Коректност на деф.

Нека $\bar{a} = \bar{a_1}$ $(a = a_1 \pmod n)$

$b = \bar{b_1}$ $(b = b_1 \pmod n)$ — едни и същ.

$\Rightarrow a+b \equiv a_1 + b_1 \pmod n \Rightarrow$ ост. на $a+b$ и на a_1+b_1 по $(\mod n)$ е

$a \cdot b \equiv a_1 \cdot b_1 \pmod n \Rightarrow ab$ и $a_1 b_1$ дават едни и същ остатък.

сл: $\bar{a} + \bar{b} = \overline{a+b}$

сл: $\bar{a} \cdot \bar{b} = \overline{ab}$

Разглеждаме $\mathbb{Z}_4$

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

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

— симетрична

---

3. Групи - определение примери и основни свойства. Подгрупи

Деф: Бинарна операция $\varphi: M \times M \to M$ е изображение, което на $\forall$ наредена двойка елементи от M съпоставя елемент от M.

$M \neq \emptyset$ $\varphi(a,b)$ $a \varphi b$, $a * b$, $a + b$, $a \cdot b$

Примери: (бинарни операции) - сума на 2 цели числа е цяло число

- сума на два вектора е вектор, - умножение на матрици,

- умножение на вектори - сума на матрици - сума на вектори...

(не бинарни операции) - скаларно произведение на два вектора е число, - умножение на вектор с число

Деф за Група: Нека $G \neq \emptyset$ с бинарна операция „$*$", т.е за $(\forall a, b \in G \times G \to a * b = G$. G е група 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) $\forall a \in G, \exists b(a) \in G: a*b = b*a = e$ Записване $(G, *)$

пр: $\mathbb{Z}$ с операция „$+$", $(\mathbb{Z}, +)$ е група

$\mathbb{Z}$ с „$\cdot$" не е група т.к не е изпълнено 3)св.

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

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ – ако нещо вади за друга, то вади и за подгрупа. Тези групи са подгрупи една на др. (О-ямна обратен ел.)

$\Rightarrow \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ е група относно "$\cdot$"

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ е група $(\mathbb{R}^*, \cdot)$

$\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ $(\mathbb{C}^*, \cdot)$ група

$\mathbb{Z}^* = \{1, -1\}$ – крайна група

$(\mathbb{R}^2, +)$ $(\mathbb{R}^3, +)$ геометр. вектор. с събир. "+"

V – линейно пространство с операцията събиране на вектори

$(V, +)$ е група, $(M_{n\times k}, +)$ – група

Деф. Групата се нарича комутативна или абелева, ако $a*b = b*a$ $\forall a, b$

Деф. Групата G е крайна, ако има краен бр. елементи

Деф. Ред на групата е бр. на елементите в групата

G – крайна $\Leftrightarrow |G| < \infty$

$M_{n\times n}$ – квадратните матрици

1) $(AB)C = A(BC)$

2) $EA = AE = A$

3) разглеждаме множ. $\forall M_{n\times n}$: $GL(n, F) = \{A \in M_{n\times n}^{(F)} \mid \det A \neq 0\}$

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

$\det(AB) = \underbrace{\det A}_{\neq 0} \cdot \underbrace{\det B}_{\neq 0} \neq 0$ – защото от полето F

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

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

$\Rightarrow$ това множество от матрици с $\det \neq 0$ формира Пълна линейна група над F относно умножението. – Пример за неабелева група.

GL – пълна линейна група.

Следствие от аксиомите: (сб. на 1 група):

сб 1) От асоциативността $(a*b)*c = a*(b*c) \Rightarrow$

$a_1 * b a_2 * \ldots$ чак до каквото и каквато са разбиванията <u>скобите</u> резултатът е същият (обобщена асоциативност)

<u>Д-во:</u> с индукция по n

а) $n = 3$ – извънлено от асоциативността

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

Нека $n > 3$ и допускаме, че за $\forall n < 3$ е изпълнено, че може да бъде приведено в горния вид (#)

б) $\underbrace{a_1 * \dots * a_n}_{\text{някакъв скоб}} = \underbrace{(a_1 * \dots * a_k)}_{\text{някакъв скоб}} * \underbrace{(a_{k+1} * \dots * a_n)}_{\text{някакъв скоб}}$

$f(a_1 * \dots, a_k) * g(a_{k+1} \dots, a_n)$ - умножение на числата със скоби разположени по някакъв начин.

