Περιεχόμενα

Παράρτημα Α

ΑΛΓΕΒΡΙΚΕΣ ΔΟΜΕΣ

Α.1 Εισαγωγή - Ορισμοί

Σύνολα (sets). Θεωρούνται γνωστά.

Σύνολα που μας ενδιαφέρουν:

N	:	φυσικοί (natural) αριθμοί
$\mathbf{N_0}$	:	μη αρνητικοί ακέραιοι, $\mathbf{N_0}=\mathbf{N}\cup\{0\}$
Z	:	ακέραιοι (integer) αριθμοί
Q	:	ρητοί (rational) αριθμοί
R	:	πραγματικοί (real) αριθμοί
C	:	μιγαδικοί (complex) αριθμοί

Διατεταγμένο ζεύγος (ordered pair), διατεταγμένη τριάδα, νιάδα, κλπ. Θεωρούνται γνωστά.

Ορισμός Α.1.1
Έστω δύο σύνολα A και B. Το σύνολο των διατεταγμένων ζευγών της μορφής (a, b) με $a \in A$ και $b \in B$ καλείται **καρτεσιανό γινόμενο** (cartesian product) και συμβολίζεται με $A \times B$:

$$A \times B = \{(a,b),\ a \in A,\ b \in B\}$$

Παρατηρήσεις

1. Η έννοια του καρτεσιανού γινομένου γενικεύεται εύκολα για περισσότερα από δύο σύνολα. Έτσι έχουμε

$$A \times B \times C = \{(a,b,c),\ \ a \in A,\, b \in B,\, c \in C\}$$

και

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n),\ \ a_i \in A_i,\, i = 1, 2, \cdots, n\}\,.$$

2. Το καρτεσιανό γινόμενο $A \times A$ ενός συνόλου με τον εαυτό του συμβολίζεται με A^2:

$$A^2 = A \times A\,.$$

Ιδιαίτερου ενδιαφέροντος είναι τα σύνολα

$$\mathbf{R}^n = \underbrace{\mathbf{R} \times \mathbf{R} \times \cdots \times \mathbf{R}}_{n \text{ φορες}}$$

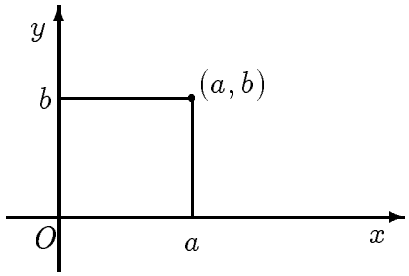
και

$$\mathbf{C}^n = \underbrace{\mathbf{C} \times \mathbf{C} \times \cdots \times \mathbf{C}}_{n \text{ φορες}}\,.$$

Υπενθυμίζουμε ότι το σύνολο

$$\mathbf{R}^2 = \{(a,b),\ a,b \in \mathbf{R}\}\,,$$

αντιστοιχεί γεωμετρικά στο **καρτεσιανό επίπεδο** (cartesian plane).



Παράδειγμα

Έστω τα σύνολα:

$$A = \{1,2,3\} \qquad \text{και} \qquad B = \{a,b\}\,.$$

Για τα καρτεσιανά γινόμενα $A \times B$ και $B \times A$ έχουμε:

$$A \times B = \{(1,a),\ (1,b),\ (2,a),\ (2,b),\ (3,a),\ (3,b)\}$$

και

$$B \times A = \{(a,1),\ (a,2),\ (a,3),\ (b,1),\ (b,2),\ (b,3)\}\,.$$

Παρατηρούμε ότι $A \times B \neq B \times A$.

Για το καρτεσιανό γινόμενο B^2 έχουμε:

$$B^2 = B \times B = \{(a,a),\ (a,b),\ (b,a),\ (b,b)\}\,.$$

Ορισμός Α.1.2

Έστω δύο σύνολα Α και Β. Ένα υποσύνολο $R \subseteq A \times B$ καλείται **διμελής σχέση** (binary relation) **από το Α στο Β**.
Αν $(a,b) \in R$ γράφουμε

$$a \; R \; \mathrm{b}$$

(*το a σχετίζεται με το b*). Ιδιαίτερα ένα υποσύνολο $R \subseteq A \times A$ καλείται **σχέση στο Α**.

Ορισμός Α.1.3

Μια σχέση $\sim$ στο σύνολο Α καλείται **σχέση ισοδυναμίας** (equivalence relation) αν:
(i) $a \sim a \quad \forall a \in A$ [αυτοπαθής ή ανακλαστική (reflective) ιδιότητα].
(ii) $a \sim \mathrm{b}$ αν και μόνο αν $\mathrm{b} \sim a, \quad a, \mathrm{b} \in A$ [συμμετρική (symmetric) ιδιότητα].
(iii) Αν $a \sim \mathrm{b}$ και $\mathrm{b} \sim \mathrm{c}$, τότε $a \sim \mathrm{c}, \quad a, \mathrm{b}, \mathrm{c} \in A$ [μεταβατική (transitive) ιδιότητα].

Παραδείγματα

1. Η ισότητα $'='$ στο σύνολο Α είναι μια σχέση ισοδυναμίας. Το υποσύνολο R του $A \times A$ που ορίζει αυτή τη σχέση είναι το

$$R \; = \; \{(a,a), \;\; a \in A\}$$

2. Η **ομοιότητα** (similarity) πινάκων είναι σχέση ισοδυναμίας. Έστω οι πίνακες $A, B \in M_{n\times n}$, όπου $M_{n\times n}$ το σύνολο των $n \times n$ πινάκων. Ο A είναι **όμοιος** (similar) με τον B αν υπάρχει αντιστρέψιμος πίνακας S τέτοιος ώστε

$$A \; = \; S^{-1} B S$$

(βλ. Ορισμό 9.4.1). Θα δείξουμε ότι η ομοιότητα πινάκων ικανοποιεί τις τρεις συνθήκες του Ορισμού Α.1.3.

(i) Γνωρίζουμε ότι ο μοναδιαίος πίνακας I είναι αντιστρέψιμος και μάλιστα $I^{-1} = I$. Αν οι A και I είναι $n \times n$ πίνακες, τότε

$$A \; = \; IAI \; = \; I^{-1} A I \, ,$$

οπότε η συνθήκη ικανοποιείται (o A είναι όμοιος με τον εαυτό του).

(ii) Αν ο A είναι όμοιος με τον B, τότε υπάρχει αντιστρέψιμος πίνακας S τέτοιος ώστε

$$A \; = \; S^{-1} B S \, .$$

Από την πιο πάνω σχέση παίρνουμε

$$S \, A \, S^{-1} \; = \; S \, (S^{-1} \, B \, S) \, S^{-1} \; = \; (S \, S^{-1}) \, B \, (S \, S^{-1}) \; = \; I \, B \, I \; = \; B \, ,$$

οπότε

$$B \; = \; P^{-1} \, A \, P$$

όπου $P{=}S^{-1}$. Επειδή ο P είναι αντιστρέψιμος, ο B είναι όμοιος με τον A.

(iii) Αν ο A είναι όμοιος με τον B και ο B όμοιος με τον C τότε υπάρχουν αντιστρέψιμοι πίνακες S και P τέτοιοι ώστε

$$A \;=\; S^{-1}BS$$

και

$$B \;=\; P^{-1}CP\,.$$

Από τις πιο πάνω σχέσεις παίρνουμε,

$$A \;=\; S^{-1}(P^{-1}CP)S \;=\; (S^{-1}P^{-1})C(PS)$$

και με βάση τις ιδιότητες των αντιστρέψιμων πινάκων

$$A \;=\; (PS)^{-1}C(PS)\,.$$

Ο PS είναι αντιστρέψιμος, ως γινόμενο αντιστρέψιμων πινάκων. Άρα, ο A είναι όμοιος με τον C. Έχουμε δείξει λοιπόν ότι η ομοιότητα πινάκων είναι πράξη ισοδυναμίας.

Ορισμός Α.1.4
Μια **διμελής πράξη** (binary operation) ή απλώς **πράξη** στο μη κενό σύνολο A είναι μια απεικόνιση $*$ του συνόλου $A \times A$ στο σύνολο A:

$$* : A \times A \longrightarrow A \qquad \text{όπου} \qquad (a,b) \longmapsto a * b.$$

Παρατηρήσεις

1. Συχνά όταν δεν υπάρχει κίνδυνος σύγχυσης το σύμβολο $*$ παραλείπεται, δηλαδή γράφουμε ab αντί $a * b$.
2. Σύμβολα που χρησιμοποιούνται συνήθως είναι τα εξής:

$+$	:	για την πρόσθεση
-	:	για την αφαίρεση
$\cdot$, $*$, $\times$	:	για τον πολλαπλασιασμό
$\circ$	:	για τη σύνθεση (composition) απεικονίσεων και μεταθέσεων

Έστω B ένα μη κενό υποσύνολο του A. Θα λέμε ότι το B είναι **κλειστό ως προς την πράξη** $*$ (closed under $*$) αν

$$\forall a,b \in B \qquad \text{ισχύει} \qquad a * b \in B.$$

Παραδείγματα

1. Θεωρούμε το σύνολο των ακεραίων $\mathbf{Z}$ με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού:

   Πρόσθεση: $+ : \mathbf{Z} \times \mathbf{Z} \longrightarrow \mathbf{Z}$ με $(x, y) \mapsto x + y$
   Πολλαπλασιασμός: $\cdot : \mathbf{Z} \times \mathbf{Z} \longrightarrow \mathbf{Z}$ με $(x, y) \mapsto xy$

   Είναι φανερό ότι το $\mathbf{Z}$ είναι κλειστό ως προς τις δύο πράξεις.

   Έστω τώρα το υποσύνολο Π των περιττών αριθμών

   $$\Pi = \{\ldots, -3, -1, 1, 3, \ldots\} .$$

   Το Π δεν είναι κλειστό ως προς την πρόσθεση αφού το άθροισμα δύο περιττών είναι άρτιος. Είναι όμως κλειστό ως προς τον πολλαπλασιασμό αφού το γινόμενο δύο περιττών είναι περιττός.

