

## АЛГЕБАРСКЕ СТРУКТУРЕ

(1)

- Постоји скуп с неким операцијама.
- Def. Нека је  $A$  непразан скуп и  $n \in N \setminus \{0\}$ . Алгебарска операција  $f$  дужине  $n$  или  $n$ -арна
- операција је свако пресликавање  $f: A^n \rightarrow A$ .
- пишемо  $\#(f) = n$  - дужина операције је  $n$
- $A^n = A \times A \times \dots \times A$  - скуп свих уређених  $n$ -торки из  $A$

$n=2$  БИНАРНЕ ОПЕРАЦИЈЕ, уместо  $f(a, b)$  пишемо  $a f b$   
 $n=1$  УНАРНЕ ОПЕРАЦИЈЕ  
 $n=0$  КОНСТАНТЕ,  $A^0 = \{\star\}$  - једночлански,  $f(\star) = a$   $\xrightarrow{\text{КОНСТАНТА}}$

примери: операције:

- сабирање, множење на  $N, Z, Q, R, C$
- одузимање чије је операција над  $N$ , над осталим јесте
- дељење чије је операција над  $N, Z, Q, R, C$ , али јесте над  $Q \setminus \{0\}, R \setminus \{0\}, C \setminus \{0\}$
- НЗД је операција над  $N$ , пишемо НЗД( $a, b$ )
- нека је  $X$  непразан скуп; што су  $n, U, \cap, \Delta$  операције над  $P(X)$
- $M_n(R)$  множење матрица
- $M_{m,n}(R)$  сабирање матрица
- $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$  - за  $m \in \mathbb{Z}$  и  $n \in N$  са  $f(m, n)$  дефинишемо

оставшак при дељењу  $m$  са  $n$  (он је јединствен);  $m = nq + r$ ,  $0 \leq r < n-1$ ,  
 и што  $f(m, n) = r$ ; што на  $\mathbb{Z}_n$  дефинишено операције  $+_n$  и  $\cdot_n$

$$(\text{за } a, b \in \mathbb{Z}_n) \text{ са: } \begin{aligned} a +_n b &= f(a+b, n) \\ a \cdot_n b &= f(ab, n) \end{aligned}$$

- ово су све бинарне операције (секундарне, која је унарна)

Def. Алгебарска структура је уређена  $(n+1)$ -торка  $A = (A, f_1, f_2, \dots, f_n)$ , где је  $A$  непразан скуп, а  $f_1, f_2, \dots, f_n$  операције на  $A$  па  $\#(f_i) \geq \#(f_{i+1})$  за  $1 \leq i \leq n-1$ . За  $A$  кажемо да је носач алгебарске структуре  $A$ .

КОМЕНТАР: Када је јасно из контекста (тешко увек) нећемо правити разлику између  $A$  и  $A$ , тако да ћемо писати (искако је формално неистрајено) „ $a \in A$ “ или „ $A$  је алгебарска структура“.

- пример:
- $(N, +, \cdot, 1)$  је алгебарска структура.
  - $(N, -, 2)$  није,  $(N, +, 2)$  јесте.
  - $(P(X), \cap, \cup, \subset, \emptyset)$  јесте.

## ГРУПЕ

**деф.** Алгебарска структуре  $(G, \cdot)$  је група ако је • бинарна операцija на  $G$ , тј. ванци:

a)  $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \forall a, b, c \in G$  - асоцијативност

b)  $(\exists e \in G) e \cdot a = a \cdot e = a, \forall a \in G$

c)  $(\forall a \in G) (\exists \bar{a} \in G) a \cdot \bar{a} = \bar{a} \cdot a = e$

**КОМЕНТАР:** Група је алгебарска структуре  $(G, \circ, +, e)$  тј. ванци a), уместо b) ванци b':

$a \cdot e = e \cdot a = a, \forall a \in G$ , а уместо c) ванци b'):  $a \cdot \bar{a} = \bar{a} \cdot a = e, \forall a \in G$ .

**КОМЕНТАР:** За елемент a је нейтрал групе, док за елемент a ћемо да је инверз елемента a.

① Нейтрал у групи је јединствен.

**доказ:** ПКС. Нека су e и f нейтрали. e је нейтрал  $\Rightarrow f \cdot e = e \cdot f = f$ .

f је нейтрал  $\Rightarrow e \cdot f = f \cdot e = e$ . Закле,  $e = f$ .

② За сваки елемент a групе G његова инверз је јединствен.

**доказ:** Нека  $\bar{a}$  и  $\tilde{a}$  задовољавају б), тј.  $\begin{cases} a \cdot \bar{a} = \bar{a} \cdot a = e \\ a \cdot \tilde{a} = \tilde{a} \cdot a = e \end{cases}$

Посматрајмо  $\begin{cases} \bar{a} \cdot (a \cdot \tilde{a}) \stackrel{b)}{=} \bar{a} \cdot e \stackrel{e)}{=} \bar{a} \\ (\bar{a} \cdot a) \cdot \tilde{a} \stackrel{b)}{=} e \cdot \tilde{a} \stackrel{e)}{=} \tilde{a} \end{cases} \Rightarrow \bar{a} = \tilde{a}$

**ПРИМЕР:** a) - на  $\mathbb{Z}$  није асоцијативна операцija

$$(1-2)-3 \neq 1-(2-3)$$

+ када је јасно о којој операцији се ради, често уместо a · b пишемо ab; често уместо „група  $(G, \cdot)$ “ квантитет „група G“

б)  $(\mathbb{Z}, +)$  је група, 0 је нейтрал, -n је инверз за n

$(\mathbb{N}, +)$  није група,  $0 \notin \mathbb{N}$

в)  $(M_n(\mathbb{R}), \cdot)$  није група, међутим  $(GL_n(\mathbb{R}), \cdot)$  је још група.

инвертибилне матрице

•  $(GL_n(\mathbb{R}), +)$  није група  
(није алгебарска структура)

$$(AB)^{-1} = B^{-1}A^{-1}$$

г)  $(M_{m,n}(\mathbb{R}), +)$  је још група.

$$A^{\wedge} = \{f: A \rightarrow A \mid f \text{ ф-ја}\}$$

$$\text{id}_A: A \rightarrow A \quad \text{id}_A(x) = x$$

$(A, \cdot)$  <sup>кохизијура</sup> није група;

нека инверз, сепак је бујекција

! д)  $(\mathbb{Z}_n, +_n)$  је још група

$+_n$  је асоцијативан (1.1. задатак)

нейтрал је 0

инверз  $a \in \mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$  је  $n-a$  сепак за  $a=0$  (инверз 0)

e)  $(\mathbb{Z}_n, \cdot_n)$  - чије је група; <sup>за  $n \geq 2$</sup>  о нека инверз

iii)  $(\mathbb{Q} \setminus \{0\}, \cdot)$  - јесме група

### ОСОБИНЕ ГРУПА

• Нека је  $(G, \cdot)$  група. За  $x_1, x_2, \dots, x_n \in G$  дефинишено  $\prod_{i=1}^n x_i$  индуктивно са:

$$a) \prod_{i=1}^1 x_i = x_1$$

$$b) \prod_{i=1}^n x_i = \prod_{i=1}^{n-1} x_i \cdot x_n$$

• уместо  $\prod_{i=1}^n x_i$  пишемо  $(x_1 \cdots x_n)$

$$+ \quad \prod_{i=1}^n x_i = \prod_{i=1}^n x_i \cdot x_n = (\prod_{i=1}^{n-1} x_i \cdot x_n \cdot x_n) = ((x_1 \cdot x_2) \cdot x_3) \cdot x_4 +$$

т) Нека су  $x_1, \dots, x_n, x_{n+1}, \dots, x_{n+m} \in G$ . Плана ванши:

$$\prod_{i=1}^n x_i \cdot \prod_{i=n+1}^m x_i = \prod_{i=1}^m x_i, \text{ тј. } (x_1 \cdots x_n)(x_{n+1} \cdots x_{n+m}) = (x_1 \cdots x_{n+m})$$

доказ: Индукцијом по  $m \geq 1$ .

БАЗА:  $m=1$  по дефиницији ✓

ИК:  $m \rightarrow m+1$

$$\begin{aligned} \text{Ванши: } (x_1 \cdots x_n)(x_{n+1} \cdots x_{n+m+1}) &\stackrel{\text{деф.}}{=} (x_1 \cdots x_n)((x_{n+1} \cdots x_{n+m}) \cdot x_{n+m+1}) \\ &\stackrel{\text{осав.}}{=} ((x_1 \cdots x_n)(x_{n+1} \cdots x_{n+m})) \cdot x_{n+m+1} \\ &\stackrel{\text{их}}{=} (x_1 \cdots x_{n+m}) \cdot x_{n+m+1} \\ &\stackrel{\text{деф.}}{=} (x_1 \cdots x_{n+m+1}) \end{aligned}$$

КОМЕНТАР: Ово јављање доказује да у сваког изразу затраже јошено изосављањем на произвљен начин. Због тога, затраже се још и изосављаш.

• специјално: За  $x_1 = x_2 = \dots = x_n = x$ , уместо  $\prod_{i=1}^n x_i$  пишемо  $x^n$ .

дев. За бинарну операцију  $*$  на  $A$  кажемо да је комутативна ако за свако  $a, b \in A$  ванши:

$$a * b = b * a.$$

т) Нека је  $(G, \cdot)$  група тј. је  $\cdot$  комутативна операција. Плана за  $x_1, \dots, x_n \in G$  и  $i_1, i_2, \dots, i_n \in \mathbb{N}$  тј.  $\{i_1, i_2, \dots, i_n\} = \{1, 2, \dots, n\}$  ванши:  $x_{i_1} \cdot x_{i_2} \cdots x_{i_n} = x_{i_1} \cdot x_{i_2} \cdots x_{i_n}$ .

доказ: Индукцијом по  $n \geq 1$ .

БАЗА:  $n=1$  привидјално ✓

ИК:  $n \rightarrow n+1$

Нека је  $i_{n+1} = k$ . Плана је  $\{i_1, \dots, i_n\} = \{1, \dots, k-1, k+1, \dots, n+1\}$ , па је по их:

$$\begin{aligned} x_{i_1} \cdots x_{i_{n+1}} &= x_{i_1} \cdots x_{k-1} \cdot x_k \cdot x_{k+1} \cdots x_{n+1} \cdot x_k = x_{i_1} \cdots x_{k-1} \underbrace{((x_{k+1} \cdots x_{n+1}) \cdot x_k)}_{a} \\ &\stackrel{\text{комут.}}{=} x_{i_1} \cdots x_{k-1} (x_k \cdot (x_{k+1} \cdots x_{n+1})) \\ &= x_{i_1} \cdots x_{k-1} \cdot x_k \cdot x_{k+1} \cdots x_{n+1} \end{aligned}$$

• Инерзни елементи означавају са  $x^{-1}$  ( $= \bar{x}$ ).

+ •  $x^0 = e$   
 $x^{-1}$  је инверз од  $x$   $x^{-n} = (x^{-1})^n$  за  $n \geq 1$

⊕ У групи  $(G, \cdot)$  за  $x, y \in G$  вали:

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

доказ: a) Како је  $x \cdot x^{-1} = x^{-1} \cdot x = e$ , због јединствености инверза,  $x$  је инверз од  $x^{-1}$ .

$$(x^{-1})^{-1} = x$$

b) Слично,  $(xy)^{-1} = y^{-1}x^{-1} \rightarrow xy \cdot y^{-1}x^{-1} \stackrel{(*)}{=} xx^{-1} \stackrel{(*)}{=} e$  и  $y^{-1}x^{-1}xy = \dots = e$ .

• Из б) индукцијом следи  $(x_1 \cdots x_n)^{-1} = x_n^{-1} \cdots x_1^{-1}$  (\*).

• За  $n \geq 1$ , сада дефинишено  $x^{-n} = (x^n)^{-1} \stackrel{(*)}{=} (x^{-1})^n$ ,  $x^0 = e$

⊕ За  $a, x, y \in G$  вали:  $a \cdot x = a \cdot y \Rightarrow x = y$ .

доказ:  $\frac{a^{-1}}{a} \cdot a \cdot x = a^{-1} \cdot a \cdot y \Rightarrow e \cdot x = e \cdot y \Rightarrow x = y$

12 (Чисто вали и због  $x^0 = e$ )

⊕ Нека је  $G$  група и  $a, b \in G$ . Тада једначина  $ax = b$  има јединствено решење.

доказ: Из  $ax = b$  следи:  $a^{-1}ax = a^{-1}b \Rightarrow x = a^{-1}b$ . Закле, постоји највише једно решење и то поштенцијално решење је  $x = a^{-1}b$ . Ако јесте решење, јер вали  $a(a^{-1}b) = ab = b$ .

⊕ Нека је  $G$  група,  $a, b \in G$  и  $n \in \mathbb{N}$ . Тада је:  $(aba^{-1})^n = ab^n a^{-1}$ .

доказ: 1 индукцијом по  $n$

2 директно: вали  $(aba^{-1})^n = \underbrace{aba^{-1} \underline{aba^{-1}} \cdots}_{e} \underbrace{aba^{-1}}_{e} = abeb \cdots ebba^{-1} = \underbrace{abeb \cdots ebba^{-1}}_n = ab^n a^{-1}$

⊕ Нека је  $G$  група,  $x \in G$  и  $m, n \in \mathbb{Z}$ . Тада вали:

- 1)  $x^{m+n} = x^m \cdot x^n$
- 2)  $x^{mn} = (x^m)^n$

доказ: 1 Ако је  $m=0$  или  $n=0$ , тврђење лако следи.

I 2 Нека су  $m, n > 0$ . Тада је  $x^{m+n} = \underbrace{x \cdot x \cdots x}_{m+n} = \underbrace{x \cdots x}_{m} \cdot \underbrace{x \cdots x}_{n} = x^m \cdot x^n$

3 Нека је  $m > 0, n > 0$ .

3.1.  $m+n > 0$ . Тада је  $x^{m+n} = \underbrace{x \cdots x}_{m+n}$ . Такође,  $x^m \cdot x^n = \underbrace{x \cdots x}_{m} \cdot \underbrace{x^{-1} \cdot x^{-1} \cdots x^{-1}}_{-n}$

$$\begin{aligned} &= \underbrace{x \cdots x}_{m+n} \cdot \underbrace{x \cdots x}_{-n} \cdot \underbrace{x^{-1} \cdots x^{-1}}_{-n} \\ &= x^{m+n} \end{aligned}$$

3.2.  $m+n < 0$ . Слично као 3.1.

4 Нека је  $m < 0, n > 0$ . Слично као 3.

\* доказ

затворени

1.8.

2ес

ПРИМЕ  
бес

кон

5 Нека су  $m, n < 0$ .  $x^{m+n} = (x^{-1})^{-m-n} = (x^{-1})^m \cdot (x^{-1})^{-n} = x^m \cdot x^n$ .

II Ако је  $m=0$  или  $n=0$ , тврђење лако следи.

$$1 m, n > 0: \text{Ваша } x^{mn} = \underbrace{x \cdots x}_{mn} = \underbrace{\underbrace{x \cdots x}_m \cdot \underbrace{x \cdots x}_m \cdots \underbrace{x \cdots x}_m}_n = \underbrace{x^m \cdot x^m \cdots x^m}_n = (x^m)^n$$

$$2 m > 0, n < 0: \text{Ваша } (x^m)^n = ((x^m)^{-n})^{-1} = (x^{-mn})^{-1} = x^{mn}$$

3 и 4: слично као 2

### ПРИМЕРИ ГРУПА

• Постматрато (за дајуо  $n \in \mathbb{N}$ ):  $C_n = \{z \in \mathbb{C} \mid z^n = 1\}$

$$\text{нпр. } C_2 = \{-1, 1\}, C_4 = \{1, -1, i, -i\}, C_3 = \{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\}$$

Решимо  $z^n = 1$  у  $\mathbb{C}$ . Представљамо  $z = r(\cos \varphi + i \cdot \sin \varphi)$ ,  
тада је  $r \in \mathbb{R}$ ,  $r \geq 0$ , а  $\varphi \in [0, 2\pi]$ . Следи:  $z^n = r^n(\cos n\varphi + i \cdot \sin n\varphi) = 1$ ,  
 $\Rightarrow r^n = 1$  и  $n\varphi = 2k\pi$ , за неке  $k \in \mathbb{Z}$ .

Цо што,  $n\varphi \in [0, 2k\pi]$ , тада је  $n\varphi = 2k\pi$  за неко  $k \in \{0, 1, \dots, n-1\}$ . Закле,  $\varphi = \frac{n}{n}$ .

$$C_n = \left\{ \cos \frac{2k\pi}{n} + i \cdot \sin \frac{2k\pi}{n} \mid 0 \leq k \leq n-1 \right\}.$$

\*  $C_n$  у односу на умножење комплексних бројева је група.

$$\text{ДОКАЗ: Важи: } (\cos \frac{2k\pi}{n} + i \cdot \sin \frac{2k\pi}{n})(\cos \frac{2l\pi}{n} + i \cdot \sin \frac{2l\pi}{n}) = \cos \frac{2(k+l)\pi}{n} + i \cdot \sin \frac{2(k+l)\pi}{n} \in C_n$$

затвореност

$$\text{АСОЦИЈАТИВНОСТ: } \checkmark \quad (z_1 z_2) z_3 = z_1 (z_2 z_3)$$

$$\text{НЕУТРАЛ: } 1 = \cos 0 + i \cdot \sin 0$$

$$\text{ИНВЕРЗ: } \cos \frac{2(n-k)\pi}{n} + i \cdot \sin \frac{2(n-k)\pi}{n} \text{ за } k \neq 0, \text{ а иначе за } k=0 \text{ је } 1.$$

• Означимо:  $\varepsilon = \cos \frac{2\pi}{n} + i \cdot \sin \frac{2\pi}{n}$ . Тада је  $C_n = \{\varepsilon^k \mid 0 \leq k \leq n-1\}$ . Јасно,  $\varepsilon^n = 1$ , па је и  $\varepsilon^m \in C_n$  за свако  $m \in \mathbb{Z}$ . ( $m = nq+r$ ,  $0 \leq r \leq n-1$ ,  $\varepsilon^m = \varepsilon^r$  (модул))

### ЦИКЛИЧНЕ ГРУПЕ

1.8.

ДЕФ. Група  $G$  је циклична ако постоји елемент  $x \in G$  тд.  $G = \{x^m \mid m \in \mathbb{Z}\}$ . Тада за  $x$

којемо да је ГЕНЕРАТОР ГРУПЕ  $G$ .

ПРИМЕР: 1)  $(C_n, \cdot)$  је циклична.

БЕСКОНАЧНЕ

2)  $(\mathbb{Z}_n, +)$  је циклична. Генератор је 1 (сваки елемент можемо добити  
сабирањем јединице "1" по горњој  
деф.)

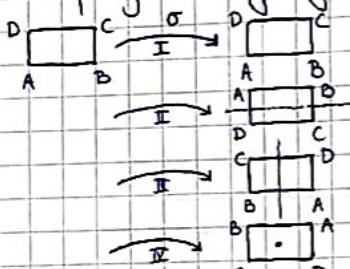
КОНАЧНА 3)  $(\mathbb{Z}, +)$  је циклична група. Генератор је 1 (или -1).

4)  $(\mathbb{Q}, +)$  није циклична група. (Из  $\frac{p}{q} \cdot m$  не можемо добити  $\frac{1}{q+1}$ )

## ГРУПЕ ФОРМИРАНЕ ОД СИМЕТРИЈА

- Нека је  $F$  фигура у равни. Посташтрано скуп:  $S(F) = \{\sigma: \mathbb{R}^2 \rightarrow \mathbb{R}^2 | \sigma \text{ је симетрија}$  од  $F\}$
- трансформације равни које чувају распољавања и притом не промењају фигуру  $F$
- $(S(F), \circ)$  је група.
  - композиција - доказ следи из тврђења да је композиција симетрија симетрија!
  - нутријал: јд инверз:  $\varphi^{-1}$  + континуитет је резултат

примери: I  $F$  = правоугаоник који није квадрат



$$\sigma = id$$

осна симетрија  $\sigma_1$

осна симетрија  $\sigma_2$

централна симетрија  $s$

- Група симетрија  $V = \{id, \sigma_1, \sigma_2, s\}$ .

\* Кејлијеве таблице групе  $V$  (таблица којој је приказана операција у коначној групи):

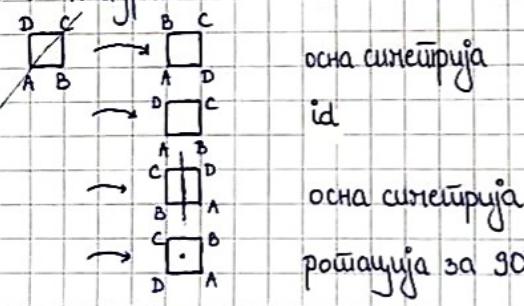
$$\begin{array}{c}
 id \quad \sigma_1 \quad \sigma_2 \quad s \\
 id \quad id \quad \sigma_1 \quad \sigma_2 \\
 \sigma_1 \quad \sigma_1 \quad id \quad s \quad \sigma_2 \\
 \sigma_2 \quad \sigma_2 \quad s \quad id \quad \sigma_1 \\
 s \quad s \quad \sigma_2 \quad \sigma_1 \quad id
 \end{array}$$

симетрија у односу на главну дијагоналу ( $\Leftrightarrow$  група је континуална)

1.5.  
2.еф

пример:

II  $F$  = квадрат



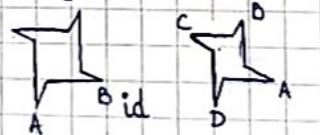
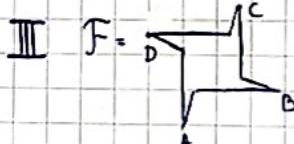
осна симетрија

id

осна симетрија

ротација за  $90^\circ$

укупно 8 симетрија квадрата



ротација за  $90^\circ$

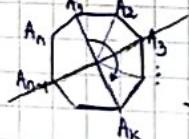
III  $F$  =

$$\{id, \rho_{90^\circ}, \rho_{180^\circ}, \rho_{270^\circ}\} = \{id, \rho_{90^\circ}, \rho_{90^\circ}, \rho_{90^\circ}\}$$

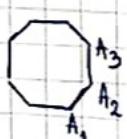
циклична група

## ДИЕДАРСКЕ ГРУПЕ

- Диедарска група, у означи  $D_n$ , је група симетрија правилног  $n$ -шојла.



Нека се  $A_1$  слика на месту  $A_k$ . Пишемо  $A_1 \mapsto A_k$ . Тада  $A_2 \mapsto A_{k-1}$ , или  $A_2 \mapsto A_{k+1}$ .



