В ОБЩИЯ СЛУЧАЙ ЗА $n \geq 2$ ПОЛУЧАВАМЕ n НА БРОЙ КЛАСА В ЗАВИСИМОСТ ОТ ОСТАТЪЦИТЕ.

$n=2 \Rightarrow$ РАЗБИВАТ СЕ НА ЧЕТНИ И НЕЧЕТНИ

$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$

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

*	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

СЪЩОТО НЕЩО МОЖЕ ДА СЕ ДЕФИНИРА ЗА ВСЕКИ ОТ КЛАСОВЕТЕ ОСТАТЪЦИ ПРИ n - ПРОИЗВОЛНО.

$\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$, $\bar{a} = \{a + kn \mid k \in \mathbb{Z}\}$

$\bar{a} + \bar{b} = \bar{r}$, КЪДЕТО r Е ОСТАТЪКЪТ ОТ $(a+b) : n$

$\bar{a} . \bar{b} = \bar{r_1}$, КЪДЕТО r_1 Е ОСТАТЪКЪТ ОТ $(a.b) : n$

КОРЕКТНОСТ НА ДЕФИНИЦИИТЕ!

Т.К. ДЕФИНИЦИИТЕ ЗАВИСЯТ ОТ ЦЕЛИ МНОЖЕСТВА, ТРЯБВА ДА СЕ ПОДСИГУРИМ, ЧЕ СА ВЕРНИ ЗА КОЙ ДА СЕ Е ЕЛЕМЕНТ.

$a \equiv a_1 (n)$ $\quad a+b \equiv a_1+b_1 (n) \Rightarrow$ ОСТАТЪКЪТ НА $a+b$ И a_1+b_1 ПО МОДУЛ n Е ЕДИН И СЪЩ.
$b \equiv b_1 (n)$

$ab \equiv a_1 b_1 (n) \Rightarrow ab$ И $a_1 b_1$ ДАВАТ ЕДИН И СЪЩИ ОСТАТЪК ПРИ ДЕЛЕНИЕ СЪС n.

$\Rightarrow \bar{a} + \bar{b} = \overline{a+b}$

$\bar{a} . \bar{b} = \overline{ab}$

$\Rightarrow$ В $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots \overline{n-1}\}$ МОЖЕМ ДА ДЕФИНИРАМЕ ОПЕРАЦИИТЕ + И . ТАКА

$\mathbb{Z}_4$

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

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

ГРУПИ

* ЛИНЕЙНО ПРОСТРАНСТВО - АБСТРАКТНО МНОЖЕСТВО, КОЕТО ИЗПЪЛНЯВА РАЗЛИЧНИ ОПЕРАЦИИ.

ГРУПА: МНОЖЕСТВО С ЕДНА БИНАРНА ОПЕРАЦИЯ.

↳ В ОБЩИЯ СЛУЧАЙ НЕ СЕ ИНТЕРЕСУВАМЕ ОТ ОБЕКТИТЕ. АКЦЕНТИРА СЕ ВЪРХУ СЪЩЕСТВУВАНЕТО НА БИНАРНА ОПЕРАЦИЯ.

$M \neq \emptyset \rightarrow$ БИНАРНА ОПЕРАЦИЯ: $\varphi : M \times M \rightarrow M$ - ИЗОБРАЖЕНИЕ НА ВСЯКА ДВОЙКА ЕЛЕМЕНТИ ОТ M СЪПОСТАВЯ ЕЛЕМЕНТ ОТ M.

! СКАЛАРНОТО ПРОИЗВЕДЕНИЕ НА ВЕКТОРИ ДАВА ЧИСЛО $\Rightarrow$ НЕ Е БИНАРНА ОПЕРАЦИЯ!

Опр Група: Нека $G \neq \emptyset$ с бинарна операция (условно $*$), G е група относно тази операция, ако е изпълнено:

1) $(a*b)*c = a*(b*c)$
2) $\exists e \in G : a*e = e*a = a$
3) $\forall a \in G \ \exists b_a \in G : a*b = e$

Пример: $\mathbb{Z}$ с $+$ (Записване $(G,*)$)

$\mathbb{Z}$ с $*$ не е група! $2 . ? = 1$ ↯

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

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ → операцията събиране се разширява

Тези множества ще наречем подгрупи

$\mathbb{Q}$ с $\cdot$ не е група заради нулата!

$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\} \Rightarrow (\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$, където

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$

$\mathbb{Z}^* = \{1, -1\} \Rightarrow (\mathbb{Z}^*, \cdot)$ - крайна подгрупа

$(M_{n\times k}, +)$

→ Дотук във всички случаи имаме комутативна операция.