   Έστω τώρα το υποσύνολο Α των άρτιων αριθμών:

   $$A = \{..., -4, -2, 0, 2, 4, ...\} .$$

   Είναι φανερό ότι το Α είναι κλειστό ως προς τις δύο συνήθεις πράξεις.

2. Στο σύνολο $M_{m\times n}$ των $m \times n$ πινάκων, ορίζουμε την πρόσθεση δύο πινάκων

   $$A = (a_{ij}) \quad \text{και} \quad B = (b_{ij}) \in M_{m\times n}$$

   ως εξής:

   $$A + B \ = \ (a_{ij} + b_{ij}) \ \in M_{m\times n} .$$

   Έτσι, εξ ορισμού, το $M_{m\times n}$ είναι κλειστό ως προς την πρόσθεση (ή, με διαφορετικά λόγια, η πρόσθεση είναι μια πράξη στο $M_{m\times n}$). Για παράδειγμα, αν

   $$A \ = \ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 0 & 4 \end{bmatrix} \quad \text{και} \quad B \ = \ \begin{bmatrix} 3 & -2 & -1 \\ 0 & 2 & 6 \end{bmatrix} \in M_{2\times 3}$$

   τότε

   $$A + B \ = \ \begin{bmatrix} 1+3 & 2-2 & 3-1 \\ 1+0 & 0+2 & 4+6 \end{bmatrix} \ = \ \begin{bmatrix} 4 & 0 & 2 \\ 1 & 2 & 10 \end{bmatrix} \in M_{2\times 3} .$$

   Έστω τώρα το υποσύνολο $S_{2\times 2}$ του $M_{2\times 2}$:

   $$S_{2\times 2} \ = \ \left\{ A \in M_{2\times 2} \ : \ A = \begin{bmatrix} a & b \\ b & c \end{bmatrix} \ , \ \ a, b, c \in \mathbf{R} \right\} .$$

   Παρατηρούμε ότι το $S_{2\times 2}$ είναι το σύνολο των συμμετρικών 2×2 πινάκων. Το $S_{2\times 2}$ είναι κλειστό ως προς την πρόσθεση. Με διαφορετικά λόγια, το άθροισμα δύο συμμετρικών πινάκων είναι επίσης συμμετρικός πίνακας. Πραγματικά, αν

   $$A = \begin{bmatrix} a & b \\ b & c \end{bmatrix} \quad \text{και} \quad B = \begin{bmatrix} d & e \\ e & f \end{bmatrix}$$

   τότε

   $$A + B = \begin{bmatrix} a+d & b+e \\ b+e & c+f \end{bmatrix} \in S_{2\times 2} .$$

3. Στο σύνολο $M_{n\times n}$ των $n \times n$ (τετραγωνικών) πινάκων μπορούμε επίσης να ορίσουμε την πράξη του πολλαπλασιασμού. Αν $A = (a_{ij})$, $B = (b_{ij}) \in M_{n\times n}$, τότε το γινόμενό τους είναι ο

$$AB = \left(\sum_{k=1}^{n} a_{ik} b_{kj} \right) \in M_{n\times n} .$$

4. Στο $\mathbf{R}^n$, η συνήθης πράξη της πρόσθεσης, $+ : \mathbf{R}^n \times \mathbf{R}^n \longrightarrow \mathbf{R}^n$, ορίζεται ως εξής: Αν

$$u = (u_1, u_2, \cdots, u_n) \qquad \text{και} \qquad v = (v_1, v_2, \cdots, v_n) ,$$

είναι δύο διανύσματα του $\mathbf{R}^n$, τότε

$$u + v \ = \ (u_1 + v_1, u_2 + v_2, \cdots, u_n + v_n) \ \in \mathbf{R}^n .$$

Παρομοίως, ορίζεται και η πρόσθεση στο $\mathbf{C}^n$.

5. Έστω $C(\mathbf{R})$ το σύνολο των συνεχών συναρτήσεων στο $\mathbf{R}$. Η συνήθης πράξη της πρόσθεσης, $+ : C(\mathbf{R}) \times C(\mathbf{R}) \longrightarrow C(\mathbf{R})$, ορίζεται ως εξής:

$$(f + g)(x) = f(x) + g(x) \qquad \forall f, g \in C(\mathbf{R}) .$$

Για παράδειγμα, αν

$$f(x) = x^2 + 1 \quad \text{και} \quad g(x) = x + \cos x ,$$

τότε

$$(f + g)(x) = f(x) + g(x) = x^2 + 1 \ + \ x + \cos x .$$

Στο $C(\mathbf{R})$ μπορούμε επίσης να ορίσουμε τη **σύνθεση συναρτήσεων** $\circ$. Αν $f, g \in C(\mathbf{R})$, τότε

$$\boxed{(f \circ g)(x) \ = \ f(g(x))}$$

(Αν οι f και g είναι συνεχείς στο $\mathbf{R}$, τότε και η σύνθεσή τους είναι συνεχής στο $\mathbf{R}$.) Αν πάρουμε τις συναρτήσεις f και g που χρησιμοποιήσαμε πιο πάνω, έχουμε:

$$(f \circ g)(x) = f(g(x)) = f(x + \cos x) = (x + \cos x)^2 + 1 .$$

6. Θεωρούμε το σύνολο των μεταθέσεων των $1, 2, \ldots, n$ που θα το συμβολίζουμε με S_n. Ως γνωστό, το S_n αποτελείται από $n!$ στοιχεία. Έτσι, το S_3 αποτελείται από $3!$=6 στοιχεία:

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Η **σύνθεση μεταθέσεων** είναι μια πράξη στο S_n, $\circ : S_n \times S_n \longrightarrow S_n$. Αν τ, $\sigma \in S_n$ με

$$\tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau_1 & \tau_2 & \cdots & \tau_n \end{pmatrix} \qquad \text{και} \qquad \sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma_1 & \sigma_2 & \cdots & \sigma_n \end{pmatrix}$$

τότε η σύνθεσή τους $\tau \circ \sigma$ ορίζεται ως εξής:

$$\boxed{\tau \circ \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau_{\sigma_1} & \tau_{\sigma_2} & \cdots & \tau_{\sigma n} \end{pmatrix}}$$

Ας δούμε ένα παράδειγμα στο S_3. Αν

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{και} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

τότε για τη σύνθεση $\tau \circ \sigma$ έχουμε:

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ \tau_{\sigma_1} & \tau_{\sigma_2} & \tau_{\sigma_3} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \tau_2 & \tau_1 & \tau_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Ορισμός Α.1.5
Η πράξη $*$ στο σύνολο Α καλείται **προσεταιριστική** (associative) αν

$$x * (y * z) = (x * y) * z \qquad \forall \ x, y, z \in A.$$

Λέμε επίσης ότι ισχύει η **προσεταιριστική ιδιότητα** (associative law).

Παραδείγματα

1. Οι πράξεις της πρόσθεσης και πολλαπλασιασμού στο σύνολο $\mathbf{Z}$ των ακεραίων είναι προσεταιριστικές.

$$x + (y + z) = (x + y) + z \qquad \forall x, y, z \in \mathbf{Z}$$

$$x(yz) = (xy)z \qquad \forall x, y, z \in \mathbf{Z}$$

2. Η πράξη της πρόσθεσης στο $\mathbf{C}^n$ είναι προσεταιριστική. Αν $u, v, w \in \mathbf{C}^n$, τότε

$$u + (v + w) = (u + v) + w \quad \forall u, v, w \in \mathbf{C}^n.$$

3. Η πρόσθεση στο $M_{m\times n}$ και ο πολλαπλασιασμός στο $M_{n\times n}$ είναι προσεταιριστικές πράξεις:
$$A+(B+C)=(A+B)+C \qquad \forall A,B,C\in M_{m\times n}$$
$$A(BC)=(AB)C \qquad \forall A,B,C\in M_{n\times n}$$

4. Η πράξη της σύνθεσης στο $C(\mathbf{R})$ είναι προσεταιριστική:
$$f\circ(g\circ h)=(f\circ g)\circ h \qquad \forall f,g,h\in C(\mathbf{R})\,.$$
Πράγματι, για τα δύο μέλη της πιο πάνω σχέσης παίρνουμε
$$[f\circ(g\circ h)](x)=f[(g\circ h)(x)]=f[g(h(x))]$$
και
$$[(f\circ g)\circ h](x)=(f\circ g)(h(x))=f[g(h(x))].$$

5. Η πράξη της σύνθεσης στο S_n είναι προσεταιριστική:
$$\tau\circ(\sigma\circ\upsilon)\;=\;(\tau\circ\sigma)\circ\upsilon \qquad \forall\tau,\sigma,\upsilon\in S_n\,.$$

6. Η πράξη της αφαίρεσης στο **Z δεν είναι** προσεταιριστική. Αν $x,y,z\in\mathbf{Z}$, τότε
$$x-(y-z)\neq(x-y)-z$$
αφού
$$x-y+z\neq x-y-z\,.$$

Παρατήρηση
Η προσεταιριστική ιδιότητα μας λέει ότι η θέση των παρενθέσεων δεν έχει σημασία. Έτσι στο $M_{n\times n}$,
$$(AB)(CD)=A(B(CD))=(A(BC))D.$$
Μπορούμε λοιπόν να γράψουμε απλά:
$$ABCD\,.$$

Ορισμός Α.1.6
Το ζεύγος $(S,*)$ όπου S ένα μη κενό σύνολο και $*$ μια πράξη στο S καλείται **ημιομάδα** (semigroup) αν η πράξη $*$ είναι προσεταιριστική.

Παραδείγματα ημιομάδων

1. Τα σύνολα $\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ με την πράξη της πρόσθεσης είναι ημιομάδες. Τα ίδια σύνολα με την πράξη του πολλαπλασιασμού είναι επίσης ημιομάδες.
2. Τα ζεύγη $(M_{m\times n}, +)$ και $(M_{n\times n}, \cdot)$ είναι ημιομάδες.
3. Τα ζεύγη $(C(\mathbf{R}), +)$ και $(C(\mathbf{R}), \circ)$ είναι ημιομάδες.
4. Το ζεύγος $(S_n, \circ)$ είναι ημιομάδα.
5. Τα ζεύγη $(\mathbf{R}^n, +)$ και $(\mathbf{C}^n, +)$ είναι ημιομάδες.