У првом случају,  $A_3 \mapsto A_{k+2}$ , а у другом  $A_3 \mapsto A_{k-2}$ , па је у првом случају пресликавате

ротација за  $\frac{2\pi(k-1)}{n}$  око 0, а у другом оси симетрија. Закле,  $|D_n| = 2n$ . Означимо са  $\beta$  ротацију за  $\frac{2\pi}{n}$  око 0, а са  $\sigma$  осну симетрију кроз симетралу дужи  $A_1A_2$ .

Плаже  $D_n = \{\underbrace{\text{id}, \beta, \beta^2, \dots, \beta^{n-1}}_{\text{проверити да ли су ово све осне симетрије (јесу)}}, \underbrace{\sigma, \sigma\beta, \sigma\beta^2, \dots, \sigma\beta^{n-1}}\}$

- Ванци  $\beta^n = \text{id}$ ,  $\sigma^2 = \text{id}$ .

$$\beta \cdot \beta^{n-1} = \beta^{n-2} = \beta^n \cdot \beta^2 = \beta^2$$

$\sigma\beta = \sigma\beta^{n-1}$  (провера геометријски)

$$\sigma\beta^i \sigma\beta^j = \underbrace{\sigma\beta\beta\cdots\beta\sigma}_{\text{i}} \sigma\beta^j = \sigma\beta\beta\cdots\beta\sigma\beta^j = \sigma\beta\sigma\beta^{n-1}\beta^j = \sigma\beta\beta^2 = \underbrace{\sigma\beta\beta^{n-1}\beta^j}_{\beta} = \beta$$

- Ванци:  $\beta^i\sigma = \sigma\beta^{n-i}$  (за бекбу; доказ индукцијом по  $i$ )

- ова група није комутативна ( $\beta\sigma \neq \sigma\beta$ ); цикличне јесу комутативне ( $x^m \cdot x^n = x^n \cdot x^m$ )

## ПОДГРУПЕ

1.5.

Def. Ако су  $(G, \cdot)$  и  $(H, *)$  групе, онда је  $(H, *)$  подгрупа групе  $(G, \cdot)$  ако ванци:

$$H \subseteq G \text{ и } x * y = xc \cdot y \text{ за све } x, y \in H$$

(нпр.  $(R, +)$ ,  $(Q, +)$ )

- пишемо  $(H, *) \leq (G, \cdot)$  или  $H \leq G$

приимер: 1)  $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$

$$2) (C_n, \cdot) \leq (C \setminus \{0\}, \cdot)$$

$$3) (\mathbb{Z}_n, +_n) \not\leq (\mathbb{Z}, +)$$

- ОСОБИНЕ:

I Нека је  $H \leq G$ . Плаже: I неутрални у  $H$  и  $G$  су једнаки

$$(H, *) \leq (G, \cdot) \quad \text{II за све } H \text{ његови инверзи у } H \text{ и } G \text{ су једнаки}$$

ДОКАЗ: I Нека је  $\epsilon$  неутрал у  $H$  и  $e$  неутрал у  $G$ . За сви  $a \in H$  имамо  $a * \epsilon = a$ . / $a^{-1}$ /,  $a * \epsilon \xrightarrow{a^{-1}}$

тје је  $a^{-1}$  инверз од  $a$  у  $G$ .

$$a^{-1} \cdot (a * \epsilon) = a^{-1} \cdot a = e \quad \Rightarrow e = \epsilon$$

$$e * \epsilon = \epsilon \quad \text{тје неутрал за.}$$

II Нека је  $\bar{x}$  инверз од  $x$  у  $H$ , а  $\tilde{x}$  инверз од  $x$  у  $G$ . Плаже  $x * \bar{x} = \bar{x} * x = \epsilon$  / $\bar{x}$ /,  $x * \bar{x} \xrightarrow{x \cdot \bar{x}} \bar{x} \cdot x = \epsilon$ , па је

$\bar{x} = \tilde{x}$  због јединствености инверза.

СТАВ: Нека је  $(G, \cdot)$  група. За пресликавање  $*: H \times H \rightarrow G$  (тје је  $H \subseteq G$ ) кажемо да је ресурсија операције • ако је  $x * y = xc \cdot y$  за све  $x, y \in H$ .

СТАВ: Непразан подскуп  $H$  групе  $G$  је подгрупа од  $G$  у односу на ресурсију операције из  $G$  ако за све  $x, y \in H$  ванци:  $xc \cdot y^{-1} \in H$  (израз  $xc \cdot y^{-1}$  „рачувано“ у  $G$ ).  
(твад симетрична при услова за подгрупу)

(P3)

**СТАГ:** Нека је  $G$  група и  $H \leq G$  подгрупа групе  $G$  у односу на ресартикују операције из  $G$ .  
Ако  $xy \in H$  за све  $x, y \in G$  ( $xy^{-1}$  рачувано у  $G$ ).

**ДОКАЗ:** Нека је  $(G, *)$  група и  $*$  ресартикују операције на  $H$ .

→ Закле,  $(H, *) \leq (G, *)$ . Нека су  $x, y \in H$ . Падаје  $y^{-1}$  инверз од  $y$  у  $H$ , па је  $xy^{-1} = x * y^{-1} \in H$ .  
↔ Сада доказујемо да је  $(H, *) \leq (G, *)$ . Већ бачни  $x * y = xy^{-1}$  односно сино десничани за  $x, y \in H$ .

1°  $*$  је операција на  $H$  - доказујемо да за  $x, y \in H$  вали  $x * y = xy \in H$ .  
За то је добијено доказаш идентичност  $y \in H \Rightarrow y^{-1} \in H$ , јер пада идентично  $xy \in H \Rightarrow xy^{-1} \in H$ , па је  $xy = xy^{-1} = xy \in H$ .

За идентичност  $y \in H \Rightarrow y^{-1} \in H$  ~~је добијено доказаш~~ је добијено доказаш  $e \in H$ , јер је што:  
 $y \in H \Rightarrow e * y = y^{-1} * y = e$ . Узимамо промењавање  $x \in H$  (оно постади јер је  $H \neq \emptyset$ ). Пада из  $x * x^{-1} = e \in H$ , чиме је доказ завршен.

2°  $(H, *)$  је група

$A: x * (y * z) = x * (y \cdot z) = (x \cdot y) \cdot z = (x * y) * z$ , ај.  $*$  је асоцијативна на  $H$ .  
 $x, y, z \in H$

$H: x \in H: x * e = x \cdot e = e * x = x$ , јер је  $e$  неутрални  $H$

$H: x \in H: \text{Падаје } x^{-1} \in H \text{ и вали } x * x^{-1} = x \cdot x^{-1} = x^{-1} \cdot x = x^{-1} * x = e$ , јер је  $x^{-1}$  инверз од  $x \in H$ .

**СТАГ:** Ако су  $H$  и  $K$  подгрупе групе  $G$ , падаје и  $H \cap K$  подгрупа од  $G$ .

**ДОКАЗ:** Користимо прештодни сабља.

1°  $H \cap K \neq \emptyset \quad e \in H, K, \text{ па } e \in H \cap K$

2°  $x, y \in H \cap K \Rightarrow xy^{-1} \in H \cap K$

$x, y \in H \cap K \Rightarrow x \in H$  и  $y \in K$ . Из прештодног сабља следи  $xy^{-1} \in H$  и  $xy^{-1} \in K$ , па је озабеже  $xy^{-1} \in H \cap K$ .

**КОМЕНТАР:** Ако је  $H, K \leq G$ , падаје  $H \cup K \leq G$  једино ако је  $H \subseteq K$  или  $K \subseteq H$ .

**Деф.** Нека је  $G$  група и  $S \subseteq G$ . Пада са  $\langle S \rangle$  означавају минималну подгрупу (у односу на инклузију) која садржи  $S$ . За  $\langle S \rangle$  кажемо да је подгрупа ГЕНЕРИСАНА СА  $S$ .

• Вали  $\langle S \rangle = \bigcap_{\substack{H \leq G \\ S \subseteq H}} H$ ; подгрупа је због сабља 1.7.

•  $\langle S \rangle = \{a_1 a_2 \dots a_n \mid n \in \mathbb{N}, a_i \in S\}$ , тј.  $\langle S \rangle = \{x^{-1} \mid x \in S\}$

**Сабља:** Користимо сабља 1.6.  $a_1 \dots a_n (b_1 \dots b_m)^{-1} = a_1 \dots a_n b_m^{-1} \dots b_1^{-1}$

$$\begin{aligned} a_i, b_j \in S &\Rightarrow a_i^{-1} \in S \text{ и } b_j^{-1} \in S \\ \text{ај. } S^{-1} &= \{a_i^{-1} \mid a_i \in S\} \\ b_j \in S^{-1} &\Rightarrow b_j^{-1} \in S \end{aligned}$$

пример: 1)  $S = \{x\}$

$\langle S \rangle = \{x^k \mid k \in \mathbb{Z}\}$  - циклична група генерирана са  $x$

2)  $D_n = \langle f, \sigma \rangle$

РЕД ЕЛЕМЕНТА И РЕД ГРУПЕ

дефиниција: Ако је група  $G$  коначна, тада је њен ред једнак  $|G|$ . Ако је  $G$  бесконачна, тада је БЕСКОНАЧНОГ РЕДА.

• Нека је  $a$  елемент групе  $G$ . Тада је ред од  $a$  у означујући  $w(a)$  најмање  $n \in \mathbb{N}$  ако  $a^n = e$

(ако постоји). Ако обаље  $n \in \mathbb{N}$  не постоји, тада је  $a$  бесконачног реда.

пример: 1)  $(\mathbb{Z}_n, +_n)$   $w(1) = n$  2)  $(D_n, \circ)$   $w(f) = n$ ,  $w(\sigma) = 2$

3)  $(G, \cdot)$   $w(e) = 1$   $w(x) = 1$  ако  $x = e$  4)  $(\mathbb{Z}, +)$  свако  $n \neq 0$  је бесконачног реда

1.10 СТАВ: Ред на који елемент једнак је реду подгрупе коју ствара елемент генерише.

доказ: Нека је  $G$  група и  $x \in G$ . Доказујемо да ватни:

1) Ако је  $x$  коначног реда, тада је  $w(x) = 1 < \infty \rangle$

2) Ако је  $x$  бесконачног реда, тада је и  $\langle x \rangle$  бесконачног реда.

1): Нека је  $w(x) = n$ . Доказујемо да ватни  $\langle x \rangle = \{e, x, x^2, \dots, x^{n-1}\}$ . (#)

По дефиницији  $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$ , па ватни  $\exists$ . Докажимо и  $\subseteq$ .

Нека је  $y \in \langle x \rangle$ . Тада је  $y = x^m$  за неко  $m \in \mathbb{Z}$ . Како је  $w(x) = n$ , тада је  $x^n = e$ . Постоји  $q, r \in \mathbb{Z}$  такви да је  $m = nq+r$ ,  $0 \leq r < n-1$  и тада ватни  $x^m = x^{nq+r} = (\underline{x^n})^q \cdot x^r = e^q \cdot x^r = x^r$ , чиме је доказ (#).

Завршен. Сада је довољно доказати да је  $x^i = x^j$  за све  $0 \leq i \leq j \leq n-1$  (тада  $\langle x \rangle$  има  $n$  елемената).

ППС.  $x^i = x^j / x^{-i} \Rightarrow e = x^{j-i}$ , а  $0 < j-i < n = w(x)$   $\Downarrow$  (дефиниција:  $n$  најмањи)

2): ППС.  $\langle x \rangle = \{x^m \mid m \in \mathbb{Z}\}$  је коначан скуп. Тада постоје  $i, j$  ако  $i \neq j$  и  $x^i = x^j$ .  $/ x^{-i}$

Следи  $e = x^{j-i}$ , а  $j-i \in \mathbb{N}$ , ако  $x$  је коначног реда.  $\Downarrow$

1.11 СТАВ: Нека је  $G$  група и  $a \in G$ . Ако је  $a$  бесконачног реда и  $m \in \mathbb{Z} \setminus \{0\}$ , тада је  $a^m$  бесконачног реда.

Ако је  $a$  коначног реда и  $m \in \mathbb{Z} \setminus \{0\}$ , тада је  $w(a^m) = H_{\mathbb{Z}}(w(a), m)$ .

доказ: I ППС.  $a^m$  је реда  $n \in \mathbb{N}$ . Тада је  $(a^m)^n = a^{mn} = e$  и  $a^{-mn} = e$ , па како је  $mn > 0$  или  $-mn > 0$ , тада је  $a^m$  коначног реда.  $\Downarrow$

II Одредимо најмање  $k \in \mathbb{N}$  таквога да  $(a^m)^k = e$  (тада је  $w(a^m) = k$ ). Џре овдја доказимо следеће:

④ Нека је  $G$  група и  $a$  коначног реда. Тада за  $l \in \mathbb{Z}$  ватни  $a^l = e$  ако  $w(a) \mid l$ .

**ДОКАЗ:**

- ↪  $\Rightarrow$  Постоји  $l = w(a) \cdot m$ , па је  $a^l = a^{\overbrace{w(a) \cdot m}^e} = (a^{\overbrace{w(a)}}^e)^m = e$
- ↪  $\Rightarrow$  Нека је  $w(a) = n$ . Постоје  $q, r \in \mathbb{Z}$  тај.  $l = nq + r$ ,  $0 \leq r < n-1$ . Тада је  $e = a^l = a^{nq+r} = (a^n)^q \cdot a^r = a^r$ ,

па тако је  $r < n$ , мора бити  $r \in \mathbb{N}$ , али  $r=0$  и  $n \mid l$ .

**НАСТАВАК ДОКАЗА С1.11:** Ватни  $a^{mk} = e$  АККО  $w(a) \mid mk$ , али АККО  $\frac{w(a)}{\text{НЗД}(w(a), m)} \mid \frac{m}{\text{НЗД}(w(a), m)} k$ .

$$\text{НЗД}\left(\frac{w(a)}{\text{НЗД}(w(a), m)}, \frac{m}{\text{НЗД}(w(a), m)}\right) = 1, \text{ па:}$$

1°: АККО  $\frac{w(a)}{\text{НЗД}(w(a), m)} \mid k$ , најмање шакво  $k$  је баш  $w(a^m)$  и једнако је  $\frac{w(a)}{\text{НЗД}(w(a), m)}$ .

ПРИМЕР: У  $\mathbb{Z}_{24}$ :  $w(14) = \frac{w(1)}{\text{НЗД}(w(1), 14)} = \frac{1}{\text{НЗД}(14, 14)} = \frac{1}{2} = 12$

- 1.14.
- (+) 1 Свака подгрупа цикличне групе је циклична.
  - 2 Ако је  $G$  циклична група реда  $n$ , тада за свако  $k \in \mathbb{N}$  шаквога  $k \mid n$  постоји јединствена подгрупа реда  $k$  од  $G$ .

**ДОКАЗ:** 1 Нека је  $G$  циклична група, али  $G = \langle a \rangle$  и  $H \leq G$ . Ако је  $H = \{e\}$ , тада је  $H = \langle e \rangle$ .

У СУПРОТНОМ  $\rightarrow$  Нека је  $k \in \mathbb{N}$  најмање шакво да  $a^k \in H$  (тада постоји јер  $H \neq \{e\}$ ). Докашњу да је  $H = \langle a^k \rangle$ .

$\supseteq$ : Из  $a^k \in H$ , због затворености следи  $(a^k)^m \in H$ , па  $\langle a^k \rangle \subseteq H$ .

$\subseteq$ : Нека је  $x \in H \leq G$ . Тада је  $x = a^l$  за неко  $l \in \mathbb{Z}$ . Постоје  $q, r \in \mathbb{Z}$  шакви да је  $l = qk + r$ ,  $0 \leq r < k-1$ , па је  $a^l = a^{qk+r} = (a^k)^q \cdot a^r \in H$ . Из  $a^k \in H$  следи  $(a^k)^q \in H$ , па је  $a^r \in H$ .

2 Нека је  $G = \langle a \rangle$ . Тада је  $w(a) = |\langle a \rangle| = |G| = n$ . Ватни:  $w(a^{\frac{n}{k}}) = \frac{w(a)}{\text{НЗД}(w(a), \frac{n}{k})} = \frac{n}{\text{НЗД}(n, k)}$

па је  $|\langle a^{\frac{n}{k}} \rangle| = w(a^{\frac{n}{k}}) = k$ . Нека је  $H \leq G$  тај.  $|H| = k$ . По дефиницији  $H$  је циклична, па је  $H = \langle a^k \rangle$ .

Из овога следи  $k = |H| = |\langle a^l \rangle| = w(a^l) = \frac{w(a)}{\text{НЗД}(w(a), l)} = \frac{n}{\text{НЗД}(n, l)}$ , па је  $\text{НЗД}(n, l) = k$ .

Одатле,  $\frac{n}{k} \mid l$ , па  $a^l \in \langle a^{\frac{n}{k}} \rangle$ , а даље следи  $(a^l)^n \in \langle a^{\frac{n}{k}} \rangle$ , али  $\langle a^l \rangle \subseteq \langle a^{\frac{n}{k}} \rangle$ .

Како  $|\langle a^l \rangle| = |\langle a^{\frac{n}{k}} \rangle|$ , следи  $H = \langle a^{\frac{n}{k}} \rangle$ .

Како  $|<a^t>| = |<a^{\frac{t}{k}}>|$ , следи  $H = <a^{\frac{t}{k}}>$ .

П4

### ИЗОМОРФИЗМИ ГРУПА

Деф. Нека су  $(G, \cdot)$  и  $(H, *)$  групе. Кашемо да су ове групе изоморфне ако постоји бијекција  $f: G \rightarrow H$  пајд. за све  $x, y \in G$  вали:  $f(x \cdot y) = f(x) * f(y)$ .

- За пресликавање  $f$  кашемо да је изоморфизам група  $G$  и  $H$ . Када су  $G$  и  $H$  изоморфне, пишемо  $G \cong H$ .

КОМЕНТАР:

$$\begin{matrix} 1, 2, 3, 4, 5, 6, \dots \\ I, II, III, IV, V, VI, \dots \end{matrix} \begin{matrix} + \\ \downarrow \end{matrix} \begin{matrix} f \\ \downarrow \end{matrix}$$

$$\begin{aligned} 2+3 &= 5 \\ \underline{II} + \underline{III} &= \underline{V} = f(2+3) \\ &\parallel \\ f(2) &+ f(3) \end{aligned}$$

ПРИМЕР:  $C_4 = \{1, -1, i, -i\}$   
 $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$f: \mathbb{Z}_4 \rightarrow C_4$  задао је  $f(0) = 1$   
 $f(1) = i$   
 $f(2) = -1$   
 $f(3) = -i$

$2+2=0 \quad f(2) \cdot f(2)=1$

$f(2+3) = ? \quad f(2) \cdot f(3)$   
 $f(1) \quad -1 \cdot (-i)$   
 $i \quad i$

1.18.  
**СТАВ:** Ако је  $e$  неуђраг у  $(G, \cdot)$ ,  $\varepsilon$  неуђраг у  $(H, *)$  и  $f: G \rightarrow H$  изоморфизам група, онда је  $f(e) = \varepsilon$ . Пакође, за свако  $x \in G$  је  $f(x^{-1}) = (f(x))^{-1}$ .

**ДОКАЗ:** Ватни  $f(e) = f(e \cdot e) \stackrel{\text{згф.}}{=} f(e) * f(e) / \varepsilon * f(e)^{-1}$   
 $\Rightarrow \varepsilon = f(e)$

**КОМЕНТАР:** Чадоказу тисмо користили да је  $f$  бијекција!  
 Уважи за сваки изоморфизам група.

Ватни  $\varepsilon = f(e) = f(x \cdot x^{-1}) \stackrel{\text{згф.}}{=} f(x) * f(x^{-1}) / (f(x))^{-1} * \varepsilon$   
 $\Rightarrow (f(x))^{-1} = (f(x))^{-1} * f(x) * f(x^{-1}) = f(x^{-1})$

**НОТАЦИЈА:** Неуђраг ћемо једном означаваш са  $e$ , чак и када имамо више група.

1.19.  
**СТАВ:** Ако је  $f: G \rightarrow H$  изоморфизам група, тада је  $f^{-1}: H \rightarrow G$  пакође изоморфизам.

**ДОКАЗ:** Јако је  $f$  бијекција, што  $f^{-1}$  поседуји и бијекција је. Зато је довољно доказати да за  $x, y \in H$  ватни:  $f^{-1}(x * y) = f^{-1}(x) \cdot f^{-1}(y)$ , где је  $*$  операција у  $H$ , а  $\cdot$  у  $G$ .

Јако је  $f$  бијекција, што поседује  $a, b \in G$  тд.  $x = f(a)$  и  $y = f(b)$ , тада је:

$$f^{-1}(x) \cdot f^{-1}(y) = f^{-1}(f(a)) \cdot f^{-1}(f(b)) \stackrel{\text{згф.}}{=} a \cdot b, \text{ док је } f^{-1}(x * y) = f^{-1}(f(a) * f(b)) \stackrel{\text{згф.}}{=} f^{-1}(f(a \cdot b)) = a \cdot b$$

1.20.  
**СТАВ:** Нека је  $f: G \rightarrow H$  изоморфизам група и  $x \in G$ .

1) Ако је  $x$  бесконачног реда, тада је и  $f(x)$  бесконачног реда.

2) Ако је  $x$  коначног реда, тада је  $\omega(x) = \omega(f(x))$ .

**ДОКАЗ:** 1) Ппс.  $f(x)$  је коначног реда. Нека је  $\omega(f(x)) = n$ . Тада је  $(f(x))^n = e$ , тада је  $f(x^n) = (f(x))^n$  ( $f$  је изоморфизам)  $= e = f(e)$ . Јако је  $f$  „1-1”, следи  $x^n = e$   $\Downarrow$ .

2) Нека је  $\omega(x) = n$ . Тада је  $x^n = e$ , тада је  $f(x^n) = (f(x))^n = f(e) = e$ , тј.  $\omega(f(x)) | n$ .

Нека је  $\omega(f(x)) = m$ . Тада је  $e = (f(x))^m = f(x^m)$ , тада је као и 1)  $x^m = e$ , тј.  $n = \omega(x) | m$ .

Следи  $n = m$ .

1.21.  
**Т** Свака циклична група изоморфна је или групи  $\mathbb{Z}$  или групи  $\mathbb{Z}_n$  за неко  $n \in \mathbb{N}$ .

**ДОКАЗ:** Нека је  $G$  циклична група и  $x \in G$  њен генератор. Тада је  $G = \langle x \rangle = \{x^m \mid m \in \mathbb{Z}\}$ .

I)  $G$  је бесконачног реда

Доказујемо да је  $f: \mathbb{Z} \rightarrow G$ , задао је  $f(m) = x^m$  за  $m \in \mathbb{Z}$  изоморфизам.

1°  $f$  је бијекција:  $f$  је „1-1” – привидјално;

$f \circ f^{-1} = \text{id}_{\mathbb{Z}}$ : ватни  $f(n) = f(m)$ . Одавде,  $x^n = x^m$ .  
 $x^{n-m} = e$ .  
 држ је  $x$  беск.  $n-m=0$   
 тј.  $n=m$

2°  $f(n+m) = f(n) \cdot f(m)$ : Вако  $f(n+m) = x^{n+m}$ , а  $f(n) \cdot f(m) = x^n \cdot x^m = x^{n+m}$ .

