3

Групи

Деф. (Група) Множество от ~~елементи~~ обекти с една бинарна операция.

Деф: (Бинарна операция)
$M = \emptyset$ (не ни вълнува естеството на елементите

$\varphi: M \times M \to M$

$\varphi(a, b)$ – запис в Анализа (функционален запис)

$a \varphi b$ – запис в Алгебрата (инфиксен запис)

$a * b$
$a + b$
$a \cdot b$

Примери за бинарна операция:
- сума на две цели числа е цяло число
- сума на два вектора е вектор

Примери за операции, които не са бинарни:
- скаларно произведение на два вектора е число
- умножение на вектор с число

Деф. (Група)
$G \neq \emptyset$ с бинарна операция $"*" \to (G, *)$
$(\forall a, b \in G \times G \to a * b \in G)$

G е група с ~~бинарна операция~~ относно $"*"$, ако са изпълнени свойствата:
1) асоциативност: $(a * b) * c = a * (b * c)$;
2) $\exists e \in G: a * e = e * a = a, \forall a \in G$;
3) $\forall a \in G, \exists b_{(a)} \in G: a * b = b * a = e$.

Примери за групи:

- цели числа с операция „+" $(\mathbb{Z}, +)$

! $\mathbb{Z}$ с операцията „*" не е група, защото липсва противоположният елемент, за да получим единичния

- $(\mathbb{Q}, +)$
- $(\mathbb{R}, +)$
- $(\mathbb{C}, +)$

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Операцията „+" се разширява

$(\mathbb{Z}, +)$ подгрупа на $(\mathbb{Q}, +)$, която е подгрупа на $(\mathbb{R}, +)$, която е подгрупа на $(\mathbb{C}, +)$.

$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\} \Rightarrow (\mathbb{Q}^*, *)$

- $(\mathbb{R}^*, *)$, където $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$
- $(\mathbb{C}^*, *)$, където $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$
- $(\mathbb{Z}^*, *)$, където $\mathbb{Z}^* = \{-1, 1\}$

$(\mathbb{Z}^*, *)$ пример за крайна група

- $(\mathbb{R}^2, +)$ - геометрични вектори в $\mathbb{R}^2$

- $(\mathbb{R}^3, +)$ - — " — $\mathbb{R}^3$

V - линейно пространство

- $(V, +)$ - група, лин.пр-во с операцията събиране на вектори

- $(M_{m\times k}, +)$ ~~Група~~

Опр: G е комутативна (Абелева), ако $a * b = b * a$, $\forall a, b$.

Опр. G - крайна, ако има краен брой елементи. $|G| < \infty$

Опр. Ред на групата G - броя на елементите в групата G.

$M_{n\times n}$

$(AB)C = A(BC)$

$EA = AE = A$

с елементи от полето F

$GL(n, F) = \{ A \in M_{n\times n}(F) \mid \det A \neq 0 \}$

$A, B \in GL(n, F) \Rightarrow \det A \neq 0, \det B \neq 0$

$\Rightarrow \det(AB) = \det A . \det B \neq 0 \Rightarrow A.B \in GL(n, F)$

$\det(E) = 1 \neq 0 \Rightarrow E \in GL$

$A \in GL \Rightarrow A^{-1}$ също е обратима, $A^{-1} \in GL$

$\Rightarrow$ $(GL(n,F), *)$ – обща линейна група от степен n над полето F

↑

пример за некомутативна (не Абелева) група

Следствия от аксиомите:

① (обобщена асоциативност)

от $(a*b)*c = a*(b*c)$ следва, че ако $a_1 * a_2 * \dots * a_n$, по каквато и да е начин да са разположени скобите, резултатът е еднаков.

Доказателство: Чрез индукция по n

$n=3$: асоциативен закон

~~ИП: Допускаме се т.в. е вярно за някое~~ ~~$k \geq 3$~~

~~ИС: Ще док. че т.в. е вярно за $k+1$~~ ИП

ИС: док. че т.в. е вярно за всички числа $< n$ т.в. е док.

Нека $n>3$ и да док. че за всички числа $< n$ т.в. е док.

