεσης και του πολλαπλασιασμού αποτελεί αντιμεταθετικό δακτύλιο με μοναδιαίο στοιχείο τη μονάδα.

Ας είναι ν ο τυχαίος ακέραιος. Τότε το σύνολο

$$\nu Z = \{\nu k \mid k\in Z\}$$

είναι κανονική υποομάδα της προσθετικής ομάδας του Z, διότι είναι $x+\nu Z-x = \nu Z$ για κάθε $x\in Z$.

Επίσης η σχέση $\equiv$ επί του Z, η οποία ορίζεται όπως παρακάτω «$x\equiv y(\nu)$, όταν υπάρχει $z\in Z$ ώστε να είναι $x-y = \nu z$» είναι συμβιβαστή με την προσθετική δομή του Z, δηλ. είναι

$$x_1\equiv y_1(\nu),\ x_2\equiv y_2(\nu) \Rightarrow (x_1+x_2)\equiv(y_1+y_2)(\nu)\ .$$

Αλλά είναι $x-y\in\nu Z$ και έτσι ορίζεται μία προσθετική πράξη επί του πηλικοσυνόλου

$$Z/\nu Z = \{\overline{x} = x+\nu Z \mid \text{για κάθε } x\in Z\}$$

η οποία είναι

$$x\dot{+}y = (x+\nu Z)\dot{+}(y+\nu Z) = x+y+\nu Z = \overline{x+y} \quad \text{για κάθε } x, y\in Z.$$

Το σύνολο $Z/\nu Z$, εφοδιασμένο με την παραπάνω πράξη, αποτελεί αντιμεταθετική ομάδα. Οι τελείες συνήθως παραλείπονται, όταν δεν υπάρχει ασάφεια. Γράφουμε συμβολικά $Z_\nu = Z/\nu Z$.

Το ουδέτερο στοιχείο είναι η κλάση

$$\overline{0} = 0+\nu Z = \nu Z.$$

Αν θέσουμε αντί ν το $-\nu$, τότε είναι

$$x-y = -\nu z = (-1)\nu z = \nu(-z), \quad \text{όπου } -\nu\in Z,$$

και άρα μπορούμε πάντα να θεωρούμε ότι είναι $\nu\geq 0$.

Κάθε υποομάδα H της προσθετικής ομάδας Z έχει τη μορφή $H=\nu Z$ για μοναδικό $\nu\in Z$ και $\nu\geq 0$. Το ν είναι το μικρότερο θετικό στοιχείο του H. Αν $H = \{0\}$, τότε είναι $\nu=0$ και όταν $H\neq\{0\}$, τότε ο ακέραιος $\nu\neq 0$.

Η σχέση $x-y = \nu z$ δείχνει ότι το ν διαιρεί τα x, y και ας είναι $x = \nu k+\tau$ και $y = \nu\lambda+s$, όπου $0\leq\tau, s<\nu$. Αλλά τότε είναι $x-y = \nu(k-\lambda)+\tau-s$ και επειδή $x-y = \nu z$, προκύπτει ότι $\tau=s$, δηλ. η σχέση $\equiv$ μπορεί να εκφρασθεί ισοδύναμα όπως παρακάτω

«$x\equiv y(\nu)$, όταν η διαίρεση των x και y με το ν δίνει το ίδιο υπόλοιπο».

Άρα, για $\nu\geq 0$, προκύπτει αμέσως ότι ότι η τάξη της ομάδας $Z/\nu Z$ είναι ν και ότι οι ακέραιοι τ, για τους οποίους είναι $0\leq\tau<\nu$, αποτελούν ένα σύστημα αντιπροσώπων των κλάσεων της $Z/\nu Z$, δηλ. τα στοιχεία της $Z/\nu Z$ είναι

$$\overline{0} = 0+\nu Z, \quad \overline{1}=1+\nu Z, \ldots, \overline{\nu-1}= (\nu-1)+\nu Z$$

όπου είναι $\overline{k} = k+\nu Z = \{k+\nu\mu \mid \text{για κάθε } \mu\in Z\}$ και $\nu\overline{k} = \overline{0}$.

Παρατηρούμε ότι για $k\geq\nu$, η κλάση $\overline{k} = k+\nu Z$ συμπίπτει με μία από τις παραπάνω. Πράγματι η διαίρεση του k δια του ν δίνει μία σχέση $k=\nu\lambda+\tau$ με $0\leq\tau<\nu$ και άρα είναι

$$\overline{k} = \tau+\nu\lambda+\nu Z = \tau+\nu Z$$

διότι το τυχαίο στοιχείο $\nu\lambda+\nu\rho\in\nu\lambda+\nu Z$ και γράφεται $\nu(\lambda+\rho)$, δηλ. $\nu(\lambda+\rho)\in\nu Z$.

Επειδή για $k\geq\nu$, το $\overline{k}= k+\nu Z$ ανήκει στο $Z/\nu Z$, ορίζεται το αντίθετο $-\overline{k}$ και ανήκει στην $Z/\nu Z$. Η εύρεση του αντιθέτου ενός $\overline{x}\in Z_\nu$, όπου είναι $Z_\nu = Z/\nu Z$, ανάγεται στον προσδιορισμό ενός $\overline{y}\in Z_\nu$ για το οποίο είναι

$$\bar{x} \dot{+} \bar{y} = \bar{0} = \nu Z.$$

Άρα το αντίθετο του $\bar{x}$ είναι το $\overline{-x} = \overline{\nu - x}$, διότι είναι $\overline{-x} \dot{+} \overline{\nu - x} = \bar{\nu} = \bar{0} = \nu Z$.

Η προσθετική ομάδα Z παράγεται από τη μονάδα και έτσι η Z_ν παράγεται από το στοιχείο $\bar{1} = 1 + \nu Z$, δηλ. η Z_ν είναι κυκλική. Κάθε πεπερασμένη κυκλική ομάδα G τάξης ν είναι ισομορφική προς την Z_ν και κάθε άπειρη κυκλική ομάδα είναι ισομορφική με την προσθετική ομάδα Z.

Ας είναι $\nu > 0$. Κάθε υποομάδα H της Z_ν έχει τη μορφή $H = \mu Z / \nu Z$ και είναι ισόμορφη με την ομάδα $Z / \rho Z$, όπου ρ είναι η τάξη της H και μ ο δείκτης της στην Z_ν, δηλ. είναι $\nu = \rho\mu$. Αντίστροφα, αν $\nu = \rho\mu$, όπου ρ και μ είνει θετικοί ακέραιοι, τότε η ομάδα νZ περιέχεται στην μZ και η $\mu Z / \nu Z$ είναι υποομάδα της Z_ν με δείκτη μ και τάξη ρ, δηλ. όταν το μ είναι διαιρέτης του ν, τότε έχουμε $\nu Z \subseteq \mu Z$ και η $\mu Z / \nu Z$ είναι υποομάδα της Z_ν.

Μία ομάδα G λέγεται **απλή**, όταν δεν περιέχει καμμία κανονική υποομάδα εκτός από τις $\{e\}$ και G, όπου e είναι το ουδέτερο στοιχείο της G. Ένας ακέραιος $p > 1$ λέγεται πρώτος, όταν ο μοναδικός μεγαλύτερης της μονάδας διαιρέτης του είναι ο ίδιος ο p. Έτσι ο p έχει την μοναδική ανάλυση $p = p1$ και άρα p είναι πρώτος ανν η Z / pZ είναι απλή ομάδα.