## II $G$ је реда $n$

Падаје  $G = \{e, x, x^2, \dots, x^n\}$  (доказано раније). Доказујемо да је  $f: \mathbb{Z}_n \rightarrow G$  задато са:

$$f(k) = x^k \text{ за } k \in \mathbb{Z}_n \text{ изоморфизам.}$$

1°  $f$  је бијекција: Следи из  $\oplus$  (наведени елементи су различити).

2°  $f(k+n, m) = f(k) \cdot f(m)$ : Вако  $f(k+n, m) = x^{k+n, m}$ , док је  $f(k) \cdot f(m) = x^k \cdot x^m = x^{k+m}$ .

Задесе,  $w(x) = |\langle x \rangle| = |G| = n$ , па је  $x^n = e$  и ако запишемо  $k+m = nq + (k+n, m)$ ,  $q \in \mathbb{Z}$ , добијамо  $x^{k+m} = x^{nq + (k+n, m)} = (\underbrace{x^n}_e)^q \cdot x^{k+n, m} = x^{k+n, m}$

## ГРУПЕ ПЕРМУТАЦИЈА

1.23.

СТАВ: Нека је  $X$  непразан скуп. Постављају скућ  $S_X$  задат са  $S_X = \{f: X \rightarrow X \mid f \text{ је бијекција}\}$ .

Падаје  $(S_X, \circ)$ , где је  $\circ$  композиција функција, трупа. Називамо је трупа пермутација скупа  $X$ .

КОМЕНТАР:  $(5, 3, 4, 1, 2)$  је пермутација скупа  $\{1, 2, 3, 4, 5\}$ . Падаје  $f: \{1, 2, 3, 4, 5\} \rightarrow \{1, 2, 3, 4, 5\}$ ,  $f(1)=5$ ,  $f(2)=3$ ,  $f(3)=4$ ,  $f(4)=1$ ,  $f(5)=2$  бијекција.

ДОКАЗ: I  $\circ$  је операција: За  $f, g \in S_X$  је  $f \circ g: X \rightarrow X$  добро дефинисано, а како су  $f$  и  $g$  бијекције, што је и  $f \circ g$  бијекција, па је  $f \circ g \in S_X$ .

II  $\circ$  је асоцијативна: ✓

III НЕУТРАЛ:  $\text{id}_X: X \rightarrow X$  ( $\text{id}_X(x) = x$ , па  $\text{id}_X \in S_X$ )

IV ИНВЕРЗ: За  $f \in S_X$  инверз је  $f^{-1}$  (како је  $f$  бијекција, што  $f^{-1}$  постоји и бијекција је).

1.24.

СТАВ: Ако постоји бијекција између  $X$  и  $Y$ , тада је  $S_X \cong S_Y$ .

ДОКАЗ: Нека је  $f: X \rightarrow Y$  бијекција. Доказујемо да је  $\Phi: S_X \rightarrow S_Y$  задато са  $\Phi(\pi) = f \circ \pi \circ f^{-1}$  за  $\pi \in S_X$  изоморфизам.

1)  $\Phi$  је добро дефинисана

Доказујемо да је  $f \circ \pi \circ f^{-1} \in S_Y$ . Ово је тачно, јер је  $f \circ \pi \circ f^{-1}: Y \rightarrow Y$  и бијекција је као композиција бијекција.

2)  $\Phi$  је бијекција

$\Phi$  је „ $1-1$ “: Вако  $\Phi(\pi_1) = \Phi(\pi_2) \Rightarrow f \circ \pi_1 \circ f^{-1} = f \circ \pi_2 \circ f^{-1} / f^{-1} \circ \underline{\circ} \circ f$   
 $\Rightarrow \pi_1 = \pi_2$

$\Phi$  је „НА“: Нека је  $\sigma \in S_Y$ . Пада вако:  $\Phi(f^{-1} \circ \sigma \circ f) = f \circ f^{-1} \circ \sigma \circ f \circ f^{-1} = \sigma$ , а  $f^{-1} \circ \sigma \circ f$  припада  $S_X$  (као  $y^1$ ).

$$3) \Phi(\pi_1 \circ \pi_2) = \Phi(\pi_1) \circ \Phi(\pi_2)$$

$$\text{Вашни } \Phi(\pi_1) \circ \Phi(\pi_2) = f \circ \pi_1 \circ \underbrace{f^{-1} \circ f}_{\text{id}} \circ \pi_2 \circ f^{-1} = f \circ \pi_1 \circ \pi_2 \circ f^{-1} = \Phi(\pi_1 \circ \pi_2)$$

- У наставку,  $X$  ће углавном бити коначан. Ако  $|X| = n$ , тада је  $S_X \cong S_{\{1, 2, \dots, n\}}$ , па зато уводимо  $S_n$  као  $S_n := S_{\{1, 2, \dots, n\}}$ .
- За  $\pi \in S_n$  често пишемо (и дефинишемо са):  $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$

ПРИМЕР:  $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 4 & 3 \end{pmatrix} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 1 & 5 & 2 \end{pmatrix}$

$$\pi \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 2 & 4 & 6 \end{pmatrix} \quad (\pi \circ \sigma)(1) = \pi(\sigma(1)) = \pi(6) = 3$$

$$\sigma \circ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 5 & 1 & 4 \end{pmatrix}, \text{ па } \sigma \circ \pi \neq \pi \circ \sigma$$

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 3 & 5 & 1 \end{pmatrix} \quad \sigma^{-1}(\sigma(1)) = 1$$

!  $|S_n| = n!$

- Нека су  $a_1, a_2, \dots, a_n \in \{1, 2, \dots, n\}$  различни. Тада цикл или циклус  $(a_1, a_2, \dots, a_k)$  је  $S_n$  дефинишено као пермутацију такога да  $\pi(a_i) = a_{i+1}$  за  $1 \leq i \leq k-1$ ,  $\pi(a_k) = a_1$ ,  $\pi(b) = b$  за  $b \notin \{a_1, \dots, a_k\}$ .

ПРИМЕР: У  $S_7$ :  $(4 \ 7 \ 1 \ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 3 & 7 & 5 & 6 & 1 \end{pmatrix}$

- (Кући  $\{a_1, a_2, \dots, a_k\}$  је носач циклуса  $(a_1, a_2, \dots, a_k)$ ).

- Задва циклуса кантено да су дисјунктни ако и тају дисјунктивне носаче.

ТВРЂЕЊЕ: Нека су  $\sigma$  и  $\pi$  дисјунктивни циклуси из  $S_n$ . Тада је  $\sigma \circ \pi = \pi \circ \sigma$ .

ДОКАЗ: Нека је  $S$  носач циклуса  $\sigma$ , а  $P$  носач циклуса  $\pi$ . Доказујемо да за свако  $x \in \{1, 2, \dots, n\}$

$$\text{Вашни } (\sigma \circ \pi)(x) = (\pi \circ \sigma)(x).$$

I  $x \in P$

Тада  $x \in S$ . Вашни  $(\sigma \circ \pi)(x) = \sigma(\underbrace{\pi(x)}_{\in P}) = \pi(x)$ , па  $\pi(x) \in S$ , као и

$$(\pi \circ \sigma)(x) = \pi(\sigma(x)) = \pi(x)$$

II  $x \in S$  као 1°

III  $x \notin S \cup P$

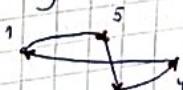
Вашни  $(\sigma \circ \pi)(x) = \sigma(\pi(x)) = \sigma(x) = x$  и слично  $(\pi \circ \sigma)(x) = x$ .

- ⊕ Свака пермутација из  $S_n$  може се на јединствен начин, до на реордер фактора, предста-  
вити као производ дисјунктивних циклуса.

ПРИМЕР:  $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 4 & 1 & 3 & 2 & 8 & 7 \end{pmatrix}$

$$\pi = (1 \ 5 \ 3 \ 4) (2 \ 6) (7 \ 8)$$

• улазни и излазни савет сваког чвора је 1



• Нека је  $\sigma = \pi_1 \pi_2 \dots \pi_k$ , где су  $\pi_1, \pi_2, \dots, \pi_k$  дисјунктивни циклуси. Тада је:  $\sigma^m = \pi_1^m \pi_2^m \dots \pi_k^m$ .

1.32. **СТАВ:** Ако је  $\sigma = \pi_1 \pi_2 \dots \pi_k$ , где су  $\pi_1, \pi_2, \dots, \pi_k$  дисјунктивни циклуси, тада је  $w(\sigma) = \text{НЗС}(w(\pi_1), \dots, w(\pi_k))$ .  
(ПОСЛЕДИЦА)

• За  $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_k)$  је  $w(\sigma) = k$ .

**ДОКАЗ:** Нека је  $l \in \mathbb{N}$  тај.  $\pi^l = \text{id}$ . Ванши:  $\pi^l = \text{id} \Leftrightarrow (\sigma_1 \dots \sigma_k)^l = \text{id} \Leftrightarrow \sigma_1^l \dots \sigma_k^l = \text{id}$  (\*), јер су  $\sigma_i$  међусобно дисјунктивни. Нека је  $x \in \{1, 2, \dots, n\}$  уносачу  $\sigma_i$ . Тада је:  $(\sigma_1^l \dots \sigma_k^l)(x) = \sigma_i^l(x) = \text{id}(x) = x$ , па закључујемо да (\*) ванши АККО  $\sigma_i^l = \text{id}$  за  $1 \leq i \leq k$  АККО  $w(\sigma_i) \mid l$  за  $1 \leq i \leq k$ .

АККО  $\text{НЗС}(w(\sigma_1), \dots, w(\sigma_k)) \mid l$ . Најмање обављео је  $w(\pi)$ , а што је баш  $\text{НЗС}(w(\sigma_1), \dots, w(\sigma_k))$ .

• Ванши:  $(a_1 a_2 \dots a_k) = (a_1 \dots a_{l-1} a_l) (a_l a_{l+1} \dots a_k)$  за  $1 \leq l \leq k$ . Сада ванши:

$$(a_1 a_2 \dots a_k) = (a_1 a_2) (a_2 a_3 \dots a_k) = (a_1 a_2) (a_2 a_3) (a_3 \dots a_k) = (a_1 a_2) (a_2 a_3) \dots (a_{k-1} a_k)$$

• Циклуси дужине 2 су транспозиције. Овим смо доказали следеће:

**СТАВ:** Свака пермутација из  $S_n$  може се записати као производ транспозиција.

**КОМЕНТАР:** а) Запис из претходног сказива нује јединствен.  $(ab)(ab) = \text{id}$

б) Оно што за сваки запис ЈЕСТЕ јединствено је парност броја транспозиција. Ако се пермутација  $\pi \in S_n$  може записати као производ парног броја транспозиција, кашено да је парна, а у случају кашено да је непарна.

• Скуп парних пермутација означавамо са  $A_n$ .

(n5)

| $S_n$ |

**СТАВ:** Нека је  $n \geq 2$ . Тада је  $A_n \leq S_n$  и ванци  $|A_n| = |S_n| = 2^n$ .

**КОМЕНТАР:** За  $n=1$  је  $A_1 = S_1 = \{\text{id}\}$ .

**ДОКАЗ:** Покажимо прво да је  $A_n \leq S_n$ . Ванци  $\sigma \in A_n$ , таје  $A_n \neq \emptyset$ , па је довољно доказати да за

$\sigma, \pi \in A_n$  ванци  $\sigma\pi^{-1} \in A_n$ .  $\sigma = \sigma_1 \dots \sigma_{2k}$ ,  $\pi = \pi_1 \dots \pi_{2l}$ , где су  $\sigma_i, \pi_j$  пермутације. Тада је:

$$\sigma\pi^{-1} = \sigma_1 \dots \sigma_{2k} (\pi_1 \dots \pi_{2l})^{-1} = \sigma_1 \dots \sigma_{2k} \pi_{2l}^{-1} \dots \pi_1^{-1} = \sigma_1 \dots \sigma_{2k} \pi_{2l} \dots \pi_1 \quad (\text{важи } \pi_i^{-1} = \pi_i) \Rightarrow \sigma\pi^{-1} \in A_n.$$

За други део је довољно доказати да ванци  $|A_n| = |S_n|$ . За ово је довољно доказати да је

$f: A_n \rightarrow S_n \setminus A_n$  задато са  $f(\pi) = T\pi$ , где је  $T$  нека фиксирана непарна пермутација (нпр. жижењо узени да је  $T$  једна пермутација), бијекција.

1°  $f$  је добро дефинисана

Нелично да докажемо да је за сваку парну пермутацију  $\pi$  пермутација  $T\pi$  непарна. Ово радијући на у доказу да је  $A_n \leq S_n$ .

2°  $f$  је „1-1“

$T_1 \circ T_2$

$$\text{Ванци } f(\pi_1) = f(\pi_2) \rightarrow T\pi_1 = T\pi_2 \Rightarrow \pi_1 = \pi_2$$

3° f je "HA"

Нека је  $\sigma \in S_n \setminus A_n$ . Тада је  $f(T'\sigma) = T T' \sigma = \sigma$ , а вати  $T'\sigma \in A_n$  (учинако  $A_n \leq S_n$ ).

④ Нека је  $\Pi \in S_n$  и  $(a_1, a_2, \dots, a_k) \in S_n$ . Тада вати:  $\Pi(a_1, a_2, \dots, a_k) \Pi^{-1} = (\Pi(a_1) \Pi(a_2), \dots, \Pi(a_k))$ .

доказ: Означимо са  $\sigma = \Pi(a_1, \dots, a_k) \Pi^{-1}$  и  $T = (\Pi(a_1), \dots, \Pi(a_k))$ . Нека је  $x \in \{1, 2, \dots, n\}$ .

1°  $x \in \{\Pi(a_1), \dots, \Pi(a_k)\}$

Нека је  $x = \Pi(a_i)$  за неко  $1 \leq i \leq k$ . Уочено да је  $i \neq k$  (за  $i=k$  доказ је сличан). Тада је:

$$\sigma(x) = (\Pi \circ (a_1, \dots, a_k) \circ \Pi^{-1})(\Pi(a_i)) = \Pi((a_1, \dots, a_k)(\Pi^{-1}(\Pi(a_i)))) = \Pi((a_1, \dots, a_k)(a_i)) = \Pi(a_i)$$

$$T(x) = \Pi(a_i)$$

2°  $x \notin \{\Pi(a_1), \dots, \Pi(a_k)\}$

Тада је  $\sigma(x) = \Pi((a_1, \dots, a_k) \underbrace{\Pi^{-1}(x)}_{\{a_1, \dots, a_k\}}) = \Pi(\Pi^{-1}(x)) = x$ .  $T(x) = x$

⑤ (Крејнијева): Свака група  $G$  изоморфна је подгрупи групе  $S_G$ .

доказ: За  $g \in G$  дефинишемо  $L_g : G \rightarrow G$  са  $L_g(x) = gx$ . Докашњимо да је  $L_g \in S_G$ , ај. га је  $L_g$  бијекуција.

1°  $L_g$  је "1-1"

$$\text{Вати } L_g(x_1) = L_g(x_2) \Rightarrow gx_1 = gx_2 / g^{-1} \Rightarrow x_1 = x_2$$

2°  $L_g$  је "HA"

Нека је  $x \in G$ . Тада вати  $L_g(g^{-1}x) = gg^{-1}x = x$ , што је  $L_g$  "HA".

Постављамо  $\mathcal{L}(G) = \{L_g \mid g \in G\}$ . Докашњимо да је  $\mathcal{L}(G) \leq S_G$ . Вати  $L_h \in \mathcal{L}(G)$ , па

$\mathcal{L}(G) \neq \emptyset$ . Води је довољно да за  $L_g, L_h \in \mathcal{L}(G)$  вати  $L_g \circ L_h \in \mathcal{L}(G)$ . За свако  $x \in G$  вати:

$$L_h^{-1}(L_h(x)) = x \text{ ај. } L_h^{-1}(hx) = x, \text{ што је } L_h^{-1}(x) = L_h^{-1}(hk^{-1}x) = h^{-1}x = L_h^{-1}(x)$$

$$\Rightarrow (L_g \circ L_h^{-1})(x) = L_g(L_h^{-1}(x)) = L_g(L_h^{-1}(x)) = L_g(h^{-1}x) = gh^{-1}x = L_g(h^{-1}(x)), \text{ што је}$$

$$L_g \circ L_h^{-1} = L_{gh^{-1}} \in \mathcal{L}(G).$$

Дакле, довољно је доказати да је  $G \cong \mathcal{L}(G)$ , а за то је довољно доказати да је  $F: G \rightarrow \mathcal{L}(G)$ ,

задато са  $F(g) = L_g$ , изоторфизам.

1° F је бијекуција

1) F је "HA" - по дефиницији  $\mathcal{L}(G)$

2) F је "1-1" - вати:  $F(g_1) = F(g_2) \Rightarrow L_{g_1} = L_{g_2} \Rightarrow L_{g_1}(x) = L_{g_2}(x)$ . За свако  $x \in G$ :  $g_1 x = g_2 x \Rightarrow g_1 = g_2$

2°  $F(g_1 g_2) = F(g_1) \circ F(g_2) :$  за  $x \in G$  вати:  $(F(g_1) \circ F(g_2))(x) = (L_{g_1} \circ L_{g_2})(x) = L_{g_1}(L_{g_2}(x)) = L_{g_1 g_2}(x)$   
 $= g_1 g_2 x = L_{g_1 g_2}(x) = F(g_1 g_2)(x)$

ДИРЕКТАН ПРОИЗВОД ГРУПА

2еф. Нека су  $(G_1, *_1), (G_2, *_2), \dots, (G_n, *_n)$  групе. Дефинишено директан производ  $(P, *)$  обухвата:

$$a) P = G_1 \times G_2 \times \dots \times G_n$$

$$b) \text{за } (g_1, \dots, g_n), (h_1, \dots, h_n) \in P \text{ је: } (g_1, \dots, g_n) * (h_1, \dots, h_n) = (g_1 *_1 h_1, \dots, g_n *_n h_n)$$

јасно,  $*$  је операција на  $P$

④  $(P, *)$  је група.

доказ: I асоцијативност

$$\begin{aligned} \text{Нека је } (g_1, \dots, g_n), (h_1, \dots, h_n), (l_1, \dots, l_n) \in P. \text{ Тада је: } & ((g_1, \dots, g_n) * (h_1, \dots, h_n)) * (l_1, \dots, l_n) = \\ & = (g_1 *_1 h_1, \dots, g_n *_n h_n) * (l_1, \dots, l_n) = ((g_1 *_1 h_1) *_2 l_1, \dots, (g_n *_n h_n) *_2 l_n) = \underbrace{(g_1 *_1 (h_1 *_2 l_1), \dots, g_n *_n (h_n *_2 l_n))}_{k_1, \dots, k_n, \text{ користе}} \\ & = (g_1, \dots, g_n) * (h_1 *_1 l_1, \dots, h_n *_n l_n) = (g_1, \dots, g_n) * ((h_1, \dots, h_n) * (l_1, \dots, l_n)) \end{aligned}$$

II неутрал:  $e = (e_1, \dots, e_n)$ , где је  $e$  неутрал у  $(G_i, *_i)$ . Зашто, вати:

$$(g_1, \dots, g_n) * (e_1, \dots, e_n) = (g_1 *_1 e_1, \dots, g_n *_n e_n) = (g_1, \dots, g_n) \text{ и слично за } (e_1, \dots, e_n) * (g_1, \dots, g_n).$$

III инверз: инверз елемента  $(g_1, \dots, g_n) \in P$  је  $(g_1^{-1}, \dots, g_n^{-1})$  где је  $g_i^{-1}$  инверз од  $g_i$  у  $(G_i, *_i)$ .

пример: У  $\mathbb{Z}_5 \times \mathbb{Z}_7$  је  $(3, 5) + (4, 1) = (3+5, 5+1) = (2, 6)$   $(3, 3) + (4, 4) = (2, 0)$

тврђење: Нека су  $G$  и  $H$  групе,  $a \in G$ ,  $b \in H$ . Тада је  $G \times H$  вати  $w(g, h) = H3C(w(g), w(h))$ .

доказ: За  $k \in \mathbb{N}$  вати:  $(g, h)^k = (e, e)$  ако  $(g^k, h^k) = (e, e)$  ако  $g^k = e$  и  $h^k = e$  ако  $w(g)^k = e$  и  $w(h)^k = e$  ако  $H3C(w(g), w(h))^k = e$

пример: У  $\mathbb{Z}_5 \times \mathbb{Z}_7$ :  $w(1, 1) = H3C(w(1), w(1)) = H3C(5, 7) = 35$

СТАБ: Једна  $\mathbb{Z}_n \times \mathbb{Z}_m$  је циклична група ако  $H3D(n, m) = 1$ .

доказ:  $\Rightarrow$  Нека  $\mathbb{Z}_n \times \mathbb{Z}_m = \langle (a, b) \rangle$ , за неке  $a \in \mathbb{Z}_n$ ,  $b \in \mathbb{Z}_m$ . Тада је  $n|m = |\mathbb{Z}_n \times \mathbb{Z}_m| = w((a, b))$

$$= H3C(w(a), w(b))$$

$$\leq w(a) w(b)$$

$$= \frac{n}{H3D(a, n)} \cdot \frac{m}{H3D(b, m)}$$

$$\leq nm,$$

шо се доказује да вати једнакости; специјално  $w(a) = n$ ,  $w(b) = m$  и  $H3C(w(a), w(b)) = w(a) w(b)$ .

$$\Rightarrow nm = H3C(n, m) = \frac{nm}{H3D(n, m)}, \text{ даје } H3D(n, m) = 1.$$

$\Leftarrow$  Поставимо  $\langle (1, 1) \rangle$ . Вати:  $\langle (1, 1) \rangle \subset \mathbb{Z}_n \times \mathbb{Z}_m$ , као и  $|\langle (1, 1) \rangle| = w(1, 1) = H3C(w(1), w(1))$

$$= H3C(n, m) = \frac{nm}{H3D(n, m)} = nm,$$

шо је  $\langle (1, 1) \rangle = \mathbb{Z}_n \times \mathbb{Z}_m$  (јер  $|\mathbb{Z}_n \times \mathbb{Z}_m| = nm$ ).

КОМЕНТАР: Ако је  $H3D(n, m) = 1$ , тада је  $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ .

- Нека су  $H, K \subseteq G$ , где је  $G$  група. Тада дефинишено  $HK = \{hk \mid h \in H, k \in K\}$ .

СТАБ: Нека је  $G$  група и  $H, K \leq G$  такве да важи: а)  $HK = G$  б)  $H \cap K = \{e\}$  в)  $(hk)^{-1} = h^{-1}k^{-1}$ .  
Тада важи  $G \cong H \times K$ .

