Ημιομάδα

$(O, \square)$ O σύνολο και $\square : O\times O \to O$ πράξη ώστε η πράξη να είναι προσεταιριστική π.χ $(\mathbb{N}, +)$

Μονοειδές

Όλα τα προηγούμενα με την ιδιότητα $\exists e \in O$ ώστε
$e\square a = a \square e = a$ $\forall a \in O$ e = μοναδιαίο ή ουδέτερο
π.χ. $(\mathbb{N}, +)$

Ομάδα

Όλα τα προηγούμενα με την επιπλέον ιδιότητα $\forall a \in O$ $\exists b \in O$ με
$a\square b = b \square a = e$ (Αντίθετος - Αντίστροφος)
π.χ $(\mathbb{Z}, +)$, $GL(n, \mathbb{R}) = \{A$ nxn πίνακες αντιστρέψιμος$\}$

Η πράξη καλείται αβελιανή αν $a\square b = b\square a$ $\forall a, b \in O$

Ερώτημα 1) Το μοναδιαίο - ουδέτερο είναι μοναδικό?
2) Το b του a είναι μοναδικό?
Ο αντίστροφος - αντίθετος είναι μοναδικός?

ΠΡΟΤΑΣΗ

Έστω $(O, \square)$ ομάδα, τότε το μοναδιαίο-ουδέτερο e είναι μοναδικό

Απόδειξη

Έστω ότι υπάρχουν e και e' με την ιδιότητα $e\square a = a\square e = a\square e' = e'\square a$ $\forall a\in O$. Θ.δ.ο $e=e'$

$$\left.\begin{aligned} e\in O &\Rightarrow e\square e' = e \quad , e' \text{ μοναδιαίο άρα} \\ e'\in O &\Rightarrow e\square e' = e' \quad , e \text{ μοναδιαίο} \end{aligned}\right\} \Rightarrow e=e'$$

ΠΡΟΤΑΣΗ

Έστω $(O,\square)$ ομάδα. Το αντίστροφο-αντίθετο ενός στοιχείου είναι μοναδικό.

Απόδειξη

Έστω $a\in O$ τυχαίο. Υποθέτουμε ότι έχει δυο αντίστροφα

$\exists\, \beta,\gamma \in O$ με $a\square \beta \overset{(++)}{=} \beta\square a = e \overset{(+)}{=} a\square \gamma = \gamma\square a$ Θ.δ.ο $\beta=\gamma$

$$\beta = \beta\square e \overset{(+)}{=} \beta\square(a\square\gamma) \xrightarrow{\text{προσεταιρ.}} (\beta\square a)\square\gamma \overset{(++)}{=} e\square\gamma = \gamma$$

Λύση εξίσωσης $a\square x = \delta$

Ερωτήματα που δημιουργούνται: Τι είναι το a,δ?

Σε ποιο σύνολο θέλω να λυθεί η εξίσ

Παραδείγματα

$3x = 4$ βρες $\beta : \beta\cdot 3 = 1$ τότε

στο $\mathbb{Z}$ ΟΧΙ $\quad \beta(3x) = \beta 4 \Rightarrow (\beta\cdot 3)x = \beta 4$

στο $\mathbb{Q}$ ΝΑΙ $\quad$ Υπάρχει το $\beta\in\mathbb{Z}$

Το 6 είναι πολλαπλασιαστικός αντίστροφος του 3

Αλλά το $(\mathbb{Z}^*, \cdot)$ δεν είναι ομάδα. Άρα δεν έχει κάθε στοιχείο αντίστροφο. Ενώ στο $\mathbb{Q}^*$ έχουμε γιατί είναι ομάδα.

Παράδειγμα

$(\mathbb{Z}, +)$ αβελιανή ομάδα

$(\mathbb{Z}_4, \oplus)$ αβελιανή ομάδα

$(\mathbb{Z}, +)$ άπειρη ομάδα $\longrightarrow$ Κάθε στοιχείο δίνεται από άθροισμα του 1 ή -1 με τον εαυτό του

γεννήτορας

$(\mathbb{Q}, +)$ άπειρη αβελιανή ομάδα $\quad \mathbb{Z} \subseteq \mathbb{Q}$

1 δεν δίνει ποτέ $\frac{1}{2}$

Ας υποθέσουμε ότι το ανάγωγο κλάσμα $\frac{r}{q}$ $\left((r,q)=1 \text{ πρώτοι μεταξύ τους}\right)$

μας δίνει κάθε ρητό $\quad \kappa \frac{r}{q} = \frac{15}{4}$

αν $r > q \Rightarrow \frac{r}{q} > 1 \Rightarrow \kappa \frac{r}{q} > 1$ (Πως θα πάρουμε το $\frac{1}{2}$;)

Θα πρέπει $r < q$

Θέλω $\kappa \in \mathbb{Z}$ τ.ω $\kappa \frac{r}{q} = \frac{q-r}{q} \Rightarrow \kappa r = q - r \Rightarrow \kappa r + r = q \Rightarrow$

