Алгебра 2

Јован Самарџић, 13/2019

Професор: Марко Радовановић

- дефиниције
- ознаке
- теореме
- докази
- примери

Година курса: 2021/22

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

1. Дејство групе

деф. **Дејство групе** G на непразном скупу X је хомоморфизам $\rho: G \to \mathcal{S}_X$. (1)

деф. Пресликавање $\theta: G \times X \to X$ је **дејство групе** G на непразном скупу X ако: (2)

1) $\theta(e, x) = x$, $\forall x \in X$, e - неутрал групе G;

2) $\theta(g, \theta(h,x)) = \theta(gh, x)$, $\forall g, h \in G$ $\forall x \in X$.

Напомена: Ове две дефиниције су еквивалентне.

Доказ: ($\Rightarrow$) Нека је ρ дејство по деф. 1.
Дефинишимо $\theta(g,x) := \underbrace{\rho(g)}_{\text{ово је нека пермутација}}(x)$, $\forall g \in G$, $\forall x \in X$.

Важи: 1) $\theta(e,x) = \rho(e)(x) \overset{\rho\text{-хом.}}{=} id_X(x) = x$;

2) $\theta(g, \theta(h,x)) = \rho(g)(\theta(h,x)) = \rho(g)(\rho(h)(x)) = (\rho(g) \circ \rho(h))(x) \overset{\rho\text{-хом.}}{=} \rho(gh)(x) = \theta(gh, x)$.

($\Leftarrow$) Нека је θ дејство по деф. 2.
Дефинишимо $\rho(g)(x) := \theta(g,x)$, $\forall g \in G$, $\forall x \in X$.

* Покажимо да је ова деф. добра, тј. $\rho(g) \in \mathcal{S}_X$.

* 1-1: $\rho(g)(x) = \rho(g)(y) \Rightarrow \theta(g,x) = \theta(g,y) \Rightarrow \theta(g^{-1}, \theta(g,x)) = \theta(g^{-1}, \theta(g,y))$

$\overset{2)}{\Rightarrow} \theta(gg^{-1}, x) = \theta(gg^{-1}, y) \Rightarrow \theta(e,x) = \theta(e,y) \Rightarrow x = y$;

* на: Нека је $y \in X$. Тражимо $x \in X$ ткд. $y = \rho(g)(x) = \theta(g,x)$

$\overset{/\cdot\theta(g^{-1},\cdot)}{\Longrightarrow} \theta(g^{-1}, y) = \theta(g^{-1}, \theta(g,x)) \overset{2)}{=} \theta(g^{-1}g, x) = \theta(e,x) = x$.

Затим: $\theta(g,x) = \theta(g, \theta(g^{-1}, y)) = \theta(gg^{-1}, y) = \theta(e,y) = y$.

* Покажимо да је ρ хомоморфизам, тј. $\rho(g) \circ \rho(h) = \rho(gh)$

$(\rho(g) \circ \rho(h))(x) = \rho(g)(\rho(h)(x)) = \rho(g)(\theta(h,x)) = \theta(g, \theta(h,x)) \overset{2)}{=} \theta(gh, x) = \rho(gh)(x)$.

Напомена: Уместо $\theta(g,x)$ писаћемо $g \cdot x$. Дакле: 1) $e \cdot x = x$;
2) $g \cdot (h \cdot x) = (gh) \cdot x$.

деф. Ако G дејствује на X, пишемо $G \curvearrowright X$.

деф. Нека $G \curvearrowright X$. **Орбита елемента** $x \in X$ је $\Omega(x) := \{g \cdot x \mid g \in G\} \subseteq X$; (или $\mathrm{Orb}(x)$)

Стабилизатор елемента $x \in X$ је $G_x := \{g \in G \mid g \cdot x = x\}$. (или $\mathrm{Stab}(x)$)

деф. $x \sim y$ акко $x \in \Omega(y)$. (то је релација на X)

Напомена: $\sim$ је релација еквиваленције.

Доказ: (Р) $x = e \cdot x \Rightarrow x \in \Omega(x)$;

(С) $x \sim y \Rightarrow x \in \Omega(y) \Rightarrow x = g \cdot y \Rightarrow g^{-1} \cdot x = g^{-1} \cdot (g \cdot y) \overset{2)}{=} (g^{-1}g) \cdot y = e \cdot y = y \Rightarrow y \in \Omega(x) \Rightarrow y \sim x$;

(Т) $x \sim y,\ y \sim z \Rightarrow x = g \cdot y,\ y = h \cdot z \Rightarrow x = g \cdot (h \cdot z) \overset{2)}{=} (gh) \cdot z \Rightarrow x \in \Omega(z) \Rightarrow x \sim z$.

Напомена: Класе еквиваленције у односу на релацију $\sim$ су баш орбите, тј. $\Omega(x)$.
То значи да орбите чине партицију скупа X.

Самим тим, важи: 1) $\forall x, y \in X \quad \Omega(x) \cap \Omega(y) = \emptyset$ или $\Omega(x) = \Omega(y)$;

2) $\forall x \in X \quad x \in \Omega(x)$;

3) **I класна једначина:** $\sum_{x \in T} |\Omega(x)| = |X|$ (T је трансверзала партиције)

деф. Скуп свих орбита означавамо са X/G.

деф. Ако неко дејство има само једну орбиту, оно је **транзитивно**.

2. Примене дејства групе

Теорема 1 (Теорема о орбити и стабилизатору):

Нека је $G \curvearrowright X$. Тада је за свако $x \in X$:

1) $G_x \leq G$;
2) постоји бијекција између G/G_x и $\Omega(x)$.

Доказ: 1) * Нека су $g, h \in G_x$: $g \cdot x = x$, $h \cdot x = x$ $\Rightarrow$ $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$ $\Rightarrow$ $gh \in G_x$;

* $e \cdot x \overset{1)}{=} x$ $\Rightarrow$ $e \in G_x$;

* Нека је $g \in G_x$: $g \cdot x = x$ $\Rightarrow$ $g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$ $\Rightarrow$ $g^{-1} \in G_x$.

Дакле: $G_x \leq G$.

2) Дефинишимо $f: G/G_x \to \Omega(x)$ са $f(gG_x) = g \cdot x$

* добра деф: $gG_x = hG_x \Leftrightarrow g^{-1}h \in G_x \Leftrightarrow (g^{-1}h) \cdot x = x \Leftrightarrow g^{-1} \cdot (h \cdot x) = x$

$\overset{/g \cdot \square}{\Rightarrow}$ $g \cdot (g^{-1} \cdot (h \cdot x)) = g \cdot x \Leftrightarrow (gg^{-1}) \cdot (h \cdot x) = e \cdot (h \cdot x) = h \cdot x = g \cdot x$

$\Leftrightarrow f(gG_x) = f(hG_x)$;

* 1-1: Довољно је доказати да из $g \cdot (g^{-1} \cdot (h \cdot x)) = g \cdot x$ $\overset{(/g^{-1} \cdot \square)}{\text{следи}}$ $g^{-1} \cdot (h \cdot x) = x$. (јер су остало еквиваленције)

А то следи из: $g^{-1} \cdot (g \cdot (g^{-1} \cdot (h \cdot x))) = g^{-1} \cdot (g \cdot x) \overset{2)}{=} x$

$(g^{-1}g)(g^{-1} \cdot (h \cdot x)) = g^{-1} \cdot (h \cdot x)$.

* на: тривијално (по деф. f)

Последица: Ако $G \curvearrowright X$ и G је коначна $\Rightarrow$ $\forall x \in X$ $|\Omega(x)| \cdot |G_x| = |G|$.

Доказ: $|\Omega(x)| \overset{T1.2)}{=} |G/G_x| = [G : G_x] = \frac{|G|}{|G_x|}$.

↑ Лагранжова теорема

Теорема 2 (Кошијева): (већ изведи на АЛГ1, али сада доказ преко дејстава)

Нека је G коначна група и p прост број који дели њен ред.

Тада у G постоји елемент реда p.

Доказ: Посматрамо скуп $X = \{(g_0, \dots, g_{p-1}) \in G^p \mid g_0 \dots g_{p-1} = e\}$.
Пре свега, приметимо: $|X| = |G|^{p-1}$ (првих $p-1$ бирамо, а $g_{p-1} = (g_0 \dots g_{p-2})^{-1}$)

Дефинишемо дејство групе $\mathbb{Z}_p$ на X: $n \cdot (g_0, \dots, g_{p-1}) = (g_{n+p\,0}, \dots, g_{n+p\,(p-1)})$ (тривијално је дејство)
По Т1: $\forall x \in X$ је $|\Omega(x)| \cdot |G_x| = |\mathbb{Z}_p| = p \Rightarrow |\Omega(x)| \in \{1, p\}$.

Са друге стране, орбите чине партицију скупа X $\Rightarrow$ $|X| = |\Omega_1| + \dots + |\Omega_k|$
($|X|$ дели се са p; $|\Omega_1|, \dots, |\Omega_k| \in \{1, p\}$; S)

Знамо да је $(e, \dots, e) \in X$ и $|\Omega(e, \dots, e)| = 1$.
То значи да у S постоји бар још једно i ткд. $|\Omega_i| = 1$.

Тада је $\Omega_i = \{(g, \dots, g)\}$ при чему $g^p = e \Rightarrow \omega(g) \mid p \overset{g \neq e}{\Rightarrow} \omega(g) = p$
↳ мора бити овог облика (иначе $n+p$ да поремети)

Теорема 3: Нека је $G \curvearrowright X$.
Ако за неке $x, y \in X$ важи $\Omega(x) = \Omega(y)$, тада су G_x и G_y конјуговане подгрупе.

Доказ:

Доказ. Из услова $\Omega(x) = \Omega(y)$ следи да је $x \in \Omega(y)$, тј. $x = g \cdot y$, за неко $g \in G$. Докажимо да је

$$\Sigma_x = g \Sigma_y g^{-1}. \quad \leftarrow \text{ово доказујемо}$$

$$\begin{aligned} h \in \Sigma_x &\iff h \cdot x = x \Leftrightarrow h \cdot (g \cdot y) = g \cdot y \\ &\xrightarrow{g^{-1}(\,)} g^{-1} \cdot (h \cdot (g \cdot y)) = g^{-1} \cdot (g \cdot y) \\ &\xrightarrow{2)} (g^{-1} h g) \cdot y = y \\ &\Leftrightarrow g^{-1} h g \in \Sigma_y \\ &\Leftrightarrow h \in g \Sigma_y g^{-1}. \end{aligned}$$

Да би доказ био потпун, треба доказати да важи импликација ($\Leftarrow$) у другом реду. Као и малопре, дејствујемо на обе стране једнакости са g и применом услова (1) и (2) из дефиниције дејства добијамо тражену импликацију.

деф. **Центар групе** је $Z(G) := \{ g \in G \mid \forall a \in G \quad ga = ag \}$.

деф. **Класа конјугованости** елемента $a \in G$ је $K_a = \{ gag^{-1} \mid g \in G \}$

Теорема 4 (II класна једначина):

Нека је G коначна група и $k_1, \dots, k_n$ бројеви елем. класа конј. са бар два елемента ове групе.

$$|G| = |Z(G)| + k_1 + \dots + k_n$$

Из то: $k_i \mid |G|$.

Доказ: Посматрамо дејство групе G на саму себе (тј. $X = G$) задато са $g \cdot a = gag^{-1}$ (тривијално јесте дејство)

Јасно: $\Omega(a) = K_a \overset{T1}{\Rightarrow} |\Omega(a)| \cdot |G_a| = |G| \Rightarrow |\Omega(a)| = |K_a| \mid |G| \Rightarrow k_i \mid |G|$

Такође, како орбите чине партицију скупа G $\Rightarrow$ $|G| = l + k_1 + \dots + k_n$

↳ број једночланих класа конј.
а са АЛГ1 знамо $l = |Z(G)|$
↳ 16 T2

деф. Нека је $H \leq G$. Уочимо скуп $X = \{ \underbrace{gHg^{-1}}_{S} \mid g \in G \}$ свих подгрупа S од G конјугованих са H.

Дејствујмо групом G на скуп X конјуговањем, тј: $g \cdot S = gSg^{-1}$.

Стабилизатор за подгрупу $H \overset{H \in X}{\nearrow}$ зове се **нормализатор подгрупе** H:

$$N(H) := \{ g \in G \mid gHg^{-1} = H \} = G_H$$

Теорема 5: 1) Ово дејство је транзитивно;

2) $|X| = [G : N(H)]$.

Доказ: 1) тривијално: $\Omega(H) = \{ g \cdot H \mid g \in G \} = \{ gHg^{-1} \mid g \in G \} = X$

2) Означимо $\Omega = \Omega(H)$ јер је орбита јединствена.

Важи: $|\Omega| \cdot |G_H| = |G|$, а како је $N(H) = G_H$ и $\Omega = X$, тврђење је тачно

3. Одређивање броја орбита

деф. Нека је $G \curvearrowright X$ и $g \in G$.
Фиксни скуп елемента g је скуп: $X^g := \{x \in X \mid g \cdot x = x\}$.

Пишемо и $\mathrm{Fix}(g)$.

Лема 1: Нека је $G \curvearrowright X$.
Ако су g и h конјуговани, тада постоји бијекција између X^g и X^h.

Доказ: Нека је $g = khk^{-1}$, $k \in G$.
Докажимо да је $F: X^g \to X^h$, $F(x) = k^{-1} \cdot x$ бијекција.

* добра деф: $x_1 = x_2 \Rightarrow k^{-1}x_1 = k^{-1}x_2$.
* 1-1: $k^{-1}x_1 = k^{-1}x_2 \Rightarrow k \cdot (k^{-1} \cdot x_1) = k \cdot (k^{-1} x_2) \Rightarrow (kk^{-1}) \cdot x_1 = (kk^{-1}) \cdot x_2 \Rightarrow e \cdot x_1 = e \cdot x_2 \Rightarrow x_1 = x_2$
* на: $y \in X^h \Rightarrow h \cdot y = y \overset{\text{конј.}}{\Rightarrow} \underbrace{k^{-1}gk}_{\in X} \cdot y = y$. Дакле $\forall y \in X^h \ \exists x \in X^g$ ($x = gk \cdot y$) $k^{-1}x = y$.

Теорема 1 (Бернсајдова лема):

Нека је G коначна и X коначан скуп ткд. $G \curvearrowright X$. Тада је:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Доказ:

Доказ. Посматрајмо скуп

$$S = \{(g, x) \in G \times X \mid g \cdot x = x\}.$$

Тада је

$$S = \bigsqcup_{g \in G} \{g\} \times X^g = \bigsqcup_{x \in X} \Sigma_x \times \{x\}.$$

или узмемо све g-ове и њихове Fix
или узмемо све x-ове и њихове Stab

Сада је

$$|S| = \boxed{\sum_{g \in G} |X^g|} = \sum_{x \in X} \boxed{|\Sigma_x|} = \sum_{x \in X} \boxed{\frac{|G|}{|\Omega(x)|}} = (\star).$$

Нека су $\Omega_1, \Omega_2, \ldots, \Omega_k$ све различите орбите, тј. елементи из X/G. Тада је

$k = |X/G|$

$$(\star) = \sum_{i=1}^{k} \sum_{x \in \Omega_i} \frac{|G|}{|\Omega(x)|} = \sum_{i=1}^{k} \sum_{x \in \Omega_i} \frac{|G|}{|\Omega_i|} = \sum_{i=1}^{k} |\Omega_i| \cdot \frac{|G|}{|\Omega_i|} = \underbrace{k} \cdot \underbrace{|G|}.$$

Пример: вежбе, задатак 12: бојење темена шестоугла са k различитих боја:

Група $\langle p \rangle$ (подгрупа од D_6) дејствује на скуп $S = \{(a_0, a_1, a_2, a_3, a_4, a_5) \mid 1 \le a_i \le k\}$

4. Теореме Силова

Теорема 1 (Прва теорема Силова):

Нека је $|G| = p^r m$. Тада за свако $s \leq r$ постоји $H \leq G$ реда p^s.

Такође, број таквих подгрупа је $s_p = 1 + pk$. (даје остатак 1 при дељењу са p)

Доказ:

Доказ. Посматрајмо $X = \{S \subseteq G \mid |S| = p^s\}$ (фамилија) и дејство групе G на X задато са $g \cdot S = gS$. Тада је

$|S| = p^s$ па од $|G|$ бирамо $|S|$

$$|X| = \binom{|G|}{p^s} = \binom{mp^r}{p^s} = \frac{mp^r(mp^r-1)\ldots(mp^r-p^s+1)}{p^s(p^s-1)\ldots 2\cdot 1} \quad (\text{читамо})$$

$$= mp^{r-s}\prod_{i=1}^{p^s-1}\frac{mp^r-i}{i}$$

хоћемо да одредимо $|X|$ (тј. колико има таквих подскупова)

Запишемо у општем облику $i = m_i p^{l_i}$, где је $p \nmid m_i$, $l_i < s \leqslant r$

$$= mp^{r-s}\underbrace{\prod_{i=1}^{p^s-1}\frac{mp^{r-l_i}-m_i}{m_i}}_{A}. \quad (\star) \qquad \left(\frac{mp^r - m_i p^{l_i}}{m_i p^{l_i}}\right)$$

Приметимо да је:

$$\left[mA\prod_{i=1}^{p^s-1}m_i\right] \overset{(\star)}{=} \left[m\prod_{i=1}^{p^s-1}(mp^{r-l_i}-m_i)\right] \equiv_p \left[m(-1)^{p^s-1}\prod_{i=1}^{p^s-1}m_i\right]$$

Како $p \nmid \prod_{i=1}^{p^s-1} m_i$, то је

$p \neq 2 \Rightarrow p^{s-1}$ парно $\Rightarrow 1$; $p=2 \Rightarrow 2^{s-1}$ непарно $\Rightarrow -1$, тј. $m \equiv_2 -m$

$$[mA] \equiv_p [m(-1)^{p^s-1}] \equiv_p [m]$$

одакле следи да је $mA = pt + m$, за неки цео број t. Сад то уврстимо у $(\star)$ и добијемо да је

$$|X| = p^{r-s}(pt+m).$$

mA

* Нека су $\Omega_1, \Omega_2, \ldots, \Omega_k$ све различите орбите. Тада је

$$|\Omega_1| + |\Omega_2| + \ldots + |\Omega_k| = |X| = p^{r-s}(pt+m). \quad (\star\star)$$

Одавде закључујемо да постоји орбита $\Omega(S)$ таква да $p^{r-s+1} \nmid |\Omega(S)|$ (јер $p \nmid m$)

Такође: $|\Sigma_S| \cdot |\Omega(S)| = |G| = mp^r \overset{\text{стаб.}}{\Rightarrow} p^s \mid |\Sigma_S| \Rightarrow |\Sigma_S| \geqslant p^s$

С друге стране, за $g \in \Sigma_S$ је $gS = S$, па за свако $h \in S$ важи $gh \in S$. Следи да је $\Sigma_S h \subseteq S$ а како важи $|gY| = |Y|$, за произвољни елемент g и коначан скуп Y, то је

$$|\Sigma_S| = |\Sigma_S h| \leqslant |S| = p^s.$$

(логично: косет има онолико елем. колико и скуп)

сендвич

Дакле, $|\Sigma_S| = p^s$ и важи $\Sigma_S h = S$.

$$h^{-1}\Sigma_S h = h^{-1}S, \quad (\text{једно } h \Rightarrow \text{једно } H)$$

H

па је $H \leqslant G$ и $|H| = p^s$ (нашли подгрупе). Како је $h^{-1}S \in \Omega(S)$ (јер $h \in S$), то је

$$\Omega(S) = \Omega(h^{-1}S) = \Omega(H) \overset{\text{део } \Omega}{=} \{gH \mid g \in G\}.$$

Дакле, $\Omega(S)$ садржи тачно једну подгрупу H реда p^s (јер ако је $g \in H$, онда је $gH = H$. (2°) Ако је $g \notin H$, онда мора бити и $g^{-1} \notin H$, па $e \notin gH$. Дакле, gH неће бити подгрупа од G) (1°)

Тиме смо успоставили бијекцију између подгрупа реда p^s (њих има s_p) и орбита чији број елемената није дељив са p^{r-s+1}.

