Ομάδες και δακτύλιοι

Θεμέλια Άλγεβρας και Γεωμετρίας

Ένα παράδειγμα

Μια νέα πράξη στο $\mathbb{R}$

Ορίζουμε την πράξη

$$* : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}, \qquad (x, y) \longmapsto x * y = x + y - xy.$$

Για παράδειγμα:

$$2 * 3 = 2 + 3 - 6 = -1, \qquad 0 * 5 = 5, \qquad 1 * 7 = 1 + 7 - 7 = 1.$$

Ερώτηση: ποιες από τις ιδιότητες που ξέρουμε έχει αυτή η πράξη;

- προσεταιριστικότητα;
- μεταθετικότητα;
- ουδέτερο στοιχείο;
- ποια στοιχεία είναι αντιστρέψιμα;

Η $*$ είναι προσεταιριστική

$$\begin{aligned}(x * y) * z &= (x + y - xy) * z \\ &= (x + y - xy) + z - (x + y - xy)z \\ &= x + y + z - xy - xz - yz + xyz\end{aligned}$$

$$\begin{aligned}x * (y * z) &= x * (y + z - yz) \\ &= x + (y + z - yz) - x(y + z - yz) \\ &= x + y + z - xy - xz - yz + xyz\end{aligned}$$

Τα δύο αποτελέσματα είναι ίδια, άρα $(x * y) * z = x * (y * z)$ για κάθε $x, y, z \in \mathbb{R}$.

Μεταθετικότητα και ουδέτερο στοιχείο

Μεταθετική:

$$x * y = x + y - xy = y + x - yx = y * x.$$

Ουδέτερο στοιχείο: ψάχνουμε y με $x * y = x$ για *κάθε* $x \in \mathbb{R}$.

$$x + y - xy = x \iff y - xy = 0 \iff y(1 - x) = 0.$$

Για να ισχύει αυτό για κάθε $x \in \mathbb{R}$, πρέπει $y = 0$. Πράγματι,

$$x * 0 = x + 0 - 0 = x = 0 * x.$$

Άρα το 0 είναι το ουδέτερο στοιχείο της $*$.

Αντιστρέψιμα στοιχεία

Για δοσμένο x ψάχνουμε y με $x * y = 0$:

$$x + y - xy = 0 \iff y(x-1) = x.$$

- Αν $x \neq 1$: $\quad y = \dfrac{x}{x-1}$. Έλεγχος:

$$x * \frac{x}{x-1} = x + \frac{x}{x-1} - \frac{x^2}{x-1} = x + \frac{x(1-x)}{x-1} = x - x = 0.$$

- Αν $x = 1$: $\quad 1 * y = 1 + y - y = 1 \neq 0$ για κάθε $y \in \mathbb{R}$.
  Άρα το 1 δεν είναι αντιστρέψιμο.

Συμπέρασμα: τα αντιστρέψιμα στοιχεία είναι ακριβώς τα στοιχεία του $\mathbb{R} \setminus \{1\}$.

Ομάδες

Ορισμός ομάδας

Ορισμός

Ομάδα είναι ένα σύνολο G εφοδιασμένο με μια πράξη $* : G \times G \to G$ με τις ιδιότητες:

1. η $*$ είναι προσεταιριστική·
2. υπάρχει ουδέτερο στοιχείο (συμβ. e ή 1_G ή 1)·
3. κάθε στοιχείο είναι αντιστρέψιμο: για κάθε $g \in G$ υπάρχει $g^{-1} \in G$ με $g * g^{-1} = g^{-1} * g = e$.

- Από το (3) προκύπτει ότι $(g^{-1})^{-1} = g$.
- Αν επιπλέον η $*$ είναι μεταθετική, η G λέγεται *αβελιανή* (ή *μεταθετική*) ομάδα.
- Γράφουμε $(G, *)$ για την ομάδα G με πράξη $*$.