По ИП $1 \le k < n$ и f и $g \Rightarrow f(a_1, \dots a_k) = a_1 * (a_2 * (\dots)) =$

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

$= \underbrace{a_1 * \dots * a_n}_{\text{някакъв скоб}} = [a_1, \dots, a_k] * [a_{k+1}, \dots, a_n] =$

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

$= a_1 * [a_2, \dots, a_n] = [a_1, \dots, a_n]$

ИП

об2 Единствеността на неутралния елемент: $\exists! e : e * a = a * e = a, \forall a$

1-во: Допускаме че $\exists e_1, e_2$ $e_1 * a = a * e_1 = a$ $\forall a$

$e_2 * a = a * e_2 = a$

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

Този единствен елемент се нарича още решаващи числа в зависимост от операцията в групата

пр: при операция събиране (+) е нулев ел.

при опер. умножение (·) е 1-ца

адитивен запис (+)	мултипликативен (·)
сума	произведение
0 - нулев ел.	1 - ца

$(-a)$ противоположен ел (разлика) обратен елемент (a^{-1}) (частно деление)

об3 Симетричния елемент относно операцията * е единствен

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

Док-во: Допускаме, че $\exists b_1$ и $b_2 \Rightarrow b_1 = b_1 * e = b_1 * (a * b_2) =$

$= (b_1 * a) * b_2 = e * b_2 = b_2 \Rightarrow b_1 = b_2 = b$ b - обратен

противоположен на a

Св 1 (Свойство за обратимите елементи)

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

Док-во: $a * x = b \mid a^{-1}$

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

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

$a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b \Rightarrow$ решението е единствено

$\Rightarrow \boxed{x = a^{-1} * b}$, $y * a = b$, $(y * a) * a^{-1} = b * a^{-1}$ $\boxed{y = b * a^{-1}}$

разбъркването на умножителите е от значение!

С-е от Св 1: (от обобщената асоциативност)

$a * a * a * \ldots * a = a^k$ - при умножаване степени с равни основи

следва от обобщената асоциативност.

при умножение $\begin{cases} a^k * a^s = a^{k+s} \\ (a^k)^s = a^{k \cdot s} \\ (a * b)^k = \underbrace{(a*b) * (a*b) * (a*b) * \ldots * (a*b)}_{k} \end{cases}$

при адитивен запис: $a + a + \ldots + a = k \cdot a$

$ka + sa = (k+s)a$ $\quad k, s \in \mathbb{N}$ (k, s елементи от различни множества)

$s(ka) = (sk)a$

Деф за Подгрупа: Нека $(G, \cdot)$ - група относно опер $(\cdot)$

H е подгрупа на G, ако H е група относно операцията в G.

Бележим $H < G$ или $H \leq G$.

Пр: за подгрупи: $\{e\} < G$; $G \leq G$; $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$

$\mathbb{Z}^* = \{-1, 1\} < \mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$

$(\mathbb{Z}^*, \cdot) \not< (\mathbb{Z}, +)$ - защото операциите са различни

Твърдение: Нека H е непразно подмножество на G. $H < G \iff$

$\begin{cases} a b \in H, \forall a, b \in H \\ a^{-1} \in H, \forall a \in H \end{cases} \left(\iff a b^{-1} \in H, \forall a, b \in H \right)$

Д-во: $\boxed{\Rightarrow}$ $H < G \Rightarrow a, b \in H \Rightarrow$ опер. "$\cdot$" е бинарна за H

$\Rightarrow a^{-1}$ от аксиома (3)

$\boxed{\Leftarrow}$ от 1) "$\cdot$" е бинарна за H

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

Нека $a \in H \Rightarrow$ от 2) $\Rightarrow a^{-1} \in H \Rightarrow e = a \cdot a^{-1} \in H$ (аксиома 2)
$\Rightarrow a \in H, \exists a^{-1} \in H : aa^{-1} = e$ (акс. 3)

