Алгебра 1

Јован Самарџић, 13/2019

Професор: Марко Радовановић

- дефиниције
- ознаке
- теореме
- докази
- примери

Година курса: 2020/21

Молим да ми све грешке пријавите преко мејла или друштвених мрежа.

1. Алгебарске структуре.

деф. Нека је A скуп. Затворена операција је функција $\omega: A^n \to A$, $n \in N$
Дужина (тип) операције је број n. Специјално, за $n=2 \to$ бинарна.
$n=1 \to$ унарна.
$n=0 \to$ константа.

деф. Алгебарска структура је уређена $(k+1)$-торка $\mathbb{A} = (A, \omega_1, \dots, \omega_k)$, где је скуп A носач, док су $\omega_1, \dots, \omega_k$ операције на A.

Ако су $n_1, \dots, n_k$ типови операција, онда је $(n_1, \dots, n_k)$ тип алгебарске структуре.

деф. Нека су $\sigma: S^k \to S$ и $\omega: A^k \to A$ истог типа и нека је $S \subseteq A$.
Тада је σ подоперација од ω ако важи:

$$\sigma(s_1, \dots, s_k) = \omega(s_1, \dots, s_k) \quad , \quad s_1, \dots, s_k \in S.$$

деф. Нека су $\mathbb{S} = (S, \sigma_1, \dots, \sigma_k)$ и $\mathbb{A} = (A, \omega_1, \dots, \omega_k)$ алгебарске структуре.
$\mathbb{S}$ је алгебарска подструктура од $\mathbb{A}$ ако је σ_1 подоперација од ω_1;
⋮
σ_k подоперација од ω_k.

деф. Нека је ω_A оп. на A, ω_B оп. на B и нека су обе типа n.
Пресликавање $f: A \to B$ је сагласно са паром (ω_A, ω_B) ако:

$$(\forall a_1, \dots, a_n \in A) \quad f(\omega_A(a_1, \dots, a_n)) = \omega_B(f(a_1), \dots, f(a_n)).$$

T1: Нека су $\omega_A, \omega_B, \omega_C$ операције на A, B, C редом.

1) Ако је $f: A \to B$ сагласна са (ω_A, ω_B) и $g: B \to C$ сагласна са (ω_B, ω_C) онда је $g \circ f: A \to C$ сагласна са (ω_A, ω_C)

2) Специјално, ако је f бијекција, $f^{-1}: B \to A$ је сагласна са (ω_B, ω_A)

Д: $\omega_A, \omega_B, \omega_C$ – типа n. $a_1, \dots, a_n \in A$ и $b_1 = f(a_1), \dots, b_n = f(a_n)$

1) $(g \circ f)(\omega_A(a_1, \dots, a_n)) = g(f(\omega_A(a_1, \dots, a_n))) = g(\omega_B(f(a_1), \dots, f(a_n))) =$
$= \omega_C((g \circ f)(a_1), \dots, (g \circ f)(a_n))$

2) $f^{-1}(\omega_B(b_1, \dots, b_n)) \overset{\text{буј.}}{=} f^{-1}(\omega_B(f(a_1), \dots, f(a_n))) = f^{-1}(f(\omega_A(a_1, \dots, a_n))) =$
$= \omega_A(f^{-1}(b_1), \dots, f^{-1}(b_n))$

деф. Нека су $\mathbb{A} = (A, \omega_1, \dots, \omega_k)$ и $\mathbb{B} = (B, \sigma_1, \dots, \sigma_k)$ алгебарске структуре истог типа.
Пресликавање $f: A \to B$ је **хомоморфизам алгебарских структура** $\mathbb{A}$ и $\mathbb{B}$ ако је f сагласно са $(\omega_1, \sigma_1), \dots, (\omega_k, \sigma_k)$.

Специјално, ако је f
1-1 : **мономорфизам** алгебарских структура.
на : **епиморфизам** алгебарских структура.
бијекција : **изоморфизам** алгебарских структура.

деф. Ако постоји изоморфизам алг. стр. $\mathbb{A}$ и $\mathbb{B}$, те групе су **изоморфне**.
Пишемо $A \cong B$

T2: $\cong$ је релација еквиваленције

Д: (Р) $id_A : A \to A$ је изоморфизам.

(С) По Т1. $f^{-1}: B \to A$ је изоморфизам.

(Т) По Т1. $g \circ f : A \to C$ је изоморфизам.

деф. Нека је $\mathbb{A} = (A, \omega_1, \dots, \omega_k)$ алг. стр., n_i тип операције ω_i и $\sim$ рел. екв. на A
Тада је $\sim$ **конгруенција** на A ако

$$\forall 1 \leq i \leq k \qquad a_1 \sim b_1, \dots, a_{n_i} \sim b_{n_i} \Rightarrow \omega_i(a_1, \dots, a_{n_i}) \sim \omega_i(b_1, \dots, b_{n_i})$$

деф. Нека је $\mathbb{A} = (A, \omega_1, \dots, \omega_k)$ алг. стр. и $\sim$ конгруенција на A
На количничком скупу $A/\sim$ дефинишемо операције $\tilde{\omega}_1, \tilde{\omega}_2, \dots, \tilde{\omega}_k$ са:

$$\tilde{\omega}_i(C_{a_1}, \dots, C_{a_{n_i}}) = C_{\omega_i(a_1, \dots, a_{n_i})}$$

Напомена: Операције $\tilde{\omega}_i$ су добро дефинисане

Д: $C_{a_1} = C_{b_1}, \dots, C_{a_{n_i}} = C_{b_{n_i}} \Rightarrow a_1 \sim b_1, \dots, a_{n_i} \sim b_{n_i}$
$\Rightarrow \omega_i(a_1, \dots, a_{n_i}) \sim \omega_i(b_1, \dots, b_{n_i})$
$\Rightarrow C_{\omega_i(a_1, \dots, a_{n_i})} = C_{\omega_i(b_1, \dots, b_{n_i})}$

деф. Нека је $\mathbb{A}$ алг. стр. и $\sim$ конгруенција на A.
Природна пројекција је $\pi : A \to A/\sim$, $\pi(a) = C_a$

Напомена: π је епиморфизам

Д: * $\pi(\omega_i(a_1, \dots, a_{n_i})) = C_{\omega_i(a_1, \dots, a_{n_i})} = \tilde{\omega}_i(C_{a_1}, \dots, C_{a_{n_i}}) = \tilde{\omega}_i(\pi(a_1), \dots, \pi(a_{n_i}))$

* Очигледно јесте на (класи C_a припада барем a)

деф. Нека је $f: A \to B$ хомоморфизам алг. стр. $\mathbb{A}$ и $\mathbb{B}$. $\mathrm{Im} f = \{ f(a) \mid a \in A \}$

Ако је $\mathbb{B} = (B, \sigma_1, \dots, \sigma_k)$, на $\mathrm{Im} f$ дефинишемо операције $\tau_i(b_1, \dots, b_{n_i}) = \sigma_i(b_1, \dots, b_{n_i})$

Напомена: $(\mathrm{Im} f, \tau_1, \dots, \tau_k)$ је алг. подструктура од $\mathbb{B}$

Д: $\tau_i(b_1, \dots, b_{n_i}) \overset{\text{на}}{=} \tau_i(f(a_1), \dots, f(a_{n_i})) \overset{\text{деф.}}{=} \sigma_i(f(a_1), \dots, f(a_{n_i})) \overset{\text{хом.}}{=} f(\omega_i(a_1, \dots, a_{n_i})) \in \mathrm{Im} f$

Дакле τ_i је подоперација од σ_i, за свако i

Факторизација хомоморфизма: Нека је $f: A \to B$ хомоморфизам алг. стр. $\mathbb{A}$ и $\mathbb{B}$

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi"'] & B \\ A/\sim \arrow[r, "\phi"] & \mathrm{Im} f \arrow[u] \end{tikzcd}$$

1) Тада је релација $a \sim a' \Leftrightarrow f(a) = f(a')$ конгруенција на A

2) $\phi : A/\sim \to \mathrm{Im} f$, $\phi(C_a) = f(a)$ је изоморфизам

3) $f = i \circ \phi \circ \pi$, где је $i : \mathrm{Im} f \to B$, $i(b) = b$

Д: 1) Тривијално је да је $\sim$ рел. екв.

Нека је $\mathbb{A} = (A, \omega_1, \dots, \omega_k)$, $\mathbb{B} = (B, \sigma_1, \dots, \sigma_k)$, при чему је f сагласно са (ω_i, σ_i)

$$\begin{aligned} a_1 \sim a_1', \dots, a_{n_i} \sim a_{n_i}' &\Rightarrow f(a_1) = f(a_1'), \dots, f(a_{n_i}) = f(a_{n_i}') \\ &\Rightarrow \sigma_i(f(a_1), \dots, f(a_{n_i})) = \sigma_i(f(a_1'), \dots, f(a_{n_i}')) \\ &\Rightarrow f(\omega_i(a_1, \dots, a_{n_i})) = f(\omega_i(a_1', \dots, a_{n_i}')) \\ &\Rightarrow \omega_i(a_1, \dots, a_{n_i}) \sim \omega_i(a_1', \dots, a_{n_i}') \end{aligned}$$

2) * $\phi(\tilde{\omega}_i(C_{a_1}, \dots, C_{a_{n_i}})) = \phi(C_{\omega_i(a_1, \dots, a_{n_i})}) = f(\omega_i(a_1, \dots, a_{n_i})) = \sigma_i(\overset{\in \mathrm{Im} f}{f(a_1)}, \dots, \overset{\in \mathrm{Im} f}{f(a_{n_i})})$

$= \tau_i(f(a_1), \dots, f(a_{n_i})) = \tau_i(\phi(C_{a_1}), \dots, \phi(C_{a_{n_i}}))$

$\Rightarrow \phi$ је хомоморфизам (за свако i)

* ϕ је на: тривијално
* ϕ је 1-1: $\phi(C_a) = \phi(C_{a'}) \Leftrightarrow f(a) = f(a') \Leftrightarrow a \sim a' \Leftrightarrow C_a = C_{a'}$

(други смер даје добру деф. ϕ)

Дакле, ϕ је хомоморфизам и бијекција, па је и изоморфизам.

3) Домени и кодомени обе стране се слажу

$(i \circ \phi \circ \pi)(a) = (i \circ \phi)(C_a) = i(f(a)) = f(a)$

2. Полугрупе и моноиди.

деф. Бинарна операција $*$ на A је **асоцијативна** акко $(\forall a_1, a_2, a_3 \in A)\ a_1 * (a_2 * a_3) = (a_1 * a_2) * a_3$

деф. Алгебарска структура $(S, *)$ је **полугрупа** акко је $*$ асоцијативна.

деф. Нека су $m, n \in N$ $(m \geq n)$, $a_n, \dots, a_m \in S$ и $*$ бинарна операција на скупу S.
Дефинишемо **производ**, у ознаци $\prod$, као:

$$1^\circ \ \prod_{i=n}^{n} a_i = a_n \quad , \quad 2^\circ \ \prod_{i=n}^{m} a_i = \prod_{i=n}^{m-1} a_i * a_m$$

деф. Специјално, $a^n = \prod_{i=1}^{n} a$, $a \in S$, $n \in N$.

Т1: Ако је $(S, *)$ полугрупа, тада: $\prod_{i=1}^{n} a_i * \prod_{i=n+1}^{m+n} a_i = \prod_{i=1}^{m+n} a_i$

Д: (БИ) $m = 1$: $\prod_{i=1}^{n} a_i * \prod_{i=n+1}^{n+1} a_i = \prod_{i=1}^{n} a_i * a_{n+1} = \prod_{i=1}^{n+1} a_i$

(ИК) $m \Rightarrow m+1$: $\prod_{i=1}^{n} a_i * \prod_{i=n+1}^{m+1+n} \overset{деф.}{=} \prod_{i=1}^{n} a_i * \left(\prod_{i=n+1}^{m+n} a_i * a_{m+n+1}\right) \overset{асоц.}{=} \left(\prod_{i=1}^{n} a_i * \prod_{i=n+1}^{m+n} a_i\right) * a_{m+n+1} =$

$$\overset{(ИХ)}{=} \prod_{i=1}^{m+n} a_i * a_{m+n+1} = \prod_{i=1}^{m+n+1} a_i$$

Закључак: У полугрупи, заграде у изразу $a_1 * \dots * a_n$ постављамо произвољно

деф. Бинарна операција $*$ на A је **комутативна** акко $(\forall a_1, a_2 \in A)\ a_1 * a_2 = a_2 * a_1$

Т2: Нека је $(S, *)$ полугрупа, $*$ је комутативна и $a_1, \dots, a_n \in S$.
Тада за сваку пермутацију $(\pi_1, \dots, \pi_n)$ скупа $\{1, 2, \dots, n\}$ важи:

$$a_{\pi_1} * \dots * a_{\pi_n} = a_1 * \dots * a_n$$

Д: (БИ) $n = 1$: тривијално

(ИК) $n \Rightarrow n+1$: $(\pi_1, \dots, \pi_{n+1})$ - пермутација, где $\pi_{n+1} = k \in \{1, 2, \dots, n\}$

$$a_{\pi_1} * \dots * a_{\pi_n} * a_{\pi_{n+1}} = a_{\pi_1} * \dots * a_{\pi_n} * a_k$$

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

$$= a_1 * \dots * a_{k-1} * \underbrace{a_k} * \underbrace{a_{k+1} * \dots * a_n}$$

деф. Нека је $*$ бинарна оп. на A
Елемент $a \in A$ је регуларан слева акко $(\forall x,y \in A)$ $a*x = a*y \Rightarrow x=y$
регуларан здесна акко $(\forall x,y \in A)$ $x*a = y*a \Rightarrow x=y$

Т3: Нека је $(S,*)$ полугрупа. Ако су $a,b \in S$ рег. слева, онда је и $a*b$ рег. слева.

Аналогно важи и ако су a,b рег. здесна.

Д: $(a*b)*x = (a*b)*y \Rightarrow a*(b*x) = a*(b*y) \Rightarrow b*x = b*y \Rightarrow x=y$

деф. Алгебарска структура $(M,*,e)$ типа $(2,0)$ је моноид акко:

1° $(M,*)$ је полугрупа,
2° $(\forall a \in M)$ $a*e = e*a = a$. Елемент e (константу) називамо неутрал.

Напомена: У моноиду $(M,*,e)$ неутрал је јединствен.

Д: $\left.\begin{array}{l} e*e' = e \\ e*e' = e' \end{array}\right\} \Rightarrow e=e'$

деф. Нека је $(M,*,e)$ моноид. Елемент $a \in M$ је инвертибилан слева акко $(\exists x \in M)$ $x*a=e$
$c \in M$ инвертибилан здесна акко $(\exists y \in M)$ $a*y=e$

Тада је x леви инверз, док је y десни инверз.

Т4: Нека је $(M,*,e)$ моноид. Ако је $a \in M$ инв. слева, онда је и рег. слева.
инв. здесна, онда је и рег. здесна.

Д: a – инв. слева $(b*a=e)$, c – инв. здесна $(c*d=e)$

$a*x = a*y \Rightarrow b*a*x = b*a*y \Rightarrow e*x = e*y \Rightarrow x=y$
$x*c = y*c \Rightarrow x*c*d = y*c*d \Rightarrow x*e = y*e \Rightarrow x=y$

Напомена: Обрнуто не важи (нпр. у $(\mathbb{N},\cdot,1)$, елемент 2 нема инверз)

T5: Ако је x леви инверз, y десни инверз од $a \in M$, онда је $x = y$

Д:
$$\left.\begin{aligned} x * a * y &= x * e = x \\ x * a * y &= e * y = y \end{aligned}\right\} \Rightarrow x = y$$

Закључак: Сваки леви инверз од $a \in M$ је једнак сваком десном.

Последица: Такав елемент (x, одн. y) је јединствен.

Д:
$$\overbrace{x * a}^{\text{леви}} = a * x = e$$
$$x' * a = \underbrace{a * x'}_{\text{десни}} = e \quad , \quad \text{па због закључка} \quad x = x'$$

деф. Нека је $(M, *, e)$ моноид. Елемент $a \in M$ је **инвертибилан** ако је инв. и слева и здесна. У том случају, постоји јединствени **инверз** за a, у ознаци a^-, ткд. $a * a^- = a^- * a = e$

T6: Нека је $(M, *, e)$ моноид и $a, b \in M$ инвертибилни. Тада важи:

1) $a * b$ је инвертибилан, $(a * b)^- = b^- * a^-$
2) a^- је инвертибилан, $(a^-)^- = a$

Д: 1)
$$a * b * b^- * a^- = a * e * a^- = a * a^- = e$$
$$b^- * a^- * a * b = b^- * e * b = b^- * b = e$$

2) $a^- * a = a * a^- = e$

Последица: $(a_1 * \ldots * a_n)^- = a_n^- * \ldots * a_1^-$

Д: Индукцијом по n.

деф. Нека је $(M, *, e)$ моноид и $a \in M$ инвертибилан. Дефинишемо:

$$a^{-n} \underset{а)}{:=} (a^-)^n \underset{б)}{=} (a^n)^- , \quad \text{за } n \in \mathbb{N} \quad (\text{јер } (a * \ldots * a)^- = a^- * \ldots * a^-)$$
$$a^0 = e$$

Напомена: Ако је $n < 0$, тј. $n = -m$, важи $a^{-n} = a^m = ((a^m)^-)^- \overset{б)}{=} (a^{-m})^- = (a^n)^-$

Такође, $(a^-)^n = (a^-)^{-m} \overset{а)}{=} ((a^-)^-)^m = a^m = (a^n)^-$

Дакле, важи $a^{-n} = (a^n)^- = (a^-)^n$ и за $n \in \mathbb{Z}$

T7: Нека je $(M, *, e)$ моноид и $a \in M$ инвертибилан. Тада за све $m, n \in \mathbb{Z}$ важи:

1) $a^{m+n} = a^m * a^n$

2) $(a^m)^n = a^{m \cdot n}$

Д: 1) 1° $m, n \geq 0$

1°_1 $m = 0 \lor n = 0$: тривијално

1°_2 $m, n > 0$: $a^{m+n} = \underbrace{a * \ldots * a}_{m+n}$, $a^m * a^n = \underbrace{a * \ldots * a}_{m} * \underbrace{a * \ldots * a}_{n}$

2° $m > 0, n < 0$: узмимо $n = -k$

2°_1 $m > k$: $\begin{cases} a^{m+n} = a^{m-k} \\ a^m * a^n = a^m * a^{-k} \overset{1^\circ_2}{=} (a^{m-k} * \overbrace{a^k) * (a^k)^-}^{e} = a^{m-k} \end{cases}$

2°_2 $m < k$: $\begin{cases} a^{m+n} = a^{m-k} = a^{-(k-m)} = (a^{k-m})^- \\ a^m * a^n = a^m * a^{-k} \overset{1^\circ_2}{=} \overbrace{a^m * ((a^-)^m}^{e} * (a^-)^{k-m}) = (a^{k-m})^- \end{cases}$

2°_3 $m = k$ $\begin{cases} a^{m+n} = a^{m-m} = a^0 = e \\ a^m * a^n = a^m * a^{-m} = e \end{cases}$

3° $m < 0, n > 0$: аналогно као 2°

4° $m, n < 0$: узмимо $m = -l$, $n = -k$

$$a^m * a^n = a^{-l} * a^{-k} = (a^-)^l * (a^-)^k \overset{1^\circ_2}{=} (a^-)^{l+k} = a^{m+n}$$

2) 1° $n = 0$: $\begin{cases} (a^m)^0 = e \\ a^{m \cdot 0} = a^0 = e \end{cases}$

2° $n > 0$: (БИ) $n = 1$: $(a^m)^1 = a^m = a^{m \cdot 1}$

(ИК) $n \Rightarrow n+1$: $(a^m)^{n+1} \overset{1)}{=} (a^m)^n * (a^m)^1 \overset{(\text{ИХ})}{=} a^{mn} * a^m \overset{1)}{=} a^{m(n+1)}$

3° $n < 0$: узмимо $n = -k$

$$(a^m)^n = (a^m)^{-k} = ((a^m)^k)^- \overset{2^\circ}{=} (a^{mk})^- = a^{-mk} = a^{mn}$$

$\boxed{3.}$ Групе - дефиниција и основна својства

деф. Алгебарска структура $(G, *, ^{-}, e)$ типа $(2,1,0)$ је **група** акко:

1.1) $(G, *, e)$ је моноид
1.2) $(\forall a \in G)\ a * a^{-} = a^{-} * a = e$

деф. Алгебарска структура $(G, *)$, где је $*$ бинарна оп., је **група** акко:

2.1) $(G, *)$ је полугрупа
2.2) $(\exists e \in G)(\forall a \in G)\ a * e = e * a = a$
2.3) $(\forall a \in G)(\exists a^{-} \in G)\ a * a^{-} = a^{-} * a = e$

T1: Наведене две дефиниције су еквивалентне.

Д: $(1 \Rightarrow 2)$
2.1) $(G, *, e)$ моноид $\Rightarrow$ $(G, *)$ полугрупа
2.2) По деф. моноида
2.3) Тривијално из 1.2

$(2 \Rightarrow 1)$
1.1) $(G, *)$ полугрупа и e јединств. неутрал $\Rightarrow (G, *, e)$ моноид
1.2) Доказали смо да (ако постоји) је инверз јединствен.
По 2.3 инверз постоји, па можемо дефинисати операцију $^{-}$

T2: Ако је $(G, *)$ полугрупа, тада су следећа тврђења еквивалентна:

(1) $(G, *)$ је група

(2) $\forall a, b \in G$ једначине $a * x = b$ и $x * a = b$ имају јединств. реш. у G

(3) $(\exists e \in G)(\forall a \in G)\ a * e = a$
$(\forall a \in G)(\exists a^{-} \in G)\ a * a^{-} = e$

Д: $(1 \Rightarrow 2)$ $a * x = b \Rightarrow a^{-} * a * x = a^{-} * b$
$\Rightarrow x = a^{-} * b$

(пошто је инверз јединствен онда је и решење јединствено)

Аналогно и за другу једначину

$(2 \Rightarrow 3)$ * Нека $c \in G$. Једначина $c * x = c$ има решење $x = e$
Знамо $\exists b \in G\ b * c = a$ (као решење једначине $x * c = a$)
Следи $a * e = b * c * e = b * c = a$

* Други део је тривијалан (a^{-} је решење)

(3 ⇒ 1) Доказујемо: (i) $\forall a \in G \quad e * a = a$
(ii) $a * b = e \Rightarrow b * a = e$

$\underbrace{b * a}_{c} * b = b * e = b$, дакле $c * b = b$

Нека је $d \in G$ $b * d = e \Rightarrow \left.\begin{array}{l} c * b * d = b * d = e \\ c * b * d = c * e = c \end{array}\right\} \Rightarrow c = e$

Дакле, $b * a = c = e$. (ii)

Такође: $\left.\begin{array}{l} a * b * a = a * e = e \\ a * b * a = e * a \end{array}\right\} \Rightarrow e * a = a$ (i)

Т3: Ако је $f: G \to H$ хомоморфизам група $(G, *)$ и $(H, \circ)$ онда је f такође хомоморфизам група $(G, *, ^{-}, e)$ и $(H, \circ, ^{\sim}, \varepsilon)$

Д: Знамо $(\forall g_1, g_2 \in G) \quad f(g_1 * g_2) = f(g_1) \circ f(g_2) \quad (*)$

Доказујемо да се f добро слаже са паровима (e, ε) и $(^{-}, ^{\sim})$, тј. $f(e) = \varepsilon$ и $f(a^{-}) = (f(a))^{\sim}$.

- $a * e = a \Rightarrow f(a * e) = f(a) \overset{(*)}{\Rightarrow} f(a) \circ f(e) = f(a) \overset{\exists! \varepsilon}{\Rightarrow} f(e) = \varepsilon.$
- $a * a^{-} = e \Rightarrow f(a * a^{-}) = f(e) = \varepsilon \overset{(*)}{\Rightarrow} f(a) \circ f(a^{-}) = \varepsilon \overset{\exists! f(a)^{\sim}}{\Rightarrow} f(a^{-}) = (f(a))^{\sim}$

Дакле, f се слаже са свим паровима операција.