$[a_1 * a_2 * \dots * a_n] = a_1 * (a_2 * (a_3 * \dots * (a_{n-1} * a_n)) \dots)$

$a_1 * \dots * a_n = (a_1 \dots a_k) * (a_{k+1} \dots a_n)$

$a_1 * \dots * a_n$ – произвол. скоби

$(a_1 \dots a_k)$ – a_1

$f(a_1, \dots, a_k) * g(a_{k+1}, \dots, a_n)$

a_1 – произв. на тези елементи с разположение по произвол. начин скоби

$1 \leq k < n$

По ИП: $[a_1, \dots, a_k] * [a_{k+1} \dots a_n] =$

$= (a_1 * [a_2 \dots a_k]) * [a_{k+1}, \dots, a_n] =$

$= a_1 * ([a_2, \dots, a_k] * [a_{k+1}, \dots, a_n]) =$

$= a_1 * [a_1, \dots, a_n] = [a_1, \dots, a_n]$

② (Единственост на неутрален елемент)

$\exists! e : e * a = a * e = a, \forall a.$

Доказателство:

Допускаме, че $\exists e_1, e_2$ с тоест св-во e_i, т.е.

$e_1 * a = a * e_1 = a$ и $e_2 * a = a * e_2 = a$

$\Rightarrow e_1 * e_2 = \begin{cases} e_2 \\ e_1 \end{cases} \Rightarrow e_1 = e_2 \Rightarrow$ елементът e

е единствен.

$+$ – адитивен запис	$*$ мултипликативен запис
сума	произведение
нула	единица
$(-a)$ противоположен	обратен (a^{-1})
разлика	частно

③ св (Единственост на симетричния елемент относно операцията)

$\forall a \in G, \exists! b(a) : a * b = b * a = e$

Док-во:

Док, че $\exists b_1, b_2 : b_1 = b_1 * e = b_1 * (a * b_2) = b_1 * a) * b_2 =$

$= e * b_2 = b_2 \Rightarrow b_1 = b_2$

④ $\forall a, b \in G$

$\exists! x \in G$ и $\exists! y \in G$: $a * x = b$

$y * a = b$

Док-во:

$a * x = b \mid \cdot a^{-1}$

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

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

$e * x = a^{-1} * b$

$x = a^{-1} * b$

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

$x = a^{-1} * b$

$y * a = b$

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

$y * e = b * a^{-1}$

$y = b * a^{-1}$

⑤ (следствие от обобщената асоциативност при мултипликация.

Ако имаме $\underbrace{a\,a\,a \ldots a\,a}_{k} = a^k$

$a^k \cdot a^5 = a^{k+5}$

$(a^k)^5 = a^{k \cdot 5}$

$(ab)^k = \underbrace{(ab)(ab)(ab)\ldots(ab)}_{k}$

при адитивен запис

$\underbrace{a+a+a\dots+a}_{k} = ka$

$ka + sa = (k+s)a \quad \in \mathbb{N}$

$k(sa) = (ks)a$

Деф: (подгрупа)

$(G, *)$ – група

H е подгрупа на G, ако H е група относно операцията в G: $H \leq G$

$\{e\} < G; \quad G \leq G$

$(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$

$(\mathbb{Z}^*, *) < (\mathbb{R}^*, *) < (\mathbb{R}^*, *) < (\mathbb{C}^*, *)$

$(\mathbb{Z}^*, *) \not< (\mathbb{Z}, +)$

(Тв) Нека $H \neq \emptyset$: $H \subset G$.

$H < G \Leftrightarrow \begin{cases} \forall ab \in H, \forall a, b \in H \\ \forall a^{-1} \in H, \forall a \in H \end{cases} \Leftarrow$ (достатъчно) $ab^{-1} \in H, \forall a, b \in H$

Доказателство:

$H < G \Rightarrow ab \in H$, "$*$" е бинарна и за H

a^{-1} от сакс (3)

$\Leftarrow$ 1) "$*$" е бинарна за H

аксиома $(ab)c = a(bc)$ важи за $G \Rightarrow$ и за H

Умно $a \in H \Rightarrow$ от 2) $\Rightarrow a^{-1} \in H \Rightarrow e = aa^{-1} \in H$