Παρατηρήσεις

1. Σύμφωνα με τον Ορισμό Α.1.6, το S είναι κλειστό ως προς την πράξη $*$ αφού η $*$ είναι μια πράξη στο S (βλ. Ορισμό Α.1.4). Έτσι, αν θέλουμε να ελέγξουμε κατά πόσο το ζεύγος $(S, *)$ είναι ημιομάδα, ελέγχουμε πρώτα αν το S είναι κλειστό ως προς την πράξη $*$ και μετά αν η πράξη είναι προσεταιριστική.
2. Αν το ζεύγος $(S, *)$ είναι ημιομάδα και το S' είναι ένα υποσύνολο του S, τότε επειδή η πράξη $*$ είναι προσεταιριστική, το $(S', *)$ είναι ημιομάδα αν το S' είναι κλειστό ως προς την πράξη $*$.

Παραδείγματα

1. Ως γνωστό, το $(\mathbf{Z}, +)$ είναι ημιομάδα. Έστω A το σύνολο των άρτιων αριθμών και B τό σύνολο των περιττών αριθμών:

$$A = \{\cdots, -4, -2, , 2, 4, \cdots\} \subset \mathbf{Z}\,,$$

$$B = \{\cdots, -3, -1, 1, 3, \cdots\} \subset \mathbf{Z}\,.$$

   Το $(A, +)$ είναι επίσης ημιομάδα αφού είναι κλειστό ως προς την πρόσθεση. Αυτό δεν ισχύει φυσικά για το υποσύνολο B.

2. Το $(\mathbf{Z}, \cdot)$, όπου $\cdot$ η συνήθης πράξη του πολλαπλασιασμού, είναι ημιομάδα. Τα $(A, \cdot)$ και $(B, \cdot)$ είναι επίσης ημιομάδες, αφού τόσο το A όσο και το B είναι κλειστά ως προς την εν λόγω πράξη.

Ορισμός Α.1.7

Η πράξη $*$ στο σύνολο Α καλείται **αντιμεταθετική** (commutative) αν

$$x * y = y * x \qquad \forall\, x, y \in A$$

Παραδείγματα

1. Η πρόσθεση και ο πολλαπλασιασμός στα σύνολα $\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}$ και $\mathbf{C}$ είναι αντιμεταθετικές πράξεις.

2. Η πρόσθεση στα σύνολα $\mathbf{R}^n$ και $\mathbf{C}^n$ είναι αντιμεταθετική.

3. Η πρόσθεση στο σύνολο $M_{m\times n}$ είναι αντιμεταθετική. Αντίθετα, ο πολλαπλασιασμός στο $M_{n\times n}$ *δεν είναι* αντιμεταθετικός. Αν $A, B \in M_{n\times n}$, τότε γενικά $AB \neq BA$. Θα δώσουμε ένα παράδειγμα στο $M_{2\times 2}$. Έστω οι πίνακες

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix} \qquad \text{και} \qquad B = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}.$$

Έχουμε για τα γινόμενα AB και BA:

$$AB = \begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2+2 & 1+2 \\ 6+0 & 3+0 \end{bmatrix} = \begin{bmatrix} 4 & 3 \\ 6 & 3 \end{bmatrix}$$

και

$$BA = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix} = \begin{bmatrix} 2+3 & 4+0 \\ 1+3 & 2+0 \end{bmatrix} = \begin{bmatrix} 5 & 4 \\ 4 & 2 \end{bmatrix}$$

Παρατηρούμε ότι $AB \neq BA$.

4. Η πρόσθεση συναρτήσεων στο $C(\mathbf{R})$ είναι αντιμεταθετική.

$$(f+g)(x) = (g+f)(x)\,, \qquad f, g, \in C(\mathbf{R}).$$

Αντίθετα, η σύνθεση *δεν είναι* αντιμεταθετική. Αν $f, g \in C(\mathbf{R})$, τότε γενικά $f \circ g \neq g \circ f$. Έστω, για παράδειγμα, οι

$$f(x) = x^2 + 1 \qquad \text{και} \qquad g(x) = \sin x.$$

Έχουμε τότε

$$(f \circ g)(x) = f(g(x)) = f(\sin x) = \sin^2 x + 1$$

και

$$(g \circ f)(x) = g(f(x)) = g(x^2+1) = \sin(x^2+1).$$

Παρατηρούμε ότι $f \circ g \neq g \circ f$.

5. Η σύνθεση μεταθέσεων στο S_n *δεν είναι* αντιμεταθετική. Έστω, για παράδειγμα, οι μεταθέσεις του S_3:

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \text{και} \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Έχουμε τότε:

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ \tau_{\sigma_1} & \tau_{\sigma_2} & \tau_{\sigma_3} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \tau_2 & \tau_1 & \tau_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

και

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ \sigma_{\tau_1} & \sigma_{\tau_2} & \sigma_{\tau_3} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \sigma_3 & \sigma_1 & \sigma_2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Παρατηρούμε ότι $\tau \circ \sigma \neq \sigma \circ \tau$.

Ορισμός Α.1.8

Ένα στοιχείο e του A καλείται **ουδέτερο στοιχείο ως προς την πράξη** $*$ αν

$$a * e = e * a = a \qquad \forall a \in A$$

Παραδείγματα

1. Στο $\mathbf{Z}$, το ουδέτερο στοιχείο ως προς την πρόσθεση είναι το 0. Το ουδέτερο στοιχείο ως προς τον πολλαπλασιασμό είναι το 1.

2. Στο $\mathbf{R}^n$ (ή το $\mathbf{C}^n$), το ουδέτερο στοιχείο ως προς την πρόσθεση είναι το **μηδενικό διάνυσμα**

$$\mathbf{0} = (0, 0, \cdots, 0)\,.$$

Έστω το $u = (u_1, u_2, \cdots, u_n) \in \mathbf{R}^n$. Έχουμε τότε,

$$\begin{aligned} u + \mathbf{0} &= (u_1, u_2, \cdots, u_n) + (0, 0, \cdots, 0) \\ &= (u_1 + 0, u_2 + 0, \cdots, u_n + 0) = (u_1, u_2, \cdots, u_n) = u. \end{aligned}$$

3. Στο $M_{m\times n}$, το ουδέτερο στοιχείο ως προς την πρόσθεση είναι ο **μηδενικός πίνακας**.

$$O = (0)_{m\times n}$$

Για κάθε πίνακα $A \in M_{m\times n}$, έχουμε

$$A + O = O + A = A\,.$$

4. Στο $M_{n\times n}$, το ουδέτερο στοιχείο ως προς τον πολλαπλασιασμό είναι ο **ταυτοτικός πίνακας**

$$I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} = (\delta_{ij})_{n\times n}$$

όπου

$$\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

το δέλτα του Kronecker. Για κάθε πίνακα $A \in M_{n\times n}$ ισχύει η

$$AI = IA = A\,.$$

5. Στο $C(\mathbf{R})$, το ουδέτερο στοιχείο ως προς την πρόσθεση είναι η μηδενική συνάρτηση:

$$0(x) = 0 \quad \forall x \in \mathbf{R} .$$

Το ουδέτερο στοιχείο του $C(\mathbf{R})$ ως προς τη σύνθεση $\circ$ είναι η **ταυτοτική συνάρτηση**:

$$e(x) = x \quad \forall x \in \mathbf{R} .$$

Πράγματι $\forall f \in C(\mathbf{R})$ παίρνουμε

$$\left.\begin{array}{l}(f \circ e)(x) = f(e(x)) = f(x) \\ (e \circ f)(x) = e(f(x)) = f(x)\end{array}\right\} \Rightarrow \quad f \circ e = e \circ f = f .$$

6. Στο S_n, το ουδέτερο στοιχείο ως προς τη σύνθεση $\circ$ είναι η **ταυτοτική μετάθεση**

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} .$$

Πραγματικά, $\forall \ \sigma \in S_n$ ισχύει

$$\sigma \circ e = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma_{e_1} & \sigma_{e_2} & \cdots & \sigma_{e_n} \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma_1 & \sigma_2 & \cdots & \sigma_n \end{pmatrix} = \sigma .$$

Η $e \circ \sigma = \sigma$ αποδεικνύεται με παρόμοιο τρόπο.

Πρόταση Α.1.9
Έστω μία πράξη $*$ στο μή κενό σύνολο Α. Αν υπάρχει το ουδέτερο στοιχείο e ως προς την πράξη $*$, τότε αυτό είναι μοναδικό.

Απόδειξη
Έστω ότι υπάρχουν δύο ουδέτερα στοιχεία e, e', οπότε $\forall\, a \in A$ ισχύουν οι:

$$a * e = e * a = a \qquad (i)$$

$$a * e' = e' * a = a \qquad (ii)$$

Από την (i) θέτοντας $a{=}e'$ παίρνουμε

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

Από την (ii) θέτοντας $a{=}e$ παίρνουμε

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

και έτσι βρίσκουμε ότι

$$e' = e .$$

Άρα το ουδέτερο στοιχείο είναι μοναδικό. □

Ορισμός Α.1.10

Έστω μια πράξη $*$ στο μη κενό σύνολο Α και $e \in A$ το ουδέτερο στοιχείο ως προς αυτή την πράξη. Αν υπάρχει στοιχείο $a' \in A$ τέτοιο ώστε:

$$a' * a = a * a' = e$$

τότε αυτό καλείται **συμμετρικό του** $a \in A$ **ως προς την πράξη** $*$.

Παραδείγματα

1. Θεωρούμε το σύνολο $\mathbf{Z}$ των ακεραίων. Το ουδέτερο στοιχείο του $\mathbf{Z}$ ως προς την πρόσθεση είναι το 0. Το συμμετρικό του $n \in \mathbf{Z}$ ως προς την πρόσθεση είναι το $-n$ αφού
$$(-n) + n = n + (-n) = 0$$

2. Το ουδέτερο στοιχείο του $\mathbf{Z}$ ως προς τον πολλαπλασιασμό είναι το 1. Τα μόνα στοιχεία του $\mathbf{Z}$ που έχουν συμμετρικό ως προς τον πολλαπλασιασμό είναι τα 1 και -1.