деф. Група $(H, \circ)$ је **подгрупа** од групе $(G, *)$ ако је њена алгебарска подструктура.

Т4: Ако је $(H, \circ)$ подгрупа од $(G, *)$, онда је и $(H, \circ, ^{\sim}, \varepsilon)$ подструк. од $(G, *, ^{-}, e)$

Д: Знамо $\forall x, y \in H \quad x \circ y = x * y$.

Доказујемо да је: $^{\sim}$ подоперација од $^{-}$, тј. $a^{\sim} = a^{-}$
ε подоперација од e, тј. $\varepsilon = e$

Како $H \subseteq G$, знамо да $\varepsilon \in G$ и $a^{\sim} \in G$

- $a \circ \varepsilon = a \overset{\circ \text{ подоп. } *}{\Rightarrow} a * \varepsilon = a \overset{\exists! e}{\Rightarrow} \varepsilon = e$
- $a \circ a^{\sim} = \varepsilon \Rightarrow a * a^{\sim} = \varepsilon = e \overset{\exists! a^{-}}{\Rightarrow} a^{\sim} = a^{-}$

4. Подгрупе

деф. Ако је $(H,\circ)$ подгрупа од $(G,*)$ тада пишемо $H \leq G$
Уместо $a*b$, скраћено пишемо ab, док инверз од a означавамо са a^{-1}.

деф. Ако подразумевамо која је операција у групи $(G,*)$ кажемо да је G група.

деф. Ако су $A,B \subseteq G$, уводимо: $AB = \{ab \mid a\in A,\ b\in B\} \subseteq G$
$A^{-1} = \{a^{-1} \mid a \in A\} \subseteq G$

T1: Ако је G група и $H \subseteq G$ непразан, тада су следећа тврђења еквивалентна:

(1) $H \leq G$
(2) $(\forall a,b \in H)\ a^{-1}b \in H$
(3) $(\forall a,b \in H)\ ab \in H,\ a^{-1} \in H$
(4) $HH = H,\ H^{-1} = H$

Д: (1⇒2) $a,b \in H \overset{(1)}{\Longrightarrow} a^{-1}, b \in H \overset{H \text{ је група}}{\Longrightarrow} a^{-1}b \in H$

(2⇒3) $H \neq \emptyset \Rightarrow \exists a \in H \overset{(2)}{\Longrightarrow} a^{-1}a = e \in H$
* $a, e \in H \Rightarrow a^{-1}e = a^{-1} \in H$
* $a^{-1}, b \in H \Rightarrow ab \in H$

(3⇒1) $a,b \in H \subseteq G \Rightarrow ab \in H$, дакле имамо подоперацију $\cdot$ на H.

* Овако деф. операција на H јесте операција (провером по деф.)
* $a, a \in H \Rightarrow a^{-1}, a \in H \Rightarrow a^{-1}a = e \in H$. Дакле, постоји неутрал.
* $a \in H \Rightarrow a^{-1} \in H$. Дакле, за свако a постоји инверз.

(3⇒4) Пошто смо доказали 3⇒1, знамо $H \leq G$, па $\exists e \in H$

* $a,b \in H \Rightarrow ab \in H$, дакле $HH \subseteq H$
$e \in H \Rightarrow HH \supseteq \{e\}H = H$, дакле $H \subseteq HH$ $\Big\} \Rightarrow HH = H$

* $a \in H \Rightarrow a^{-1} \in H \Rightarrow H^{-1} \subseteq H$
Даље, $(H^{-1})^{-1} \subseteq H^{-1} \Rightarrow H \subseteq H^{-1}$ $\Big\} \Rightarrow H^{-1} = H$

(4⇒3) * $HH = H \Rightarrow HH \subseteq H \Rightarrow (\forall a,b \in H)\ ab \in H$
$H^{-1} = H \Rightarrow H^{-1} \subseteq H \Rightarrow (\forall a \in H)\ a^{-1} \in H$

T2: Нека су $H, K \leq G$. Тада: $HK \leq G \iff HK = KH$

Д: (⇒) $HK \leq G \Rightarrow (HK)^{-1} = HK \Rightarrow K^{-1}H^{-1} = HK \Rightarrow KH = HK$

(⇐) * $(HK)^{-1} = K^{-1}H^{-1} \overset{\substack{(H,K\leq G)\\ K^{-1}=K\\ H^{-1}=H}}{=} KH = HK$, дакле $HK = (HK)^{-1}$
* $H\underbrace{KH}_{HK}K = \underbrace{HH}_{H}\underbrace{KK}_{K} = HK$, дакле $(HK)(HK) = HK$, па је, по T1(4), $HK \leq G$

* Нека је G група и $S \subseteq G$. Тражимо најмањи скуп који садржи S, а да је група.
Означимо Π_S фамилију свих подгрупа од G које садрже S (јасно $G \in \Pi_S$)

деф. Подгрупа од G генерисана подскупом S је скуп $\langle S \rangle = \bigcap_{H \in \Pi_S} H$

T3: Нека је G група. 1) $H_i \leq G$ за све $i \in I$, тада $\bigcap_{i \in I} H_i \leq G$

2) $H, K \leq G$, тада $H \cup K \leq G \iff K \subseteq H \vee H \subseteq K$

Д: 1) * $\bigcap H_i \neq \emptyset$, јер $e \in H_i$ за свако $i \in I$, па $e \in \bigcap H_i$
* $a, b \in \bigcap H_i \Rightarrow \forall i \; a, b \in H_i$, а пошто $H_i \leq G \Rightarrow \forall i \; a^{-1}b \in H_i \Rightarrow a^{-1}b \in \bigcap H_i$

2) ($\Rightarrow$) ппс. $K \nsubseteq H \wedge H \nsubseteq K \Rightarrow \exists h \in H \setminus K$, $\exists k \in K \setminus H$. Знамо и $H \cup K \leq G$
$h, k \in H \cup K \Rightarrow hk \in H \cup K \Rightarrow hk \in H \vee hk \in K$
1° $hk \in H$, знамо $h \in H \Rightarrow h^{-1}hk = k \in H$ $\lightning$
2° $hk \in K$, тада $(hk)^{-1} = k^{-1}h^{-1} \in H \Rightarrow kk^{-1}h^{-1} = h^{-1} \in K \Rightarrow h \in K$ $\lightning$

($\Leftarrow$) Без умањења општости, нека је $H \subseteq K$. Тада $H \cup K = H$, а $H \leq G$

Последица: $\langle S \rangle \leq G$

Дакле, $\langle S \rangle$ заиста јесте подгрупа, а очигледно је и најмања (по инклузији).

деф. $\langle \emptyset \rangle = \{e\}$; $\langle a \rangle = \langle \{a\} \rangle$

T4: Ако је G група, тада: $\langle S \rangle = \{ a_1 a_2 \dots a_n \mid n \in \mathbb{N}_0, a_i \in S \cup S^{-1} \}$ $(S \subseteq G)$

Д: Означимо скуп са десне стране са H (доказујемо да је H најмања подгрупа) која садржи S

* Јасно, $S \subseteq H$ (само ставимо $n=1$)

* Докажимо $H \leq G$:
Знамо $H \neq \emptyset$, дакле $\exists a, b \in H \Rightarrow a = a_1 \dots a_n$, $b = b_1 \dots b_m$ $(a_i, b_j \in S \cup S^{-1})$
Пошто $a_i^{-1} \in (S \cup S^{-1})^{-1} = S^{-1} \cup (S^{-1})^{-1} = S \cup S^{-1} \Rightarrow a^{-1} \in H$
Дакле, $a^{-1}b = a_n^{-1} \dots a_1^{-1} b_1 \dots b_m \Rightarrow a^{-1}b \in H \Rightarrow H \leq G$

* Докажимо да је H најмања подгрупа:
Нека $K \leq G$ садржи S. Тада $a_1, \dots, a_n \in S \cup S^{-1} \subseteq K$ $\left(\begin{array}{l} x \in S \Rightarrow x \in K \\ K \leq G \underset{T1(3)}{\Rightarrow} x^{-1} \in K \end{array} \right)$
Пошто је K подгрупа $\underset{T1(3)}{\Rightarrow} a_1 \dots a_n \in K \Rightarrow H \subseteq K$

Одавде следи: $\langle S \rangle = H$

5. Лагранжова теорема.

деф. Нека је $H \leq G$. Уводимо релацију $\sim$ на Gткд. $a \sim b \iff a^{-1}b \in H$

T1: $\sim$ је релација еквиваленције на G

Д: (Р) $a^{-1}a = e \in H \Rightarrow a \sim a$

(С) $a \sim b \Rightarrow a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} = b^{-1}a \in H \Rightarrow b \sim a$

(Т) $a \sim b,\ b \sim c \Rightarrow a^{-1}b,\ b^{-1}c \in H \Rightarrow a^{-1}bb^{-1}c = a^{-1}c \in H \Rightarrow a \sim c$

* $C_a = \{b \in G \mid a^{-1}b \in H\} = \{b \in G \mid a^{-1}b = h$, за неко $h \in H\} = \{b \in G \mid b = ah\} = \{ah \mid h \in H\}$

деф. Леви косет подгрупе H је скуп $aH = \{ah \mid h \in H\}$. Кажемо и леви положај.

T2:
1) $a \in aH$
2) $\forall a,b \in G \quad aH \cap bH \neq \emptyset$ или $aH = bH$
3) $\forall a,b \in G \quad aH = bH \iff a^{-1}b \in H$
4) $aH = H \iff a \in H$
5) $\bigcup_{a \in G} aH = G$
6) $S \subseteq H \Rightarrow SH = H$

Д: aH је по деф. класа еквиваленције, па су ове особине последице тога.

деф. Скуп левих косета подгрупе H означавамо са $G_L(H)$.

Аналогно:

деф. Нека је $H \leq G$. Уводимо релацију $\backsim$ на G ткд. $a \backsim b \iff ab^{-1} \in H$

Она је такође релација еквиваленције.

деф. Десни косет подгрупе H је скуп $Ha = \{ha \mid h \in H\}$ Кажемо и десни положај.

деф. Скуп десних косета подгрупе H означавамо са $G_D(H)$.

Напомена: Постоји бијекција између $G_L(H)$ и $G_D(H)$. То је нпр. $f(aH) = Ha^{-1}$

деф. Ако је G коначан скуп, ред групе G је бр. елемената G, у ознаци $|G|$.
Иначе, кажемо да је G бесконачног реда.

деф. Количнички скуп је скуп $G/H = G_L(H)$

деф. Ако је G/H коначан, индекс подгрупе H у групи G је $[G:H] = |G/H|$
Иначе, кажемо да је H бесконачног индекса у G.

Лагранжова теорема: Нека је G коначна група и $H \leq G$. Тада $|H| \cdot [G:H] = |G|$

Д: * Докажимо $\forall a \in G \quad |aH| = |H|$.

За то је довољно доказати да је $f: H \to aH$, $f(h) = ah$ бијекција.

- f је на: тривијално
- f је 1-1: $f(h_1) = f(h_2) \Rightarrow ah_1 = ah_2 \Rightarrow h_1 = h_2$

* Нека су $a_1H, \ldots, a_kH$ сви различити косети. Тада $k = [G:H]$.
Уз то, ови скупови чине партицију скупа G.

$$\Rightarrow |G| = |a_1H| + \ldots + |a_kH| = |H| + \ldots + |H| = k \cdot |H| = |H| \cdot [G:H]$$

ТЗ: Нека $K \leq H \leq G$ и нека су $[G:H], [H:K]$ коначни. Тада: $[G:K] = [G:H] \cdot [H:K]$.

Д: (Ако је G коначна, доказ следи из Лагранжове теореме)

Означимо $[G:H] = k$ и нека су $g_1H, \ldots, g_kH$ сви леви косети подгрупе H у G.
Означимо $[H:K] = n$ и нека су $h_1K, \ldots, h_nK$ сви леви косети подгрупе K у H.

* Докажимо $[G:K] \geq kn$, тако што ћемо доказати да су косети g_ih_jK различити за $1 \leq i \leq k$, $1 \leq j \leq n$

ппс. $g_ih_jK = g_lh_sK \Rightarrow (g_lh_s)^{-1}g_ih_j \in K$

$\Rightarrow h_s^{-1}g_l^{-1}g_ih_j = k' \in K \quad / h_s * \_ * h_j^{-1} \qquad (*)$

$\Rightarrow g_l^{-1}g_i = h_sk'h_j^{-1} \in H \quad$ (јер $K \leq H$)

$\Rightarrow g_lH = g_iH \overset{\text{сви разл.}}{\Rightarrow} g_l = g_i \Leftrightarrow l = i$

Такође, $g_l = g_i \overset{(*)}{\Rightarrow} h_s^{-1}h_j = k' \in K \Rightarrow h_sK = h_jK \Rightarrow h_s = h_j \Rightarrow s = j$ ↯

* Докажимо $[G:K] \leq kn$

$([G:K] = m,\ u_i \in G)$

ппс. $[G:K] > kn$. Нека су $u_1K, \ldots, u_mK$ сви леви косети подгрупе K у G.

Посматрајмо $u_1H, \ldots, u_mH$. Сваки од њих је једнак неком $g_1H, \ldots, g_kH$.
Како је $kn < m$, постоји $1 \leq i \leq k$, ткд. је бар $n+1$ косета од $u_1H, \ldots, u_mH$ једнако g_iH
Зато, нека је $u_{r_j}H = g_iH$ за све $1 \leq j \leq n+1$
Тада је $g_i^{-1}u_{r_j} \in H$, тј. $g_i^{-1}u_{r_j} = v_j \in H$, дакле $u_{r_j} = g_iv_j$

Посматрајмо сад $v_1K, \ldots, v_{n+1}K$. Ово су леви косети подгрупе K у H.
Како оваквих косета има n, то значи да су нека два једнака, нпр. $v_aK = v_bK$

$$K \ni v_a^{-1}v_b = (g_i^{-1}u_{r_a})^{-1}g_i^{-1}u_{r_b} = u_{r_a}^{-1}u_{r_b} \in K \Rightarrow u_{r_a}K = u_{r_b}K \text{ ↯}$$

Дакле, $\left.\begin{array}{l} [G:K] \leq kn \\ [G:K] \geq kn \end{array}\right\} \Rightarrow [G:K] = kn = [G:H][H:K]$

$\boxed{6.}$ Цикличне групе; ред елемента у групи.

* Због $\boxed{4}$ Т4, знамо: $\langle a\rangle = \{a^k \mid k\in\mathbb{Z}\} \leq G$

деф. Група G је **циклична** ако постоји $a\in G$ ткд. $G=\langle a\rangle$
Елемент a је **генератор** групе $\langle a\rangle$.

деф. Нека је G група и $a\in G$. **Ред елемента** a је најмање $n\in\mathbb{N}$, ткд. $a^n=e$
Означавамо га $\omega(a)$, или $\rho(a)$, $r(a)$, $ord(a)$
Ако такво n не постоји, кажемо да је a **бесконачног реда**.

Т1: Нека је $G=\langle a\rangle$ циклична група

1) Ако је a бесконачног реда, тада је и G бесконачног реда.

2) Иначе, важи $|G|=\omega(a)$

Д: 1) ппс. $G=\{a^k \mid k\in\mathbb{Z}\}$ је коначан скуп. Дакле, у низу $e, a^1, a^2, \dots$ има једнаких.
Нека је $a^i=a^j$. То значи $a^{i-j}=e$. ↯

2) $G=\{a^k \mid k\in\mathbb{Z}\}$. Означимо $\omega(a)=n$ и $A=\{e, a, a^2, \dots, a^{n-1}\}$

* Докажимо $G=A$:

($\supseteq$) тривијално

($\subseteq$) Нека је $a^k\in G$, $k\in\mathbb{Z}$. Знамо $a^n=e$. Нека је $k=nq+r$
Тада: $a^k=a^{nq+r}=(a^n)^q a^r = a^r \in A$

* Докажимо да су $e, a, a^2, \dots, a^{n-1}$ међусобно различити:

ппс. $a^i=a^j$, $0\leq i\leq j\leq n$ $\Rightarrow$ $a^{j-i}=e$, а $j-i\leq n$ ↯

Последица: Ако је G коначна, тада $\omega(a) \mid |G|$

Д: $\omega(a)=|\langle a\rangle|$ и $\langle a\rangle\leq G$. По Лагранжовој теореми: $|\langle a\rangle| \mid |G|$

T2: Нека је G група и $a \in G$.

1) Нека је $n = \omega(a) < +\infty$. Тада $a^m = e$ акко $n \mid m$

2) Ако је a бесконачног реда, тада је за $\forall m \in \mathbb{Z} \setminus \{0\}$ и a^m бесконачног реда.

Иначе: $\omega(a^m) = \dfrac{\omega(a)}{NZD(\omega(a), m)}$

Д: 1) $(\Rightarrow)$ $a^m = e$, $a^n = e$. Запишимо $m = nq + r$, $0 \leq r \leq n-1$
$e = a^m = a^{nq+r} = (a^n)^q a^r$. Дакле $a^r = e \overset{r<n}{\Rightarrow} r = 0 \Rightarrow n \mid m$

$(\Leftarrow)$ тривијално

2) 1° ппс. $\omega(a^m) = n$. Тада: $e = (a^m)^n = a^{mn} = a^{|mn|} \overset{|mn| \neq 0}{\Longrightarrow}$ a коначног реда $\lightning$

2° Означимо $\omega(a) = n$, $\omega(a^m) = t$. Посматрајмо све l ткд. $(a^m)^l = e$.
Нека је $NZD(n, m) = s$, $m = s \cdot u$, $n = s \cdot v$, дакле $NZD(u, v) = 1$.

$(a^m)^l = e \iff n \mid ml \iff sv \mid sul \iff v \mid ul \iff v \mid l$

Тражено t је једнако најмањем од свих l.
Због еквиваленција, t је најмањи број којег v дели, па је $t = v$.

$$\omega(a^m) = t = v = \frac{n}{s} = \frac{\omega(a)}{NZD(\omega(a), m)}$$

T3: 1) Нека је $f: G \to H$ хомоморфизам и $x \in G$ коначног реда. Тада:

$$\omega(f(x)) \mid \omega(x)$$

2) Ако је f изоморфизам, важи $\omega(f(x)) = \omega(x)$

Д: Означимо $\omega(x) = n$

1) Важи $f(x)^n = f(x) \dots f(x) = f(x \dots x) = f(x^n) = f(e) = e$
Зато је $f(x)$ коначног реда, па знамо $\omega(f(x)) \mid n$, тј. $\omega(f(x)) \mid \omega(x)$

2) Тада је f^{-1} хомоморфизам, па применимо 1) на f^{-1}

Т4: 1) **Подгрупа цикличне групе је такође циклична.** (и за коначне и за бесконачне)

2) **Ако је $G=\langle a\rangle$ реда n (коначна) и $k \mid n$, тада G има тачно једну подгрупу реда k.**

3) **Ако је $\langle a^l\rangle$ реда k ($k \mid n$), важи: $\langle a^l\rangle = \langle a^{NZD(n,l)}\rangle$** (за коначне)

Д: 1) Нека је $G=\langle a\rangle$ циклична група и $H \leq G$.

Довољно је доказати да постоји $l \in \mathbb{Z}$ т.к.д. $H=\langle a^l\rangle$

Нека је l најмањи природан број т.к.д. $a^l \in H$ $\longrightarrow$ (сви из G су облика a на нешто, а $H \in G$, па су и сви из H тог облика и постоји најмањи такав број у $\mathbb{N}$ $(a^k \in H \Rightarrow a^{-k} \in H)$)

$(\supseteq)$ $a^l \in H \overset{H \leq G}{\Longrightarrow} \langle a^l\rangle \leq H$

$(\subseteq)$ Нека је $h \in H$, тада $h=a^t$, $t \in \mathbb{Z}$ (јер важи $h \in G=\langle a\rangle$)

$\underbrace{a^t}_{\in H} = a^{lq+r} = \underbrace{(a^l)^q}_{\in\langle a^l\rangle \leq H} a^r \Longrightarrow a^r \in H$

Како је $r<l \Rightarrow r=0 \Rightarrow t=lq \Rightarrow h=a^t=(a^l)^q \in \langle a^l\rangle$

2) * Докажимо да постоји бар једна подгрупа реда k:

$H=\langle a^{\frac{n}{k}}\rangle$ је реда k јер: $\omega(a^{\frac{n}{k}}) = \dfrac{\omega(a)}{NZD(\omega(a),\frac{n}{k})} = \dfrac{n}{NZD(n,\frac{n}{k})} = \dfrac{n}{\frac{n}{k}} = k$

* Докажимо да је то једина таква подгрупа:

Узмимо $K \leq G$, $|K|=k$. По 1), K је циклична, па $K=\langle a^l\rangle$

$k=|K|=\omega(a^l)=\dfrac{\omega(a)}{NZD(\omega(a),l)} = \dfrac{n}{NZD(n,l)}$. Означимо $NZD(n,l)=d \Rightarrow k=\dfrac{n}{d}$

Дакле $d=\dfrac{n}{k}$, тј. $\dfrac{n}{k} \mid l \Rightarrow a^l \in H \Rightarrow \left.\begin{array}{l}\langle a^l\rangle = K \subseteq H \\ |K|=|H|=k\end{array}\right\} \Rightarrow K=H$

3) По претходном: $\underset{K}{\underset{\parallel}{\langle a^l\rangle}} = \underset{H}{\underset{\parallel}{\langle a^{\frac{n}{k}}\rangle}} = \langle a^d\rangle = \langle a^{NZD(n,l)}\rangle$

Последица: **a^l је генератор групе $G=\langle a\rangle$ реда n акко $NZD(n,l)=1$.**

Д: Из 3): $\langle a^l\rangle = \langle a^{NZD(n,l)}\rangle = \langle a^1\rangle = \langle a\rangle = G$

7. Класификација цикличних група.

Т1: Свака циклична група је изоморфна са $\mathbb{Z}$ или са $\mathbb{Z}_n$ $(n \in \mathbb{N})$.

Д: Нека је $G = \langle a \rangle$

1° G – бесконачног реда

Знамо $G = \{a^k \mid k \in \mathbb{Z}\}$
Докажимо да је $f: G \to \mathbb{Z}$, $f(a^k) = k$ изоморфизам.

* Докажимо добру дефинисаност:

$$a^k = a^l \Rightarrow a^{l-k} = e \Rightarrow l-k = 0 \Rightarrow l = k$$

иначе је a коначног реда

* Докажимо да је хомоморфизам:

$$f(a^k * a^l) = f(a^{k+l}) = k + l = f(a^k) + f(a^l)$$

* Докажимо да је бијекција:

1-1: $f(a^k) = f(a^l) \Rightarrow k = l \Rightarrow a^k = a^l$
на: тривијално

2° G – коначног реда, $|G| = n$

Тада је $\omega(a) = |G| = n$. Такође: $G = \{e, a, a^2, \dots, a^{n-1}\}$ (сви елементи су различити)
Докажимо да је $f: G \to \mathbb{Z}_n$, $f(a^k) = k$, $0 \leq k \leq n-1$

* Докажимо добру дефинисаност: аналогно

* Докажимо да је хомоморфизам:

$$f(a^k * a^l) = f(a^{k+l}) = f(a^{nq + (k +_n l)}) = f(a^{k +_n l}) = k +_n l = f(a^k) +_n f(a^l)$$

* Докажимо да је бијекција: аналогно

Последица: Ако је p прост број, свака група са p елемената је изоморфна са $\mathbb{Z}_p$

Д: $|G| = p$ и $\omega(a) \mid p$ и p - прост $\Rightarrow \omega(a) = p \Rightarrow G$ - циклична $\overset{T1}{\Rightarrow} G \cong \mathbb{Z}_p$

8. Директан производ група.