$\Rightarrow (\kappa+1) r = q \Rightarrow r / q$ άτοπο αφού $(r,q)=1$

Το στοιχείο 1 στο $(\mathbb{Z},+)$ δημιουργεί - παράγει - γεννά κάθε στοιχείο και καλείται γεννήτορας

Στο $(\mathbb{Q},+)$ δεν υπάρχει τέτοιο στοιχείο

$(\mathbb{Z}_5, \oplus)$ Το $[1]$ με τον εαυτό του μας δίνει κάθε στοιχείο

$(\mathbb{Z}_4, \oplus)$ το $[1]$ είναι γεννήτορας ενώ το $[2]$ όχι

$(\mathbb{Z}_5^*, \odot) = \{[1], [2], [3], [4]\}$

$4 = \varphi(5) = ord_5(a)$ $\quad a$ πρωταρχική ρίζα

$2 \,,\ 2^2 = 4 \,,\ 2^3 = 8 \equiv 3 \quad 2^4 = 3 \cdot 2 = 1$

Το $[2]$ είναι γεννήτορας της ομάδας $(\mathbb{Z}_5^*, \odot)$

$(\mathbb{Z}_4^*, \odot) = \{[1], [2], [3]\}$ Δεν είναι καν ομάδα αφού το 2 δεν έχει αντίστροφο

ΟΡΙΣΜΟΣ

Τάξη μιας ομάδας O θα είναι το πλήθος των στοιχείων του συνόλου O. Συμβολισμός $|O|$

a) $|O| < \infty$ πεπερασμένη ομάδα

$(\mathbb{Z}_4, \oplus)$, $(\mathbb{Z}_7, \oplus)$, $(\mathbb{Z}_7^*, \oplus)$

b) $|O| = \infty$ άπειρη ομάδα

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, σύνολο των συνεχών συναρτήσεων

ΟΡΙΣΜΟΣ

Τάξη ενός στοιχείου μιας ομάδας G είναι ο μικρότερος φυσικός n ώστε $a^n = 1 = e$ μοναδιαίο.
Αν δεν υπάρχει τέτοιο n, τότε λέμε ότι το a έχει άπειρη τάξη.
Συμβολισμός $o(a) \begin{cases} n \\ \infty \end{cases}$

Παράδειγμα

$(\mathbb{Z}, +)$ $o(1) = \infty$

$o(2) = \infty$

$o(-3) = \infty$

$(\mathbb{Z}_5, \oplus)$ $o([1]) = 5$

$o([3]) = 5$ επειδή $(3,5) = 1$ το 3 έχει ότι και το 1

$(\mathbb{Z}_4, \oplus)$ $o([1]) = 4$

$o([2]) = 2$

ΟΡΙΣΜΟΣ

Μια ομάδα $(G, \cdot)$ θα καλείται κυκλική αν υπάρχει στοιχείο $a \in G$ ώστε κάθε άλλο στοιχείο $b \in G$ να δίνεται από δύναμη του a : $\exists k \in \mathbb{Z}$ με $a^k = b$. Συμβολισμός $G = \langle a \rangle$

γεννήτορας

Παράδειγμα

$\mathbb{Z} = \langle 1 \rangle$

$\mathbb{Z}_4 = \langle [1] \rangle$

$\mathbb{Z}_5^* = \langle [2] \rangle$

$\mathbb{Q}$ όχι κυκλική

$\underline{(M(2\times 2, \mathbb{R}), +)}$ ← αβελιανή ομάδα $\qquad |M(2\times 2, \mathbb{R})| = \infty$

Το σύνολο αυτό είναι $\mathbb{R}^4$, το $\mathbb{R}$ είναι υπεραριθμήσιμο άρα όχι κυκλική

$GL(2, \mathbb{R})$ ← ομάδα όχι αβελιανή $\qquad |GL(2, \mathbb{R})| = \infty$

$o\left(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right) = 2$ αφού

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$o\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = \infty$ αφού

αποδεικνύεται με επαγωγή

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \ldots \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^K = \begin{pmatrix} 1 & K \\ 0 & 1 \end{pmatrix}$$

Ιδιότητες σε μια ομάδα $(G,\odot)$

1) Αβελιανή ανν $ab=ba \quad \forall a,b\in G$

2) $(a^{-1})^{-1}=a$ αφού $\left.\begin{aligned}(a^{-1})^{-1}\cdot a^{-1}&=1\\ a\cdot a^{-1}&=1\end{aligned}\right\}\xrightarrow[\text{μοναδικότητας}]{\text{λόγω}}(a^{-1})^{-1}=a$

3) $(a\cdot b)^{-1}=b^{-1}a^{-1}$

Θα πρέπει $\left.\begin{aligned}&(a\cdot b)(ab)^{-1}=1\\ &(a\cdot b)(b^{-1}a^{-1})=1=a\cdot a^{-1}=1\end{aligned}\right\}\xrightarrow[\text{μοναδικότητας}]{\text{λόγω}}(a\cdot b)^{-1}=b^{-1}a^{-1}$

$(ab)^{-1}=a^{-1}\cdot b^{-1} \iff G$ αβελιανή