$\Rightarrow a \in H, \exists a^{-1} \in H, \; a a^{-1} = e$ (а к с 3)

---

n-ти корени на единицата

$C_n = \{ x \in \mathbb{C} \mid x^n = 1 \} = \{ \omega_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} \mid k = 0, 1, \dots, n-1 \}$

Да док, че C_n е подгрупа на $(\mathbb{C}, *)$:

$x, y \in C_n \qquad x^n = 1; \; y^n = 1$

$(xy)^n = x^n y^n \Rightarrow xy \in C_n$

$\left(x^{-1}\right)^n = \left(\frac{1}{x}\right)^n = \frac{1}{x^n} = 1 \Rightarrow x^{-1} \in C_n$

$\Rightarrow C_n < \mathbb{C}^*$

$C_n = \{ 1, \omega_1, \omega_1^2, \omega_1^3, \dots, \omega_1^{n-1} \}$ – циклична група от ред n

$\omega_k = \left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)^k$

За домашно: $\forall M_{n\times n}: \det(M_{n\times n}) = 1$.

Да се док, че $(M_{n\times n}, *)$ е група, т.е. $(M_{n\times n}, *) < (GL(n,K), *)$

↓

специална линейна група

Симетрична група

$M \neq \emptyset$

$S(M)$ – симетрична група на мн-вото M

$S(M) = \{ \varphi : M \to M \text{ (биекция)} \}$

$\varphi \circ \psi (x) = \varphi(\psi(x)), \quad x \in M$

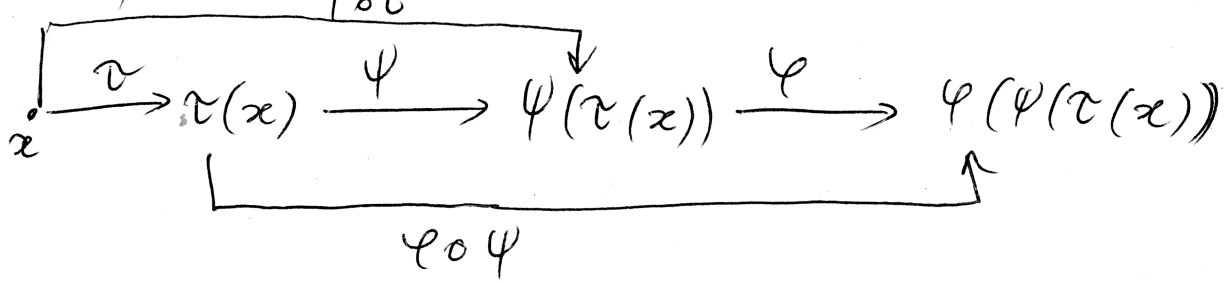
$\varphi \circ \psi \in S(M)$

1) асоциативност:

$\varphi, \psi, \tau \in S(M)$ - биекции за M, $x \in M$

$((\varphi \circ \psi) \circ \tau)(x) = (\varphi \circ \psi)(\tau(x)) = \varphi(\psi(\tau(x)))$

$(\varphi \circ (\psi \circ \tau))(x) = \varphi \circ ((\psi \circ \tau)(x)) = \varphi(\psi(\tau(x)))$



$\Rightarrow (\varphi \circ \psi) \circ \tau = \varphi \circ (\psi \circ \tau)$

② неутрален елемент

$id \circ \varphi = \varphi \circ id = \varphi$

③ противоположен елемент

$\exists \varphi^{-1}$

$\varphi \circ \varphi^{-1} = id = \varphi^{-1} \circ \varphi$

т.е. $S(M)$ е симетрична група за множеството M

$|M| = n, \quad M = \{1, 2, \ldots, n\}$

$\varphi \in S(M) = S_n$ - симетрична група от степен n
$\Rightarrow M$ има n елемента

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix}, \quad i_s = \varphi(s)$$

пермутация на числата от 1 до n

$|S_n| = n!$ - броя на всичките пермутации на числата от 1 до n

$\Rightarrow S_2 < S_3 < \dots < S_n$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$\varphi \circ \varphi$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

В общем случай операцията композиция не е комутативна. При $n > 2$, при S_n о не е комутативно.