деф. Нека су $(G, *)$ и $(H, \circ)$ групе. Директан производ, $G \times H$, ових група је алг. стр. чији је носач $G \times H$, а операција $\bullet$ деф. са $(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 \circ h_2)$

T1: Директан производ група је група.

Д: * асоцијативност: једноставно
* неутрал: (e_G, e_H)
* инверз: (g^{-1}, h^{-1})

T2: Нека је $(a,b) \in G \times H$. Тада: $\omega(a,b) = NZS(\omega(a), \omega(b))$

Д: Означимо $\omega(a) = n$, $\omega(b) = m$. Тражимо најмање k ткд. важи:

$$\underset{e_G\ \ e_H}{(e, e)} = (a,b)^k = (a,b) * \ldots * (a,b) = (a^k, b^k) \iff a^k = e \wedge b^k = e$$
$$\iff n \mid k \wedge m \mid k$$
$$\iff NZS(n,m) \mid k$$

Дакле, $k = NZS(\omega(a), \omega(b))$

T3: Група $\mathbb{Z}_m \times \mathbb{Z}_n$ је циклична акко $NZD(m,n) = 1$.

Д: $(\Rightarrow)$ Нека је $\mathbb{Z}_m \times \mathbb{Z}_n = \langle (a,b) \rangle$. Важи $\omega(a,b) = |\mathbb{Z}_m \times \mathbb{Z}_n| = mn$
Са друге стране, $\omega(a,b) = NZS(\omega(a), \omega(b))$.

Како $a \in \mathbb{Z}_m \Rightarrow \omega(a) \mid |\mathbb{Z}_m| \Rightarrow \omega(a) \mid m$. Аналогно, $\omega(b) \mid n$

Самим тим: $mn = \omega(a,b) = NZS(\omega(a), \omega(b)) \leq NZS(m,n) \Rightarrow NZS(m,n) = mn$
а знамо да је $NZS(m,n) = mn$ акко $NZD(m,n) = 1$

$(\Leftarrow)$ Докажимо да је $(1,1)$ генератор групе $\mathbb{Z}_m \times \mathbb{Z}_n$

$$\omega(1,1) = NZS(\omega(1), \omega(1)) = NZS(m,n) \underset{NZD(m,n)=1}{=} mn \Rightarrow \omega(1,1) = mn = |\mathbb{Z}_m \times \mathbb{Z}_n|$$

Последица: Ако је $NZD(m,n) = 1$, тада $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$

Д: $NZD(m,n) = 1 \iff \mathbb{Z}_m \times \mathbb{Z}_n$ је циклична

По класификацији, свака коначна циклична група реда k је изоморфна са $\mathbb{Z}_k$.

T4: Нека је $G_1 \cong H_1$, $G_2 \cong H_2$. Тада: $G_1 \times G_2 \cong H_1 \times H_2$

Д: $F: G_1 \times G_2 \to H_1 \times H_2$, $F(g_1, g_2) = (f_1(g_1), f_2(g_2))$ (где $\underset{\text{изоморфизам}}{f_1}: G_1 \to H_1$ и $\underset{\text{изоморфизам}}{f_2}: G_2 \to H_2$)

Види се да је и F изоморфизам

деф. Нека су $H, K \leq G$ ткд. важи:
1° $G = HK$
2° $H \cap K = \{e\}$
3° $\forall h \in H, k \in K$ $hk = kh$

Тада је G **унутрашњи директни производ** подгрупа H и K.

T5: Нека је G унутр. дир. пр. од H и K. Тада $G \cong H \times K$

Д: Докажимо да је $f: H \times K \to G$, $f(h,k) = hk$ изоморфизам

* Докажимо добру дефинисаност: очигледно

* Докажимо да је хомоморфизам:

$$f((h_1,k_1)\cdot(h_2,k_2)) = f(h_1h_2, k_1k_2) = h_1h_2k_1k_2 \overset{3°}{=} h_1k_1h_2k_2 = f(h_1,k_1)\cdot f(h_2,k_2)$$

* Докажимо да је бијекција:

1-1: $f(h_1,k_1) = f(h_2,k_2) \Rightarrow h_1k_1 = h_2k_2 \Rightarrow \underbrace{h_2^{-1}h_1}_{H} = \underbrace{k_2k_1^{-1}}_{K}$

$$\overset{2°}{\Rightarrow} \left.\begin{array}{l} h_2^{-1}h_1 = e \Rightarrow h_1 = h_2 \\ k_2k_1^{-1} = e \Rightarrow k_1 = k_2 \end{array}\right\} \Rightarrow (h_1,k_1) = (h_2,k_2)$$

на: из 1°

9. Групе пермутација - основна својства, скупови генератора, ред пермутације.

деф. Нека је X непразан скуп. $S_X = \{ f: X \to X \mid f$ је бијекција $\}$.

T1: $(S_X, \circ)$ је група.

Д: * асоцијативност: важи увек, па и за овај случај
* неутрал: id
* инверз: f^{-1}

деф. S_X је група пермутација скупа X.
Често се назива и симетрична група и означава са $\mathrm{Sym}X$.

T2: Ако је $|X| = |Y|$, тада $S_X \cong S_Y$

Д: Нека је $\phi: X \to Y$ бијекција
Докажимо да је $F: S_X \to S_Y$, $F(f) = \phi \circ f \circ \phi^{-1}$ изоморфизам.

* Докажимо добру дефинисаност: јесте бијекција и јесте $Y \to Y$

* Докажимо да је хомоморфизам:

$$F(f_1 \circ f_2) = \phi \circ f_1 \circ f_2 \circ \phi^{-1} = \phi \circ f_1 \circ \phi^{-1} \circ \phi \circ f_2 \circ \phi^{-1} = F(f_1) \circ F(f_2)$$

* Докажимо да је бијекција:

1-1: $F(f_1) = F(f_2) \Rightarrow \phi \circ f_1 \circ \phi^{-1} = \phi \circ f_2 \circ \phi^{-1} \Rightarrow f_1 = f_2$
на: Нека $g \in S_Y$. Тада: $F(\underbrace{\phi^{-1} \circ g \circ \phi}_{\text{бијекција } X \to X}) = \phi \circ \phi^{-1} \circ g \circ \phi \circ \phi^{-1} = g$

деф. За $X = \{1, 2, \dots, n\}$, уместо S_X, пишемо S_n.

Напомена: $|S_n| = n!$

Последица: Ако је $|Y| = n$, онда $S_Y \cong S_n$

деф. Циклус, у ознаци $\lceil a_1, \dots, a_k \rfloor = \pi$ је пермутација из скупа S_n ткд. важи:

1° $a_1, \dots, a_k$ су различити елементи из $\{1, 2, \dots, n\}$
2° $\pi(a_i) = a_{i+1}$, за $1 \le i \le k-1$ и $\pi(a_k) = a_1$
3° $\pi(b) = b$, за $b \notin \{a_1, \dots, a_k\}$

Носач циклуса је $P = \{a_1, \dots, a_k\}$

деф. Циклуси су дисјунктни ако су им носачи дисјунктни.

Т3: Ако су $\sigma, \pi \in S_n$ дисјунктни циклуси. Важи: $\sigma \circ \pi = \pi \circ \sigma$

Д: Нека је S носач од σ, P носач од π и $a \in \{1, 2, \dots, n\}$

1° $a \notin S$, $a \notin P$: $(\sigma \circ \pi)(a) = \sigma(\pi(a)) = \sigma(a) = a$
$(\pi \circ \sigma)(a) = \pi(\sigma(a)) = \pi(a) = a$

2° $a \notin S$, $a \in P$: $(\sigma \circ \pi)(a) = \sigma(\pi(a)) = \pi(a)$ (напомена: $a \notin S \Rightarrow \pi(a) \notin S$)
$(\pi \circ \sigma)(a) = \pi(\sigma(a)) = \pi(a)$

3° $a \in S$, $a \notin P$: аналогно као 2°

Т4: Нека су $\sigma_1, \dots, \sigma_k$ дисјунктни циклуси из S_n. Тада важи:

$$\omega(\sigma_1 \circ \dots \circ \sigma_k) = NZS(\omega(\sigma_1), \dots, \omega(\sigma_k))$$

Д: Тражимо све t за које важи: $(\sigma_1 \circ \dots \circ \sigma_k)^t = id$

$$(\sigma_1 \dots \sigma_k)^t = \sigma_1 \dots \sigma_k \sigma_1 \dots \sigma_k \dots \sigma_1 \dots \sigma_k = \sigma_1^t \dots \sigma_k^t = id$$

Нека $a \in \{1, \dots, n\}$.
Ако се a не налази ни у једном носачу P_i, онда је $\sigma_1^t \dots \sigma_k^t(a) = a$.
Ако $a \in P_i$, тада га „помера" само σ_i, па важи:
$$(\sigma_1^t \dots \sigma_k^t)(a) = (\sigma_i^t \sigma_1^t \dots \sigma_{i-1}^t \sigma_{i+1}^t \dots \sigma_k^t)(a) = \sigma_i^t(a)$$

Дакле: $\sigma_1^t \dots \sigma_k^t = id \iff \sigma_1^t = id, \dots, \sigma_k^t = id \iff \omega(\sigma_1) \mid t, \dots, \omega(\sigma_k) \mid t$
$\iff NZS(\omega(\sigma_1), \dots, \omega(\sigma_k)) \mid t$

Самим тим, $\omega(\sigma_1, \dots, \sigma_k) = NZS(\omega(\sigma_1), \dots, \omega(\sigma_k))$

Последица: Ако је $\sigma = \lceil a_1, \dots, a_k \rfloor$ циклус, тада је $\omega(\sigma) = k$

Д: * Јасно, $\sigma^l(a_1) = \sigma(\dots(\sigma(a_1))\dots) = \sigma(\dots \sigma(a_2) \dots) = a_{l+1}$
па за $1 \le l \le k-1$, $\sigma^l \ne id$

* Слично, $\sigma^k(a) = a$, за све $a \in \{1, 2, \dots, n\}$

Т5: Свака пермутација $\pi \in S_n$ се јединствено, до на распоред, може записати као производ дисјунктних циклуса.

Д: * Уводимо релацију $a \sim b \iff b = \pi^k(a),\ k \geq 0$. Докажимо да је $\sim$ рел. екв.

(„$a \sim b \iff$ у истом су циклу")

разбијамо на класе

(р) $a \sim a$, јер $\pi^0(a) = a$

(с) Знамо $\pi^k(a) = b$. S_n је група коначног реда $\Rightarrow \exists t \geq 0 \ \pi^t = id$

Изаберемо $l \geq 0$ т.д. $t \mid k+l$, па добијамо $a = \pi^{k+l}(a) = \pi^l(b) \Rightarrow b \sim a$

(т) Знамо $\pi^k(a) = b$, $\pi^l(b) = c \Rightarrow \pi^{k+l}(a) = c$

(овде се понављају)

* Посматрајмо класу екв. неког a: $C_a = \{a, \pi(a), \pi^2(a), \dots\}$

Нека је $s \geq 1$ најмањи бр. т.д. $\pi^s(a) = a$ (s постоји јер је π коначног реда)

Докажимо тада да је $C_a = \{a, \pi(a), \dots, \pi^{s-1}(a)\}$ и да су сви различити.

ког су облика класе

* $\pi^k(a) = \pi^{qs+r}(a) = \pi^r((\pi^s)^q(a)) = \pi^r(a)$, где $k = sq+r$, $0 \leq r \leq n-1$ $\quad k = sq + r$

па је за свако $k \geq 0$, $\pi^k(a) \in \{a, \pi(a), \dots, \pi^{s-1}(a)\}$.

* Различити су, јер $\pi^i(a) = \pi^j(a) \Rightarrow \pi^{j-i}(a) = a$, али важи $0 < j-i \leq s-1$ ↯

свакој класи доделимо циклус

* Нека су $C_{a_1}, \dots, C_{a_k}$ све различите класе еквив. у односу на $\sim$.

Ако је $C_{a_i} = \{a_i, \pi(a_i), \dots, \pi^{s_i-1}(a_i)\}$, тада њој додељујемо циклус $\sigma_i = \lceil a_i, \pi(a_i), \dots, \pi^{s_i-1}(a_i) \rfloor$ (*)

Пошто су C_{a_i} класе екв., ови циклуси су дисјунктни и унија носача је $\{1, 2, \dots, n\}$.

Докажимо да је $\pi = \sigma_1 \sigma_2 \dots \sigma_k$ и да је представљање јединствено.

* Нека је $a \in \{1, 2, \dots, n\}$. Тада је a у тачно једном носачу, нпр. C_{a_i}, па важи:

$$(\sigma_1 \dots \sigma_k)(a) = \sigma_i(a) = \pi(a)$$ (погледати како изгледа (*))

* Нека је $\pi = \sigma_1 \dots \sigma_k = \overset{\text{дисјунктни}}{\tau_1 \dots \tau_l}$. Узмимо да су $\sigma_1, \dots, \sigma_k$ горе деф. циклуси

Нека је T_j носач циклуса τ_j, за све $1 \leq j \leq l$.

Посматрамо a_i за $1 \leq i \leq k$, оно се налази у неком T_j. Тада $\tau_j = \lceil a_i, \pi(a_i), \dots \rfloor$

$\tau_j(a_i) = \pi(a_i)$

Зато је T_j управо C_{a_i}, па је $\sigma_i = \tau_j$

Скратимо σ_i и τ_j, па наставимо поступак. (то може због дисј. $\Rightarrow$ комут.)

Дакле добијамо да су сва представљања једнака (до на распоред циклуса)

деф. Представљање пермутације у облику из теореме је **циклусна декомпозиција** пермутације.

деф. Транспозиција је циклус чији носач има 2 елемента.

Т6: $\lceil a_1, \dots, a_k \rfloor = \lceil a_1, \dots, a_i \rfloor \lceil a_i \dots a_k \rfloor$ за све $k \geq 1$, $1 \leq i \leq k$

Д: Провером за све i.

Последица: Свако $\sigma \in S_n$ се може записати као производ транспозиција.

Д: Директно из Т6.

10. Групе пермутација - Кејлијева теорема

деф. Знак пермутације $\pi \in S_n$ је $sgn(\pi) = (-1)^{n-m}$, где је m број свих циклуса који учествују у циклусној декомпозицији пермутације π.

деф. Ако је $sgn(\pi) = 1$, пермутација је парна.
Ако је $sgn(\pi) = -1$, пермутација је непарна.

T1: За $\pi, \sigma \in S_n$ важи: $sgn(\pi\sigma) = sgn(\pi) \cdot sgn(\sigma)$

Д: * Размотримо прво случај $\sigma = [a, b]$ $(a \neq b)$ и $\pi = \pi_1 \dots \pi_k$ је цикл. декомп. π
Тада $sgn(\pi) = (-1)^{n-k}$ и $sgn(\sigma) = -1$. Тражимо $sgn(\pi_1 \dots \pi_k \sigma)$. Нека је P_i носач од π_i.

1° $a \in P_i$, $b \in P_j$ $(1 \leq i < j \leq k)$.

Нека је $\pi_i = [a, a_1, \dots, a_l]$, $\pi_j = [b, b_1, \dots, b_s]$.
Тада је $\pi_i \pi_j \sigma = [a, a_1, \dots, a_l][b, b_1, \dots, b_s][a, b] = [a, b_1, \dots, b_s, b, a_1, \dots, a_l]$
Дакле, $\pi_1 \dots \pi_k \sigma = \underbrace{\pi_1 \dots \pi_k}_{\text{без } i, j} \pi_i \pi_j \sigma = \pi_1 \dots \pi_k [a, b_1, \dots, b_s, b, a_1, \dots, a_l]$

То је управо цикл. декомп. од $\pi\sigma$ (која нам је и требала), па по деф.

$$sgn(\pi\sigma) = (-1)^{n-(k-2+1)} = (-1)^{n-k+1} = (-1)^{n-k} \cdot (-1) = sgn(\pi) \cdot sgn(\sigma)$$

2° $a, b \in P_i$, за неко $1 \leq i \leq k$

Нека је $\pi_i = [a, a_1, \dots, a_l, b, b_1, \dots, b_s]$
Тада је $\pi_i \sigma = [a, a_1, \dots, a_l, b, b_1, \dots, b_s][a, b] = [a, b_1, \dots, b_s][b, a_1, \dots, a_l]$
Дакле, $\pi_1 \dots \pi_k \sigma = \underbrace{\pi_1 \dots \pi_k}_{\text{без } i} \pi_i \sigma = \pi_1 \dots \pi_k [a, b_1, \dots, b_s][b, a_1, \dots, a_l]$

То је управо цикл. декомп. од $\pi\sigma$ (која нам је и требала), па по деф.

$$sgn(\pi\sigma) = (-1)^{n-(k-1+2)} = (-1)^{n-k-1} = (-1)^{n-k} \cdot \underbrace{(-1)^{-1}}_{(-1)^{-1} = -1} = sgn(\pi) \cdot sgn(\sigma)$$

* Размотримо случај произвољне пермутације σ.
Знамо да се σ може записати као производ транспозиција, $\sigma = \tau_1 \dots \tau_m$, па важи

$$sgn(\pi\sigma) = sgn(\pi \tau_1 \dots \tau_m) = sgn(\pi \tau_1 \dots \tau_{m-1}) \, sgn(\tau_m) = \dots = sgn(\pi) \, sgn(\tau_1) \dots sgn(\tau_m)$$

$$= sgn(\pi) \cdot sgn(\tau_1 \tau_2) \, sgn(\tau_3) \dots sgn(\tau_m) = sgn(\tau_1 \tau_2 \tau_3) \dots sgn(\tau_m)$$

$$\dots = sgn(\pi) \, sgn(\tau_1 \dots \tau_m) = sgn(\pi) \, sgn(\sigma)$$

Последица: $sgn: S_n \to \{-1, 1\}$ је хомоморфизам.

Последица: Пермутација је парна акко се може записати као производ парног броја транспозиција.

деф. Алтернирајућа група је $A_n = \{\sigma \in S_n \mid sgn(\sigma) = 1\}$.

Напомена: $A_n \leq S_n$

Д: Знамо $A_n \neq \emptyset$, јер $id \in A_n$. Довољно је доказати $\sigma, \pi \in A_n \Rightarrow \sigma^{-1}\pi \in A_n$

$sgn(\sigma^{-1}\pi) = sgn(\sigma^{-1})\, sgn(\pi) \overset{(*)}{=} \underset{A_n}{sgn(\sigma^{-1})}\ \underset{A_n}{sgn\, \pi} = 1 \cdot 1 = 1$

(*) $1 = sgn(id) = sgn(\sigma\sigma^{-1}) = sgn(\sigma)\, sgn(\sigma^{-1}) \Rightarrow sgn(\sigma^{-1}) = sgn(\sigma)$

Т2: За $n \geq 2$, $|A_n| = |S_n \setminus A_n|$

Д: Нека је τ произвољна пермутација из $S_n \setminus A_n$ (постоји, нпр. транспозиције, јер $n \geq 2$)
Тада је $f: A_n \to S_n \setminus A_n$, $f(\pi) = \tau\pi$ бијекција.

* Докажимо добру деф.: $sgn(\tau\pi) = sgn(\tau)\, sgn(\pi) = (-1)\cdot 1 = -1 \Rightarrow \tau\pi \in S_n \setminus A_n$
* Докажимо да је 1-1: $f(\pi_1) = f(\pi_2) \Rightarrow \tau\pi_1 = \tau\pi_2 \Rightarrow \pi_1 = \pi_2$
* Докажимо да је на: $\sigma \in S_n \setminus A_n \Rightarrow f(\underset{A_n}{\tau^{-1}\sigma}) = \tau\tau^{-1}\sigma = \sigma$, а јасно $\tau^{-1}\sigma \in A_n$

Последица: $|A_n| = |S_n \setminus A_n| = \frac{n!}{2}$

Л: Ако је $f: G \to H$ хомоморфизам, тада $Im f \leq H$

Д: * $Im(f) \neq \emptyset$: зато што $e = f(e)$
* Нека је $a, b \in Im(f)$. Тада: $h_1, h_2 \in Im(f) \Rightarrow h_1 = f(g_1),\ h_2 = f(g_2)$
$\Rightarrow h_1^{-1}h_2 = f(g_1)^{-1} f(g_2) = f(g_1^{-1}g_2) \Rightarrow h_1^{-1}h_2 \in Im f$

Кејлијева теорема: Свака група G је изоморфна подгрупи групе S_G.

Д: Посматрајмо $F: G \to S_G$, $F(g) = f_g$, где је $f_g: G \to G$, $f_g(x) = gx$.

* Докажимо добру дефинисаност: довољно је доказати да је f_g бијекција.
  * јесте 1-1: $f_g(x) = f_g(y) \Rightarrow gx = gy \Rightarrow x = y$
  * јесте на: $f_g(g^{-1}y) = y$

* Докажимо да је хомоморфизам: $F(g_1g_2) = f_{g_1g_2}(x) = g_1g_2x = g_1 f_{g_2}(x) = f_{g_1}(f_{g_2}(x)) = (f_{g_1} \circ f_{g_2}) = x$

* Докажимо да је 1-1: $F(g_1) = F(g_2) \Rightarrow g_1 x = g_2 x \Rightarrow g_1 = g_2$

Функција F не мора бити на, јер G и S_G не морају имати исти бр. елем.
Зато посматрамо рестрикцију $\tilde{F}: G \to Im F$, оно је јасно на, па је изоморфизам.

Дакле, $G \cong Im F \overset{Л}{\leq} S_G$

11. Ојлерова група, функција и теорема.

деф. $\Phi(n) = \{ k \mid 1 \leq k \leq n,\ NZD(k,n)=1 \}$

Т1: $(\Phi(n), \cdot_n)$ je група, $n \geq 2$

Д. * Докажимо затвореност: доказујемо да за $a,b \in \Phi(n) \Rightarrow a \cdot_n b \in \Phi(n)$.
Нека $ab = nq + (a \cdot_n b)$, па je довољно доказати $NZD(a \cdot_n b, n)=1$
ппс. Постоји $d \geq 2$, $d \mid n$ и $d \mid a \cdot_n b$. Због тога $d \mid ab$.
То значи да бар један од a и b има зај. делилац са n $\lightning$

* Докажимо асоцијативност: Нека $ab = nq_1 + (a \cdot_n b)$ и $(a \cdot_n b)\cdot c = nq_2 + (a \cdot_n b)\cdot_n c$
Тада $(a \cdot_n b)\cdot_n c = (a \cdot_n b)\cdot c - nq_2 = (ab - nq_1)c - nq_2 = abc - n(q_1 c + q_2)$
Дакле, $(a \cdot_n b)\cdot_n c$ je остатак abc при дељењу са n.
Аналогно, $a \cdot_n (b \cdot_n c)$ je остатак abc при дељењу са n.

* Неутрал: $1 \in \Phi(n)$

* Инверз: Нека $a \in \Phi(n)$. Докажимо да постоји $b \in \Phi(n)$ $a \cdot_n b = 1$
За све $x \in \Phi(n)$, посматрамо елемент $a \cdot_n x \in \Phi(n)$.
Ако докажемо да су сви различити, неки од њих мора бити једнак 1.
ппс. $a \cdot_n x = a \cdot_n y$, за $x,y \in \Phi(n)$, $x \neq y$. Нека $ax = nq_1 + a \cdot_n x$, $ay = nq_2 + a \cdot_n y$
Тада $ax - ay = nq_1 - nq_2 \Rightarrow a(x-y) = n(q_1 - q_2)$, а знамо $n \nmid a$ и $n \nmid x-y$ $\lightning$

деф. Група $(\Phi(n), \cdot_n)$ назива се **Ојлерова група**.

деф. Ред групе $\Phi(n)$ означавамо $\varphi(n)$.
Функција $\varphi: N \to N$ je **Ојлерова функција**.