Πρόταση Α.1.11

Έστω μια πράξη $*$ στο μη κενό σύνολο Α. Αν υπάρχει το ουδέτερο στοιχείο ως προς την πράξη $*$ και η πράξη αυτή είναι προσεταιριστική, τότε το συμμετρικό ενός στοιχείου $a \in A$ ως προς την πράξη $*$ (αν υπάρχει) είναι μοναδικό.

Απόδειξη

Έστω a' και a'' δύο συμμετρικά του $a \in A$ ως προς την πράξη $*$, οπότε ισχύουν οι

$$a' * a = a * a' = e \qquad (i)$$

$$a'' * a = a * a'' = e \qquad (ii)$$

Έχουμε διαδοχικά:

$$\begin{array}{rcll} a'' & = & a'' * e & (\text{ορισμός του ουδέτερου στοιχείου}) \\ & = & a'' * (a * a') & (\text{από την } (i)) \\ & = & (a'' * a) * a' & (\text{προσεταιριστική ιδιότητα}) \\ & = & e * a' & (\text{από την } (ii)) \\ & = & a' & (\text{ορισμός του ουδέτερου στοιχείου}) \end{array}$$

Άρα το συμμετρικό στοιχείο του $a \in A$ είναι μοναδικό. □

Στη συνέχεια, θα λέμε **πρόσθεση** μια πράξη για την οποία χρησιμοποιούμε το σύμβολο $+$. Το ουδέτερο στοιχείο ως προς την πρόσθεση καλείται **μηδενικό στοιχείο** και το συμβολίζουμε με

$$0 \quad \text{ή} \quad \mathbf{0} \quad \text{ή} \quad O.$$

Το συμμετρικό ενός στοιχείου $a \in A$ ως προς την πρόσθεση καλείται **αντίθετο** του α και το συμβολίζουμε με $-a$. Συνοψίζουμε τους μέχρι τώρα ορισμούς για την πρόσθεση στον πιο κάτω πίνακα.

Πρόσθεση $+ : A \times A \longrightarrow A$		
Προσεταιριστική ιδιότητα (αν ισχύει)	$x + (y + z) = (x + y) + z$	$\forall x, y, z \in A$
Αντιμεταθετική ιδιότητα (αν ισχύει)	$x + y = y + x$	$\forall x, y \in A$
Για το μηδενικό στοιχείο $0 \in A$ (αν υπάρχει στο A)	$x + 0 = 0 + x = x$	$\forall x \in A$
Για το αντίθετο στοιχείο (αν υπάρχει στο A)	$x + (-x) = (-x) + x = 0$	$x,\ -x \in A$

Μια πράξη για την οποία χρησιμοποιούμε το σύμβολο $\cdot$, που συνήθως παραλείπεται, καλείται συνήθως **πολλαπλασιασμός**. Το ουδέτερο στοιχείο ως προς τον πολλαπλασιασμό καλείται **μοναδιαίο** ή **ταυτοτικό στοιχείο** και το συμβολίζουμε με

$$1 \quad \text{ή} \quad e \quad \text{ή} \quad I.$$

Το συμμετρικό ενός στοιχείου $a \in A$ ως προς τον πολλαπλασιασμό καλείται **αντίστροφο** του α και το συμβολίζουμε με a^{-1}. Στον πιο κάτω πίνακα, συνοψίζουμε τους μέχρι τώρα ορισμούς για τον πολλαπλασιασμό.

Πολλαπλασιασμός $\cdot : A \times A \longrightarrow A$		
Προσεταιριστική ιδιότητα (αν ισχύει)	$x(yz) = (xy)z$	$\forall x, y, z \in A$
Αντιμεταθετική ιδιότητα (αν ισχύει)	$xy = yx$	$\forall x, y \in A$
Για το μοναδιαίο στοιχείο $e \in A$ (αν υπάρχει στο A)	$xe = ex = x$	$\forall x \in A$
Για το αντίστροφο στοιχείο (αν υπάρχει στο A)	$xx^{-1} = x^{-1}x = e$	$x,\ x^{-1} \in A$

Παραδείγματα

1. Θεωρούμε την πράξη της πρόσθεσης στο $\mathbf{C}^n$. Η πρόσθεση είναι προσεταιριστική, δηλαδή
$$u + (v + w) = (u + v) + w \quad \forall u, v, w \in \mathbf{C}^n\ .$$
Είναι επίσης αντιμεταθετική:
$$u + v = v + u \quad \forall u, v \in \mathbf{C}^n\ .$$
Το μηδενικό στοιχείο του $\mathbf{C}^n$ είναι το
$$\mathbf{0} = (0, 0, \cdots, 0)\ .$$

για το οποίο ισχύει η

$$u + \mathbf{0} = \mathbf{0} + u = u \quad \forall u \in \mathbf{C}^n \, .$$

Το αντίθετο στοιχείο του

$$u = (u_1, u_2, \cdots, u_n) \in \mathbf{C}^n$$

είναι το

$$-u = (-u_1, -u_2, \cdots, -u_n) \, .$$

2. Θεωρούμε την πράξη της πρόσθεσης στο $M_{m\times n}$. Η πρόσθεση πινάκων είναι προσεταιριστική, αφού

$$A + (B + C) = (A + B) + C \quad \forall A, B, C \in M_{m\times n} \, .$$

Είναι επίσης αντιμεταθετική:

$$A + B = B + A \quad \forall A, B \in M_{m\times n} \, .$$

Το μηδενικό στοιχείο του $M_{m\times n}$ είναι ο μηδενικός πίνακας

$$O \; = \; (0)_{m\times n}$$

για τον οποίο ισχύει η

$$A + O = O + A = A \quad \forall A \in M_{m\times n} \, .$$

Το αντίθετο στοιχείο του $A = (a_{ij}) \in M_{m\times n}$ είναι ο πίνακας

$$-A \; = \; (-a_{ij}) \, ,$$

οπότε ισχύει η

$$A + (-A) = (-A) + A = O \, .$$

(Ο $-A$ καλείται *αντίθετος του* A.)

3. Θεωρούμε την πράξη του πολλαπλασιασμού στο σύνολο $M_{n\times n}$. Ο πολλαπλασιασμός πινάκων είναι προσεταιριστικός, αφού

$$A(BC) = (AB)C \quad \forall A, B, C \in M_{n\times n} \, .$$

Δεν είναι όμως αντιμεταθετικός. Αν $A, B \in M_{n\times n}$, τότε γενικά

$$AB \neq BA \, .$$

(Αν οι πίνακες $A, B \in M_{n\times n}$ ικανοποιούν την $AB = BA$, τότε καλούνται **αντιμεταθέσιμοι**.) Το μοναδιαίο στοιχείο του $M_{n\times n}$ είναι ο μοναδιαίος πίνακας

$$I \; = \; (\delta_{ij})_{n\times n}$$

για τον οποίο ισχύει η

$$AI = IA = A \quad \forall A \in M_{n\times n} \, .$$

Σημειώνουμε τέλος ότι δεν έχουν όλοι οι τετραγωνικοί πίνακες αντίστροφο. Αν ο πίνακας $A \in M_{n\times n}$ είναι **αντιστρέψιμος**, τότε ο αντίστροφός του A^{-1} ικανοποιεί την

$$A^{-1}A = AA^{-1} = I \, .$$

4. Θεωρούμε την πράξη της σύνθεσης στο σύνολο $C(\mathbf{R})$. Γνωρίζουμε ήδη ότι η σύνθεση είναι προσεταιριστική αλλά όχι αντιμεταθετική. Με διαφορετικά λόγια,

$$f \circ (g \circ h) = (f \circ g) \circ h \quad \forall f, g, h \in C(\mathbf{R}) \,,$$

ενώ αν $f, g \in C(\mathbf{R})$, έχουμε *γενικά*

$$f \circ g \neq g \circ f \,.$$

Το μοναδιαίο στοιχείο του $C(\mathbf{R})$ είναι η ταυτοτική συνάρτηση,

$$e(x) \;=\; x \quad \forall x \in \mathbf{R} \,,$$

για την οποία ισχύει η

$$f \circ e \;=\; e \circ f \;=\; f \quad \forall f \in C(\mathbf{R}) \,.$$

Γνωρίζουμε επίσης ότι δεν είναι όλες οι συνεχείς συναρτήσεις αντιστρέψιμες. Αν μια συνάρτηση $f \in C(\mathbf{R})$ είναι αντιστρέψιμη, τότε η αντίστροφή της f^{-1} ικανοποιεί την

$$f^{-1} \circ f \;=\; f \circ f^{-1} \;=\; e \,.$$

5. Θεωρούμε, τέλος, την πράξη της σύνθεσης στο σύνολο S_n. Η σύνθεση μεταθέσεων είναι προσεταιριστική, δηλαδή

$$\sigma \circ (\tau \circ \upsilon) = (\sigma \circ \tau) \circ \upsilon \quad \forall \sigma, \tau, \upsilon \in S_n \,,$$

αλλά όχι αντιμεταθετική, δηλαδή αν $\sigma, \tau \in S_n$, έχουμε *γενικά*

$$\sigma \circ \tau \neq \tau \circ \sigma \,.$$

Το μοναδιαίο στοιχείο του S_n είναι η ταυτοτική μετάθεση,

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

για την οποία ισχύει η

$$\sigma \circ e = e \circ \sigma = \sigma \quad \forall \sigma \in S_n.$$

Όλες οι μεταθέσεις του S_n έχουν αντίστροφη. Η αντίστροφη της

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma_1 & \sigma_2 & \cdots & \sigma_n \end{pmatrix} \in S_n$$

είναι η

$$\sigma^{-1} = \begin{pmatrix} \sigma_1 & \sigma_2 & \cdots & \sigma_n \\ 1 & 2 & \cdots & n \end{pmatrix} .$$

Για παράδειγμα, η αντίστροφη της

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix} \in S_5$$

είναι η

$$\sigma^{-1} = \begin{pmatrix} 2 & 5 & 1 & 3 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix} .$$

Κλείνουμε αυτή την παράγραφο με μια απλή άσκηση.

