Групи

Бинарна операция $M \neq \emptyset$

$\varphi: M \times M \to M$ е бинарна операция

$a, b \to \varphi(a,b) \in M$

$\exists\ \exists$

в алгебрата $+, \cdot, *, \circ, \oplus, \heartsuit$

$a+b$
$a-b$
$a \cdot b$
$a * b$
$\vdots$

Деф. Нека $M \neq \emptyset$ и „$*$" бинарна операция в M $\Rightarrow \forall a,b \in M \to a*b \in M$

M е група относно „$*$", когато $(M,*)$ изпълнява

1) $(a*b)*c = a*(b*c)$, $\forall a,b,c \in M$
2) $\exists e \in M$: $a*e = e*a = a$, $\forall a \in M$
3) $\forall a \in M$, $\exists b_{(a)} \in M$: $a*b_{(a)} = b_{(a)}*a = e$

$\mathbb{N}, +$ не група

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

F - поле $(F,+)$

$(V,+)$

V е лин. пр-во

Деф. Ако $(M,*)$ група и ако $a*b = b*a$, $\forall a,b \in M$, тогава M - абелева / комутативна

Абелеви

$(\mathbb{Q}^*, \cdot)$ лиснва образен ел. на числ. 0

$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ $\quad \mathbb{R}^* = \mathbb{R} \setminus \{0\}$; $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$

$(\mathbb{Q}^*, \cdot)$ $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$

$\mathbb{Z}^* = \{1, -1\}$ $(\mathbb{Z}^*, \cdot)$. Абелева

$E = \{1\}$ $(E, \cdot)$.

$\mathcal{M}_{n \times n}(F)$

$EA = AE = A$

$A(BC) = (AB)C$

A, $\exists B$: $AB = BA = E$

$GL(n, F) = GL_n(F) = \{A \in \mathcal{M}_{n \times n}(F) \mid \det A \neq 0\}$

$A, B \in GL(n, F) \Rightarrow A \cdot B \in GL(F)$

$\det(AB) = \det A \cdot \det B$

$A \in GL(n, F) \Rightarrow \det(A^{-1}) = (\det A)^{-1}$

$A^{-1} \in GL(n, F)$

Неабелева група

Св-во 1) Неутр. елем. е единствен
за който $a*e=e*a=a$, $\forall a \in G$

Допускаме се e_1, e_2 изпълняват

$e_1 \overset{=}{=} e_1 e_2 = e_2 \Rightarrow e_1 = e_2$

Св-во 2) Ако $a \in G \Rightarrow \exists! b$: $a*b=b*a=e$
този елемент е единствен за a

Допускаме, че b_1, b_2 изпълняват св-ва

$b_1 \overset{=}{=} b_1 e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$

$\Rightarrow b_1 = b_2$

Св-ва $a, b \in G$ $\exists! x$: $a*x=b$

$\exists! y$: $y*a=b$

$a*x=b$

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

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

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

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

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

$y+a=b \quad (+)$

$y+a+(-a) = b+(-a)$

$y = b+(-a) = b-a$

+	$\bullet, *, \circ$
адитивна	мултипликат
нулев ел. 0	единичен $e, E, 1,$ id
противопол. $-a$	обратен елемент a^{-1}
кратен на a $a+\dots+a = \underbrace{}_{x} = x(a)$	степен на a $a.a.\dots.a = \underbrace{}_{x} = a^x$

Пример $a \equiv b \pmod n$ сравнение по модулю

Далее $\Leftrightarrow n \mid (a-b) \Leftrightarrow$ имеют равные остатки при делении на n

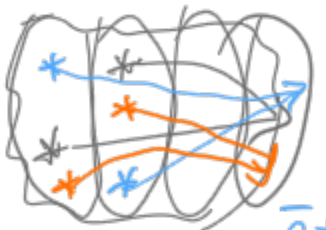
(1) $a \equiv a \pmod n$

(2) $a \equiv b \pmod n \Leftrightarrow b \equiv a \pmod n$

(3) $a \equiv b \pmod n$ и $b \equiv c \pmod n$ $\Rightarrow a \equiv c \pmod n$

$a_1 \in \bar{a}$, $b_1 \in \bar{b}$, $a_1 + b_1 \in \bar{r}$

$a + b = nq + r$, $0 \le r < n$



$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

$\bar{a} + \bar{b} = \bar{r}$ | $r \equiv a+b \pmod n$

$\bar{a} + \bar{b} = \overline{a+b}$ | Абелевы

$\bar{a} = \{a + kn \mid k \in \mathbb{Z}\}$

классовые остатки

$\mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2} \cup \dots \cup \overline{n-1}$

$\bar{0}$ $-\bar{a} = \overline{n-a}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$\mathbb{Z}_5$

$a_1 \equiv b_1 \pmod n$, $a_2 \equiv b_2 \pmod n$ $\Rightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod n$