Ојлерова теорема: За свако $n \geq 2$ и $x \in Z$ за које $NZD(x,n)=1$ важи $x^{\varphi(n)} \equiv 1 \pmod n$

Д: Нека $y \in Z_n$, $x \equiv y \pmod n$, тј. $x = nq + y$

Докажимо да $y \in \Phi(n)$.
ппс. Постоји $d > 1$ ткд. $d \mid n$ и $d \mid y$. Тада $d \mid (nq+y)$, тј. $d \mid x$ $\lightning$ $(NZD(x,n)=1)$

У групи $\Phi(n)$ важи $y^{\varphi(n)} = e = 1$ (jер $\omega(y) \mid \varphi(n)$, ред елем. дели ред групе)
У групи Z ово даје $y^{\varphi(n)} \equiv 1 \pmod n$

$x^{\varphi(n)} - y^{\varphi(n)} = (x-y)(x^{\varphi(n)-1}y + \ldots + xy^{\varphi(n)-1}) = nq(\ldots)$, па $x^{\varphi(n)} \equiv y^{\varphi(n)} \equiv 1 \pmod n$

Мала Фермаова теорема: Ако je p прост, $x \in Z$ ткд. $p \nmid x$, тада $x^{p-1} \equiv 1 \pmod p$

Д: Пошто je p прост $\Rightarrow \varphi(p) = p-1$, па тврђење следи из Ојлерове теореме.

деф. Функција $f: N \to N$ је **мултипликативна** ако за све $m,n \in N$, $NZD(m,n)=1$ важи $f(mn)=f(m)f(n)$

T2: $\varphi(n)$ је мултипликативна.

Д: Нека је $NZD(m,n)=1$.
Јасно, број који је узајамно прост са mn акко је узајамно прост и са m и са n

$$\begin{array}{cccccc}
1 & 2 & 3 & \dots & m-1 & m \\
m+1 & m+2 & m+3 & \dots & 2m-1 & 2m \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
(n-1)m+1 & (n-1)m+2 & (n-1)m+3 & \dots & nm-1 & nm
\end{array}$$

Бројеви у свакој врсти дају остатке $1,2,3,\dots,m-1,0$ по модулу m.
Такође, у i-тој колони сви бројеви дају остатак i при дељењу са m. (у m-тој колони ост. 0)

Како је $NZD(x,m)=1 \iff$ остатак при дељењу x са m је узајамно прост са m,
то су бројеви једне колоне или сви уз. прости са m или ни један није уз. прост са m
↳ ових колона има $\varphi(m)$ ↳ ове су све остале
Сада је довољно одредити колико је од ових бројева уз. просто са n.
Докажимо да су остаци при дељењу са n сваке колоне различити

ппс. Два броја у истој колони, $km+i$ и $lm+i$, дају исти остатак при дељењу са n
$n \mid (km+i)-(lm+i) \Rightarrow n \mid m(k-l) \Rightarrow n \mid k-l$ ↯ $(k-l<n)$

Дакле, бројеви једне колоне дају све остатке при дељењу са n, па је тачно $\varphi(n)$ бројева сваке колоне уз. просто са n

Закључујемо да у свакој од $\varphi(m)$ претходно изабраних колона има по $\varphi(n)$ бројева који су уз. прости и са m и са n, па отуд $\varphi(mn)=\varphi(m)\varphi(n)$.

Последица: За $n=p_1^{\alpha_1}\dots p_k^{\alpha_k}$, где су $p_1<\dots<p_k$ прости, $\alpha_1,\dots,\alpha_k\in N$ важи:

$$\varphi(n)=(p_1^{\alpha_1}-p_1^{\alpha_1-1})\dots(p_k^{\alpha_k}-p^{\alpha_k-1})$$

Д: $\varphi(n)=\varphi(p_1^{\alpha_1}\dots p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}\dots p_{k-1}^{\alpha_{k-1}})\cdot\varphi(p_k^{\alpha_k}) = \dots = \varphi(p_1^{\alpha_1})\cdot\dots\cdot\varphi(p_k^{\alpha_k})$

а јасно $\varphi(p^k)=p^k-\frac{p^k}{p}=p^k-p^{k-1}$ (зато што је број уз. прост са p^k акко није дељиво са p па „бришемо" сваки p-ти)

Напомена: лепши запис: $\varphi(n)=n(1-\frac{1}{p_1})\dots(1-\frac{1}{p_k})$. (само извучемо $p_i^{\alpha_i}$ испред сваке заграде)

12. Класе конјугованости - основне особине и примери.

деф. Нека је G група. Елемент y је **конјугован** елементу x акко $\exists g \in G \quad y = gxg^{-1}$

деф. Уводимо релацију $\sim$ на G са: $\quad x \sim y \iff y$ конјугован елементу x

Напомена: $\sim$ је релација еквиваленције

деф. **Класа конјугованости** од a је класа екв. a у односу на $\sim$. Тада $K_a = \{ gag^{-1} \mid g \in G \}$

T1: 1) $a \in K_a$
2) $K_a = K_b \quad \vee \quad K_a \cap K_b = \emptyset$
3) $\bigcup K_a = G$

Д: K_a је по деф. класа еквиваленције, па су ове особине последице тога.

* Класе конјугованости у комутативним групама: (специјално, у $\mathbb{Z}$ и $\mathbb{Z}_n$)

$$K_a = \{ gag^{-1} \mid g \in G \} = \{ gg^{-1}a \mid g \in G \} = \{ a \}$$

* Класе конјугованости у $D_n = \{ \varepsilon, \rho, \dots, \rho^{n-1}, \sigma, \sigma\rho, \dots \sigma\rho^{n-1} \}$:

Знамо $\rho^n = \varepsilon, \ \sigma^2 = \varepsilon \quad$ и $\quad \rho^i \sigma = \sigma \rho^{n-i} = \sigma\rho^{-i}$

$$* K_{\rho^i} = \{ g\rho^i g^{-1} \mid g \in D_n \} = \{ \rho^j \rho^i \rho^{-j} \mid 0 \le j \le n-1 \} \cup \{ (\sigma\rho^j)\rho^i(\sigma\rho^j)^{-1} \mid 0 \le j \le n-1 \} =$$

$$= \{ \rho^i \} \cup \{ \sigma\rho^j \rho^i (\sigma\rho^j)^{-1} \mid 0 \le j \le n-1 \} = \{ \rho^i \} \cup \{ \sigma\rho^j\rho^i\rho^{-j}\sigma \mid 0 \le j \le n-1 \} = \{ \rho^i \} \cup \{ \sigma\rho^i\sigma \} =$$

$$= \{ \rho^i, \sigma\sigma\rho^{n-i} \} = \{ \rho^i, \rho^{n-i} \}$$

$$* K_{\sigma\rho^i} = \{ g\sigma\rho^i g \mid g \in D_n \} = \{ \rho^j \sigma \rho^i \rho^{n-j} \mid 0 \le j \le n-1 \} \cup \{ \sigma\rho^j \sigma\rho^i (\sigma\rho^j)^{-1} \mid 0 \le j \le n-1 \} =$$

$$= \dots = \{ \sigma\rho^{n+i-2j} \mid 0 \le j \le n-1 \} \cup \{ \sigma\rho^{2j-i} \mid 0 \le j \le n-1 \}$$

$$= \{ \sigma\rho^{i-2j} \mid 0 \le j \le n-1 \} \cup \{ \sigma\rho^{n-i+2j} \mid 0 \le j \le n-1 \}$$

1° $2 \mid n$:
$$K_{\sigma\rho^i} = \begin{cases} \{ \sigma, \sigma\rho^2, \sigma\rho^4, \dots, \sigma\rho^{n-2} \}, & 2 \mid i \\ \{ \sigma\rho, \sigma\rho^3, \sigma\rho^5, \dots, \sigma\rho^{n-1} \}, & 2 \nmid i \end{cases}$$
(ови из уније се поклапају)

2° $2 \nmid n$:
$$K_{\sigma\rho^i} = \{ \sigma, \sigma\rho, \sigma\rho^2, \dots, \sigma\rho^{n-1} \}, \quad \text{за све } 0 \le i \le n-1$$
(ови из уније се не поклапају)

* Класе конјугованости у S_n

Т2: За све $\pi \in S_n$ и циклус $\lceil a_1, \dots, a_k \rfloor \in S_n$ важи:

$$\pi \lceil a_1, \dots, a_k \rfloor \pi^{-1} = \lceil \pi(a_1), \dots, \pi(a_k) \rfloor$$

Д: Нека $a \in \{1, 2, \dots, n\}$, $\sigma = \pi \lceil a_1, \dots, a_k \rfloor \pi^{-1}$, $\tau = \lceil \pi(a_1), \dots, \pi(a_k) \rfloor$ (доказујемо $\sigma = \tau$)

Дискусија у зависности од тога „да ли је a у τ".

1° $a = \pi(a_i)$ за неко $1 \leq i \leq k$

$\tau(a) = \tau(\pi(a_i)) = \pi(a_{i+1})$ и $\tau(\pi(a_k)) = \pi(a_1)$

$\sigma(a) = (\pi \circ \lceil a_1, \dots, a_k \rfloor \circ \pi^{-1})(\pi(a_i))$
$= (\pi \circ \lceil a_1, \dots, a_k \rfloor)(a_i) = \pi(a_{i+1})$ и $\sigma(\pi(a_k)) = \pi(a_1)$

2° $a \notin \{\pi(a_1), \dots \pi(a_k)\}$

$\tau(a) = a$

$\sigma(a) = (\pi \circ \lceil a_1, \dots, a_k \rfloor \circ \pi^{-1})(a) = (\pi \circ \lceil a_1, \dots, a_k \rfloor)(\pi^{-1}(a))$
$= \pi(\lceil a_1, \dots, a_k \rfloor (\pi^{-1}(a)) = \pi(\pi^{-1}(a)) = a$

* Нека је $\sigma \in S_n$ произвољна пермутација са цикл. декомп. $\sigma = \sigma_1 \dots \sigma_t$ (сви дисјунктни)

$$\pi \circ \sigma \circ \pi^{-1} = \pi \circ \sigma_1 \circ \dots \circ \sigma_k \circ \pi^{-1} = \underbrace{\pi \circ \sigma_1 \circ (\pi^{-1}}_{\sigma_1'} \circ \underbrace{\pi) \circ \sigma_2 \circ (\pi^{-1}}_{\sigma_2'} \circ \pi) \circ \dots \circ (\pi^{-1} \circ \underbrace{\pi) \circ \sigma_t \circ \pi^{-1}}_{\sigma_t'} = \sigma_1' \dots \sigma_t'$$

По претходној теореми, σ_i' је циклус исте дужине као σ_i и при томе су сви σ_i', σ_j' дисјунктни.

Дакле, $\pi \sigma \pi^{-1}$ има исту циклусну декомпозицију као σ
А за све π тачно добијамо све пермутације са истом цикл. декомп. као σ. (истом по облику, не букв. истом)

Закључак: K_σ је скуп свих пермутација са истом цикл. декомп. као σ.

14. Центар групе и централизатор скупа.

деф. Нека је G група и $S \subseteq G$, $S \neq \emptyset$.
Тада је **централизатор скупа** S скуп $Z(S) = \{ g \in G \mid (\forall s \in S) \; gs = sg \}$.

T1: $Z(S) \leq G$

Д: * Знамо $e \in Z(S)$ (значи $Z(S) \neq \emptyset$).

* $g_1, g_2 \in Z(S) \Rightarrow \forall s \in S \; g_1 s = s g_1 \wedge g_2 s = s g_2 \overset{g_1^{-1} \cdot \_ \cdot g_1^{-1}}{\Rightarrow} \forall s \in S \; s g_1^{-1} = g_1^{-1} s \wedge g_2 s = s g_2$
Сада је $g_1^{-1} g_2 s = g_1^{-1} s g_2 = s g_1^{-1} g_2$, па $g_1^{-1} g_2 \in Z(S)$.

деф. Скуп $Z(G)$ је **центар групе** G.

T2: 1) $Z(G) \leq G$
2) Центар групе је унија једночланих класа конјугованости.

Д: 1) спец. случај T1 ($S = G$)

2) $x \in Z(G) \Leftrightarrow \forall g \in G \; gx = xg \Leftrightarrow \forall g \in G \; gxg^{-1} = x \Leftrightarrow K_x = \{x\}$.

T3 (Једначина класа): Нека је G коначна група и нека су $n_1, \dots, n_s$ кардиналности разних класа конјугованости у G које имају бар 2 елемента.

Тада: $|G| = n_1 + n_2 + \dots + n_s + |Z(G)|$.

Д: Нека су $K_1, \dots, K_s$ класе конјуг. ткд. $|K_i| = n_i$, а једночлане класе су $K_{s+1}, \dots, K_t$.
По претходном: $Z(G) = K_{s+1} \cup \dots \cup K_t$. Такође знамо да све класе чине разбијање G.

$$|G| = |K_1| + \dots + |K_s| + |K_{s+1}| + \dots + |K_t| = n_1 + \dots + n_s + 1 + \dots + 1 = n_1 + \dots + n_s + Z(G).$$

T4: Нека је G коначна група и $a \in G$. Тада: $|K_a| = [G : Z(a)] = |G/Z(a)|$.

Д: Довољно је доказати да је $f: K_a \to G/Z(a)$, $f(gag^{-1}) = gZ(a)$, бијекција.
$\hookrightarrow Z(a) = \{g \in G \mid ga = ag\}$

* докажимо добру дефинисаност:

$gag^{-1} = hah^{-1} \Leftrightarrow h^{-1}ga = ah^{-1}g \Leftrightarrow h^{-1}g \in Z(a) \Leftrightarrow gZ(a) = hZ(a)$
$\Leftrightarrow f(gag^{-1}) = f(hah^{-1})$

* докажимо 1-1: већ доказано (читамо у другом смеру)

* докажимо на: тривијално (по дефиницији пресликавања f)

T5: Свака група G реда p^n (p - прост, $n \in \mathbb{N}$) има нетривијални центар. $(Z(G) \neq \{e\})$

Д: По једначини класа (Т3): $p^n = |G| = \sum_{i=1}^{s} n_i + |Z(G)|$ $(*)$ $\left(\begin{array}{l} K_1, \dots, K_s \text{ класе конј.} \\ \text{у } G \text{ са бар 2 елем.} \end{array}\right)$

ппс. $|Z(G)| = 1$

За све $i \leq s$, постоји неко $g_i \in G$ чија је класа конј. баш K_i.

Важи: $n_i = |K_i| = |K_{g_i}| = [G : Z(g_i)] \overset{\text{Лагранж}}{=} \dfrac{|G|}{|Z(g_i)|} = \dfrac{p^n}{|Z(g_i)|} \overset{n_i > 1}{>} 1$

Дакле, $n_i = p^{k_i}$, $k_i > 0$ ($k_i \neq 0$, јер $n_i > 1$) (мора бити степен p)

Заменом у $(*)$: $p^n = \sum p^{k_i} + 1$ $\lightning$ $\left(\begin{array}{l} \text{лева стр. дељива са } p, \\ \text{док десна није} \end{array}\right)$

T6: Ако је p прост број, тада је свака група реда p^2 изоморфна са $\mathbb{Z}_p \times \mathbb{Z}_p$ или $\mathbb{Z}_{p^2}$.

Д: Нека је G група реда p^2.

1° у G постоји елемент реда p^2: онда је G циклична $\overset{\boxed{7}\text{T1}}{\Rightarrow}$ $G \cong \mathbb{Z}_{p^2}$

2° у G не постоји елемент реда p^2: по претх. теореми $\Rightarrow \exists h \in Z(G) \setminus \{e\}$.

Тада је $\omega(h) = p$ $\left(\begin{array}{l} \text{јер } \omega(h) \mid |G| = p^2 \quad \leftarrow h \in G \\ \text{а } \omega(h) \neq 1, \text{ јер } h \neq e \\ \text{и } \omega(h) < p^2 \end{array}\right)$

Нека је $H = \langle h \rangle$, тада $|H| = \omega(h) = p$.

Нека је $k \in G \setminus \langle h \rangle$, тада $\omega(k) = p$. $\left(\begin{array}{l} \text{јер } H \leq G \Rightarrow e \in H \Rightarrow k \neq e \Rightarrow \omega(k) \neq 1 \\ \text{а знамо да у } G \text{ нема елем. реда } p^2 \end{array}\right)$. Узмимо $K = \langle k \rangle$, тада $|K| = p$.

По $\boxed{8}$Т5, да би $G \cong H \times K$, довољно је доказати да је G дир. ун. пр. H и K.

Доказујемо три својства из деф. дир. унутр. производа.

* докажимо $H \cap K = \{e\}$:

ппс. $\overset{(|H \cap K| \,\mid\, |H|)}{|H \cap K| = p}$ $\Rightarrow H = H \cap K = K$ $\lightning$ $(x \in K \Rightarrow x \notin H)$

* докажимо $G = HK$:

Важи $HK = \{h^r k^s \mid 0 \leq r, s < p\}$. Докажимо да међу овим елем. нема истих.

ппс. $h^r k^s = h^t k^u$ и нпр. $r \geq t$. Тада $H \ni h^{r-t} = k^{u-s} \in K$, а $H \cap K = \{e\}$

$\Rightarrow r = t,\ s = u$

Дакле у HK, као и у G, има p^2 различитих елемената, па је $G = HK$.

* докажимо $\forall h' \in H, k' \in K$ $h'k' = k'h'$:

Знамо $h' = h^s$, $0 \leq s < p$. Како $h \in Z(G) \Rightarrow \forall g \in G,\ hg = gh$, па $hk' = k'h$

Сада је: $h'k' = h^s k' = h^{s-1} h k' = \underbrace{h^{s-1} k'}\, h = \dots = k' h^s = k' h'$

Коначно, пошто сада знамо $G \cong H \times K$, а $H = \langle h \rangle \overset{\boxed{7}\text{T1}}{\cong} \mathbb{Z}_p$, $K = \langle k \rangle \overset{\boxed{7}\text{T1}}{\cong} \mathbb{Z}_p$ $\overset{\boxed{8}\text{T4} + \boxed{1}\text{T2}}{\Longrightarrow}$ $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

13. Нормалне подгрупе и количничке групе.

деф. Нека је G група и $H \leq G$. Кажемо да је H **нормална подгрупа** од G, у ознаци $H \triangleleft G$, ако је H унија неколико класа конјугованости.

Напомена: ова деф. се може записати и као: $H \triangleleft G \Leftrightarrow H \leq G$ и $(\forall a)\ a \in H \Rightarrow K_a \subseteq H$.

T1: Нека је $H \leq G$. Следећи услови су еквивалентни:

(1) $H \triangleleft G$
(2) $(\forall g \in G) \quad gHg^{-1} \subseteq H$
(3) $(\forall g \in G) \quad gH = Hg$.

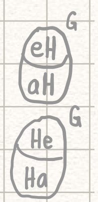
Д: $(1 \Rightarrow 2)$ $h \in H \Rightarrow K_h \subseteq H \Rightarrow (\forall g \in G)\ ghg^{-1} \in H \Rightarrow (\forall g \in G)\ gHg^{-1} \subseteq H$

$(2 \Rightarrow 3)$
$$\left.\begin{array}{l} gHg^{-1} \subseteq H \Rightarrow gH \subseteq Hg \\ g^{-1}H(g^{-1})^{-1} \subseteq H \Rightarrow Hg \subseteq gH \end{array}\right\} \Rightarrow gH = Hg$$

$(3 \Rightarrow 1)$ Нека $ghg^{-1} \in K_h$. Како $gh \in gH = Hg \Rightarrow \exists h'\ gh = h'g \Rightarrow ghg^{-1} = h' \in H \Rightarrow K_h \subseteq H$

T2: Свака подгрупа индекса 2 је нормална.

Д: Нека је $H \leq G$ и $[G:H] = 2$.
Тада је $|G/H| = 2$, па је $G/H = \{H, aH\}$, за неко $a \in G$. Како $aH \neq H \Rightarrow a \notin H$
Важи и $|G_D(H)| = 2$, па је $G_D(H) = \{H, Ha\}$ (јер $a \notin H$, па $H \neq Ha$)
исто a
Пошто оба чине разбијање G (слика), видимо да је $aH = Ha$.



По T1 под (3), довољно је доказати да за све $g \in G$ важи $gH = Hg$.

1° $g \in H \Rightarrow gH = H = Hg$
2° $g \notin H \Rightarrow \left.\begin{cases} gH \neq H \Rightarrow gH = aH \\ Hg \neq H \Rightarrow Hg = Ha \end{cases}\right\} \Rightarrow gH = aH = Ha = Hg$

Закључујемо: $H \triangleleft G$.

T3: $Z(G) \triangleleft G$

Д: Последица $\boxed{14}$ T2 1) + 2) (добијамо букв. дефиницију $\triangleleft$).

T4:
1) $K \leq H \leq G \Rightarrow K \leq G$
2) $K \triangleleft H \triangleleft G \not\Rightarrow K \triangleleft G$ ($\triangleleft$ није транзитивна)
3) $K \leq H \leq G,\ K \triangleleft G \Rightarrow K \triangleleft H$. $\underbrace{K \leq H \leq G}_{\triangleleft} \Rightarrow K \triangleleft H$

Д:
1) тривијално
2) нпр. $G = D_4$; $H = \{\varepsilon, \rho^2, \sigma, \sigma\rho^2\}$; $K = \{\varepsilon, \sigma\}$ $\left(\begin{array}{l}[G:H]=2\\ [H:K]=2\end{array},\ \text{али } \sigma \in K, \text{ а } K_\sigma \overset{\boxed{12}}{=} \{\sigma, \sigma\rho^2\} \nsubseteq K\right)$
3) тривијално

Нека је $H \triangleleft G$. Посматрамо релацију: $a \sim_H b \iff a^{-1}b \in H$ (ово смо за $\leqslant$ већ увели у 5. питању)

T5: $\sim_H$ је конгруенција на G.

Д: У 5. питању, Т1, доказали смо да је $\sim_H$ рел. екв.
па је довољно још доказати да: $a_1 \sim_H b_1,\ a_2 \sim_H b_2 \Rightarrow a_1a_2 \sim_H b_1b_2$ (пошто је G група па има бин. операцију)
тј. $a_1^{-1}b_1 \in H,\ a_2^{-1}b \in H \Rightarrow (a_1a_2)^{-1}b_1b_2 \in H$

$$(a_1a_2)^{-1}b_1b_2 = a_2^{-1}\underbrace{a_1^{-1}b_1}_{\in H}b_2 = \underbrace{a_2^{-1}\underbrace{a_1^{-1}b_1}_{\in H}a_2}_{\in H}\underbrace{a_2^{-1}b_2}_{\in H} \in H \Longrightarrow (a_1a_2)^{-1}b_1b_2 \in H$$

(јер $H \triangleleft G \overset{(2)}{\iff} (\forall g \in G)\ gHg^{-1} \subseteq H$)

T6: Ако $a \sim_H b$, тада је и $a^{-1} \sim_H b^{-1}$.

Д: $a^{-1}b \in H \overset{H \leq G}{\Longrightarrow} (a^{-1}b)^{-1} = b^{-1}a \in H \Rightarrow \underbrace{a\underbrace{b^{-1}a}_{\in H}a^{-1}}_{\in H} = ab^{-1} \in H$ (опет по (2))

Напомена: $e \sim_H e$

Класе еквиваленције у односу на $\sim_H$ су леви косети подгрупе H, тј. aH.
Дефинишемо операције $\cdot,\ ^{-1}$ и e на скупу G/H:

$aH = bH \iff a \sim_H b$

* $aH \cdot bH = (ab)H$, јер смо још у 1 увели $\tilde{\omega}_i(C_{a_1}, \dots, C_{a_k}) = C_{\omega_i(a_1,\dots,a_k)}$ (добро деф. по Т5)
* $(aH)^{-1} = a^{-1}H$ (добро деф. по Т6)
* $eH = H$ (константа)

T7: $(G/H, \cdot, ^{-1}, eH)$ је група.

