24/02/2020

Έστω $S \neq \emptyset$ σύνολο. Μας φτιάχνει αν η $*$ είναι (καλά ορισμένη) πράξη στο S. Ή πρέπει να επιβεβαιώσουμε:

1) Αν υπάρχουν παρανοήσεις και μηδενίζονται

Παράδειγμα:

Αν $S = \mathbb{R} \setminus \{0\}$ η έκφραση: $a * b = \frac{a}{b}$, για $a, b \in S$ ορίζει (καλά ορισμένη) πράξη στο S

Αν $S = \mathbb{R}$ ΔΕΝ ΟΡΙΖΕΙ

2) Αν ισχύει $a * b \in S$ $a, b \in S$

Παράδειγμα:

Αν το $S = [0, 2020] \subseteq \mathbb{R}$ η έκφραση:

"$a * b = a + b$ για $a, b \in S$"

ΔΕΝ ορίζει πράξη στο S, γιατί $a = b = 2020$, $a * b \notin S$

Έστω το $S = \{x \in \mathbb{R} : x > 0\}$, η έκφραση:

"$a * b = a + b$ για $a, b \in S$"

ορίζει πράξη στο S, γιατί $a > 0$ και $b > 0$ συνεπάγεται $a + b > 0$.

3) Επιβεβαιώνουμε τυχόν εξάρτηση από αντιπροσώπους

Παράδειγμα:

Έστω $S = \mathbb{Z}_5$ = ακέραιοι modulo 5

Ορίζει η έκφραση:

"$[a]_5 + [b]_5 = [a+b]_5$, για $a, b \in \mathbb{Z}$" πράξη στο $\mathbb{Z}_5$;

ΝΑΙ, γιατί από Πρόταση από θ. Αριθμών αν $a, b, a', b \in \mathbb{Z}$ και $[a]_5 = [a']_5$ και $[b]_5 = [b']_5$ τότε

$$[a+b]_5 = [a'+b']_5$$

Παράδειγμα:

Ορίζει η έκφραση: "$g: \mathbb{Z}_2 \to \mathbb{Z}_6$, $g([a]_2) = [a]_6$, για $a \in \mathbb{Z}$" (καλά ορισμένη) συνάρτηση από το $\mathbb{Z}_2 \to \mathbb{Z}_6$;

ΟΧΙ, γιατί για $a = 2$, $a' = 4$ έχουμε $[a]_2 = [a']_2 = [0]_2$ ενώ $[a]_6 \neq [a']_6$.

Παράδειγμα

Ορίζει η έκφραση: "$h: \mathbb{Z}_6 \to \mathbb{Z}_2$, $h([a]_6) = [a]_2$, για $a \in \mathbb{Z}$"
(καλά ορισμένη) συνάρτηση από το $\mathbb{Z}_6$ στο $\mathbb{Z}_2$;
ΝΑΙ, γιατί αν $a, a' \in \mathbb{Z}$ με $[a]_6 = [a']_6$ έχουμε $6 | (a'-a)$
άρα $2 | (a'-a)$ συνεπώς $[a']_2 = [a]_2$

Παράδειγμα

Ορίζει η έκφραση: "$g: \mathbb{Z}_2 \to \mathbb{Z}_6$, $g([a]_2) = [3a]_6$ για $a \in \mathbb{Z}$"
(καλά ορισμένη) συνάρτηση από το $\mathbb{Z}_2$ στο $\mathbb{Z}_6$;
ΝΑΙ, γιατί αν $a, a' \in \mathbb{Z}$ με $[a]_2 = [a']_2$ έχουμε $2 | (a'-a)$
συνεπώς $3 \cdot 2 | 3(a'-a)$ άρα $6 | (3a'-3a)$.
Συνεπώς $[3a']_6 = [3a]_6$

Άσκηση

Έστω $n, m \geq 2$ ακέραιοι. Δείξτε ότι η έκφραση:
"$f: \mathbb{Z}_n \to \mathbb{Z}_m$, $f([a]_n) = [a]_m$ για $a \in \mathbb{Z}$" ορίζει
(καλά ορισμένη) συνάρτηση από το $\mathbb{Z}_n$ στο $\mathbb{Z}_m$ αν-ν
το m διαιρεί το n.

Φυλλάδιο

Άσκηση 1: Έστω $S = \mathbb{R} - \{0\}$ (καλά ορισμένη).