ДОКАЗ: Доказујемо да је  $F: H \times K \rightarrow G$  задатак  $F(h, k) = hk$  изоморфизам.

1°  $F$  је бијекција

1)  $F$  је "НА" по услову а)

2)  $F$  је "1-1": важи  $F(h_1, k_1) = F(h_2, k_2) \Rightarrow h_1 k_1 = h_2 k_2$

$$\Rightarrow g \in H \cap K \Rightarrow g = e = h_2^{-1} h_1 = k_2 k_1^{-1} \Rightarrow h_1 = h_2 \text{ и } k_1 = k_2$$

2°  $F(h_1, k_1) F(h_2, k_2) = F((h_1, k_1)(h_2, k_2))$

важи:  $F(h_1, k_1) F(h_2, k_2) = h_1 k_1 \cdot h_2 k_2 \stackrel{b)}{=} h_1 h_2 k_1 k_2 = F(h_1 h_2, k_1 k_2) = F((h_1, k_1)(h_2, k_2))$

### ЛАГРАНЖНОВА ТЕОРЕМА

ДЕФ. Нека је  $G$  група,  $x \in G$ ,  $H \leq G$ . Тада је скуп  $xH = \{xh \mid h \in H\}$  леви косет (подгрупа) подгрупе  $H$  у групи  $G$ . Слично,  $Hx = \{hx \mid h \in H\}$  је десни косет (подгрупа) подгрупе  $H$  у групи  $G$ .

ПРИМЕР:  $G = D_4 = \{id, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$

$$H = \langle \rho \rangle = \{id, \rho, \rho^2, \rho^3\} \quad \sigma H = \{\sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\} \quad \sigma^2 H = \{\sigma^2, \sigma^2\rho, \sigma^2\rho^2, \sigma^2\rho^3\}$$

СТАБ: Важи следеће: 1)  $xH = yH$  ако  $x^{-1}y \in H$

2) ако  $xH \neq yH$ , тада је  $xH \cap yH = \emptyset$ .

ДОКАЗ: 1) ( $\Rightarrow$ ): Како је  $x \in H$ , тада је  $y \in yH$ , па како је  $yH = xH$ , тада је  $y \in xH$ . Закле, посматрају  $h \in H$  тако да је  $y = xh$ .  $\therefore x^{-1}y = h \in H$ . Следи  $x^{-1}y \in H$ .

( $\Leftarrow$ ): Доканчимо прво да је  $xH \subseteq yH$ . Нека је  $g \in xH$ . Тада посматрају  $h \in H$  тај да  $g = xh$ , па је

$$g = y y^{-1} x h = y \underbrace{(x^{-1}y)^{-1}}_{\in H} h \in yH.$$

Доканчимо да је  $yH \subseteq xH$ . Нека је  $g \in yH$ . Тада посматрају  $h \in H$  тај да  $g = yh$ , па је по дефини

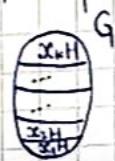
$$g = x x^{-1} y h \in xH.$$

2) ППС. Нека је  $g \in xH \cap yH$ . Како је  $g \in xH$ , посматрају  $h \in H$  тај да  $g = xh$ . Слично, посматрају  $h' \in H$  тај да  $g = yh'$ . Тада је  $xh = yh'$ .  $\therefore x^{-1}y \cdot h^{-1}h' \in H$ , па је по дефини

1)  $xH = yH$ , што је контрадикција.

КОМЕНТАР: Важи  $x \in xH$ . Слично томе, сви различити леви косети подгрупе  $H$  у групи  $G$  чине

партицију скупа  $G$ .



$(\text{еси } + \text{и } \varphi)$  (у)

даје, ако је  $\varphi$

тада је  $d = 1$ . С

•  $n$  је осцијација

НЕУТРАЛ:

локалнијо да

што постоје

брештходне

локалнијо и

шта ако је  $H$

•  $n$  је константа

дефиницја

• дефиниција

последица (Ојлерова

доказ: Нека је  $G$

што је  $H$

последица (Мала о

доказ: Како

брештходна

? Како

1° Задатак

2° Ако

доказ: 1° као

2° Задатак

3°

пример: Одре

3°

што

- Овога је доказано следеће:

СТАВ: Нека је  $G$  група и  $H \leq G$ . Тада је  $G$  дисјунктивна унција различитих левих косета подгрупе  $H$ .

ДЕФ: Нека је  $G$  група и  $H \leq G$ . Тада скуп левих косета од  $H$  у  $G$  означавамо са  $G/H = \{xH \mid x \in G\}$

и називамо количничким скупом.

- Ако је  $G/H$  коначан, тада за  $|G/H|$  кажемо да је индекс подгрупе  $H$  у групи  $G$  и означавамо га са  $[G : H]$ . Ако је  $G/H$  бесконачан, кажемо да је  $H$  бесконачног индекса у  $G$ .

(+) (Лагранџева): Нека је  $G$  коначна група и  $H \leq G$ . Тада вали:  $|G| = |H| \cdot [G : H]$ . Слично,

ред подгрупе дели ред (коначне) групе.

ДОКАЗ: Нека су  $x_1H, x_2H, \dots, x_kH$  сви различити леви косети подгрупе  $H$  у  $G$ . Тада је  $[G : H] = k$ .

Локалнијо да за свако  $i, 1 \leq i \leq k$  вали  $|H| = |x_iH|$ . За ово је довољно доказати да је

$f: H \rightarrow x_iH$ , задашо са  $f(h) = x_ih$ , бијекција.

1°  $f$  је "НА": на основу дефиниције скупа  $x_iH$

2°  $f$  је "1-1": вали  $f(h_1) = f(h_2) \Rightarrow x_ih_1 = x_ih_2 \Rightarrow h_1 = h_2$ .

Како вали  $G = x_1H \sqcup x_2H \sqcup \dots \sqcup x_kH$ , што је  $|G| = |x_1H| + \dots + |x_kH| = k \cdot |H|$ .

ПОСЛЕДИЦА: Ред сваког елемената коначне групе дели ред твеје групе.

ДОКАЗ: Нека је  $G$  коначна група и  $x \in G$ . Како је  $w(x) = \langle x \rangle \leq G$ , што  $w(x)$  дели  $|G|$  по Лагранџевој теореми.

ПОСЛЕДИЦА: Свака група простијег реда је циклична.

ДОКАЗ: Нека је  $p$  простији број и  $G$  група реда  $p$ . Тада за свако  $x \in G$  вали  $w(x) \mid p$ , па  $w(x) \in \{1, p\}$ .

Закле, за свако  $x \neq e$  је  $w(x) = \langle x \rangle = p = |G|$ , па је  $G = \langle x \rangle$ .

КОМЕНТАР: Ако је  $|G| = p$ , где је  $p$  простији број, тада је  $G \cong \mathbb{Z}_p$ .

ПОСЛЕДИЦА: Ако је  $G$  коначна група и  $x \in G$ , тада је  $x^{|G|} = e$ .

ДОКАЗ: Како  $w(x) \mid |G|$ , што је  $x^{|G|} = e$ .

### Ојлерова група, функција и теорема

•  $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$

СТАВ:  $\Phi(n) = \{k \mid 1 \leq k \leq n, \text{НЗД}(k, n) = 1\}$ . За  $n \geq 2$ ,  $\Phi(n) \subseteq \mathbb{Z}_n$ .

ДОКАЗ:  $n$  је операција на  $\Phi(n)$ : Нека су  $x, y \in \Phi(n)$ . Како је  $\text{НЗД}(x, n) = \text{НЗД}(y, n) = 1$ , постоје

$u', u'', u''' \in \mathbb{Z}$  такви да је  $xu' + nu'' = 1$ ,  $yu'' + nu''' = 1$ . Множењем добијамо:

$xu' + nyu'' + nu''' = 1$ , што је  $xu' + ny = 1$ .

$$(xu' + nv') (yu'' + nv'') = 1, \text{ тј. } xy' + n(xu'' + yu') + nv'v'' = 1. \text{ Одавде следи } \text{НЗД}(xy, n) = 1.$$

Зато, ако је  $xy = nq + (x, y)$  ( $q \in \mathbb{Z}$ ), тада из НЗД( $x, y, n$ ) = d следи  $d | nq + x, y = xy$ , па је  $d = 1$ . Следи,  $x, y \in \Phi(n)$ .

•  $n$  је асоцијативна: ✓ ■

НЕУТРАЛ:  $1 \in \Phi(n)$  ■

у Г. Доказано да свако  $k \in \Phi(n)$  има инверз, тј. да постоји  $l \in \Phi(n)$  тдг.  $k \cdot l = 1$ . Како је  $k \in \Phi(n)$ , то постоје  $u, v \in \mathbb{Z}$  тдг.  $ku + nv = 1$ . Нека је  $\bar{l}$  остатак при делењу  $l$  са  $n$ . Тада из прештодне једнакости следи  $k \cdot \bar{l} = 1$ .

Доказано и да је  $l \in \Phi(n)$ , тј. да је  $\text{НЗД}(l, n) = 1$ . Запишемо ( $q' \in \mathbb{Z}$ ):  $kl = nq' + (k, l) = nq' + 1$ , па ако је  $\text{НЗД}(l, n) = d$ , вати  $d | kl$ ,  $d | n$ , ше  $d | kl - nq' = 1$ , тј.  $d = 1$ . ■

•  $n$  је комутативна: ✓ ■

Деф. Група  $(\Phi(n), \cdot)$  је Ојлерова група.

• Дефинишећо  $\varUpsilon: N \rightarrow N$  са  $\varUpsilon(n) = |\Phi(n)|$ .

ПОСЛЕДИЦА (Ојлерова теорема): Ако је  $n > 2$  и  $x \in \mathbb{Z}$  тдг.  $\text{НЗД}(x, n) = 1$ , тада је  $x^{\varUpsilon(n)} \equiv 1 \pmod{n}$ .

ДОКАЗ: Нека је  $\bar{x}$  остатак при делењу  $x$  са  $n$ . Тада је  $\bar{x}^{\varUpsilon(n)} \equiv x^{\varUpsilon(n)} \pmod{n}$ , а како вати  $\text{НЗД}(\bar{x}, n) = 1$ , то је  $\text{НЗД}(\bar{x}, n) = 1$ , тј.  $\bar{x} \in \Phi(n)$ . Како у  $\Phi(n)$  вати  $\bar{x}^{|\Phi(n)|} = \bar{x}^{\varUpsilon(n)} = 1$ , тврђење следи.

ПОСЛЕДИЦА (Мала Фермајевा): Ако је  $p$  прост број и  $x \in \mathbb{Z}$  тдг.  $p \nmid x$ , тада је  $x^{p-1} \equiv 1 \pmod{p}$ .

ДОКАЗ: Јако  $p \nmid x$ , па је  $\text{НЗД}(x, p) = 1$ , а  $\Phi(p) = \{1, 2, \dots, p-1\}$ , па је  $\varUpsilon(p) = p-1$ , ше тврђење следи из прештодног.

? Јако одредити  $\varUpsilon(n)$ ?

1° За  $m, n \in \mathbb{N}$  тдг.  $\text{НЗД}(m, n) = 1$  вати  $\varUpsilon(mn) = \varUpsilon(m) \cdot \varUpsilon(n)$ .

2° Ако је  $p$  прост број и  $k \in \mathbb{N}$ , тада је  $\varUpsilon(p^k) = p^{k-1}(p-1)$ .

ДОКАЗ: 1° Касније

2° За  $x \in \mathbb{Z}$  вати  $\text{НЗД}(x, p^k) = 1$  ако  $x$  није делив са  $p$ . Следи  $\varUpsilon(p^k) = p^k - \frac{1}{p} = p^{k-1}(p-1)$ .

Дакле, ако је  $n = p_1^{d_1} \cdots p_k^{d_k}$ , где су  $p_i$  различити прости бројеви, вати:

$$\varUpsilon(n) = \varUpsilon(p_1^{d_1} \cdots p_k^{d_k}) = \varUpsilon(p_1^{d_1}) \cdots \varUpsilon(p_k^{d_k}) = \cdots = \varUpsilon(p_1^{d_1}) \cdots \varUpsilon(p_k^{d_k}) = p_1^{d_1-1} (p_1-1) \cdots p_k^{d_k-1} (p_k-1)$$

ПРИМЕР: Одредити остатак при делењу броја  $3^{2024}$  са 10.

$$3^1 = 3, 3^2 = 9, 3^3 \equiv_{10} 7, 3^4 \equiv_{10} 1, 3^5 \equiv_{10} 3, \dots$$

$$\omega(3) = 4 \text{ у } \Phi(10)$$

$$3^{2024} = 1 \text{ у } \Phi_{10}, \text{ јер } \omega(3) | 2024.$$

(+) (Конјугација): Ако је  $G$  коначна група и  $p$  прости број који дели њен ред, тада у  $G$  постоји

(уоквирено) елементијарни реда  $p$ .

ПРИМЕР: Свака група реда 6 изоморфна је или са  $\mathbb{Z}_6$  или са  $D_3$ .

ДОКАЗ: Нека је  $G$  група реда 6. Тада постоје  $x, y \in G$  тај.  $w(x)=3, w(y)=2$ . Означито:

$H = \langle x \rangle = \{e, x, x^2\}$ ,  $K = \langle y \rangle = \{e, y\}$ . Када  $y \notin H$  (уједно 2. елементнији члану), тада је

$H \cap yH = \emptyset$ . Закле,  $G = H \sqcup yH$ , ај.  $G = \{e, x, x^2, y, yx, yx^2\}$ . Постављају сх. Ванци су же

јер  $y \neq x^2$ ,  $xy \neq x$  (јер  $y \neq e$ ),  $xy \neq x^2$  (јер  $y \neq x$ ),  $xy \neq y$  (јер  $x \neq e$ ). (који су же)

I  $xy = yx$ : Ванци  $Kh = G$ ,  $K \cap H = \{e\}$  и за све  $k \in K$ ,  $kh = hk$ . (који су же)

Следи:  $G \cong K \times H \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$   $\downarrow_{\text{НЗД}(2, 3) = 1}$

II  $xy = yx^2$ : Тада је  $G \cong D_3$  уз изоморфизам  $f(y^i x^j) = \sigma^i \delta^j$

(17)

## НОРМАЛНЕ ПОДГРУПЕ

ДЕФ. Нека је  $G$  група и  $x, y \in G$ . Тада кажемо да је у конјугован елементу  $x$  ако постоји  $g \in G$  тај.  $y = gxg^{-1}$ .

- Ако на  $G$  увеђено релацију  $\sim$  са:  $x \sim y$  ако у конјугован са  $x$ , тада је  $\sim$  релација еквиваленције. Записа: (P)  $x \sim x$  јер је  $x = exe^{-1}$

(C) Нека је  $x \sim y$ . Тада постоји  $g \in G$  тај.  $y = gxg^{-1}$ . Следи:  $x = g^{-1}y g = g^{-1}y(g^{-1})^{-1}$ , па је  $y \sim x$ .

(T) Нека је  $x \sim y$  и  $y \sim z$ . Тада постоје  $g, h \in G$  тај.

$y = gxg^{-1}$  и  $z = hyh^{-1}$ . Следи:  $z = hg x g^{-1} h^{-1} = hg(xh)^{-1}$ , па је  $x \sim z$ .

- Класе еквиваленције у односу на  $\sim$  су  $K_x = \{y \mid x \sim y\} = \{gxg^{-1} \mid g \in G\}$  и називају их КЛАСАМА КОНЈУГАЦИЈЕ (или конјугованостим).

ОСОБИНЕ:

- 1)  $x \in K_x$
- 2) за све  $x, y \in G$  је  $K_x = Ky$  или  $K_x \cap Ky = \emptyset$ .
- 3)  $\bigcup_{x \in G} K_x = G$

ДЕФ. Нека је  $G$  група и  $H \leq G$ . Тада је  $H$  нормална подгрупа од  $G$  ако је  $H$  унија неких класа конјугације. У том случају, пишемо  $H \triangleleft G$ .

КОМЕНТАР: Ако је  $x \in H$  и  $H \triangleleft G$ , тада је  $K_x \subseteq H$ .

КОМЕНТАР:  $K_e = \{geg^{-1} \mid g \in G\}$ , тај.  $K_e = \{e\}$ . Следи  $\{e\} \triangleleft G$ , а ванци и  $G \triangleleft G$ .

ПРИМЕР:  $D_3 = \{\text{id}, s, s^2, \sigma, \sigma s, \sigma s^2\}$

$$H = \langle s \rangle = \{\text{id}, s, s^2\} \leq D_3 \quad K = \langle \sigma \rangle = \{\text{id}, \sigma\} \leq D_3$$

$K_\sigma = \{g\sigma g^{-1} \mid g \in D_3\}$ , па  $\sigma\sigma\sigma^{-1} = \sigma\sigma^2\sigma^{-1} = \sigma\sigma \in K_\sigma$ , али  $\sigma \notin K$ , па  $K \not\subseteq D_3$ .

С друге стране,  $H \triangle D_3$  јер је  $H = K_{id} \cup K_g$  (за већину,  $K_g = \{g, g^2\}$ )

**КОМЕНТАР:** Ако је  $G$  комутативна група, тада за свако  $H \leq G$  вали  $H \triangle G$  (јер је  $K_x = \{x\}$ ).  
1.64.

**СТАВ:** Нека је  $H \leq G$ . Тада је следеће еквивалентно:

$$1. H \triangle G$$

$$2. \text{за све } g \in G \text{ је } gHg^{-1} \subseteq H$$

$$3. \text{за све } g \in G \text{ је } gH = Hg$$

**ДОКАЗ:**  $1^\circ \Rightarrow 2^\circ \Rightarrow 3^\circ \Rightarrow 1^\circ$

$1^\circ \Rightarrow 2^\circ$ : Нека је  $y \in gHg^{-1}$ . Тада је  $y = ghg^{-1}$  за неко  $h \in H$ . Како је  $ghg^{-1} \in K_h$ , па из  $K_h \subseteq H$  следи  $ghg^{-1} \in H$ .

$2^\circ \Rightarrow 3^\circ$ :  $\subseteq$  = Нека је  $y \in gH$ . Тада постоји  $h \in H$  таквога да је  $y = gh$ . Следи  $y = ghg^{-1}g \in Hg$ .

$\supseteq$ : Нека је  $y \in Hg$ . Тада постоји  $h \in H$  таквога да је  $y = hg$ . Следи:

$$y = gg^{-1}hg = gg^{-1}h(g^{-1})^{-1} \in gH.$$

$3^\circ \Rightarrow 1^\circ$ : Довољно је доказати да за свако  $x \in H$  вали  $K_x \subseteq H$ , јер је тада  $H = \bigcup_{x \in H} K_x$ .

Нека је  $y \in K_x$ . Тада је  $y = gxg^{-1}$  за неко  $g \in G$ . Како је  $gxg^{-1} \in Hg$ , па постоји  $h \in H$  тако да је  $gx = xg$ . Следи  $y = gxg^{-1} = xgg^{-1} = x \in H$ .

1.65.

**СТАВ:** Свака подгрупа индекса 2 је нормална.

**ДОКАЗ:** Нека је  $G$  група и  $H \leq G$  па  $[G : H] = 2$ . Тада постоји  $a \in G$  па се  $aH = H$  и  $aH$  леви

косети од  $H$  и  $G$ . Како  $H \neq aH$ , па  $a \notin H$ . Да бисмо доказали да је  $H \triangle G$ , па прешодном ставу довољно је доказати да је  $gH = Hg$  за свако  $g \in G$ . Пре свега, како  $H \neq Ha$  (јер  $a \notin H$  - за већину), па је  $G = H \sqcup aH = H \sqcup Ha$  и следи  $aH = Ha$ . Развојимо следећа 2 случаја:

1.  $a \in H$ : Тада је  $gH = H$  и слично  $Hg = H$ , па је  $gH = Hg$ .

2.  $a \notin H$ : Тада  $gH \neq H$ , па је  $gH = Ha$ . Слично,  $Hg \neq H$ , па је  $Hg = Ha$ . Следи:

$$gH = aH = Ha = Hg.$$

Докрићи

$$\frac{1}{2} |D_n|$$

**ПРИМЕР:**  $D_n$ ,  $|D_n| = 2n$ ,  $|\langle s \rangle| = n$ , па је  $[D_n, \langle s \rangle] = \frac{|D_n|}{|\langle s \rangle|} = 2$  и следи  $\langle s \rangle \triangle D_n$ .

**ПРИМЕР:**  $A_n \triangle S_n$  за  $n \geq 2$ , јер  $[S_n, A_n] = 2$ .

**ПРИМЕР:** У  $D_3$  је  $[D_3, \langle \sigma \rangle] = \frac{|\langle \sigma \rangle|}{|\langle \sigma \rangle|} = \frac{3}{2} = 3$ , а  $\langle \sigma \rangle \not\triangle D_3$ .

### КОЛИЧНИЧКЕ ГРУПЕ

- Нека је  $G$  група и  $x, y \in G$ . Тада дефинишење  $X \cdot Y = \{xy \mid x \in X, y \in Y\}$ .

**ПОДСЕТНИК:** За  $H \leq G$  је  $G/H = \{aH \mid a \in G\}$ .

<sup>1.69.</sup>  
СТАВ: Нека је  $G$  група и  $H \triangleleft G$ . Плажаје  $(G/H, \cdot)$  група у односу на пресекодно дефинисано  
множење подскупова од  $G$ .

док.

ДОКАЗ: 1.  $\circ$  је операција

Нека су  $a, b \in G$ . Надимо да докажемо да је  $aH \cdot bH$  шакође леви косар од  $H$ .  
Зашто доказујемо да ћати  $aH \cdot bH = (ab)H$ ? Ватни:  $aH \cdot bH = \{ah \cdot bk \mid h, k \in H\} =$   
 $\stackrel{(H \triangleleft)}{=} \{ahb \mid h \in H\} \cdot \{k \mid k \in H\} = (a(bH)) \cdot H = \{abh \mid h \in H\} \cdot \{k \mid k \in H\} = \{abhk \mid h, k \in H\} = (ab) \cdot (H \cdot H)$

1.80  
СТАВ

док.

Закле, добављено је доказати да је  $H \cdot H = H$ . Ово следи из:

(за  $h, k \in H$  је  $hk \in H$ )

1°  $H \cdot H \subseteq H$ , јер је  $h \in H$

$H \cdot H \subseteq H \cdot H$ .

2°  $H \subseteq H \cdot H$ , јер је

2.  $\circ$  је асоцијативна

$$! ((aH) \cdot (bH)) \cdot (cH) \stackrel{!}{=} (ab)H \cdot cH \stackrel{!}{=} ((ab)c)H = (a(bc))H \stackrel{!}{=} aH \cdot (bc)H \\ \stackrel{!}{=} (aH) \cdot ((bc)H)$$

1.81  
СТАВ

док.

3. Неутрал је  $eH = H$ , јер је  $aH \cdot eH = (ae)H = aH$  и  $eH \cdot aH = (ea)H = aH$ .