Д: * асоцијативност: $(aH \cdot bH)\cdot cH = (ab)H \cdot cH = (abc)H$
$aH \cdot (bH \cdot cH) = aH \cdot (bc)H = (abc)H$

* неутрал: $aH \cdot eH = (ae)H = aH$
$eH \cdot aH = (ea)H = aH$

* инверз: $aH \cdot (a^{-1})H = (aa^{-1})H = eH$
$(a^{-1})H \cdot aH = (a^{-1}a)H = eH$

деф. G/H називамо **количничка група**.

Напомена: $K, H \triangleleft G$, $K \cong H \not\Rightarrow G/K \cong G/H$.

Д: нпр. $G = \mathbb{Z}$; $K = \mathbb{Z}$; $H = \langle 2 \rangle = 2\mathbb{Z}$ $\left(\mathbb{Z} \cong 2\mathbb{Z},\ \begin{matrix}|G/K| = |\mathbb{Z}/\mathbb{Z}| = 1 \\ |G/H| = |\mathbb{Z}/2\mathbb{Z}| = 2\end{matrix}\right\} \Rightarrow G/K \not\cong G/H\right)$

$\boxed{15.}$ Комутаторска подгрупа и Абелизација групе.

деф. Нека је G група и $x, y \in G$. Комутатор елемената x и y је $[x,y] = x^{-1}y^{-1}xy$.

Напомена: $[x,y] = e \iff x^{-1}y^{-1}xy = e \iff xy = yx$.

деф. Нека је G група. Комутаторска подгрупа од G је: $G' = \langle [x,y] \mid x,y \in G \rangle$.
Каже се и извод групе G.

Т1: 1) $[x,y]^{-1} = [y,x]$

2) $g[x,y]g^{-1} = [gxg^{-1}, gyg^{-1}]$.

Д: 1) $[x,y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx = [y,x]$.

2) $g[x,y]g^{-1} = gx^{-1}y^{-1}xyg = gx^{-1}g^{-1}gy^{-1}g^{-1}gxg^{-1}gyg^{-1} = (gxg^{-1})^{-1}(gyg^{-1})^{-1}gxg^{-1}gyg^{-1}$
$= [gxg^{-1}, gyg^{-1}]$.

Т2: Нека је G група.

1) $G' \triangleleft G$
2) Нека је $H \triangleleft G$. Тада: G/H је комутативна акко $G' \leq H$.
Специјално, G/G' је комутативна.

Д: 1) По Т1 под 1), G' је скуп елемената облика $[x_1,y_1]\cdot\ldots\cdot[x_k,y_k]$, где $k \in \mathbb{N}$, $x_i, y_i \in G$.
По деф. $G' \leq G$, па је довољно доказати да за $a \in G'$, $g \in G$ важи $gag^{-1} \in G'$.
(услов (2))

Знамо $a = [x_1,y_1]\ldots[x_k,y_k] \Rightarrow gag^{-1} = g[x_1,y_1]\ldots[x_k,y_k]g^{-1} = g[x_1,y_1]g^{-1}g\ldots g^{-1}g[x_k,y_k]g^{-1}$

$\overset{2)}{=} [gx_1g^{-1}, gy_1g^{-1}]\ldots[gx_kg^{-1}, gy_kg^{-1}] \in G'$.

2) $(aH)\cdot(bH) = (bH)\cdot(aH) \iff (ab)H = (ba)H \iff (ab)^{-1}ba \in H$
$\iff b^{-1}a^{-1}ba \in H \iff [b,a] \in H$

Дакле, G/H је комутативна акко $[b,a] \in H$, за све $a,b \in G$
акко $G' = \langle [b,a] \mid b,a \in G \rangle \leq H$.

деф. Нека je G група. Абелизација групе G je група $G^{Ab} := G/G'$.

Т3: Ако je $G \cong H$, тада $G^{Ab} \cong H^{Ab}$.

Д: Нека je $f: G \to H$ изоморфизам.
Уочимо: $f([x,y]) = f(x^{-1}y^{-1}xy) = f(x)^{-1} f(y)^{-1} f(x) f(y) = [f(x), f(y)]$.

Докажимо да je $F: G^{Ab} \to H^{Ab}$, $F(gG') = f(g)H'$ изоморфизам.

* докажимо добру дефинисаност:

$$g_1 G' = g_2 G' \iff g_1^{-1} g_2 \in G' \iff g_1^{-1} g_2 = [x_1, y_1] \dots [x_k, y_k]$$

$$\iff f(g_1^{-1} g_2) = f([x_1, y_1] \dots [x_k, y_k])$$

$$\iff f(g_1)^{-1} f(g_2) = f([x_1, y_1]) \dots f([x_k, y_k])$$

$$\iff f(g_1)^{-1} f(g_2) = [f(x_1), f(y_1)] \dots [f(x_k), f(y_k)] \in H'$$

$$\iff f(g_1) H' = f(g_2) H' \iff F(g_1 G') = F(g_2 G')$$

* докажимо 1-1: већ доказано (читамо у другом смеру)

* докажимо на: пошто je f на, онда je и F на.

* докажимо да je хомоморфизам:

$$F((g_1 G')(g_2 G')) = F((g_1 g_2) G') = f(g_1 g_2) H' = (f(g_1) f(g_2)) H' =$$

$$= (f(g_1) H')(f(g_2) H') = F(g_1 G') F(g_2 G')$$

Дакле, F je изоморфизам, па je $G^{Ab} \cong H^{Ab}$.

$\boxed{16.}$ Кошијева теорема.

Кошијева теорема: Нека је G коначна група и p прост број који дели $|G|$. Тада у G постоји елемент реда p.

Д: Потпуном индукцијом по $|G| = n$.

(БИ) $n = p$: Знамо да је $G \cong \mathbb{Z}_p$ (7. питање последица), па је циклична.
За a ткд. $\langle a \rangle = G$ важи $\omega(a) = |G| = p$.

(ИК) $<n \to n$: Гледамо два случаја:

1° G – комутативна: Нека $a \in G \setminus \{e\}$.

1°_1 $p \mid \omega(a)$: $\omega\left(a^{\frac{\omega(a)}{p}}\right) = \dfrac{\omega(a)}{NZD\left(\omega(a), \frac{\omega(a)}{p}\right)} = \dfrac{\omega(a)}{\frac{\omega(a)}{p}} = p$.

1°_2 $p \nmid \omega(a)$: Посматрамо $G/\langle a \rangle$ (знамо $\langle a \rangle \trianglelefteq G$, јер свака подгрупа комут. групе је нормална јер $K_a = \{a\}$ $\boxed{12}$)

Важи $|G/\langle a \rangle| \overset{\boxed{5}}{=} \dfrac{|G|}{|\langle a \rangle|} = \dfrac{|G|}{\omega(a)}$
Пошто $p \nmid \omega(a)$, важи $p \mid |G/\langle a \rangle|$ и $|G/\langle a \rangle| < n$.
По (ИХ) у $G/\langle a \rangle$ постоји елемент реда p, нпр. $b\langle a \rangle$

Означимо $\omega(b) = t$. Важи: $(b\langle a \rangle)^t = b^t \langle a \rangle = e\langle a \rangle = \langle a \rangle$.
Због тога, $\omega(b\langle a \rangle) \mid t$, па $p \mid t$, тј. $p \mid \omega(b)$.
Тиме смо 1°_2 свели на 1°_1, па га завршавамо на исти начин.

2° G – није комутативна: Тада $G \neq Z(G)$, тј. $|Z(G)| < |G| = n$.

2°_1 $p \mid |Z(G)|$: по (ИХ) у $Z(G)$ постоји елем. реда p, а он је и у G.

2°_2 $p \nmid |Z(G)|$: по једначини класа: $|G| = \sum_{i=1}^{s} n_i + |Z(G)|$.

Како $p \mid |G|$, следи да постоји i ткд. $p \nmid |K_i|$, нпр. $K_i = K_{a_i}$.

Тада: $n_i = |K_{a_i}| \overset{\boxed{14}\,T4}{=} [G : Z(a_i)] = \dfrac{|G|}{|Z(a_i)|} \overset{(n_i > 1)}{>} 1$, па зато $p \mid |Z(a_i)|$.
Takође, одавде видимо $|Z(a_i)| < |G|$.
По (ИХ), у $|Z(a_i)|$ постоји елем. реда p, а он је и у G.

T1: Нека је $p>2$ прост.
Тада је свака група реда $2p$ изоморфна са D_p или $\mathbb{Z}_{2p}$.

Д: Нека је G група ткд. $|G| = 2p$

1° у G постоји елем реда $2p$: онда је G циклична $\overset{7\,T1}{\Rightarrow}$ $G \cong \mathbb{Z}_{2p}$

2° у G не постоји елем реда $2p$: тада су сви елементи реда $1, 2$ или p.

По Кошију: $\exists a, b \in G: \ \omega(a) = p, \ \omega(b) = 2$
Важи $\langle a \rangle = \{e, a, a^2, \dots, a^{p-1}\}$ и $b\langle a \rangle = \{b, ba, \dots, ba^{p-1}\}$.
Пошто $b \notin \langle a \rangle$ (у $\langle a \rangle$ су сви реда 1 или p), то је $G = \langle a \rangle \cup b\langle a \rangle = \{e, a, \dots, a^{p-1}, b, ba, \dots, ba^{p-1}\}$. ($|G| = 2p$, а сви су различити)

Посматрајмо ab: $\omega(ab) \in \{1, 2, p, 2p\}$.

2°_1 $\omega(ab) = 1$: $ab = e \Rightarrow b = a^{-1} \Rightarrow b \in \langle a \rangle$ ↯

2°_2 $\omega(ab) = 2p$: ↯ (у G не постоји елем. реда $2p$)

2°_3 $\omega(ab) = p$: $(ab)^p = e$

$[G : \langle a \rangle] = 2 \overset{13\,T2}{\Rightarrow} \langle a \rangle \triangleleft G$ и очигледно $|G/\langle a \rangle| = 2$, па $\omega(ab\langle a \rangle) \in \{1, 2\}$.
Такође, важи и $(ab\langle a \rangle)^p = (ab)^p \langle a \rangle = e\langle a \rangle = \langle a \rangle \overset{\omega(ab\langle a \rangle) \mid p}{\Rightarrow} \omega(ab\langle a \rangle) = 1$
Важи: $ab\langle a \rangle = \langle a \rangle \Leftrightarrow ab \in \langle a \rangle \Rightarrow ab = a^k \Rightarrow b = a^{k-1} \in \langle a \rangle$ ↯

Закључујемо да мора бити $\omega(ab) = 2 \Rightarrow abab = e \overset{\substack{\omega(a)=p \\ \omega(b)=2}}{\Rightarrow} ab = ba^{p-1}$

Коначно, $f: G \to D_p$, $f(b^j a^i) = \sigma^j \rho^i$ је изоморфизам.

17. Аутоморфизми група.

деф. Нека је G група. Тада је: $Aut(G) = \{ f: G \to G \mid f$ је изоморфизам$\}$.
Чланови тог скупа су аутоморфизми.

T1: $(Aut(G), \circ)$ је група.

Д: на стандардан начин.

деф. Унутрашњи аутоморфизам групе G је свако пресликавање $u_g: G \to G$, $u_g(x) = gxg^{-1}$. $(g \in G)$

T2: u_g заиста јесте аутоморфизам.

Д: * хомоморфизам: $u_g(xy) = g(xy)g^{-1} = gxg^{-1}gyg^{-1} = u_g(x)\, u_g(y)$

* бијекција: * 1-1: $u_g(x) = u_g(y) \Rightarrow gxg^{-1} = gyg^{-1} \Rightarrow x = y$
* на: $u_g(g^{-1}yg) = gg^{-1}ygg^{-1} = y \in G$

деф. Скуп свих ун. аутоморфизама од G означавамо $Inn(G) = \{ u_g \mid g \in G \}$.

T3: $Inn(G) \triangleleft Aut(G)$

Д: * Докажимо $Inn(G) \leq Aut(G)$.

* $Inn(G) \neq \emptyset$: зато што $u_e(x) = exe^{-1} = x$, па $id(x) \in Inn(G)$.

* $u_g^{-1} u_h \in Inn(G)$: важи: $u_g^{-1}(u_g(x)) = id(x) = x$
$u_g^{-1}(u_g(x)) = u_g^{-1}(\underbrace{gxg^{-1}}_{y})$, тј. $u_g^{-1}(y) = x = g^{-1}yg = g^{-1}y(g^{-1})^{-1}$

Закључујемо: $u_g^{-1}(y) = u_{g^{-1}}(y)$, $y \in G$

Дакле: $u_g^{-1} u_h(x) = u_{g^{-1}} u_h(x) = g^{-1}hxh^{-1}g = (g^{-1}h)x(g^{-1}h)^{-1}$
Одавде, видимо $u_g^{-1} u_h = u_{g^{-1}h} \in Inn(G)$

* Докажимо услов (2) - $f\, Inn(G)\, f^{-1} \subseteq Inn(G)$, за све $f \in Aut(G)$:

Нека је $g \in G$. Тада: $(f \circ u_g \circ f^{-1})(x) = f(u_g(f^{-1}(x))) = f(g f^{-1}(x) g^{-1}) = f(g)\, f(f^{-1}(x))\, f(g^{-1})$

Дакле: $(f \circ u_g \circ f^{-1})(x) = f(g)\, x\, f(g)^{-1} = u_{f(g)}(x) \in Inn(G)$.

T4: $\mathrm{Inn}(G) \cong G/Z(G)$.

Д: Докажимо да је $f: G/Z(G) \to \mathrm{Inn}(G)$, $f(gZ(G)) = u_g$ изоморфизам.

* докажимо добру дефинисаност:

$$g_1 Z(G) = g_2 Z(G) \Leftrightarrow g_1^{-1} g_2 \in Z(G) \overset{(\forall x \in G)}{\Leftrightarrow} g_1^{-1} g_2 x = x g_1^{-1} g_2 \overset{(\forall x \in G)}{\Leftrightarrow} g_2 x g_2^{-1} = g_1 x g_1^{-1}$$
$$\Leftrightarrow u_{g_1}(x) = u_{g_2}(x), \ (\forall x \in G) \Leftrightarrow u_{g_1} = u_{g_2}$$

* докажимо 1-1: већ доказано (читамо у другом смеру)
* докажимо на: тривијално
* докажимо да је хомоморфизам:

$$f\left(g_1 Z(G))(g_2 Z(G))\right) = f(g_1 g_2 Z(G)) = g_1 g_2 x g_2^{-1} g_1^{-1} = u_{g_1} u_{g_2} = f(g_1 Z(G)) f(g_2 Z(G))$$

T5: Ако је $\mathrm{Inn}(G)$ / $G/Z(G)$ циклична група, онда је $\mathrm{Inn}(G) = \{id_G\}$ / $G/Z(G) = \{Z(G)\}$.

Д: По претходном, пошто $\mathrm{Inn}(G) \cong G/Z(G)$, да би било $\mathrm{Inn}(G) = \{id_G\}$, довољно је доказати $G/Z(G) = \{Z(G)\}$, тј. $G = Z(G)$, тј. да је G комутативна.

Нека је $G/Z(G) = \langle aZ(G) \rangle$, $a \in G$.
Тада за свако $g \in G$, важи: $gZ(G) = (aZ(G))^k = a^k Z(G)$, $k \in \mathbb{Z} \overset{a^k \sim g}{\Longrightarrow} a^{-k} g \in Z(G)$
и означимо $a^{-k} g = x \in G$, тј. $g = a^k x$.

Нека су $g, h \in G$. За њих постоје $k, l \in \mathbb{Z}$ и $x, y \in Z(G)$ ткд. $g = a^k x$, $h = a^l y$.

$$gh = a^k x a^l y \overset{x \in Z(G)}{=} a^k a^l y x = a^{k+l} y x = a^l a^k y x \overset{y \in Z(G)}{=} a^l y a^k x = hg,$$ па је G комутативна.

T6: $\mathrm{Aut}(\mathbb{Z}_n) \cong \Phi(n)$

Д: * Доказујемо да је $F: \mathrm{Aut}(\mathbb{Z}_n) \to \Phi(n)$, $F(f) = f(1)$ изоморфизам.
Ако означимо $f(1) = a$, да би F било добро деф., морамо доказати да $a \in \Phi(n)$.
Приметимо: $f(k) = f(1 +_n \dots +_n 1) = f(1) +_n \dots +_n f(1) = a +_n \dots +_n a = k \cdot_n a$, дакле $f(k) = k \cdot_n a$, за све $k \in \mathbb{Z}_n$.

* Сада гледамо $\overset{\text{„неко друго f"}}{f}: \mathbb{Z}_n \to \mathbb{Z}_n$, $f(k) = k \cdot_n f(1)$, тј. $f(k) = k \cdot_n a$ (не знамо ништа више)
Лако се проверава да је овако уведено f хомоморфизам за свако $a \in \mathbb{Z}_n$,
па нас занима какво a мора бити да би f било и бијекција. (самим тим аутоморфизам)
Докажимо: f је бијекција $\Leftrightarrow$ $a \in \Phi(n)$.

($\Rightarrow$) ппс. $f(k) = k \cdot_n a$ – бијекција и $NZD(a,n) = d > 1$. Тада је $\frac{n}{d} \cdot_n a$ остатак $\frac{n}{d} \cdot a \pmod n$.
Како $d \mid a$, овај остатак је 0, па је $f(\frac{n}{d}) = 0 = f(0)$, па f није 1-1 ↯

($\Leftarrow$) $a \in \Phi(n)$: Знамо да постоји $b \in \Phi(n)$ ткд. $b \cdot_n a = 1$ (инверз)
$\Rightarrow \forall c \in \mathbb{Z}_n \ f(c \cdot_n b) = (c \cdot_n b) \cdot_n a = c \cdot_n (b \cdot_n a) = c \Rightarrow f$ је на $\overset{\text{(домен и кодомен исте кардиналности)}}{\Longrightarrow} f$ је бијекција

Дакле, $f \in \mathrm{Aut}\,\mathbb{Z}_n \Leftrightarrow f(1) = a \in \Phi(n)$, па је почетно f добро деф. и бијекција + лако се доказује да је хомоморфизам

T7: Ако је $G \cong H$, тада је $Aut(G) \cong Aut(H)$.

Д: Нека је $\varphi: G \to H$ изоморфизам и $f \in Aut(G)$. Дефинишемо

Докажимо да је $F: Aut(G) \to Aut(H)$, $F(f) = \varphi \circ f \circ \varphi^{-1}$

* докажимо добру дефинисаност: $\varphi \circ f \circ \varphi^{-1}$ јесте аутоморфизам.
* докажимо да је бијекција: као композиција бијекција.
* докажимо да је хомоморфизам:

$$F(f_1 \circ f_2) = \varphi \circ f_1 \circ f_2 \circ \varphi^{-1} = \varphi \circ f_1 \circ \varphi^{-1} \circ \varphi \circ f_2 \circ \varphi^{-1} = F(f_1)\, F(f_2).$$

T8: Нека су G, H групе ткд. $|G| = m$, $|H| = n$, $NZD(m,n) = 1$. Тада: $Aut(G \times H) \cong Aut(G) \times Aut(H)$.

Д: Нека је $f: G \times H \to G \times H$ аутоморфизам.
Циљ је да покажемо да постоје $\varphi \in Aut(G)$, $\theta \in Aut(H)$, ткд. $f(g,h) = (\varphi(g), \theta(h))$.

* Докажимо да постоје такви хомоморфизми φ, θ.

Почнимо прво од: $f(g,e) = (\varphi(g), \psi(g))$, где знамо само $\varphi: G \to G$, $\psi: G \to H$.
Докажимо да φ, ψ морају бити хомоморфизми:

$$f((g_1,e)(g_2,e)) = f(g_1 g_2, e) = (\varphi(g_1 g_2), \psi(g_1 g_2)).$$

$$\overset{f\text{-хомоморфизам}}{\|}$$

$$f(g_1,e) \cdot f(g_2,e) = (\varphi(g_1), \psi(g_1)) \cdot (\varphi(g_2), \psi(g_2)) = (\varphi(g_1) \cdot \varphi(g_2), \psi(g_1) \cdot \psi(g_2))$$

Даље, како је $|G| = m \Rightarrow \forall g \in G,\ g^m = e \Rightarrow (g,e)^m = (g^m, e^m) = (\overset{G}{\underset{\in}{e}}, \overset{H}{\underset{\in}{e}})$.
$(e,e) = f(e,e) = f((g,e))^m = (\varphi(g), \psi(g))^m = (\varphi(g)^m, \psi(g)^m) = (e, \psi(g)^m) \Rightarrow \psi(g)^m = e$.
Одавде $\omega(\psi(g)) \mid m$, а по посл. $\boxed{6}$T1: $\omega(\psi(g)) \mid n \xRightarrow[NZD(m,n)=1]{} \omega(\psi(g)) = 1 \Rightarrow \psi(g) = e$.

Дакле, $f(g,e) = (\varphi(g), e)$ за одређени хомоморфизам $\varphi: G \to G$.

Аналогно, $f(e,h) = (e, \theta(h))$ за одређени хомоморфизам $\theta: H \to H$.

па важи: $f(g,h) = f((g,e),(e,h)) = f(g,e)\, f(e,h) = (\varphi(g), e) \cdot (e, \theta(h)) \Rightarrow f(g,h) = (\varphi(g), \theta(h))$.
(*) (φ, θ - јединств.)

* Докажимо да су φ, θ бијекције (самим тим и аутоморфизми) (већ смо доказали да су хомоморф. па ће онда бити и аутоморфизми)

  * 1-1: $\varphi(g_1) = \varphi(g_2) \Rightarrow (\varphi(g_1), e) = (\varphi(g_2), e) \Rightarrow f(g_1, e) = f(g_2, e) \xRightarrow{f\text{ - }1\text{-}1} g_1 = g_2$
  * на: пошто је f на, онда је и φ на.

Аналогно и за θ.

Сада знамо $f(g,h) = (\varphi(g), \theta(h))$, где $\varphi \in Aut(G)$, $\theta \in Aut(H)$

* Важи и обрнуто: за $\varphi \in Aut(G)$, $\theta \in Aut(H)$, ф-ја $f(g,h) = (\varphi(g), \theta(h))$ је аутоморфизам $G \times H$.
(**)

Дакле, ф-ја $F: \mathrm{Aut}(G\times H) \to \mathrm{Aut}(G)\times \mathrm{Aut}(H)$, $F(f) = (\varphi, \theta)$ је добро деф. и бијекција
$\uparrow \forall f \exists! \varphi, \theta$ $\uparrow$ 1-1 (*) на (**)

Докажимо и да је хомоморфизам:

Пошто: $(\underbrace{f_1 \circ f_2}_{\mathrm{Aut}(G\times H)})(g,h) = f_1(f_2(g,h)) = (\varphi_1(\varphi_2(g)), \theta_1(\theta_2(h))) = ((\varphi_1\circ\varphi_2)(g), (\theta_1\circ\theta_2)(h))$

важи: $F(f_1\circ f_2) = (\varphi_1\circ\varphi_2, \theta_1\circ\theta_2) = (\varphi_1,\theta_1)\cdot(\varphi_2,\theta_2) = F(f_1)\cdot F(f_2)$

Одавде, F је изоморфизам, па $\mathrm{Aut}(G\times H) \cong \mathrm{Aut}(G)\times\mathrm{Aut}(H)$.

Последица: Ако је $NZD(n,m)=1$, тада је $\varphi(mn) = \varphi(m)\varphi(n)$. (Ојлерова функција)

Д: Напомена: ово смо већ доказали ($\boxed{11}$ T2), али ово је други начин.