Πίσω στο παράδειγμα: είναι η $(\mathbb{R} \setminus \{1\}, *)$ ομάδα;

Ελέγχουμε όλα τα σημεία του ορισμού για το σύνολο $G = \mathbb{R} \setminus \{1\}$:

0. **Η $*$ είναι πράξη στο G:** αν $x, y \neq 1$, τότε $x * y \neq 1$, γιατί

$$1 - x * y = 1 - x - y + xy = (1 - x)(1 - y) \neq 0.$$

1. **Προσεταιριστική:** ισχύει σε όλο το $\mathbb{R}$, άρα και στο G.
2. **Ουδέτερο:** το 0 ανήκει στο G, αφού $0 \neq 1$.
3. **Αντίστροφα:** για $x \in G$, το $\dfrac{x}{x-1}$ ανήκει κι αυτό στο G, γιατί $\dfrac{x}{x-1} = 1 \iff x = x - 1$, αδύνατο.

Άρα η $(\mathbb{R} \setminus \{1\}, *)$ είναι αβελιανή ομάδα.

Παραδείγματα ομάδων

- $\{1_G\}$: η *τετριμμένη ομάδα*, με $1_G * 1_G = 1_G$.
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.
- $(n\mathbb{Z}, +)$, όπου $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$, και $(\mathbb{R}^n, +)$ με πρόσθεση κατά συντεταγμένες.
- $(\mathbb{K}[x], +)$: πολυώνυμα με συντελεστές στο σώμα $\mathbb{K}$.
- $(\{-1, 1\}, \cdot)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, όπου $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ κτλ.
- $(\mathbb{R}_{>0}, \cdot)$: οι θετικοί πραγματικοί με τον πολλαπλασιασμό.
- $(\{f : A \to A \mid f \text{ 1-1 και επί}\}, \circ)$: οι *μεταθέσεις* του συνόλου A.
- $(\mathbb{R} \setminus \{1\}, *)$ με $x * y = x + y - xy$.

Παρατήρηση. Όταν λέμε «η ομάδα $\mathbb{Z}$» εννοούμε την $(\mathbb{Z}, +)$, και «η ομάδα $\mathbb{R}^*$» την $(\mathbb{R}^*, \cdot)$.

Υποομάδες

Ορισμός

Έστω $(G, *)$ ομάδα. *Υποομάδα* της G είναι ένα υποσύνολο $H \subseteq G$ τέτοιο ώστε η $(H, *)$ να είναι ομάδα. Γράφουμε $H \leq G$.

Παραδείγματα (με πράξη την πρόσθεση):

$$\mathbb{Z} \leq \mathbb{Q}, \qquad \{0\} \leq \mathbb{Z}, \qquad \{1, -1\} \not\leq \mathbb{Z}.$$

Πότε ένα υποσύνολο είναι υποομάδα;

Έστω $(G, *)$ ομάδα και $\emptyset \neq H \subseteq G$. Η $(H, *)$ είναι ομάδα αν και μόνο αν:

1. η $*$ είναι πράξη στο H: για κάθε $h_1, h_2 \in H$ έχουμε $h_1 * h_2 \in H$.
2. η $*$ είναι προσεταιριστική στο H (ισχύει πάντα, γιατί η G είναι ομάδα).
3. $1_G \in H$.
4. για κάθε $h \in H$ ισχύει $h^{-1} \in H$.

Παραδείγματα: κάθε συνθήκη χρειάζεται

- $\{1, -1\} \not\leq (\mathbb{Z}, +)$, γιατί $0 \notin \{1, -1\}$: αποτυγχάνει το (3).
- $\{-1, 0, 1\} \not\leq (\mathbb{Z}, +)$: περιέχει το 0 και τα αντίθετα όλων των στοιχείων του, αλλά $1 + 1 = 2 \notin \{-1, 0, 1\}$: αποτυγχάνει το (1).
- $\{2^n \mid n \in \mathbb{N}\} \not\leq (\mathbb{Q}^*, \cdot)$: είναι κλειστό ως προς τον πολλαπλασιασμό και περιέχει το $1 = 2^0$, αλλά $2^{-1} = \frac{1}{2}$ δεν ανήκει στο σύνολο: αποτυγχάνει το (4).
- Αντίθετα, $\{2^n \mid n \in \mathbb{Z}\} \leq (\mathbb{Q}^*, \cdot)$ και $2\mathbb{Z} \leq (\mathbb{Z}, +)$.