Επειδή κάθε ιδεώδες του Z είναι προσθετική υποομάδα του, θα έχει τη μορφή νZ για κάποιο ακέραιο $\nu \geq 0$. Αλλά το νZ είναι το κύριο ιδεώδες $(\nu) = \nu Z$, διότι είναι $\nu Z = Z\nu$. Επειδή η μονάδα 1 είναι το μόνο αντιστρεπτό στοιχείο του Z, θα έχουμε $(1) = Z$. Το ιδεώδες $\{0\} = 0Z = 0$. Άρα, για κάθε $\nu > 1$, είναι $(\nu) = \nu Z \neq Z$ και $\nu = \nu 1 \in \nu Z$. Επίσης είναι $\nu Z \subseteq \mu Z$ ανν $\nu = \mu k$.

Άρα κάθε μεγιστοποιημένο ιδεώδες του Z θα έχει τη μορφή pZ, όπου p είναι πρώτος αριθμός. Έτσι προκύπτει ότι ο δακτύλιος $Z_p = Z / pZ$ είναι σώμα ανν ο p είναι πρώτος αριθμός.

Το σώμα Z_p περιέχει p στοιχεία και λέμε ότι είναι χαρακτηριστικής p. Τα σώματα Z_p είναι τα βασικά πεπερασμένα σώματα για τις εφαρμογές. Για κάθε στοιχείο $\bar{x} \in Z_p$ είναι $p\bar{x} = \bar{0} = pZ$.

Για κάθε φυσικό αριθμό ν και κάθε πρώτο αριθμό $p > 1$ υπάρχει ένα πεπερασμένο σώμα K με p^ν στοιχεία, το οποίο περιέχει ένα υπόσωμα F ισομορφικό με το σώμα $Z_p = Z / pZ$. Έτσι θεωρούμε ότι το Z_p είναι υπόσωμα του K και επεκτείνοντας το Z_p με μία απλή διαδικασία μπορούμε να προσδιορίσουμε το σώμα K μετά ένα πεπερασμένο πλήθος βηματισμών.

Παραδείγματα

1. Το σύνολο N των φυσικών αριθμών αποτελεί ημιομάδα ως προς την

πρόσθεση και μονοειδές ως προς τον πολλαπλασιασμό.

Το σύνολο $N_0 = N \cup \{0\}$ αποτελεί μονοειδές ως προς την πρόσθεση. Το μηδέν είναι πολ/κό απορροφητικό στοιχείο του N.

2. Θεωρούμε ένα τυχαίο σύνολο A επί του οποίου ορίζουμε την πράξη $\alpha\beta=\alpha$ για κάθε $\alpha, \beta \in A$. Τότε το A γίνεται ημιομάδα, η οποία ονομάζεται αριστερή μηδενική. Με αντίστοιχο τρόπο ορίζεται η δεξιά μηδενική ημιομάδα .

3. Θεωρούμε δυο μη-κενά σύνολα A και B και επί του καρτεσιανού γινομένου $A \times B$ ορίζουμε την πράξη $(\alpha, \beta)(\gamma, \delta) = (\alpha, \delta)$. Τότε το $A \times B$ γίνεται ημιομάδα και ονομάζεται ορθογώνιο τμήμα.

4. Αν $P(A)$ είναι το σύνολο των υποσυνόλων ενός μη-κενού συνόλου A, τότε μπορούμε να ορίσουμε επί του $P(A)$ τις πράξεις της ένωσης $\cup$ και της τομής $\cap$ ως προς καθεμιά από τις οποίες το $P(A)$ είναι μονοειδές. Το κενό σύνολο $\varnothing$ είναι απορροφητικό ως προς την τομή και ουδέτερο ως προς την ένωση. Το A είναι απορροφητικό ως προς την ένωση και ουδέτερο ως προς την τομή.

5. Στον προτασιακό λογισμό είναι απαραίτητο να γνωρίζουμε αν μία πρόταση είναι αληθής ή ψευδής, αλλά όχι συγχρόνως αληθής και ψευδής. Όταν έχουμε σύνθετες προτάσεις, δηλ. εκφράσεις αποτελούμενες από δύο ή περισσότερες προτάσεις, τότε είναι απαραίτητο να γνωρίζουμε την αλήθεια ή το ψεύδος της σύνθετης πρότασης. Η αλήθεια ή το ψεύδος μιας πρότασης λέγονται αληθείς τιμές της. Εδώ έχουμε δύο πράξεις τη σύζευξη, συμβολικά $\wedge$, και τη διάζευξη, συμβολικά $\vee$, οι οποίες εκφράζονται με τις λέξεις «και» και «ή» αντίστοιχα. Επίσης υπάρχει μία απεικόνιση που λέγεται άρνηση, συμβολικά $\neg$, και εκφράζεται με τη λέξη «όχι». Η $\neg$ λέγεται συμπληρωματική απεικόνιση.

Στο λογισμό γράφουμε προσθετικά και πολ/κά τις πράξεις $\vee$ και $\wedge$ αντίστοιχα και χρησιμοποιούμε τα σύμβολα 0 και 1 για τις αληθείς τιμές «ψευδής» και «αληθής» αντίστοιχα. Έτσι έχουμε τους ακόλουθους πίνακες των πράξεων στο σύνολο $A = \{0, 1\}$.

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

$\neg$	
0	1
1	0

Το A είναι μονοειδές ως προς την πρόσθεση και ημιομάδα ως προς τον πολλαπλασιασμό και ονομάζεται αλγεβρικό δίκτυο.

6. Ονομάζουμε **σχέση** επί ενός συνόλου A κάθε υποσύνολο ρ του καρτεσιανού γινομένου $A \times A$. Ας είναι $R(A)$ το σύνολο των σχέσεων επί του A. Στο $R(A)$

ορίζουμε τη σύνθεση, συμβολικά $\circ$, ως πράξη όπως παρακάτω

$$\rho\circ s = \{(\alpha, \gamma)\in A\times A \mid (\exists\, \beta\in A) : (\alpha, \beta)\in \rho \text{ και } (\beta, \gamma)\in s\}.$$

Τότε το $R(A)$ αποτελεί μονοειδές με ουδέτερο στοιχείο την ταυτοτική σχέση

$$1_A = \{(\alpha, \alpha) \mid \alpha\in A\}.$$

Άλλες πράξεις που ορίζονται στο $R(A)$ είναι η ένωση $\cup$

$$\rho\cup s = \{(\alpha_i, \alpha_j)\in A\times A \mid (\alpha_i, \alpha_j)\in \rho \text{ ή } (\alpha_i, \alpha_j)\in s\}$$

και η τομή

$$\rho\cap s = \{(\alpha_i, \alpha_j)\in A\times A \mid (\alpha_i, \alpha_j)\in \rho \text{ και } (\alpha_i, \alpha_j)\in s\}.$$

Επίσης, για κάθε σχέση ρ, ορίζονται η αντίστροφή της

$$\rho^{-1} = \{(\alpha, \beta) \mid (\beta, \alpha)\in \rho\}$$

και η συμπληρωματική σχέση $\rho^c = (A\times A)-\rho$.

7. Το σύνολο $2Z = \{2\nu/\nu\in Z\}$ είναι κανονική υποομάδα της προσθετικής ομάδας Z. Είναι

$$2k+2\lambda = 2(k+\lambda)\in 2Z, \qquad 2k-2k = 0, \qquad 2k+0 = 2k \text{ και } \mu+2k-\mu = 2k\in 2Z$$

για κάθε $k, \lambda, \mu\in Z$.