$M \neq \emptyset$ $\quad S(M) = \{ \varphi \mid \varphi : M \to M$ биекция $\}$ симетрична група на мн-во M

$\varphi, \psi \in S(M) \Rightarrow \varphi \circ \psi (x) = \varphi(\psi(x))$ композиция

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

$id : M \to M$ $\quad \varphi \circ id = id \circ \varphi = \varphi$ // $\exists \varphi^{-1} : \varphi \circ \varphi^{-1} = id$

16) когато $|M| > 2 \Rightarrow S(M)$ е **некомутативна**

Нека $x, y, z \in M$ различни

$\varphi \begin{cases} x \to y \\ y \to x \\ z$ и пр.ел. остават

$\psi \begin{cases} x \to z \\ z \to x \\ y$ и останалите не пред.

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

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

$\Rightarrow \varphi \circ \psi \neq \psi \circ \varphi$

$|M| = n \quad M = \{1, 2, \dots, n\} \quad \varphi \in S(M)$

$\varphi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & \dots & & i_n \end{pmatrix} \quad i_k = \varphi(k)$

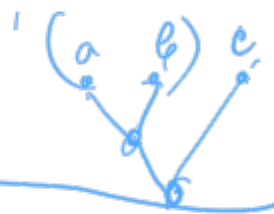
φ - биекция $\Rightarrow i_1, \dots, i_n$ са перм. на числ. $1, \dots, n$

$S(M) = S_n$ елементите са наричат пермутации

$|S_n| = n!$

S_n – симетрична група от степен n

$(G, \cdot)$ $(ab)c = a(bc)$



Обобщена асоциативност

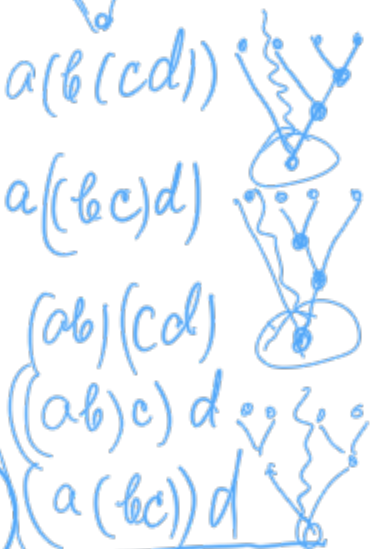
$a_1, a_2, \dots, a_k \in (G, \cdot)$

$a_1 \cdot a_2 \cdot \dots \cdot a_k$ не произвежда нищо разполагане скобите винаги се получава един и същи резултат

инд. по k

$k = 3$ асоциативния закон

Нека е док. за $3 \le k \le n$ // Разглеждаме за $(n+1)$



$g(a_1, \dots, a_{n+1}) = h(a_1, \dots, a_s) \cdot t(a_{s+1} \dots a_{n+1})$

$t(a_1, a_2, \dots, a_{n+1}) = (((a_1 a_2) a_3) a_4 \dots | a_{n+1} \Rightarrow$ $t(a_1, \dots a_{n+1}) = t(a_1, \dots a_n) \cdot a_{n+1}$

t - приложане инд. $\to t = t$

$g(a_1 \dots a_{n+1}) = h(a_1 \dots a_s) t(a_{s+1} \dots a_{n+1}) =$

$= h(a_1 \dots a_s) [t(a_{s+1}, \dots, a_n) \cdot a_{n+1}] = (h(a_1 \dots a_s) t(a_{s+1} \dots a_n)] a_n$

$= t(a_1 \dots a_n) \cdot a_{n+1} = t$

$(G,\cdot)$ $a_1 a_2 \dots a_n$ без да сагаме скоби

$(L,+)$ $x_1 + x_2 + \dots + x_n$ — // —

$(G,\cdot)$ $a \in G$

$a \cdot a \cdot \dots \cdot a = a^x$ $(x \in \mathbb{N})$
(x)

① $a^x \cdot a^s = a \cdot \dots \cdot a \cdot a \cdot \dots \cdot a = a^{x+s}$
(x) (s)

② $(a^x)^s = (a \dots a) \dots (a \dots a) = a^{x \cdot s}$
(x) (x) (s)

$(L,+)$ $x \in L$ $x \in S \in \mathbb{N}$

$x + \dots + x = x(x)$
(x)

$x(x) + s(x) = (x+s)(x)$

$s(x(x)) = (s \cdot x)x$

$x(x+y) \neq x(x) + x(y)$

$(ab)^x = ab \cdot ab \dots ab \neq a^x b^x$
(x)