Κριτήριο υποομάδας

Λήμμα

Έστω $(G, *)$ ομάδα και $\emptyset \neq H \subseteq G$. Τότε

$$H \leq G \iff h_1 * h_2^{-1} \in H \text{ για κάθε } h_1, h_2 \in H.$$

Απόδειξη. Η κατεύθυνση «⇒» είναι προφανής. Για την «⇐»:

- Έστω $h \in H$. Τότε $h * h^{-1} = 1_G \in H$: ισχύει το (3).
- Αφού $1_G \in H$, έχουμε $1_G * h^{-1} = h^{-1} \in H$: ισχύει το (4).
- Έστω $h_1, h_2 \in H$. Από το (4), $h_2^{-1} \in H$, άρα

$$h_1 * (h_2^{-1})^{-1} = h_1 * h_2 \in H : \text{ ισχύει το (1).}$$

Το (2) ισχύει πάντα. □

Άσκηση: ευθύ γινόμενο ομάδων

Άσκηση

Αν $(G_1, *)$ και $(G_2, \circ)$ είναι ομάδες, τότε το σύνολο $G = G_1 \times G_2$ με πράξη

$$\big((a, b), (c, d)\big) \longmapsto (a * c,\ \ b \circ d)$$

είναι ομάδα, με ουδέτερο στοιχείο το $(1_{G_1}, 1_{G_2})$.

Η ομάδα G με αυτή την πράξη λέγεται *ευθύ γινόμενο* των ομάδων G_1 και G_2.

Δακτύλιοι

Ορισμός δακτυλίου

Ορισμός

Δακτύλιος είναι ένα σύνολο R εφοδιασμένο με δύο πράξεις

$$+ : R \times R \to R \qquad \text{και} \qquad \cdot : R \times R \to R$$

που ικανοποιούν τις συνθήκες:

- η $(R, +)$ είναι αβελιανή ομάδα, με ουδέτερο στοιχείο 0_R·
- ο πολλαπλασιασμός είναι προσεταιριστικός·
- ισχύει η *επιμεριστική ιδιότητα* για κάθε $a, b, c \in R$:

$$(a + b) \cdot c = a \cdot c + b \cdot c, \qquad a \cdot (b + c) = a \cdot b + a \cdot c.$$

Ειδικοί τύποι δακτυλίων

Έστω $(R, +, \cdot)$ ένας δακτύλιος.

Ορισμοί

- Αν ο πολλαπλασιασμός έχει ουδέτερο στοιχείο, λέμε ότι ο R είναι *δακτύλιος με μονάδα*. Η μονάδα συμβολίζεται 1_R.
- Αν ο πολλαπλασιασμός είναι μεταθετικός, λέμε ότι ο R είναι *μεταθετικός δακτύλιος*.
- Αν ο R έχει μονάδα και κάθε στοιχείο του $R \setminus \{0_R\}$ είναι αντιστρέψιμο ως προς τον πολλαπλασιασμό, λέμε ότι ο R είναι *δακτύλιος με διαίρεση*.
- Αν ισχύουν όλα τα παραπάνω και $0_R \neq 1_R$, δηλαδή αν η $(R^*, \cdot)$, όπου $R^* = R \setminus \{0_R\}$, είναι αβελιανή ομάδα, λέμε ότι ο R είναι *σώμα*.

Δηλαδή: σώμα = μεταθετικός δακτύλιος με διαίρεση, με $0_R \neq 1_R$.

Παραδείγματα

Δακτύλιοι:

- $\{0\}$: ο *μηδενικός δακτύλιος*.
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
- $2\mathbb{Z}$: δακτύλιος *χωρίς* μονάδα ($1 \notin 2\mathbb{Z}$).
- οι συναρτήσεις $\mathbb{R} \to \mathbb{R}$, με πρόσθεση και πολλαπλασιασμό σημείο προς σημείο.
- $\mathbb{K}[x]$, και γενικότερα $R[x]$ όπου R δακτύλιος.

Δεν είναι δακτύλιοι:

- $\mathbb{N}$: η $(\mathbb{N}, +)$ δεν είναι ομάδα (δεν υπάρχουν αντίθετα).
- $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$: η πρόσθεση δεν είναι πράξη σε αυτό, αφού $1 + (-1) = 0 \notin \mathbb{R}^*$.
- Οι περιττοί ακέραιοι: $1 + 1 = 2$ δεν είναι περιττός.