Η $2Z$ γράφεται αναλυτικά

$$(2) = 2Z = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}.$$

Το πηλικοσύνολο $Z_2 = Z/2Z = \{\overline{0}, \overline{1}\} = \{2Z, 1+2Z\}$ είναι προσθετική ομάδα με ουδέτερο στοιχείο την κλάση $\overline{0} = 2Z$, διότι έχουμε $\overline{0}+\overline{0} = \overline{0}$ και $\overline{0}\dot{+}\overline{1} = \overline{1}$. Το αντίθετο του $\overline{1}$ είναι το ίδιο το $\overline{1}$, διότι

$$\overline{1}\dot{+}\overline{1} = (1+2Z)\dot{+}(1+2Z) = 2+2Z = 2Z.$$

Η ομάδα $2Z$ είναι κυκλική, διότι παράγεται από το στοιχείο $2 = 2\cdot 1$, επειδή η Z παράγεται από τη μονάδα 1. Έτσι η Z_2 είναι κυκλική και παράγεται από το $\overline{1} = 1+2Z$.

Ας δούμε μερικά στοιχεία της Z_2: Έχουμε

$$\overline{3} = 3+2Z = 1+2+2Z = 1+2Z = \overline{1}$$

$$\overline{8} = 8+2Z = 2\cdot 4+2Z = 2Z = \overline{0}$$

$$\overline{-5} = -5+2Z = -5+2\cdot 3+2Z = 1+2Z = \overline{1}$$

$\overline{-8} = -8+2Z = -8+2\cdot 4+2Z = 0+2Z = \overline{0}$

$\overline{7} = 7+2Z = 1+2\cdot 3+2Z = 1+2Z = \overline{1}$

$\overline{-7} = -(7+2Z) = (-1)\cdot(7+2Z) = -7+2Z = (1-2\cdot 4)+2Z = 1-2\cdot 4+2Z = 1+2(-4)+2Z =$

$=1+2Z = \overline{1}.$

Η πράξη σε μία ομάδα Z_2 παριστάνεται με τον πίνακα

$\dot{+}$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

όπου τα στοιχεία της Z_2 γράφονται στην πρώτη γραμμή και πρώτη στήλη και το αποτέλεσμα της πράξης στη διασταύρωση κάθε γραμμής με κάθε στήλη.

Το $2Z$ είναι το ιδεώδες (2) που παράγεται από το 2. Επειδή το $2>1$ είναι πρώτος αριθμός, το Z_2 είναι σώμα. Είναι το μικρότερο πεπερασμένο σώμα με χαρακτηριστική 2. Η πολ/κή πράξη είναι $\overline{k}\cdot\overline{\mu} = (k+2Z)\cdot(\mu+2Z) = k\mu+2Z = \overline{k\mu}$ για κάθε $k, \mu\in Z$ και ως προς αυτήν το Z_2 αποτελεί αντιμεταθετική ομάδα.

9. Θεωρούμε το ιδεώδες $(6) = 6Z = (\ldots, -12, -6, 0, 6, 12, \ldots\}$. Τότε το πηλικοσύνολο $Z_6 = Z/6Z$ αποτελεί δακτύλιο και είναι

$$Z_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$$

όπου έχουμε τις κλάσεις

$\overline{0} = 6Z$; $\overline{1} = 1+6Z = \{\ldots, -11, -5, 1, 7, 13, \ldots\}$

$\overline{2} = 2+6Z = \{\ldots, -10, -4, 2, 8, 14, \ldots\}$; $\overline{3} = 3+6Z = \{\ldots, -9, -3, 3, 9, 15,\ldots\}$

$\overline{4} = 4+6Z = \{\ldots, -8, -2, 4, 10, 16, \ldots\}$, $\overline{5} = 5+6Z = \{\ldots, -7, -1, 5, 11, 17,\ldots\}$

Ας δούμε τα αποτελέσματα μερικών πράξεων στον Z_6. Είναι

$\overline{4}\dot{+}\overline{5} = (4+6Z)\dot{+}(5+6Z) = (4+5)+6Z = 9+6Z = 3+6\cdot 1+6Z = 3+6Z = \overline{3}$

$\overline{4}\cdot\overline{5} = (4\cdot 5)+6Z = 20+6Z = 2+6\cdot 3+6Z = 2+6Z = \overline{2}.$

Το αντίθετο $-\overline{4}$ του $\overline{4}$ είναι το $\overline{2}$, διότι

$$\overline{4}\dot{+}\overline{2} = (4+2)+6Z = 6\cdot 1+6Z = 6Z = \overline{0}$$

Μέγιστος κοινός διαιρέτης δύο ακεραίων είναι ο μεγαλύτερος ακέραιος, ο οποίος

διαιρεί αυτούς. Δύο ακέραιοι λέγονται **σχετικά πρώτοι,** όταν ο μέγιστος κοινός διαιρέτης τους είναι η μονάδα.

Τα αντιστρεπτά στοιχεία ενός δακτυλίου Z_ν είναι οι κλάσεις $\overline{k} = k+\nu Z$, όπου οι ακέραιοι k και ν είναι σχετικά πρώτοι.

Άρα το μοναδικό αντιστρεπτό στοιχείο του Z_6, είναι το $\overline{5}$, διότι οι ακέραιοι 5 και 6 είναι σχετικά πρώτοι. Έχουμε

$$\overline{5}\cdot\overline{5} = \overline{25} = 25+6Z = 1+6\cdot 4+6Z = 1+6Z = \overline{1}$$

δηλ. το αντίστροφο του $\overline{5}$ είναι το $\overline{5}$.

Ας δούμε μία βασική διαφορά μεταξύ των δακτυλίων και των σωμάτων. Θεωρούμε το πολυώνυμο $\varphi(x) = \overline{1}x^2+\overline{5}x$ με συντελεστές από το δακτύλιο Z_6. Τότε είναι

$$\varphi(\overline{0}) = \overline{0}, \quad \varphi(\overline{1}) = \overline{1}\,\overline{1}^2+\overline{5}\,\overline{1} = \overline{8} = \overline{0}, \quad \varphi(\overline{2}) = \overline{1}\,\overline{2}^2+\overline{5}\,\overline{2} = \overline{14} = \overline{2}$$

$$\varphi(\overline{3}) = \overline{3}^2+\overline{5}\,\overline{3} = \overline{9}+\overline{15} = \overline{24} = \overline{0}, \qquad \varphi(\overline{4}) = \overline{16}+\overline{20} = \overline{0}, \quad \varphi(\overline{5}) = \overline{25}+\overline{25} = \overline{50} = \overline{2}$$

και άρα το $\varphi(x)$ έχει ρίζες $\overline{0}, \overline{1}, \overline{3}$ και $\overline{4}$ στον δακτύλιο Z_6, δηλ. ένα πολυώνυμο δευτέρου βαθμού έχει 4 ρίζες στο Z_6. Αυτό δεν μπορεί να συμβεί σε ένα σώμα K, όπου ένα πολυώνυμο βαθμού μ δεν μπορεί να έχει περισσότερες από μ ρίζες στο K.

10. Ο δακτύλιος $Z_5 = Z/5Z$ είναι σώμα, διότι ο ακέραιος 5 είναι πρώτος. Είναι $Z_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ και $Z_5-\{\overline{0}\} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

Το $Z_5-\{\overline{0}\}$ αποτελεί πολλαπλασιαστική ομάδα και ας υπολογίσουμε τα αντίστροφα των στοιχείων του. Γνωρίζουμε ότι το αντίστροφο του τυχαίου $\overline{k}$ είναι το $\overline{k}^{5-2} = \overline{k}^3$.

Πράγματι, όταν ένας δακτύλιος Z_ν είναι σώμα, για κάθε στοιχείο του $\overline{k}$ έχουμε $\overline{k}^{\nu-1} = \overline{1}$, διότι η πολλαπλασιαστική ομάδα $Z_\nu-\{\overline{0}\}$, έχει τάξη $\nu-1$. Άρα είναι $\overline{k}\overline{k}^{\nu-2} = \overline{1}$ δηλ. η αντίστροφη κλάση της $\overline{k}$ είναι η $\overline{k}^{\nu-2}$. Επίσης είναι $\nu\overline{k} = \overline{0}$ και $\overline{k}^\nu = \overline{k}$.