Опр Групата се нарича комутативна или Абелева, ако $a*b = b*a$.

Опр Ред на групата: броят на елементите на групата.

$M_{n\times n} \rightarrow (AB)C = A(BC)$

$AE = EA = A$

- обратими матрици $- \det A \neq 0$

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

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

$\det(AB) = \det A \cdot \det B \neq 0$

Асоциативността важи за $\forall$

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

$\det A \neq 0 \Rightarrow \det A^{-1} \neq 0 \Rightarrow A^{-1} \in GL(n,F)$

$(GL(n,F), \cdot)$ - обща линейна група от степен n над поле F.

↳ не е комутативна!

Следствия от аксиомите / свойства на всяка група

(1) Обобщена асоциативност

От $(a*b)*c = a*(b*c) \Rightarrow a_1 * a_2 * \ldots * a_n$ → по какъвто и начин да са разположени скобите, резултатът е еднаков.

- ДОКАЗВА СЕ С ИНДУКЦИЯ ПО $n \geq 3$

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

НЕКА $n > 3$ И ДА ДОПУСНЕМ, ЧЕ Е ДОКАЗАНО ЗА $\forall k < n$

$a_1 x \dots * a_n$ С НЯКАКВИ СКОБИ $= \underbrace{(a_1 \dots a_k)}_{f(a_1 \dots a_k)} * \underbrace{(a_{k+1} \dots a_n)}_{g(a_{k+1} \dots a_n)} \overset{\text{ИП}}{=}$

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

$= a_1 * [a_2 \dots a_k] * [a_{k+1} \dots a_n] \overset{\text{ИП}}{=} a_1 * [a_2 \dots a_n] = [a_1 \dots a_n]$

② ЕДИНСТВЕНОСТ НА НЕУТРАЛНИЯ ЕЛЕМЕНТ

ДОПУСКАМЕ, ЧЕ e_1 И e_2 – НЕУТРАЛНИ.

$e_1 * a = a * e_1 = a$; $e_2 * a = a * e_2 = a$

$e_1 * e_2 = \begin{cases} e_1 \\ e_2 \end{cases} \Rightarrow \underbrace{e_1 = e_2}_{e_2} \Rightarrow$ ЕЛЕМЕНТЪТ Е ЕДИНСТВЕН;

$+$ – АДИТИВЕН ЗАПИС

$*$ – МУЛТИПЛИКАТИВЕН ЗАПИС

$+$	$*$	
СУМА	ПРОИЗВЕДЕНИЕ	ОПЕРАЦИЯ
НУЛЕВ	ЕДИНИЧЕН	НЕУТР. ЕЛ.
ПРОТИВОПОЛ.	ОБРАТЕН	$b: a*b = b*a = e$
РАЗЛИКА	ЧАСТНО	ОБРАТНА ОПЕР

③ $\forall a \in G \; \exists ! \, b_a \in G : a*b = b*a = e$

ДОПУСКАМЕ, ЧЕ $\exists \, b_1$ И $b_2 \Rightarrow b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$

$\Rightarrow b_1 \equiv b_2 \equiv b$

④ $\forall a, b \in G \; \exists ! x \in G$ И $\exists ! y \in G : a*x = b$ И $y*a = b$

ДОКАЗАТЕЛСТВО:

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

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

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

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

$a * (a^{-1} * b) \overset{?}{=} b \to (a * a^{-1}) * b = b$

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

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

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

В ОБЩИЯ СЛУЧАЙ $x \neq y$.

⑤ ОТ ОБОБЩЕНАТА АСОЦИАТИВНОСТ

$\underbrace{a*a*\ldots*a}_{k\text{ ПЪТИ}} = a^k$ ПРИ МУЛТИПЛИКАТИВЕН ЗАПИС

$a^k . a^s = a^{k+s}$

$(a^k)^s = a^{k.s}$

$(ab)^k = \underbrace{abab\ldots ab}_{k\text{ ПЪТИ}}$! НЯМА ГО СВОЙСТВОТО $(ab)^k = a^k b^k$

ПРИ АДИТИВЕН ЗАПИС

$\underbrace{a+a+\ldots+a}_{k\text{ ПЪТИ}} = ka$ (k-КРАТНО НА ЕЛЕМЕНТА a)

$ka+sa=(k+s)a$ } В ОБЩИЯ СЛУЧАЙ a Е ЕЛЕМЕНТ НА ГРУПАТА,
$s(ka)=(sk)a$ } А k И s СА $\mathbb{N}$.

! НЕ Е ДИСТРИБУТИВНОСТ И АСОЦИАТИВНОСТ !