1) Ν.Σ.Ο. η έκφραση: "$* : S \times S \to S$, $a * b = a \cdot |b|$ ορίζει πράξη στο S.
2) Δείξτε ότι $*$ είναι προσεταιριστική
3) Δείξτε ότι $\exists e \in S$ τ.ω. $a * e = a$, για κάθε $a \in S$
4) Έχει το S ουδέτερο στοιχείο;
5) Είναι το S ομάδα;

Λύση

1) Έστω $a, b \in S$. Αφού $a \neq 0$ και $b \neq 0$ έπεται ότι $a \cdot |b| \neq 0$. Άρα $a \cdot |b| \in S$.
Συνεπώς η πράξη $*$ είναι καλά ορισμένη στο S.
2) Έστω $a, b, c \in S$. Τότε $(a*b)*c = (a \cdot |b|) * c = (a \cdot |b|) \cdot |c| = a \cdot |b| \cdot |c|$
ενώ $a*(b*c) = a*(b \cdot |c|) = a \cdot |b \cdot |c|| = a \cdot |b| \cdot |c|$
Συνεπώς $(a*b)*c = a*(b*c)$

3) Θέλουμε $e=1$. Τότε, φανερά αν $e = a \cdot 1 = a$, $\forall a \in S$.
Παρατηρούμε ότι και για $e'=-1$ έχουμε $a * e' = 0$, $\forall a \in S$.
4) Όχι, το S δεν έχει ουδέτερο στοιχείο, γιατί έστω ότι το $e' \in S$ είναι ουδέτερο. Τότε:
$1 = e' * 1 = e' = e' * (-1) = -1$ (e' ουδέτερο)
αντίφαση γιατί στο $\mathbb{R}$, $1 \neq -1$.
Συνεπώς $(S, *)$ όχι ομάδα.

ΤΕΧΝΙΚΕΣ ΙΔΙΟΤΗΤΕΣ ΟΜΑΔΩΝ

Παρατήρηση: Έστω $(G, *)$ ένα δομή η πράξη είναι προεταιριστική δεν χρειάζονται παρενθέσεις.

Πρόταση: (Κανόνας διαγραφής). Έστω $(G, *)$ ομάδα και $a, b, c \in G$.
1) Αν $a*b = a*c$ τότε $b=c$
2) Αν $b*a = c*a$ τότε $b=c$
Απόδειξη:
1) $a*b = a*c \Rightarrow a^{-1} * (a*b) = a^{-1} * (a*c)$
$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c$
$\Rightarrow e_G * b = e_G * c \Rightarrow b = c$
όπου e_G το ουδέτερο στοιχείο της G και a^{-1} ο αντίστροφος του a στην G.
2) $b*a = c*a \Rightarrow (b*a) * a^{-1} = (c*a) * a^{-1}$
$\Rightarrow b * (a * a^{-1}) = c * (a * a^{-1}) \Rightarrow b * e_G = c * e_G \Rightarrow b = c$

Πρόταση: Έστω G ομάδα και $a, b \in G$
1) Η εξίσωση (για $x \in G$): $a * x = b$
έχει μοναδική λύση στο G το $x = a^{-1} * b$.

2) Η εξίσωση (για $x \in G$) $x * a = b$ έχει μοναδική λύση στο G το $x = b * a^{-1}$.

3) Έστω $a, b, c \in G$. Η εξίσωση (για $x \in G$)

$$a * x * b = c$$

έχει μοναδική λύση $x = a^{-1} * c * b^{-1}$

Απόδειξη

1) ΜΟΝΑΔΙΚΟΤΗΤΑ: Έστω $x \in G$ λύση. Τότε

$$a * x = b \Rightarrow a^{-1} * (a * x) = a^{-1} * b$$
$$\Rightarrow (a^{-1} * a) * x = a^{-1} * b \Rightarrow$$
$$\Rightarrow e_G * x = a^{-1} * b \Rightarrow x = a^{-1} * b$$

ΥΠΑΡΞΗ ΛΥΣΗΣ: Έστω $x = a^{-1} * b$. Τότε

$$a * x = a * (a^{-1} * b) = (a * a^{-1}) * b = e_G * b = b$$

Οι αποδείξεις των 2, 3 παρόμοιες.

Παρατήρηση: Προσοχή αν $(S, *)$ ΔΕΝ είναι ομάδα μπορεί οι παραπάνω προτάσεις να μην ισχύουν. Για παράδειγμα το $(\mathbb{R}, \cdot)$ ΔΕΝ είναι ομάδα και δεν ισχύει ο κανόνας διαγραφής, γιατί $0 \cdot 1 = 0 \cdot 2$ αλλά $1 \neq 2$.