Έτσι έχουμε

$$\overline{1}\,\overline{1}^3 = \overline{1}\,\overline{1} = \overline{1}, \quad \overline{2}\,\overline{2}^3 = \overline{2}\,\overline{8} = \overline{16} = 1+5\cdot 3+5Z = 1+5Z = 1,$$

$$\overline{3}\,\overline{3}^3 = \overline{3}\,\overline{27} = \overline{81} = 81+5Z = 1+5\cdot 16+5Z = 1+5Z = \overline{1},$$

$$\overline{4}\,\overline{4}^3 = \overline{4}\,\overline{64} = \overline{256} = 1+5\cdot 51+5Z = 1+5Z = \overline{1} \quad \text{και είναι}$$

$$\overline{1}^3 = \overline{1}, \quad \overline{2}^3 = \overline{8} = 8+5Z = 3+5\cdot 1+5Z = 3+5Z = \overline{3},$$

$\overline{3}^3 = \overline{27} = 27+5Z = 2+5\cdot 5+5Z = 2+5Z = \overline{2}$,

$\overline{4}^3 = \overline{64} = 64+5Z = 4+5\cdot 12+5Z = 4+5Z = \overline{4}$.

Άρα τα αντίστροφα των $\overline{1}$, $\overline{2}$, $\overline{3}$ και $\overline{4}$ είναι αντιστοίχως τα $\overline{1}$, $\overline{3}$, $\overline{2}$ και $\overline{4}$.

Θεωρούμε μία ομάδα G με ουδέτερο στοιχείο e, ένα μη-κενό σύνολο X, τη συμμετρική ομάδα $S(X)$ και το σύνολο X^X όλων των απεικονίσεων

$$\sigma: X\to X.$$

Τα σύνολα $S(X)$ και X^X με πράξη τη σύνθεση των συναρτήσεων αποτελούν αντίστοιχα ομάδα και μονοειδές με ουδέτερο στοιχείο την ταυτοτική απεικόνιση $1: X\to X$.

Κάθε απεικόνιση $h: G\to X^X$ ονομάζεται **δράση** της ομάδας G επί του συνόλου X. Η απεικόνιση $F: GxX\to X$ (αντ. $F: XxG\to X$) που ορίζεται με $F(g, x) = h(g)(x)$ (αντ. $F(x, g) = h(g)(x)$) λέγεται αριστερός (αντ. δεξιός) νόμος της δράσης. Το στοιχείο $h(g)(x)$ λέγεται μετασχηματισμός του $x\in X$ ως προς την δράση και γράφουμε συμβολικά $h(g)(x) = gx$ (αντ. $h(g)(x) = xg$) όταν ο νόμος F είναι αριστερός (αντ. δεξιός).

Όταν h και σ είναι δράσεις της G επί των συνόλων X και Y, τότε μία απεικόνιση $\varphi: X\to Y$ λέγεται συμβιβαστή με τις δράσεις της G, όταν είναι

$$\varphi\circ h(g) = \sigma(g)\circ\varphi.$$

Μία δράση $h: G\to X^X$ λέγεται αριστερή (αντ. δεξιά) **ενέργεια** ή **εξωτερική** πράξη της G επί του X, όταν είναι

$$h(e)=1 \text{ και } h(g_1g_2) = h(g_1)\circ h(g_2) \quad (\text{αντ. } h(e)=1,\ h(g_1g_2) = h(g_2)\circ h(g_1))$$

Για να αποφύγουμε τον αντιομομορφισμό $h(g_1g_2) = h(g_2)\circ h(g_1)$ θα θεωρούμε αριστερή ενέργεια και έτσι προκύπτει ότι η ενέργεια h είναι ένας ομομορφισμός $h: G\to S(X)$, διότι είναι $h(e) = h(gg^{-1}) = h(g)\circ h(g^{-1}) = 1$ και άρα έχουμε $h(g^{-1}) = h(g)^{-1}$, δηλ. υπάρχει η αντίστροφη απεικόνιση $h(g)^{-1}$ της $h(g)$ για κάθε $g\in G$ και άρα η $h(g)$ είναι μία μετάθεση του X. Όταν υπάρχει μία ενέργεια της G επί ενός συνόλου X, τότε το X λέγεται G-**σύνολο.**

Παρατήρηση: Ακριβώς όπως παραπάνω, μπορούμε να ορίσουμε δράση ενός τυχαίου συνόλου A επί ενός συνόλου X. Επίσης μπορούμε να ορίσουμε ενέργεια μιας τυχαίας αλγεβρικής δομής επί ενός συνόλου X.

Ας είναι X και Y δύο G-σύνολα με ενέργειες h και σ αντιστοίχως. Μία απεικόνιση $f: X\to Y$ λέγεται **ομομορφισμός** των G-συνόλων, όταν είναι $f\circ h(g) = \sigma(g)\circ f$. Τότε λέμε ότι η f είναι συμβιβαστή με τις ενέργειες της G.

Θεωρούμε ένα ομομορφισμό $f: G \to H$ των ομάδων G και H, ένα G-σύνολο X με ενέργεια h και ένα H-σύνολο Y με ενέργεια σ. Μία απεικόνιση $\varphi: X \to Y$ που ικανοποιεί τη σχέση $\varphi \circ h(g) = \sigma(f(g)) \circ \varphi$ λέγεται f-**ομομορφισμός** του X στο Y.

Ας είναι G μία ομάδα, X ένα G-σύνολο με ενέργεια h και x τυχαίο στοιχείο του X. Ένα στοιχείο $y \in X$ λέγεται **συζυγές** του x ως προς την h, όταν υπάρχει ένα στοιχείο $g \in G$ ώστε να είναι $h(g)(x) = y$, συμβολικά $gx=y$. Τότε το σύνολο C_x όλων των συζυγών στοιχείων του x

$$C_x = \{y \in X \mid h(g)(x) = y,\ g \in G\}$$

λέγεται **τροχιά** του x στο X. Η ενέργεια h ονομάζεται **μεταβατική,** όταν υπάρχει ένα στοιχείο $x \in X$ με τροχιά $C_x = X$. Το G-σύνολο X λέγεται **ομογενές,** όταν η ενέργεια h της G επί του X είναι μεταβατική.

Παρατηρήσεις

1. Αφού h είναι ενέργεια, η h(g) είναι μία μετάθεση του X και άρα είναι $h(g)(x) = y$ ανν $h(g)^{-1}(y) = x = h(g^{-1})(y)$.

2. Η απεικόνιση $F: G \to X$ που ορίζεται με $F(g) = h(g)(x)$ ονομάζεται **τροχιακή.**

3. Μπορούμε να ορίσουμε ενέργεια μιας ομάδας G επί την ίδια την G με την απεικόνιση

$$\sigma: G \to S(G), \quad \sigma(g)(x) = gx$$

για κάθε $g, x \in G$, διότι είναι $\sigma(e)x = ex = x = 1(x)$ και

$$\sigma(g_1 g_2)(x) = (g_1 g_2)x = g_1(g_2 x) = (\sigma(g_1) \circ \sigma(g_2))(x).$$

4. Το $x \in C_x$, διότι είναι $h(e)(x) = x$.

5. Η σχέση «y είναι συζυγές του x», συμβολικά $x \equiv y$, είναι μία σχέση ισοδυναμίας επί του X. Έτσι η σχέση ≡ διαμερίζει το X σε κλάσεις ισο δυναμίας και κάθε κλάση ισοδυναμίας είναι μία τροχιά.