Παραδείγματα: τι είδους δακτύλιος;

- $\mathbb{Z}$: μεταθετικός δακτύλιος με μονάδα, όχι με διαίρεση (2 δεν είναι αντιστρέψιμο στο $\mathbb{Z}$).
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$: σώματα.
- $\mathbb{K}[x]$: μεταθετικός δακτύλιος με μονάδα, όχι με διαίρεση (x δεν είναι αντιστρέψιμο).
- $2\mathbb{Z}$: μεταθετικός δακτύλιος *χωρίς* μονάδα.
- Συναρτήσεις $\mathbb{R} \to \mathbb{R}$: μεταθετικός δακτύλιος με μονάδα (τη σταθερή συνάρτηση 1), όχι με διαίρεση (η $f(x) = x$ δεν έχει αντίστροφη ως προς τον πολλαπλασιασμό, αφού $f(0) = 0$).

Παρατήρηση. Στον μηδενικό δακτύλιο $\{0\}$ ισχύει $0 = 1$. Γι' αυτό στον ορισμό του σώματος ζητάμε $0_R \neq 1_R$.

Ένας μη μεταθετικός δακτύλιος με διαίρεση: τα τετραδόνια

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\},$$

με πρόσθεση κατά συντεταγμένες και πολλαπλασιασμό που ορίζεται από τους κανόνες

$$i^2 = j^2 = k^2 = -1, \qquad ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik.$$

- Ο $\mathbb{H}$ είναι δακτύλιος με διαίρεση: κάθε $q = a + bi + cj + dk \neq 0$ έχει αντίστροφο

$$q^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}.$$

- Δεν είναι μεταθετικός, αφού $ij = k \neq -k = ji$. Άρα δεν είναι σώμα.

Γινόμενο δακτυλίων

Αν R_1, R_2 είναι δακτύλιοι, τότε το $R_1 \times R_2$ είναι δακτύλιος με

$$(a, b) + (c, d) = (a +_{R_1} c,\ b +_{R_2} d), \qquad (a, b) \cdot (c, d) = (a \cdot_{R_1} c,\ b \cdot_{R_2} d).$$

- $0_{R_1 \times R_2} = (0_{R_1}, 0_{R_2})$.
- Αν οι R_1, R_2 είναι μεταθετικοί, τότε και ο $R_1 \times R_2$ είναι μεταθετικός.
- Αν οι R_1, R_2 έχουν μονάδα, τότε $1_{R_1 \times R_2} = (1_{R_1}, 1_{R_2})$.

Ο $R_1 \times R_2$ δεν είναι σώμα: αν (a, b) ήταν αντίστροφος του $(0, 1)$, τότε

$$(a, b) \cdot (0, 1) = (1, 1) \ \Rightarrow\ a \cdot 0 = 1, \quad \text{αδύνατο}.$$

Λήμμα

Έστω R δακτύλιος. Για κάθε $a \in R$ ισχύει $a \cdot 0_R = 0_R \cdot a = 0_R$.

Απόδειξη.

$$\begin{aligned} a \cdot 0_R = a \cdot (0_R + 0_R) = a \cdot 0_R + a \cdot 0_R \;&\Rightarrow\; a \cdot 0_R + 0_R = a \cdot 0_R + a \cdot 0_R \\ &\Rightarrow\; 0_R = a \cdot 0_R, \end{aligned}$$

προσθέτοντας το αντίθετο του $a \cdot 0_R$ και στα δύο μέλη. Όμοια $0_R \cdot a = 0_R$. □

Υποδακτύλιοι

Ορισμός

Ένα μη κενό υποσύνολο S ενός δακτυλίου R λέγεται *υποδακτύλιος* αν είναι δακτύλιος ως προς τις ίδιες πράξεις και με τα ίδια ουδέτερα στοιχεία με τον R.

Δηλαδή $0_R \in S$ και, αν ο R έχει μονάδα, $1_R \in S$.

Παράδειγμα. Το $\mathbb{Z}$ είναι υποδακτύλιος του $\mathbb{Q}$.

Κριτήριο υποδακτυλίου

Λήμμα

Έστω R δακτύλιος με μονάδα και $\emptyset \neq S \subseteq R$. Το S είναι υποδακτύλιος του R αν και μόνο αν:

1. $a - b \in S$ για κάθε $a, b \in S$.
2. $a \cdot b \in S$ για κάθε $a, b \in S$.
3. $1_R \in S$.