Пошто $NZD(n,m)=1 \xRightarrow{\boxed{8}\text{T3 послед.}} \mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$,

$$\xRightarrow{T7} \mathrm{Aut}(\mathbb{Z}_{nm}) \cong \mathrm{Aut}(\mathbb{Z}_n\times\mathbb{Z}_m) \overset{T8}{\cong} \mathrm{Aut}(\mathbb{Z}_n)\times\mathrm{Aut}(\mathbb{Z}_m)$$

$$\mathrm{Aut}(\mathbb{Z}_{nm}) \overset{T6}{\cong} \Phi(nm), \qquad \mathrm{Aut}(\mathbb{Z}_n)\times\mathrm{Aut}(\mathbb{Z}_m) \overset{T6 + \boxed{8}T4}{\cong} \Phi(n)\times\Phi(m)$$

Дакле: $\varphi(nm) = |\Phi(nm)| = |\Phi(n)\times\Phi(m)| = |\Phi(n)|\cdot|\Phi(m)| = \varphi(n)\varphi(m)$.

18. Теореме о факторизацији, о изоморфизму и о факторијелу.

деф. Нека је $H \triangleleft G$. Тада је $\pi: G \to G/H$, $\pi(g) = gH$ природна пројекција. (То смо већ увели у 1. питању. Тамо смо доказали и да је π епиморфизам.)

деф. Нека је $f: G \to H$ хомоморфизам. $Ker(f) = \{a \in G \mid f(a) = e\} \leq G$, $Im(f) = \{f(a) \mid a \in G\} \leq H$

T1: Нека је $f: G \to H$ хомоморфизам. Тада је: 1) $Ker(f) \triangleleft G$ 2) $Im(f) \leq H$.

Д: 1) * докажимо $Ker(f) \leq G$:

* $Ker(f) \neq \emptyset$: зато што $f(\overset{G}{e}) = \overset{H}{e}$.
* Нека је $a, b \in Ker(f)$. Тада: $f(a) = e$, $f(b) = e$ $\Rightarrow$ $f(a^{-1}b) = f(a)^{-1} f(b) = e$ $\Rightarrow$ $a^{-1}b \in Ker(f)$.

* сада докажимо $Ker(f) \triangleleft G$:

Довољно је доказати: $g\, Ker(f)\, g^{-1} \subseteq Ker(f)$

$h \in Ker(f) \Rightarrow f(h) = e$

$f(ghg^{-1}) = f(g) f(h) f(g^{-1}) = f(g)\, e\, f(g)^{-1} = e$ $\Rightarrow$ $ghg^{-1} \in Ker(f)$, за свако $h \in Ker(f)$.

2) Већ доказано ($\boxed{10}$ Л)

Теорема о факторизацији хомоморфизма:

Нека је $f: G \to K$ хомоморфизам и $H \triangleleft G$. Ако је $\pi: G \to G/H$ природна пројекција и $H \leq Ker(f)$, тада постоји јединствен хомоморфизам $F: G/H \to K$ ткд. $F \circ \pi = f$.

При томе, F је 1-1 акко $H = Ker(f)$.

Д: Дефинишемо $F: G/H \to K$, $F(gH) = f(g)$.

* докажимо добру дефинисаност: $g_1 H = g_2 H \Leftrightarrow g_1^{-1} g_2 \in H \leq Ker f \overset{(*)}{\Rightarrow} g_1^{-1} g_2 \in Ker f$
$\Leftrightarrow f(g_1^{-1} g_2) = e \Leftrightarrow f(g_1)^{-1} f(g_2) = e$
$\Leftrightarrow f(g_1) = f(g_2) \Leftrightarrow F(g_1 H) = F(g_2 H)$

* докажимо да је хомоморфизам: $F(g_1 H) \cdot F(g_2 H) = f(g_1) f(g_2) = f(g_1 g_2) = F(g_1 H \cdot g_2 H)$

Јасно, $(F \circ \pi)(g) = F(\pi(g)) = F(gH) = f(g)$ $\Rightarrow$ $F \circ \pi = f$. Такође, F је јединствено.
иначе не би била добро дефинисана

* Докажимо и други део:

($\Rightarrow$) пс. $\exists g \in Ker f \setminus H$. Тада је $F(gH) = f(g) = e = f(e) = F(eH) \overset{F \text{ је } 1\text{-}1}{\Longrightarrow} gH = eH \Rightarrow g \in H$ $\lightning$

($\Leftarrow$) У делу где смо доказали добру деф., $(*)$ је сада $\Leftrightarrow$ уместо само $\Rightarrow$, па је F 1-1.

Прва теорема о изоморфизму за групе:
Нека је $f: G \to K$ хомоморфизам, $\pi: G \to G/\mathrm{Ker} f$ природна пројекција и $i: \mathrm{Im} f \to K$ инклузија.
Тада постоји јединствен хомоморфизам $\phi: G/\mathrm{Ker} f \to \mathrm{Im} f$ ткд. $f = i \circ \phi \circ \pi$.

При томе, ϕ је изоморфизам, тј. $G/\mathrm{Ker} f \cong \mathrm{Im} f$.

Д: По претх. теореми, постоји јед. хомоморфизам $F: G/\mathrm{Ker} f \to K$, $f = F \circ \pi$, такође F је 1-1.

$\mathrm{Im} F = \mathrm{Im} f \Rightarrow F$ се факторише у облику: $F = i \circ \phi$, где $\phi: G/\mathrm{Ker} f \to \mathrm{Im} f$, $\phi(g\mathrm{Ker} f) = F(g\mathrm{Ker} f) = f(g)$.

Јасно, ϕ је на, а по претх. је и 1-1 $\Rightarrow \phi$ изоморфизам. Одавде $G/\mathrm{Ker} f \cong \mathrm{Im} f$.

Теорема о факторијелу: Нека је $H \leq G$ ткд. $[G:H] = n < +\infty$.
Тада постоји $N \trianglelefteq G$, $N \subseteq H$ ткд. $[G:N] \mid n!$.

Д: $n = |G/H|$. Означимо $X = G/H$ и дефинишемо $f: G \to S_X$, $f(g) = f_g$, где $f_g: X \to X$, $f_g(aH) = gaH$

* докажимо добру дефинисаност f:

* докажимо да је f_g 1-1: $f_g(a_1H) = f_g(a_2H) \Leftrightarrow ga_1H = ga_2H \Leftrightarrow (ga_1)^{-1}ga_2 \in H$
$\Leftrightarrow a_1^{-1}g^{-1}ga_2 \in H \Leftrightarrow a_1^{-1}a_2 \in H$
$\Leftrightarrow a_1H = a_2H$

* докажимо да је f_g на: Нека $a \in G \Rightarrow f_g(g^{-1}aH) = gg^{-1}aH = aH$

* докажимо да је f хомоморфизам:

$(f(g_1) \circ f(g_2))(aH) = (f_{g_1} \circ f_{g_2})(aH) = f_{g_1}(f_{g_2}(aH)) = g_1g_2aH = f_{g_1g_2}(aH) = f(g_1g_2)(aH)$, $\forall aH$

Одавде: $f(g_1) \circ f(g_2) = f(g_1g_2)$

По првој теореми о изоморфизму: $G/\mathrm{Ker} f \cong \mathrm{Im} f$.
Знамо, по Т1, да је $\mathrm{Ker} f \trianglelefteq G$, а по Лагранжу: $|\mathrm{Im} f| \mid |S_X|$, тј. $|\mathrm{Im} f| \mid n!$

$$\Rightarrow [G:\mathrm{Ker} f] = |G/\mathrm{Ker} f| = |\mathrm{Im} f| \mid n!$$

Узмимо зато $N = \mathrm{Ker} f$. Морамо још доказати $N \subseteq H$.

$N = \mathrm{Ker} f = \{g \in G \mid f_g = id_X\} = \{g \in G \mid f_g(aH) = aH, \text{ за све } a \in G\} = \{g \in G \mid gaH = aH, \text{ за све } a \in G\}$

$= \{g \in G \mid a^{-1}ga \in H, \text{ за све } a \in G\} = \{g \in G \mid g \in aHa^{-1}, \text{ за све } a \in G\} = \bigcap_{a \in G} aHa^{-1}$

Специјално, за $a = e$ добијамо $\bigcap_{a \in G} aHa^{-1} \subseteq eHe^{-1} = H$, па $N \subseteq H$.

деф. $\mathrm{Core}(H) = \bigcap_{a \in G} aHa^{-1}$. (Ово је тражена нормална подгрупа)

19. Друга и трећа теорема о изоморфизму.

Друга теорема о изоморфизму за групе: Нека су $K \leq G$ и $H \triangleleft G$.

Тада: $H \cap K \triangleleft K$ и важи $HK/H \cong K/H \cap K$.

Д: Дефинишемо $f: K \to G/H$, $f(k) = kH$.

* докажимо да је f хомоморфизам:

$$f(k_1 k_2) = k_1 k_2 H = (k_1 H)(k_2 H) = f(k_1) f(k_2) \qquad \text{(овде користимо } H \triangleleft G\text{)}$$

* одредимо $\mathrm{Ker} f$ и $\mathrm{Im} f$:

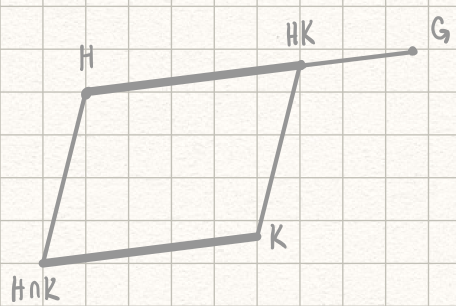
$$\mathrm{Ker} f = \{k \in K \mid f(k) = H\} = \{k \in K \mid kH = H\} = \{k \in K \mid k \in H\} = K \cap H = H \cap K \qquad (\Rightarrow H \cap K \triangleleft K)$$

$$\mathrm{Im} f = \{aH \mid aH = kH, \text{ за неко } k \in K\} = \{aH \mid k^{-1}a \in H, \text{ за неко } k \in K\} =$$

$$= \{aH \mid k^{-1}a = h, \text{ за неке } k \in K, h \in H\} = \{aH \mid a = kh, \text{ за неке } k \in K, h \in H\} =$$

$$= \{khH \mid k \in K, h \in H\} = KH/H \underset{H \triangleleft G \Rightarrow \forall k \in K\ kH = Hk}{=} HK/H$$

По првој теореми о изоморфизму за групе је $K/H \cap K = K/\mathrm{Ker} f \cong \mathrm{Im} f = HK/H$



Трећа теорема о изоморфизму за групе: Нека је $H \triangleleft G$.

Тада постоји бијекција која слика $K \mapsto K/H$, где: K - подгрупа од G који садржи H
K/H - подгрупа од G/H

Уз то, $K \triangleleft G$ акко $K/H \triangleleft G/H$. Такође, ако $K \triangleleft G$ онда $(G/H)/(K/H) \cong G/K$.

Д: Нека је $\mathcal{K} = \{K \le G \mid H \le K\}$ и $\mathbb{K} = \{\mathbb{K} \mid \mathbb{K} \le G/H\}$.

→ Докажимо да је $F: \mathcal{K} \to \mathbb{K}$, $F(K) = K/H$ бијекција коју тражимо.

* докажимо добру дефинисаност: (тј. да за $K \le G$ ткд. $H \le K$ важи $K/H \le G/H$)

$$k_1, k_2 \in K \Rightarrow (k_1H)^{-1}k_2H = k_1^{-1}Hk_2H = k_1^{-1}k_2H \Rightarrow (k_1H)^{-1}k_2H \in K/H \underset{+\,K/H \neq \emptyset}{\Longrightarrow} K/H \le G/H$$

* докажимо 1-1:

ппс. Нека је $F(K_1) = F(K_2)$, тј. $K_1/H = K_2/H$, али $K_1 \neq K_2$, па постоји $k_1 \in K_1 \setminus K_2$.
$k_1H \in K_1/H = K_2/H \Rightarrow \exists k_2 \in K_2 : k_1H = k_2H \Rightarrow k_2^{-1}k_1 \in H \Rightarrow k_2^{-1}k_1 = h \Rightarrow k_1 = \underset{K_2}{k_2}\,\underset{H \le K_2}{h} \in K_2$ ↯

* докажимо на:

Нека $\mathbb{K} \in \mathbb{K}$, тј. $\mathbb{K} \le G/H$. Нека је $K = \{k \in G \mid kH \in \mathbb{K}\}$. Доказујемо $K \le G$ и $K \ge H$

* $K \ge H$: очигледно, јер $hH = H \in \mathbb{K}$, за све $h \in H$, па $h \in K$, тј. $H \le K$.
* $k_1, k_2 \in K \Rightarrow k_1H, k_2H \in \mathbb{K} \overset{\mathbb{K} \le G/H}{\Longrightarrow} (k_1H)^{-1}k_2H \in \mathbb{K} \Rightarrow k_1^{-1}k_2H \in \mathbb{K} \Rightarrow k_1^{-1}k_2 \in K \Rightarrow K \le G$.

По доброј деф. важи $\mathbb{K} = K/H$, па $F(K) = K/H = \mathbb{K}$. (за свако $\mathbb{K} \in \mathbb{K}$ смо нашли $K \in \mathcal{K}$ које се слика у њега)

→ Докажимо други део, тј. $K \triangleleft G$ акко $K/H \triangleleft G/H$.

(⇒) Нека $gH \in G/H$. Довољно је доказати $(gH)\,K/H\,(gH)^{-1} \subseteq K/H$. (то је услов (2))

Нека је $kH \in K/H$. Важи: $gH\,kH\,(gH)^{-1} = (gkg^{-1})H \in K/H$
($K \triangleleft G \Rightarrow gkg^{-1} \in K$)

(⇐) Нека $g \in G$. Довољно је доказати $gKg^{-1} \subseteq K$.

Нека је $k \in K$. Знамо: $gH\,kH\,(gH)^{-1} = (gkg^{-1})H \in K/H \Rightarrow \exists k' : gkg^{-1}H = k'H$
$\Rightarrow (k')^{-1}gkg^{-1} \in H \Rightarrow (k')^{-1}gkg^{-1} = h$, за неко $h \in H \Rightarrow gkg^{-1} = \underset{K}{k'}\,\underset{H \le K}{h} \in K$

→ Докажимо трећи део, тј. $K \triangleleft G \Rightarrow (G/H)/(K/H) \cong G/K$

Дефинишемо $f: G/H \to G/K$, $f(gH) = gK$.
Оно је, очигледно, добро деф. и хомоморфизам. Такође је на, тј. $\mathrm{Im} f = G/K$.

Важи: $\mathrm{Ker} f = \{aH \mid a \in G, f(aH) = \overset{e_K}{K}\} = \{aH \mid a \in G, aK = K\} = \{aH \mid a \in K\} = K/H$.

Дакле, $(G/H)/(K/H) = (G/H)/\mathrm{Ker} f \cong \mathrm{Im} f = G/K$ (прва теорема о изоморфизму за групе)

20. Низови подгрупа - решиве подгрупе.

деф. Нека је G група. Тада је $G_\bullet : G = G_0 \geq G_1 \geq G_2 \geq \dots \geq G_n$ низ подгрупа од G.

деф. Низ је нормалан ако $G_i \triangleright G_{i+1}$, за $0 \leq i \leq n-1$.

Низ је Абелов ако је нормалан и G_i / G_{i+1} је Абелова група, за $0 \leq i \leq n-1$.

Низ је цикличан ако је нормалан и G_i / G_{i+1} је циклична, за $0 \leq i \leq n-1$.

деф. Група је решива акко постоји Абелов низ подгрупа од G који се завршава са $\{e\}$.

деф. Извод вишег реда групе G уводимо рекурзивно: $G^{(1)} = G'$, $G^{(n+1)} = (G^{(n)})'$, $n \geq 1$
Напомена: $G^{(0)} = G$

T1: Група G је решива акко за низ $G \geq G^{(1)} \geq G^{(2)} \geq \dots \geq G^{(n)} \geq \dots$ постоји $m \in \mathbb{N}_0$ ткд. $G^{(m)} = \{e\}$.

Д: ($\Rightarrow$) Нека је $G_\bullet : G = G_0 \geq G_1 \geq \dots \geq G_m = \{e\}$ Абелов низ. G/G_1 је Абелова $\overset{\boxed{15}\,T2}{\Rightarrow} G_1 \supseteq G'$
Докажимо индукцијом по $n \geq 0$ да $G_n \supseteq G^{(n)}$

(БИ) $n=0$: тривијално $(G = G_0 = G^{(0)})$
(ИК) $n \to n+1$: Знамо да је G_n / G_{n+1} Абелова група $\Rightarrow G_{n+1} \overset{\boxed{15}\,T2}{\supseteq} G_n' \overset{(\text{ИХ}) + H \leq K \Rightarrow H' \leq K'}{\supseteq} (G^{(n)})' = G^{(n+1)}$

Како је $G_m = \{e\} \supseteq G^{(m)}$, то је $G^{(m)} = \{e\}$.

($\Leftarrow$) Докажимо да је $G_\bullet : G = G^{(0)} \geq G^{(1)} \geq \dots \geq G^{(m)} = \{e\}$ Абелов низ који се завршава са $\{e\}$.

* Очигледно се завршава са $\{e\}$
* Јесте Абелов, зато што је $(G^{(i)})' \underset{\boxed{15}\,T2,\,1)}{\triangleleft} G^{(i)}$ и $G^{(i)} / (G^{(i)})'$ је $\underset{\boxed{15}\,T2,\,2)\ \text{(специјално)}}{\text{Абелова група}}$.

Прво прочитати доказ Т3.

Т2: Нека је G коначна група.
Тада сваки Абелов низ подгрупа од G има циклично профињење. (деф. у сл. питању)

Д: Нека је $\mathcal{G}$: $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_n$ Абелов низ подгрупа од G.

Довољно је доказати да за G и H, где $G \triangleright H$ и G/H Абелова, постоји цикл. проф. низа $G \trianglerighteq H$
(и онда то применимо на свака два узастопна у $\mathcal{G}$)

Урадимо прво случај када је G Абелова група, а $H = \{e\}$, и то индукцијом по $|G| = t$

(БИ) $t = 1$: тривијално ($\{e\}$ већ јесте цикл.)

(ИК) $t \to t+1$: Нека је $a \in G \setminus \{e\}$.

1° $\langle a \rangle = G$: онда је $G \trianglerighteq \{e\}$ тражени низ.

2° $\langle a \rangle \neq G$: посматрајмо низ $G \trianglerighteq \langle a \rangle \trianglerighteq \{e\}$, он очигледно јесте Абелов

Посматрајмо сада $G/\langle a \rangle \trianglerighteq \{\langle a \rangle\}$. На ово можемо применити (ИХ), (јер $\langle a \rangle \neq G$)
па постоји цикличан низ $G/\langle a \rangle = \mathbb{G}_0 \trianglerighteq \mathbb{G}_1 \trianglerighteq \mathbb{G}_2 \trianglerighteq \ldots \trianglerighteq \langle a \rangle / \langle a \rangle = \{\langle a \rangle\}$
$\mathbb{G}_1 = G_1/\langle a \rangle$, $\mathbb{G}_2 = G_2/\langle a \rangle$ ... (исти начин као у Т3)

Тада је $(G_i/\langle a \rangle)/(G_{i+1}/\langle a \rangle)$ циклична.
Пошто је $(G_i/\langle a \rangle)/(G_{i+1}/\langle a \rangle) \cong G_i/G_{i+1}$ (по III т.о.и.), онда је и G_i/G_{i+1} циклична.

Због тога, низ $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq \langle a \rangle \trianglerighteq \langle e \rangle$ је цикличан низ подгрупа од G.

Вратимо се на проблем са почетка: $G \triangleright H$ и G/H је Абелова група.

По претх., постоји цикл. низ $G/H \trianglerighteq G_1/H \trianglerighteq \ldots \trianglerighteq G_n/H = \{H\}$. $\overset{\text{III т.о.и.}}{\Longrightarrow}$ $G \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_n = H$ је цикличан.

$(K=G_i)$

Т3: Нека је $H \triangleleft G$. Тада је G решива акко су H и G/H решиве.

Д: $(\Leftarrow)$ Нека су $H_\bullet : H = H_0 \trianglerighteq H_1 \trianglerighteq \dots \trianglerighteq H_n = \{e\}$ и $\mathbb{G}_\bullet : G/H = \mathbb{G}_0 \trianglerighteq \mathbb{G}_1 \trianglerighteq \dots \trianglerighteq \mathbb{G}_m = \{H\}$ Абелови низови.

По трећој теореми о изоморфизму, $\forall \mathbb{G}_i \ \exists G_i \le G,\ G_i \supseteq H$ ткд. $\mathbb{G}_i = G_i/H$. (узмемо $K=G_i$, $\mathbb{K}=\mathbb{G}_i$)

Уз то, како је $\mathbb{G}_i \trianglerighteq \mathbb{G}_{i+1}$, онда је и $G_i \trianglerighteq G_{i+1}$, тј. $G_{i+1} \triangleleft G_i$.

Зато је $G_\bullet : G = G_0 \trianglerighteq G_1 \trianglerighteq \dots \trianglerighteq G_m = H = H_0 \trianglerighteq H_1 \trianglerighteq \dots \trianglerighteq H_n = \{e\}$ нормалан низ подгрупа од G који се завршава са $\{e\}$.

Да би $G_\bullet$ био Абелов низ, довољно је доказати још да је G_i/G_{i+1} Абелова група. (зато што знамо да је свака H_i/H_{i+1} Абелова, јер је $H_\bullet$ Абелов)

По трећој теореми о изоморфизму: $G_i/G_{i+1} \cong (G_i/H)/(G_{i+1}/H) \cong \mathbb{G}_i/\mathbb{G}_{i+1}$.
Пошто је $\mathbb{G}_\bullet$ Абелов низ, онда је $\mathbb{G}_i/\mathbb{G}_{i+1}$ Абелова, па је и G_i/G_{i+1} Абелова група.

$(\Rightarrow)$ Нека је $G_\bullet : G = G_0 \trianglerighteq G_1 \trianglerighteq \dots \trianglerighteq G_n = \{e\}$ Абелов низ подгрупа од G.

* Докажимо да је H решива:

Нека је $H_\bullet : H = H_0 \trianglerighteq H_1 \trianglerighteq \dots \trianglerighteq H_n = \{e\}$ низ подгрупа од H, задат са $H_i = H \cap G_i$.
Докажимо да је $H_\bullet$ Абелов низ.

Знамо $G_{i+1} \triangleleft G_i$ и $H \cap G_i \le G_i$, и важи: $(H\cap G_i) \cap G_{i+1} = H \cap (G_i \cap G_{i+1}) = H \cap G_{i+1} = H_{i+1}$

$(K = H\cap G_i,\ H = G_{i+1},\ G = G_i)$

По другој теореми о изоморфизму, $(H \cap G_i) \cap G_{i+1} \triangleleft H \cap G_i$, тј. $H_{i+1} \triangleleft H_i$.
По истој теореми, важи и $(G_i \cap H)/(G_{i+1} \cap H) \cong G_{i+1}(G_i \cap H)/G_{i+1} \le G_i/G_{i+1}$
што значи $H_i/H_{i+1} \le G_i/G_{i+1}$.
Пошто је $G_\bullet$ Абелов $\Rightarrow$ G_i/G_{i+1} Абелова, па је и њена подгрупа H_i/H_{i+1} Абелова.
па је $H_\bullet$ Абелов низ.

Дакле, $H_\bullet$ је Абелов низ који се завршава са $\{e\}$, па је H решива група.

* Докажимо да је G/H решива:

Нека је $\mathcal{G}_\circ$: $G/H = GH/H \geqslant G_1H/H \geqslant \dots \geqslant G_nH/H = \{H\}$ и докажимо да је Абелов.