Παράδειγμα
Έστω το σύνολο των ρητών αριθμών $\mathbf{Q}$ και η πράξη $*$:

$$a * b = a + b - ab, \quad a, b \in \mathbf{Q}$$

(α) Να βρεθούν οι $3 * 4, \quad 2 * (-5)$και $7 * \frac{1}{2}$.
(β) Είναι το ζεύγος $(\mathbf{Q}, *)$ ημιομάδα;
(γ) Είναι η πράξη $*$ αντιμεταθετική;
(δ) Να βρεθεί το ουδέτερο στοιχείο ως προς την πράξη $*$.
(ε) Ποιά στοιχεία του $\mathbf{Q}$ δεν έχουν συμμετρικό στοιχείο ως προς την πράξη $*$;

Λύση
(α)

$$\begin{array}{lcl} 3 * 4 & = & 3 + 4 - 3\,(4) = 7 - 12 = -5 \\ 2 * (-5) & = & 2 + (-5) - (2)(-5) = -3 + 10 = 7 \\ 7 * \frac{1}{2} & = & 7 + \frac{1}{2} - 7\left(\frac{1}{2}\right) = \frac{15}{2} - \frac{7}{2} = 4 \end{array}$$

(β) Παρατηρούμε πρώτα ότι η $*$ είναι πράξη στο $\mathbf{Q}$, ότι δηλαδή το $\mathbf{Q}$ είναι κλειστό ως προς την $*$, αφού αν $a, b \in \mathbf{Q}$, τότε $(a + b - ab) \in \mathbf{Q}$. Για να είναι το ζεύγος $(\mathbf{Q}, *)$ ημιομάδα, πρέπει επιπλέον η πράξη $*$ να είναι προσεταιριστική, δηλαδή να ισχύει:

$$a * (b * c) = (a * b) * c \qquad \forall a, b, c \in \mathbf{Q} \qquad (i)$$

Για τα δυο μέλη της (i) έχουμε:

$$\begin{array}{rcl} a * (b * c) & = & a * (b + c - bc) \\ & = & a + b + c - bc - a(b + c - bc) \\ & = & a + b + c - bc - ab - ac + abc \end{array}$$

και

$$\begin{array}{rcl} (a * b) * c & = & (a + b - ab) * c \\ & = & a + b - ab + c - (a + b - ab)c \\ & = & a + b - ab + c - ac - bc + abc \\ & = & a + b + c - bc - ab - ac + abc \end{array}$$

Η (i) ισχύει, άρα η $*$ είναι προσεταιριστική και έτσι το ζεύγος $(\mathbf{Q}, *)$ είναι ημιομάδα.
(γ) Παρατηρούμε ότι $\forall a, b \in Q$,

$$a * b = a + b - ab = b + a - ba = b * a\,.$$

Άρα η $*$ είναι αντιμεταθετική.

(δ) Το ουδέτερο στοιχείο ως προς την πράξη $*$ είναι το 0. Πράγματι,

$$a * 0 = a + 0 - a0 = a \qquad \forall a \in Q \, ,$$

οπότε

$$a * 0 = 0 * a = a \qquad \forall a \in Q \, ,$$

αφού η $*$ είναι αντιμεταθετική.

(ε) Έστω ένα στοιχείο $a \in \mathbf{Q}$. Αν υπάρχει το συμμετρικό του ως προς την πράξη $*$,

έχουμε

$$a * a^{-1} = 0 \, ,$$

αφού το ουδέτερο στοιχείο (ως προς την πράξη $*$) είναι το 0, και έτσι

$$a + a^{-1} - aa^{-1} = 0 \qquad \Rightarrow \qquad a = a^{-1}\,(a-1) \qquad \Longrightarrow$$

$$a^{-1} \; = \; \frac{a}{a-1}$$

Είναι φανερό ότι κάθε στοιχείο $a \in Q$ με $a \neq 1$ έχει συμμετρικό ως προς την πράξη $*$ που δίνεται από την πιο πάνω σχέση. □

A.2 Ομάδες

Οι ομάδες και οι δακτύλιοι είναι δύο από τις πιο απλές αλλά ταυτόχρονα και πιο σπουδαίες αλγεβρικές δομές. Τις ομάδες χρησιμοποίησαν πρώτοι οι Galois[1] και Lagrange όταν μελετούσαν την επιλυσιμότητα των εξισώσεων. Η ανάπτυξη της θεωρίας των ομάδων ήταν ραγδαία τα τελευταία εξήντα χρόνια. Ο λόγος είναι ότι με τη βοήθεια τους μπορούν να περιγραφούν και να μελετηθούν σε βάθος πολλές μαθηματικές, φυσικές και χημικές θεωρίες. Οι δακτύλιοι, από την άλλη μεριά, εισήχθησαν στα πλαίσια της προσπάθειας των ερευνητών να επιλύσουν το γνωστό πρόβλημα του Fermat.

Ορισμός A.2.1

Ομάδα (group) καλείται ένα ζεύγος $(G, \cdot)$, όπου G ένα μη κενό σύνολο και $\cdot$ μια πράξη στο σύνολο G, με τις εξής ιδιότητες:
(i) Η πράξη είναι προσεταιριστική, δηλαδή

$$a(bc) = (ab)c \quad \forall a, b, c \in G \, .$$

(ii) Υπάρχει το μοναδιαίο στοιχείο $e \in G$ τέτοιο ώστε

$$ae = ea = a \quad \forall a \in G \, .$$

(iii) Κάθε $a \in G$ έχει αντίστροφο, δηλαδή $\forall a \in G, \quad \exists a^{-1} \in G$ τέτοιο ώστε

$$a^{-1}a = aa^{-1} = e \, .$$

Αν επιπλέον,
(iv) Η πράξη είναι αντιμεταθετική, δηλαδή

$$ab = ba \quad \forall a, b \in G \, ,$$

η ομάδα καλείται **αντιμεταθετική** (commutative) ή **αβελιανή** (abelian).

Παρατηρήσεις

1. Όταν η πράξη συμβολίζεται με $\cdot$ (ή $*$ ή $\circ$) λέμε ότι είναι πολλαπλασιασμός και η $(G, \cdot)$ καλείται **πολλαπλασιαστική ομάδα** (multiplicative group). Οταν η πράξη συμβολίζεται με $+$ λέμε ότι είναι πρόσθεση και η $(G, +)$ καλείται **προσθετική ομάδα** (additive group). Στην περίπτωση της πρόσθεσης, το ουδέτερο στοιχείο στη συνθήκη (ii) είναι το μηδενικό, 0, για το οποίο ισχύει

   $$a + 0 = 0 + a = a \qquad \forall a \in G \, ,$$

   ενώ το συμμετρικό στοιχείο στη (iii) είναι το αντίθετο στοιχείο $-a \in G$, για το οποίο ισχύει η

   $$(-a) + a = a + (-a) = 0 \, .$$

[1] **Galois, Évariste** (1811-1832). Γάλλος μαθηματικός με τεράστια συμβολή στις θεωρίες συναρτήσεων, εξισώσεων και αριθμών. Θεμελιωτής της θεωρίας ομάδων.

Στη συνέχεια θα λέμε απλά *η ομάδα* G χωρίς να γράφουμε το σύμβολο της πράξης, εφόσον δεν υπάρχει περίπτωση σύγχυσης.

2. Είναι φανερό ότι οι ιδιότητες (ii) και (iii) καθιστούν μια ημιομάδα ομάδα, και η ιδιότητα (iv) καθιστά μια ομάδα αντιμεταθετική.

Παραδείγματα

1. Τα σύνολα $\mathbf{Z}, \mathbf{Q}, \mathbf{R}$ και $\mathbf{C}$ με τη συνήθη πράξη της πρόσθεσης αποτελούν αβελιανές ομάδες. Ας πάρουμε, για παράδειγμα, το σύνολο $\mathbf{C}$:
   (i)
   $$z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3 \quad \forall z_1, z_2, z_3 \in \mathbf{C}$$
   (ii) Το μηδενικό στοιχείο του $\mathbf{C}$ είναι το $0 = 0 + 0\,i$, για το οποίο έχουμε
   $$z + 0 = 0 + z = z \quad \forall z \in \mathbf{C}\,.$$
   (iii) Το αντίθετο του $z = a + b\,i \in \mathbf{C}$ είναι το
   $$-z = -a - b\,i \in \mathbf{C}\,.$$
   (iv)
   $$z_1 + z_2 = z_2 + z_1 \quad \forall z_1, z_2 \in \mathbf{C}\,.$$

2. Το σύνολο των φυσικών αριθμών $\mathbf{N}$ με την πράξη της πρόσθεσης δεν αποτελεί ομάδα γιατί το $0 \notin \mathbf{N}$, άρα δεν ικανοποιείται η συνθήκη (ii) του Ορισμού Α.2.1. Όμως, ούτε το σύνολο $\mathbf{N_0} = \mathbf{N} \cup \{0\}$ είναι ομάδα (με την πράξη της πρόσθεσης) αφού δεν ικανοποιείται η συνθήκη (iii).

3. Τα σύνολα
   $$\mathbf{Q}^* = \mathbf{Q} - \{0\}\,, \quad \mathbf{R}^* = \mathbf{R} - \{0\}\,, \quad \mathbf{C}^* = \mathbf{C} - \{0\}$$
   αποτελούν αβελιανές ομάδες ως προς το συνήθη πολλαπλασιασμό (γιατί εξαιρέσαμε το 0 από τα πιο πάνω σύνολα;). Παίρνοντας ως παράδειγμα το σύνολο $\mathbf{R}^*$, έχουμε:
   (i) $x(yz) = (xy)z \qquad \forall x, y, z \in \mathbf{R}^*$.
   (ii) Το μοναδιαίο στοιχείο είναι το $1 \in \mathbf{R}^*$:
   $$x1 = 1x = x \qquad \forall x \in \mathbf{R}^*.$$
   (iii) Κάθε $x \in \mathbf{R}^*$ έχει αντίστροφο, το $x^{-1} = \frac{1}{x}$ που ικανοποιεί την
   $$x^{-1}x = xx^{-1} = 1\,.$$
   (iv) $xy = yx \qquad \forall x, y \in \mathbf{R}^*$.