Απόδειξη («$\Leftarrow$»).

- Από το (1) και το κριτήριο υποομάδας, η $(S, +)$ είναι υποομάδα της $(R, +)$, άρα $0_R \in S$. είναι αβελιανή, αφού η $+$ είναι μεταθετική στο R.
- Από το (2), ο πολλαπλασιασμός είναι πράξη στο S. η προσεταιριστικότητα και η επιμεριστικότητα ισχύουν στο R, άρα και στο S.
- Από το (3), το S έχει την ίδια μονάδα με τον R. □

Παραδείγματα υποδακτυλίων

- $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$: κάθε ένας είναι υποδακτύλιος του επόμενου.
- $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ είναι υποδακτύλιος του $\mathbb{R}$:

$$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2},$$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2},$$

  και $1 = 1 + 0\sqrt{2}$.
- Τα σταθερά πολυώνυμα σχηματίζουν υποδακτύλιο του $\mathbb{R}[x]$, που «είναι» το $\mathbb{R}$.

Μη παραδείγματα: κάθε συνθήκη χρειάζεται

- $\mathbb{N} \subseteq \mathbb{Z}$: $1 - 2 = -1 \notin \mathbb{N}$, αποτυγχάνει το (1).
- Τα πολυώνυμα βαθμού ≤ 1 στο $\mathbb{R}[x]$: είναι κλειστά ως προς την αφαίρεση και περιέχουν το 1, αλλά $x \cdot x = x^2$: αποτυγχάνει το (2).
- $2\mathbb{Z} \subseteq \mathbb{Z}$: είναι κλειστό ως προς αφαίρεση και πολλαπλασιασμό (και είναι δακτύλιος), αλλά $1 \notin 2\mathbb{Z}$: αποτυγχάνει το (3).
- $\mathbb{R} \times \{0\} \subseteq \mathbb{R} \times \mathbb{R}$: είναι δακτύλιος με μονάδα το $(1, 0)$, αλλά η μονάδα του $\mathbb{R} \times \mathbb{R}$ είναι το $(1, 1) \notin \mathbb{R} \times \{0\}$. Άρα δεν είναι υποδακτύλιος.

Ερώτηση 1 / 13

Η απεικόνιση f: Z→Z με f(n)=2n είναι:

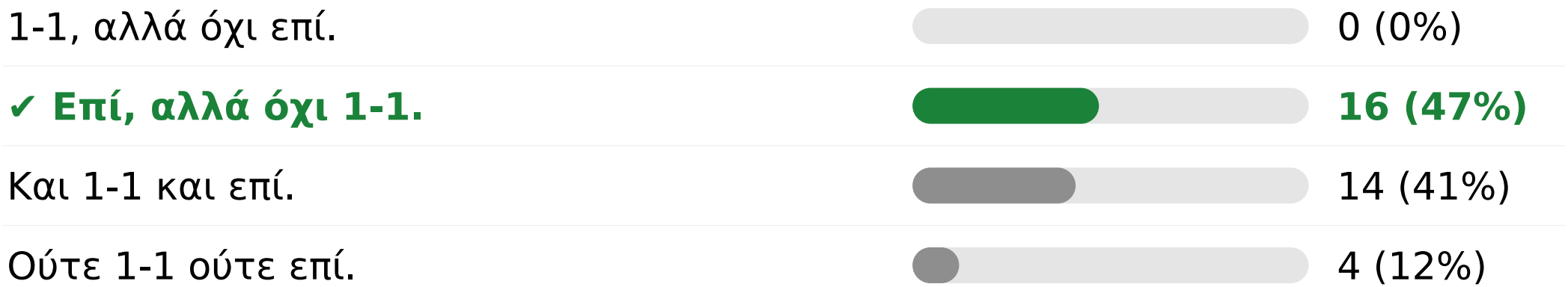
35 συμμετέχοντες

✔ 1-1, αλλά όχι επί.		**14 (40%)**
Επί, αλλά όχι 1-1.		0 (0%)
Και 1-1 και επί.		20 (57%)
Ούτε 1-1 ούτε επί.		1 (3%)

Ερώτηση 2 / 13

Έστω N={0,1,2,...} και f: N→N με f(0)=0 και f(n)=n−1 για n≥1. Η f είναι:

34 συμμετέχοντες



Ερώτηση 3 / 13

Έστω f: A→B και g: B→C. Αν η σύνθεση g∘f είναι 1-1, τι μπορούμε να συμπεράνουμε σίγουρα;

35 συμμετέχοντες

✔ Η f είναι 1-1.		**16 (46%)**
Η g είναι 1-1.		4 (11%)
Και οι δύο είναι 1-1.		5 (14%)
Τίποτα από τα παραπάνω.		10 (29%)

Ερώτηση 4 / 13

Ποια από τις παρακάτω απεικονίσεις R→R είναι αντιστρέψιμη;

31 συμμετέχοντες

$f(x)=x^2$	4 (13%)
$f(x)=\|x\|$	1 (3%)
$f(x)=e^x$	10 (32%)
✔ $f(x)=x^3$	**16 (52%)**

Ερώτηση 5 / 13

Έστω f: R→R με f(x)=x². Ποια είναι η εικόνα f([−2,1]) του διαστήματος [−2,1];

33 συμμετέχοντες

[1,4]		16 (48%)
✔ [0,4]		16 (48%)
[0,1]		1 (3%)
[−2,1]		0 (0%)

Ερώτηση 6 / 13

Έστω f: R→R με f(x)=x². Ποια είναι η αντίστροφη εικόνα f⁻¹([1,4]) του διαστήματος [1,4];

33 συμμετέχοντες

[1,2]		7 (21%)
✔ [−2,−1]υ[1,2]		**21 (64%)**
[1,16]		1 (3%)
[−2,2]		4 (12%)

Ερώτηση 7 / 13

Έστω f: A→B και Γ ένα υποσύνολο του B. Ποιο από τα παρακάτω ισχύει ΠΑΝΤΑ;

34 συμμετέχοντες

$f(f^{-1}(\Gamma))=\Gamma$		6 (18%)
✔ $f(f^{-1}(\Gamma))\subseteq\Gamma$		**20 (59%)**
$\Gamma\subseteq f(f^{-1}(\Gamma))$		4 (12%)
Κανένα από τα παραπάνω δεν ισχύει πάντα.		4 (12%)

Ερώτηση 8 / 13

Έστω N={0,1,2,...}. Ποια από τις παρακάτω είναι εσωτερική πράξη στο N;

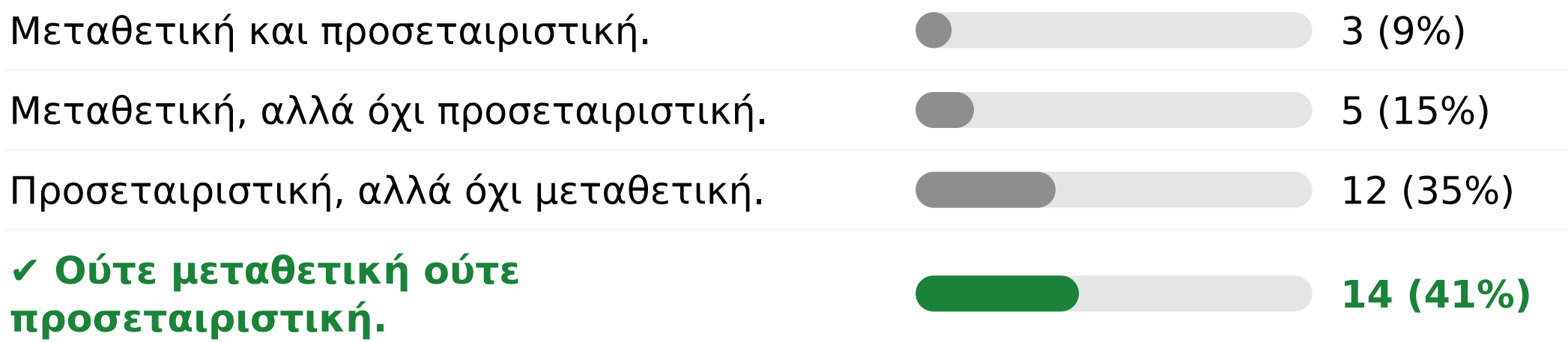
34 συμμετέχοντες

a*b=a−b		1 (3%)
a*b=a/b		3 (9%)
✔ a*b=a+2b	**correct**	**20 (59%)**
a*b=√(ab)		10 (29%)