Приметимо на крају да из $|\Sigma_S| = p^s$ следи

$$|\Omega(S)| = \frac{|G|}{|\Sigma_S|} = mp^{r-s},$$

користећи то и $(\star\star)$ имамо да је

$$s_p mp^{r-s} + bp^{r-s+1} = p^{r-s}(pt+m),$$

- Имамо s_p орбита чији бр. елем. није дељив са p^{r-s+1} (због успостављене бијекције)
- и имамо орбите које чији бр. елем. јесте дељив (има их $bp \cdot k^{p^{r-s+1}} = bp^{r-s+1}$)

одакле следи да је

$$p(t-b) = m(s_p - 1), \quad \overset{p \nmid m}{\Rightarrow} \quad p \mid s_p - 1$$

деф. Нека је $|G| = p^r \cdot m$ (p - прост, $p \nmid m$)

Подгрупа $H \leq G$ реда p^r је **Силовљева / S_p - подгрупа** од G.

Теорема 2 (Друга теорема Силова):

Нека је $|G| = p^r m$. Тада је свака подгрупа од G реда p^s ($s \leq r$) подгрупа неке S_p - подгрупе.

Уз то, све S_p - подгрупе су међусобно конјуговане.

Такође, важи и $r_p = [G : N(H)]$ (H је нека S_p - подгрупа) и $r_p \mid m$.

↓
исто што и S_p само за $s=r$ (p^r)

Доказ:

Доказ. Нека је $H \leqslant G$ подгрупа са p^s елемената и S нека p-подгрупа од G. Тада дефинишемо дејство $H \circlearrowright X$, где је $X = \{gS \mid g \in G\}$, са

$|H| = p^s$; G/S ; $h \cdot gS = hgS$. ↷ дејство H на G/S

Нека су Ω_i, $1 \leqslant i \leqslant k$, различите орбите при овом дејству, тада важи

$$|\Omega_1| + |\Omega_2| + \ldots + |\Omega_k| = |X| = [G : S] = m.$$ ← $|S| = p^r$

Како за свако $T \in X$ важи $|\Omega(T)| \cdot |\Sigma_T| = |H|$, то је $|\Omega(T)| = p^l$, за неко $0 \leqslant l \leqslant s$. Из претходног реда и чињенице да $p \nmid m$ следи да постоји i такво да је $p \nmid |\Omega_i|$, односно $|\Omega_i| = 1$. Нека је $T = gS$ ← фиксирамо такво да $|\Omega(T)| = 1$, тада је $\Omega(T) = \{T\}$, тј. за све $h \in H$ важи $hT = T$, односно $hgS = gS$.

конјугат подгрупе је подгрупа ; $\overset{/\cdot g^{-1}}{\Rightarrow}$; $h \underbrace{gSg^{-1}}_{K} = gSg^{-1}$, ; $hK = K$; $\Rightarrow$; $h \in K$. ; $H \leqslant K$; $|K| = |S|$

а како је $K \leqslant G$ $\Rightarrow$ $h \in K$. Закључујемо да је $H \leqslant K$, а како је $|K| = |S|$, то је први део тврђења доказан. Нека је сада H такође p-подгрупа. Из претходног је $H \leqslant gSg^{-1}$, па из $|H| = |gSg^{-1}|$ следи да је $H = gSg^{-1}$. Дакле, ако је S једна p-подгрупа, скуп свих p-подгрупа је

$$\{gSg^{-1} \mid g \in G\},$$

а он има $[G : N(S)]$ елемената по 2. особини нормализатора. На крају, важи $S \leqslant N(S) \leqslant G$, па је ← нормализатор је стабилизатор

$$\underbrace{[G : N(S)]}_{r_p} \cdot [N(S) : S] = [G : S] = m$$

одакле следи да $r_p \mid m$.

Последица: За S_p - подгрупу H од G важи: $H \trianglelefteq G \Leftrightarrow r_p = 1$ (јединствена је)

Доказ: $r_p = 1 \overset{T2}{\Leftrightarrow} [G : N(H)] = 1 \Leftrightarrow |N(H)| = |G_H| = |G| \Leftrightarrow \forall g \in G \; gHg^{-1} = H$, тј. $H \trianglelefteq G$.

нормализатор је стабилизатор

5. Теорема о разлагању

* Подсетник:

Лема 1 (Теорема о разлагању):

Нека су $H_1, \dots, H_k \leq G$ такве да: 1) $H_1 \dots H_k = G$
2) $(H_1 \dots H_i) \cap H_{i+1} = \{e\}$
3) $h_i h_j = h_j h_i$, $\forall h_i \in H_i,\ h_j \in H_j,\ 1 \leq i < j \leq k$

Тада је G директан производ тих подгрупа, тј: $G \cong H_1 \times \dots \times H_k$.

* Теорема 1 (посебно случај Силовљевих подгрупа):

Коначна група G је директан производ својих S_p-подгрупа акко су све те подгрупе нормалне.

Доказ: Нека је $|G| = p_1^{\alpha_1} \dots p_k^{\alpha_k}$

($\Rightarrow$) Нека је H_i, $1 \leq i \leq k$, S_{p_i}-подгрупа од G ткд. је G директ. производ од $H_1, \dots, H_k$

Тада свако $g \in G$ може да се запише као $g = h_1 h_2 \dots h_k$, где $h_i \in H_i$ (по Л1.1)

$$gH_i = h_1 \dots h_k H_i \overset{Л1.3}{=} h_i h_1 \dots h_{i-1} h_{i+1} \dots h_k H_i \overset{Л1.3}{\underset{1 \text{ по } 1}{=}} h_i H_i h_1 \dots h_{i-1} h_{i+1} \dots h_k$$

$$\overset{h_i \in H_i}{=} H_i h_i h_1 \dots h_{i-1} h_{i+1} \dots h_k \overset{Л1.3}{\underset{1 \text{ по } 1}{=}} H_i h_1 \dots h_k = H_i g \quad \Rightarrow \quad H_i \circ G.$$

($\Leftarrow$) Нека је H_i S_{p_i} - подгрупа од G реда $p_i^{\alpha_i}$. Пошто $H_i \trianglelefteq G \overset{\text{4T2}}{\Rightarrow}$ H_i је једина S_{p_i} - подгрупа.

Довољно је да докажемо 3 својства из Л1:

1) Нека је $g \in G$ и $|G| = p_1^{\alpha_1} \dots p_k^{\alpha_k} = n$.

Како је $\text{НЗД}\left(\frac{n}{p_1^{\alpha_1}}, \dots, \frac{n}{p_k^{\alpha_k}}\right) = 1 \Rightarrow \exists m_1, \dots, m_k \in \mathbb{Z} \quad m_1 \frac{n}{p_1^{\alpha_1}} + \dots + m_k \frac{n}{p_k^{\alpha_k}} = 1$

$$\Rightarrow g = g^{m_1 \frac{n}{p_1^{\alpha_1}} + \dots + m_k \frac{n}{p_k^{\alpha_k}}} = \left(g^{\frac{n}{p_1^{\alpha_1}}}\right)^{m_1} \dots \left(g^{\frac{n}{p_k^{\alpha_k}}}\right)^{m_k} = g_1^{m_1} \dots g_k^{m_k}$$

Приметимо: $g_i^{(p_i^{\alpha_i})} = g_i^n = e \Rightarrow \omega(g_i) = p_i^{\beta_i}$, за неко $\beta_i \leq \alpha_i$

$$\Rightarrow |\langle g_i \rangle| = p_i^{\beta_i}$$

По 4T2: $\langle g_i \rangle$ је подгрупа неке S_{p_i} - подгрупе $\Rightarrow \langle g_i \rangle \leq H_i$, тј. $g_i \in H_i$

Дакле, заиста је $g \in H_1 H_2 \dots H_k$

3) Посматрамо $h_i \in H_i$, $h_j \in H_j$: $[h_i, h_j] = \underbrace{h_i}_{\in H_i} \underbrace{h_j h_i^{-1} h_j^{-1}}_{\in H_i \ (\text{јер } H_i \trianglelefteq G)} \in H_i \cap H_j$

По Лагранжу: $|H_i \cap H_j| \mid |H_i|, |H_j| \Rightarrow H_i \cap H_j = \{e\} \Rightarrow [h_i, h_j] = e \Rightarrow h_i h_j = h_j h_i$.

2) Довољно је доказати $|H_1 \dots H_i| = p_1^{\alpha_1} \dots p_i^{\alpha_i}$

(зато што знамо $|H_{i+1}| = p_{i+1}^{\alpha_{i+1}}$, па закључак следи на исти начин као у 3)

НАПОМЕНА: $H_1 H_2 \dots H_i$ јесте подгрупа од G зато што $H_1, \dots, H_i \trianglelefteq G \Rightarrow$ може Лагранж

То показујемо (тоталном) индукцијом:

$(j<i \Rightarrow i)$ $H_1 \dots H_i = \{h_1 \dots h_i \mid h_1 \in H_1, \dots, h_i \in H_i\}$ има $p_1^{\alpha_1} \dots p_i^{\alpha_i}$ елем. (сви $h_1 h_2 \dots h_i$ различити)

$h_1 \dots h_i = h_1' \dots h_i' \Rightarrow \underbrace{(h_1')^{-1} h_1 \dots (h_{i-1}')^{-1} h_{i-1}}_{\in H_1 \dots H_{i-1}} = \underbrace{h_i' h_i^{-1}}_{H_i} \overset{j<i}{=} e \Rightarrow h_i = h_i'$ итд.

6. Полудиректан производ група

деф. Нека је G група и $N, H \leq G$.
G је (унутрашњи) полудиректни производ група N и H, у ознаци $G = N \rtimes H$, ако:

1) $NH = G$;

2) $N \cap H = \{e\}$;

3) $N \trianglelefteq G$. (само једна)

Пример: $N = \{\varepsilon, \rho, \dots, \rho^{n-1}\} \trianglelefteq D_n$, $H = \{\varepsilon, \sigma\} \Rightarrow D_n = N \rtimes H$

Теорема 1: Нека је $G = N \rtimes H$. Тада је $G/N \cong H$.

Такође, сваки елемент $g \in G$ се јединствено може записати у облику nh. $(n \in N, h \in H)$

Доказ: * Подсетимо се II теореме о изоморфизму: $H \leq G$, $N \trianglelefteq G \Rightarrow N \cap H \trianglelefteq H$ и $NH/N \cong H/N \cap H$.

У нашем случају: $G/N \cong H/\{e\}$, тј. $G/N \cong H$.

* Из $NH = G \Rightarrow \exists n \in N \ \exists h \in H \ g = nh$

Докажимо и јединственост: $nh = n'h' \Rightarrow \underbrace{(n')^{-1}n}_{\in N} = \underbrace{h^{-1}h'}_{\in H} \overset{N \cap H = \{e\}}{\Rightarrow} n = n', \ h = h'$

Теорема 2: Нека је $\phi: H \to \mathrm{Aut}(N)$ хомоморфизам група.

Уведимо операцију $\cdot$ на скупу $N \times H$ са: $(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot \phi(h_1)(n_2),\ h_1 h_2)$.

1) $(N \times H, \cdot)$ је група, тзв. (спољашњи) полудиректни производ група N и H: $N \rtimes_\phi H$.

2) Нека је $\mathcal{N} = N \times \{e_H\}$, $\mathcal{H} = \{e_N\} \times H$.
Тада је $N \rtimes_\phi H$ унутрашњи полудир. производ $\mathcal{N}$ и $\mathcal{H}$, тј. $\mathcal{N} \rtimes \mathcal{H} = N \rtimes_\phi H$.

Доказ: 1)

* *Операција $\cdot$ је асоцијативна.*

$$\begin{aligned}((n_1,h_1)\cdot(n_2,h_2))\cdot(n_3,h_3) &= (n_1\Phi(h_1)(n_2),h_1h_2)\cdot(n_3,h_3)\\ &= (n_1\Phi(h_1)(n_2)\Phi(h_1h_2)(n_3),h_1h_2h_3)\\ (n_1,h_1)\cdot((n_2,h_2),(n_3,h_3)) &= (n_1,h_1)\cdot(n_2\Phi(h_2)(n_3),h_2h_3)\\ &= (n_1\Phi(h_1)(n_2\Phi(h_2)(n_3)),h_1h_2h_3)\\ &= (n_1\Phi(h_1)(n_2)\Phi(h_1)(\Phi(h_2)(n_3)),h_1h_2h_3)\\ &= (n_1\Phi(h_1)(n_2)(\Phi(h_1)\circ\Phi(h_2))(n_3),h_1h_2h_3)\\ &= (n_1\Phi(h_1)(n_2)\Phi(h_1h_2)(n_3),h_1h_2h_3).\end{aligned}$$

Приметимо да смо у преласку са четвртог на пети и са шестог на седми ред користили да је Φ хомоморфизам.

* *Постојање неутрала.* Неутрал за ову групу је, интуитивно, елемент (e_N, e_H). Званично, показујемо да је овај елемент и леви и десни неутрал. Заиста, како је пресликавање Φ хомоморфизам, важи

$$(n,h)\cdot(e_N,e_H) = (n\Phi(h)(e_N),he_H) = (ne_N,h) = (n,h).$$

Слично,

$$(e_N,e_H)(n,h) = (e_N\Phi(e_H)(n),e_Hh) = (e_N id_N(n),h) = (e_Nn,h) = (n,h).$$

* *Постојање инверза.* Означимо са (n',h') инверз од (n,h). Пошто је

$$(n',h')\cdot(n,h) = (n'\Phi(h')(n),h'h) = (e_N,e_H),$$

одмах имамо да је $h' = h^{-1}$. Затим је

$$n'\Phi(h')(n) = e_N \ \Rightarrow\ n' = (\Phi(h')(n))^{-1} = \Phi(h^{-1})(n^{-1})$$

Битно: $(n,h)^{-1} = (\phi(h^{-1})(n^{-1}),\ h^{-1})$

2) Прво проверимо да су $\mathcal{N}$ и $\mathcal{H}$ заиста подгрупе од $N \rtimes_\phi H$ $\quad (A \le B \iff a_1^{-1}a_2 \in A)$

$$(n_1,e_H)^{-1}\cdot(n_2,e_H) = (\phi(e)^{-1}(n_1^{-1}),\ e_H)\cdot(n_2,e_H) = (n_1^{-1},e_H)(n_2,e_H) = (n_1\phi(e)(n_2),\ e_H)$$

$$= (n_1^{-1}n_2,\ e_H) \in \mathcal{N} \qquad \text{(аналогно за } \mathcal{H})$$

Показујемо три својства из деф. $N \rtimes H$ (са почетка питања):

1) $(n,e)\cdot(e,h) = (n\phi(e)(e),\ h) = (n,h) \quad \Rightarrow \quad \mathcal{N}\mathcal{H} = N \rtimes_\phi H$

2) $\mathcal{N} \cap \mathcal{H} = \{(e,e)\}$: очигледно

3) $(n',h')\cdot(n,e)\cdot(n',h')^{-1} = (n'\phi(h')(n),\ h')\cdot(\phi(h')^{-1}(n'^{-1}),\ (h')^{-1})$

$$= (\underbrace{n'\cdot\phi(h')(n)\cdot\phi(h')(\phi(h')^{-1}(n'^{-1}))}_{\in N},\ e) \in \mathcal{N} \quad \Rightarrow \quad \mathcal{N} \lhd N \rtimes_\phi H$$

Теорема 3: Нека је $G = N \rtimes H$.
Тада је $N \rtimes_\phi H \cong G$, где је $\phi: H \to \mathrm{Aut}(N)$ задат са: $\phi(h)(n) = hnh^{-1}$.

Доказ: * Прво приметимо да је ϕ заиста добро деф, тј. да заиста $\phi(h) \in \mathrm{Aut}\, N$:

Пошто $N \trianglelefteq G \Rightarrow hnh^{-1} \in N, \forall h \in H \Rightarrow \phi(h)(n) \in N, \forall h \in H \Rightarrow \phi(h): N \to N$

* Докажимо да је $F: N \rtimes_\phi H \to G$ задато са $F(n,h) = nh$ изоморфизам:

→ хомоморфизам: $F((n_1,h_1)\cdot(n_2,h_2)) = F(n_1\phi(h_1)(n_2), h_1h_2) = F(n_1h_1n_2h_1^{-1}, h_1h_2)$

$= n_1h_1n_2h_1^{-1}h_1h_2 = n_1h_1n_2h_2 = F(n_1,h_1)\cdot F(n_2,h_2)$

→ бијекција: тривијално, јер се свако $g \in G$ јединс. може записати као nh (по T1)

7. Кратки тачни низови група

деф. У овом питању, тривијалну групу $\{e\}$ ћемо означавати са 1.