   Το $\mathbf{Z}^* = \mathbf{Z} - \{0\}$ δεν είναι ομάδα. Γιατί;

4. Το σύνολο S_n με την πράξη της σύνθεσης είναι ομάδα. Πράγματι,
   (i) Η σύνθεση είναι προσεταιριστική:

$$\sigma(\tau\upsilon) = (\sigma\tau)\upsilon \qquad \forall \sigma, \tau, \upsilon \in S_n.$$

   (ii) Το μοναδιαίο στοιχείο του S_n είναι η ταυτοτική μετάθεση

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} \in S_n \,,$$

   για την οποία ισχύει

$$\sigma e = e\sigma = \sigma \qquad \forall \sigma \in S_n \,.$$

   (iii) Κάθε μετάθεση

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma_1 & \sigma_2 & \cdots & \sigma_n \end{pmatrix} \in S_n$$

   έχει αντίστροφη που είναι η

$$\sigma^{-1} = \begin{pmatrix} \sigma_1 & \sigma_2 & \cdots & \sigma_n \\ 1 & 2 & \cdots & n \end{pmatrix} .$$

   Το S_n δεν είναι αβελιανή ομάδα αφού η σύνθεση δεν είναι αντιμεταθετική.

5. Το σύνολο $M_{m\times n}$ με την πράξη της πρόσθεσης είναι αβελιανή ομάδα.

6. Το σύνολο $M_{n\times n}$ με την πράξη του πολλαπλασιασμού δεν είναι ομάδα αν και ο πολλαπλασιασμός είναι προσεταιριστικός και υπάρχει το μοναδιαίο στοιχείο που είναι ο μοναδιαίος πίνακας I γιατί δεν έχουν όλοι οι $n \times n$ πίνακες αντίστροφο [δεν ικανοποιείται η (iii)].

   Το σύνολο $\mathcal{M}^*_{n\times n}$ των αντιστρέψιμων $n \times n$ πινάκων με την πράξη του πολλαπλασιασμού είναι ομάδα. (Είναι το $S_{n\times n}$ κλειστό ως προς τον πολλαπλασιασμό; Γιατί;) Δεν είναι όμως αβελιανή αφού ο πολλαπλασιασμός πινάκων δεν είναι αντιμεταθετικός.

7. Το σύνολο $C(\mathbf{R})$ με την πράξη της πρόσθεσης είναι αβελιανή ομάδα.

8. Το σύνολο $C(\mathbf{R})$ με την πράξη της σύνθεσης δεν είναι ομάδα αν και η σύνθεση είναι προσεταιριστική και υπάρχει το μοναδιαίο στοιχείο, που είναι η ταυτοτική συνάρτηση

$$e(x) = x \qquad \forall x \in \mathbf{R} \,,$$

   γιατί δεν έχουν όλες οι συναρτήσεις αντίστροφη [δεν ικανοποιείται η (iii)].

   Το σύνολο $C^*(\mathbf{R})$ των αντιστρέψιμων συνεχών συναρτήσεων είναι ομάδα (γιατί;). Δεν είναι όμως αβελιανή, αφού η σύνθεση δεν είναι αντιμεταθετική.

9. Έστω P_n το σύνολο των πολυωνύμων βαθμού μικρότερου ή ίσου του n:

$$P_n \;=\; \{p = a_0 + a_1 x + \cdots + a_n x^n \,,\;\; a_i \in \mathbf{R},\;\; i = 1, 2, \cdots, n\} \;.$$

Ορίζουμε την πράξη της πρόσθεσης στο P_n ως εξής: αν $p, q \in P_n$ με

$$\begin{aligned} p &= a_0 + a_1 x + \cdots + a_n x^n \,, \\ q &= b_0 + b_1 x + \cdots + b_n x^n \,, \,, \end{aligned}$$

τότε

$$p + q = (a_0 + b_0) + (a_1 + b_1)\, x + \cdots + (a_n + b_n)\, x^n \;\in P_n \;.$$

(Γιατί δεν ορίσαμε το P_n ως το σύνολο των πολυωνύμων **βαθμού** n;) Το $(P_n, +)$ είναι ομάδα. Πραγματικά,
(i) $p + (q + r) = (p + q) + r \quad \forall p, q, r \in P_n$.
(ii) Το μηδενικό στοιχείο του P_n είναι το

$$0(x) = 0 + 0x + \cdots + 0x^n = 0 \,,$$

για το οποίο ισχύει

$$p + 0 = 0 + p = p \quad \forall p \in P_n \;.$$

(iii) Το αντίθετο του $p = a_0 + a_1 x + \cdots + a_n x^n \in P_n$ είναι το

$$-p = (-a_0) + (-a_1)x + \cdots + (-a_n)x^n \,,$$

οπότε

$$p + (-p) = (-p) + p = 0 \;.$$

Επιπλέον, το $(P_n, +)$ είναι αβελιανή ομάδα, αφού

$$p + q = q + p \quad \forall p, q \in P_n \;.$$

Ας ορίσουμε τώρα μια πράξη πολλαπλασιασμού στο P_2:

$$\begin{aligned} &(a_0 + a_1 x + a_2 x^2)\,(b_0 + b_1 x + b_2 x^2) \\ &\quad = \;\; a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + (a_1 b_2 + a_2 b_1)x^3 + a_2 b_2 x^4 \\ &\quad = \;\; \gamma_0 + \gamma_1 x + \gamma_2 x^2 + \gamma_3 x^3 + \gamma_4 x^4 \,, \end{aligned}$$

όπου

$$\gamma_k = \sum_{i+j=k} a_i \beta_j, \qquad\qquad k = 0, 1, 2, 3, 4 \;.$$

(Εννοείται ότι $i = 1, 2$ και $j = 1, 2$.) Ο πολλαπλασιασμός δύο πολυωνύμων του P_n ορίζεται ανάλογα, με $k = 0, 1, 2, \cdots, 2n$.

Το $(P_n, \cdot)$ δεν είναι ομάδα αφού το P_n δεν είναι κλειστό ως προς τον πολλαπλασιασμό. Ας θεωρήσουμε τώρα το σύνολο P_∞ όλων των πολυωνύμων και ας εξετάσουμε αν το $(P_\infty, \cdot)$ είναι ομάδα. Παρατηρούμε πρώτα ότι το P_∞ είναι κλειστό ως προς τον πολλαπλασιασμό. Η ιδιότητα (i) του Ορισμού Α.2.1 ικανοποιείται αφού

$$p(qr) = (pq)r \quad \forall p, q, r \in P_\infty \;.$$

(Άρα το $(P_\infty, \cdot)$ είναι ημιομάδα.) Επίσης, ικανοποιείται και η ιδιότητα (ii), αφού υπάρχει το μοναδιαίο στοιχείο που είναι το πολυώνυμο $e(x) = 1$:

$$pe = ep = p \quad \forall p \in P_\infty \, .$$

Όμως, η ιδιότητα (iii) δεν ικανοποιείται αφού τα μόνα στοιχεία του P_∞ που έχουν αντίστροφο είναι τα σταθερά πολυώνυμα $p(x) = c \neq 0$, $c \in \mathbf{R}$. Συμπεραίνουμε ότι το $(P_\infty, \cdot)$ δεν είναι ομάδα.

Ορισμός Α.2.2
Έστω $(G, \cdot)$ μια ομάδα και $H \subseteq G$. Το υποσύνολο H καλείται **υποομάδα** (subgroup) της G αν ισχύουν τα εξής:
(i) $e \in H$.
(ii) Αν $x, y, \in H$ τότε $xy \in H$ (το H είναι κλειστό ως προς την πράξη $\cdot$).
(iii) Αν $x \in H$ τότε $x^{-1} \in H$ (το H είναι κλειστό ως προς την αντιστροφή).

Παρατηρήσεις

1. Ο Ορισμός Α.2.2 μας λέει ότι το H είναι υποομάδα της G αν είναι και αυτό ομάδα ως προς την ίδια πράξη.

2. Αν αντί του πολλαπλασιασμού έχουμε την πρόσθεση $+$, τότε οι συνθήκες (i)-(iii) παίρνουν την μορφή:
   (i) $0 \in H$.
   (ii) Αν $x, y \in H$ τότε $x + y \in H$.
   (iii) Αν $x \in H$ τότε $-x \in H$.

3. Αν $H \subset G$ και η $(H, \cdot)$ ικανοποιεί τις συνθήκες (i)-(iii) λέμε ότι η H είναι **γνήσια υποομάδα** (proper subroup) της G.

Παραδείγματα

1. Είναι φανερό από τη συνθήκη (i) ότι μια υποομάδα περιέχει τουλάχιστον ένα στοιχείο, το ουδέτερο στοιχείο. Είναι εύκολο να δούμε ότι το $(\{e\}, \cdot)$ είναι υποομάδα της $(G, \cdot)$ και το $(\{0\}, +)$ είναι υποομάδα της $(G, +)$. Οι δύο αυτές υποομάδες καλούνται **τετριμμένες υποομάδες** (trivial subgroups).

2. Η ομάδα $(\mathbf{Z}, +)$ είναι υποομάδα της $(\mathbf{Q}, +)$.

3. Οι άρτιοι αριθμοί $S = \{\cdots, -4, -2, 0, 2, 4, \cdots\}$ με την πράξη της πρόσθεσης αποτελούν μια (γνήσια) υποομάδα της $(\mathbf{Z}, +)$. Πραγματικά,
   (i) $0 \in S$
   (ii) το άθροισμα δύο άρτιων είναι άρτιος.
   (iii) Αν $x \in S$ τότε $-x \in S$ (ο αντίθετος ενός άρτιου είναι άρτιος).

4. Είδαμε προηγουμένως ότι το $(P_\infty, +)$ είναι ομάδα. Το $(P_n, +)$ είναι υποομάδα του $(P_\infty, +)$.