Ερώτηση 9 / 13

Η πράξη a*b=a−b στο Z είναι:

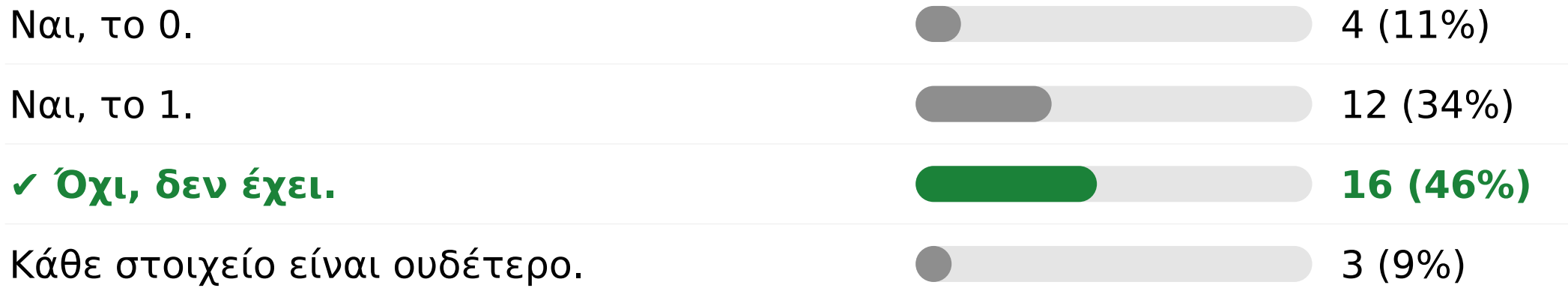
34 συμμετέχοντες



Ερώτηση 10 / 13

Έστω N={0,1,2,...}. Η πράξη a*b=min(a,b) στο N έχει ουδέτερο στοιχείο;

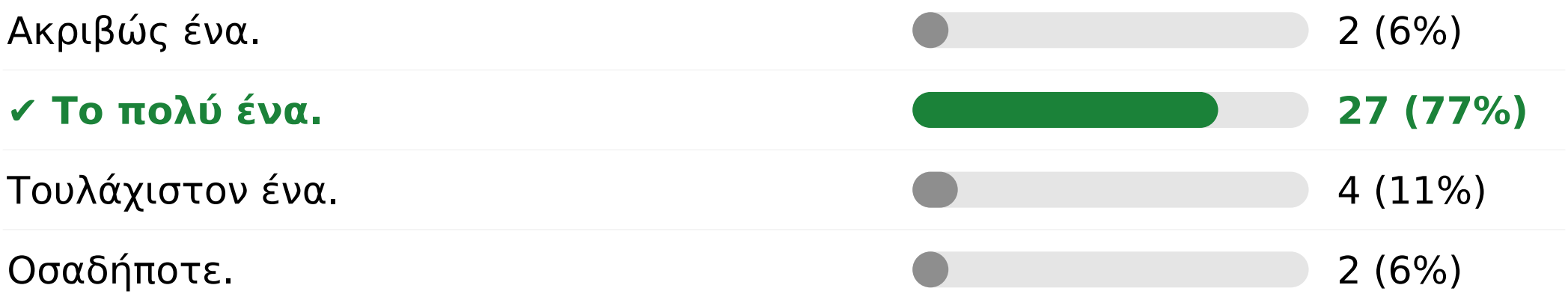
35 συμμετέχοντες



Ερώτηση 11 / 13

Πόσα ουδέτερα στοιχεία μπορεί να έχει μια εσωτερική πράξη;

35 συμμετέχοντες



Ερώτηση 12 / 13

Στο Z ορίζουμε την πράξη a*b=a+b+ab. Ποιο είναι το ουδέτερο στοιχείο της;

34 συμμετέχοντες

✔ **Το 0.**	**17 (50%)**
Το 1.	2 (6%)
Το −1.	5 (15%)
Δεν υπάρχει.	10 (29%)

Ερώτηση 13 / 13

Στο Z ορίζουμε την πράξη a*b=a+b+ab, με ουδέτερο στοιχείο το 0. Ποια στοιχεία του Z είναι αντιστρέψιμα;

34 συμμετέχοντες