$(G, \cdot)$

① $(a^{-1})^{-1} = a$

② $(ab)^{-1} = b^{-1}a^{-1}$

Проверка

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

$a(bb^{-1})a^{-1} = aea^{-1} = e$

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

при аддитивной записи $(\mathbb{Z}, +)$

① $-(-x) = x$

② $-(a+b) = -b-a$

$(a+b)+(-b)+(-a) =$

$a+0+(-a) = 0$

Опр. Нека $(G,*)$ група $\emptyset \neq H \subset G$ $\boxed{H < G}$ $(H,*)$
Ако H е група относно операцията $*$
тогава H се нарича подгрупа на G

Т. $\emptyset \neq H \subset G$, то $H < G \Leftrightarrow$ $\begin{cases} ab \in H, \forall a,b \in H \\ a^{-1} \in H, \forall a \in H \end{cases}$

$\boxed{ab^{-1} \in H, \forall a,b \in H} \Rightarrow$

Дво $H < G \Rightarrow$ $\begin{cases} "*" \text{ бинарна опер. в } H \\ \Rightarrow ab \in H, \forall a,b \in H \\ \forall a, \exists a^{-1} \in H \Rightarrow^{e} = a \cdot a^{-1} \in H \end{cases}$

$\begin{cases} a \cdot b \in H, \forall a,b \in H \\ a^{-1} \in H, \forall a \in H \end{cases} \Rightarrow$ $"\cdot"$ е бинарна за H
$a,b,c \in H \subset G \Rightarrow (ab)c = a(bc)$
$a^{-1} \in H, \forall a \in H \Rightarrow^{e} a \cdot a^{-1} \in H$

$a^{-1} \in H$, когато $a \in H$

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

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

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

$\emptyset \neq K \subset \mathcal{U}$ $\quad S(K) \leq S(\mathcal{U})$

$SL(n,\mathbb{R}) = \{ A \in \mathcal{U}_{n\times n}(\mathbb{R}) \mid \det(A) = 1 \}$

$A, B \in SL$ $\quad \det(AB) = \det A \cdot \det B = 1 \cdot 1 = 1$

$\Rightarrow AB \in SL(n,\mathbb{R})$

$A^{-1} \in SL$

$4\mathbb{Z} = \{ 4k \mid k \in \mathbb{Z} \} < (\mathbb{Z},+)$ $\quad n\mathbb{Z} < \mathbb{Z}$

$\mathbb{C}$ $\quad C_n = \{ x \in \mathbb{C} \mid x^n = 1 \}$ $\quad C_n < \mathbb{C}^*$

$n \in \mathbb{N}$

$x^n = 1,\ y^n = 1 \Rightarrow (xy)^n = 1 \Rightarrow xy \in C_n$

$x^n = 1 \Rightarrow (x^{-1})^n = (x^n)^{-1} = 1$

$x^{-1} \in C_n$

аналогично группа

Ред на елемент и цикличност на група

$\forall Z = \{k(4) = \underbrace{4 + \cdots + 4}_{k} \mid k \in \mathbb{Z}\}$

$(\mathbb{N}, +) \quad k > 0$

$k(x) = \underbrace{x + \cdots + x}_{k}$

$S = -k$

$S(x) = -k(x) = \underbrace{(-x) + (-x) + \cdots + (-x)}_{k}$

$(t+k)x = t(x) + k(x)$

$0(x) = 0$

$(G, \circ) \quad k \geq 0$

$\underbrace{a\,a \cdots a}_{k} = a^k$

$S = -k$

$a^S = \underbrace{(a^{-1})(a^{-1}) \cdots (a^{-1})}_{k}$

$a^0 = e$

$a^t a^k = a^{t+k}$

$3 \in (\mathbb{R}^*_{1,\cdot}) \Rightarrow \langle 3 \rangle = \{3^k \mid k \in \mathbb{Z}\}$

$\langle x \rangle = \{k(x) \mid k \in \mathbb{Z}\}$

циклична подгрупа породена от x

$a \in G$

$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$

мултипликативна подгр. породена от x

св-во 1

Нека $(G, \cdot)$, $a \in G$

$\Rightarrow \langle a \rangle^1 \subset H$ | $H < G$ и $a \in H$

$\langle a \rangle < H$

$a \in H \Rightarrow \underbrace{a \cdot a \cdots a}_{k} \in H$, $a^{-1} \in H \Rightarrow \underbrace{(a^{-1}) \cdots (a^{-1})}_{k} \in H$

$\Rightarrow \langle a \rangle \subset H$

Циклична подгр. $\langle a \rangle$ е най-малката подгрупа, която съдържа a

$3 \in (\mathbb{Q}^*, \cdot) \Rightarrow \langle 3 \rangle = \{3^k \mid k \in \mathbb{Z}\}$

$3 \in (\mathbb{Q}, +) \Rightarrow \langle 3 \rangle = \{k.3 \mid k \in \mathbb{Z}\} = 3\mathbb{Z}$