6. Όταν η ενέργεια h είναι μεταβατική, τότε υπάρχει ένα $g \in G$ για κάθε x, $y \in X$ ώστε να είναι $h(g)(x) = y$.

7. Ένα στοιχείο $x \in X$ λέγεται **σταθερό** ή **αναλλοίωτο** ως προς την ενέργεια h της G επί του X, όταν είναι $h(g)(x) = x$ για κάθε $g \in G$.

Ένα υποσύνολο Y του X λέγεται **ολικά** (αντ. **σημειακά**) αναλλοίωτο ή σταθερό ως προς τη ενέργεια h, όταν είναι $h(g)(y) \in Y$ (αντ. $h(g)(y) = y$) για κάθε $g \in G$ και κάθε $y \in Y$.

Για $x\in X$, το σύνολο $G_x = \{g\in G \mid h(g)(x) = x\}$ είναι μια υποομάδα της G και λέγεται **ισότροπη** υποομάδα της G στο X.

8. Όταν μια ομάδα G ενεργεί επί ενός συνόλου X με συνάρτηση ενέργειας h και πάρουμε ένα υποσύνολο Y του X, τότε το βασικό πρόβλημα είναι ο προσδιορισμός μιας υποομάδας H της G ως προς την οποία το Y να είναι αναλλοίωτο, δηλ. να είναι

$$H = \{g\in G \mid h(g)(y)\in Y \text{ για κάθε } y\in Y\}$$

Μια τέτοια ομάδα λέγεται ομάδα συμμετρίας του Y.

Για κάθε σύνολο X, υπάρχει μια ομάδα συμμετρίας G του X, διότι η ταυτοτική απεικόνιση $1:X\to X$ είναι μία μετάθεση του X. Αν η G περιέχει μόνο το ουδέτερο στοιχείο, τότε λέγεται εκφυλισμένη.

9. Κάθε υποομάδα της συμμετρικής ομάδας $S(X)$ λέγεται ομάδα **μετασχηματισμών** επί του X. Κάθε ομάδα G θεωρείται μία ομάδα μετασχηματισμών της G, επειδή η G είναι ισόμορφη με μία υποομάδα της $S(G)$ ως προς την απεικόνιση

$$f: G \to S(G)\ ,\quad f(g)(x) = gx$$

η οποία είναι ενριπτική.

Κάθε ενριπτική ενέργεια λέγεται πιστή.

10. Ας πάρουμε την ισότροπο ομάδα $G_x = \{g\in G \mid h(g)(x) = x\}$ και ας είναι $h(\alpha)(x) = y$ για $\alpha\in G$ και $x, y\in X$. Τότε η θήκη

$$\alpha G_x = \{\alpha g \mid g\in G,\ h(\alpha g)(x) = (h(\alpha)\circ h(g))(x) = h(\alpha)(x) = y\}$$

αποτελείται από εκείνα τα στοιχεία της ομάδας G, τα οποία απεικονίζουν το x σε ένα σταθερό στοιχείο y με την ενέργεια h.

Κάθε στοιχείο αg της θήκης γράφεται $\alpha g = (\alpha g\alpha^{-1})\alpha$. Άρα είναι

$$h(g)(x) = x \text{ ανν } h(\alpha g\alpha^{-1})(h(\alpha)(x)) = h(\alpha)(x)$$

δηλ. η $h(g)$ διατηρεί το x σταθερό ανν η $h(\alpha g\alpha^{-1}) = h(\alpha)\circ h(g)\circ h(\alpha)^{-1}$ διατηρεί το $h(\alpha)(x) = y$ σταθερό. Άρα είναι $\alpha G_x\alpha^{-1} = \{\alpha g\alpha^{-1} / g\in G_x\} = G_y$, δηλ. οι ισότροπες ομάδες G_x και G_y είναι συζυγείς και άρα ισομορφικές.

Επίσης είναι $h(g)(z) = u$ ανν $h(\alpha g\alpha^{-1})(h(\alpha)(z) = h(\alpha)(u))$.

11. Ας πάρουμε την τροχιά του x

$$C_x = \{y\in X \mid h(\beta)(x) = y\} = \{y\in X \mid y\equiv x\}$$

Τότε είναι $h^{-1}(\beta)(y) = h(\beta^{-1})(y) = x$ και άρα $C_x = C_y$. Επίσης είναι $\beta G_x\beta^{-1} = G_y$ και άρα στοιχεία της ίδιας τροχιάς έχουν συζυγείς ισότροπες ομάδες.

12. Θεωρούμε την απεικόνιση $F : C_x \to G/G_x$ που ορίζεται με τη σχέση

$$F(y) = \beta G_x \quad \text{ανν} \quad h(\beta)(x) = y$$

Εύκολα βλέπουμε ότι η F είναι αμφιμονότιμη απεικόνιση της τροχιάς C_x επίτο πηλικοσύνολο G/G_x των αριστερών θηκών της G_x στη G.

Άρα το πλήθος $\pi(C_x)$ των στοιχείων της C_x είναι ίσο με $\pi(G)/\pi(G_x)$.

13. Ας πάρουμε τον εσωτερικό αυτομορφισμό

$$\varphi(\alpha) : G \to G \quad \varphi(\alpha)(g) = \alpha g \alpha^{-1}$$

Τότε είναι $\varphi(\alpha) : G_x \to \alpha G_x \alpha^{-1} = G_y$ και άρα έχουμε

$$h(\varphi(\alpha)(g)) \circ h(\alpha) = h(\alpha) \circ h(g)$$

Θεωρούμε ένα δακτύλιο K. Ένα σύνολο V λέγεται **αριστερό μόντουλι** επί του K ή αριστερό K-μόντουλι, όταν ικανοποιούνται οι ακόλουθες ιδιότητες.

1. Το V είναι αντιμεταθετική ομάδα και η πράξη συμβολίζεται συνήθως προσθετικά.

2. Ορίζεται μία αριστερή ενέργεια $K \times V \to V$ με τη σχέση $(\lambda, x) \to \lambda x$ που ικανοποιεί τα αξιώματα

α. $\lambda(x+y) = \lambda x + \lambda y$, **β.** $(\lambda+\mu)x = \lambda x + \mu x$

και επιπλέον τις ιδιότητες της ενέργειας που είναι

γ. $1x = x$, **δ.** $(\lambda\mu)x = \lambda(\mu x)$

για κάθε $x, y \in V$ και κάθε $\lambda, \mu \in K$.

Αντίστοιχα μπορούμε να ορίσουμε ένα δεξιό K-μόντουλι με μία ενέργεια $V \times K \to V$.

Λέμε ότι το V είναι K-μόντουλι, όταν ο δακτύλιος K είναι αντιμεταθετικός.

Ένα K-μόντουλι V ονομάζεται **αριστερός** (αντ. **δεξιός**) **διανυσματικός χώρος,** όταν ο δακτύλιος K είναι σώμα. Αν ο K είναι αντιμεταθετικό σώμα, τότε το V λέγεται **διανυσματικός χώρος.**

Άρα το V είναι διαν. χώρος επί ενός σώματος K όταν ισχύουν οι παρακάτω ιδιότητες.

1. $(x+y)+z = x+(y+z)$

2. $(\forall\, x \in V),\ (\exists \mid 0 \in V) : x+0 = 0+x = x$

3. $(\forall\, x \in V),\ (\exists \mid -x \in V) : x+(-x) = (-x+x) = 0.$ Είναι $-x = (-1)x$.

4. $x+y = y+x$

5. $\lambda(x+y) = \lambda x + \lambda y$;

6. $(\lambda+\mu)x = \lambda x+\mu x$

7. $(\lambda\mu)x = \lambda(\mu x)$;

8. $1x = x$

για κάθε $x, y, z \in V$ και κάθε $\lambda, \mu \in K$.