деф. Нека су G, H, N групе.

Тада је $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} H \to 1$ **кратак тачан низ** група ако су $\alpha: N \to G$, $\beta: G \to H$ хомоморфизми тд.:

1) α је 1-1;

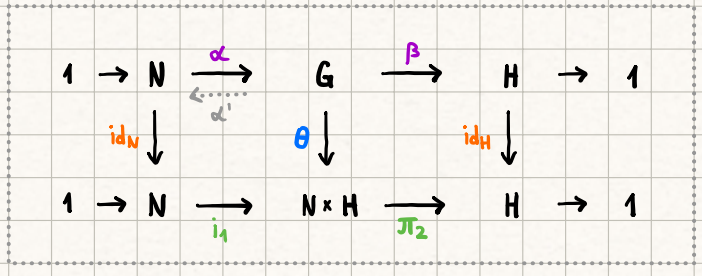
2) β је на;

3) $\operatorname{Im}\alpha = \operatorname{Ker}\beta$. (дакле $\beta(\alpha(n)) = e_H$, $\forall n \in N$)

Теорема 1: Нека је $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} H \to 1$ кратак тачан низ група. Следеће је еквивалентно:

1) Постоји хомоморфизам $\alpha': G \to N$, $\alpha' \circ \alpha = id_N$;

2) Постоји изоморфизам $\theta: G \to N \times H$, тд. следећи дијаграм комутира:



при чему је $i_1: N \to N \times H$ инклузија задата са $i_1(n) = (n, e)$

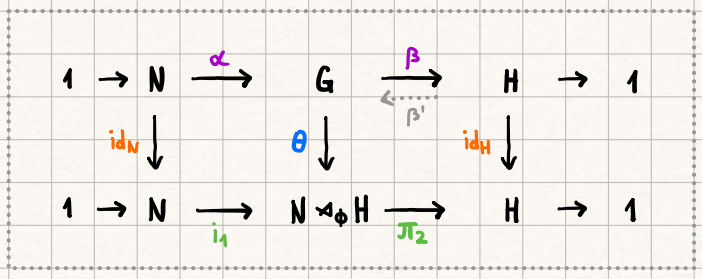
и $\pi_2: N \times H \to H$ пројекција задата са $\pi_2(n, h) = h$.

Доказ: сличан као доказ следеће теореме.

Теорема 2: Нека је $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} H \to 1$ кратак тачан низ група. Следеће је еквивалентно:

1) Постоји хомоморфизам $\beta' : H \to G$, $\quad \beta \circ \beta' = id_H$;

2) Постоји хомоморфизам $\phi : H \to Aut(N)$
и изоморфизам $\theta : G \to N \rtimes_\phi H$ ткд. следећи дијаграм комутира:



Доказ:

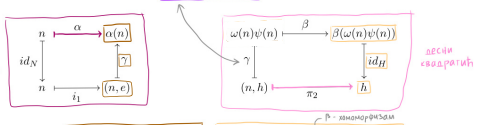
Доказ.

(1) ⇒ (2) Конструисаћемо Φ и изоморфизам $\gamma : N \rtimes_\Phi H \to G$ такво да је (θ ће бити инверзија овога)

($\Phi : H \to Aut(N)$ – хомоморф.)

$$\gamma \circ i_1 \circ id_N = \alpha \text{ и } id_H \circ \beta \circ \gamma = \pi_2.$$

Пресликавање γ тражимо у облику $\gamma(n,h) = \omega(n)\psi(h)$. Желимо да је



Дакле, мора бити $\alpha(n) = \gamma(n,e) = \omega(n)\psi(e)$ и $h = \beta(\omega(n)\psi(n)) = \beta(\omega(n))\beta(\psi(h))$. (β - хомоморфизам) Узимо да је $\psi = \beta'$ и $\omega = \alpha$ и проверимо да ли су испуњени претходни услови. Прво важи $\psi(e) = \beta'(e) = e$, јер је β' хомоморфизам. Даље, ($\alpha(n) \cdot \alpha(n)^{-1} = e$ ✓)

$$\beta(\omega(n))\beta(\psi(n)) = \underbrace{\beta(\alpha(n))}_{e}\,\underbrace{\beta(\beta'(h))}_{h} = h,$$

јер је $\operatorname{Im}\alpha = \operatorname{Ker}\beta$. Дакле, за пресликавање $\gamma(n,h) = \alpha(n)\beta'(h)$ дијаграм комутира.

Одредимо $\Phi : H \to \operatorname{Aut}(N)$ такво да је γ хомоморфизам. Важи

$$\begin{aligned}\gamma((n_1,h_1)(n_2,h_2)) &= \gamma(n_1\Phi(h_1)(n_2), h_1h_2)\\ &= \alpha(n_1\Phi(h_1)(n_2))\beta'(h_1h_2)\\ &\overset{\alpha,\beta'\text{-хом.}}{=} \alpha(n_1)\alpha(\Phi(h_1)(n_2))\beta'(h_1)\beta'(h_2)\end{aligned}$$

С друге стране,

$$\gamma(n_1,h_1)\gamma(n_2,h_2) = \alpha(n_1)\beta'(h_1)\alpha(n_2)\beta'(h_2).$$

Да би γ био хомоморфизам довољно је да важи

$$\alpha(n_1^{-1})\alpha(\Phi(h_1)(n_2))\beta'(h_1)\beta'(h_2) = \alpha(n_1^{-1})\beta'(h_1)\alpha(n_2)\beta'(h_2), \quad / \cdot \beta'(h_1)^{-1}$$

односно

$$\alpha(\Phi(h_1)(n_2)) = \beta'(h_1)\alpha(n_2)\beta'(h_1)^{-1}.$$

Дакле, да бисмо дефинисали $\Phi(h_1)(n_2)$ потребно је да постоји $m \in N$ такво да је (α и $N \to G$; $\Phi(h_1)(n_2)$ ће бити m)

$$\alpha(m) = \beta'(h_1)\alpha(n_2)\beta'(h_1)^{-1},$$

односно

$$\beta'(h_1)\alpha(n_2)\beta'(h_1)^{-1} \in \operatorname{Im}\alpha = \operatorname{Ker}\beta. \quad \text{тј. } \beta(\dots) = e$$

(иначе Φ неће бити хомоморфизам)

(одмах видимо да ће бити)

Међутим, из чињенице да је β хомоморфизам, да је $(\beta \circ \alpha)(n) = e$, за свако $n \in N$ и да је $\beta \circ \beta' = id_H$, то је

$$\beta(\beta'(h_1)\alpha(n_2)\beta'(h_1)^{-1}) = h_1eh_1^{-1} = e,$$

па тражено m постоји и јединствено је јер је α 1-1 (по деф.). Дакле, Φ је дефинисано на следећи начин

$$\alpha(\Phi(h)(n)) = \beta'(h)\alpha(n)\beta'(h)^{-1}.$$

– $\Phi(h)$ је аутоморфизам за све $h \in H$. (тј. добра дефинисаност)

* Покажимо прво да је $\Phi(h)$ хомоморфизам. Како је α „1-1“, довољно је да важи (само додали α споља, то мање јер је α 1-1)

$$\alpha(\Phi(h)(n_1n_2)) = \alpha(\Phi(h)(n_1)\Phi(h)(n_2)),$$

а то важи јер је

$$\begin{aligned}\alpha(\Phi(h)(n_1)\Phi(h)(n_2)) &\overset{\alpha\text{-хом.}}{=} \alpha(\Phi(h)(n_1))\alpha(\Phi(h)(n_2))\\ &= \beta'(h)\alpha(n_1)\,\beta'(h)^{-1}\beta'(h)\alpha(n_2)\beta'(h)^{-1}\\ &\overset{\alpha\text{-хом.}}{=} \beta'(h)\alpha(n_1n_2)\beta'(h)^{-1}\\ &= \alpha(\Phi(h)(n_1n_2)).\end{aligned}$$

* $\Phi(h)$ је "1-1": ако је $\Phi(h)(n_1) = \Phi(h)(n_2) \overset{/\alpha(\cdot)}{\Rightarrow} \alpha(\Phi(h)(n_1)) = \alpha(\Phi(h)(n_2))$
$\Rightarrow \beta'(h)\alpha(n_1)\beta'(h)^{-1} = \beta'(h)\alpha(n_2)\beta'(h)^{-1}$, тј. $\alpha(n_1) = \alpha(n_2) \Rightarrow n_1 = n_2$. ($\alpha$ је 1-1)

* НА: Доказујемо да за свако $m \in N$ постоји $n \in N$ такво да $\Phi(h)(n) = m$, тј. $/\alpha(\cdot)$
$\beta'(h)\alpha(n)\beta'(h)^{-1} = \alpha(m) \overset{\alpha(n) = \beta'(h)^{-1}\alpha(m)\beta'(h)}{\Leftrightarrow}$
тј. довољно је да важи $\beta'(h)^{-1}\alpha(m)\beta'(h) \in \operatorname{Im}\alpha = \operatorname{Ker}\beta$, што важи као пре

– Φ је хомоморфизам. (исто као пре)

Показујемо да је

$$\Phi(h_1h_2)(n) = (\Phi(h_1) \circ \Phi(h_2))(n) = \Phi(h_1)(\Phi(h_2)(n)),$$

односно да је

$$\alpha(\Phi(h_1h_2)(n)) = \alpha(\Phi(h_1)(\Phi(h_2)(n))),$$

а то важи јер

$$\begin{aligned}\alpha(\Phi(h_1)(\Phi(h_2)(n))) &= \beta'(h_1)\alpha(\Phi(h_2)(n))\beta'(h_1)^{-1}\\ &= \beta'(h_1)\beta'(h_2)\alpha(n)\beta'(h_2)^{-1}\beta'(h_1)^{-1}\\ &\overset{\beta'\text{-хом.}}{=} \beta'(h_1h_2)\alpha(n)\beta'(h_1h_2)^{-1}\\ &= \alpha(\Phi(h_1h_2)(n)).\end{aligned}$$

γ је изоморфизам. ($\gamma : N \rtimes_\Phi H \to G$)

* Да је γ хомоморфизам изабрали смо при конструкцији Φ. ✓

* 1-1:
$$\begin{aligned}\gamma(n_1,h_1) = \gamma(n_2,h_2) &\Rightarrow \alpha(n_1)\beta'(h_1) = \alpha(n_2)\beta'(h_2)\\ &\Rightarrow \alpha(n_2)^{-1}\alpha(n_1) = \beta'(h_2)\beta'(h_1)^{-1}\\ &\overset{\alpha\text{-хом.}}{\Rightarrow} \alpha(n_2n_1^{-1}) = \beta'(h_2h_1^{-1}) \qquad (*)\\ &\overset{/\beta(\cdot)}{\Rightarrow} \underbrace{\beta(\alpha(n_2^{-1}n_1))}_{e} = \underbrace{\beta(\beta'(h_2h_1^{-1}))}_{h_2h_1^{-1}}\\ &\Rightarrow h_1 = h_2.\end{aligned}$$

А онда по (*): $\alpha(n_2n_1^{-1}) = \beta'(e) = e \overset{\alpha\text{ 1-1}}{\Rightarrow} n_1 = n_2$

* НА. За $g \in G$, тражимо $(n,h) \in N \rtimes_\Phi H$ ткд:

$$g = \gamma(n,h) = \alpha(n)\beta'(h)$$

$$/\beta(\cdot) \Rightarrow \beta(g) = \beta(\alpha(n)\beta'(h)) \overset{\beta\text{-хом.}}{=} \underbrace{\beta(\alpha(n))}_{e}\underbrace{\beta(\beta'(h))}_{h} = h.$$

Дакле, довољно је наћи $n \in N$ такво да је $g = \alpha(n)\beta'(\beta(g))$, тј. $\alpha(n) = g\beta'(\beta(g))^{-1}$.

тј. $g\beta'(\beta(g))^{-1} \in \operatorname{Im}\alpha = \operatorname{Ker}\beta$,

То важи јер: $\beta(g\beta'(\beta(g))^{-1}) = \beta(g)\underbrace{\beta(\beta'(\beta(g)^{-1}))}_{\beta(g)^{-1}} \overset{\beta\text{-хом.}}{=} \beta(g)\beta(g)^{-1} = e.$

Конструисали смо γ тако да дијаграм комутира. Дефинишимо $\theta = \gamma^{-1}$, што је легитимно јер је γ бијекција и хомоморфизам. За ово θ је довољно показати да дијаграм комутира, тј. да је $\theta \circ \alpha = i_1 \circ id_N$ и $\pi_2 \circ \theta = id_H \circ \beta$. (гледати слику из формулације)

Знамо $\gamma \circ i_1 \circ id_N = \alpha$,

$$/\theta\circ \Rightarrow \theta \circ \alpha = \theta \circ \gamma \circ i_1 \circ id_N = i_1 \circ id_N.$$

Слично, знамо $id_H \circ \beta \circ \gamma = \pi_2$

$$/\circ\theta \Rightarrow \pi_2 \circ \theta = id_H \circ \beta \circ \gamma \circ \theta = id_H \circ \beta.$$

(2) ⇒ (1) Нека је $\gamma = \theta^{-1}$. Слично као малопре, покаже се да за γ дијаграм комутира, ако комутира за θ
Дефинишемо $\beta'(h) = \gamma(e,h)$. Овако дефинисано β' је хомоморфизам, јер (γ^{-1} изморф.)

$$\beta'(h_1h_2) = \gamma(e,h_1h_2) \overset{\gamma\text{ изморф.}}{=} \gamma(e,h_1)\gamma(e,h_2) = \beta'(h_1)\beta'(h_2),$$

Користећи комутативност десног квадратића, имамо

$$(\beta \circ \beta')(h) = \beta(\beta'(h)) = \beta(\gamma(e,h)) = \underbrace{id_H}_{\text{додали}}(\beta(\gamma(e,h))) = \pi_2(e,h) = h,$$

чиме је доказ завршен.

Теорема 3: Нека је H циклична група и $\phi, \psi : H \to Aut(N)$ мономорфизми ткд. $\phi(H) = \psi(H)$.

Тада је: $N \rtimes_\phi H \cong N \rtimes_\psi H$.

8. Комутативни прстени са јединицом

деф. Алгебарска структура $(A, +, \cdot, 1)$ типа $(2,2,0)$ је **комутативни прстен са јединицом** ако:

1) $(A, +)$ је Абелова група;

2) $(A, \cdot, 1)$ је комутативни моноид;

3) $x \cdot (y+z) = x \cdot y + x \cdot z$, $\forall x, y, z \in A$

деф. Неутрал за $+$ означавамо са 0.

Примери: 1) $(\mathbb{Z}, +, \cdot, 1)$

2) $(\mathbb{Z}[X], +, \cdot, 1)$

3) $(\mathbb{Z}_n, +_n, \cdot_n, 1)$

4) $(M_n(R), +, \cdot, E)$ - није комутативан (за $n \geq 2$)

Теорема 1: 1) $a \cdot 0 = 0$;

2) Ако је $0 = 1 \Rightarrow A = \{0\}$

Доказ: 1) $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0 \Rightarrow a \cdot 0 = 0$;

2) Нека је $a \in A$. Тада је $a = a \cdot 1 = a \cdot 0 \overset{1)}{=} 0 \Rightarrow A = \{0\}$.

↳ неутрал за $\cdot$

* деф. Елемент $a \in A$ је **делитељ нуле** ако постоји $b \in A \setminus \{0\}$ ткд. $ab = 0$.
Специјално, ако је $a \neq 0$, он је **прави делитељ нуле**.

Скуп свих делитеља нуле у кпј A означавамо са $Z(A)$.

Пример: 1) $Z(\mathbb{Z}) = \{0\}$ 2) $Z(\mathbb{Z}_6) = \{0, 2, 3, 4\}$

* деф. Елемент $a \in A$ је **регуларан** ако: $\forall x, y \in A \quad a \cdot x = a \cdot y \Rightarrow x = y$.

Скуп свих регуларних елем. у кпј A означавамо са $R(A)$.

Теорема 2: $A = Z(A) \sqcup R(A)$.

Доказ: * Нека $a \in Z(A) \Rightarrow \exists b \neq 0 \quad ab = 0$; Знамо и: $a \cdot 0 = 0$ $\Rightarrow a \cdot 0 = a \cdot b$, али $b \neq 0 \Rightarrow a \notin R(A)$;

* Нека $a \notin Z(A)$. Претпоставимо $a \cdot b = a \cdot c \Rightarrow a \cdot (b - c) = 0 \overset{a \notin Z(A)}{\Rightarrow} b = c \Rightarrow a \in R(A)$.

* деф. Елемент $a \in A$ је **инвертибилан** ако: $\exists b \in A \quad a \cdot b = 1$
Инверз од a означавамо са a^{-1}.

Скуп свих инвертибилних елем. у кпј A означавамо са $U(A)$.

Теорема 3: $U(A) \subseteq R(A)$.

Доказ: Нека $a \in U(A)$. Претпоставимо $a \cdot b = a \cdot c \overset{/a^{-1}}{\Rightarrow} b = c \Rightarrow a \in R(A)$.

У општем случају, обрнуто не важи (нпр. $U(\mathbb{Z}) = \{1, -1\}$, $R(\mathbb{Z}) = \mathbb{Z} \setminus \{0\}$)

Теорема 4: Ако је A коначан кпј, онда $R(A) = U(A)$.

Доказ: Показујемо само $R(A) \subseteq U(A)$, $|A| < \infty$

Нека $a \in R(A) \Rightarrow \{a \cdot x \mid x \in A\}$ има све различите елементе $\Rightarrow$ има исти бр. елем. као A (овде користимо $|A| < \infty$)
$\Rightarrow \{a \cdot x \mid x \in A\} = A$

Дакле: $1 \in \{a \cdot x \mid x \in A\} \Rightarrow \exists x \in A \quad a \cdot x = 1 \Rightarrow a \in U(A)$

Теорема 5: $(U(A), \cdot)$ је група.

Доказ: Пошто $1 \in U(A) \Rightarrow U(A) \neq \emptyset \Rightarrow \exists a, b \in U(A)$. Докажимо $a^{-1}b \in U(A)$:

$a^{-1}b \cdot \underline{b^{-1}a} = a^{-1} \cdot 1 \cdot a = a^{-1} \cdot a = 1 \Rightarrow$ има инверз $\Rightarrow a^{-1}b \in U(A)$

деф. Нека је A кпј.