5. Οι μιγαδικοί αριθμοί με μοναδιαίο μέτρο, $S = \{z | z \in \mathbf{C} \text{ και } |z| = 1\}$ αποτελούν υποομάδα της $(\mathbf{C}^*, \cdot)$, όπου $\mathbf{C}^*=\mathbf{C} - \{0\}$. Πραγματικά,
(i) $1 \in S$ αφού $|1| = 1$.
(ii) Αν $z_1, z_2 \in S$, οπότε $|z_1| = |z_2| = 1$, έχουμε

$$|z_1 z_2| = |z_1||z_2| = 1 \cdot 1 = 1 \quad \Longrightarrow \quad z_1 z_2 \in S \, .$$

(iii) Αν $z \in S$, τότε

$$|z^{-1}| = \frac{1}{|z|} = \frac{1}{1} = 1 \quad \Longrightarrow \quad z^{-1} \in S \, .$$

Άρα το S είναι υποομάδα της $(\mathbf{C}^*, \cdot)$.

Ορισμός Α.2.3
Ο αριθμός των στοιχείων μιας ομάδας $(G, \cdot)$ καλείται **τάξη** (order) της G και συμβολίζεται με $|G|$. Αν το $|G|$ είναι πεπερασμένο, δηλ. $|G| \in \mathbf{N}$, η G καλείται **πεπερασμένη ομάδα** (finite group).

Παράδειγματα

1. Είδαμε προηγουμένως ότι το $(S_n, \circ)$ είναι (μη αβελιανή) ομάδα. Ως γνωστό, το S_n περιέχει $n!$ στοιχεία, δηλαδή $|S_n| = n!$. Άρα το S_n είναι πεπερασμένη ομάδα.

2. Η μόνη γνήσια υποομάδα του

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\} ,$$

είναι το μονοσύνολο

$$S' = \{e\} = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \right\}$$

(τετριμμένη υποομάδα). Ο αναγνώστης μπορεί εύκολα να επαληθεύσει τις συνθήκες (ii) και (iii) του Ορισμού Α.2.2.

Θεώρημα Α.2.4 (Θεώρημα Lagrange**)**
Έστω $(G, \cdot)$ μια πεπερασμένη ομάδα και H μια υποομάδα της G. Τότε, η τάξη $|H|$ της H διαιρεί ακριβώς την τάξη $|G|$ της G.

Απόδειξη
Εκτός των στόχων αυτής της παραγράφου. □

Α.3 Δακτύλιοι και σώματα

Ορισμός Α.3.1

Δακτύλιος (ring) είναι μια τριάδα $(R, +, \cdot)$ που αποτελείται από ένα μη κενό σύνολο R και δύο πράξεις, την πρόσθεση $+$ και τον πολλαπλασιασμό $\cdot$, που ικανοποιούν τα εξής:

(i) Το ζεύγος $(R, +)$ είναι αβελιανή ομάδα, δηλαδή

(α) $x + (y + z) = (x + y) + z \qquad \forall x, y, z \in R.$

(β) $\exists$ το μηδενικό στοιχείο $0 \in R$ τέτοιο ώστε

$$x + 0 = 0 + x = x \qquad \forall x \in R\,.$$

(γ) $\forall x \in R$ υπάρχει το αντίθετό του $-x$, τέτοιο ώστε

$$x + (-x) = (-x) + x = 0 \qquad \forall x \in R\,.$$

(δ) $x + y = y + x \qquad \forall x, y \in R.$

(ii) Το ζεύγος $(R, \cdot)$ είναι ημιομάδα, δηλαδή η πράξη $\cdot$ είναι προσεταιριστική:

$$x(yz) = (xy)z \quad \forall x, y, z \in R$$

(iii) Η πράξη $\cdot$ είναι επιμεριστική ως προς την πράξη $+$, δηλαδή

$$x\,(y + z) = xy + xz \quad \forall x, y, z \in R$$

και

$$(y + z)\,x = yx + zx \quad \forall x, y, z \in R\,.$$

Αν επιπλέον,

(iv) $\exists$ το μοναδιαίο στοιχείο $e \in R$, τέτοιο ώστε

$$xe = ex = x \qquad \forall x \in R\,,$$

τότε ο δακτύλιος καλείται **δακτύλιος με μοναδιαίο** (ring with identity) ή **1-δακτύλιος**.

Επίσης, αν ο πολλαπλασιασμός $\cdot$ είναι αντιμεταθετικός, δηλαδή

$$xy = yx \qquad \forall x, y \in R\,,$$

τότε ο δακτύλιος καλείται **αντιμεταθετικός δακτύλιος** (commutative ring).

Παρατηρήση

Όταν δεν υπάρχει περίπτωση σύγχυσης, θα λέμε απλά *ο δακτύλιος* R χωρίς να αναφέρουμε τις πράξεις.

Παραδείγματα

1. Τα παρακάτω σύνολα με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού είναι αντιμεταθετικοί δακτύλιοι με μοναδιαίο στοιχείο το 1.

$(\mathbf{Z},+,\cdot)$: δακτύλιος των ακεραίων
$(\mathbf{Q},+,\cdot)$: δακτύλιος των ρητών
$(\mathbf{R},+,\cdot)$: δακτύλιος των πραγματικών
$(\mathbf{C},+,\cdot)$: δακτύλιος των μιγαδικών

2. Ο $(M_{n\times n},+,\cdot)$ είναι δακτύλιος (βλ. πρόβλημα 6).

3. Ο $(P_\infty,+,\cdot)$ είναι αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο το $e(x)=1$ και καλείται **δακτύλιος των πολυωνύμων**.

Ορισμός Α.3.2
Έστω ο δακτύλιος $(R,+,\cdot)$. Κάθε στοιχείο $a\in R$ που έχει αντίστροφο $a^{-1}\in R$, τέτοιο ώστε

$$aa^{-1}=a^{-1}a=e\,,$$

καλείται **μονάδα** (unit) του R.

Παραδείγματα

1. Οι μονάδες του $(\mathbf{Z},+,\cdot)$ είναι οι 1 και -1.

2. Οι μονάδες του $(\mathbf{Q},+,\cdot)$ είναι όλα τα στοιχεία του $\mathbf{Q}$ με εξαίρεση το 0.

3. Οι μονάδες του $(P_\infty,+,\cdot)$ είναι τα σταθερά πολυώνυμα $p(x)=c\neq 0,\quad c\in\mathbf{R}$.

Ορισμός Α.3.3
Σώμα (field) είναι ένα σύνολο K με δύο πράξεις, τις $+$ και $\cdot$, τέτοιες ώστε:
(i) Η τριάδα $(K,+,\cdot)$ είναι ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο.
(ii) Το ζεύγος $(K^*,\cdot)$, όπου $K^*=K-\{0\}$ και 0 το μηδενικό στοιχείο, είναι μια ομάδα.

Συνοπτικά, μπορούμε να πούμε ότι το σώμα είναι ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο του οποίου όλα τα μη μηδενικά στοιχεία είναι μονάδες, δηλαδή έχουν αντίστροφο. Αναλυτικότερα, σε ένα σώμα K ισχύουν τα εξής:

Για την πρόσθεση:

1. (i) $x+(y+z)=(x+y)+z\quad\forall x,y,z\in K$.
   (ii) $x+y=y+x\quad\forall x,y\in K$.
   (iii) $\exists$ το μηδενικό στοιχείο $0\in K$, τέτοιο ώστε

$$x+0=x\quad\forall x\in K\,.$$

   (iv) $\forall x\in K$ υπάρχει το αντίθετό του $-x\in K$, τέτοιο ώστε

$$x+(-x)=0\,.$$

Για τον πολλαπλασιασμό:

2. (i) $x(yz) = (xy)z \quad \forall x, y, z \in K$.
   (ii) $xy = yx \quad \forall x, y \in K$.
   (iii) $\exists$ το μοναδιαίο στοιχείο $1 \in K$ με $1 \neq 0$, τέτοιο ώστε
   $$1x = x1 = x \quad \forall x \in K \ .$$
   (iv) $\forall x \in K$ με $x \neq 0$, υπάρχει το αντίστροφό του x^{-1}, τέτοιο ώστε
   $$x^{-1}x = 1 \ .$$

3. Η πράξη $\cdot$ είναι επιμεριστική ως προς την $+$:
   $$x(y+z) = xy + xz \quad \forall x, y, z \in K \ .$$

Παρατήρηση
Ένα σώμα έχει τουλάχιστον δύο στοιχεία, τα 0 και 1. Το σύνολο $\{0\}$ ικανοποιεί τις παραπάνω ιδιότητες εκτός της 2(iii) και επομένως δεν αποτελεί σώμα.

Παραδείγματα

1. Τα σύνολα $\mathbf{Q}$, $\mathbf{R}$ και $\mathbf{C}$ με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού είναι σώματα.

2. Η τριάδα $(\mathbf{Z}, +, \cdot)$ δεν αποτελεί σώμα γιατί τα μόνα μη μηδενικά στοιχεία που έχουν αντίστροφο είναι τα 1 και -1.

3. Το σύνολο $\{0, 1\}$ με τις συνήθεις πράξεις δεν είναι σώμα. Το σύνολο δεν είναι κλειστό ως προς την πρόσθεση αφού
   $$1 + 1 = 2 \notin \{0, 1\} \ .$$
   Ορίζουμε τώρα τις δύο πράξεις ως εξής:
   $$\begin{aligned} 0 + 0 = \quad & 1 + 1 = \quad 0 \\ 1 + 0 = \quad & 0 + 1 = \quad 1 \\ 0 \cdot 0 = \quad & 0 \cdot 1 = \quad 1 \cdot 0 = 0 \\ 1 \cdot 1 = \quad & 1 \end{aligned}$$
   Παρατηρούμε ότι το $\{0, 1\}$ είναι κλειστό ως προς τις δύο πράξεις και ότι το αντίθετο του 1 είναι ο εαυτός του! Το $\{0, 1\}$ με τις πιο πάνω πράξεις είναι σώμα και συμβολίζεται με $\mathbf{F}_2$ ή $\mathbf{Z}_2$.