Παρατηρήσεις

1. Κάθε αντιμεταθετική ομάδα G, της οποίας η πράξη συμβολίζεται προσθετικά, είναι μόντουλι επί του δακτυλίου Z των ακεραίων, διότι ορίζεται η εξωτερική πράξη

$$ZxG \to G,\ (\nu, x) \to \nu x$$

η οποία ικανοποιεί τα παραπάνω αξιώματα.

2. Εκτός από μερικά παραδείγματα και μερικές εφαρμογές όλη η παραπέρα ανάπτυξη της θεωρίας αναφέρεται σε διανυσματικούς χώρους, όπου τα βασικά σώματα είναι το σώμα R των πραγματικών και το σώμα C των μιγαδικών αριθμών, τα οποία είναι αντιμεταθετικά.

3. Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι διαν. χώροι επί σωμάτων με πεπερασμένο πλήθος στοιχείων, δηλ. σωμάτων με χαρακτηριστική ένα πρώτο άριθμό $p>1$. Τότε απαιτείται ιδιαίτερη, προσοχή, διότι είναι $px=0$ για κάθε διάνυσμα $x\neq 0$.

Από τον ορισμό του διαν. χώρου V προκύπτουν οι ακόλουθες ιδιότητες.

α. Για κάθε $x, y \in V$ υπάρχει μοναδικό $z \in V$ ώστε να είναι $x+z=y$, διότι έχουμε $(-x)+x+z = (-x)+y \Rightarrow z = y+(-x)$. Γράφουμε $y+(-x) = y-x$.

Άρα είναι $x+z = x$ ανν $z=0$.

β. Είναι $\lambda x=0$ ανν $\lambda=0$ ή $x=0$, όπου $\lambda \in K$.
Έχουμε $0x+\lambda x = (0+\lambda)x = \lambda x$ και άρα $0x=0$. Ομοίως είναι $\lambda 0=0$.
Χρησιμοποιούμε το ίδιο σύμβολο 0 για τα μηδενικά διανύσματα όλων των διαν. χώρων και τον μηδενικό αριθμό του σώματος K.
Αν $\lambda\neq 0$, τότε είναι

$$\lambda x = 0 \Rightarrow 0 = \lambda^{-1}(\lambda x) = (\lambda^{-1}\lambda)x = 1x = x.$$

γ. Είναι $(-\lambda)x = \lambda(-x) = -\lambda x$.

Παραδείγματα

1. Το σύνολο $K^v = Kx \ldots xK$ των διατεταγμένων ν-άδων $x = (x_1, \ldots, x_v)$ με στοιχεία x_i από το σώμα K αποτελεί διαν. χώρο με πράξη

$$x+y = (x_1, \ldots, x_\nu) + (y_1, \ldots, y_\nu) = (x_1+y_1, \ldots, x_\nu+y_\nu)$$

και ενέργεια

$$\lambda x = \lambda(x_1, \ldots, x_\nu) = (\lambda x_1, \ldots, \lambda x_\nu)$$

Το μηδενικό διάνυσμα είναι $0 = (0, \ldots, 0)$ και το αντίθετο του x το

$$-x = (-x, \ldots, -x_\nu).$$

2. Το σύνολο V των συναρτήσεων $\varphi : A \to K$ ενός τυχαίου συνόλου A με τιμές στο σώμα K και πράξεις $\varphi+g$ και $\lambda\varphi$, οι οποίες ορίζονται με τις σχέσεις $(\varphi+g)(\alpha) = \varphi(\alpha)+g(\alpha)$ και $(\lambda\varphi)(\alpha) = \lambda\varphi(\alpha)$, αποτελεί διαν. χώρο, επί του σώματος K με ουδέτερο στοιχείο τη μηδενική συνάρτηση $0(\alpha) = 0$ και αντίθετο του φ που ορίζεται με $(-\varphi)(\alpha) = -\varphi(\alpha)$.

Γενικά η πράξη της πρόσθεσης συναρτήσεων και η ενέργεια επί συναρτήσεων θα ορίζονται όπως παραπάνω.

3. Το σύνολο V των πολυωνύμων $\varphi(t) = \alpha_0+\alpha_1 t + \ldots + \alpha_\nu t^\nu$ βαθμού $\leq \nu$ με συντελεστές α_i από ένα σώμα K είναι διαν. χώρος επί του K με τις συνήθες πράξεις των πολυωνύμων.

4. Το σύνολο $\{0\}$ αποτελούμενο μόνο από το μηδενικό διάνυσμα αποτελεί διαν. χώρο.

5. Αν A είναι δακτύλιος, τότε ορίζεται μία δομή A-μόντουλι επί του συνόλου $A^\nu = Ax \ldots xA$ των διατεταγμένων ν-άδων $\alpha = (\alpha_1, \ldots, \alpha_\nu)$ με πράξεις οριζόμενες όπως παρακάτω

$$\alpha+\beta = (\alpha_1, \ldots, \alpha_\nu)+(\beta_1,\ldots, \beta_\nu) = (\alpha_1+\beta_1,\ldots, \alpha_\nu+\beta_\nu)$$

$$\lambda\alpha = \lambda(\alpha_1, \ldots, \alpha_\nu) = (\lambda\alpha_1, \ldots, \lambda\alpha_\nu).$$

Αν το A είναι σώμα, τότε το A^ν είναι διαν. χώρος

6. Τώρα ας πούμε μερικά στοιχεία από τα συστήματα αριθμών. Ονομάζουμε **ν-αδικό σύστημα** αριθμών τον δακτύλιο ή το σώμα $Z_\nu = Z/\nu Z$. Τότε κάθε ακέραιος α γράφεται με τη μορφή $\alpha = \alpha_0\nu^0+\alpha_1\nu^1+\alpha_2\nu^2+ \ldots$, όπου οι συντελεστές $\alpha_i \in Z_\nu$ και έτσι ο α συμβολίζεται με μία από τις παρακάτω μορφές

$$\alpha = (\alpha_0, \alpha_1, \alpha_2, \ldots), \quad \alpha = \ldots \alpha_2\alpha_1\alpha_0.$$

Αν το ανάπτυγμα του α τελειώνει στον k όρο, δηλ. είναι

$$\alpha = \alpha_0\nu^0+\alpha_1\nu^1+\ldots + \alpha_k\nu^k,$$

τότε μπορούμε να τοποθετήσουμε όσα θέλουμε μηδενικά στο τέλος της πρώτης ή στην αρχή της δεύτερης συμβολικής γραφής, διότι μπορούμε να γράψουμε

$$\alpha = \alpha_0\nu^0+ \ldots + \alpha_k\nu^k+0\nu^{k+1}+0\nu^{k+2} +\ldots$$

και έτσι έχουμε αντίστοιχα

$$\alpha = (\alpha_0, \ldots, \alpha_k, 0, 0, \ldots) \,, \quad \alpha = 0\,0 \ldots\, 0\alpha_k \ldots\, \alpha_0$$

Έτσι κάθε ακέραιος α εκφράζεται ως ένα στοιχείο ενός Z-μόντουλι

$$Z_\nu^\mu = Z_\nu \times \ldots \times Z_\nu$$

μ-φορές και μπορούμε να ορίσουμε τις πράξεις της πρόσθεσης και της ενέργειας επί του Z_ν^μ, οι οποίες είναι

$$(\overline{\alpha}, \ldots, \overline{\alpha}_\mu) \dot{+} (\overline{\beta}_1, \ldots, \overline{\beta}_\mu) = (\overline{\alpha}_1 \dot{+} \overline{\beta}_1, \ldots, \overline{\alpha}_\mu \dot{+} \overline{\beta}_\mu)$$

$$\lambda(\overline{\alpha}_1, \ldots, \overline{\alpha}_\mu) = (\lambda\overline{\alpha}_1, \ldots, \lambda\overline{\alpha}_\mu)$$

για $\lambda \in Z$. Εδώ παραλείπουμε τις παύλες και τις τελείες.