4. Инверз од  $aH$  је  $a^{-1}H$ , јер је  $aH \cdot a^{-1}H = (aa^{-1})H = eH$  и  $a^{-1}H \cdot aH = (a^{-1}a)H = eH$ .

⊕

ПРИМЕР:  $G = \mathbb{Z}$ ,  $H = \langle 3 \rangle = \{0, 3, -3, 6, -6, \dots\} = 3\mathbb{Z}$

Одредимо  $G/H = \mathbb{Z}/3\mathbb{Z}$ . ( $\cong \mathbb{Z}_3$ )

$$0 + 3\mathbb{Z} = 3\mathbb{Z} = \{0, 3, -3, 6, -6, \dots\}$$

$$1 + 3\mathbb{Z} = \{1, 4, -2, 7, -5, \dots\} \quad \stackrel{!}{=} 3 + 3\mathbb{Z}$$

$$2 + 3\mathbb{Z} = \{2, 5, -1, 8, -4, \dots\}$$

$$(1 + 3\mathbb{Z}) + (2 + 3\mathbb{Z}) = (1+2) + 3\mathbb{Z}$$

$$= 3 + 3\mathbb{Z}$$

$$= 0 + 3\mathbb{Z}$$

гор

### ХОМОМОРФИЗМИ ГРУПА

ДЕФ. Нека су  $(G, \cdot)$  и  $(H, *)$  групе. Плажаје  $f: G \rightarrow H$  хомоморфизам група ако за све  $x, y \in G$  ватни  $f(x \cdot y) = f(x) * f(y)$ .

• ИЗОМОРФИЗМ = БИЈЕКЦИЈА + ХОМОМОРФИЗАМ

КОМЕНТАР: Уз доказ као код изоморфизма, доказује се да за хомоморфизам  $f: G \rightarrow H$  ватни:  $f(e) = e$  и  $f(x^{-1}) = f(x)^{-1}$ .

ДЕФ. Нека је  $f: G \rightarrow H$  хомоморфизам група. Језгро овог хомоморфизма је  $\text{Ker}(f) = \{a \in G \mid f(a) = e\}$ , а слика је  $\text{Im}(f) = \{f(a) \mid a \in G\}$ .

Језгро хомоморфизма  $f: G \rightarrow H$  је нормална подгрупа од  $G$ .

1.79.

СТАВ:

ано

**доказ:**  $\text{Ker}(f) \leq G$ . Вајни  $e \in \text{Ker}(f)$  јер је  $f(e) = e$ , па  $\text{Ker}(f) \neq \emptyset$ . За то је довољно доказати да за  $x, y \in \text{Ker}(f)$  већи  $xy^{-1} \in \text{Ker}(f)$ . За  $x, y \in \text{Ker}(f)$  већи:  $f(x) = f(y) = e$ , тј.  $xy^{-1} \in \text{Ker}(f)$ .

**Ker(f) ▲ G:** Довољно је доказати да за свако  $g \in G$  већи  $g \cdot \text{Ker}(f) \cdot g^{-1} \subseteq \text{Ker}(f)$ .

Нека је  $y \in g \cdot \text{Ker}(f) \cdot g^{-1}$ . Тада постоји  $x \in \text{Ker}(f)$  тај.  $y = gxg^{-1}$  и  $f(x) = e$ . Следи:

$$f(y) = f(gxg^{-1}) = f(g) \cdot f(x) \cdot f(g^{-1}) = f(g) \cdot f(g^{-1}) = e, \text{ тј. } y \in \text{Ker}(f).$$

1.80.

**СТАВ:** Хомоморфизам група  $f: G \rightarrow H$  је „1-1“ ако је  $\text{Ker}(f) = \{e\}$ .

**доказ:** ( $\Rightarrow$ ) Нека је  $x \in \text{Ker}(f)$ . Тада је  $f(x) = e = f(e)$ , па како је  $f$  „1-1“, следи  $x = e$ .

( $\Leftarrow$ ) Из  $f(x) = f(y) / f(y)^{-1}$  следи  $e = f(x) f(y)^{-1} = f(xy^{-1})$ , па како је  $\text{Ker}(f) = \{e\}$ , већи  $xy^{-1} = e$ , тј.  $x = y$ .

1.82.

**СТАВ:** Слика хомоморфизма група  $f: G \rightarrow H$  је подгрупа од  $H$ .

**доказ:** Већи  $f(e) \in \text{Im}(f)$ , па  $\text{Im}(f) \neq \emptyset$ . За то је довољно доказати да за  $x, y \in \text{Im}(f)$  већи  $xy^{-1} \in \text{Im}(f)$ . Из  $x, y \in \text{Im}(f)$  следи да постоје  $a, b \in G$  тај.  $x = f(a), y = f(b)$ , па је  $xy^{-1} = f(a) f(b)^{-1} = f(ab^{-1}) \in \text{Im}(f)$ .

**Т** (теорема о изоморфизму за групе): Нека је  $f: G \rightarrow H$  хомоморфизам група. Тада је  $\tilde{f}: G / \text{Ker}(f) \rightarrow \text{Im}(f)$ , задато са  $\tilde{f}(a \text{Ker}(f)) = f(a)$ , је изоморфизам групе. Свеујално,  $G / \text{Ker}(f) \cong \text{Im}(f)$ .

**доказ:** •  $\tilde{f}$  је добро дефинисано: Довољно је доказати да из  $a \text{Ker}(f) = b \text{Ker}(f)$  следи  $f(a) = f(b)$ .

Засима,  $a \text{Ker}(f) = b \text{Ker}(f)$  ако  $a^{-1}b \in \text{Ker}(f)$  ако  $f(a^{-1}b) = e$  ако  $f(a) = f(b)$ .

•  $\tilde{f}$  је „НА“: по дефиницији  $\text{Im}(f)$ .

•  $\tilde{f}$  је хомоморфизам: Већи  $\tilde{f}(a \text{Ker}(f) \cdot b \text{Ker}(f)) = \tilde{f}((ab) \text{Ker}(f)) = f(ab) = f(a) f(b)$

$$= \tilde{f}(a \text{Ker}(f)) \cdot \tilde{f}(b \text{Ker}(f))$$

1.83.

## ДЕЈСТВА ГРУПА

1.92.

**Деф.** Нека је  $G$  група и  $X$  непразан скуп. Пог дејством групе  $G$  на скупу  $X$  поразумевамо свако пресликавање  $\Theta: G \times X \rightarrow X$  такво да већи: 1.  $\Theta(e, x) = x, \forall x \in X$   
2.  $\Theta(g, \Theta(h, x)) = \Theta(gh, x), \forall g, h \in G, \forall x \in X$

1.93.

**Деф.** Нека је  $G$  група и  $X$  непразан скуп. Пог дејством групе  $G$  на скупу  $X$  поразумевамо сваки хомоморфизам  $\Psi: G \rightarrow S_X$ .

- Доказати да свако дејство из д. 1.92 задаје једно дејство из д. 1.93 и обратно.

( $\Rightarrow$ ): Нека је  $\Theta: G \times X \rightarrow X$  дејство. Дефинишемо  $\Psi: G \rightarrow S_X$  са  $\boxed{\Psi(g)(x)} = \Theta(g, x)$  и доказати

предузеће

да је дејство по д. 1.92.

1°  $\Psi$  је добро дефинисано, тј.  $\Psi(g)$  је бујекција:

1.1°  $\Psi(g)$  је "1-1":

Некаје  $\Psi(g)(x) = \Psi(g)(y)$ , тј.  $\Theta(g, x) = \Theta(g, y)$ . Птадаје  $\Theta(g^{-1}, \Theta(g, x)) = \Theta(g^{-1}, \Theta(g, y))$ , па корије  $\Theta(g^{-1}, \Theta(g, x)) \stackrel{?}{=} \Theta(g^{-1}, \Theta(g, y)) = \Theta(e, x) \stackrel{?}{=} x$  и слично  $\Theta(g^{-1}, \Theta(g, y)) = y$ , па је  $x=y$ .

1.2°  $\Psi(g)$  је "ИИ":

Некаје  $y \in X$ . Птадаје  $\Psi(g)(\Theta(g^{-1}, y)) = \Theta(g, \Theta(g^{-1}, y)) \stackrel{?}{=} \Theta(gg^{-1}, y) = \Theta(e, y) \stackrel{?}{=} y$ .

СТАВ:

2°  $\Psi$  је хомоморфизам:

Вашти  $\Psi(gh)(x) = \Theta(gh, x) \stackrel{?}{=} \Theta(g, \Theta(h, x)) = \Psi(g)(\Theta(h, x)) = \Psi(g)(\Psi(h)(x)) = (\Psi(g) \circ \Psi(h))(x)$

( $\Leftarrow$ ): Некаје  $\Psi: G \rightarrow S_X$  хомоморфизам. Дефинишемо  $\Theta: G \times X \rightarrow X$  да  $\Theta(g, x) := \Psi(g)(x)$ . Докажимо да  $\Theta$  задовољава 1), 2) из А1.92.

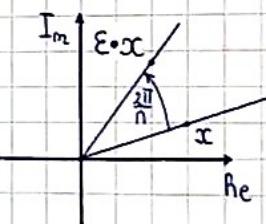
$$\begin{aligned} 1) \quad \Theta(e, x) &= \Psi(e)(x) \stackrel{(*)}{=} (d(x)) = x \quad (*) : \Psi \text{ је хомоморфизам} \Rightarrow \text{Некаје симетрија у Некаји}: \Psi(e) = id \\ 2) \quad \Theta(gh, x) &= \Psi(gh)(x) = (\Psi(g) \circ \Psi(h))(x) = \Psi(g)(\Psi(h)(x)) = \Theta(g, \Theta(h, x)) \end{aligned}$$

КОМЕНТАР: Чини смо  $\Theta(g, x)$  из А1.92 скраћено пишемо  $g \cdot x$ . Птада се 1) и 2) записују:

$$\begin{aligned} 1) \quad e \cdot x &= x \\ 2) \quad g \cdot (h \cdot x) &= (gh) \cdot x \end{aligned}$$

ПРИМЕР:  $X = \mathbb{C}$  и  $G = C_n = \{1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}\}$   $\varepsilon = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$

Птада  $G$  дејствује на  $X$  са:  $g \cdot x = gx$ .



ПРИМЕР:  $X = \{1, 2, \dots, n\}$ ,  $G = S_n$ . Птада  $G$  дејствује на  $X$  са  $\Pi \cdot x = \Pi(x)$ .

ПРИМЕР: Некаје  $G$  група. Птада  $G$  дејствује на  $G$  са:  $g \cdot x = gxg^{-1}$ . (којјусаџија)

Овоје је заметна дејативо, јер: 1)  $e \cdot x = exe^{-1} = x$

$$2) \quad g \cdot (h \cdot x) = g \cdot (hxh^{-1}) = ghxh^{-1}h^{-1} = ghx(h^{-1}h) = (gh) \cdot x$$

ДЕФ. Нека група  $G$  дејствује на скупу  $X$ . ОВАДА елеменита  $x \in X$  у означи  $\Omega(x)$ , дефинише се са:  $\Omega(x) = \{g \cdot x \mid g \in G\}$ , а СТАБИЛIZATOR, у означи  $\Sigma_x$ ,  $\Sigma_x = \{g \in G \mid g \cdot x = x\}$ .

КОМЕНТАР:  $\Omega(x) \subseteq X$ ,  $\Sigma_x \subseteq G$ . Птакоје,  $x \in \Omega(x)$ , а  $e \in \Sigma_x$ .

- На  $X$  уводимо релацију  $\sim$  са  $x \sim y$  ако  $y = g \cdot x$  за неко  $g \in G$ . Докажимо да је  $\sim$  релација еквиваленције.

(P):  $x \sim x$ , јер је  $x = e \cdot x$

(C): Некаје  $x \sim y$ . Птада постоји  $g \in G$  тај.  $y = g \cdot x / g^{-1} \cdot e$ . Следи  $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) \stackrel{?}{=} x$

$$\stackrel{?}{=} (g^{-1}g) \cdot x = e \cdot x \stackrel{?}{=} x, па је  $y \sim x$ .$$

ПОСЛЕДИЦА:

док

(T)

gov

a = b

(T): Нека је  $x \sim y$  и  $y \sim z$ . Тада постоје  $g, h \in G$  па  $y = g \cdot x$ , а  $z = h \cdot y$ . Следи:  
 $z = h \cdot y = h \cdot (g \cdot x) \stackrel{?}{=} (hg) \cdot x$ , па је  $x \sim z$ .

• Класа еквиваленције елемента  $x$  у односу на  $\sim$  је:  $\{y \mid x \sim y\} = \Omega(x)$ , па ћати:

$$1. x \in \Omega(x)$$

$$2. \text{за све } x, y \in X \text{ је } \Omega(x) \cap \Omega(y) = \emptyset \text{ или } \Omega(x) = \Omega(y)$$

$$\bigcup_{x \in X} \Omega(x) = X$$

 X  
издевен на орбите.

СТАВ: Нека је  $X$  непразан скуп и  $G$  група која дејствује на  $X$ . Тада за свако  $x \in X$  ванти  $\Sigma_x \leq G$  и постоји бијекција између  $\Omega(x)$  и  $G/\Sigma_x$ .

ДОКАЗ: Докажимо прво да је  $\Sigma_x \leq G$ . Како је  $e \in \Sigma_x$ , ако  $\Sigma_x + \emptyset$ , па је добар доказати да за  $g, h \in \Sigma_x$  ванти  $gh^{-1} \in \Sigma_x$ . Ванти  $g \cdot x = x$  и  $h \cdot x = x / h^{-1}$ . Тада је  $h^{-1} \cdot x = h^{-1} \cdot (h \cdot x) \stackrel{?}{=} (h^{-1}h) \cdot x = e \cdot x \stackrel{?}{=} x$ , па је  $(gh^{-1}) \cdot x \stackrel{?}{=} g \cdot (\underbrace{h^{-1} \cdot x}_{x}) = g \cdot x = x$ , па је заиста  $gh^{-1} \in \Sigma_x$ . Докажимо и други део.  
Добар је доказати да је  $F: G/\Sigma_x \rightarrow \Omega(x)$ , задато са  $F(g\Sigma_x) = g \cdot x$ , бијекција.

1°  $F$  је добро дефинисано:

$$\text{Ванти } g \Sigma_x = h \Sigma_x \text{ ако } g^{-1}h \in \Sigma_x \text{ ако } (g^{-1}h) \cdot x = x / g \cdot x$$

$$\stackrel{(*)}{\rightarrow} g \cdot x = g \cdot ((g^{-1}h) \cdot x) \stackrel{?}{=} (gg^{-1}h) \cdot x = h \cdot x \text{ ако } F(g \Sigma_x) = F(h \Sigma_x).$$

2°  $F$  је бијекција

2.1°  $F$  је "НА": по дефиницији  $\Omega(x)$

2.2°  $F$  је "1-1": добар је доказати да на месецу (\*) ванти ( $\leftrightarrow$ ), тј. да из  $g \cdot x = h \cdot x$  следи  $(g^{-1}h) \cdot x = x$ . Заиста, ванти  $g^{-1}(g \cdot x) = g^{-1}(h \cdot x) \stackrel{?}{=} (g^{-1}h) \cdot x$   
 $\stackrel{P_2}{\rightarrow} (g^{-1}g) \cdot x = e \cdot x \stackrel{?}{=} x$ .

ПОСЛЕДИЦА: Ако коначна група  $G$  дејствује на скупу  $X$ , па за свако  $x \in X$  ванти  $|G| = |\Omega(x)| \cdot |\Sigma_x|$ .

ДОКАЗ: Још преходном ставу је  $|\Omega(x)| = |G/\Sigma_x| = [G : \Sigma_x] = \frac{|G|}{|\Sigma_x|}$  Лагранж

(+) (Клашијева): Нека је  $G$  коначна група и  $p$  прости број који дели  $|G|$ . Тада у  $G$  постоји елемент реда  $p$ .

ДОКАЗ: Нека је  $X = \{(g_0, g_1, \dots, g_{p-1}) \mid g \in G, g_0 \cdots g_{p-1} = e\}$ . Тада ванти:  $|X| = |G|^p$ , јер је  $g^{p-1}$

јединствено одређен избором  $g_0, \dots, g_{p-2}$  ( $g_{p-1} = (g_0 \cdots g_{p-2})^{-1}$ ). Свејујмо, редни  $|X|$ .

Примештајмо да је  $w(g) = p$  ако  $g \neq e$  и  $w(g) = 1$  (јер тада  $w(g) \mid p$  и  $w(g) \neq 1$ ) ако  $g = e$

и  $(g, g, \dots, g) \in X$ . Дефинишемо дејство групе  $Z_p$  на  $X$  са:  $n \cdot (g_0, g_1, \dots, g_{p-1}) = (g_0, g_{(n+1) \cdot p}, \dots, g_{(n+(p-1)) \cdot p})$ .

Ово је дејство, јер је  $(g_0, g_1, \dots, g_{p-1}, g_0, g_1, \dots, g_{p-1}) \in X$  (из  $(g_0, \dots, g_{p-1}) = e$  следи

$a = g^{-1} \leftarrow g_0 \cdots g_{p-1} = (g_0 \cdots g_{p-1})^{-1}$ , па је). Правила 1) и 2) се тако проверавају. Нека су  $\Omega_1, \dots, \Omega_k$  све

различне орбите при овом дејству. Тада ванти:  $|\Omega_1| + |\Omega_2| + \dots + |\Omega_k| = |X|$ , а за свако  $\Omega_i$  ванти

$|\Omega_i|$  дели  $|Z^g| = p$ , па  $|\Omega_i| \in \{1, p\}$ . Примештавши да је  $\Omega(e, e, \dots, e) = \{(e, e, \dots, e)\}$ , па како је  $|X|$  делив са  $p$ , што посматрији барем  $p$  бројева  $1 \leq i \leq k$  таквих да  $|\Omega_i| = 1$ . Свеукупно, постоји  $1 \leq i \leq k$  тај  $\Omega_i = \{(g, \dots, g)\}$  за неко  $g \neq e$ . Платаје и  $w(g) = p$ , чиме је доказ завршен.

- Нека је  $G$  група која дејствује на  $X$ . Платаја  $\Omega$  дефинишено  $X^g = \{x \in X \mid g \cdot x = x\}$ , што је фикси скуп елемената  $g \in G$ .

(†) (Бернсдова лема): Нека коначна група  $G$  дејствује на коначном скупу  $X$ . Платајни:

$$|X/G| = \frac{|G|}{|\Omega|} \cdot \sum_{g \in G} |\Omega^g|, \text{ где је } X/G \text{ означен скуп орбита при овом дејству.}$$

ДОКАЗ: Помните да је  $S = \{(g, x) \in G \times X \mid g \cdot x = x\}$ . Платајни:

ОВДЕ ЧИНЕ ОПРЕДЕЛУЈУЋИ

$$S = \bigsqcup_{g \in G} \{g\} \times X^g = \bigsqcup_{g \in G} \sum_{x \in X^g} \{x\}, \text{ па је } |S| = \sum_{g \in G} |X^g| = \sum_{x \in X} |\sum_{x \in \Omega_x}|. \text{ Нека су } \Omega_1, \Omega_2, \dots, \Omega_k \text{ све различите орбите при овом дејству. Платаје: } \sum_{x \in X} |\sum_{x \in \Omega_x}| = \sum_{i=1}^k \sum_{x \in \Omega_i} |\sum_{x \in \Omega_x}| \stackrel{(*)}{=} \sum_{i=1}^k \sum_{x \in \Omega_i} |\Omega(x)|$$

$$(*) : |G| = |\Omega(x)| \cdot |\sum_{x \in \Omega_x}|$$

$$(**) : x \in \Omega_i \Rightarrow \Omega_i = \Omega(x)$$

$$\begin{aligned} & \stackrel{(**)}{=} \sum_{i=1}^k \sum_{x \in \Omega_i} \frac{|G|}{|\Omega_i|} \\ & = \sum_{i=1}^k |\Omega_i| \frac{|G|}{|\Omega_i|} \\ & = \sum_{i=1}^k |G| = k \cdot |G| \\ & = |X/G| \cdot |G| \end{aligned}$$

ПРИМЕР: Округла торба је подељена на 4 једнака парчета. На свако парче дејствује посебаној цветнију једне од 3 боје. На колико различитих начина што можемо да уредимо?



$X$ - скуп украсавања „фиксиране“ торбе:  $|X| = 3^4$ . На  $X$  дејствује група  $\{id, S, S^2, S^3\}$ , где је  $S$  ротација за  $90^\circ$  око центра. Оно што нас занима је статистика разних орбита при овом дејству.

$$|X^0| = 3 \quad |X^{S^2}| = 3^2 \quad |X^{S^3}| = 3 \quad |X^{id}| = 3^4$$

САМО 1 БОЈА

4

4 4  
ПЧ ПЧ  $\sim 120^\circ$ -иста

•  $D_6$  (множина га окрећају)

1.105.

СТАБ:

Нека  $G$  дејствује на  $X$ . Ако су  $g, h \in G$  конјуговани елементи, тада постоји бијекција између  $X^g$  и  $X^h$ .

6

## КОНАЧНО ГЕНЕРИСАНЕ АБЕЛОВЕ ГРУПЕ

ПОДСЕТНИК:  $G$  је генерирана скупом  $S$  ако ванни  $G = \langle S \rangle$ , ш.  $G = \langle S \rangle = \{x_1, x_2, \dots, x_n \mid n \in \mathbb{N}, x \in S \cup S^{-1}\}$

НОТАЦИЈА: Једанаест група операција означавају се  $+$  (а не  $a \cdot$ ). Платаји  $n$ -ти степен елемената а означавају се  $(a^n)$ .

Инверз елемената означавају се  $-a$ , а неутрал са 0.

- Нека је  $A$  Абелова група генерисана конечним скупом  $S = \{a_1, a_2, \dots, a_k\}$ . Тада је:
 
$$A = \langle S \rangle = \{n_1 a_1 + n_2 a_2 + \dots + n_k a_k \mid n_i \in \mathbb{Z}\}.$$
 Приметимо да је  $\langle a_i \rangle = \{n_i a_i \mid n_i \in \mathbb{Z}\}$ , па је:
 
$$A = \langle S \rangle = \langle a_1 \rangle + \langle a_2 \rangle + \dots + \langle a_k \rangle.$$
  - Нека је  $A$  Абелова група и  $A_1, A_2, \dots, A_k \leq A$ . Тада је  $A$  сума ових подгрупа ако вати:
 
$$A = A_1 + A_2 + \dots + A_k.$$
 Ова сума је директна ако се сваки елемент  $a \in A$  може записати на јединствен начин:
 
$$a_1 + a_2 + \dots + a_k = a,$$
 где је  $a_i \in A_i$ , за  $1 \leq i \leq k$ .
  - Абелова група  $A$  је директна сума свога подгрупа  $A_1, A_2, \dots, A_k$  ако  $(A_1 + \dots + A_{i-1}) \cap A_i = \{0\}$ 

у облику:

$\vdash$

15: Абелова група  $A$  је директна сума свога подгрупа  $A_1, A_2, \dots, A_k$  ако  $(A_1 + \dots + A_{i-1}) \cap A_i = \{0\}$

Ипредпоставка:  
да сваки подгрупа

тк.  
јесто  
да је та директна

а3:  $\vdash$

због јединствености записа, вати  $a_1 = 0, a_2 = 0, \dots, a_{i-1} = 0, 0 = a_i$ , па је  $a = 0$ .