Ако је $Z(A) = \{0\}$, кажемо да је A **домен / област целих.**

Ако је $U(A) = A \setminus \{0\}$, кажемо да је A **поље.**

Пример: 1) $\mathbb{Z}$, $\mathbb{Z}[X]$ су домени; 2) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ су поља.
$(\mathbb{Z}_n, +_n, \cdot_n, 1)$ је поље $\Leftrightarrow$ n је прост.

Напомена: поље $\Rightarrow$ домен.

деф. Кпј $(B, +, \cdot, 1)$ је **потпрстен** кпј $(A, +, \cdot, 1)$ ако је његова алгебарска подструктура.

деф. **Хомоморфизам кпј.** је $f: A \to B$ ткд:

1) $f(a_1 + a_2) = f(a_1) +' f(a_2)$;

2) $f(a_1 \cdot a_2) = f(a_1) \cdot' f(a_2)$;

3) $f(1) = 1'$.

деф. **Изоморфизам кпј** је хомоморфизам кпј. који је бијективан.
Ако постоји изоморфизам између кпј A и B, пишемо $A \cong B$.

Теорема 6: $A \cong B \Rightarrow U(A) \cong U(B)$.

Доказ:

Доказ. Нека је $f : A \to B$ изоморфизам комутативних прстена са јединицом. Нека је пресликавање $g : U(A) \to U(B)$ дефинисано са $g(a) = f(a)$. Покажимо да је g добро дефинисано односно $a \in U(A)$ ако и само ако је $f(a) \in U(B)$.

($\Rightarrow$) Нека је $a \in U(A)$. Тада постоји $b \in A$ такво да је $ab = 1$. Сада је

$$1 = f(1) = f(ab) = f(a)f(b), \quad \Rightarrow \quad f(a) \in U(B)$$

(f хом.)

($\Leftarrow$) Нека је $f(a) \in U(B)$, тада постоји $b \in B$ такво да је $f(a)b = 1$. Како је f „НА“, то постоји $b' \in A$ такво да је $b = f(b')$. Сад је

$$f(1) = 1 = f(a)f(b') \overset{f\ хом.}{=} f(ab'), \quad \overset{f\ 1\text{-}1}{\Rightarrow} \quad ab' = 1 \quad \Rightarrow \quad a \in U(A)$$

Покажимо сада да је g хомоморфизам група. То важи јер

$$g(ab) = f(ab) \overset{f\ хом.}{=} f(a)f(b) = g(a)g(b).$$

Остаје још да испитамо да је g бијекција. Ако је $g(a) = g(b)$, онда је $f(a) = f(b)$, па је $a = b$. $\Rightarrow$ 1-1
Нека је $b \in U(B)$. Тада је $b = f(a)$, за неко $a \in A$, јер је f „НА“. и при томе је $a \in U(A)$ по доказаном. Дакле, $b = f(a) = g(a)$.

(f хом.)

* **деф.** Нека је R домен.
За $a, b \in R$, $a \neq 0$ кажемо да a **дели** b, $a|b$, ако постоји $c \in R$ ткд. $b = c \cdot a$.

9. Идеали кпј

деф. Нека је A кпј и $I \subseteq A$, $I \neq \emptyset$. Тада је I **идеал** од A, $I \trianglelefteq A$, ако важи:

1) $x+y \in I$, $\forall x,y \in I$

2) $a \cdot x \in I$, $\forall a \in A$, $x \in I$

Напомена: $I \trianglelefteq A \Rightarrow 0 \in I$ (јер $a \in I \Rightarrow (-1)\cdot a \in I \Rightarrow a-a \in I$)

Напомена: За сваки кпј. A су $\{0\}$ и A његови идеали.

деф. Нека је A кпј. и $x \in A$.

Скуп $\langle x \rangle := \{ax \mid a \in A\}$ је **идеал генерисан са x / главни идеал.** (тривијално јесте идеал)

Примери: 1) $A = \mathbb{Z}$. Тада је $I = \langle n \rangle = n\mathbb{Z}$ (скуп бројева дељивих са n)

Сваки идеал у $\mathbb{Z}$ је главни, јер за $I \trianglelefteq \mathbb{Z}$ важи $(I,+) \leq (\mathbb{Z},+)$,
а како је $\mathbb{Z}$ циклична, знамо да су јој и подгрупе цикличне, тј. облика $\langle n \rangle = n\mathbb{Z}$.

2) $A = \mathbb{Z}[X]$. Тада је $I = \{ P(X) \mid a_0$ је паран, $P(x) \in \mathbb{Z}[X] \}$ идеал, али није главни.

* $p+q \in I$, $\forall p,q \in I$
  $rp \in I$, $\forall r \in \mathbb{Z}[X]$, $p \in I$ (слободан члан остаје паран)

* ппс. $I = \langle f \rangle$, $f \in \mathbb{Z}[X] \Rightarrow 2 \in I = \langle f \rangle \Rightarrow \exists g \in \mathbb{Z}[X]$ $fg = 2$
  Значи f, g су константни полиноми и то $f \in \{1,-1,2,2\}$

  1° $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}[X] \neq I$ ↯
  2° $\langle 2 \rangle = \langle -2 \rangle$ не садржи нпр. полином $2+X$ (који припада I) ↯

Теорема 1: I садржи неки инвертибилан елемент $\Leftrightarrow$ $I = A$

Доказ: ($\Leftarrow$) тривијално

($\Rightarrow$) Нека $i \in I \cap U(A)$ и $a \in A$ $\Rightarrow$ $a = (a\underbrace{i^{-1}}_{\in I \text{ (по 2)}}) \cdot i$ $\Rightarrow$ $a \in I$

Последица: Ако је F поље, једини идеали у F су $\{0\}$ и F.

Доказ: ппс. $I \lhd F$, $I \neq \{0\}$, $I \neq F$

$x \in I \overset{x \in F}{\Rightarrow} \exists x' \; x' \cdot x = 1 \overset{2)}{\Rightarrow} 1 \in I \overset{T1}{\Rightarrow} I = F.$

Теорема 2: Ако је F поље, сваки идеал у $F[X]$ је главни.

Доказ: Знамо да важи теорема о кол. и остатку: $\forall f, g \in F[X]$, $g \neq 0$ $\exists q, r \in F[X]$ $f = gq + r$, $\deg r < \deg g$.

По томе, за $I \lhd F[X]$ важи $I = \langle f \rangle$, где је f неки ненула полином најнижег степена из I.

↳ Заиста, $\forall g \in I$ $g = fq + r$, $\deg r < \deg f$ $\overset{r = g - fq \in I}{\Rightarrow}$ $r = 0$ $\Rightarrow$ $\forall g \in I$ $g = fq$

деф. Нека су I, J идеали кпј. A.

Тада дефинишемо: 1) $I + J := \{x + y \mid x \in I, \; y \in J\}$ – min идеал који садржи $I \cup J$.

2) $I \cdot J := \{x_1 y_1 + \ldots + x_n y_n \mid n \in \mathbb{N}, \; x_i \in I, \; y_j \in J\}$ – min идеал који садржи све xy.

Теорема 3: 1) $I \cap J$ је идеал; (може и општије)
2) $I + J$ је идеал;
3) $I \cdot J$ је идеал.

Доказ: тривијално по деф.

Теорема 4: У прстену $\mathbb{Z}$ важи: 1) $\langle n \rangle \cap \langle m \rangle = \langle \text{НЗС}(n,m) \rangle$;
2) $\langle n \rangle + \langle m \rangle = \langle \text{НЗД}(n,m) \rangle$;
3) $\langle n \rangle \cdot \langle m \rangle = \langle nm \rangle$.

Доказ:

1. $\langle n \rangle \cap \langle m \rangle = \langle \text{NZS}(n,m) \rangle$, јер $n \mid a$ и $m \mid a$ ако и само ако $\text{NZS}(n,m) \mid a$.
2. $\langle n \rangle + \langle m \rangle = \langle \text{NZD}(n,m) \rangle$.

($\subseteq$) Означимо са $d = \text{NZD}(n,m)$. Нека је $a \in \langle n \rangle + \langle m \rangle$ тј. $a = b + c$, где $n \mid b$ и $m \mid c$. Како $d \mid n$ и $d \mid m$, то $d \mid b$ и $d \mid c$, одакле следи да $d \mid a$, односно $a \in \langle d \rangle$. Следи $\langle n \rangle + \langle m \rangle \subseteq \langle d \rangle$.

($\supseteq$) С друге стране, према Безуовој релацији постоје $u, v \in \mathbb{Z}$ такви да $un + vm = d$ па како је $un \in \langle n \rangle$, односно $vm \in \langle m \rangle$, то је $\langle d \rangle \subseteq \langle n \rangle + \langle m \rangle$.

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

Очигледно је $\langle n \rangle \cdot \langle m \rangle \subseteq \langle nm \rangle$, јер је сваки елемент из $\langle n \rangle \langle m \rangle$ дељив са nm. Такође, $nm \in \langle n \rangle \cdot \langle m \rangle$, па важи и $\langle nm \rangle \subseteq \langle n \rangle \cdot \langle m \rangle$.

10. Хомоморфизми кпј

Подсетимо се из [8]

деф. **Хомоморфизам кпј.** је $f: A \to B$ ТКД:

1) $f(a_1 + a_2) = f(a_1) +' f(a_2)$;

2) $f(a_1 \cdot a_2) = f(a_1) \cdot' f(a_2)$;

3) $f(1) = 1'$.

деф. $\operatorname{Ker} f := \{a \in A \mid f(a) = 0\}$

$\operatorname{Im} f := \{f(a) \mid a \in A\}$

Теорема 1: 1) $\operatorname{Ker} f \lhd A$;

2) $J \lhd B \Rightarrow f^{-1}[J] \lhd A$;

3) ако је f на и $I \lhd A \Rightarrow f[I] \lhd B$.

Доказ:

Доказ.

(1) Нека су $x, y \in \operatorname{Ker} f \Rightarrow f(x) = f(y) = 0$

$\Rightarrow f(x+y) = f(x) + f(y) = 0 + 0 = 0, \Rightarrow x+y \in \operatorname{Ker} f$

За $a \in A$ и $x \in \operatorname{Ker} f$ важи

$$f(ax) = f(a)f(x) = f(a) \cdot 0 = 0.$$

Дакле, $\operatorname{Ker} f \lhd A$.

(2) Посматрајмо произвољне $x, y \in f^{-1}[J] \Rightarrow f(x), f(y) \in J$

$\Rightarrow f(x+y) = f(x) + f(y) \in J, \Rightarrow x+y \in f^{-1}[J]$

Слично, за $a \in A, x \in f^{-1}[J]$ важи

$$f(ax) = \underbrace{f(a)}_{\in B}\underbrace{f(x)}_{\in J} \in J.$$

Значи, $f^{-1}[J] \lhd A$.

(3) Коначно, нека су $u, v \in f[I]$. $\Rightarrow u = f(x), v = f(y)$

$$u + v = f(x) + f(y) = f(x+y) \in f[I].$$

За $b \in B, u \in f[\mathbf{I}]$ важи $u = f(x)$, $b = f(y)$ за неке $x \in I$ и $y \in A$, пошто је f „НА“. Тада

$$bu = f(y)f(x) = f(\underbrace{yx}_{\in I}) \in f[I],$$

Напомена: Услов f је НА је неопходан. (нпр. $f: \mathbb{Z} \to \mathbb{Q}$, $f(x) = x$)

деф. Нека је A кпј и $I \lhd A$.

Дефинишемо релацију (на A) **конгруентно по модулу I** са: $x \equiv y \pmod I \Leftrightarrow x-y \in I$

Теорема 2: $\equiv$ је **конгруенција** на A (рел. екв. и „слаже се" са $+$ и $\cdot$)

Доказ:

(P) Важи $a \equiv a \pmod I$, јер $a - a = 0 \in I$.

(C) Нека је $a \equiv b \pmod I$. Тада је $a - b \in I$, па је $b - a = (-1)(a - b) \in I$, те је $b \equiv a \pmod I$.

(T) Нека је $a \equiv b \pmod I$ и $b \equiv c \pmod I$. Тада је $a-b \in I$, $b-c \in I$, па је $a-c = a-b+b-c \in I$. Имамо да је $a \equiv c \pmod I$.

$+$: Нека је $a_1 \equiv b_1 \pmod I$ и нека је $a_2 \equiv b_2 \pmod I$. То значи да је $a_1 - b_1 \in I$, $a_2 - b_2 \in I$, па је $a_1 + a_2 - (b_1 + b_2) \in I$ тј. $\boxed{a_1 + a_2 \equiv b_1 + b_2 \pmod I}$.

$\cdot$: Такође, како је $I \lhd A$, важи $\boxed{a_2 \ (a_1 - b_1) \in I}$ (по 2) из деф. идеала) и аналогно $\boxed{b_1(a_2 - b_2) \in I}$ па је $a_1a_2 - b_1b_2 = a_2(a_1 - b_1) + b_1(a_2 - b_2) \in I$ тј. $\boxed{a_1a_2 \equiv b_1b_2 \pmod I}$.

Приметимо: По деф. релације важи $b \equiv a \pmod I \Leftrightarrow b = a+x$, $x \in I$

То значи да су класе еквиваленције C_a заправо леви косети подгрупе $(I,+)$ групе $(A,+)$.

Тиме су дефинисане операције: 1) $(a+I) + (b+I) = (a+b) + I$
2) $(a+I) \cdot (b+I) = (ab) + I$
3) $1 = 1 + I$

Теорема 3: $(A/I, +, \cdot)$ (скуп косета) је кпј

Доказ: тривијално по деф.

Теорема 4 (Теорема о изоморфизму за прстене):

Нека је $f: A \to B$ хомоморфизам кпј. Тада је $F: A/\underbrace{Ker f}_{\text{постоји јер } Ker f \lhd A} \to Im f$, $F(a + ker f) = f(a)$ изоморфизам кпј

тј. $A/ker f \cong Im f$

Доказ: * добро деф ($\Rightarrow$) и 1-1 ($\Leftarrow$): $a_1 + ker f = a_2 + ker f \overset{\equiv}{\Leftrightarrow} a_1 - a_2 \in ker f \Leftrightarrow f(a_1 - a_2) \overset{f \text{ хом.}}{=} f(a_1) - f(a_2) = 0$

$\Leftrightarrow f(a_1) = f(a_2)$

$\Leftrightarrow F(a_1 + ker f) = F(a_2 + ker f)$

* НА: тривијално

* хомоморфизам: тривијално по деф.

11. Директан производ КПЈ

деф. Нека су $(A_1, +_1, \cdot_1, 1_1), \dots, (A_n, +_n, \cdot_n, 1_n)$ КПЈ.

Тада на скупу $A = A_1 \times \dots \times A_n$ дефинишемо операције:

→ $(a_1, \dots, a_n) + (a_1', \dots, a_n') = (a_1 +_1 a_1', \dots, a_n +_n a_n')$;

→ $(a_1, \dots, a_n) \cdot (a_1', \dots, a_n') = (a_1 \cdot_1 a_1', \dots, a_n \cdot_n a_n')$;

→ $1 = (1_1, \dots, 1_n)$.

Теорема 1: $(A, +, \cdot, 1)$ је КПЈ.

Доказ: тривијално по деф.

Напомена: 1) $0 = (0_1, \dots, 0_n)$;
2) $-(a_1, \dots, a_n) = (-a_1, \dots, -a_n)$.

Теорема 2: $A_i \cong A_i'$, $1 \le i \le n$ $\Rightarrow$ $A_1 \times \dots \times A_n \cong A_1' \times \dots \times A_n'$.

Доказ: тривијално: докажемо да је $f(a_1, \dots, a_n) = (f_1(a_1), \dots, f_n(a_n))$ изоморфизам КПЈ.

Теорема 3: $U(A) = U(A_1) \times \dots \times U(A_n)$.

Доказ: Нека је $a = (a_1, \dots, a_n)$.

$$a \in U(A) \Leftrightarrow \exists b \in A \ \ ab = 1 \Leftrightarrow \exists b_1 \in A_1, \dots, b_n \in A_n \ \ (a_1 b_1, \dots, a_n b_n) = 1$$
$$\Leftrightarrow \exists b_1 \in A_1, \dots, b_n \in A_n \ \ a_1 b_1 = 1_1, \dots, a_n b_n = 1_n$$
$$\Leftrightarrow a_1 \in U(A_1), \dots, a_n \in U(A_n)$$
$$\Leftrightarrow a = (a_1, \dots, a_n) \in U(A_1) \times \dots \times U(A_n)$$

Последица: Ако је $НЗД(n, m) = 1$, онда $\varphi(nm) = \varphi(n)\varphi(m)$

Доказ: Са АЛГ1 знамо $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$ (уз. прости)

$\Rightarrow U(\mathbb{Z}_{nm}) \cong U(\mathbb{Z}_n) \times U(\mathbb{Z}_m)$, а знамо $U(\mathbb{Z}_{nm}) = \phi(nm)$

$\Rightarrow \varphi(nm) = |\phi(nm)| = |U(\mathbb{Z}_n) \times U(\mathbb{Z}_m)| = |\phi(\mathbb{Z}_n) \times \phi(\mathbb{Z}_m)| = \varphi(n) \cdot \varphi(m)$.

деф. $I, J \lhd A$ су **узајамно прости идеали** ако $I + J = A$.

Лема 1: Ако су I, J уз. прости и I, K уз. прости $\Rightarrow$ I, JK су уз. прости.

Доказ: Знамо да $\exists\, x_1 \in I,\ y \in J$ тако да $x_1 + y = 1$
$\exists\, x_2 \in I,\ z \in K$ тако да $x_2 + z = 1$
$\Rightarrow$ $1 = (x_1+y)(x_2+z) = \underbrace{x_1x_2 + x_1z + yx_2}_{\in I} + \underbrace{yz}_{\in JK} \in I + JK$

$\Rightarrow$ $I + JK = A$ $\Rightarrow$ I, JK узајамно прости

Последица: I_j уз. прост са свим I_k, $k \neq j$ $\Rightarrow$ $I_j, \prod_{\substack{k=1 \\ k\neq j}}^{n} I_k$ су узајамно прости

Теорема 4 (Општа Кинеска теорема о остацима):

Нека су $I_1, I_2, \dots, I_n \lhd A$ узајамно прости у паровима. Тада важи:

$$A/(I_1 \cap \dots \cap I_n) \cong A/I_1 \times \dots \times A/I_n.$$

Доказ: Намештамо на теорему о изоморфизму T4: $f: A \to (A/I_1 \times \dots \times A/I_n)$, $f(x) = (x+I_1, \dots, x+I_n)$

* f јесте хомоморфизам (тривијално по деф.)
* $\ker f = \{x \in A \mid f(x) = 0\} = \{x \in A \mid x + I_i = 0_i,\ 1 \le i \le n\} = \{x \in A \mid x \in I_i,\ 1 \le i \le n\} = I_1 \cap \dots \cap I_n$.
* Желимо да $\operatorname{Im} f = A/I_1 \times \dots \times A/I_n$, тј. да је f НА.