$(\mathbb{Z}, +)$ $\langle 1 \rangle = \mathbb{Z}$; $\langle -1 \rangle = \mathbb{Z}$ $\Rightarrow$ $\mathbb{Z}$ е цикличне

Опр. $(G, \cdot)$ е цикл. група, когато $\exists\, a \in G$: $\langle a \rangle = G \Leftrightarrow \{a^k \mid k \in \mathbb{Z}\}$

Пр. $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \ldots, \bar{5}\}$

$\mathbb{Z}_6 = \langle \bar{1} \rangle = \{\bar{0}, \bar{1}, 2(\bar{1}) = \bar{2}; 3(\bar{1}) = \bar{3}, \ldots, 5(\bar{1}) = \bar{5}\}$

аналогично $\mathbb{Z}_n = \langle \bar{1} \rangle$ $n \in$ произв.

$\mathbb{Z}_n$ цикличен

$$C_n = \{x \in \mathbb{C} \mid x^n = 1\} \subset \mathbb{C}^*$$

$$\omega_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad k = 0, 1, \dots, n-1$$

$$C_n = \{\underset{\parallel}{\omega_0}, \omega_1, \omega_2, \dots, \omega_{n-1}\} = \{1, \omega_1, \omega_1^2, \omega_1^3, \dots, \omega_1^{n-1}\}$$
$$\omega_0 = 1$$

$$\omega_k = \left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)^k = \omega_1^k \qquad \omega_1^n = 1$$

$C_n = \langle \omega_1 \rangle$ циклична група от степен n

Св-во Ако $G = \langle a \rangle \Rightarrow G$ е Абелева

$\mathbb{Z}_n = \langle \bar{1} \rangle \qquad n(\bar{1}) = \underbrace{\bar{1} + \dots + \bar{1}}_{n} = \bar{0}$

$\mathbb{Z} = \langle 1 \rangle \qquad n(1) = n \neq 0 \quad$ за $n \neq 0$

Опр. $a \in G$, $(G, \cdot)$
реда на a е k, когато k е най-мал. ест. число, за което $a^k = e$

$(L, *)$
$x \in L$
k-тий ест. число
$k(x) = 0$

Ако $\forall k \in \mathbb{N}$ е изпълнено че $a^k \neq e \Rightarrow a$ има ред ∞

$|a| = k$ или $0(a) = k$; $\operatorname{ord}(a) = k$

Тв Нека $(G, \cdot)$ $a \in G$ и $|a| = k$
Тогава:
а) $a^s = e \Leftrightarrow k \mid s$
б) $a^s = a^t \Leftrightarrow s \equiv t \pmod k$

Док-во Нека $|a| = k$ и $a^s = e \Rightarrow s = kq + r$, $0 \leq r < k$
$\Rightarrow e = a^s = a^{kq+r} = a^{kq} \cdot a^r = (a^k)^q \cdot a^r = e \cdot a^r = a^r$
$\Rightarrow$ единствено възм. е $r = 0 \Rightarrow k \mid s$
$\Leftarrow k \mid s \Rightarrow s = kt \Rightarrow a^s = a^{kt} = (a^k)^t = e$

б) $a^s = a^t \Leftrightarrow a^s \cdot a^{-t} = e \Leftrightarrow a^{s-t} = e \Leftrightarrow k \mid (s-t) \Leftrightarrow$
$s \equiv t \pmod k$

Тв. Нека $(G,\cdot)$ е група и $a \in G$
$\Rightarrow |\langle a \rangle| = |a|$

Д-во Нека $|a| = k \ (\neq \infty)$

Нека $s \in \mathbb{Z}$; $s = kq + r$, $0 \le r < k$

$a^s = a^{kq+r} = (a^k)^q \cdot a^r = e \cdot a^r = a^r$

$\Rightarrow a^s = a^r \in \{a^0, a^1, \dots, a^{k-1}\}$

Ако $s \neq t$ и $s, t \in \{0, 1, \dots, k-1\}$

$a^s \neq a^t$, защото $k \nmid (s-t)$

$\Rightarrow \langle a \rangle = \{a^0, a^1, \dots, a^{k-1}\}$

$|\langle a \rangle| = k$

Когато $|a| = \infty$

$\Rightarrow a^k \neq e$ за $k \neq 0$

$\Rightarrow a^k \neq a^s$ за $k \neq s$

$\Rightarrow \{a^k \mid k \in \mathbb{Z}\}$ няма повтарящи се елементи

$\Rightarrow |\langle a \rangle| = \infty$

$C_n = \langle \omega_1 \rangle =$

$= \{1, \omega_1, \omega_1^2, \dots, \omega_1^{n-1}\}$

$= \{\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \mid 0 \le k < n\}$

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

$= \{\bar{0}, \bar{1}, 2(\bar{1}), \dots, (n-1)\bar{1}\}$