Опр $(G,\circ)$: H СЕ НАРИЧА ПОДГРУПА НА G, АКО H Е ГРУПА ОТНОСНО ОПЕРАЦИЯТА В G И $H \subset G$. ! ОПЕРАЦИЯТА Е БИНАРНА !

$H \leqq G$; $\{e\} \leqq G$; $G \leqq G$; $(\mathbb{Z},+) \leqq (\mathbb{Q},+) \leqq (\mathbb{R},+) \leqq (\mathbb{C},+)$.

Тв НЕКА $H \neq \emptyset$ И $H \subset G$; $H \leqq G \Leftrightarrow$ $\begin{cases} (1) ab \in H, \forall a,b \in H \\ (2) a^{-1} \in H, \forall a \in H. \end{cases} \Rightarrow \begin{cases} ab^{-1} \in H \\ \forall a,b \in H \end{cases}$

Доказателство:

$H < G \Rightarrow ab \in H \Rightarrow$. Е БИНАРНА И ЗА H

$a^{-1} \in H$ ОТ 3-ТА АКСИОМА

В ОБРАТНА ПОСОКА

ОПЕРАЦИЯТА Е БИНАРНА ЗА H

$(ab)c = a(bc)$ ВАЖИ ЗА $G \Rightarrow$ ВАЖИ И ЗА H

ОТ 3-ТА АКСИОМА:

$a \in H \Rightarrow$ ОТ 2) $\Rightarrow a^{-1} \in H \Rightarrow e = a.a^{-1} \in H \Rightarrow$ ИМАМЕ АКСИОМА 2.

$\forall a \in H \Rightarrow a^{-1} \in H : a.a^{-1} = e \Rightarrow$ ИЗПЪЛНЕНА Е 3-ТА АКСИОМА.

Примери за подгрупи

① $(\mathbb{C}^*,\cdot) \rightarrow C_n = \{x \in \mathbb{C} \mid x^n = 1\} = \{\omega_k = \cos\frac{2\pi k}{n} + \sin\frac{2\pi k}{n} \mid k = \overline{0,n-1}\}$

$x,y \in C_n : x^n = 1, y^n = 1$

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

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

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

$\omega_0 = 1$

$\omega_1 \dots \omega_{n-1}$

$\omega_1^n = \omega_1^0$ → ЗАТВАРЯ СЕ ЦИКЪЛА → ЦИКЛИЧНА ГРУПА

$(C_n, \cdot)$ – ЦИКЛИЧНА ГРУПА ОТ РЕД n.

② СИМЕТРИЧНА ГРУПА НА МНОЖЕСТВО M

$M \neq \emptyset$

$S(M) = \{\varphi : M \to M \mid \varphi$ – БИЕКЦИЯ$\}$

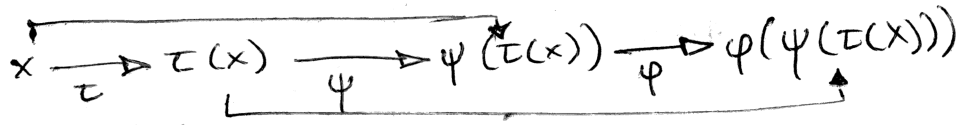
$\varphi \circ \psi(x) = \varphi(\psi(x)), \forall x \in M$

$\varphi \circ \psi \in S(M)$ → СИМЕТРИЧНА ГРУПА ЗА МНОЖЕСТВОТО M

$\varphi, \psi, \tau \in S(M)$

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

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



КОМПОЗИЦИЯТА НА ИЗОБРАЖЕНИЯ ПО ПРИНЦИП Е БИЕКТИВНА.

$e = id$

φ – БИЕКЦИЯ $\Rightarrow \exists \varphi^{-1} : \varphi \circ \varphi^{-1} = id$

КОГАТО M Е КРАЙНО МНОЖЕСТВО С n ЕЛЕМЕНТА $\Leftrightarrow M = \{1, 2 \dots n\}$

$\varphi \in S(M) = S_n$ – СИМЕТРИЧНА ГРУПА ОТ СТЕПЕН n.

$\varphi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}$ → ПЕРМУТАЦИЯ НА $\{1 \dots n\} \Rightarrow |S_n| = n! = P_n$

$i_s = \varphi(s)$

↳ ЕЛЕМЕНТИТЕ НА S_n НОЩЕМ ДА НАРИЧАМЕ ПЕРМУТАЦИИ/СУБСТИТУЦИИ

$S_2 < S_3 < S_4 < S_5 \dots$

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{matrix} \psi \curvearrowright \\ \varphi \curvearrowright \end{matrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

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

В ОБЩИЯ СЛУЧАЙ КОМПОЗИЦИЯТА НЕ Е КОМУТАТИВНА.