Πρόταση Α.3.4
Αν το K' είναι υποσύνολο του $\mathbf{C}$, το $(K', +, \cdot)$ είναι σώμα αν ισχύουν τα εξής:
(α) $0 \in K'$ και $1 \in K'$.
(β) Το K' είναι κλειστό ως προς τις πράξεις $+$ και $\cdot$.
(γ) Αν $x \in K'$, τότε $-x \in K'$.
(δ) Το $K' - \{0\}$ είναι κλειστό ως προς την αντιστροφή.

Τα στοιχεία ενός σώματος K θα τα καλούμε **αριθμούς** (numbers), αν δεν υπάρχει κίνδυνος σύγχυσης, ή **βαθμωτά** (scalars).

Α.4 Εξωτερικές πράξεις

Στην παράγραφο 1, ορίσαμε την έννοια της διμελούς πράξης στο μη κενό σύνολο Α:

$$* : A \times A \to A \qquad \text{όπου } (a, b) \mapsto a * b$$

Η πιο πάνω πράξη λέμε ότι είναι **εσωτερική** αφού όλα τα εμπλεκόμενα στοιχεία ανήκουν στο A. Δίνουμε τώρα τον ορισμό μιας *εξωτερικής πράξης*.

Ορισμός Α.4.1
Έστω δύο μη κενά σύνολα Α και Β. Καλούμε **εξωτερική πράξη** στο Α, μια απεικόνιση της μορφής $\cdot : B \times A \to A$ με

$$(\lambda, a) \mapsto \lambda \cdot a\,, \quad \lambda \in B\,,\ a \in A\,.$$

Παρατηρήσεις

1. Εφόσον δεν υπάρχει κίνδυνος σύγχυσης, θα παραλείπουμε το σύμβολο της πράξης, δηλαδή θα γράφουμε λα αντί $\lambda \cdot a$. Επίσης, είναι προφανές από τον ορισμό ότι $\lambda a \in A$. Θεωρούμε δηλαδή ότι το Α είναι κλειστό ως προς την πράξη $\cdot$.
2. Μια εξωτερική πράξη όπως την ορίσαμε πιο πάνω μπορεί να περιγραφεί και με ένα σύνολο μονομελών πράξεων, μια για κάθε $\lambda \in B$. Πράγματι, για κάθε $\lambda \in B$ ορίζεται μια απεικόνιση
$$\cdot : A \to A \ \text{ με } \ a \mapsto \lambda a\,,$$
που είναι εξ ορισμού μια μονομελής πράξη.

Έστω K ένα σώμα και Α ένα μη κενό σύνολο. Θα καλούμε **βαθμωτό πολλαπλασιασμό** (scalar multiplication) μια εξωτερική πράξη της μορφής

$$\cdot : K \times A \to A$$

με

$$(\lambda, a) \mapsto \lambda a\,, \quad \lambda \in K\,, a \in A\,.$$

Το λa καλείται **βαθμωτό πολλαπλάσιο** (scalar product) του a. Σημειώνουμε ότι ο βαθμωτός πολλαπλασιασμός δεν ορίζεται για οποιοδήποτε σύνολο Α (π.χ. για το S_n).

Παραδείγματα

1. Στο K^n (K=**Q** ή **R** ή **C**) ο βαθμωτός πολλαπλασιασμός ορίζεται ως εξής: αν $u = (u_1, u_2, \cdots, u_n) \in K^n$ και $\lambda \in K$, τότε
$$\lambda u = (\lambda u_1, \lambda u_2, \cdots, \lambda u_n) \in K^n\,.$$
2. Στο $M_{m\times n}$, αν $A = (a_{ij}) \in M_{m\times n}$ και $\lambda \in K$, τότε
$$\lambda A = (\lambda a_{ij}) \in M_{m\times n}\,.$$

3. Στο $C(\mathbf{R})$, αν $f \in C(\mathbf{R})$ και $\lambda \in \mathbf{R}$, τότε

$$(\lambda f)(x) = \lambda f(x) \in C(\mathbf{R}) .$$

4. Στο P_n, αν $p = a_0 + a_1 x + \cdots + a_n x^n \in P_n$ και $\lambda \in \mathbf{R}$, τότε

$$(\lambda p)(x) = (\lambda a_0) + (\lambda a_1)x + \cdots (\lambda a_n)x^n \in P_n .$$

Α.5 Προβλήματα

1. Έστω ένα σύνολο S και μια πράξη $*$ που ορίζεται ως εξής:

$$a * b = a\,, \quad a, b \in S\,.$$

   (α) Να δειχθεί ότι το ζεύγος $(S, *)$ είναι ημιομάδα.

   (β) Είναι η πράξη $*$ μεταθετική;

2. Θεωρούμε το σύνολο $\mathbf{R}$ των πραγματικών αριθμών και την πράξη $*$ που ορίζεται ως εξής:

$$x * y = 3xy + x + y, \quad x, y \in \mathbf{R}\,.$$

   (α) Να βρεθούν οι $2 * 1$ και $1.2 * 3$.
   (β) Είναι το ζεύγος $(\mathbf{R}, *)$ ημιομάδα;
   (γ) Είναι η πράξη $*$ μεταθετική;
   (δ) Να βρεθεί το ουδέτερο στοιχείο ως προς την πράξη $*$.
   (ε) Ποιά στοιχεία του $\mathbf{R}$ δεν έχουν συμμετρικό ως προς την πράξη $*$;

3. Να βρεθούν όλες οι υποομάδες της $(S_3, \circ)$.
   Σημείωση: Το $\circ$ συμβολίζει τη σύνθεση μεταθέσεων.

4. Αν η $(G, \cdot)$ είναι μια ομάδα με τάξη $|G| = 19$, να βρεθούν όλες οι υποομάδες της.

5. Αν το $(G, \cdot)$ είναι ομάδα, να δειχθούν τα εξής:

   (α) $(a^{-1})^{-1} = a \quad \forall\, a \in G.$

   (β) $(ab)^{-1} = b^{-1}a^{-1} \quad \forall a, b \in G.$

6. Έστω $M_{n\times n}$ το σύνολο των $n \times n$ πινάκων.
   (α) Να δειχθεί ότι το $M_{n\times n}$ με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού είναι δακτύλιος.
   (β) Έχει ο $(M_{n\times n}, +, \cdot)$ μοναδιαίο στοιχείο;
   (γ) Είναι ο $(M_{n\times n}, +, \cdot)$ μεταθετικός;
   (δ) Ποιές είναι οι μονάδες του $(M_{n\times n}, +, \cdot)$;

7. Να οριστούν κατάλληλες πράξεις πρόσθεσης και πολλαπλασιασμού για να είναι σώμα το υποσύνολο $\{-1, 0, 1\}$ του $\mathbf{Z}$.

8. Έστω S το υποσύνολο του $\mathbf{R}$ που ορίζεται ως εξής:

$$S \;=\; \left\{x \in \mathbf{R} \mid x = p + q\sqrt{3}, \quad p, q \in \mathbf{Q}\right\}\,.$$

   Να δειχθεί ότι το S με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού είναι σώμα.

9. Εξηγήστε γιατί το σύνολο $M_{n\times n}$ των $n \times n$ πινάκων με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού δεν είναι σώμα.

Παράρτημα Β

Η ΕΝΝΟΙΑ ΤΗΣ ΑΛΓΕΒΡΑΣ

Ορισμός Β.1.1

Ένας διανυσματικός χώρος V πάνω σε ένα σώμα K, στον οποίο έχει οριστεί ένας πολλαπλασιασμός $\cdot$ που σε κάθε ζεύγος $(x, y) \in V \times V$ αντιστοιχεί ακριβώς ένα στοιχείο $x \cdot y \in V$ ονομάζεται **γραμμική άλγεβρα** ή, απλούστερα, **άλγεβρα πάνω στο** K, αν για κάθε $x, y, z \in V$ και $\lambda \in K$ ισχύουν οι ιδιότητες:

(i) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

(ii) $x \cdot (y + z) = x \cdot y + x \cdot z$
$(y + z) \cdot x = y \cdot x + z \cdot x$

(iii) $\lambda (x \cdot y) = (\lambda x) \cdot y = x \cdot (\lambda y)$

Αν επιπλέον,

(iv) $x \cdot y = y \cdot x$,

η άλγεβρα καλείται **αντιμεταθετική**.

Αν υπάρχει ένα στοιχείο $e \in V$, τέτοιο ώστε για κάθε $x \in V$ να ισχύει

$$x \cdot e = e \cdot x = x \, ,$$

αυτό είναι μοναδικό και ονομάζεται **μοναδιαίο στοιχείο** της άλγεβρας.

Παραδείγματα

1. Το σύνολο $\mathbf{C}$ των μιγαδικών αριθμών με το συνήθη πολλαπλασιασμό είναι μια άλγεβρα πάνω στο σώμα $\mathbf{R}$ των πραγματικών αριθμών.

2. Ο δακτύλιος P_∞ των πραγματικών πολυωνύμων αποτελεί μια άλγεβρα πάνω στο $\mathbf{R}$.

3. Ο χώρος $M_{n \times n}(K)$ με την πράξη του πολλαπλασιασμού (πινάκων) είναι μια άλγεβρα πάνω στο K. Το μοναδιαίο στοιχείο της άλγεβρας αυτής είναι ο μοναδιαίος $n \times n$ πίνακας I, αφού

$$AI = IA = A \quad \forall A \in M_{n \times n} \, .$$

Επειδή ο πολλαπλασιασμός πινάκων δεν είναι αντιμεταθετικός, η άλγεβρα αυτή δεν είναι αντιμεταθετική.

4. Το σύνολο

$$\mathcal{L}(V) \;=\; \{T : V \longrightarrow V\,, \quad T \text{ γραμμικός } \}$$

των γραμμικών τελεστών πάνω στο γραμμικό K-χώρο V με την πράξη της σύνθεσης είναι μια άλγεβρα πάνω στο K. Η άλγεβρα αυτή δεν είναι αντιμεταθετική. Το μοναδιαίο της στοιχείο είναι ο ταυτοτικός τελεστής.