а<sub>i</sub> ∈ A<sub>i</sub>

тј јер је  $a \in A_1 + A_2 + \dots + A_{i-1}$

тј јер је  $a \in A_i$

а = a<sub>1</sub> + a<sub>2</sub> + ... + a<sub>i</sub> = a<sub>1</sub>' + a<sub>2</sub>' + ... + a<sub>i</sub>', где је a<sub>i</sub>, a<sub>i</sub>' ∈ A<sub>i</sub>. Тада је

3

- Враћају се на случај  $A = \langle S \rangle$ , где је  $S = \langle a_1, a_2, \dots, a_k \rangle$ . Потој  $A = \langle a_1 \rangle + \langle a_2 \rangle + \dots + \langle a_k \rangle$ , а ова сума је директна АККОУЗ  $\eta_1 a_1 + \eta_2 a_2 + \dots + \eta_k a_k = 0$  следи  $\eta_1 a_1 = 0, \eta_2 a_2 = 0, \dots, \eta_k a_k = 0$ .
  - Ако је  $A$  директна сума свогих подструја  $A_1, \dots, A_k$ , тада пишемо:  $A = A_1 \oplus A_2 \oplus \dots \oplus A_k$ .

**СТАВ:** Нека је  $A$  једногодишња трупа која је директна сума свогих подтрупа  $A_1, \dots, A_k$ . Тада је:

$$A \cong A_1 \times A_2 \times \dots \times A_k$$

**доказ:** Довољно је доказати да је  $F: A_1 \times A_2 \times \dots \times A_k \rightarrow A_1 \oplus A_2 \oplus \dots \oplus A_k$ , загатио са  $F(a_1, \dots, a_k) = a_1 + \dots + a_k$  изоморфизам.

$$1^{\circ} F \text{ је хомонорфизам: } \begin{aligned} \text{Ваша формула: } F((a_1, \dots, a_k) + (a'_1, \dots, a'_k)) &= F(a_1 + a'_1, a_2 + a'_2, \dots, a_k + a'_k) \\ &= a_1 + a'_1 + a_2 + a'_2 + \dots + a_k + a'_k \\ &= a_1 + a_2 + \dots + a_k + a'_1 + a'_2 + \dots + a'_k \\ &= F(a_1, \dots, a_k) + F(a'_1, \dots, a'_k) \end{aligned}$$

(комутативност)

2º Fje δυσκολια:

2.1°  $F_{je, HA}$ : по дефиницији  $A_1 + \dots + A_k$

2.2 Fje „1-1“: Bemerk  $F(a_1, \dots, a_k) = F(a'_1, \dots, a'_k)$  wenn  $a_1 + \dots + a_k = a'_1 + \dots + a'_k = a$ , und um

єдинственості записа елемента  $a$  сліди  $a_i = a'_i$ ,  $1 \leq i \leq k$ .

- Нека је  $A$  Абелова група и  $x_1, x_2, \dots, x_k \in A$ . Тада је  $\langle x_1, x_2, \dots, x_k \rangle = \langle x_1 + n_1 x_2 + \dots + n_k x_k, x_2, \dots, x_k \rangle$  за произвољне  $n_1, \dots, n_k \in \mathbb{Z}$ .

**доказ:** Означимо  $B = \langle x_1, \dots, x_k \rangle$  и  $C = \langle x_1 + n_1 x_2 + \dots + n_k x_k, x_2, \dots, x_k \rangle$ . Јако је  $B$  (односно  $C$ ) минимална подгрупа од  $A$  која садржи скуп  $\{x_1, \dots, x_k\}$  (односно  $\{x_1 + n_1 x_2 + \dots + n_k x_k, x_2, \dots, x_k\}$ ), па је довољно доказати да је  $\{x_1, \dots, x_k\} \subseteq C$  и  $\{x_1 + n_1 x_2 + \dots + n_k x_k, x_2, \dots, x_k\} \subseteq B$ , ај.  $x_i \in C$  и  $x_1 + n_1 x_2 + \dots + n_k x_k \in B$ . Друго следи директно, а прво из  $x_i = 1 \cdot (x_1 + n_1 x_2 + \dots + n_k x_k) + (-n_1)x_2 + \dots + (-n_k)x_k$ .

### НОРМАЛНА ФОРМА КОНАЧНО ГЕНЕРИСАНЕ АБЕЛОВЕ ГРУПЕ

- ⊕ Нека је  $A$  коначно генерисана Абелова група. Тада постоји  $k, l > 0$  и  $d_1, d_2, \dots, d_k \geq 2$  т.д.

$d_1 | d_2, d_2 | d_3, \dots, d_{k-1} | d_k$  и  $A \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \dots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^l$ . Уз то, такви  $k, l$  и  $d_i$  су јединствени.

**КОМЕНТАР:** Ако је  $k=0$ , тада је  $A \cong \mathbb{Z}^l$ , а ако је  $l=0$ , тада је  $A \cong \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_k}$ .

$$\text{пример: 1) } \mathbb{Z}_3 \times \mathbb{Z}_{20} = \mathbb{Z}_3 \times \mathbb{Z}_{4 \cdot 5} \stackrel{\text{НДД}(4,5)=1}{=} \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \stackrel{\text{НДД}(4,5)=1}{=} \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \stackrel{\text{НДД}(3,5)=1}{=} \mathbb{Z}_4 \times \mathbb{Z}_{15} \stackrel{\text{НДД}(4,15)=1}{=}$$

$$\text{2) } \mathbb{Z}_{20} \times \mathbb{Z}_{30} \times \mathbb{Z}_{50} = \mathbb{Z}_{2 \cdot 5} \times \mathbb{Z}_{2 \cdot 3 \cdot 5} \times \mathbb{Z}_{8 \cdot 5^2} \stackrel{\text{НДД}(2,5)=1}{=} \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2} \\ \stackrel{\text{НДД}(2,5)=1}{=} \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_5}_{\mathbb{Z}_{10}} \times \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_3}_{\mathbb{Z}_6} \times \underbrace{\mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5}_{\mathbb{Z}_{300}} \stackrel{\text{НДД}(6,300)=1}{=} \mathbb{Z}_{10} \times \mathbb{Z}_6 \times \mathbb{Z}_{300}$$

⊕

### ГЕНЕРАТОРЦИ И РЕЛАЦИЈЕ

пример: 1)  $D_n = \langle \varphi, \sigma \rangle$ , а релације су  $\varphi^n = \text{id}$ ,  $\sigma^2 = \text{id}$ ,  $\varphi\sigma = \sigma\varphi^{n-1}$

2)  $\mathbb{Z} = \langle 1 \rangle$ , нема релације (слободна група - не монично добијен о сабирању јединица)

3)  $\mathbb{Z}_n = \langle 1 \rangle$ , а релација је  $n \cdot 1 = 0$ .

- \* Нека је  $A$  Абелова група генерисана скупом  $\{x_1, \dots, x_k\}$  који задовољава систем релација:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1k}x_k &= 0 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2k}x_k &= 0 \\ \vdots & \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mk}x_k &= 0 \end{aligned}$$

$$(*) \quad \text{т.д. су } a_{ij} \in \mathbb{Z}.$$

пример: Пресликавање  $f_n: \mathbb{Z} \rightarrow \mathbb{Z}_n$  задато са  $f_n(k) =$  осцилација при дешету  $k$  са  $n$  је хомоморфизам, па по

⊕ о изоморфизму вали  $\mathbb{Z}/\text{Ker } f_n \cong \text{Im } f_n$ . Како је  $\text{Im } f_n = \mathbb{Z}_n$ , а  $\text{Ker } f_n = n \cdot \mathbb{Z} = \langle n \rangle$ ,

што је  $\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$ .

\* Група разматрана на почетку дотлаква задати генераторима и релацијама је изоморфна са

$\mathbb{Z}^k / \langle (a_{11}, a_{12}, \dots, a_{1k}), \dots, (a_{m1}, a_{m2}, \dots, a_{mk}) \rangle$ . Генератору  $x_i$  одговара  $(0, 0, \dots, 1, 0, \dots, 0) + \langle (a_{1i}, a_{2i}, \dots, a_{ki}) \rangle$ .

Систему релација  $(*)$  придржаној матрици

$$\left[ \begin{array}{cccc} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mk} \end{array} \right] = M_{m,k}(\mathbb{Z}).$$

пример

2ed

НОТА

$\mathbb{Z}$  (матрице)  
ко:

$(1, 0, \dots, 0)$ ,

$(0, 1, \dots, 0)$ ,

$(0, 0, \dots, 0, 1)$ .

- Наровно, и свакој матрици из  $M_{m,k}(\mathbb{Z})$  може приврзанији један систем релација.
- Примешавши да ако на матрицу применено следеће операције, структурата група се не мења:

$$\begin{array}{ll} 1 & V_i \leftrightarrow V_j \quad (\text{замена места } i\text{-тре и } j\text{-тре врсте}) \\ 2 & V_i \rightarrow -V_i \\ 3 & V_i \rightarrow V_i + \lambda V_j, \text{ за } i \neq j, \lambda \in \mathbb{Z} \end{array}$$

• Оваки операцијама се не мења структура којом "сечено" (за последњу операцију) обављају из творења (\*)-кета)

- Слично, група се не мења ни када исте операције применимо на колоне (што чини, добијамо групу изоморфну полазнији).

$$\begin{array}{ll} 1 & K_i \leftrightarrow K_j \quad (\text{замена места } i\text{-те и } j\text{-те колоне - замена } x_i \text{ и } x_j \text{ - координате}) \\ 2 & K_i \rightarrow -K_i \quad (\text{замена генератора } x_i \text{ са } -x_i) \\ 3 & K_i \rightarrow K_i + \lambda K_j, \text{ за } i \neq j, \lambda \in \mathbb{Z} \quad (\text{добијамо следећи систем релација:}) \end{array}$$

$$\begin{aligned} a_{11}x_1 + \dots + (a_{1i} + \lambda a_{1j})x_i + \dots + a_{1j}x_j - \lambda x_i + \dots + a_{1k}x_k &= 0 \\ a_{m1}x_1 + \dots + (a_{mi} + \lambda a_{mj})x_i + \dots + a_{mj}x_j - \lambda x_i + \dots + a_{mk}x_k &= 0 \end{aligned}$$

• Група се не мења јер је довољно генератор  $x_j$  заменити генератором  $x_j - \lambda x_i$  (што не мења групу по (\*))

- Абелова група генерирана са  $\{x_1, \dots, x_k\}$  и системом релација:  $d_1x_1 = 0$ ,  $d_2x_2 = 0$ ,  $\dots$ ,  $d_kx_k = 0$ , за  $t \leq k$ ,

шагаје  $A \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \dots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^{k-t}$ .

- (t) Нека је  $M \in M_{m,k}(\mathbb{Z})$ . Пада се матрица  $M$  постоту операција над колонама и врстама које смо прешходно навели јоне свесни на матрицу облика:  $\begin{bmatrix} d_1 & 0 & 0 & 0 & 0 \\ 0 & d_2 & 0 & 0 & 0 \\ 0 & 0 & d_3 & 0 & 0 \\ 0 & 0 & 0 & d_4 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$ , за неко  $t \leq k$  и  $d_1, \dots, d_t \in \mathbb{N}$  тј.  $d_1d_2, d_2d_3, \dots, d_{t-1}d_t$ .

пример:  $k=3, t=4$

$$\begin{array}{c} \leftarrow \\ \begin{bmatrix} 6 & 4 & -8 \\ 4 & -12 & 6 \\ 10 & 6 & -8 \\ -8 & 12 & 14 \end{bmatrix} \sim \begin{bmatrix} 2 & 16 & -14 \\ 4 & -12 & 6 \\ 10 & 6 & -8 \\ -8 & 12 & 14 \end{bmatrix} \xrightarrow{\begin{array}{l} \text{1. } \\ \text{2. } \\ \text{3. } \\ \text{4. } \end{array}} \begin{bmatrix} 2 & 16 & -14 \\ 0 & -44 & 34 \\ 0 & -74 & 62 \\ 0 & 76 & -42 \end{bmatrix} \sim \begin{bmatrix} 2 & 0 & 0 \\ 0 & -44 & 34 \\ 0 & -74 & 62 \\ 0 & 76 & -42 \end{bmatrix} \xrightarrow{\begin{array}{l} \text{1. } \\ \text{2. } \\ \text{3. } \\ \text{4. } \end{array}} \begin{bmatrix} 2 & 0 & 0 \\ 0 & 24 & 34 \\ 0 & 50 & 62 \\ 0 & -8 & -42 \end{bmatrix} \sim \begin{bmatrix} 2 & 0 & 0 \\ 0 & 24 & 10 \\ 0 & 50 & 12 \\ 0 & -8 & -34 \end{bmatrix} \sim \dots \end{array}$$

обе остале које су уквирених - тоје 2

П10

## КОМУТАТИВНИ ПРСТЕНИ СА ЈЕДИНИЦОМ

дефиниција: Абеларска структура  $(A, +, \cdot)$  је комутативни прстен са јединицом ако су  $+$  и  $\cdot$  бинарне

- операције за које важи:
- $(A, +)$  је Абелова група
  - $\cdot$  је обликјативна и комутативна
  - постоји чврсто за  $\cdot$
  - $(\forall x, y, z \in A) x \cdot (y + z) = (x \cdot y) + (x \cdot z)$

нотација: Неуштрај за  $\cdot$  означавамо са  $1$  (или  $1_A$ , ако постоји могућност забуње), а неуштрај за  $+$  са  $0$  (или  $0_A$ ). Чврз у односу на сабирање елемената а означавамо са  $-a$  и пишемо  $a-b$

(или  $0_A$ ). Чврз у односу на умножавање елемената а означавамо са  $-a$  и пишемо  $x-y$  и  $x-z$ . За бисмо поједноставши запис, учинамо да  $\cdot$  има превосност у односу на  $+$ , па унесмо  $(x-y) + (x-z)$  пишемо  $xy + xz$ .

примери: 1)  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$

} КПЈ

2)  $(\mathbb{Z}, +, \cdot)$

3)  $(\mathbb{Z}_n, +_n, \cdot_n)$

4)  $(M_n(\mathbb{R}), +, \cdot)$  је прешен са јединицом.

тврђење

доку

терђење: Нека је  $A$  кпј и  $a \in A$ . Тада ватни: 1)  $0 \cdot a = 0$  2)  $-a = (-1) \cdot a$  3)  $(-a) \cdot b = -(a \cdot b)$  ( $b \in A$ )

доказ: 1) Ватни:  $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$  / $-(0 \cdot a)$ , па следи  $0 = 0 \cdot a$ .

2) Следи из 3).

3) Ватни:  $0 \neq 0 \cdot b = (a+(-a)) \cdot b = a \cdot b + (-a) \cdot b$ , па из јединствености инверза за  $a$  следи

$$-(a \cdot b) = (-a) \cdot b$$

коментар: Под инверзом ћемо увек подразумевати инверз у односу на  $\cdot$ .

деф. Нека је  $A$  кпј. Тада скуп свих елемената из  $A$  који имају инверз означавамо са:

$$U(A) = \{a \in A \mid (\exists b \in A) a \cdot b = 1\}$$

инверз елемената (ако постоји)  $x$  означавамо са  $x^{-1}$ .

ст

гол

терђење: Нека је  $A$  кпј. Тада је  $(U(A), \cdot)$  група.

доказ: Како је  $1 \in U(A)$  (јер  $1 \cdot 1 = 1$ ), па  $U(A) \neq \emptyset$ , па је довољно доказати да за  $x, y \in U(A)$  ватни су  $x^{-1}$  и  $y^{-1}$ .

Из  $x, y \in U(A)$  следи да постоји  $z, t \in A$  тај.  $xz = 1$  и  $yt = 1$ . Тада је  $t = y^{-1}$ , па ватни:

$$xy^{-1}yz = xtyz = \underset{-1}{xz} \underset{-1}{yt} = 1, \text{ тј. } xy^{-1} \in U(A)$$

примери: 1)  $U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$ ,  $U(\mathbb{R}) = \mathbb{R} \setminus \{0\}$   $U(\mathbb{C}) = \mathbb{C} \setminus \{0\}$

2)  $U(\mathbb{Z}) = \{1, -1\}$

3)  $U(\mathbb{Z}_n) = \overline{\Phi}(n)$

2e

деф. Кпј  $A$  је поље ако ватни  $U(A) = A \setminus \{0\}$ .

примери:  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$  су поља, а  $(\mathbb{Z}, +, \cdot)$  није поље.

$(\mathbb{Z}_n, +_n, \cdot_n)$  је поље ако је  $n$  прости број.

пример: Нека је  $A$  кпј. Тада је  $A[x]$  (прешен полинома са коефицијентима у  $A$ ):  $(A[x], +, \cdot)$  кпј.

За  $p \in A[x]$  са  $\deg(p)$  означавамо степен полинома  $p$ . Тада:  $\deg(pq) \leq \deg(p) + \deg(q)$ .

У  $\mathbb{Z}_6[x]$  не мора да ватни једнакост, јер је нпр.  $(2x+1)(3x+1) = 5x+1$ .

деф. Нека је  $A$  кпј. За елемент  $a \in A \setminus \{0\}$  кажемо да је ПРАВИ ДЕЛИТЕЉ НУЛЕ ако постоји  $b \in A \setminus \{0\}$  тај.  $a \cdot b = 0$ . Скуп свих делитеља нула означавамо са  $I(A)$  (то су прави делитељеви нуле и 0).

деф. Нека је  $A$  кпј. За елемент  $a \in A$  кажемо да је РЕГУЛАРАН ако за све  $x, y \in A$  ватни:  $ax = ay \Rightarrow x = y$ . Скуп свих регуларних елемената означавамо са  $R(A)$ .

примери: 1)  $I(\mathbb{Q}) = \{0\}$ ,  $R(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$ ,  $U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$

2)  $I(\mathbb{Z}) = \{0\}$ ,  $R(\mathbb{Z}) = \mathbb{Z} \setminus \{0\}$ ,  $U(\mathbb{Z}) = \{1, -1\}$  и слично за  $\mathbb{R}$  и  $\mathbb{C}$ .

3)  $I(\mathbb{Z}_n) = \mathbb{Z}_n \setminus \overline{\Phi}(n)$ ,  $R(\mathbb{Z}_n) = \overline{\Phi}(n)$ ,  $U(\mathbb{Z}_n) = \overline{\Phi}(n)$

2

пр

о

п

т

**тврђење:** Нека је  $A$  кпј. Тада је  $U(A) \subseteq R(A)$ .

**доказ:** Нека је  $a \in U(A)$ . Тада постоји  $b \in A$  па  $a \cdot b = 1$ . Зашто вати:  $ax = ay \Rightarrow bx = by \Rightarrow x = y$ , па је  $a \in R(A)$ .

**тврђење:** Нека је  $A$  кпј. Тада је елемент  $a \in A$  регуларан ако и тоје делитељ нуле.

**доказ:** ( $\Rightarrow$ ): Нека је  $a \cdot b = 0$ . Довољно је доказати да тада мора бити  $b = 0$ .

Како је  $a \cdot b = 0 = a \cdot 0$ , из  $a \in R(A)$  следи  $b = 0$ .

( $\Leftarrow$ ): Нека је  $ax = ay$ . Следи  $ax - ay = a(x - y) = 0$ , па како а није делитељ нуле, то је  $x - y = 0$ , што је  $x = y$ . Следи  $a \in R(A)$ .

\* Код коначних кпј: РЕГУЛАРАН  $\Leftrightarrow$  ЧИНЕРГИЧАН

**став:** Нека је  $A$  кпј. Тада вати  $U(A) = R(A)$ .

**доказ:** Нека је  $a \in R(A)$ . Довољно је доказати да је  $a \in U(A)$ , тј. да постоји  $b \in A$ , па  $a \cdot b = 1$ .

Посматрајмо скуп  $\{a \cdot b \mid b \in R(A)\}$ . Како је  $a \in R(A)$ , то су елементи  $a \cdot b$  различити, па вати

$|\{a \cdot b \mid b \in R(A)\}| = |R(A)|$ . Зашто је довољно доказати да  $\{a \cdot b \mid b \in R(A)\} \subseteq R(A)$ , јер тада

$1 \in R(A) = \{a \cdot b \mid b \in R(A)\}$ . другачија, довољно је доказати да за  $a, b \in R(A)$  вати  $a \cdot b \in R(A)$ .

Заснива се, за  $x, y \in A$  вати  $abx = aby \Rightarrow bx = by \Rightarrow x = y$ .

јер  $a \in R(A)$  јер  $b \in R(A)$

**деф.** Нека је  $A$  кпј. Тада је  $A$  обласц целих (или домен) ако вати  $R(A) = A \setminus \{0\}$ .

- $A$  ПОЉЕ  $\Rightarrow A$  ДОМЕН
- $A$  КОНАЧАН И ДОМЕН  $\Rightarrow A$  ПОЉЕ

### ПОТПРСТЕН И ИДЕАЛ

**деф.** Нека су  $(A, +, \cdot)$  и  $(B, +', \cdot')$  кпј. Тада је  $(B, +', \cdot')$  потпрстен од  $(A, +, \cdot)$  ако вати  $B \subseteq A$ ,

$1_B = 1_A$  и за све  $x, y \in B$  вати  $x+y = x'+y'$  и  $x \cdot y = x' \cdot y'$ .

**пример:**  $(\mathbb{Z}, +, \cdot)$  је потпрстен од  $(\mathbb{Q}, +, \cdot)$ , а  $(\mathbb{Q}, +, \cdot)$  је потпрстен од  $(\mathbb{C}, +, \cdot)$ .

**деф.** Нека је  $A$  кпј. За  $I \subseteq A$ ,  $I \neq \emptyset$ , кажемо да је ИДЕАЛ у  $A$  ако вати:

- 1  $(\forall x, y \in I) x+y \in I$
- 2  $(\forall a \in A)(\forall x \in I) a \cdot x \in I$

Пишемо:  $I \triangleleft A$ .

**пример:** Нека је  $A$  кпј и  $x \in A$ . Тада је ГЛАВНИ ИДЕАЛ ГЕНЕРИСАН СА  $x$   $\langle x \rangle := \{ax \mid a \in A\}$ .

**тврђење:**  $\langle x \rangle \triangleleft A$ .

**доказ:** Доказ изводимо по дефиницији.

1 Нека су  $u, v \in \langle x \rangle$ . Тада је  $u=ax$ ,  $v=bx$ , па је  $u+v = ax+bx = (a+b)x \in \langle x \rangle$ .