Нека је $(a_1+I_1, \dots, a_n+I_n) \in A/I_1 \times \dots \times A/I_n$.
Тражимо $a \in A$ тако да $(a_1+I_1, \dots, a_n+I_n) = f(a) = (a+I_1, \dots, a+I_n)$.

По Л1, постоје $x_j \in I_j$, $y_j \in \prod_{\substack{k=1 \\ k\neq j}}^{n} I_k$ тако да $x_j + y_j = 1$, $\forall\, 1 \le j \le n$

Узмимо $a = \sum_{j=1}^{n} a_j y_j$ и докажимо $a + I_k = a_k + I_k$, $\forall\, 1 \le k \le n$, тј. $a - a_k \in I_k$

Пошто по Л2 (сл. стр.): $y_j \in I_k$, $\forall j \neq k$ $\Rightarrow$ $a_j y_j \in I_k$, $\forall j \neq k$

Значи, треба још да важи $a_k y_k - a_k \in I_k$, а то је тривијално: $a_k(y_k - 1) = a_k x_k \in I_k$ ($x_k \in I_k$)

Лема 2: $I, J \trianglelefteq A$ узајамно прости $\Rightarrow$ $IJ = I \cap J$.

Доказ:

Доказ.

($\subseteq$) За произвољан сабирак суме $\sum_{i=1}^{n} x_i y_i$, $x_i \in I, y_i \in J$, важи

$\in IJ$

$$\underbrace{x_i}_{\in I} \cdot \underbrace{y_i}_{\in A} \overset{J1}{\in} I \quad \text{и} \quad \underbrace{x_i}_{\in A} \cdot \underbrace{y_i}_{\in J} \overset{J1}{\in} J$$

па се и сваки збир по $n \in \mathbb{N}$ налази и у I и у J, тј у пресеку $I \cap J$.

($\supseteq$) Нека је $z \in I \cap J$. Пошто су I и J уз. прости, то значи да постоје $x \in I$ и $y \in J$ такви да је $x + y = 1$. Сада је

$$z = z \cdot 1 = z(x+y) = \underbrace{zx}_{\in I} + \underbrace{zy}_{\in J} \overset{(*)}{\in} I \cdot J$$

(*) Сабирак zx припада $I \cdot J$, јер је $\underbrace{x}_{\in I}, \underbrace{z}_{\in J}$, а то важи и за сабирак zy, јер сада $\underbrace{z}_{\in I}, \underbrace{y}_{\in J}$

Последица: $I_1, \dots, I_n$ уз. прости $\Rightarrow$ $I_1 I_2 \dots I_k = I_1 \cap \dots \cap I_k$ (индукција)

Теорема 5 (Кинеска теорема о остацима у $\mathbb{Z}$)

Нека су $m_1, \dots, m_n \in \mathbb{Z}$ узајамно прости бројеви. Тада је:

$$\mathbb{Z}/(m_1 \dots m_n \mathbb{Z}) \cong \mathbb{Z}/(m_1\mathbb{Z}) \times \dots \times \mathbb{Z}/(m_n\mathbb{Z}).$$

Доказ: Применимо Т4 на $A = \mathbb{Z}$, $I_k = \langle m_k \rangle = m_k\mathbb{Z}$.

Напомена: $\langle m_i \rangle$ и $\langle m_j \rangle$ заиста јесу уз. прости: $\langle m_i \rangle + \langle m_j \rangle \overset{\text{Т4}}{=} \langle \text{НЗД} \rangle = \langle 1 \rangle = \mathbb{Z}$

Такође, $I_1 I_2 \dots I_n \overset{J2}{=} I_1 \cap \dots \cap I_n \overset{\text{Т4}}{=} \langle m_1 \dots m_n \rangle = m_1 \dots m_n \mathbb{Z}$

Теорема 6 (Кинеска теорема о остацима у $\mathbb{Z}$ - алтернативни облик)

Нека су $m_1, \dots, m_n \in \mathbb{Z}$ узајамно прости бројеви и $x_1, \dots, x_n \in \mathbb{Z}$.

Тада постоји $x \in \mathbb{Z}$: $x \equiv x_1 \pmod{m_1}$, ..., $x \equiv x_n \pmod{m_n}$.

Уз то, ако је $x' \in \mathbb{Z}$ решење овог система конгруенција $\Rightarrow$ $x \equiv x' \pmod{m_1 m_2 \dots m_n}$.

Доказ: Посматрајмо f из Т4: $f: A \to (A/I_1 \times \dots \times A/I_n)$, $f(x) = (x+I_1, \dots, x+I_n)$

↑ кад уврстимо

Егзистенција x следи јер је одговарајуће f НА.

„Јединственост" x следи јер је одговарајуће F 1-1.

↳ из теореме о изоморфизму

12. Прости идеали КПЈ

деф. **Прост идеал** је $P \lhd A$ ткд. $P \neq A$ и $xy \in P \Rightarrow x \in P \vee y \in P$.

Дефиниција се може индуктивно уопштити: $x_1 x_2 \dots x_n \in P \Rightarrow x_1 \in P \vee \dots \vee x_n \in P$.

Теорема 1: Нека је $P \lhd A$ и $P \neq A$. Тада је следеће еквивалентно:

(1) P је прост идеал; (по деф.)

(2) за $I, J \lhd A$ важи: $I \cdot J \leq P \Rightarrow I \leq P \vee J \leq P$;

(3) прстен A/P је домен. [8]

Доказ: (1⇒2) ппс. $\exists a \in I \setminus P$ (разлика), $b \in J \setminus P \Rightarrow ab \in IJ \leq P \overset{\text{прост}}{\Rightarrow} a \in P \vee b \in P$ ↯

(2⇒3) Показујемо $Z(A/P) = \{0\}$, тј. A/P нема правих делитеља нуле.

Узмимо $a+P \in A/P$ ткд. $a+P \neq 0+P$ и претпоставимо $(a+P)(b+P) = 0$, за неко $b \in A$.

$(a+P)(b+P) = 0 \Rightarrow ab+P = 0+P \Rightarrow ab \in P$

$\Rightarrow \langle ab \rangle \leq P \overset{\langle ab \rangle = \langle a \rangle \cdot \langle b \rangle}{\underset{(2)}{\Rightarrow}} \langle a \rangle \leq P$ или $\langle b \rangle \leq P$

$\Rightarrow a \in P \vee b \in P \Rightarrow a+P = 0+P \vee b+P = 0+P$

$\Rightarrow b+P = 0+P$ (ни један дел. нуле није прави)

(3⇒1) $ab \in P \Rightarrow ab+P = 0+P \Rightarrow 0+P = (a+P)(b+P)$

$\overset{\text{нема правих дел. нуле}}{\Rightarrow} a+P = 0+P \vee b+P = 0+P \Rightarrow a \in P \vee b \in P$

Теорема 2: 1) Нека су $P_1, \dots, P_n$ прости идеали кпј A, а $I \trianglelefteq A$ ткд. $I \subseteq \bigcup_{i=1}^{n} P_i$.

Тада је $I \subseteq P_i$, за неко $1 \le i \le n$;

2) Нека су $I_1, \dots, I_n$ идеали кпј A, а $P \trianglelefteq A$ прост идеал ткд. $\bigcap_{i=1}^{n} I_i \subseteq P$.

Тада је $I_i \subseteq P$, за неко $1 \le i \le n$.

Доказ: 1) (би) тривијално;

(ик) $I \subseteq \bigcup_{j=1}^{n} P_j = \bigcup_{\substack{j=1 \\ j\neq i}}^{n} P_j \cup P_i$: ако за неко i важи: $I \subseteq \bigcup_{\substack{j=1 \\ j\neq i}}^{n} P_j$, тврђење следи по (ик).

$n-1 \Rightarrow n$

Зато, пп. $I \not\subseteq \bigcup_{\substack{j=1 \\ j\neq i}}^{n} P_j$, $\forall 1 \le i \le n \Rightarrow$ постоје $x_i \in I \setminus \bigcup_{\substack{j=1 \\ j\neq i}}^{n} P_j \subseteq \bigcup_{j=1}^{n} P_j \setminus \bigcup_{\substack{j=1 \\ j\neq i}}^{n} P_j \Rightarrow x_i \in P_i$

ппс. $I \not\subseteq P_i$, за $1 \le i \le n$.

Посматрајмо елемент: $x = \sum_{i=1}^{n} \prod_{\substack{j=1 \\ j\neq i}}^{n} x_j \in I \subseteq \bigcup_{i=1}^{n} P_i \Rightarrow x \in P_k$, за неко $1 \le k \le n$

Приметимо да за $i \neq k$ је: $A := \prod_{\substack{j=1 \\ j\neq i}}^{n} x_j \in P_k$ ($x_k \in P_k$, па по деф.[2] идеала)

(ознака)

Самим тим и ако узмемо $i = k$, производ ће бити у P_k $\left(\prod_{\substack{j=1 \\ j\neq k}}^{n} x_j = \underset{\in P_k}{x} - \underset{\in P_k}{A} \in P_k \right)$

$\overset{P_k \text{ прост}}{\Rightarrow} x_1 \in P_k \vee \dots \vee x_{k-1} \in P_k \vee \underset{i \neq k}{x_{k+1} \in P_k} \vee \dots \vee x_n \in P_k$ ↯

2) ппс. $\forall i$ $I_i \not\subseteq P \Rightarrow \exists x_i \in I_i \setminus P \Rightarrow x = x_1 x_2 \dots x_n \in I_i$, $\forall i$

$\Rightarrow x \in \bigcap I_i \overset{\text{пп.}}{\Rightarrow} x \in P$ ↯ (P - прост)

* деф. Нека је R домен. Елемент $p \in R \setminus (U(R) \cup \{0\})$ је:

* **прост:** $p \mid ab \Rightarrow p \mid a$ или $p \mid b$, $\forall a, b \in R$;

* **нерастављив:** $p = ab \Rightarrow a \in U(R)$ или $b \in U(R)$, $\forall a, b \in R$;

} у главноид. домену ово је исто [15]

Лема 1: Нека је R домен. $p \in R$ прост $\Leftrightarrow$ $\langle p \rangle$ прост идеал.

Доказ: ($\Rightarrow$) $xy \in \langle p \rangle \Rightarrow xy = p \cdot c \Rightarrow p \mid xy \Rightarrow p \mid x$ или $p \mid y$

$\Rightarrow x = pa$ или $x = pb \Rightarrow x \in \langle p \rangle$ или $y \in \langle p \rangle \Rightarrow \langle p \rangle$ прост.

($\Leftarrow$) $p \mid ab \Rightarrow pc = ab \Rightarrow ab \in \langle p \rangle \Rightarrow a \in \langle p \rangle$ или $b \in \langle p \rangle \Rightarrow p \mid a$ или $p \mid b$.

Лема 2: Нека је R домен. $p \in R$ прост $\Rightarrow$ $p \in R$ нерастављив.

Доказ: $p = ab \Rightarrow p \mid ab \overset{p\text{-прост}}{\Rightarrow} p \mid a$ или $p \mid b \overset{\text{буо}}{\Rightarrow} p \mid a \Rightarrow a = pc \Rightarrow a = abc$

$\overset{a\text{-регул.}}{\Rightarrow} bc = 1 \Rightarrow b \in U(R) \Rightarrow p$ је нерастављив.

Пример: Обрнуто не важи.

Пример 12.1. У прстену $\mathbb{Z}[\sqrt{-5}]$, елемент 3 је нерастављив, али није прост. Подразумевамо $(\sqrt{-5})^2 = -5$, а прстен $\mathbb{Z}[\sqrt{-5}]$ дефинишемо

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}.$$

Да бисмо показали да 3 није прост, посматраћемо факторизацију броја 9 у $\mathbb{Z}[\sqrt{-5}]$. Имамо да је $9 = 3 \cdot 3$, али и $9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$. Одатле, важи

$$3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5}),$$

али $3 \nmid 2 + \sqrt{5}$ и $3 \nmid 2 - \sqrt{5}$, па 3 није прост. Покажимо сада је 3 нерастављив. Нека је $3 = uv$, за неке $u, v \in \mathbb{Z}[\sqrt{-5}]$. Тада је $|3|^2 = |u|^2 \cdot |v|^2$, а како су $|u|^2, |v|^2 \in \mathbb{Z}$, то је $|u|^2, |v|^2 \in \{1, 3, 9\}$. Како не може бити $|u|^2 = 3$, нека је $|u|^2 = 1$, без умањења општости. Тада је $|u|^2 = u \cdot \overline{u} = 1$, па је $u \in U(\mathbb{Z}[\sqrt{-5}])$ или $\overline{u} = U(\mathbb{Z}[\sqrt{-5}])$.

13. Максимални идеали кпј

строго подскуп!

деф. **Максимален идеал** је $M \triangleleft A$ ткд. $M \neq A$ и не постоји $I \triangleleft A$ ткд. $M \subset I \subset A$.

Теорема 1: Идеал $M \triangleleft A$ је максималан $\Leftrightarrow$ A/M је поље [8]

Доказ: ($\Rightarrow$) Нека је $a \in A$ ткд. $a+M \neq 0+M$, тј. $a \notin M$. $\Rightarrow$ $\langle a \rangle + M$ је идеал који је већи од M

$\overset{\text{није прави}}{\Rightarrow}$ $\langle a \rangle + M = A$ $\overset{1 \in \langle a \rangle + M}{\Rightarrow}$ $\exists b \in A, m \in M$ $ab+m=1$ $\Rightarrow$ $1-ab=m$, тј. $1-ab \in M$

$\Rightarrow$ $1+M = ab+M = (a+M)(b+M)$ $\Rightarrow$ $b+M$ инверз $a+M$ $\Rightarrow$ A/M је поље

($\Leftarrow$) Нека је $I \triangleleft A$, $M \subset I$. Докажимо $I = A$.

Изаберимо $a \in I \setminus M$ $\Rightarrow$ $a+M \neq 0+M$ $\overset{A/M \text{ поље}}{\Rightarrow}$ $1+M = (a+M)(b+M) = ab+M$ $\Rightarrow$ $1-ab \in M$

$\Rightarrow$ $1-ab = m$ $\Rightarrow$ $1 = \underbrace{ab}_{\in I} + \underbrace{m}_{\in M \subset I}$ $\Rightarrow$ $1 \in I$ $\Rightarrow$ $I = A$

Последица: I максималан $\Rightarrow$ I прост

Доказ:

максималан		I прост
Т1 $\Updownarrow$		$\Updownarrow$ 42 Т1
A/I поље	$\overset{8}{\Rightarrow}$	A/I домен

Пример: Обрнуто не важи: у $\mathbb{Z}[X]$, $\langle X \rangle$ јесте прост, али није максималан:

$$\underbrace{\langle X \rangle}_{M} \subsetneq \underbrace{\langle 2 \rangle + \langle X \rangle}_{I} \subsetneq \underbrace{\mathbb{Z}[X]}_{A}$$

Лема 1 (Цорнова лема):

Нека је $\leq$ уређење на непразном скупу S.
Ако сваки ланац у S има горње ограничење, у S постоји макс. елемент.

Теорема 2: Нека је $I \lhd A$ прави идеал $(I \neq A)$

Тада постоји максимални идеал $M \lhd A$ такав да садржи I, тј. $I \subseteq M$.

Доказ: Нека је $S = \{J \lhd A \mid I \subseteq J \neq A\}$ - фамилија свих правих идеала који садрже I.

По ЛМ, S садржи макс. елемент M и управо то ће бити макс. идеал. (тиме је доказ завршен)

Али да бисмо применили ЛМ, докажимо да су испуњени услови за њу:

1° S јесте непразан, јер $I \in S$.

2° Нека је $\mathcal{L} = \{I_\lambda \mid \lambda \in \Lambda\}$ ланац елем. из S.
Показујемо да је $J = \bigcup I_\lambda$ горње огр.

Јасно, J је горње огр. за $\mathcal{L}$, па је довољно доказати $J \in S$.

* $J \lhd A$: ово доказујемо по деф.

  * $x, y \in J \Rightarrow x \in I_\alpha,\ y \in I_\beta$. $\overset{\mathcal{L}\text{-ланац}}{\Rightarrow}$ (БУО) $I_\alpha \subseteq I_\beta \Rightarrow x, y \in I_\beta$

    $\Rightarrow x+y \in I_\beta \Rightarrow x+y \in \bigcup I_\lambda = J$;

  * $x \in J,\ a \in A \Rightarrow x \in I_\alpha \overset{I_\alpha\text{-идеал}}{\Rightarrow} ax \in I_\alpha \Rightarrow ax \in \bigcup I_\lambda = J$;

* $I \subseteq J$: Како $I \subseteq I_\lambda$ за све $\lambda \in \Lambda \Rightarrow I \subseteq \bigcup I_\lambda = J$;

* $J \neq A$: ппс. $1 \in J = \bigcup I_\lambda \Rightarrow \exists \alpha \in \Lambda\ 1 \in I_\alpha \Rightarrow I_\alpha = A \Rightarrow I_\alpha \notin S$ ↯

Последица: Нека је A кпј и $a \in A \setminus U(A)$.

Тада постоји максимални идеал $M \lhd A$ такав да садржи a.

Доказ: Идеал $\langle a \rangle$ је прави, јер $a \notin U(A)$. Значи може претх. теорема.

* **Теорема 3:** Нека је A домен. Тада је:

$a \in A$ је нерастављив $\Leftrightarrow$ идеал $\langle a \rangle$ је максималан у скупу свих правих главних идеала од A.

Доказ:

Доказ.

($\Rightarrow$) Претпоставимо супротно, нека постоји $b \in A$ такав да је

$$\langle a \rangle \subsetneq \langle b \rangle \subsetneq A.$$

Одатле је $a \in \langle b \rangle$, па је $a = bc$, за неко $c \in A$. Како је елемент a нерастављив, важи $b \in U(A)$ или $c \in U(A)$. Ако је $b \in U(A)$, тада је $\langle b \rangle = A$, што је контрадикција. Ако је, пак, $c \in U(A)$, тада постоји c' такав да је $cc' = 1$. Како је $a = bc$, то је $ac' = bcc' = b$, односно $b \in \langle a \rangle$. Према последњем, добијамо да је $\langle a \rangle = \langle b \rangle$. Контрадикција.