Παράδειγμα: Έστω $(G, *) = ((-1, 1), *)$ όπου $a * b = \frac{a+b}{1+a \cdot b}$ (που είναι ομάδα)

Να λυθεί στο G η εξίσωση:

$$0.5 * x = 0.7.$$

Λύση:

Αφού $(G,*)$ ομάδα, η εξίσωση έχει (στο G) μοναδική λύση, την $x=(0.5)^{-1}*0.7$, όπως προτάθηκε.

Έχουμε $(0,5)^{-1}=-0,5$

Άρα $x=(-0.5)*0,7=\frac{-0,5+0,7}{1+(-0,5)(0,7)}=\frac{0,2}{1-0,35}=\frac{0,2}{0,65}$

Παραδείγματα (Υπενθύμιση)

$U(\mathbb{Z}_8)=\{[1]_8,[3]_8,[5]_8,[7]_8\}$

	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$[1]_8$	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$[3]_8$	$[3]_8$	$[1]_8$	$[7]_8$	$[5]_8$
$[5]_8$	$[5]_8$	$[7]_8$	$[1]_8$	$[3]_8$
$[7]_8$	$[7]_8$	$[5]_8$	$[3]_8$	$[1]_8$

Παρατηρούμε ότι σε κάθε γραμμή (και σε κάθε στήλη) εμφανίζεται κάθε στοιχείο της $U(\mathbb{Z}_8)$ ΑΚΡΙΒΩΣ ΜΙΑ ΦΟΡΑ. Αυτό γενικεύεται σε κάθε ομάδα ως εξής:

ΠΡΟΤΑΣΗ: Έστω G ομάδα, $a\in G$. Ορίζουμε συναρτήσεις $l_a:G\to G$ και $r_a:G\to G$ με $l_a(b)=a*b$ και $r_a(b)=b*a$, για $b\in G$.

Τότε $l_a:1-1$ και επί και $r_a:1-1$ και επί.

Επιπλέον ισχύει $(l_a)^{-1}=l_{a^{-1}}$ και $(r_a)^{-1}=r_{a^{-1}}$ > αντίστροφοι συνάρτηση.

Απόδειξη

Θα δείξουμε ότι η $f_a(b) = a * b$ είναι 1-1 για κάθε $a \in G$.

$f_a(b) = f_a(b') \Rightarrow a * b = a * b' \Rightarrow b = b'$

Θα δείξουμε ότι η f_a είναι επί για κάθε $a \in G$, δηλαδή η εξίσωση $a * x = b$ έχει λύση στο G για κάθε $b \in G$.

Έχουμε $(f_a \circ f_{a^{-1}})(b) = f_a(f_{a^{-1}}(b)) = f_a(a^{-1} * b) =$

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

$= e_G * b = b.$

Συνεπώς $f_a \circ f_{a^{-1}} = id_G \leftarrow$ ταυτοτική συνάρτηση στο G.

Παρόμοια $f_{a^{-1}} \circ f_a = id_G$ και οι αντίστροφες ιδιότητες της συνάρτησης και: $G \to G$.

Πρόταση: Έστω $(G, *)$ ομάδα και $a, b \in G$. Τότε:

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

Απόδειξη: $(a * b) * (b^{-1} * a^{-1}) = a * b * b^{-1} * a^{-1}$

$= a * e_G * a^{-1} =$

$= a * a^{-1} = e_G$

και $(b^{-1} * a^{-1}) * (a * b) = b^{-1} * a^{-1} * a * b$

$= b^{-1} * e_G * b = b^{-1} * b = e_G$

Συνεπώς από τη μοναδικότητα του αντιστρόφου έπεται ότι $(a * b)^{-1} = b^{-1} * a^{-1}$.

Ορισμός: Έστω G ομάδα, και $a \in G$. Ορίζουμε a^n, για $n \in \mathbb{Z}$ ως εξής: $a^0 = e_G$

Για $a > 0$ $a^n = \underbrace{a * a * \dots * a}_{n \text{ φορές}}$

Για $a < 0$ $a^n = \underbrace{a^{-1} * a^{-1} * \dots * a^{-1}}_{|n| \text{ φορές}}$

Παράδειγμα

Πάντα $a^{-1} = a$, $a^2 = a * a$,

a^{-1} είναι αντίστροφος του a, $a^{-2} = a^{-1} * a^{-1}$

ΠΡΟΣΟΧΗ

Αν η G είναι αβελιανή ισχύει $(a*b)^n = a^n * b^n$.

Αν η G δεν είναι αβελιανή, γενικά δεν ισχύει.