2 Нека је  $a \in A$  и  $u \in \langle x \rangle$ . Тада је  $u=bx$ , па је  $au = abx \in \langle x \rangle$ .

**коментар:** Некаје  $I \triangleleft A$ . Тада за  $I$  важи  $0 \cdot x = 0 \in I$ , као и  $(-1) \cdot x = -x \in I$ , па је  $(I, +) \leq (A, +)$ .

**СТАВ:** Сваки идеал у  $\mathbb{Z}$  је тачни.

**ДОКАЗ:** Некаје  $I \triangleleft \mathbb{Z}$ . Тада је  $(I, +) \leq (\mathbb{Z}, +)$ , такавкоје  $(\mathbb{Z}, +)$  циклична, па је и  $(I, +)$  циклична, па је  $I = \langle n \rangle$ .

- Слично вали за  $(\mathbb{Z}_n, +_n, \cdot_n)$  (узвишени доказ).

**СТАВ:** Некаје  $K$  подаје и  $I \triangleleft K$ . Тада је  $I = \{0\}$  или  $I = K$ . (стријулни идеали)

**ДОКАЗ:** Довољно је доказати да ако посматрију  $a \in I \setminus \{0\}$  да је тада  $I = K$ . Некаје  $x \in K$ . Тада пошто је  $a \in K \setminus \{0\}$ , посматрију  $a^{-1} \in K$ , а сматријим  $xa^{-1}a = x \in I$ .

**ДЕФ.** Некаје  $A$  куп и  $I, J \triangleleft A$ . Тада дефинишење:

$$\begin{aligned} 1) \quad I+J &= \{x+y \mid x \in I, y \in J\} \\ 2) \quad I \cdot J &= \{x_1y_1 + \dots + x_ny_n \mid n \in \mathbb{N}, x_i \in I, y_i \in J\}. \end{aligned}$$

**СТАВ:** Некаје  $A$  куп и  $I, J \triangleleft A$ . Тада су  $I \cap J$ ,  $I+J$  и  $I \cdot J$  идеали у  $A$ .

**ДОКАЗ:** 1) Нека су  $x, y \in I \cap J$ . Тада је  $x, y \in I$  и  $x, y \in J$ , па је  $x+y \in I$ ,  $x+y \in J$  (јер  $I, J \triangleleft A$ ), па је  $x+y \in I \cap J$ .

Некаје  $a \in A$  и  $x \in I \cap J$ . Тада је  $x \in I$ ,  $x \in J$ , па је  $ax \in I$  и  $ax \in J$  (јер  $I, J \triangleleft A$ ), па је  $ax \in I \cap J$ .

2) Нека су  $x, y \in I+J$ . Тада је  $x = u_1 + v_1$ ,  $y = u_2 + v_2$ , за неке  $u_1, u_2 \in I$ ,  $v_1, v_2 \in J$ . Следи  $x+y = u_1 + v_1 + u_2 + v_2 = \underbrace{u_1 + u_2}_{\in I} + \underbrace{v_1 + v_2}_{\in J} \in I+J$ .

Некаје  $a \in A$  и  $x \in I+J$ . Тада је  $x = u+v$  за неке  $u \in I$ ,  $v \in J$ , па је  $ax = a(u+v) = au+av \in I+J$ .

3) Нека су  $x, y \in I \cdot J$ . Тада је  $x = u_1v_1 + \dots + u_nv_n$  и  $y = w_1t_1 + \dots + w_mt_m$  за неке  $u_i \in I$ ,  $v_i \in J$ ,  $w_j \in I$ ,  $t_j \in J$ . Следи  $x+y = u_1v_1 + \dots + u_nv_n + w_1t_1 + \dots + w_mt_m \in I \cdot J$ .

Некаје  $a \in A$  и  $x \in I \cdot J$ . Тада је  $x = u_iv_i + \dots + u_nv_n$  за неке  $u_i \in I$ ,  $v_i \in J$ . Следи:

$$ax = \underbrace{a u_1 v_1}_{\in I \cdot J} + \dots + \underbrace{a u_n v_n}_{\in I \cdot J} \in I \cdot J.$$

**ПРИМЕР:** Нека су  $m, n \in \mathbb{Z}$ .

$$\langle n \rangle \cap \langle m \rangle = \langle \text{H3C}(n, m) \rangle$$

$$\langle n \rangle + \langle m \rangle = \{kn+lm \mid k, l \in \mathbb{Z}\} = \langle \text{H3A}(n, m) \rangle$$

$$\langle n \rangle \cdot \langle m \rangle = \langle nm \rangle$$

**СТАВ:** Нека је  $K$  топс. Тада је сваки идеал у  $K[x]$  главни.

**СКИЦА ДОКАЗА:** У простијену  $K[x]$  важи лема о количнику и остатку, тј. за све  $f, g \in K[x]$ ,  $g \neq 0$ , постоје  $q, r \in K[x]$  тако да  $f = qg + r$  и  $\deg r < \deg g$ . Доказ у доказу I. Нека је сага  $I \triangleleft K[x]$ ,  $I \neq \{0\}$ . Узимамо  $g \in I \setminus \{0\}$  тако да  $\deg g$  најмање могуће. Испимо да доказатено даје  $I = \langle g \rangle$ . За ово је довољно доказати да за свако  $f \in I$  важи  $g \mid f$ . Нека је  $f \in I$ . Тада је  $f = qg + r$  за неке  $q, r \in K[x]$  тако да  $\deg r < \deg g$ . Важи  $r = f - qg \in I$ , па је  $r = 0$ , тј.  $g \mid f$ .

**КОМЕНТАР:** У  $\mathbb{Z}[x]$  НЕ ВАЖИ лема о количнику и остатку; најр. за  $f = x^2$ ,  $g = 2x$ :

$$x^2 = 2x \cdot \square + \square \quad \text{НЕ МОЖЕ!}$$

const.

**СТАВ:** У  $\mathbb{Z}[x]$  постоје идеали који нису главни.

**ДОКАЗ:** Доказатимо да идеал  $I = \langle 2 \rangle + \langle x \rangle$  нису главни. Важи  $I = \{a_0x^i + \dots + a_ix + 2a_0 \mid a_0, a_1, \dots, a_i \in \mathbb{Z}\}$ .

Доказатимо да  $I$  нису главни. ППС:  $I = \langle f \rangle$ . Када је  $2 \in I$ , па је  $f \mid 2$ , па је  $f \in \{1, 2, -1, -2\}$ .

Важи  $f \notin \{-1, 1\}$ , јер је у супротном  $\langle f \rangle = \mathbb{Z}[x] \neq I$ . Следи  $f \in \{2, -2\}$ . Међутим,  $2 \notin I$ , а  $-2 \in I$ .

### ХОМОНОРФИЗМИ КПЈ

**ДЕФ.** Нека су  $(A, +, \cdot)$  и  $(B, +', \cdot')$  кпј. Функција  $f: A \rightarrow B$  је хомонорфизам кпј ако за све  $x, y \in A$

- 1  $f(x+y) = f(x) +' f(y)$
- 2  $f(x \cdot y) = f(x) \cdot' f(y)$
- 3  $f(1_A) = 1_B$

**ПРИМЕР:** Нека је  $f_n: \mathbb{Z} \rightarrow \mathbb{Z}_n$  задато са  $f_n(k) =$  остатак при дељењу  $k$  на  $n$ . Тада је  $f_n$  хомонорфизам кпј.

**ДЕФ.** Нека је  $f: A \rightarrow B$  хомонорфизам кпј. ЈЕЗГРО овог хомонорфизма је  $\text{Ker}(f) = \{a \in A \mid f(a) = 0_B\}$ , а слика је  $\text{Im}(f) = \{f(a) \mid a \in A\}$ .

**СТАВ:** Нека је  $f: A \rightarrow B$  хомонорфизам кпј. Тада важи:

- 1  $\text{Ker}(f) \triangleleft A$
- 2 ако је  $J \triangleleft B$ , тада је  $f^{-1}[J] \triangleleft A$
- 3 ако је  $I \triangleleft A$  и  $f \circ h$ , тада је  $f[I] \triangleleft B$ .

**ДОДЕЛНИК:**  $f^{-1}[S] = \{x \in A \mid f(x) \in S\}$

**ДОКАЗ:** Важи  $\text{Ker}(f) = f^{-1}[\{0_B\}]$ , па како је  $\{0_B\} \triangleleft B$ , што 1 следи из 2.

2: Нека су  $x, y \in f^{-1}[J]$ . Тада је  $f(x), f(y) \in J$ , па је  $f(x) + f(y) = f(x+y)$ , тј.  $x+y \in f^{-1}[J]$ .

Нека је  $a \in A$  и  $x \in f^{-1}[J]$ . Тада је  $f(ax) = f(a) \cdot f(x) \in J$  (јер је  $J \triangleleft B$ ), па је  $ax \in f^{-1}[J]$ .

3: Нека су  $x, y \in f(I)$ . Тада је  $x = f(a_1)$ ,  $y = f(a_2)$  за неке  $a_1, a_2 \in I$ . Следи:  $x+y = f(a_1) + f(a_2) = f(\underbrace{a_1+a_2}_{\in I}) \in f(I)$ .

Нека је  $b \in B$  и  $x \in f(I)$ . Тада је  $x = f(a)$  за неко  $a \in I$ , као и  $b = f(a')$  за неко  $a' \in I$  (јер је  $f$  „на“), па је  $bx = f(a) \cdot f(a') = f(a'a) \in f(I)$ .

по  
дифиницији  
ЧЛЕНА  
(1), (2)

по  
дифиницији  
ЧЛЕНА  
(1), (2)

КОЛИЧНИЧКИ ПРСТЕН

2еф. Нека је  $A$  кпј и  $I \triangleleft A$ . Птага на  $A$  уврдито релацију  $\equiv (\text{mod } I)$  са  $a \equiv b \pmod{I}$  ако и дај.

КОМЕНТАР:  $\exists I = \langle n \rangle$ . Птага  $a \equiv b \pmod{n}$  ако  $a - b \in \langle n \rangle$  ако и дај  $a - b$ .

СТАВ:  $\equiv (\text{mod } I)$  је релација еквиваленције.

ДОКАЗ: (P):  $a \equiv a \pmod{I}$  јер је  $a - a = 0 \in I$ .

(C): Нека је  $a \equiv b \pmod{I}$ . Птага је  $a - b \in I$ , па је  $(-1)(a - b) = b - a \in I$  и следи  $b \equiv a \pmod{I}$ .

(T): Нека је  $a \equiv b \pmod{I}$ ,  $b \equiv c \pmod{I}$ . Птага је  $a - b, b - c \in I$ , па је  $\frac{a-b}{\in I} + \frac{b-c}{\in I} = a - c \in I$  и следи  $a \equiv c \pmod{I}$ .

ТВРЂЕЊЕ:  $\equiv (\text{mod } I)$  се сматре са  $+ \cdot$ .

ДОКАЗ: +: Доказујемо да из  $a_1 \equiv b_1 \pmod{I}$  и  $a_2 \equiv b_2 \pmod{I}$  следи  $a_1 + a_2 \equiv b_1 + b_2 \pmod{I}$ . Зашто, из  $a_1 \equiv b_1 \pmod{I}$  и  $a_2 \equiv b_2 \pmod{I}$  следи  $a_1 - b_1 \in I$  и  $a_2 - b_2 \in I$ , па  $a_1 - b_1 + a_2 - b_2 =$   
 $= (a_1 + a_2) - (b_1 + b_2)$ , тј.  $a_1 + a_2 \equiv b_1 + b_2 \pmod{I}$ .

•: Ако је  $a_1 \equiv b_1 \pmod{I}$  и  $a_2 \equiv b_2 \pmod{I}$ , па је  $a_1 - b_1, a_2 - b_2 \in I$ , па је  $a_1 a_2 - b_1 b_2 =$   
 $= \underbrace{a_2(a_1 - b_1)}_{\in I} + \underbrace{b_1(a_2 - b_2)}_{\in I} \in I$  и следи  $a_1 a_2 \equiv b_1 b_2 \pmod{I}$ .

⊗ Класе еквиваленције у односу на  $\equiv (\text{mod } I)$  су  $\{b | b \equiv a \pmod{I}\} = \{b | b - a \in I\} = a + I$ , што је очигледно леви посед поструге  $I$  у  $A$ .

⊗ Количнички скуп је  $A/I = \{a+I | a \in A\}$ . На  $A/I$  дефиниране увесишне операције  $+$  и  $\cdot$  са:

$$(a+I) + (b+I) := (a+b)+I ; \quad (a+I) \cdot (b+I) := (ab)+I .$$

Ове операције су добро дефинисане, јер ако је  $a+I = a'+I$  и  $b+I = b'+I$ , па је  $a \equiv a' \pmod{I}$  и  $b \equiv b' \pmod{I}$ , па је  $a+b \equiv a'+b' \pmod{I}$  и  $ab \equiv a'b' \pmod{I}$  и следи  $(a+b)+I = (a'+b')+I$  и  $(ab)+I = (a'b')+I$ .

ТВРЂЕЊЕ:  $(A/I, +, \cdot)$  је КПЈ. (доказ: венда; јединица:  $1+I$ )

⊕ (о изоморфизму): Нека је  $f: A \rightarrow B$  хомоморфизам кпј. Птага је  $\tilde{f}: A/\text{Ker}(f) \rightarrow \text{Im}(f)$ , задато са

изоморфизам + биномијум

$$\tilde{f}(a+\text{Ker}(f)) = f(a),$$
 изоморфизам кпј. Специјално,  $A/\text{Ker}(f) \cong \text{Im}(f)$ .

ДОКАЗ:  $\tilde{f}$  је добро дефинисано: Важи  $a+\text{Ker}(f) = b+\text{Ker}(f)$  ако  $a \equiv b \pmod{\text{Ker}(f)}$  ако  $a - b \in \text{Ker}(f)$

ако  $f(a - b) = 0$  ако  $f(a) - f(b) = 0$

ако  $f(a) = f(b)$  ако  $\tilde{f}(a+\text{Ker}(f)) = \tilde{f}(b+\text{Ker}(f))$ .

$\tilde{f}$  је „на“: по дефиницији  $\text{Im}(f)$

$\tilde{f}$  је хомоморфизам: Важи:  $\tilde{f}((a+\text{Ker}(f)) \cdot (b+\text{Ker}(f))) = \tilde{f}(ab+\text{Ker}(f)) = f(ab) - f(a) \cdot f(b)$

Покотје,  $\tilde{f}(1+\text{Ker}(f)) = f(1) = 1$ .

СТАВ  
(КТО)

ДОКАЗ:  
Класа са једном  $b \equiv a \pmod{m}$  има

КОМЕНТАР

⊕ (УТО)

ДОКАЗ

ПРИМЕР: За  $f_n: \mathbb{Z} \rightarrow \mathbb{Z}_n$ :  $\text{Ker } f_n = n\mathbb{Z}$ ,  $\text{Im } f_n = \mathbb{Z}_n$ , па је  $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ .

### ДИРЕКТАН ПРОИЗВОД ПРСТЕНА

ДЕФ. Нека су  $(A_1, +^1, \cdot^1), (A_2, +^2, \cdot^2), \dots, (A_n, +^n, \cdot^n)$  КПЈ. Тада је њихов ДИРЕКТАН ПРОИЗВОД КПЈ  $(A, +, \cdot)$ , где је  $A = A_1 \times A_2 \times \dots \times A_n$ , а операцije  $+$  и  $\cdot$  дефинишено са:

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 +^1 b_1, a_2 +^2 b_2, \dots, a_n +^n b_n)$$

⊗  $(A, +, \cdot)$  је КПЈ. (већије доказ за већију); НУЛЯ:  $(0, 0, \dots, 0)$ , ЈЕДИНИЦА:  $(1, 1, \dots, 1)$

Проверити дистрибутивнос. Нека су  $x, y, z \in A$ . Тада је  $x = (a_1, \dots, a_n), y = (b_1, \dots, b_n)$  и  $z = (c_1, \dots, c_n)$

$$\begin{aligned} \text{ДАВ: } & \text{Нека су } m_1, \dots, m_n \text{ упоредни уздајни прости природни бројеви. Тада вати:} \\ & \mathbb{Z}/(m_1, \dots, m_n)\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_n\mathbb{Z}. \\ \text{ДОКАЗ: } & \text{Кориснији теорем о изоморфизму за КПЈ. Постављамо пресликавање } f: \mathbb{Z} \rightarrow \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_n\mathbb{Z}, \\ & \text{задајући да } f(k) = (k+m_1\mathbb{Z}, \dots, k+m_n\mathbb{Z}). \text{ Тада је } f \text{ хомоморфизам. Зашто, } f(k+l) = (k+l+m_1\mathbb{Z}, \dots, k+l+m_n\mathbb{Z}) = \\ & = (k+m_1\mathbb{Z} + l+m_1\mathbb{Z}, \dots, k+m_n\mathbb{Z} + l+m_n\mathbb{Z}) = (k+m_1\mathbb{Z}, \dots, k+m_n\mathbb{Z}) + (l+m_1\mathbb{Z}, \dots, l+m_n\mathbb{Z}) = \\ & = f(k) + f(l). \text{ Слично за } \cdot. \text{ Дакле, } \text{Ker}(f) = \{k \in \mathbb{Z} \mid f(k) = 0\} = \{k \in \mathbb{Z} \mid (k+m_1\mathbb{Z}, \dots, k+m_n\mathbb{Z}) = (0+m_1\mathbb{Z}, \dots, 0+m_n\mathbb{Z})\} \\ & = \{k \in \mathbb{Z} \mid k \in m_1\mathbb{Z}, \dots, k \in m_n\mathbb{Z}\} = \{k \in \mathbb{Z} \mid m_1 | k, m_2 | k, \dots, m_n | k\} \\ & = (m_1, m_2, \dots, m_n) \mathbb{Z} \end{aligned}$$

Дакле,  $\mathbb{Z}/(m_1, \dots, m_n)\mathbb{Z} = \mathbb{Z}/\text{Ker}(f) \cong \text{Im}(f)$ . Као је  $\mathbb{Z}/(m_1, \dots, m_n)\mathbb{Z} \cong \mathbb{Z}_{m_1, \dots, m_n}$ , па је

$|\mathbb{Z}/(m_1, \dots, m_n)\mathbb{Z}| = m_1, \dots, m_n$ , па и  $|\text{Im}(f)| = m_1, \dots, m_n$ . Са друге стране,  $|\mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_n\mathbb{Z}| = m_1, \dots, m_n$ ,

даје  $f$  „НА“, тј.  $\text{Im}(f) = \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_n\mathbb{Z}$ .

КОМЕНТАР: Ово је у вези са  $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$  ако  $\text{НЗД}(m, n) = 1$  (за групе).

⊕ (кто) Нека су  $m_1, \dots, m_n \in \mathbb{N}$  уздајни прости природни бројеви упоредни и  $x_1, \dots, x_n \in \mathbb{Z}$ . Тада честоји чео број са шт.

$x \equiv x_i \pmod{m_i}, \dots, x \equiv x_n \pmod{m_n}$ . Ушто, ако и  $x' \in \mathbb{Z}$  задовољава ове конструенције, вати

$$x \equiv x' \pmod{m_1, \dots, m_n}.$$

ДОКАЗ: Приметишмо да је  $x \equiv x_i \pmod{m_i}$  еквивалентно са  $x + m_i\mathbb{Z} = x_i + m_i\mathbb{Z}$ , па је сисак конструенција

еквивалентан са  $f(x) = (x_1 + m_1\mathbb{Z}, \dots, x_n + m_n\mathbb{Z})$ , где је  $f$  из претходног сабака. Овакво  $x$

задовољава ове конструенције, вати  $f(x) = f(x')$ , тј.  $f(x - x') = 0$ .

$$f(x - x') = 0. \text{ Дакле, } x - x' \in \text{Ker } f = (m_1, \dots, m_n)\mathbb{Z}, \text{ тј. } x \equiv x' \pmod{m_1, \dots, m_n}.$$

П12

ТВРЂЕЊЕ:  $\Psi(m,n) = \Psi(m) \cdot \Psi(n)$  за  $\text{НЗД}(m,n)=1$ .

ТВРЂЕЊЕ: Нека су  $A, A', B, B'$  купј  $\text{тјг. } A \cong A'$  и  $B \cong B'$ . Тада је  $A \times B \cong A' \times B'$ .

СЛИЦА ДОКАЗА: Нека су  $f: A \rightarrow A'$  и  $g: B \rightarrow B'$  изоморфизми. Тада је  $F: A \times B \rightarrow A' \times B'$ , задашо  $(f(a), g(b))$  изоморфизам (за венчу - по координатама).

$F(a,b) = (f(a), g(b))$ , изоморфизам (за венчу - по координатама).

СТАВ: Ако су купј  $A$  и  $B$  изоморфни, тада су и претње  $U(A)$  и  $U(B)$  изоморфне.

ДОКАЗ: Нека је  $f: A \rightarrow B$  изоморфизам купј. Довољно је доказати да је  $g: U(A) \rightarrow U(B)$ , задашо  $g(x) := f(x)$ , изоморфизам.

1° је добро дефинисано: Довољно је проверити да за  $x \in U(A)$  вали  $f(x) \in U(B)$ . Ово следи из  $f(x^{-1}) = f(x)^{-1}$ , па је  $f(x) \in U(B)$ .

2° је хомоморфизам: Ово вали јер је  $g(x \cdot y) = f(x \cdot y) = f(x) \cdot f(y) = g(x) \cdot g(y)$ .

3° је бијекција: 3.1° је "1-1" јер је  $f$  "1-1"

3.2° је "НА": Нека је  $y \in U(B)$ . Како је  $f$  "НА", посматрајмо  $\exists x \in U(A)$  тај  $f(x) = y$ . Довољно је доказати да је  $x \in U(A)$ , јер је тада  $f(x) = g(x) = y$ . Постављамо  $y^{-1}$ . Тада посматрајмо  $\exists x' \in U(A)$  тај  $f(x') = y^{-1}$  и вали  $1 = yy^{-1} = f(x) \cdot f(x') = f(xx')$ , а шакође  $1 = f(1)$ , па је  $1 = xx'$ , тј.  $x' = x^{-1}$  (јер је  $f$  "1-1").

СТАВ: Нека су  $A_1, A_2, \dots, A_n$  купј. Тада вали:  $U(A_1 \times \dots \times A_n) = U(A_1) \times \dots \times U(A_n)$ .

ДОКАЗ: Вали:  $(a_1, a_2, \dots, a_n) \in U(A_1 \times \dots \times A_n)$  АККО посматрајмо  $(b_1, \dots, b_n) \in A_1 \times \dots \times A_n$  тај.