Пример:
$\mathbb{C}_n = \{ x \in \mathbb{C} \mid x^n = 1 \} = \{ \omega_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} \mid k = 0, 1, \dots n-1 \}$
(n-тите корени на 1-цата в комплексни числа)
Ще док. че това е подгрупа на мултипликативната група на комплексните числа.
Док-во: //

$x, y \in \mathbb{C}_n \quad x^n = 1, \ y^n = 1$
$(x \cdot y)^n = x^n \cdot y^n = 1 \Rightarrow x \cdot y \in \mathbb{C}_n$
$(x^{-1})^n = \left(\frac{1}{x}\right)^n = \frac{1}{x^n} = 1 \Rightarrow x^{-1} \in \mathbb{C}_n$
$\Rightarrow \mathbb{C}_n < \mathbb{C}^*$

$\omega_k = \left(\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}\right)^k$ (от Формулата на Моавър)
$\Rightarrow \mathbb{C}_n = \{ 1, \omega_1^1, \omega_1^2, \dots, \omega_1^{n-1} \}$ - циклична група от ред n.

Деф: За симетрична група: //
Нека $M \neq \emptyset$ и $S(M) = \{ \varphi : M \to M \mid \varphi$ - биекция $\}$ $\varphi \circ \psi(x) = \varphi(\psi(x))$ $x \in M$.
$\varphi \circ \psi \in S(M)$ $S(M)$ - симетрична група на множ. M.
$\varphi, \psi, \tilde{\iota} \in S(M)$ - биекции за M, $x \in M$
1) $(\varphi \circ \psi) \circ \tilde{\iota}(x) = (\varphi \circ \psi)(\tilde{\iota}(x)) = \varphi(\psi(\tilde{\iota}(x)))$
2) $\varphi \circ (\psi \circ \tilde{\iota})(x) = \varphi((\psi \circ \tilde{\iota})(x)) = \varphi(\psi(\tilde{\iota}(x)))$
графично: $x \xrightarrow{\tilde{\iota}} \tilde{\iota}(x) \xrightarrow{\psi} \psi(\tilde{\iota}(x)) \xrightarrow{\varphi} \varphi(\psi(\tilde{\iota}(x)))$, $\varphi \circ \psi$

$\Rightarrow$ има асоциативност $(\varphi \circ \psi) \circ \tilde{\iota} = \varphi \circ (\psi \circ \tilde{\iota})$
id - неутрален елемент $\tilde{\iota} d \circ \varphi = \varphi \circ id = \varphi$
т.к. φ - биекция $\Rightarrow \exists \varphi^{-1}$ $\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = id$
$\Rightarrow$ симетрична група за множ. M.
В случай, че M е крайно:
$|M| = n$ - с елементи $M = \{ 1, 2, \dots, n \}$ тогава $\forall$ една биекция $\varphi \in S(M) = S_n$ - симетрична група от степен n.

сл. $\psi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}$ $i_s = \psi(s)$ – пермутация на числата от 1 до n.

$\forall$ пермутация има обратна $\Rightarrow$ броят на елементите в S_n е толкова, колкото са всичките пермутации на числата от 1 до n.

$|S_n| = n!$

$S_2 < S_3 < S_4 < \dots$

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

$\psi \circ \psi \rightarrow$

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

В общия случай операцията композиция (∘) е некомутативна !! (само на 2 и 1 елем е комутативна)

4. Ред на елемент. Циклични групи

Дефиниция Група която се поражда от един свой елемент a, т.е $G = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ – циклична група

$a^k = \underbrace{aaa \dots a}_{k}$, $k > 0$

$a^0 = e$

$a^k = \underbrace{a^{-1}a^{-1} \dots a^{-1}}_{|k|}$ $k < 0$

В адитивен вайс $G = \langle a \rangle = \{ka \mid k \in \mathbb{Z}\}$

$ka = \underbrace{a + a + \dots + a}_{k}$, $k > 0$

$ka = \underbrace{(-a) + (-a) + \dots + (-a)}_{|k|}$, $k < 0$

Пример за циклични групи:

$(\mathbb{Z}_n, +^*) = C_2$, $\mathbb{Z}$ – циклична група порядък от 1 или –1.

G – цикл. група $a \in G$ $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\} < G$

тук