Παράδειγμα

$G = GL_2(\mathbb{R})$ = 2×2 αντιστρέψιμοι πραγματικοί πίνακες.

$$A = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$ Τότε:

$$A^2 = \begin{bmatrix} 4 & 0 \\ 0 & 1 \end{bmatrix}, \quad B^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

$$A \cdot B = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 0 & 1 \end{bmatrix}$$

Τότε $(A \cdot B)^2 = \begin{bmatrix} 2 & 2 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 6 \\ 0 & 1 \end{bmatrix}$

ενώ $A^2 \cdot B^2 = \begin{bmatrix} 4 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 8 \\ 0 & 1 \end{bmatrix}$

Άρα $(A*B)^2 \neq A^2 * B^2$

Πρόταση: Έστω G ομάδα, $n, m \in \mathbb{Z}$ και $a \in G$. Τότε

1) $a^n * a^m = a^{n+m}$

2) $(a^n)^m = a^{n \cdot m}$

Απόδειξη

Περίπτωση 1) Για $n, m > 0$

Έστω $n \geq 1$. Επαγωγή στο m.

για $m=1$ $(a^n) * a^1 = \underbrace{(a * \dots * a)}_{n\text{-φορές}} * a = a^{n+1}$

και $(a^n)^1 = a^n$

Υποθέτουμε $m \geq 1$ και ότι $a^n * a^m = a^{n+m}$

$(a^n)^m = a^{n \cdot m}$

Τότε $a^n * a^{m+1} = a^n * a^m * a = a^{n+m} * a = a^{n+m+1}$

άρα ισχύει. ↑ υποθ. επαγ.

Επίσης $(a^n)^{m+1} = (a^n)^m * (a^n) = a^{n \cdot m} * a^n$

$= \underbrace{(a * \dots * a)}_{n\text{-φορές}} * \underbrace{(a * \dots * a)}_{n\text{-φορές}}$

$= a^{n*m+n} = a^{n(m+1)}$

Για $n=0$ ή $m=0$ η απόδειξη είναι εύκολη

Αν $n<0$ ($n \cdot m < 0$) δουλεύουμε όπως στην περίπτωση 1. με το a^{-1} αντίστροφο του a.

Πόρισμα: Έστω G ομάδα, $a \in G$ και $n > 0$.

Τότε $(a^n)^{-1} = a^{-n} = (a^{-1})^n$

Απόδειξη: Από πρόταση $a^n * a^{-n} = a^{n-n} = a^0 = e_G$

και $a^{-n} * a^n = a^{-n+n} = a^0 = e_G$

Άρα $(a^n)^{-1} = a^{-n}$ πρόταση

και $a^{-n} = a^{(-1)\cdot n} = (a^{-1})^n$

Παρατήρηση: Αν $(S, *)$ όχι ομάδα μπορεί η ύψωση στοιχείου σε αρνητική δύναμη να μην έχει νόημα. Το ίδιο και η ύψωση στη μηδενική δύναμη.

Παράδειγμα: Έστω $G = GL_2(\mathbb{R})$ και $A = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

Υπολογίστε το A^{2020}, A^{-2020}, B^{2020}, B^{-2020}

Λύση: Έχουμε $A^{-1} = \begin{bmatrix} 1/2 & 0 \\ 0 & 1 \end{bmatrix}$

Αφού A διαγώνιος για $k>0$, $A^k = \begin{bmatrix} 2^k & 0 \\ 0 & 1^k \end{bmatrix}$

Συνεπώς $A^{2020} = \begin{bmatrix} 2^{2020} & 0 \\ 0 & 1 \end{bmatrix}$

Παρόμοια επειδή A^{-1} διαγώνιος: $(A^{-1})^k = \begin{bmatrix} (1/2)^k & 0 \\ 0 & 1^k \end{bmatrix}$

άρα $A^{-2020} = \begin{bmatrix} (1/2)^{2020} & 0 \\ 0 & 1 \end{bmatrix}$

$$B^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

$$B^3 = B \cdot B^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$$

Ισχυρισμός: Για $k>0$, $B^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$

Απόδειξη: επαγωγή στο k. Για $k=1$ ισχύει.

Έστω $k \geq 1$ και ισχύει για k. Τότε

$$B^{k+1} = B\,B^k = B \cdot \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & k+1 \\ 0 & 1 \end{bmatrix}$$

Συνεπώς $B^{2020} = \begin{bmatrix} 1 & 2020 \\ 0 & 1 \end{bmatrix}$

Εύκολα υπολογίζουμε ότι $B^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$

και με παρόμοια επιχειρήματα

$$(B^{-1})^k = \begin{bmatrix} 1 & -k \\ 0 & 1 \end{bmatrix} \quad \forall k>0$$

Συνεπώς $B^{-2020} = (B^{-1})^{2020} = \begin{bmatrix} 1 & -2020 \\ 0 & 1 \end{bmatrix}$