$(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = (1, 1, \dots, 1)$  АККО посматрајмо  $b_i \in A_i$  тај.  $a_i \cdot b_i = 1$  за  $1 \leq i \leq n$

АККО  $a_i \in U(A_i)$  за  $1 \leq i \leq n$  АККО  $(a_1, \dots, a_n) \in U(A_1) \times \dots \times U(A_n)$ .

⑤ Нека су  $m_1, m_2, \dots, m_n$  упоредиви узедамно прости природни бројеви. Тада вали:

$\mathbb{Z}_{m_1, \dots, m_n} \cong \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_n}$ , као и  $\Phi(m_1, \dots, m_n) \cong \Phi(m_1) \times \dots \times \Phi(m_n)$ .

Специјално,  $\Psi(m_1, \dots, m_n) = \Psi(m_1) \cdot \dots \cdot \Psi(m_n)$ .

ДОКАЗ: Користимо да је  $\mathbb{Z}/k\mathbb{Z} \cong \mathbb{Z}_k$ , за  $k \in \mathbb{N}$ . Јо С33Ч (процличас), вали:

$\mathbb{Z}/(m_1, \dots, m_n)\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_n\mathbb{Z}$ , па први изоморфизам следи из првог

шарта са овог часа. За други изоморфизам, користимо да је  $\Phi(k) = U(\mathbb{Z}_k)$  за  $k \in \mathbb{N}$ ,

што он следи из С33С, С33Ч и преходног изоморфизма. Коначно, последња једнакост

следи употребљавањем броја елемената.

## КОНАЧНЕ ПОДГРУПЕ МУЛТИПЛИКАТИВНЕ ГРУПЕ ПОЉА

- Нека је  $F$  поље. Тада је  $U(F) = F \setminus \{0\}$ .

**пример:**  $F = \mathbb{Z}_p$ :  $(U(\mathbb{Z}_p), \cdot_p) = (\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ ,  $p$  прост

- Нека је  $G$  коначна подгрупа мултипликативне групе  $(U(F), \cdot)$  поља  $F$ . Тада је  $G$  циклична група.

- Прво доказујемо следеће појноћно тврђење.

**тврђење:** Нека је  $F$  поље и  $f \in F[x] \setminus \{0\}$  симплена  $n$ . Тада  $f$  има највише  $n$  нула у  $F$ .

**доказ:** Индукцијом по  $n$ .

**БАЗА:**  $n=1$ : Тада је  $f=ax+b$ , па је његова јединица нула  $x = -ba^{-1}$ .

**ИК:** Нека је  $f$  симплена  $n$  и нека је  $\lambda \in F$  нула од  $f$ . По лези о количнику и остатку, постоји  $q \in F[x]$  и  $c \in F$ :  $f = (x-\lambda)q + c$ . Зашемо  $\lambda$  добијамо:

$0 = f(\lambda) = (\lambda-\lambda)q(\lambda) + c$ , па је  $c=0$  тј.  $f = (x-\lambda)q$ . Следи да је  $q$  симплена  $n-1$ ,

па по  $u$  има највише  $n-1$  нула. Причешћимо да ако је  $\beta \neq \lambda$  нула од  $f$ , тада вати:

$0 = f(\beta) = (\beta-\lambda)q(\beta)$ , па је  $\beta$  нула од  $q$ . Одавде следи тврђење.

**доказ теореме:** Како је  $G$  коначна и Абелова, можемо применити (I) о нормалној форми. Закле,

$G \cong \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_k}$  за неке  $d_1 | d_2, d_2 | d_3, \dots, d_{k-1} | d_k$ ,  $d_1 \geq 2$ . Из овога следи да за свако  $a \in G$  вати  $a^{d_k} = 1$ . Специјално, сваки елемент групе  $G$  је нула полинома  $x^{d_k} - 1$ , па по претходном тврђењу следи  $d_k \geq |G| = d_1 \cdot d_2 \cdots \cdot d_k$ . Следи  $k=1$ , тј.

$G \cong \mathbb{Z}_{d_1}$ .

**пример:**  $F = \mathbb{Z}_p$ ,  $p$  прост и  $G = U(\mathbb{Z}_p) = \mathbb{Z}_p \setminus \{0\} = \{1, 2, \dots, p-1\}$ . Наравно,  $(G, \cdot_p)$  је група и по претходном, она је циклична тј. постоји  $g \in \mathbb{Z}_p \setminus \{0\}$  тај.  $\mathbb{Z}_p \setminus \{0\} = \langle g \rangle = \{1, g, g^2, \dots, g^{p-2}\}$ . Специјално, нека је  $p=7$ . За  $g=2$ :  $\begin{matrix} 1, & 2, & 2^2, & 2^3 \\ 1, & 2, & 4, & 1 \end{matrix}$   $\omega(2)=3 \neq p-1$ , па 2 није примитивни корен.

За  $g=3$ :  $\begin{matrix} 1, & 3, & 3^2, & 3^3, & 3^4, & 3^5 \\ 1, & 3, & 2, & 6, & 4, & 5 \end{matrix}$ , па је 3 примитиван корен по модулу 7.

**тврђење:** Нека је  $g$  примитивни корен по модулу  $p$ . Тада за  $a, b \in \mathbb{Z}_p \setminus \{0\}$  постоје  $u, v \in \{0, 1, \dots, p-2\}$

т.д.  $a = g^u$ ,  $b = g^v$  и следи  $a \cdot_p b = g^u \cdot_p g^v = g^{u+p-1}v$ .

## РАШИРЕЊА ПОЉА

$$\begin{aligned} \bullet & x^2 = 2 & \pm \sqrt{2} \\ \bullet & x^2 = -1 & \pm i \end{aligned}$$

у  $F[x]$

$\nabla$

Задатак. За полином  $f \in F[x] \setminus \{0\}$ , где је  $F$  поље, казнено да је НЕРАСТАВЉАВЉУЩЕ Ако не постоји неконстантни полиноми  $g, h \in F[x]$  тај.  $f = gh$ .

пример:  $x^2 - 2$  нерасстављив у  $\mathbb{Q}[x]$   
расстављив у  $\mathbb{R}[x]$   $(x - \sqrt{2})(x + \sqrt{2})$

2. део.

пример:

(+) (Кронекерова конструкуција): Нека је  $F$  поље и  $f \in F[x] \setminus \{0\}$  нерасстављив полином. Тада вали:

1  $E := F[x] \setminus \langle f \rangle$  је поље.

2 Поље  $E$  садржи пошто поље изоморфно пољу  $F$  (другим речима,  $E$  је РАШИРЕЊЕ поља  $F$ ).

3 Полином  $f$  има нулу у  $E$ .

4  $[E : F] = \deg f$  (Битије дефинисано кофицијент)

доказ: 1  $E$  је кпј, па је довољно доказати да сваки ненула елеменат из  $E$  има инверз.

Нека је  $g + \langle f \rangle \neq 0 + \langle f \rangle$  (тада је  $g \in F[x]$ ). Тада  $g \notin \langle f \rangle$ , тј.  $f \nmid g$ . Како у  $F[x]$  валичи лема о количнику и осташку, што за свака два пољинома пошто конструисати Еуклидов алгоритам који доје НЗД, тих пољинома. Како НЗД  $(f, g) = c \in F$ . Отивши, из Еуклидовог алгоритма, следи да постоје  $u, v \in F[x]$  тај.  $fu + gv = \text{НЗД}(f, g) = c$ , па је  $fc^{-1}u + gc^{-1}v = 1$ . Следи:

$$(g + \langle f \rangle)(c^{-1}u + \langle f \rangle) = gc^{-1}u + \langle f \rangle = 1 + \langle f \rangle, \text{ јер је } 1 - gc^{-1}u = fc^{-1}u \in \langle f \rangle.$$

Закле,  $g + \langle f \rangle$  је инвертибилан.

2 Нека је  $F' = \{c + \langle f \rangle \mid c \in F\}$ . Тада је  $\Upsilon: F \rightarrow F'$ , задато са  $\Upsilon(c) = c + \langle f \rangle$ , изоморфизам (за венчу).

3 Нека је  $f = a_n x^n + \dots + a_1 x + a_0$ . Означимо  $\tilde{x} = x + \langle f \rangle \in E$  и докажимо да је  $\tilde{x}$  нула пољинома  $f$ . Записа,  $f(\tilde{x}) = a_n \tilde{x}^n + \dots + a_1 \tilde{x} + a_0 (1 + \langle f \rangle) =$   
 $= a_n (x + \langle f \rangle)^n + \dots + a_1 (x + \langle f \rangle) + a_0 + \langle f \rangle$   
 $= a_n x^n + \langle f \rangle + \dots + a_1 x + \langle f \rangle + a_0 + \langle f \rangle$   
 $= f + \langle f \rangle = 0 + \langle f \rangle$  (по дефиницији идеала)  $a + I = b + I \text{ ако } a - b \in I$

4 НА СЛЕДЕЋЕМ ЧАСУ

пример:  $F = \mathbb{R}$ ,  $f = x^2 + 1$

$$E = \mathbb{R}[x] / \langle x^2 + 1 \rangle \cong \mathbb{C}$$

$$g \in \mathbb{R}[x]: g = (x^2 + 1)q + ax + b$$

$$g + \langle x^2 + 1 \rangle = ax + b + \langle x^2 + 1 \rangle$$

$$a, b \in \mathbb{R}$$

$$ax+b + \langle x^2+1 \rangle = a \cdot \underbrace{(x+\langle x^2+1 \rangle)}_t + b \cdot \underbrace{(1+\langle x^2+1 \rangle)}_1$$

$$\begin{aligned} t^2 &= (x+\langle x^2+1 \rangle)^2 \\ &= x^2 + \langle x^2+1 \rangle \\ &= -1 + \langle x^2+1 \rangle \end{aligned}$$

/\*  $\sqrt{2}$  конструирано са  $\mathbb{Q}[x]/\langle x^2-2 \rangle$ ,  $x+\langle x^2-2 \rangle \neq 0$

**Def.** Нека је  $E$  расширење поља  $F$ . Тада  $E$  јачено посматраши као векторски простор над  $F$ . Ако је  $E$  коначне димензије над  $F$ , тада са  $[E:F]$  означавамо димензију од  $E$  над  $F$  и јачено да је она СТЕПЕН РАШИРЕЊА  $E$  над  $F$ .

ПРИМЕР:  $[\mathbb{C}:\mathbb{R}] = 2$

$[1, i]$  је база за  $\mathbb{C}$  над  $\mathbb{R}$ .  $x \cdot 1 + y \cdot i$ ,  $x, y \in \mathbb{R}$

ДОКАЗ I):  $[E:F] = \deg f$  - степен расширења

Довољно је доказати да је  $[1+\langle f \rangle, x+\langle f \rangle, \dots, x^{n-1}+\langle f \rangle]$  база за  $E$  над  $F$  (тј.  $n = \deg f$ ).

1° В је генераториса

$E = F[x]/\langle f \rangle$ . Изаберико  $g+\langle f \rangle \in E$ . Довољно је доказати да  $\exists c_0, c_1, \dots, c_{n-1} \in F$  такви да је  $g+\langle f \rangle = c_0(1+\langle f \rangle) + c_1(x+\langle f \rangle) + \dots + c_{n-1}(x^{n-1}+\langle f \rangle)$ .

НАПОМЕНА: у  $c_i(x^i+\langle f \rangle)$ , под  $c_i$  подразумевају се  $c_i+\langle f \rangle$ .

По леми о количнику и остатку, постоји  $q, r \in F[x]$  такви да је  $g = fq+r$ ,  $\deg r < \deg f$ .

Тада је  $g-r = fq \in \langle f \rangle$ , па је  $g+\langle f \rangle = r+\langle f \rangle$ . Када је  $\deg r < n$ , па постоји  $c_0, c_1, \dots, c_{n-1} \in F$  такви да је  $r = c_0 + c_1 x + \dots + c_{n-1} x^{n-1}$ , па вакви (\*).

2° В је линеарно независан

Довољно је доказати да из  $c_0(1+\langle f \rangle) + c_1(x+\langle f \rangle) + \dots + c_{n-1}(x^{n-1}+\langle f \rangle) = 0+\langle f \rangle$  следи

$c_0 = c_1 = \dots = c_{n-1} = 0$ . Засиша, из  $c_0(1+\langle f \rangle) + c_1(x+\langle f \rangle) + \dots + c_{n-1}(x^{n-1}+\langle f \rangle) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1} + \langle f \rangle = 0+\langle f \rangle$  следи

$c_0 + c_1 x + \dots + c_{n-1} x^{n-1} \in \langle f \rangle$ , тј.  $f | c_0 + c_1 x + \dots + c_{n-1} x^{n-1}$ . Четврти, полином са десне стране

је степена мањег од  $n$ , па је он нула полином, тј.  $c_0 = c_1 = \dots = c_{n-1} = 0$ .

ПРИМЕР: Конструисаши поље од 8 елемената.

(Сва коначна поља издују  $p^n$  елемената, где је  $p$  прост.)

РЕШЕЊЕ: Ово поље шрафити у облику  $F[x]/\langle f \rangle$ , где је  $f$  нераспаљив полином. Зашто бирајмо  $F = \mathbb{Z}_2$  (у општем случају  $\mathbb{Z}_p$ ), а за  $f$  неки нераспаљив полином степена 3 (у општем случају  $n$ ). Полином степена 3 је нераспаљив у  $\mathbb{Z}_2[x]$  ако нема нула у  $\mathbb{Z}_2$ . Закле, за  $f$  јачено узети  $x^3+x+1$ , тј.  $\mathbb{Z}_2[x]/\langle x^3+x+1 \rangle$  је поље са 8 елемената.

$f = x^3+x+1$ , тј.  $\mathbb{Z}_2[x]/\langle x^3+x+1 \rangle$  је поље са 8 елемената.

? Како рачунамо у оваком пољу?

Сваки елемент је облика  $ax^2+bx+c+\langle x^3+x+1 \rangle$ , где су  $a, b, c \in \mathbb{Z}_2$ . Сабирање је лако и врши се по координатама.

$$ax^2+bx+c + \langle x^3+x+1 \rangle + a'x^3+b'x^2+c'x+\langle x^3+x+1 \rangle = (a+a')x^2+(b+b')x+(c+c')+\langle x^3+x+1 \rangle$$

Множење је компликованије. Ватни:  $x^3+x+1 + \langle x^3+x+1 \rangle = 0 + \langle x^3+x+1 \rangle$ , па је  $\overline{x}^3+\langle x^3+x+1 \rangle = 1M+\langle x^3+x+1 \rangle$

$$\text{и следи } \overline{x}^3+\langle x^3+x+1 \rangle = x^3+x+\langle x^3+x+1 \rangle. \text{ Сада је:}$$

$$(ax^2+bx+c+\langle x^3+x+1 \rangle)(ax^2+b'x+c'+\langle x^3+x+1 \rangle) =$$

$$= aa'x^4+(ba'+b'a)x^3+(ac+c'a+bc')x^2+(bc+c'b+cc')x+cc'+bd+ba+ca'x^1+$$

$$- (ac+c'a+bb'+aa')x^3 + (bc+c'b+cc'+ba+b'a)x^2 + cc'+bd+ba+ca'x^1$$

**ПОСЛЕДИЦА:** Нека је  $F$  поље и  $f \in F[x]$ . Тада постоећи расширење  $E$  поља  $F$  у коме се  $f$  факторише на линеарне факторе (тј. што сме нуле).

**Зеф.** Нека је  $f \in F[x] \setminus \{0\}$ , где је  $F$  поље. Коренско поље полинома  $f$  је најмање расширење поља  $F$  у коме  $f$  има линеарну факторизацију.

(П13)

### АЛГЕБАРСКИ ЕЛЕМЕНТИ

- Нека је  $F$  поштовање поља  $C$ . За  $\lambda \in C$  дефинишењем  $F[\lambda] = \{c_0 + c_1\lambda + \dots + c_n\lambda^n \mid n \in \mathbb{N}, c_i \in F\}$ . Тада  $F[\lambda]$  садржи  $F \cup \{\lambda\}$  и  $(F[\lambda], +, \cdot)$  је кпј. Уз то,  $F[\lambda]$  је најмањи кпј који садржи  $F \cup \{\lambda\}$ .
- Нека је  $F(\lambda)$  најмање поље које садржи  $F \cup \{\lambda\}$ . Јасно,  $F[\lambda] \subseteq F(\lambda)$ .

**Зеф.** Нека је  $F$  поље од  $C$  и  $\lambda \in C$ . Тада је  $\lambda \in$  алгебарски над  $F$  ако постоећи  $f \in F[x] \setminus \{0\}$  такође је  $f(\lambda) = 0$ .

**ПРИМЕР:**  $\sqrt{2}$  је алгебарски над  $\mathbb{Q}$ , док  $\pi$  није алгебарски над  $\mathbb{Q}$ . Обајесу алгебарска над  $\mathbb{R}$ . За  $\lambda = \sqrt{2} \rightarrow x^2 - 2$ .

**Зеф.** За минималан полином који је минималне степене да задовољава горњу дефиницију кажемо да је МИНИМАЛНИ ПОЛИНОМ ЗА  $\lambda$  НАД  $F$ , у означу  $M_\lambda$ . (минималн = водећи кофицијент је 1)

- ОСОБИНЕ:**
- 1  $M_\lambda$  је јединствен.
  - 2  $M_\lambda$  је нерасчланиљив у  $F[x]$ .
  - 3  $r_{M_\lambda} = 0$  ако  $M_\lambda$  је  $(\text{за } p \in F[x])$

**ДОКАЗ:** 1 Нека је  $M_\lambda$  минимални полином. Тада је  $M_\lambda(\lambda) = 0$ ,  $M'_\lambda(\lambda) = 0$  и  $\deg M_\lambda = \deg M'_\lambda$ .

Полином  $M_\lambda - M'_\lambda$  је минималне степене од  $M_\lambda$  и  $M'_\lambda$  и ватни  $(M_\lambda - M'_\lambda)(\lambda) = 0$ , па након бити  $M_\lambda - M'_\lambda = 0$ , па је  $M_\lambda = M'_\lambda$ .

2 ППС.  $M_\lambda = f \cdot g$ , где су  $f, g \in F[x]$  степена барем 1. Тада је  $0 = M_\lambda(\lambda) = f(\lambda)g(\lambda)$ , па је  $f(\lambda) = 0$  или  $g(\lambda) = 0$ , што није могуће јер је  $\deg f, \deg g < \deg M_\lambda$ .

3 Полеми о количнику и осташку, постоји  $q, r \in F[x]$  такви да је  $p = q \cdot M_\lambda + r$ ,  $\deg r < \deg M_\lambda$ .  
Па је  $p(\lambda) = q(\lambda)M_\lambda(\lambda) + r(\lambda)$ , тј.  $p(\lambda) = r(\lambda)$ . Закле,  $p(\lambda) = 0$  ако  $r(\lambda) = 0$  (јер је  $\deg r < \deg M_\lambda$ )  
ако  $r = 0$   
ако  $M_\lambda \mid p$ .

**СТАВ:** Нека је  $F$  поље њега  $C$  и  $\lambda \in C$ . Тада је  $F[\lambda] = F(\lambda)$  ако је  $\lambda$  алгебарски над  $F$ .

- доказ:**  $\rightarrow$ : Из  $F[\alpha] = F(\alpha)$  следи да је  $F[\alpha]$  поле. Сакаш што, извеља се да  $(\frac{1}{\alpha} - \alpha)$  се налази у  $F[\alpha]$ , па је  $\frac{1}{\alpha} - \alpha \in F[\alpha]$  за неко  $p \in F[\alpha]$ . Следи  $\alpha p(\alpha) - 1 = 0$ , па је  $p(\alpha) = 0$  па  $f(\alpha) = 0$  па  $f = \alpha \cdot p - 1$ , што је  $\alpha$  алгебарски над  $F$ .
- $\leftarrow$ : Довољно је доказати да је  $F[\alpha]$  поле. Користимо  $\Phi$  о изоморфизму за ктј. Постављамо пресликавање  $\Phi: F[x] \rightarrow F[\alpha]$  задато са  $\Phi(p) = p(\alpha)$ . Ово пресликавање (што је евидентно) је хомоморфизам ктј ( $\Phi(pq) = (pq)(\alpha) = p(\alpha)q(\alpha) = \Phi(p) \cdot \Phi(q)$ ). Следи:  $F[x]/\text{Ker } \Phi \cong \text{Im } \Phi$ . Јасно,  $\text{Im } \Phi = F[\alpha]$  (јер је  $\Phi$  "на"), па је довољно доказати да је  $F[\alpha]/\text{Ker } \Phi$  поле. Као што је  $\text{Ker } \Phi \subset F[x]$ , па је  $\text{Ker } \Phi$  главни, што  $\text{Ker } \Phi = \langle f \rangle$ , и то што желимо изабрали да је финитан. У  $\text{Ker } \Phi$  се налазе сви рационални  $p(\alpha) = 0$ , па како  $f \mid p$ , па је  $f$  најниже степена, шако да је  $f(\alpha) = 0$  (а  $f \neq 0$ ), па је  $f = \mu_\alpha$ . Као што је  $\mu_\alpha$  нераспаљиво, то је по Кронекеровој конструкцији  $F[x]/\langle \mu_\alpha \rangle = F[\alpha]$  поле.
- Када је  $\alpha$  алгебарски над  $F$ , вати:  $F[x]/\langle \mu_\alpha \rangle \cong F(\alpha) = F[\alpha]$  и следи  $[F(\alpha):F] = \deg \mu_\alpha$ .

**пример:**  $F = \mathbb{Q}$ ,  $\alpha = \sqrt{2}$

$$\mu_{\sqrt{2}} = x^2 - 2, \quad \mathbb{Q}[x]/\langle x^2 - 2 \rangle \cong \mathbb{Q}(\sqrt{2})$$

желано поле које садржи  $\mathbb{Q} \cup \{\sqrt{2}\}$

**пример:**  $\alpha = \sqrt{2} + \sqrt{3}$ . Одредиш  $\alpha$  у облику  $p(\alpha)$  за неки полином  $p(x) \in \mathbb{Q}[x]$ .

$$\frac{1}{\alpha} = p(\alpha) \Leftrightarrow \alpha p(\alpha) - 1 = 0$$

Знамо  $\mu_\alpha(d) = 0$ , па ако је с слободан члан у  $\mu_\alpha$ , вати:

$$\mu_\alpha = x^2 - 2x - 1. \quad \text{Следи } \alpha p(\alpha) + c = 0, \text{ па је } \frac{1}{\alpha} = \frac{-c}{p(\alpha)}.$$

**Зад.** Нека су  $E$  и  $F$  пошто да је  $E$  шаква да је Е рачирење пола  $F$ . Тада је  $E$  конично расширење од  $F$  ако  $E$  је конечно димензионални простор над  $F$ .

**(t) (о првијашњем елементу):** Свако конично расширење  $E$  пола  $\mathbb{Q}$  је облика  $E = \mathbb{Q}(\alpha)$  за неко  $\alpha \in E$ . Елемент  $\alpha$  је примитивни елемент расширења  $E$ .