($\Leftarrow$) Опет, претпоставимо супротно, да a није нерастављив, већ $a = bc$, где $b, c \notin (U(A) \cup \{0\})$. То, надаље, значи да $a \in \langle b \rangle$, па је $\langle a \rangle \subseteq \langle b \rangle$. Приметимо да не може бити $\langle b \rangle = A$, јер $b \notin U(A)$, а A је домен. Како је, по претпоставци, идеал $\langle a \rangle$ максималан, мора бити $\langle a \rangle = \langle b \rangle$. Сада знамо да $b \in \langle a \rangle$, тј. $b = ad$, за неко $d \in A$. Коначно, имамо да је

$$a = bc = adc.$$

Посматрано A је домен, $a \neq 0$ па онда мора да је

$$dc = 1 \quad \Leftrightarrow \quad c \in U(A),$$

одакле изводимо контрадикцију.

14. Нилрадикал и Џејкобсонов радикал

деф. За $a \in A$ кажемо да је **нилпотентан** ако постоји $n \in \mathbb{N}$ ткд. $a^n = 0$.

Скуп свих нилпотентних елем. из кпј A је **нилрадикал** N.

Теорема 1: N је идеал у A.

Такође, у A/N нема нилпотентних елем. различитих од нуле.

Доказ:

Доказ. Докажимо прво да је $N \lhd A$.

(1) Нека су $x, y \in N$, тј је $x^n = 0$ и $y^m = 0$, за неке $m, n \in \mathbb{N}$. Пошто је A комутативни прстен са јединицом, онда можемо применити биномну формулу и добити

$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}.$$

Приметимо да за свако $0 \le k \le n+m$ важи

$$k \ge n \quad \text{или} \quad n+m-k \ge m.$$

Дакле, важи

$$x^k = 0 \quad \text{или} \quad y^{n+m-k} = 0,$$

што аутоматски значи да је сваки сабирак у суми једнак 0, па је и цела сума 0. Дакле, $x + y \in N$.

(2) Нека је $x \in N$ и $a \in A$. Тада је $x^n = 0$, за неко $n \in N$. Пошто је A комутативни прстен са јединицом важи

$$(ax)^n = a^n x^n = a^n \cdot 0 = 0,$$

па је и $ax \in N$.

Треба још показати да A/N нема нилпотентне елементе. Претпоставићемо супротно, нека је $a + N \neq N$ нилпотентан елемент у A/N. То значи да важи $(a+N)^n = N$, за неко $n \in \mathbb{N}$. Тада је $a^n + N = N$, односно $a^n \in N$. Дакле, можемо наћи $b \in N$ такав да је $b = a^n$, што значи да је за неко $m \in \mathbb{N}$

$$0 = b^m = a^{nm},$$

па је самим тим и $a \in N$, тј. $a + N = N$, а то је контрадикција.

Теорема 2: Нилрадикал N је пресек свих простих идеала у кпј A

Доказ:

Доказ. Нека је $\mathcal{P}$ скуп свих простих идеал од A, показујемо да је

$$\boxed{N = \bigcap_{P \in \mathcal{P}} P.} \quad \text{– ово доказујемо}$$

($\subseteq$) Нека је $x \in N$, па је $x^n = 0$, за неко $n \in \mathbb{N}$. Нека је и $P \in \mathcal{P}$ произвољно. Пошто је $x^n = 0 \in P \overset{P \text{ прост}}{\Longrightarrow} x \in P$. Како је P произвољно, то важи за свако $P \in \mathcal{P}$, чиме смо показали једну инклузију.

($\supseteq$) Обележимо са N' пресек свих простих идеала. Дакле,

десна страна

$$N' = \bigcap_{P \in P} P. \qquad (\text{доказујемо } N' \subseteq N)$$

Претпоставимо супротно, $x \in N' \setminus N$, односно x није нилпотентан. Тада за свако $n \in \mathbb{N}$ је $x^n \neq 0$. Посматрајмо све идеале I такве да $x^n \notin I$, за свако $n \in \mathbb{N}$, тј.

$$\mathcal{S} = \{I \lhd A \mid (\forall n \in \mathbb{N})\ x^n \notin I\}.$$

1) Према претходном, важи да $\{0\} \in \mathcal{S}$, па је $\mathcal{S}$ непразан. 2) Произвољан ланац у $\mathcal{S}$ има горње ограничење, јер је унија свих елемената ланца то ограничење. Према Цорновој леми, $\mathcal{S}$ има максималан елемент. Обележимо га са $\mathcal{J}$ и докажимо да је $\mathcal{J}$ прост. Нека је $ab \in \mathcal{J}$ и претпоставимо супротно, $a \notin \mathcal{J}$, $b \notin \mathcal{J}$. Посматрајмо $\mathcal{J} + \langle a \rangle \lhd A$. Тада је $\mathcal{J} \subsetneq \mathcal{J} + \langle a \rangle$, па $\mathcal{J} + \langle a \rangle \notin \mathcal{S}$, односно постоји $n \in \mathbb{N}$ такав да је

јер је $\mathcal{J}$ макс. у $\mathcal{S}$

$$x^n \in \mathcal{J} + \langle a \rangle.$$

Слично, постоји $m \in \mathbb{N}$ такво да је

$$x^m \in \mathcal{J} + \langle b \rangle$$

Расписујући, добијамо

$$x^n = at + p_1, \quad p_1 \in \mathcal{J},\ t \in A,$$
$$x^m = bs + p_2, \quad p_2 \in \mathcal{J},\ s \in A.$$

Множећи ове две једнакости, добијамо

$$x^{n+m} = \underbrace{p_1 p_2 + a t p_2 + b s p_1}_{\in \mathcal{J}} + \underbrace{abts}_{\in \langle ab \rangle}.$$

Како је $ab \in \mathcal{J}$, то је $\langle ab \rangle \in \mathcal{J}$, па је $x^{n+m} \in \mathcal{J}$, што је контрадикција. Дакле, $\mathcal{J}$ је прост идеал. Коначно, како $x \notin \mathcal{J}$ и како је $\mathcal{J}$ прост, то

$\mathcal{J} \in \mathcal{S}$ $n=1$

$$x \notin N',$$

(јер $N' = \bigcap_{P \in P} P$, по мора бити у сваком простом, а то овде није случај)

па добијамо контрадикцију.

деф. Пресек свих максималних идеала у кпј A је **Џејкобсонов радикал** R.

Теорема 3: $x \in R \iff 1-xy \in U(A)$, за све $y \in A$

Доказ: ($\Rightarrow$) Нека је $x \in R$ и ппс. $1-xy \notin U(A)$.

Тада постоји максималан идеал M који садржи $1-xy$. (по последици 13 T2)

Како је M макс. $\Rightarrow$ $R = \underset{\text{макс.}}{\bigcap} M_i \subseteq M \Rightarrow x \in M \overset{\text{M-идеал}}{\Rightarrow} xy \in M$

$\Rightarrow 1-xy+xy \in M \Rightarrow 1 \in M \Rightarrow M = A$ ↯

($\Leftarrow$) Желимо да докажемо да за сваки макс. идеал M_i важи $x \in M_i$.

ппс. $x \notin M \Rightarrow M \overset{\text{строго}}{\subset} \langle x \rangle + M \overset{\text{M-макс.}}{\Rightarrow} \langle x \rangle + M = A$

$\Rightarrow 1 \in \langle x \rangle + M \Rightarrow 1 = xy + m$, за неке $y \in A$, $m \in M$

$\Rightarrow m = 1-xy \Rightarrow m \in U(A) \overset{9\ \text{T1}}{\Rightarrow} M = A$ ↯

15. Главноидеалски домени

деф. Нека је A домен.
За елементе $a,b \in A$ кажемо да су **придружени** ако $a = \varepsilon b$, за неко $\varepsilon \in U(A)$.

На A дефинишемо релацију: $a \sim b$ акко a,b придружени.

Напомена: $\sim$ је релација еквиваленције. (тривијално)

Лема 1: 1) a је прост $\Leftrightarrow$ εa је прост, $\forall a \in A,\ \varepsilon \in U(A)$

2) a је нерастављив $\Leftrightarrow$ εa је нерастављив, $\forall a \in A,\ \varepsilon \in U(A)$

Доказ: тривијално по деф.

Лема 2: Нека је A домен.
Ако $a|b$ и $b|a$ $\Rightarrow$ a,b су придружени.

Доказ: $\left.\begin{array}{l} a|b \Rightarrow b = ac \\ b|a \Rightarrow a = bd \end{array}\right\} \Rightarrow a = acd \overset{a \neq 0}{\Rightarrow} cd = 1 \Rightarrow c,d \in U(A) \Rightarrow a \sim b$

деф. A је **домен са једнозначном факторизацијом**, у ознаци **UFD**, ако:

за свако $a \in A \setminus (U(A) \cup \{0\})$ постоје нерастављиви елементи $p_1, \dots, p_r$ ткд. $a = p_1 p_2 \dots p_r$

и при томе, ако је $a = q_1 q_2 \dots q_s$ за неке нерастављиве $q_1, \dots, q_s$,
тада $r = s$ и постоји $\sigma \in S_r$ ткд. су p_i и $q_{\sigma(i)}$ придружени за све $1 \leq i \leq r$.

Примери: 1) $\mathbb{Z}$: $30 = 2 \cdot 3 \cdot 5 = (-5) \cdot 2 \cdot (-3)$: $\sigma: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

2) $\mathbb{R}[X]$

3) $\mathbb{Z}[X]$

Теорема 1: Домен A је UFD $\Leftrightarrow$ $\forall a \in A \setminus (U(A) \cup \{0\})$ се може записати као производ простих елемената.

Доказ:

Доказ.

($\Leftarrow$) Прости елементи су нерастављиви, па постоји факторизација на нерастављиве. Нека је

$$a = p_1 p_2 ... p_r = q_1 q_2 ... q_s,$$

где су $p_1, p_2, ..., p_r$ прости, а $q_1, q_2, ..., q_s$ нерастављиви. Из претходног реда имамо да

$$p_1 \mid q_1 q_2 ... q_3,$$

па $p_1 \mid q_i$, за неко $1 \leqslant i \leqslant s$. Тада је $q_i = p_1 t$, па како је q_i нерастављив, а $p_1 \notin U(A)$, то је $t \in U(a)$, односно $p_1 \sim q_i$. Настављајући овај поступак добијамо тражено тврђење.

($\Rightarrow$) Довољно је показати да је сваки нерастављив елемент уједно и прост. Нека је $p \in A$ нерастављив и $p \mid ab$, за неке $a, b \in A$. Тада је, за неко $c \in A$, $pc = ab$. Елементе a, b и c можемо записати као

$$a = a_1 a_2 ... a_k, \quad b = b_1 b_2 ... b_l, \quad c = c_1 c_2 ... c_m,$$

где су $a_1, a_2, ..., a_k, b_1, b_2, ..., b_l, c_1, c_2, ..., c_m$ нерастављиви. Дакле,

$$pc_1 c_2 ... c_m = a_1 a_2 ... a_k b_1 b_2 ... b_l = d$$

су две факторизације елемента d на производ нерастављивих, па је p придружен неком од $a_1, a_2, ...a_k, b_1, b_2, ...b_l$. Без умањења општости, нека је $p \sim a_i$, тада је $a_i = up$, где је $u \in U(A)$. Коначно,

$$a = a_1 ... a_{i-1} p u a_{i+1} ... a_k,$$

па p дели a, тј. p је прост.

деф. Нека је A домен и $a, b \in A$. Тада је:

1) $d \in A$ **nzd** елемената a, b: ако за $\forall c \in R$ важи: $c \mid a$ и $c \mid b \Leftrightarrow c \mid d$;

2) $s \in A$ **nzs** елемената a, b: ако за $\forall c \in R$ важи: $a \mid c$ и $b \mid c \Leftrightarrow s \mid c$;

Напомена: nzs и nzd не морају да постоје;
Ако постоје, онда су јединствени до на придруженост.

деф. A је **главноидеалски домен**, у ознаци **PID**, ако је сваки идеал у A главни.

Теорема 2: Свака два (ненула) елемента главноид. домена A имају nzd.

Доказ:

Доказ. Нека су $a, b \in A$ и нека је $I = \langle a \rangle + \langle b \rangle$. Како је I главни идеал, важи $I = \langle d \rangle$. Докажимо да је d NZD од a и b , односно да је за $c \in A$ испуњено

$$c \mid a \quad \text{и} \quad c \mid b \quad \Leftrightarrow \quad c \mid d.$$

($\Rightarrow$) Нека $c \mid a$ и $c \mid b$, за неко $c \in A$, тада је $a = cu_1$ и $b = cv_1$, за неке $u_1, v_1 \in A$. Даље је $d \in \langle d \rangle = \langle a \rangle + \langle b \rangle$, па важи $d = au + bv$, за неке $u, v \in A$. Комбинујући претходно,

$$d = au + bv = cu_1u + cv_1v = c(u_1u + v_1v),$$

па $c \mid d$.

($\Leftarrow$) Како је

$$\langle a \rangle \subseteq \langle a \rangle + \langle b \rangle = \langle d \rangle,$$

то је $a \in \langle d \rangle$, тј. $a = du$. С друге стране, како $c \mid d$, то је $d = cv$. На крају, $a = cvu$, односно $c \mid a$. Слично се покаже да $c \mid b$.

Последица (Безуова релација): (види се из доказа)

Нека је A главноид. домен и d је nzd за a, b $\Rightarrow$ $\exists x, y \in A$ $ax + by = d$.

Лема 3: Нека је A главноид. домен и $a \mid bc$.

Ако је 1 nzd за a, b $\Rightarrow$ $a \mid c$.

Доказ: $a \mid bc \Rightarrow \exists d$ $ad = bc$

Безу $\Rightarrow \exists x, y$ $ax + by = 1 \Rightarrow acx + bcy = c \Rightarrow acx + ady = c \Rightarrow a(cx + dy) = c \Rightarrow a \mid c$

Теорема 3: A је главноидеалски домен $\Rightarrow$ A је домен са јединственом факторизацијом.

Доказ:

Доказ. Докажимо прво да је сваки нерастављи елемент уједно и прост елемент у A. Нека је p нерастављив и нека $p \mid ab$. Претпоставимо да $p \nmid a$. Знамо да постоји NZD од a и p једнак неком d. Тада $d \mid p$, па је $p = ud$. Ако је $d \in U(A)$, онда је NZD од a и p један. С друге стране, ако је $d \notin U(A)$, тада је $u \in U(A)$, па из $d \mid a$ следи $p \mid a$, што је контрадикција са претпоставком. Дакле, NZD од a и p јесте 1, па према леми следи да $p \mid b$.
Према теореми 15.2 довољно је доказати да се свако $a \in A \setminus (U(A) \cup \{0\})$ може представити као производ нерастављивих елемената. Нека је

$$\Sigma = \{\langle a \rangle \mid a \in A \setminus (U(A) \cup \{0\}),\ a \text{ се не може записати као производ нерастављивих}\}.$$

Ако је $\Sigma = \emptyset$ доказ је завршен. Нека је $\Sigma \neq \emptyset$. Нека је $\mathcal{L}$ ланац елемената из Σ, у односу на инклузију. Доказујемо да $\mathcal{L}$ има горње ограничење у Σ. Нека је

$$I = \bigcup_{\langle a \rangle \in \mathcal{L}} \langle a \rangle.$$

Тада је I идеал. Како је A главноидеалски домен, то је $I = \langle c \rangle$. Тада је

$$c \in \langle c \rangle = \bigcup_{\langle a \rangle \in \mathcal{L}} \langle a \rangle,$$

па је $c \in \langle a \rangle$, тј. $c = at$, за неке $a, t \in A$. Следи $\langle c \rangle \subseteq \langle a \rangle$. Дакле, мора бити $\langle c \rangle = \langle a \rangle$. Тада из $a \in \langle c \rangle$ следи $a = cu$, па је $c = cut$, где су $u, t \notin U(A)$. Дакле, c се не може записати као производ нерастављивих, па је $I = \langle c \rangle \in \Sigma$. Према Цорновој леми, у Σ постоји максималан елемент. Нека је то $\langle b \rangle$. Дакле, b се не може записати као производ нерастављивих елемената. Одатле следи да b није нерастављив, па је $b = uv$, где $u, v \notin U(A)$. Тада $\langle b \rangle \subsetneq \langle u \rangle$ и $\langle b \rangle \subsetneq \langle v \rangle$, па се u и v могу записати као производ нерастављивих. Међутим, тада се и uv може записати као производ нерастављивих, што је контрадикција. Дакле $\Sigma = \emptyset$.

16. Домени са једнозначном факторизацијом и прстени полинома

Лема 1: Нека је A домен.
Ако је p прост у A $\Rightarrow$ p је прост и у $A[X]$.