Ας ασχοληθούμε ιδιαίτερα με το δυικό σύστημα αριθμών $Z_2 = Z/2Z$. Οι πράξεις σε κάθε άλλο σύστημα αριθμών είναι ανάλογες.

Ορισμένοι υπολογισμοί επί των αριθμητικών συστημάτων

Ο αριθμός 30.000 στο δεκαδικό συστήμα όπου οι συντελεστές είναι

$$0, 1, 2, \ldots, 9$$

γράφεται

$$30.000 = \alpha_0 10^0 + \alpha_1 10^1 + \alpha_2 10^2 + \alpha_3 10^3 + \alpha_4 10^4 + \alpha_5 10^5 + \ldots = \alpha 10^4 = 3 \cdot 10^4$$

και είναι

$$30.000 = 0 \cdot 10^0 + 0 \cdot 10 + 0 \cdot 10^2 + 0 \cdot 10^3 + 3 \cdot 10^4 + 0 \cdot 10^5 + \ldots = 00\,30000$$

Ο αριθμός 30.000 στο 16αδικό σύστημα γράφεται

$$30.000 = \alpha_0 16^0 + \alpha_1 16^1 + \alpha_2 16^2 + \alpha_3 16^3 + \alpha_4 16^4 + \ldots =$$
$$= 0 \cdot 16^0 + 3 \cdot 16^1 + 5 \cdot 16^2 + 7 \cdot 16^3 + 0 \cdot 16^4 + 0 \cdot 16^5 + \ldots = 0 \ldots 007530$$

Οι συντελεστές α_i μπορούν να πάρουν ακέραιες τιμές από 0 μέχρι 15. Το τελικό αποτέλεσμα αποτελείται από τη διαδοχή των συντελεστών με την αντίστροφη σειρά, δηλ. είναι 7530. Η κατασκευή δείχνει ότι μπροστά από τον αριθμό 7530 μπορούμε να θέσουμε όσα μηδενικά θέλουμε.

Στο δυικό, όπου οι συντελεστές μπορούν να είναι 0 και 1, έχουμε

$$\begin{aligned} 30.000 &= \alpha_0 2^0 + \alpha_1 2^1 + \alpha_2 2^2 + \alpha_3 2^3 + \alpha_4 2^4 + \alpha_5 2^5 + \alpha_6 2^6 + \alpha_7 2^7 + \alpha_8 2^8 + \alpha_9 2^9 + \alpha_{10} 2^{10} + \\ &\quad + \alpha_{11} 2^{11} + \alpha_{12} 2^{12} + \alpha_{13} 2^{13} + \alpha_{14} 2^{14} + \alpha_{15} 2^{15} + \ldots = \\ &= 0 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4 + 1 \cdot 2^5 + 0 \cdot 2^6 + 0 \cdot 2^7 + 1 \cdot 2^8 + 0 \cdot 2^9 + 1 \cdot 2^{10} + \\ &\quad + 0 \cdot 2^{11} + 1 \cdot 2^{12} + 1 \cdot 2^{13} + 1 \cdot 2^{14} + 0 \cdot 2^{15} + \ldots = 0 \ldots 0111010100110000 \end{aligned}$$

Πράγματι είναι

$2^4+2^5+2^8+2^{10}+2^{12}+2^{13}+2^{14} = 16+32+256+1.024+4.096+8.192+16.384 =$
$= 30.000$

Έτσι έχουμε $\alpha = \alpha_0 2^0+\alpha_1 2^1+\alpha_2 2^2+ \dots + \alpha_k 2^k + \dots$ όπου $\alpha_i \in Z_2$, και είναι

$$\alpha = (\alpha_0, \alpha_1, \dots, \alpha_k, \dots) \quad \text{ή} \quad \alpha = \dots \alpha_k \dots \alpha_2\alpha_1\alpha_0.$$

Π.χ. είναι $0 = 0\cdot 2^0+0\cdot 2^1+0\cdot 2^2+0\cdot 2^3$ και άρα $0 = (0) = (0, 0, 0, 0) = 0000 = 0$. Αντίστοιχα έχουμε

$2^0=1 = 1\cdot 2^0+0\cdot 2+0\cdot 2^2+0\cdot 2^3$ και $2^0=1 = (1, 0, 0, 0) = 0001 = 1$
$2 = 2^1 = 0\cdot 2^0+1\cdot 2^1+0\cdot 2^2+0\cdot 2^3$ και $2 = (0, 1, 0, 0) = 0010 = 10$
$2^2 = 4 = 0\cdot 2+0\cdot 2^1+1\cdot 2^2+0\cdot 2^3$ και $2^2= (0, 0, 1, 0) = 0100$
$2^3= 8 = 0\cdot 2^0+0\cdot 2^1+0\cdot 2^2+1\cdot 2^3$ και $2^3 = (0, 0, 0, 1) = 1000$
$10 = 0\cdot 2^0+1\cdot 2^1+0\cdot 2^2+1\cdot 2^3$ και $10 = (0, 1, 0, 1) = 1010$
$11 = 1\cdot 2^0+1\cdot 2^1+0\cdot 2^2+1\cdot 2^3$ και $11 = (1, 1, 0, 1) = 1011$

Έτσι ένας ακέραιος α εκφράζεται ως ένα στοιχείο του Z-μόντουλι

$$Z_2^4 = Z_2\times Z_2\times Z_2\times Z_2.$$

Ας δούμε την πρόσθεση. Θεωρούμε δύο μη-αρνητικούς ακεραίους α και β και έχουμε

$\alpha = \alpha_0 2^0+\alpha_1 2^1+ \dots + \alpha_k 2^k+ \dots$, $\beta = \beta_0 2^0+\beta_1 2^1+ \dots + \beta_k 2^k+ \dots$ όπου $\alpha_k, \beta_k \in Z_2$.

Τότε το άθροισμα είναι

$$\alpha+\beta = (\alpha_0+\beta_0)2^0+(\alpha_1+\beta_1)2^1+ \dots + (\alpha_k+\beta_k)2^k+ \dots$$

Αν $\alpha_k+\beta_k<2$, τότε ο όρος $\alpha_k+\beta_k$ παραμένει συντελεστής του 2^k στο ανάπτυγμα $\alpha+\beta$.

Όμως όταν είναι $\alpha_k+\beta_k= 2$, τότε έχουμε

$$(\alpha_k+\beta_k)2^k = 1\cdot 2^{k+1}$$

και έτσι μηδενίζεται ο συντελεστής του 2^k και ο συντελεστής του 2^{k+1} γίνεται $1+\alpha_{k+1}+\beta_{k+1}$.