нормалан: да би важило $G_iH/H \triangleright G_{i+1}H/H$, довољно је (по трећој теореми о изоморфизму) доказати да $G_iH \triangleright G_{i+1}H$

$g \in G_iH$, тј. $g = g_iH$. Тада: $gG_{i+1}H = g_ihG_{i+1}H \overset{h\in G_{i+1}}{=} g_iG_{i+1}H \overset{h\in H}{=} g_iG_{i+1}Hh \overset{G_{i+1}\triangleleft G_i}{=} G_{i+1}g_iHh \overset{H\triangleleft G}{=} G_{i+1}Hg_ih$

Дакле, $gG_{i+1}H = G_{i+1}Hg$, па по услову (3) из $\boxed{13}$T1 $\Rightarrow G_{i+1}H \triangleleft G_iH$

Абелов: доказујемо да је $(G_iH/H)/(G_{i+1}H/H)$ Абелова група.
За то је довољно доказати да је $G_iH/G_{i+1}H$ Абелова група. (по трећој теореми о изоморфизму)

Знамо $G_iG_{i+1}H = G_iH$
Важи и $G_iH/G_{i+1}H \cong G_i/(G_i \cap G_{i+1}H)$ (по другој теореми о изоморфизму)
Како је G_i/G_{i+1} Абелова, то је $G_{i+1} \supseteq (G_i)'$ ($\boxed{15}$T2 под 2) (*)

Такође, да би $G_i/(G_i \cap G_{i+1}H)$ била Абелова, довољно је да $G_i \cap G_{i+1}H \supseteq (G_i)'$

То важи јер $\underbrace{G_i}_{\supseteq G_{i+1}} \cap \underbrace{G_{i+1}H}_{\supseteq G_{i+1}} \supseteq G_{i+1} \overset{(*)}{\supseteq} (G_i)'$, па $\mathcal{G}_\circ$ јесте и Абелов низ.

Како је $\mathcal{G}_\circ$ и нормалан и Абелов, то значи да је G/H решива.

21. Теорема о лептиру и примене на низове група.

Теорема о лептиру: Нека су A, B, A_1, B_1 подгрупе од G т.к.д. $A_1 \triangleleft A$, $B_1 \triangleleft B$.

Тада је $A_1(A\cap B_1) \triangleleft A_1(A\cap B)$ и $(A_1\cap B)B_1 \triangleleft (A\cap B)B_1$

и важи $A_1(A\cap B)/A_1(A\cap B_1) \cong (A\cap B)B_1/(A_1\cap B)B_1$.

Д: * Докажимо да је $A_1(A\cap B_1) \triangleleft A_1(A\cap B)$.

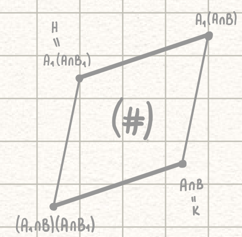
Нека је $g \in A_1(A\cap B)$, тј. $g = a_1 b$ $\left(\begin{smallmatrix} a_1 \in A_1 \\ b \in A\cap B \end{smallmatrix}\right)$ и докажимо да је $gA_1(A\cap B_1) = A_1(A\cap B_1)g$. (услов 3 13Т1)

$$a_1 b A_1(A\cap B_1) \overset{A_1 \triangleleft A}{=} a_1 A_1 b (A\cap B_1) \overset{A\cap B_1 \triangleleft A\cap B}{=} a_1 A_1 (A\cap B_1) b \overset{a_1 \in A_1(A\cap B_1)}{=} A_1(A\cap B_1) b = A_1(A\cap B_1) a_1 b.$$

$$(*)\quad \left.\begin{array}{r} A\cap B \leq B \\ B_1 \triangleleft B \\ (A\cap B)\cap B_1 = A\cap B_1 \end{array}\right\} \overset{\text{II т.о.и.}}{\Longrightarrow} A\cap B_1 \triangleleft A\cap B$$

* Докажимо да је $(A_1\cap B)B_1 \triangleleft (A\cap B)B_1$: аналогно

* Докажимо да је $A_1(A\cap B)/A_1(A\cap B_1) \cong (A\cap B)B_1/(A_1\cap B)B_1$



Желимо да имамо (#), да бисмо наместили на II т.о.и.
По претх., важи: $A_1(A\cap B_1) \triangleleft A_1(A\cap B)$ и по $(*)$ важи: $A\cap B_1 \triangleleft A\cap B$
Дакле, довољно је доказати: i) $A_1(A\cap B_1)(A\cap B) = HK = A_1(A\cap B)$
ii) $A_1(A\cap B_1)\cap A\cap B = H\cap K = (A_1\cap B)(A\cap B_1)$

i) тривијално, јер $A\cap B_1 \subseteq A\cap B$ (па као да $A\cap B_1$ „утопимо" у $A\cap B$)

ii) $(\supseteq)$: $\left.\begin{array}{l} A_1\cap B \subseteq A\cap B \\ A\cap B_1 \subseteq A\cap B \end{array}\right\} \Rightarrow (A_1\cap B)(A\cap B_1) \subseteq A\cap B$

очигледно: $\underbrace{(A_1\cap B)}(A\cap B_1) \subseteq \underbrace{A_1}(A\cap B_1)$ $\Big\} \Rightarrow (A_1\cap B)(A\cap B_1) \subseteq A_1(A\cap B_1) \cap (A\cap B)$

$(\subseteq)$: Нека $g \in A_1(A\cap B_1)\cap A\cap B$. Пошто $g \in A_1(A\cap B_1)$, запишимо га $g = a_1 b_1$ $\left(\begin{smallmatrix} a_1 \in A_1 \\ b_1 \in A\cap B_1 \end{smallmatrix}\right)$

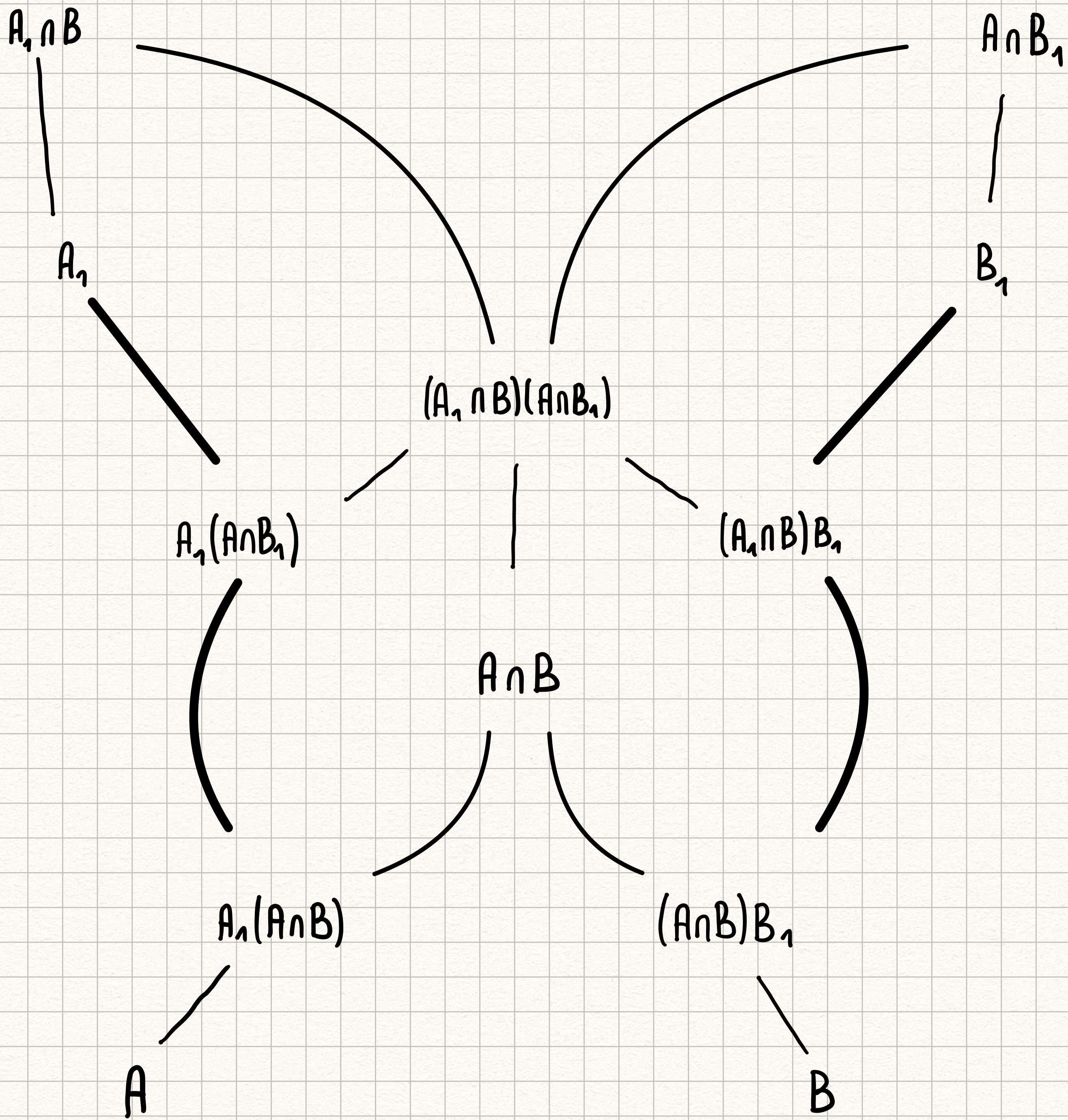
Да би важило $g \in (A_1\cap B)(A\cap B_1)$, довољно је доказати још $a_1 \in A_1\cap B$ (јер $b_1 \in A\cap B_1$)

Како $g \in B \Rightarrow g = b \in B \Rightarrow a_1 b_1 = b \Rightarrow a_1 = b b_1^{-1} \in B \Rightarrow a_1 \in B \Rightarrow a_1 \in A_1\cap B$

Искористимо сада II т.о.и.: $A_1(A\cap B)/A_1(A\cap B_1) \cong (A\cap B)/(A_1\cap B)(A\cap B_1)$

Аналогно: $(A\cap B)B_1/(A\cap B_1)A_1 \cong (A\cap B)/(A_1\cap B)(A\cap B_1)$

Одавде: $A_1(A\cap B)/A_1(A\cap B_1) \cong (A\cap B)B_1/(A\cap B_1)A_1$


$A_1 \cap B$
$A \cap B_1$
A_1
B_1
$(A_1 \cap B)(A \cap B_1)$
$A_1(A \cap B_1)$
$(A_1 \cap B)B_1$
$A \cap B$
$A_1(A \cap B)$
$(A \cap B)B_1$
A
B

деф. Нека су $G_\cdot : G = G_0 \geqslant G_1 \geqslant \dots \geqslant G_m$ и $H_\cdot : G = H_0 \geqslant H_1 \geqslant \dots \geqslant H_n$ низови подгрупа од G.
Тада је $H_\cdot$ профињење $G_\cdot$ ако за свако $1 \leq i \leq m$ постоји $1 \leq j \leq n$ ткд. $G_i = H_j$

деф. Ако су $G_\cdot$ и $H_\cdot$ нормални низови који се завршавају са $\{e\}$ (тј. $G_m = \{e\}$, $H_n = \{e\}$) и $G_i \neq G_{i+1}$, $H_i \neq H_{i+1}$,
тада су ти низови еквивалентни ако је $n = m$ и постоји пермутација $\sigma \in S_n$ ткд. $G_{i-1}/G_i \cong H_{\sigma(i)-1}/H_{\sigma(i)}$

Шредерова теорема: Два нормална низа подгрупа од G која се завршавају са $\{e\}$, имају еквивалентна профињења.

Д: Нека су $G_\cdot : G = G_0 \geqslant G_1 \geqslant \dots \geqslant G_m = \{e\}$ и $H_\cdot : G = H_0 \geqslant H_1 \geqslant \dots \geqslant H_n = \{e\}$ нормални низови од G.
У претх. теореми, доказали смо да важи: $A_1(A \cap B_1) \triangleleft A_1(A \cap B)$ и $(A_1 \cap B) B_1 \triangleleft (A \cap B) B_1$
Посматрајмо низове које добијемо кад применимо теорему о лептиру:

$$
\begin{aligned}
\mathcal{G}_\cdot :\ G = G_{0,0} &= G_1(\overbrace{G_0 \cap H_0}^{G_0}) \triangleright G_1(G_0 \cap H_1) \triangleright \dots \triangleright G_1(\overbrace{G_0 \cap H_n}^{\{e\}}) = G_1 = G_{1,0} \\
= G_{1,0} &= G_2(G_1 \cap H_0) \triangleright G_2(G_1 \cap H_1) \triangleright \dots \triangleright G_2(G_1 \cap H_n) = G_2 = G_{2,0} \\
&\vdots \\
G_{m-1} = G_{m-1,0} &= G_m(G_{m-1} \cap H_0) \triangleright \dots \triangleright G_m(G_{m-1} \cap H_n) = G_m = \{e\}
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{H}_\cdot :\ G = H_{0,0} &= (G_0 \cap H_0) H_1 \triangleright (G_1 \cap H_0) H_1 \triangleright \dots \triangleright (G_m \cap H_0) H_1 = H_1 = H_{1,0} \\
= H_{1,0} &= (G_0 \cap H_1) H_2 \triangleright (G_1 \cap H_1) H_2 \triangleright \dots \triangleright (G_m \cap H_1) H_2 = H_2 = H_{2,0} \\
&\vdots \\
H_{n-1} = H_{n-1,0} &= (G_0 \cap H_{n-1}) H_n \triangleright (G_1 \cap H_{n-1}) H_n \triangleright \dots \triangleright (G_m \cap H_{n-1}) H_n = H_n = \{e\}
\end{aligned}
$$

Ово су нормални низови подгрупа од G – $\mathcal{G}_\cdot$ је профињење $G_\cdot$, а $\mathcal{H}_\cdot$ је профињење $H_\cdot$.

Означимо: $G_{i,j} = G_{i+1}(G_i \cap H_j)$ и $H_{i,j} = (G_j \cap H_i) H_{i+1}$ (то смо заправо већ писали)

Важи: $G_{i,j} / G_{i,j+1} = G_{i+1}(G_i \cap H_j) / G_{i+1}(G_i \cap H_{j+1})$

$\overset{\text{лептир}}{\cong} (G_i \cap H_j) H_{j+1} / (G_{i+1} \cap H_j) H_{j+1} = H_{j,i} / H_{j,i+1}$ $\Rightarrow$ $\mathcal{G}_\cdot$ и $\mathcal{H}_\cdot$ су еквивалентни.

деф. Група G је **проста** ако нема нормалну подгрупу различиту од $\{e\}$ и G.

Жордан-Хелдерова теорема: Нека је $G_\bullet : G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_n = \{e\}$ нормалан низ подгрупа од G ткд. је $G_i \neq G_{i+1}$ и G_i / G_{i+1} проста за $0 \leq i \leq n-1$.

Тада је сваки нормалан низ подгрупа од G који задовољава исте услове еквивалентан са $G_\bullet$.

Д: Нека је $H_\bullet$ други такав низ. По Шредеру, ови низови имају екв. профињења.

Међутим, $G_\bullet$ и $H_\bullet$ се не могу даље профинити (*), па су та профињења баш $G_\bullet$ и $H_\bullet$.

(*) $G_\bullet$ не можемо профинити, јер ако би постојало K ткд. $G_i \trianglerighteq K \trianglerighteq G_{i+1}$, $K \notin \{G_i, G_{i+1}\}$

по III т.о.и. је $K/G_{i+1} \triangleleft G_i/G_{i+1}$, што је немогуће (услов + деф. простог низа)

22. Коначно генерисане слободне Абелове групе.

(прво погледати питања 24 и 25, па се вратити на 22 и 23)

У овом питању, операцију означавамо са $+$
„степеновање" означавамо са $n \cdot a = \underbrace{a + \ldots + a}_{n}$
неутрал је 0.

деф. Нека је A Абелова група и $A_1, \ldots, A_k \leq A$.

Сума подгрупа је $A_1 + \ldots + A_k = \{a_1 + \ldots + a_k \mid a_i \in A_i\}$.
Ова сума је директна ако $(A_1 + \ldots + A_{i-1}) \cap A_i = \{0\}$, $2 \leq i \leq k$. Пишемо $A_1 \oplus \ldots \oplus A_k$.

T1: $A_1 \oplus \ldots \oplus A_k \cong A_1 \times \ldots \times A_k$

Д: Нека је $f: A_1 \times \ldots \times A_k \to A_1 \oplus \ldots \oplus A_k$, $f(a_1, \ldots, a_k) = a_1 + \ldots + a_k$
На стандардан начин, доказује се да је f изоморфизам.

деф. Нека је $x_1, \ldots, x_n \in F$ и F је Абелова група.
Тада је F слободна Абелова група са системом слободних генератора (ссг) $[x_1, \ldots, x_n]$ ако за сваку Абелову групу A и $a_1, \ldots, a_n \in A$ постоји јединствен хомоморфизам $f: F \to A$ ткд. $f(x_i) = a_i$, $1 \leq i \leq n$.

$$\begin{tikzcd} & F \arrow[d, dashed, "f"] \\ X \arrow[ur, "i"] \arrow[r, "\theta = f_X"'] & A \end{tikzcd} \qquad X = \{x_1, \ldots, x_n\}$$

$f_X(x_i) = a_i$ (рестрикција f на X)

Ово је спец. случај слободне групе.

T2: Ако је F сл. Аб. гр. са ссг $[x_1, \ldots, x_n]$, тада је $F = \langle \{x_1, \ldots, x_n\} \rangle$.

Д: Аналогно $\boxed{24}$ T1

T3: Ако је F сл. Аб. гр. са ссг $[x_1, \ldots, x_n]$ и F' сл. Аб. гр. са ссг $[x_1', \ldots, x_n']$, тада је $F \cong F'$.

Д: Аналогно $\boxed{24}$ T2

T4: Ако је F сл. Аб. гр. са ссг $[x_1, \ldots, x_n]$ и ако је $m_1 x_1 + \ldots + m_n x_n = 0$, $m_i \in \mathbb{Z}$, тада $m_1 = \ldots = m_n = 0$.

Д: ппс. Нека је, б.у.о., $m_1 \neq 0$

Посматрајмо $a_1 = 1$, $a_2 = \ldots = a_n = 0$ и хомоморфизам $f: F \to \mathbb{Z}$, $f(x_i) = a_i$

$$\begin{tikzcd} & F \arrow[d, dashed, "f"] \\ X \arrow[ur, "i"] \arrow[r, "\theta"'] & \mathbb{Z} \end{tikzcd}$$

Међутим: $0 = f(m_1 x_1 + \ldots + m_n x_n) = m_1 f(x_1) + m_2 f(x_2) + \ldots + m_n f(x_n)$
$= m_1 \underbrace{a_1}_{1} + m_2 \underbrace{a_2}_{0} + \ldots + m_n \underbrace{a_n}_{0} = m_1$ $\lightning$

T5: Група $\mathbb{Z}^n$ је сл. Аб. гр. са ссг $[(1,0,0,\dots,0), (0,1,0,\dots,0), \dots, (0,0,0,\dots,1)]$.

Д: Нека је A Абелова група и $a_1, \dots, a_n \in A$.
Желимо да докажемо постоји јединствени хомоморфизам $f: \mathbb{Z}_n \to A$ ткд. $f(0,\dots,0,\overset{i}{1},0,\dots,0) = a_i$

Дефинишемо: $f: \mathbb{Z}^n \to A$, $f(m_1,\dots,m_n) = m_1 a_1 + \dots + m_n a_n$

* За f важи поменути услов (јер $f(0,\dots,0,1,0,\dots,0) = 0\cdot a_1 + \dots + 1\cdot a_i + \dots + 0\cdot a_n = a_i$)
* f је хомоморфизам:

$$\begin{aligned} f((m_1,\dots,m_n)+(m_1'+\dots+m_n')) &= f(m_1+m_1', \dots, m_n+m_n') = (m_1+m_1')a_1 + \dots + (m_n+m_n')a_n \\ &= m_1 a_1 + \dots + m_n a_n + m_1' a_1 + \dots + m_n' a_n \\ &= f(m_1,\dots,m_n) + f(m_1'+\dots+m_n') \end{aligned}$$

* f је једини такав хомоморфизам:

$$f((m_1,\dots,m_n)) = f(m_1(1,0,\dots,0) + \dots + m_n(0,\dots,0,1)) \overset{f\text{ хом.}}{=} m_1 f(1,\dots,0) + \dots + m_n f(0,\dots,1) = m_1 a_1 + \dots + m_n a_n.$$

па постоји највише један овакав хомоморфизам. (сви су једнаки)

T6: Ако је $\mathbb{Z}^r \cong \mathbb{Z}^s$, тада је $r=s$.

Д: Аналогно $\boxed{24}$ Т3

T7: Ако је $[x_1,\dots,x_n]$ ссг сл. Аб. гр. F и $t_2,\dots,t_n \in \mathbb{Z}$, тада је и $[x_1+t_2x_2+\dots+t_nx_n, x_2, \dots, x_n]$ ссг за F.

Д: Нека је A Абелова група и $a_1,\dots,a_n \in A$.
За исту ту групу, посматрајмо елементе $b_1 = a_1 - t_2a_2 - \dots - t_na_n$, $b_2 = a_2$, ..., $b_n = a_n$. $(b_1,\dots,b_n \in A)$
Тада постоји хомоморфизам $f': F \to A$ ткд. $f'(x_i) = b_i$ (јер је $[x_1,\dots,x_n]$ ссг).

Докажимо да ово f' задовољава $f'(y_i) = a_i$, где је $y_1 = x_1 + t_2x_2 + \dots + t_nx_n$, $y_2 = x_2$, ..., $y_n = x_n$.

1° $i \geq 2$: тривијално $(f'(y_i) = f'(x_i) = b_i = a_i)$
2° $i = 1$:
$$\begin{aligned} f'(y_1) &= f'(x_1 + t_2x_2 + \dots + t_nx_n) = f'(x_1) + t_2 f'(x_2) + \dots + t_n f'(x_n) \\ &= b_1 + t_2b_2 + \dots + t_nb_n = (a_1 - t_2a_2 - \dots - t_na_n) + t_2a_2 + \dots + t_na_n = a_1 \end{aligned}$$

Коначно, докажимо да је f' једини такав хомоморфизам.

?

23. Нормална и елементарна форма коначно генерисане Абелове групе.

Л1: $H_1 \triangleleft G_1,\ H_2 \triangleleft G_2.$ 1) $G_1 \times G_2 / H_1 \times H_2 \cong G_1/H_1 \times G_2/H_2$
2) $H_1 \times H_2 \triangleleft G_1 \times G_2.$

Д: Докажимо да је $f: G_1 \times G_2 \to G_1/H_1 \times G_2/H_2$, $f(g_1,g_2) = (g_1H_1, g_2H_2)$ хомоморфизам.

$$f((g_1,g_2)(g_1',g_2')) = f(g_1g_1', g_2g_2') = (g_1g_1'H_1, g_2g_2'H_2) = (g_1H_1, g_2H_2)(g_1'H_1, g_2'H_2) = f(g_1,g_2)f(g_1',g_2').$$

$\mathrm{Im} f = G_1/H_1 \times G_2/H_2$ (јер је f очигледно на)

$\mathrm{Ker} f = \{(g_1,g_2) \mid f(g_1,g_2) = (H_1,H_2)\} = \{(g_1,g_2) \mid g_1H_1 = H_1,\ g_2H_2 = H_2\} = \{(g_1,g_2) \mid g_1 \in H_1,\ g_2 \in H_2\} = H_1 \times H_2.$

1) По I т.о.и. важи $G_1 \times G_2 / \mathrm{Ker} f \cong \mathrm{Im} f$, па кад уврстимо следи тврђење.

2) По $\boxed{18}$ Т1 важи $\mathrm{Ker} f \triangleleft G_1 \times G_2$, па кад уврстимо следи тврђење.

деф. Нека је A Абелова група.
Торзиона подгрупа од A, $T(A)$, је скуп свих елемената из A коначног реда.

Л2: $T(A) \leq A$ (Торзиона подгрупа заиста јесте подгрупа).