Доказ:

Доказ. Нека је $p \in A$ прост. Тада је $\langle p \rangle$ прост идеал, јер је $ab \in \langle p \rangle$ ако и само ако $p \mid ab$. Тада $p \mid a$ или $p \mid b$, односно $a \in \langle p \rangle$ или $b \in \langle p \rangle$. Закључујемо да је

$$\overline{A} = A/\langle p \rangle$$

домен. Тада је и $\overline{A}[X]$ домен, јер је за

$$0 = (a_n X^n + \ldots + a_0)(b_m X^m + \ldots + b_0) = a_n b_m X^{n+m} + \ldots + a_0 b_0,$$

где су сви коефицијенти полинома са десне стране различити од нуле, јер је $a_n \neq 0$ и $b_m \neq 0$, за произвољне m и n. Приметимо да је p прост у $A[X]$ ако и само ако је $\langle p \rangle$ прост идеал од $A[X]$ што је еквивалентно с тим да је $A[X]/\langle p \rangle$ домен. Докажимо да је

$$\overline{A}[X] \cong A[X]/\langle p \rangle.$$

Посматрајмо пресликавање $\pi : A[X] \to \overline{A}[X]$ задато са

$$\pi(a_0 + a_1 X + \ldots + a_n X^n) = (a_0 + \langle p \rangle) + (a_1 + \langle p \rangle)X + \ldots + (a_n + \langle p \rangle)X^n.$$

Овако дефинисано π је хомоморфизам. Нека је $m > n$, где су $m, n \in \mathbb{N}_0$, тада је

$$\begin{aligned}
&\pi((a_0 + a_1 X + \ldots + a_n X^n) + (b_0 + b_1 X + \ldots + b_m X^m)) \\
&= \pi((a_0 + b_0) + (a_1 + b_1)X + \ldots + (a_n + b_n)X^n + b_{n+1}X^{n+1} + \ldots + b_m X^m) \\
&= (a_0 + b_0 + \langle p \rangle) + (a_1 + b_1 + \langle p \rangle)X + \ldots + (a_n + b_n + \langle p \rangle)X^n + (b_{n+1} + \langle p \rangle)X^{n+1} + \ldots + (b_m + \langle p \rangle)X^m \\
&= (a_0 + \langle p \rangle) + \ldots + (a_n + \langle p \rangle)X^n + (b_0 + \langle p \rangle) + \ldots + (b_m + \langle p \rangle)X^m \\
&= \pi(a_0 + a_1 X + \ldots + a_n X^n) + \pi(b_0 + b_1 X + \ldots + b_m X^m).
\end{aligned}$$

Слично, само са више рачуна се покаже да је π хомоморфно и за $\cdot$. Такође, важи $\pi(1) = 1 + \langle p \rangle$. Дакле, π јесте хомоморфизам прстена. Јасно, π је „НА“ по дефиницији и $\operatorname{Ker} \pi = \langle p \rangle$, па је и „1-1“.

деф. Нека је A домен са једнозначном факторизацијом.

$a_n X^n + \ldots + a_1 X + a_0 \in A[X]$ је **примитиван полином** ако је 1 nzd елемената $a_0, \ldots, a_n$.

(Пре леме, погледати локализацију која иде на крају овог питања)

Лема 2: Нека је $f \in A[X]$ примитивни полином. Тада је:

f нерастављив у $A[X]$ $\Leftrightarrow$ f нерастављив у $A\setminus[X]$

Доказ:

Доказ.

($\Leftarrow$) Нека је $u = fg$, где су $f, g \in A[X]$. Како је $f, g \in \mathbb{A}[X]$, то је без умањења општости $f \in U(\mathbb{A}[X])$. Дакле, $f \in A$, а како је u примитива, то је $f \in U(A)$. Коначно, $f \in U(A[X])$.

($\Rightarrow$) Покажимо прво да ако су f и g примитивни, онда је и fg примитиван. Претпоставимо супротно, нека постоји $c \in A \setminus (U(A) \cup \{0\})$ такво да је

$$c \mid fg.$$

Из једнозначне факторизације имамо да постоји просто $p \in A$ такво да је $p \mid c$. Из претходне леме је $p \mid f$ или $p \mid g$, што је контрадикција. Дакле, ако су f и g примитивни, онда је и fg примитиван. Нека је сада $u = fg$, где су $f, g \in \mathbb{A}[X]$. Покажимо да је u нерастављив. Претпоставимо супротно, нека f и g нису инвертибилни. Тада за f и g постоје $a, b, c, d \in A$ и $v, w \in A[X]$ такви да је

$$f = \frac{a}{b}u, \quad g = \frac{c}{d}w,$$

при чему су v и w примитивни. Дакле,

$$u = \frac{a'}{b'}vw,$$

при чему је NZD од a' и b' баш 1. Тада у прстену $A[X]$ важи

$$b' \mid a'vw,$$

па као у претходном делу, ако $b' \notin U(A)$, за неки прост елемент p важи $p \mid b'$ и $p \mid a'vw$, па је NZD за p и a' један, односно $p \mid vw$, што је немогуће. Ако је $b \in U(A)$, тада је $u = a'vw$, па је без умањења општости $v \in U(A[X])$, па је и $f \in U(\mathbb{A}[X])$, што је такође немогуће.

Теорема 1: A је UFD $\Rightarrow$ A[X] је UFD.

Доказ:

Доказ. Нека је $\mathbb{A}$ поље разломака над A. Тада је $A[X]$ домен са једнозначном факторизацијом. Покажимо да се свако $f \in A[X]$ може факторисати на нерастављиве и да је сваки нерастављив прост. Како је $f \in A[X]$, то је $f \in \mathbb{A}[X]$, па постоје $f_1, f_2, ..., f_k \in \mathbb{A}[X]$ који су нерастављиви у $\mathbb{A}[X]$ такви да је

$$f = f_1 f_2 ... f_k.$$

Као у претходној леми, важи

$$f = \frac{a}{b} v_1 v_2 ... v_l,$$

где су $a, b \in A$, $v_1, v_2, ..., v_l \in A[X]$ примитивни. При томе, $v_i = c_i f_i$, где је $c_i \in \mathbb{A}[X]$, па како је $c_i f_i$ нерастављив у $\mathbb{A}[X]$, то је према претходној леми и v_i нерастављив у $A[X]$. Уз то, $v_1 v_2 ... v_k$ је примитиван, па како је $\frac{a}{b} v_1 v_2 ... v_k \in A[X]$, то $b \mid a$, тј. постоји $c \in A$ такво да је

$$f = c v_1 v_2 ... v_k.$$

Ако раставимо у A c на нерастављиве, добијамо факторизацију полинома f у $A[X]$ на нерастављиве. Докажимо и да је сваки нерастављив $p \in A[X]$ прост. Ако је $p \in A$, тада је p нерастављив, па како је A домен са једнозначном факторизацијом, то је p прост у A, па је према првој леми прст и у $A[X]$. Нека је сада $\deg p > 1$ и $p \mid fg$, где су $f, g \in A[X]$. Елемент p је примитиван у $A[X]$, па је p нерастављив у $\mathbb{A}[X]$ из претходне леме. Како је $\mathbb{A}[X]$ домен са једнозначном факторизацијом, то је p прост у $\mathbb{A}[X]$. Тада, без умањења општости, $p \mid f$ у $\mathbb{A}[X]$. Дакле, $f = ph$, за $h \in \mathbb{A}[X]$. Нека је $h = \frac{a}{c} u$, где су $a, c \in A$ и $u \in A[X]$ примитиван. Тада из чињенице да је $f = \frac{a}{c} up \in A[X]$ и да је up примитиван следи да $c \mid a$, јер $\deg u > 1$ и $\deg p \geqslant 1$. Дакле, $f = bup$, за $b \in A$, па је $p \mid f$ у $A[X]$.

Последица: Z[X], Z[X,Y], ... су UFD.

Теорема 2 (Ајзенштајнов критеријум):

Нека је A UFD и $f = a_n x^n + ... + a_1 x + a_0 \in A[X]$ примитиван полином.

Ако у A постоји нерастављиво p ткд. $p \mid a_0, a_1, ..., a_{n-1}$, $p \nmid a_n$, $p^2 \nmid a_0$

$\Rightarrow$ f је нерастављив у A[X] (самим тим и у $\mathbb{A}$[X])

Доказ:

Доказ. Нека је $\overline{A} = A/\langle p \rangle$. Тада је $\overline{A}$ домен из прве леме. Нека је $\pi : A[X] \to \overline{A}[X]$ дефинисана као у првој леми. Тада са $\tilde{f}$ означимо $\pi(f)$, где је $f \in A[X]$. Тада је

$$\overline{u} = a_n x^n.$$

Нека је $u = vw$, где су $v, w \in A[X]$. Тада је $\overline{u} = \overline{vw}$, па је $\overline{v} = bc^k$ и $\overline{w} = cx^{n-k}$, где су $b, c \in \overline{A}$ и $0 \leqslant k \leqslant n$, јер је $\overline{A}$ домен. Сада је

$$v = b_k x^k + ... + b_0 \text{ и } w = c_{n-k} x^{n-k} + ... + c_0.$$

Приметимо да не можемо имати чланове b_{k+1} и c_{n-k+1}, јер мора бити $\deg u = \deg v + \deg w$, јер је A домен. Такође, мора важити $p \mid b_i$, за $0 \leqslant i \leqslant k-1$ и $p \mid c_i$, за $0 \leqslant i \leqslant n-k-1$. Међутим, $a_0 = b_0 c_0$, па ако је $k \geqslant 1$, или $n - k \geqslant 1$, тада $p^2 \mid a_0$, јер $p \mid b_0$ и $p \mid c_0$.

Локализација

деф. Нека је A домен.
На скупу $A \times (A \setminus \{0\})$ дефинишемо релацију: $(a,b) \sim (c,d)$ акко $ad = bc$.

Напомена: $\sim$ је релација еквиваленције. (тривијално)

деф. Класу еквив. $C_{(a,b)}$ означавамо $\frac{a}{b}$.

деф. **Поље разломака** је скуп $A = \left\{ \frac{a}{b} \mid a \in A,\ b \in A \setminus \{0\} \right\}$.

На њему дефинишемо операције: 1) $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$

2) $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$

Напомена: Ове операције су добро деф:

Доказ:

Напомена. Потребно је показати да је претходна дефиниција добра. За почетак, скуп S је мултипликативан, што значи да $s, t \in S$ повлачи $st \in S$, па претходни записи имају смисла. Треба још показати да резултати не зависе од избора представника.

– Докажимо да је дефиниција за $+$ добра. Нека је $(a_1, s_1) \sim (a_2, s_2)$ и $(b_1, t_1) \sim (b_2, t_2)$. Тада је $a_1 s_2 = a_2 s_1$ и $b_1 t_2 = b_2 t_1$. Сада је

$$\frac{a_1}{s_1} + \frac{b_1}{t_1} = \frac{a_1 t_1 + b_1 s_1}{s_1 t_1},$$

$$\frac{a_2}{s_2} + \frac{b_2}{t_2} = \frac{a_2 t_2 + b_2 s_2}{s_2 t_2},$$

па је довољно показати да је

$$(a_1 t_1 + b_1 s_1, s_1 t_1) \sim (a_2 t_2 + b_2 t_2, s_2 t_2).$$

Претходно је еквивалентно са

$$\begin{aligned} &(a_1 t_1 + b_1 s_1) s_2 t_2 = s_1 t_1 (a_2 t_2 + b_2 s_2) \\ \Leftrightarrow\ &a_1 t_1 s_2 t_2 + b_1 s_1 s_2 t_2 = s_1 t_1 a_2 t_2 + s_1 t_1 b_2 s_2. \\ \Leftrightarrow\ &a_1 s_2 t_1 t_2 + b_1 t_2 s_1 s_2 = a_2 s_1 t_1 t_2 + b_2 t_1 s_1 s_2. \end{aligned}$$

Последњи ред је тачан, јер је $a_1 s_2 = a_2 s_1$ и $b_1 t_2 = b_2 t_1$.

– Докажимо да је дефиниција за $\cdot$ добра. Нека је $(a_1, s_1) \sim (a_2, s_2)$ и $(b_1, t_1) \sim (b_2, t_2)$. Тада је $a_1 s_2 = a_2 s_1$ и $b_1 t_2 = b_2 t_1$. Сада је

$$\frac{a_1}{s_1} \cdot \frac{b_1}{t_1} = \frac{a_1 b_1}{s_1 t_1},$$

$$\frac{a_2}{s_2} \cdot \frac{b_2}{t_2} = \frac{a_2 b_2}{s_2 t_2},$$

па је довољно показати да је

$$(a_1 b_1, s_1 t_1) \sim (a_2 b_2, s_2 t_2).$$

Претходно је еквивалентно са

$$a_1 b_1 s_2 t_2 = a_2 b_2 1 s_1 t_1.$$

Што је тачно због $a_1 s_2 = a_2 s_1$ и $b_1 t_2 = b_2 t_1$.

Напомена: $(A, +, \cdot)$ је поље.

Доказ: тривијално по деф.

(нула је $\frac{0}{b}$, јер $\frac{0}{b} = \frac{c}{d} \Leftrightarrow bc = 0 \Leftrightarrow c = 0$, па $(0,b) \sim (c,d)$)

17. Раширења поља

деф. Нека су K, L поља.

Кажемо да је L **раширење поља** K, у ознаци $K \leq L$, ако L садржи потпоље изоморфно са K.

У том случају, кажемо и да је L **натпоље** од K. (у наставку поистовећујемо)

Сетимо се: пошто су у L дефинисане операције $+$ и множење елементима из K (скаларима), L можемо посматрати као векторски простор над K.

деф. **Степен раширења** L над K је: $[L:K] := \dim_K L$ (димензија векторског простора)

Пример: 1) $[C:R] = 2$ (база: $[1, i]$)

2) $[R:\mathbb{Q}]$ је бесконачно (доказујемо касније)

Теорема 1: Нека је $K \leq F$ и $F \leq L$

Ако су $[F:K]$, $[L:F]$ коначни $\Rightarrow$ $[L:K] = [F:K] \cdot [L:F]$

Доказ:

Доказ. Нека је $[F : L] = n$ и $[L : K] = m$ и нека је $e = [e_1, e_2, ..., e_n]$ база за F над L, односно $f = [f_1, f_2, ..., f_m]$ база за L над K. Доказујемо да је

$$g = [e_i f_j \mid 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m]$$

БИТНО!

база за F над K.

– *Линеарна независност.* Нека је

$$\sum_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}} \alpha_{ij} e_i f_j = 0,$$

за неке $\alpha_{ij} \in K$. Тада је

$$\sum_{i=1}^{n} \left(\sum_{j=1}^{m} \alpha_{ij} f_j \right) e_i = \sum_{i=1}^{n} \beta_i e_i = 0,$$

где је $\beta_i = \sum_{j=1}^{m} \alpha_{ij} f_j \in L$. Како је e линеарно независно, то је $\beta_1 = \beta_2 = ... = \beta_n = 0$. Тада је $\sum_{j=1}^{m} \alpha_{ij} f_j = 0$, за свако $1 \leqslant i \leqslant n$, па је и $\alpha_{i1} = \alpha_{i2} = ... = \alpha_{im} = 0$, за свако $1 \leqslant i \leqslant n$, јер је f линеарно независно над K.

– *g је генератриса.* Нека је $a \in F$. Тада постоје $\beta_1, \beta_2, ..., \beta_n \in L$ такви да је

$$a = \sum_{i=1}^{n} \beta_i e_i,$$

јер је e генератриса за F над L. Даље, за свако β_i постоје $\alpha_{i1}, \alpha_{i2}, ..., \alpha_{im} \in K$ такви да је

$$\beta_i = \sum_{j=1}^{m} \alpha_{ij} f_j,$$

јер је f генератриса за L над K. Тада је

$$a = \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_{ij} e_i f_j,$$

чиме је тврђење показано.

деф. Нека је $K \leq L$ и $\alpha \in L$.

$$K[\alpha] := \{ p(\alpha) : \ p \in K[X] \};$$

$$K(\alpha) := \left\{ \frac{a}{b} : \ a, b \in K[\alpha] \right\}.$$

Напомена: 1) $K[\alpha]$ је минимални прстен који садржи $K \cup \{\alpha\}$;

2) $K(\alpha)$ је минимално поље разломака над $K[\alpha]$ које садржи $K \cup \{\alpha\}$.

3) $K \leq K(\alpha)$. За $K(\alpha)$ кажемо да је **просто раширење**.

деф. Нека је $K \leq L$ и $\alpha \in L$.

Ако постоји $p \in K[X] \setminus \{0\}$ ткд. $p(\alpha) = 0$, α је **алгебарски елемент** над K.
Иначе је **трансцедентан**.

деф. Нека је α алгебарски елем. над K.
Минимални полином за α над K, у ознаци μ_α, је полином из $K[X] \setminus \{0\}$ ткд:

1) $\mu_\alpha(\alpha) = 0$;
2) μ_α је моничан;
3) μ_α је најмањег степена ткд. важе 1) и 2). (*)

Теорема 2: Нека је $K \leq L$ и $\alpha \in L$. Тада је: α алгебарски над K $\iff$ $K[\alpha] = K(\alpha)$.

У том случају је: 1) $\forall p \in K[X] \quad p(\alpha) = 0 \Rightarrow \mu_\alpha \mid p$.
2) μ_α је нерастављив; (**)
3) μ_α је јединствен;

4) $[K(\alpha) : K] = \deg(\mu_\alpha)$.

Доказ:

Доказ. Доказ изводимо на следећи начин. Показаћемо да ако је α алгебарски елемент, онда важе прве три особине, које ћемо искористити за доказ једног смера. Касније ћемо показати и последњу особину, и коначно и други смер.
Нека је α алгебарски над K.

(1) За свако $p \in K[X]$ постоје $q, r \in K[X]$ такви да је $p = q\mu + r$, где је $\deg r < \deg \mu$. Сада је $p(\alpha) = q(\alpha)\mu(\alpha) + r(\alpha) = r(\alpha)$, јер је $\mu(\alpha) = 0$. Тада је $p(\alpha) = 0$ ако и само ако је $r(\alpha) = 0$, што је еквивалентно с тим да је $r \equiv 0$, јер је μ минималан, односно $m \mid p$.

(2) Нека је $\mu = fg$, тад је $f(\alpha)g(\alpha) = 0$, па је $f(\alpha) = 0$ или $g(\alpha) = 0$, одакле је $\deg f \geq \deg \mu$ или $\deg g \geq \deg \mu$. Како је $\deg \mu \geq \deg f$ и $\deg \mu \geq \deg g$, то је g константан полином или је f константан полином. Дакле, μ је нерастављив.

(3) Нека су μ и σ минимални полиноми за α. Ако је $\mu \neq \sigma$, тада за моничны полином

$$\theta = c(\mu - \sigma),$$

важи $\theta(\alpha) = 0$ и $\deg \theta < \deg \mu$, што је контрадикција. Дакле, важи јединственост.

($\Rightarrow$) Довољно је показати да за $p \in K[X]$ за који је $p(\alpha) \neq 0$, постоји $q \in K[X]$, такав да је

$$\frac{1}{p(\alpha)} = q(\alpha).$$

Како $p(\alpha)$ није 0, то по (1) значи да $\mu \nmid p$, па како је μ нерастављив, а тиме и прост NZD од μ и p је 1. Како је $K[X]$ главноидеалски домен, то постоје $u, v \in K[X]$ такви да је $u\mu + vp = 1$. Следи да је

$$u(\alpha)\underbrace{\mu(\alpha)}_{=0} + v(\alpha)p(\alpha) = 1,$$

односно, $\frac{1}{p(\alpha)} = v(\alpha)$.

(4) Покажимо да је база за $K(\alpha)$ над K баш $e = [1, \alpha, ..., \alpha^{n-1}]$, где је $n = \deg \mu$.