Ας προσθέσουμε τους ακεραίους 3 και 9 στο Z_2^4. Είναι

$3 = 1\cdot 2^0+1\cdot 2^1+0\cdot 2^2+0\cdot 2^3 = (1, 1, 0, 0) = 0011$
$9 = 1\cdot 2^0+0\cdot 2^1+0\cdot 2^2+1\cdot 2^3 = (1, 0, 0, 1) = (1, 0, 0, 1) = 1001$

Έτσι έχουμε

$3+9 = 2\cdot2^0+1\cdot2^1+0\cdot2^2+1\cdot2^3 = 0\cdot2^2+2\cdot2^1+0\cdot2^2+1\cdot2^3 = 0\cdot2^0+0\cdot2^1+1\cdot2^2+1\cdot2^3 =$

$= (0, 0, 1, 1) = 1100 = 12.$

Γράφουμε την πράξη με τη μορφή

$$\begin{array}{rcccc} & 0 & 0 & 1 & 1 \\ + & 1 & 0 & 0 & 1 \\ \hline & 1 & 1 & 0 & 0 \end{array}$$

Το γινόμενο Z_2^4 είναι διατεταγμένο με τη λεξικογραφική διάταξη, η οποία ορίζεται όπως παρακάτω

$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) < (\beta_1, \beta_2, \beta_3, \beta_4)$ ανν $\alpha_1<\beta_1$ ή $\alpha_1=\beta_1$,

$\alpha_2<\beta_2$, ή $\alpha_1=\beta_1$, $\alpha_2=\beta_2$, $\alpha_3<\beta_3$ ή $\alpha_1=\beta_1$, $\alpha_2=\beta_2$, $\alpha_3=\beta_3$, $\alpha_4<\beta_4$.

Η διάταξη ονομάζεται λεξικογραφική, διότι είναι ακριβώς εκείνη που εφαρμόζεται στην τοποθέτηση των λέξεων στα λεξικά και αυτή μας επιτρέπει να γνωρίζουμε το σύνολο των ακεραίων με τους οποίους μπορούμε να προσθέτουμε στο Z_2^4, διότι το ελάχιστο στοιχείο είναι ο ακέραιος $(0, 0, 0, 0) = 0$ και το μέγιστο το $(1, 1, 1, 1) = 15$. Άρα ένα γινόμενο της μορφής Z_2^4 παριστάνει ένα σύνολο ακεραίων, το οποίο είναι φραγμένο.

Φυσικά μπορούμε να αυξήσουμε το πλήθος των ακεραίων π.χ. παίρνοντας το Z_2^5 και τότε έχουμε ακεραίους από το $(0, 0, 0, 0, 0) = 0$ μέχρι

$$(1, 1, 1, 1, 1) = 1\cdot2^0+1\cdot2^1+1\cdot2^2+1\cdot2^3+1\cdot2^4 = 31.$$

Ας δούμε τη μορφή των αρνητικών ακεραίων. Θεωρούμε το τυχαίο καρτεσιανό γινόμενο του $Z_\nu = Z/\nu Z$ και το ακόλουθο σύνολο.

$$Z'_\nu = \begin{cases} \{-\frac{\nu}{2}\ ,\ -\frac{\nu}{2}+1\ , \dots , -1, 0, 1, \dots, \frac{\nu}{2}-1\} & \text{για } \nu \text{ άρτιο} \\ \{-\frac{\nu-1}{2}\ ,\ -\frac{\nu-1}{2}+1\ , \dots , -1, 0, 1, \dots, \frac{\nu-1}{2}\} & \text{για } \nu \text{ περιττό} \end{cases}$$

Το σύνολο Z'_ν συμπίπτει με το Z_ν, διότι είναι $-\mu = \nu-\mu$ για $0 \le \mu < \nu$ και άρα $\mu+\nu-\mu = \nu = 0$.

Π.χ. για το σώμα $Z_5 = \{0, 1, 2, 3, 4\}$ είναι $Z'_5 = \{-2, -1, 0, 1, 2\}$, διότι έχουμε $-2 = 5-2 = 3$ και $-1 = 5-1 = 4$. Για το $Z_2 = \{0, 1\}$ είναι $Z'_2 = \{-1, 0\}$, όπου $-1 = 1 = 2-1$.

Ας πάρουμε το καρτεσιανό γινόμενο $Z_2\times Z_2\times Z_2\times Z_2\times Z'_2$.

Τότε έχουμε το σύνολο των ακεραίων από τον ακέραιο

$$(0, 0, 0, 0, -1) = (-1)\,2^4 = -16$$

μέχρι τον $(1, 1, 1, 1, 0) = 15$ και έτσι μπορούμε να εκφράσουμε αρνητικούς ακεραίους ως γραμμικούς συνδυασμούς των $2^0, 2^1, 2^2, 2^3, 2^4$. Π.χ. είναι

$$-14 = 0\cdot 2^0+1\cdot 2^1+0\cdot 2^2+0\cdot 2^3+(-1)2^4 = (0, 1, 0, 0, 1) = 10010$$

σύμφωνα με τα παραπάνω και έχουμε

$$14 = 0\cdot 2^0+1\cdot 2^1+1\cdot 2^2+1\cdot 2^3+0\cdot 2^4 = (0, 1, 1, 1, 0) = 01110.$$

Έτσι προκύπτει $-14+14 = (0, 0, 0, 0, 0) = 0$.

Ας δούμε τα γινόμενα $4\cdot 3 = 12$ και $(-4)\cdot 3 = -12$ στο Z-μόντουλι Z_2^5. Είναι

$3 = 1\cdot 2+1\cdot 2^1+0\cdot 2^2+0\cdot 2^3+0\cdot 2^4$,

$4 = 0\cdot 2^0+0\cdot 2^1+1\cdot 2^2+0\cdot 2^3+0\cdot 2^4$ και $-4 = 0\cdot 2^0+0\cdot 2^1+1\cdot 2^2+1\cdot 2^3-1\cdot 2^4$.

Έτσι έχουμε

$$4\cdot 3 = 4\cdot 2^0+4\cdot 2^1+0\cdot 2^2+0\cdot 2^3+0\cdot 2^4 = 4+8 = (0, 0, 1, 0, 0) + (0, 0, 0, 1, 0) =$$
$$= (0, 0, 1, 1, 0) = 0\cdot 2^0+0\cdot 2^1+1\cdot 2^2+1\cdot 2^3+0\cdot 2^4 = 12 \quad \text{και}$$
$$(-4)\cdot 3 = -4\cdot 2^0+(-4)\cdot 2^1+0\cdot 2^2+0\cdot 2^3+0\cdot 2^4 = (-4)+(-8) =$$
$$= (0, 0, 1, 1, 1)+(0, 0, 0, 1, 1) = 1\cdot 2^3-1\cdot 2^4 = -12.$$

2. Διανυσματικοί υπόχωροι

Θεωρούμε ένα διαν. χώρο V επί ενός σώματος K.

Ένα μη-κενό υποσύνολο W του V λέγεται διανυσματικός **υπόχωρος** του V, όταν είναι διαν. χώρος επί του K ως προς τις πράξεις του V.

ΠΡΟΤΑΣΗ 1. Το W είναι διαν. υπόχωρος του V ανν είναι $x+y\in W$ και $\lambda x\in W$ για κάθε $x, y\in W$ και κάθε $\lambda\in K$.

Απόδειξη. Προφανώς ισχύουν όλες οι ιδιότητες ενός διαν. χώρου και έχουμε $0 = 0x\in W$ και $-x = (-1)x\in W$ για κάθε $x\in W$.

Πόρισμα 1. Το W είναι διαν. υπόχωρος του V ανν έχουμε $\lambda x+\mu y\in W$ για κάθε $x, y\in W$ και κάθε $\lambda, \mu\in K$.

ΠΡΟΤΑΣΗ 2. Η τομή $V_1\cap V_2 = \{x\in V \mid x\in V_1 \text{ και } x\in V_2\}$ των διαν. υποχώρων V_1 και V_2 του V είναι διαν. υπόχωρος του V.

Απόδειξη. Αν $x, y\in V_1\cap V_2$, τότε είναι $x, y\in V_1$ και $x, y\in V_2$. Έτσι έχουμε $x+y\in V_1$ και $x+y\in V_2$ και άρα είναι $x+y\in V_1\cap V_2$.

Επίσης για $x\in V_1\cap V_2$ είναι $\lambda x\in V_1\cap V_2$.