Д: * $T(A) \neq \emptyset$ $(0 \in T(A))$
* $a, b \in T(A)$, докажимо да $a - b \in T(A)$ (ab^{-1}): $\exists n, m \in \mathbb{N}: na = 0,\ mb = 0.$ Тада $nm(a-b) = 0.$

Л3: Ако су A, B Абелове и $A \cong B$, тада је: 1) $T(A) \cong T(B)$
2) $A/T(A) \cong B/T(B)$

Д: Нека је $f: A \to B$ изоморфизам.

1) За $a \in T(A)$, по $\boxed{6}$ Т3, је $\omega(a) = \omega(f(a)) \Rightarrow f[T(A)] \subseteq T(B).$
За $b \in T(B)$, како је f на, постоји $a \in A$ т.д. $f(a) = b$ и важи $\omega(f(a)) = \omega(a) \Rightarrow a \in T(A) \Rightarrow b = f(a) \in f[T(A)]$
$\Rightarrow T(B) \subseteq f[T(A)]$

Дакле $f[T(A)] = T(B)$, па рестрикција f на $T(A)$ је $g: T(A) \to T(B)$ $\Rightarrow$ $T(A) \cong T(B)$
које је изоморфизам

2) Нека је $F: A/T(A) \to B/T(B)$, $F(a + T(A)) = f(a) + T(B)$.
На стандардан начин, доказује се да је f изоморфизам.

Теорема о нормалној форми: Нека је A коначно генерисана Абелова група.
Тада постоје јединствени $k, l \geq 0$ и $n_1, \dots, n_k \in \mathbb{N}$ ткд. $n_1 | n_2 | \dots | n_k$

и важи $A \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k} \times \mathbb{Z}^l$.

Доказ изводимо уз помоћ неколико тврђења.

Т1: Нека је $q \in \mathbb{Z} \setminus \{0\}$ и $n \geq 2$. Тада је број решења једначине $q \cdot x = 0$ у $\mathbb{Z}_n$ једнак $NZD(q, n)$.
(овде мислимо на множење у $\mathbb{Z}$)

Д: $q \cdot x = 0$ акко $n | qx$. Означимо $d = NZD(q,n)$: тада $n = du$, $q = dv$ и $NZD(u,v) = 1$.
$n | qx \iff du | dvx \iff u | vx \iff u | x$.

Дакле, $x \in \{0, u, 2u, \dots, (d-1)u\}$, па има $d = NZD(q,n)$ решења.

Последица: Број решења једначине $q \cdot x = 0$ у $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ је $NZD(q, n_1) \cdot \dots \cdot NZD(q, n_k)$.

Д: За $x = (x_1, \dots, x_n)$ важи $q \cdot x = 0$ акко $q \cdot x_1 = 0, \dots, q \cdot x_k = 0$.
Дакле, за свако $1 \leq i \leq k$, x_i можемо „одабрати" на $NZD(q, n_i)$ начина. Одавде следи тврђење.

Доказ јединствености у ТНФ:

ппс. $L = \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k} \times \mathbb{Z}^l \cong \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_s} \times \mathbb{Z}^r = R$, при чему је $n_1 | \dots | n_k$ и $m_1 | \dots | m_s$.

Како је $L \cong R \overset{\text{Л3}}{\Rightarrow} T(L) \cong T(R)$. Јасно $T(L) = \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k} \times \{0\}^l \cong \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ (*) (у $\mathbb{Z}_{n_i}$ су сви коначног реда у $\mathbb{Z}^l$ само $(0, \dots, 0)$)
$T(R) = \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_s} \times \{0\}^r \cong \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_s}$

Сада користимо последицу, тј. бројимо решења једначине $q \cdot x = 0$ у $T(L)$ и у $T(R)$ за разне q
(не мора их бити једнако)

Нека је, нпр., $k \geq s$ (тако их распоредимо на почетку)
Узмимо $q = n_1$: број решења $n_1 \cdot x = 0$ у $T(L)$ је: $NZD(n_1, n_1) \cdot \dots \cdot NZD(n_1, n_k) = n_1 \dots n_1 = n_1^k$

$\overset{(*)}{=} NZD(n_1, m_1) \cdot \dots \cdot NZD(n_1, m_s) \leq n_1 \cdot \dots \cdot n_1 = n_1^s$

па је $n_1^k \leq n_1^s \overset{k \geq s}{\Longrightarrow}$ **$k = s$**.
Уз то, знак $\leq$ изнад је зато $=$, па је $NZD(n_1, m_1) = n_1$, тј. $n_1 | m_1$

Узмимо $q = m_1$: аналогно: $m_1 | n_1$, па зато **$n_1 = m_1$**
Даље, аналогно добијамо **$n_2 = m_2, \dots, n_k = m_s$** (доказали смо $k = s$).

Како је $L \cong R \overset{\text{Л3}}{\Rightarrow} L / T(L) \cong R / T(R)$

па је: $L/T(L) = (\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k} \times \mathbb{Z}^l) / (\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k} \times \{0\}^l)$

$\overset{\text{Л1}}{\cong} (\mathbb{Z}_{n_1} / \mathbb{Z}_{n_1}) \times \dots \times (\mathbb{Z}_{n_k} / \mathbb{Z}_{n_k}) \times (\mathbb{Z} / \{0\})^l \cong \mathbb{Z}^l$

аналогно: $R / T(R) \cong \mathbb{Z}^r$

Дакле, $\mathbb{Z}^l \cong \mathbb{Z}^r$, па по $\boxed{22}$ Т6 $\Rightarrow$ **$l = r$** $\overset{\bullet}{\Rightarrow} L = R$. ↯

T2: Нека је F сл. Аб. гр. са ссг од n елемената и $R \leq F$.
Тада постоји ссг $[x_1, \dots, x_n]$ групе F и ненегативни $d_1, \dots, d_n \in \mathbb{Z}$ ткд. $d_1 | \dots | d_n$ (узимамо $0|0$) и важи $R = \langle d_1 x_1 \rangle \oplus \dots \oplus \langle d_n x_n \rangle$

Д: Индукцијом по n.

(БИ) $n=0$: тада је $R = \{0\}$, па можемо узети $d_1 = \dots = d_n = 0$.

(ИК) $n-1 \to n$: дефинишимо $d_1 = \min\{d_1 > 0 \mid$ постоје $x \in R$ и ссг $[x_1, \dots, x_n]$ за F ткд. $x = d_1 x_1 + \dots + d_n x_n\}$.
Оно је добро деф. јер можемо пп. $R \neq \{0\}$ (то смо већ испитали)

?

Доказ егзистенције у ТНФ:

Нека је A генерисана скупом $\{a_1, \dots, a_n\}$, тј. $A = \langle \{a_1, \dots, a_n\} \rangle$.
Нека је F сл. Аб. гр. са ссг $[x_1, \dots, x_n]$
Тада постоји хомоморфизам $f: F \to A$ ткд. $f(x_i) = a_i$, за све $1 \le i \le n$.

Како је $\mathrm{Im} f \le A$ и $\mathrm{Im} f \ge \{a_1, \dots, a_n\}$ $\Rightarrow$ $\mathrm{Im} f = A$ $\overset{\text{I т.о.и.}}{\Longrightarrow}$ $F / \mathrm{Ker} f \cong A$.

По Т2, како је $\mathrm{Ker} f \le F$, то постоје $d_1 | \dots | d_n$ $(d_i \in \mathbb{N} \cup \{0\})$ и ссг $[y_1, \dots, y_n]$ за F ткд.

$$\mathrm{Ker} f = \langle d_1 y_1 \rangle \oplus \dots \oplus \langle d_n y_n \rangle$$

Следи: $A \cong F/\mathrm{Ker} f = (\langle y_1 \rangle \oplus \dots \oplus \langle y_n \rangle) / (\langle d_1 y_1 \rangle \oplus \dots \oplus \langle d_n y_n \rangle)$

$$\overset{\boxed{22}\,\text{Т1}}{\cong} (\langle y_1 \rangle \times \dots \times \langle y_n \rangle) / (\langle d_1 y_1 \rangle \times \dots \times \langle d_n y_n \rangle)$$

$$\overset{\text{Л1}}{\cong} (\langle y_1 \rangle / \langle d_1 y_1 \rangle) \times \dots \times (\langle y_n \rangle / \langle d_n y_n \rangle)$$

Како је $\langle x \rangle / \langle dx \rangle = \begin{cases} \mathbb{Z}_d, & d > 0 \\ \mathbb{Z}, & d = 0 \end{cases}$, тврђење следи.

фали елементарна форма

24. Слободне групе - основни појмови и особине.

деф. Група F је слободна на скупу $X \subseteq F$ ако за сваку групу G и свако пресликавање $\theta: X \to G$ постоји јединствен хомоморфизам $\theta': F \to G$ ткд. $\theta = \theta' \circ i$, где је $i: X \to F$, $i(x) = x$ инклузија.

$$\begin{tikzcd} & F \arrow[d, dashed, "\theta'"] \\ X \arrow[ur, "i"] \arrow[r, "\theta"'] & G \end{tikzcd}$$

(може било које G и било које θ)

T1: Ако је F слободна на X, тада X генерише F.

Д: Јасно, $\langle X \rangle \leq F$.
Узмимо за $\theta = i': X \to \langle X \rangle$ $(i'(x) = x)$. За њега постоји хомоморфизам $\theta': F \to \langle X \rangle$.

$$\begin{tikzcd} & F \arrow[d, "\theta'"] \\ X \arrow[ur, "i"] \arrow[r, "i'"] \arrow[dr, "i"'] & \langle X \rangle \arrow[d, "i''"] \\ & F \end{tikzcd}$$

Посматрајмо и инклузију $i'': \langle X \rangle \to F$.
Важи $i'' \circ \theta' \circ i = i$.

$$F \xrightarrow{\theta'} \langle X \rangle \xrightarrow{i''} F$$

Како (по деф.) постоји јединствени хомоморфизам за F и i то је $i'' \circ \theta'$ баш тај хомоморфизам.
Међутим, $id_F: F \to F$ такође задовољава тај услов, па је $i'' \circ \theta' = id_F$.
Дакле, $i'' \circ \theta'$ је на, па како је i'' инклузија, ово је могуће једино ако је $F = \langle X \rangle$.

T2: Ако је F_i слободна на X_i за $i \in \{1,2\}$ и $|X_1| = |X_2|$, тада $F_1 \cong F_2$.

Д: Нека је $f: X_1 \to X_2$ бијекција. Нека су $i_1: X_1 \to F_1$, $i_2: X_2 \to F_2$ инклузије.

За $i_2 \circ f: X_1 \to F_2$ постоји хомоморфизам $\theta_1: F_1 \to F_2$ ткд. $\theta_1 \circ i_1 = i_2 \circ f$
За $i_1 \circ f^{-1}: X_2 \to F_1$ постоји хомоморфизам $\theta_2: F_2 \to F_1$ ткд. $\theta_2 \circ i_2 = i_1 \circ f^{-1}$

$$\begin{tikzcd} & F_1 \arrow[dr, dashed, "\theta_1"] & \\ X_1 \arrow[ur, "i_1"] \arrow[r, "f"'] & X_2 \arrow[r, "i_2"'] & F_2 \end{tikzcd}$$

$$\begin{tikzcd} & F_2 \arrow[dr, dashed, "\theta_2"] & \\ X_2 \arrow[ur, "i_2"] \arrow[r, "f^{-1}"'] & X_1 \arrow[r, "i_1"'] & F_1 \end{tikzcd}$$

Сада имамо: $\theta_2 \circ \theta_1 \circ i_1 = \theta_2 \circ i_2 \circ f = i_1 \circ f^{-1} \circ f = i_1$.
Како је и $id_{F_1} \circ i_1 = i_1$, то је $\theta_2 \circ \theta_1 = id_{F_1}$

Аналогно, $\theta_1 \circ \theta_2 = id_{F_2}$.

Због тога, θ_1 и θ_2 су бијекције. (нашли смо им инверзе)

(већ смо доказали да су хомоморфизми, самим тим θ_1 и θ_2 су изоморфизми $\Rightarrow F_1 \cong F_2$)

деф. Hom $(G, H) = \{\theta' : G \to H \mid \theta'$ је хомоморфизам$\}$, где су G, H групе.

деф. Map $(X, G) = \{\theta : X \to G\}$, где је X произвољан скуп.

T3: Ако је F_i слободна на X_i за $i \in \{1,2\}$ и $F_1 \cong F_2$, тада $|X_1| = |X_2|$.

Д: 1° X_1 - коначан:

* Приметимо да за $i \in \{1,2\}$ постоји бијекција између $Hom(F_i, Z_2)$ и $Map(X_i, Z_2)$.

Дефинишимо ову бијекцију са $F : Hom(F_i, Z_2) \to Map(X_i, Z_2)$ са $F(\theta') = \theta' \circ i_i$

Докажимо да то заиста јесте бијекција:

$$\begin{tikzcd} & F_i \arrow[d, dashed, "\theta'"] \\ X_i \arrow[ur, "i_i"] \arrow[r, "\theta"'] & Z_2 \end{tikzcd}$$

* 1-1: $F(\theta') = F(\theta'') \Rightarrow \theta = \theta' \circ i_i = \theta'' \circ i_i$, па пошто постоји јед. такав хомоморфизам $\Rightarrow \theta' = \theta''$.
* на: Нека $\theta \in Map(X_i, Z_2)$. Тада постоји $\theta' \in Hom(F_i, Z_2)$ ткд. $\theta = \theta' \circ i_i$, па је $F(\theta') = \theta$.

Дакле, важи: $|Hom(F_1, Z_2)| = |Map(X_1, Z_2)|$ и $|Hom(F_2, Z_2)| = |Map(X_2, Z_2)|$

* Даље, како је $F_1 \cong F_2$, постоји и бијекција између $Hom(F_1, Z_2)$ и $Hom(F_2, Z_2)$

Ако је $f : F_1 \to F_2$ изоморфизам, можемо деф. биј. $\Phi : Hom(F_1, Z_2) \to Hom(F_2, Z_2)$, $\Phi(\gamma) = \gamma \circ f^{-1}$

Докажимо да Φ заиста јесте бијекција:

* 1-1: $F(\gamma_1) = F(\gamma_2) \Rightarrow \gamma_1 \circ f^{-1} = \gamma_2 \circ f^{-1} \Rightarrow \gamma_1 = \gamma_2$.
* на: Нека $\theta \in Hom(F_2, Z_2)$. Тада је $\Phi(\theta \circ f) = \theta \circ f \circ f^{-1} = \theta$.

Дакле, важи: $|Hom(F_1, Z_2)| = |Hom(F_2, Z_2)| = |Map(X_2, Z_2)| \Rightarrow$

* Закључујемо да $|Map(X_1, Z_2)| = |Hom(F_1, Z_2)| = |Hom(F_2, Z_2)| = |Map(X_2, Z_2)|$

Како је X_1 коначан, $|Map(X_1, Z_2)| = 2^{|X_1|} = |Map(X_2, Z_2)| \Rightarrow Map(X_2, Z_2)$ - коначан $\Rightarrow X_2$ - коначан

На крају, пошто $|Map(X_2, Z_2)| = 2^{|X_2|} = 2^{|X_1|}$, следи $|X_1| = |X_2|$.

2° X_1 - бесконачан:

Како је $|F_i| = |\langle X_i \rangle| \overset{(*)}{=} |X_i|$ и важи $|F_1| = |F_2|$, то је и $|X_1| = |X_2|$.

(*) по $\boxed{4}$ T4 и чињенице да је X_i бар ем пребројив.

25. Егзистенција слободне групе.

деф. Дат је скуп X чије елементе зовемо слова. Уведимо $X^- = \{x^- \mid x \in X\}$, где су x^- нова слова.

Формирамо скуп речи W_n, за свако $n \geq 0$: * $W_0 = \{\varepsilon\}$ (ε - празна реч)
* $W_n = (X \cup X^-)^n$ (скуп n-торки)

Затим посматрамо скуп редукованих речи $\tilde{W}_n \subseteq W_n$, који се састоји од елемената из W_n код којих никоје две узастопне координате нису x, x^- или x^-, x (за $x \in X$).

деф. $F(X) := \bigcup_{n \geq 0} \tilde{W}_n$

Напомене: * речи пишемо и без заграда (нпр. уместо (a,b) пишемо ab).

* за $a \in X \cup X^-$ означавамо $a^{-1} = \begin{cases} a^-, & a \in X \\ x, & a = x^- \text{ за } x \in X. \end{cases}$

* за пар $(a,b) \in (X \cup X^-)^2$ кажемо да је скратив ако је $a = b^{-1}$.

Уводимо операцију:

деф. Нека су $a = (x_1, \dots, x_l) \in \tilde{W}_l$, $b = (y_1, \dots, y_m) \in \tilde{W}_m$. Тада је $a \cdot b = (x_1, \dots, x_{l-r}, y_{r+1}, \dots, y_m)$ при чему су парови $(x_l, y_1), (x_{l-1}, y_2), \dots, (x_{l-r+1}, y_r)$ скративи, а пар (x_{l-r}, y_{r+1}) није скратив.
(спојимо речи и скраћујемо колико можемо)

Т1: $F(X)$ је слободна група над X.

Д: * $F(X)$ је група:

* добра деф. операције (затвореност): $a, b \in F(X) \Rightarrow ab \in F(X)$ (тј. и ab је редукована).
* неутрал: ε - празна реч
* инверз: за $a = (x_1, \dots, x_l)$ је $a^{-1} = (x_l^{-1}, \dots, x_1^{-1})$.

* асоцијативност: $a = (x_1, \dots, x_l) \in \tilde{W}_l$, $b = (y_1, \dots, y_m) \in \tilde{W}_m$, $c = (z_1, \dots, z_n) \in \tilde{W}_n$ $(\tilde{W}_i \subseteq F(X))$

Нека је: $a \cdot b = (x_1, \dots, x_{l-r}, y_{r+1}, \dots, y_m)$ и $b \cdot c = (y_1, \dots, y_{m-s}, z_{s+1}, \dots, z_n)$ (знамо: $r \leq a, r \leq b$, $s \leq b, s \leq c$)

Доказ изводимо „индукцијом" по укупној дужини (по $l+m+n$).

1° $r + s < m$

$(a \cdot b) \cdot c = (x_1, \dots, x_{l-r}, y_{r+1}, \dots, y_m)(z_1, \dots, z_n) = (x_1, \dots, x_{l-r}, y_{r+1}, \dots, y_{m-s}, z_{s+1}, \dots, z_n)$

$a \cdot (b \cdot c) = (x_1, \dots, x_l)(y_1, \dots, y_{m-s}, z_{s+1}, \dots, z_n) = (x_1, \dots, x_{l-r}, y_{r+1}, \dots, y_{m-s}, z_{s+1}, \dots, z_n)$

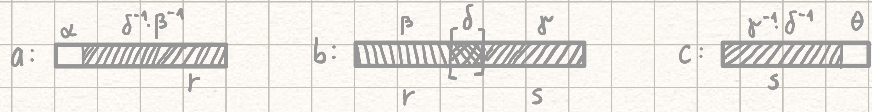
$2^\circ \quad r+s=m$

$$(a\cdot b)\cdot c = (x_1,\dots,x_{l-r},\underbrace{y_{r+1},\dots,y_m}_{\substack{m-r=s\\ m-s=r}})(z_1,\dots,z_n) = (x_1,\dots,x_{l-r},z_{s+1},\dots,z_n)$$

$$a\cdot(b\cdot c) = (x_1,\dots,x_l)\,(\overbrace{y_1,\dots,y_{m-s}},z_{s+1},\dots,z_n) = (x_1,\dots,x_{l-r},z_{s+1},\dots,z_n)$$

(Случајеви $r=0, s=m$ и $r=m, s=0$ су такође обухваћени овим)

$3^\circ \quad r+s>m$



$$(a\cdot b)\cdot c = (\alpha\gamma)c \overset{(\text{„ux"})}{=} \alpha(\gamma c) = \alpha(\gamma\gamma^{-1}\delta^{-1}\theta) = \alpha(\delta^{-1}\theta)$$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \| \ (\text{„ux"})$

$$a\cdot(b\cdot c) = a(\beta\theta) \overset{(\text{„ux"})}{=} (a\beta)\theta = (\alpha\delta^{-1}\beta^{-1}\beta)\theta = (\alpha\delta^{-1})\theta$$

* $F(X)$ је слободна група:

$$\begin{tikzcd} & F(X) \arrow[d, "\theta'"] \\ X \arrow[ur, "i"] \arrow[r, "\theta"'] & G \end{tikzcd}$$

Нека је G произвољна група и $\theta: X\to G$.
Желимо да докажемо постоји јединствени хомоморфизам $\theta': F(X)\to G$ ткд. $(\theta'\circ i)(a)=\theta(a)$ (за $a\in X$)
тј. $\theta'(a)=\theta(a)$, за $a\in X$

Дефинишемо: $\theta': F(X)\to G$, $\theta'(\underbrace{x_1,\dots,x_l}_{\in\tilde{W}_l}) = \theta'(x_1)\dots\theta'(x_l)$, где $\theta'(x_i) = \begin{cases}\theta(x_i), & x_i\in X\\ \theta(x_i^{-1})^{-1}, & x_i\in X^-\end{cases}$

* За θ' важи поменути услов (јер $(\theta'\circ i)(a) = \theta'(i(a)) = \theta'(a) = \theta(a)$, $a\in X$, не X^-).
* θ' је хомоморфизам:

* добра деф.: $(x_1,\dots,x_l) = (y_1,\dots,y_l) \Rightarrow \theta'(x_1,\dots,x_l) = \theta'(x_1)\dots\theta'(x_l) = \theta'(y_1)\dots\theta'(y_l) = \theta'(y_1,\dots,y_l)$

* хомоморфизам: $a=(x_1,\dots,x_l)$, $b=(y_1,\dots,y_m)$ и $ab=(x_1,\dots,x_{l-r},y_{r+1},\dots,y_m)$.

$$\theta'(ab) = \theta'(x_1)\dots\theta'(x_{l-r})\,\theta'(y_{r+1})\dots\theta'(y_m)$$

$$\theta'(a)\theta'(b) = \theta'(x_1)\dots\theta'(x_{l-r})\underbrace{\theta'(x_{l-r+1})\dots\theta'(x_l)\theta'(y_1)\dots\theta'(y_r)}_{(*)}\theta'(y_{r+1})\dots\theta'(y_m)$$

$$= \theta'(x_1)\dots\theta'(x_{l-r})\,\theta'(y_{r+1})\dots\theta'(y_m)$$

(*) (x_l, y_1) - скратив $\Rightarrow$ 1° $x_l\in X$, $y_1 = x_l^{-1} \Rightarrow \theta'(x_l)\,\theta'(y_1) = \theta(x_l)\,\theta((x_l^{-1})^{-1})^{-1} = \theta(x_l)\theta(x_l)^{-1} = \varepsilon$
(аналогно остали) 2° $y_1\in X$, $x_l = y_1^{-1} \Rightarrow \theta'(x_l)\,\theta'(y_1) = \theta((y_1^{-1})^{-1})^{-1}\,\theta(y_1) = \theta(y_1)^{-1}\theta(y_1) = \varepsilon$

* θ' је једини такав хомоморфизам:

$\theta'(x_1,\dots,x_l) = \theta'(x_1)\dots\theta'(x_l)$.
Свако $\theta'(x_i)$ је или $\theta(x_i)$ или $\theta(x_i^{-1})^{-1}$, ткд. израз десно не зависи од θ' (тј. избора хом.)
па постоји највише један овакав хомоморфизам. (сви су једнаки)

T3: Свака група изоморфна је количнику неке слободне групе.

Д: Нека је G група. Посматрајмо слободну групу над G, тј. $F(G)$.

Тада за $id_G : G \to G$ и $i : G \to F(G)$ постоји хомоморфизам $f : F(G) \to G$ ткд. $f \circ i = id_G$

Одавде, за све $g \in G$ следи $g = id_G(g) = (f \circ i)(g) = f(g)$, па је f на, тј. $\mathrm{Im} f = G$.

По I т.о.и.: $F(G)/\mathrm{Ker} f \cong \mathrm{Im} f = G$, што је и требало доказати.