– *e је генератриса.* Показали смо да је

$$K(\alpha) = K[\alpha] = \{p(\alpha) \mid p \in K[X]\}.$$

Нека је

$$\mu(X) = X^n + (\deg \leqslant n-1),$$

где $(\deg \leqslant n-1)$ означава полином степена мањег од $n-1$. Тада је

$$\alpha^n + (\deg \leqslant n-1) = 0,$$

односно

$$\alpha^n = -(\deg \leqslant n-1).$$

Дакле, α^n припада линеалу $\mathcal{L}(e)$. Сада је $\alpha^{n+1} \in \mathcal{L}(e \cup \{\alpha^n\}) = \mathcal{L}(e)$. Сада се индукцијом покаже да за свако $k \geqslant n$ важи $\alpha^k \in \mathcal{L}(e)$.

– *Линеарна независност.* Нека је $a_0 + a_1\alpha + ... + a_{n_1}\alpha^{n-1} = 0$. Тада за

$$p(X) = a_{n-1}X^{n-1} + ... + a_1X + a_0$$

важи $p(\alpha) = 0$, Међутим, како је $\deg p < \deg \mu$, мора бити $p \equiv 0$, односно

$$a_0 = a_1 = ... = a_{n-1} = 0.$$

($\Leftarrow$) Посматрајмо $\frac{1}{\alpha} \in K(\alpha) = K[\alpha]$. Постоји $p \in K[X]$ такав да је $\frac{1}{\alpha} = p(\alpha)$, па је $p(\alpha)\alpha - 1 = 0$, тј. α је корен ненула полинома

$$q(X) = Xp(X) - 1.$$

Последица: (због 1) Услов (*) можемо заменити са (**).

деф. Нека је $K \leq L$, $K(\alpha)$ просто раширење поља K и $\alpha_1, \dots, \alpha_n \in L$.

$$K[\alpha_1, \dots, \alpha_n] := \underbrace{K[\alpha_1, \dots, \alpha_{n-1}]}[\alpha_n];$$

$$K(\alpha_1, \dots, \alpha_n) := K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n).$$

Напомена: $K(\alpha_1, \dots, \alpha_n)$ је минимално поље које садржи $K \cup \{\alpha_1, \dots, \alpha_{n-1}\}$.

Теорема 3: Нека је $K \leq L$ и $\alpha_1, \dots, \alpha_n \in L$.

Ако је за свако $1 \leq r \leq n$, елемент α_r алгебарски над $K(\alpha_1, \dots, \alpha_{r-1})$

тада је $K[\alpha_1, \dots, \alpha_r] = K(\alpha_1, \dots, \alpha_r) = K_r$ и сви елем. у пољу K_r су алгебарски.

Доказ:

Доказ. Прва део тврђења следи индукцијом из претходне теореме и претходне дефиниције

$$K(\alpha_1, \alpha_2, ..., \alpha_r) = K(\alpha_1, \alpha_2, ..., \alpha_{r-1})(\alpha_r) = K(\alpha_1, \alpha_2, ..., \alpha_{r-1})[\alpha_r].$$

Нека је $\alpha \in K_r$. По претходној теореми важи

$$[K_r : K] = \underbrace{[K_r : K_{r-1}]}_{\deg \mu_r} \underbrace{[K_{r-1} : K_{r-2}]}_{\deg \mu_{r-1}} \cdots \underbrace{[K_1 : K]}_{\deg \mu_1}.$$

Како је $K(\alpha)$ векторски потпростор од K_r, то је $[K(\alpha) : K] \leqslant [K_r : K] < +\infty$, а самим тим је и $K(\alpha) \supseteq [1, \alpha, \alpha^2, ...]$ линеарно зависан. Дакле, α је алгебарски над K.

Допуна дефиниције:

деф. Нека је $K \leq L$.
Алгебарско затворење је скуп $K[L]$ свих алгебарских елем. над K који се налазе у L.

Специјално, елем. скупа $\mathbb{Q}[\mathbb{C}]$ зову се алгебарски бројеви.

Теорема 4: $K[L]$ је потпоље од L.

Доказ:

Доказ. Довољно је доказати да за $\alpha, \beta \in K[L] \setminus \{0\}$ важи да су $\alpha - \beta$ и $\alpha^{-1}\beta$ у $K[L]$. То важи тривијално, јер су по претходном тврђењу сви елементи из $K(\alpha, \beta)$ алгебарски над K, па је

$$\alpha - \beta, \alpha^{-1}\beta \in K(\alpha, \beta) \subseteq K[L].$$

деф. Раширење L од K је алгебарско раширење ако је $K[L] = L$.

Теорема 5: Ако је $[L:K] < \infty \Rightarrow$ L је алгебарско раширење од K.

Доказ:

Доказ. За $\alpha \in L$ важи $K(\alpha) \leqslant L$, па је $[K(\alpha) : K] < +\infty$. Дакле, систем $[1, \alpha, \alpha^2, ...] \subseteq K(\alpha)$ је линеарно зависно, па је α алгебарски.
Напомена. Обрнуто не важи, тј. алгебарска раширења не морају бити коначна. На пример $[\mathbb{Q}[\mathbb{C}] : \mathbb{Q}]$ није коначан.

18. Коренско поље полинома

деф. Раширење L поља K је **коренско поље полинома** $p \in K[X]$ ако постоје $\alpha_1, \dots, \alpha_n \in L$ ткд:

1) $L = K[\alpha_1, \dots, \alpha_n]$;

2) $p(x) = a(x-\alpha_1)\dots(x-\alpha_n)$, за неко $a \in K$.

Теорема 1 (Кронекерова конструкција):

Нека је K поље и $f \in K[X] \setminus \{0\}$ нерастављив, моничан полином. Тада важи:

1) $L = K[X]/\langle f \rangle$ је поље и то раширење поља K;

2) Полином f има барем један корен α у L, и важи: $L = K(\alpha)$;

3) $[L:K] = \deg f$. (следи из претходног)

Доказ:

Доказ.

(1) Докажимо прво да је L поље. То је еквивалентно са тим да је $\langle f(X)\rangle$ максималан идеал од $K[X]$. Заиста, ако би било $\langle f(X)\rangle \leqslant I \lhd K[X]$, тада би постојало $p(X) \in I$, такво да $f \mid p$, па би NZD од f и p био један. Дакле, постоје u и v такви да је

$$\underbrace{up + vf}_{\in I} = 1,$$

па би морало бити $I = K[X]$. Покажимо сада да је L раширење од K. Посматрајмо пресликавање $F : K \to K_0$ задатко са $F(c) = c + \langle f(X)\rangle$. Овако пресликавање је изоморфизам. F је хомоморфизам прстена, јер је

$$F(c+d) = c + d + \langle f(X)\rangle = (c + \langle f(X)\rangle) + (d + \langle f(X)\rangle) = F(c) + F(d),$$

$$F(cd) = cd + \langle f(X)\rangle = (c + \langle f(X)\rangle)(d + \langle f(X)\rangle) = F(c)F(d)$$

и $F(1) = 1 + \langle f(X)\rangle$. Функција F је по конструкцији бијекција. Тиме смо показали да је K изоморфно са потпољем K_0, дакле L је раширење од K. Можемо поистоветити K_0 и K у наставку.

(2) Нека је $f(X) = a_n X^n + \dots + a_1 X + a_0 \in K[X]$. Тада у L важи

$$\begin{aligned} f(X + \langle f(X)\rangle) &= a_n(X + \langle f(X)\rangle)^n + \dots + a_0(1 + \langle f(X)\rangle) \\ &= (a_n + \langle f(X)\rangle)(X^n + \langle f(X)\rangle) + \dots + (a_0 + \langle f(X)\rangle)(1 + \langle f(X)\rangle) \\ &= (a_n X^n + \dots + a_1 X + a_0) + \langle f(X)\rangle \\ &= f(X) + \langle f(X)\rangle \\ &= 0 + \langle f(X)\rangle \in L. \end{aligned}$$

Ако је $r(X)$ остатак при дељењу неког полинома $p \in K[X]$ са $f(X)$, онда је

$$p(X) + \langle f(X)\rangle = r(X) + \langle f(X)\rangle,$$

јер је $p(X) = q(X)f(X) + r(X)$, па је $q(X)f(X) \in \langle f(X)\rangle$, а $p(X)$ можемо схватити као $p(X) + \langle f(X)\rangle$ у $K_0[X]$. Одакле следи да је

$$L = \{a_0 + a_1 X + \dots + a_{n-1}X^{n-1} + \langle f(X)\rangle \mid a_0, a_1, \dots, a_{n-1} \in K\},$$

где је $n = \deg f$. Покажимо да је $\alpha = X + \langle f(X)\rangle$. Довољно је доказати да је минимални полином за α баш f, јер је онда $[1, \alpha, \dots, \alpha^{n-1}]$ база за $K_0(\alpha)$ над K_0. Приметимо да увек важи ако је f моничан и нерастављив полином, такав да је $f(\alpha) = 0$, онда је f минималан полином за α. Претходно важи тривијално, јер ако је g минималан полином, тада $g \mid f$, на како је f нерастављив и оба су монична, мора бити $f = g$. Дакле, довољно је доказати да је f нерастављив, што јесте по претпоставци. Дакле, f је минималан полином за α над K, односно K_0.

Теорема 2: Нека је K поље.
Тада сваки полином $p \in K[X]$ степена највише n има бар једно коренско поље $F = K[\alpha_1, \dots, \alpha_n]$.

Уз то, ако је $\sigma: c \to \bar{c}$ изоморфизам K и неког поља $\bar{K}$
и ако је $\bar{F}$ коренско поље полинома $\bar{p} = \sum_{i=0}^{n} \bar{a}_i x^i$ (где је $p = \sum_{i=0}^{n} a_i x^i$), тада је $F \cong \bar{F}$.

Доказ:

Доказ. Први део доказа изводимо индукцијом по n.

(БИ) Ако је $n = 1$, тада је $F = K = K[\alpha_1]$, где је $\alpha_1 \in K$.

(ИХ) Претпоставимо да тврђење важи за n.

(ИК) Нека је f нерастављив полином за који је $f \mid p$. Тада постоји поље $L = K[\alpha_1]$ такво да је α_1 нула полинома f. Тада је $p(X) = (X - \alpha_1)h(X)$, где је $h \in L[X]$. Како је $\deg h = \deg p - 1$, по индуктивној претпоставци постоји $F \geqslant L$ такво да је

$$F = L[\beta_1, \beta_2, ..., \beta_{n-1}]$$

и

$$h(X) = c(X - \beta_1)...(X - \beta_{n-1}).$$

Сада је

$$F = K[\alpha_1][\beta_1, \beta_2, ..., \beta_{n-1}] = K[\alpha_1, \beta_1, ..., \beta_{n-1}]$$

и

$$p(X) = c(X - \alpha_1)(X - \beta_1)...(X - \beta_{n-1}).$$

Тиме је показана егситенција коренског поља. Други део теореме нам каже да је за сваки полином коренско поље јединствено до на изоморфизам. Покажимо то. Нека је $f \mid p$ нерастављив. Тада је $\overline{f}$ такође нерастављив и важи

$$K[X]/\langle f(X)\rangle \cong \overline{K}[X]/\langle \overline{f}(X)\rangle.$$

Нека је $F = K[\alpha_1, \alpha_2, ..., \alpha_n]$ и $\overline{F} = \overline{K}[\beta_1, \beta_2, ..., \beta_n]$. Можемо узети да је α_1 нула полинома f, а β_1 нула полинома $\overline{f}$. Тада је

$$K[\alpha_1] \cong K[X]/\langle f(X)\rangle \text{ и } \overline{K}[\beta_1] \cong \overline{K}[X]/\langle \overline{f}(X)\rangle.$$

Јасно, $F = K[\alpha_1, \alpha_2, ..., \alpha_n]$ је коренско поље полинома $\dfrac{p}{X - \alpha_1} \in K[\alpha_1][X]$, а $\overline{F} = K[\beta_1, \beta_2, ..., \beta_n]$ је коренско поље полинома $\dfrac{\overline{p}}{X - \beta_1} \in K[\beta_1][X]$. Као и у првом делу, користимо индукцију, желимо да је по (ИХ) $F \cong \overline{F}$. Међутим, ово је тачно јер за изоморфизам $\Phi : K[\alpha_1] \to \overline{K}[\beta_1]$ важи да се c слика у $\bar{c}$, за свако $c \in K$ и $\alpha_1 \mapsto X + \langle f(X)\rangle \mapsto \overline{X} + \langle \overline{f}(X)\rangle \mapsto \beta_1$, па полиному $\dfrac{p}{X - \alpha_1}$ одговара полином $\dfrac{\overline{p}}{X - \beta_1}$.

19. Примитивни елементи

деф. **Карактеристика** кпј K, у ознаци $\operatorname{char} K$, је најмањи природан број n такав да $\underbrace{1+1+\ldots+1}_{n} \cdot 1 = 0$.

Ако такав број не постоји, K је **карактеристике нула**.

Примери: 1) $\operatorname{char} \mathbb{Z}_n = n$; 2) $\operatorname{char} \mathbb{Z} = 0$; 3) $\operatorname{char} \mathbb{Z}_n[X] = n$;

Напомена: Карактеристика поља је увек прост број.

Доказ: ппс. $p = n \cdot m \Rightarrow 0 = nm \cdot 1 = (n \cdot 1) \cdot (m \cdot 1) \Rightarrow n \cdot 1 = 0$ или $m \cdot 1 = 0$ ↯

Лема 1: Мултипликативна група коначног поља је циклична.

Доказ:

Доказ. Нека је F посматрано поље и $F^* = F \setminus \{0\}$. Како је F^* Абелова група и како је коначна по претпоставци, то има нормалну форму

$$F^* \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \ldots \times \mathbb{Z}_{d_k},$$

где важи $d_1 \mid d_2 \mid \ldots \mid d_k$. Одавде је ред сваког елемента из F^* делилац од d_k, па за све $\alpha \in F^*$ важи $\alpha^{d_k} = 1$. Самим тим, полином $X^{d_k} - 1$ има барем $|F^*|$ нула у F^*. Како он има ньавише d_k нула и $|F^*| = d_1 d_2 \ldots d_k$, то мроа бити $k = 1$, одакле следи тврђење.

деф. Нула полинома f је **проста** ако $(x-\alpha) \mid f$, $(x-\alpha)^2 \nmid f$.

Лема 2: Полином $f \in K[X]$ степена бар 1 има све просте нуле $\Leftrightarrow$ f је узајамно прост са f'. (извод)

Специјално, нуле нерастављивог полинома f су просте $\Leftrightarrow$ $f' \neq 0$.

Доказ:

Доказ. Нека је $d \in K[X]$ неки NZD за f и f'. Тада постоје $u, v \in K[X]$ такво да је $uf + vf' = d$.

($\Leftarrow$) Нека је $d = 1$. Тада, ако је α нула од f и f', онда $X - \alpha \mid uf + vf'$ у $F[X]$, где је F коренско поље. Контрадикција.

($\Rightarrow$) Ако $d \notin K$, тада d у $F[X]$ има нулу α, тј. $X - \alpha \mid d$. Међутим, $d \mid f$ и $d \mid f'$, па је α нула f и f'.

Ако је f нераставиљв, онда је NZD од f и f' баш f или 1. При томе је једнак f ако и само ако $f \mid f'$ што је еквивалнетно с тим да је $f' = 0$, јер је $\deg f' < \deg f$.

Теорема 1 (Теорема о примитивном елементу):

Нека је K коначно поље или поље карактеристике нула.

Ако је L коначно раширење од K, тада постоји $\alpha \in L$ такво да $L = K[\alpha]$.

(елемент α је примитивни елемент раширења L над K)

Доказ:

Доказ. Прво, постоје $\alpha_1, \alpha_2, ..., \alpha_n$ такви да је $L = K(\alpha_1, \alpha_2, ..., \alpha_n)$. Њих можемо изабрати тако да је $\alpha_1 \in L \setminus K$, тада је $[K(\alpha_1) : K] > 1$, па је $[L : K(\alpha_1)] < [L : K]$. Затим наставимо поступак за L и $K(\alpha_1)$. Довољно је доказ извести за $n = 2$. Заиста, тада доказ можемо извести индукцијом

$$K(\alpha_1, \alpha_2, ..., \alpha_n) = \underbrace{K(\alpha_1, \alpha_2, ..., \alpha_{n-1})}_{K(\alpha)}(\alpha_n) = K(\alpha)(\alpha_n) = K(\alpha, \alpha_n) = K(\beta).$$

Посматрајмо $L = K(\alpha, \beta)$. Нека су p и q минимални полиноми за α и β, редом, и нека су $\alpha_1, \alpha_2, ..., \alpha_k$ и $\beta_1, \beta_2, ..., \beta_l$ преостале нуле полинома p, односно q у неком коренском пољу. Нека је

$$L' = K(\alpha, \beta, \alpha_1, ..., \alpha_k, \beta_1, ..., \beta_l).$$

Тражимо $\lambda = \alpha + c\beta$, за неко $c \in K$. Нека је $F = K(\lambda)$. Јасно, $F \leqslant L$ и $F \leqslant L'$. Нека је

$$f(X) = p(\lambda - cX) \in F[X],$$

где је $\deg f = \deg p$. Важи

$$f(\beta) = p(\alpha) = 0,$$

где је β заједничка нула за f и q. Изаберемо c такво да је $\lambda - c\beta_i \neq \alpha_j$, односно да је $\alpha + c\beta \neq \alpha_j + c\beta_i$, тј.

$$c \neq \frac{\alpha_j - \alpha}{\beta_i - \beta}.$$

Идеја нам је да β буде једина заједничка нула за f и q. Ако је K карактеристике нула, за нерастављив полином s важи $s' \neq 0$. Дакле, p и q немају вишеструке нуле. Сада g и f имају тачно једну заједничку нулу, вишеструкости 1,па како се факторишу на линеарне факторе у $L'[X]$, то им је НЗД $X - \beta$ у $L'[X]$. Како су f и q из $F[X]$, то је $X - \beta \in F[X]$, па је $\beta \in F$. Одатле је и $\alpha \in F$, па је $F = L$. Случај када је K коначно је тривијалан, јер је тада и L коначно, па према претходној теореми $L^* = L \setminus \{0\}$ је циклична, па постоји $\alpha \in F^*$ такво да је

$$F^* = \{\alpha^k \mid k \geqslant 0\}.$$

Тада је $K(\alpha) = L$.