

# АЛГЕБРА 3 (ППТГ)

ВОРИША КУЗЕЉЕВИЋ И ПЕТАР МАРКОВИЋ

Ово је преглед материјала који је обрађен у зимском семестру 2024. године на курсу *Алгебра 3*. Основна литература су предавања професора Груловића [3, 2] и додаци професора Марковића [8]. Литература за задатке су збирке професора Груловића [4], као и наша збирка [5]. Виште информација може се пронаћи у стандардним књигама из Алгебре, на пример [6, 9, 7, 1].

Мала напомена о нотацији: скуп природних бројева увек означавамо  $\mathbb{N} = \{1, 2, 3, \dots\}$ , скуп рационалних бројева увек означавамо  $\mathbb{Q}$ , скуп реалних бројева увек означавамо  $\mathbb{R}$ , а скуп комплексних бројева увек означавамо  $\mathbb{C}$ . Ове четири ознаке никад неће означавати ништа друго. Обратите пажњу да, на пример, ознаке  $\mathbb{N}$  и  $N$  не сматрамо истим, па ознака  $N$  може означавати разне објекте у овом материјалу. Ако је  $f : A \rightarrow B$  функција и  $X \subseteq A$  и  $Y \subseteq B$  онда је  $f[X] = \{f(x) : x \in A\}$  и  $f^{-1}[Y] = \{x \in A : f(x) \in Y\}$ .

Испитна питања су наслови секција у овом фајлу, питања обележена звездицом треба знати само ако се одговара за оцене девет и десет. Студенти који имају фонд часова мањи од 4 + 2 не одговарају питања чији наслов почиње са  $x -$ .

## Садржај

1. Дефиниција и основне особине прстена	2
2. Потпрстени, хомоморфизми прстена	4
3. Идеали	5
4. Главни и прости идеали	5
5. Фактор прстен, количничко поље интегралног домена	6
6. $x -$ Мреже потпрстена, левих идеала, десних идеала и идеала	6
7. Лема Цасенхауса, Теореме о изоморфизму и Теорема о кореспонденцији у прстенима	7
8. $x -$ Директни производи и директне суме прстена. Унутрашње суме	7
9. Кинеска теорема о остацима	8
10. Идеали комутативних прстена	9
11. Еуклидови домени и домени главних идеала	9
12. Домени једнозначне факторизације 1	10
13. Домени једнозначне факторизације 2	10
14. $x -$ *Домени једнозначне факторизације 3	11
15. $x -$ Домени једнозначне факторизације 4	11
16. Несводљивост полинома	11
17. Основне особине поља	12
18. Кронекерова теорема	12
19. Алгебарски затворена поља	12
20. $x -$ *Лема о пропширењу утапања поља	13
21. Минимално потпоље и поље разлагања	13
22. Нормална проширења	13
23. $x -$ Карактеризација нормалних проширења	13
24. Сепарабилна проширења	14
25. Теорија Галоа	14
26. Конструкције шестаром и лењиром	14
Литература	17

## 1. ДЕФИНИЦИЈА И ОСНОВНЕ ОСОБИНЕ ПРСТЕНА

**Дефиниција 1.** Прстен је алгебарска структура са две операције  $R = (R; +, \cdot)$  таква да важи:

- $(R; +)$  је Абелова група,
- $(R; \cdot)$  је полујупа ( $\cdot$  је асоцијативна операција),
- множење се дистрибуира према сабирању и са леве и са десне стране; другим речима, за све елементе  $x, y, z \in R$  важе једнакости

$$x(y+z) = xy + xz \text{ и } (y+z)x = yx + zx.$$

Неутрални елемент за сабирање прстена обично се обележава са  $0$ , а инверзни елемент за сабирање елемента  $a \in R$  обично се обележава са  $-a$ . Џакле, за све  $a \in R$  је  $a + (-a) = 0$ . За прстен  $R$  кажемо да је *прстен са јединицом* ако постоји неутрални елемент за множење. Приметимо да је неутрални елемент за множење, ако постоји, јединствен јер ако би  $e_1$  и  $e_2$  били такви, имали бисмо  $e_1 = e_1 e_2 = e_2$ . Неутрални елемент за множење прстена  $R$  обично обележавамо са  $1$  и зовемо јединица прстена  $R$ . За прстен  $R$  кажемо да је *комутативан* ако важи  $xy = yx$  за све  $x, y \in R$ .

**Дефиниција 2.** Нека је  $R$  прстен са јединицом и  $a \in R$ . Кажемо да је  $b \in R$  инверз за  $a$  ако је  $ab = 1$  и  $ba = 1$ . Тада за  $a$  кажемо да је *инвертибилан*, а скуп свих инвертибилних елемената прстена  $R$  обележавамо  $R^*$ .

Приметимо да је инверз за  $a \in R$ , ако постоји, јединствен. Наиме, ако су  $b_1$  и  $b_2$  инверзи за  $a$ , имамо  $b_1 = b_1 1 = b_1 ab_2 = 1b_2 = b_2$ . Инверз елемента  $a$  означавамо са  $a^{-1}$ .

**Дефиниција 3.** За комутативан прстен са јединицом у коме су сви ненула елементи инвертибилни кажемо да је *поле*.

**Пример 4.** Приметимо да су  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  комутативни прстени са јединицом, при чему  $\mathbb{Z}$  није поље док  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  то јесу.

**Пример 5.** Приметимо да за све природне бројеве  $n \geq 2$ , скуп  $n \times n$  матрица над пољем реалних бројева чини прстен са стандардним операцијама сабирања и множења матрица. Овај прстен обележавамо  $M_n(\mathbb{R})$ . Генерално, са  $M_n(R)$  обележаваћемо прстен  $n \times n$  матрица над произвољним прстеном  $R$  (на исти начин се проверава да овај скуп чини прстен са стандардним операцијама сабирања и множења матрица).

Ако је  $R$  прстен,  $a \in R$ ,  $n \in \mathbb{Z}$ , елемент  $na$  дефинишемо са

$$na = \begin{cases} \underbrace{a + a + \cdots + a}_n, & \text{ако } n > 0, \\ 0, & \text{ако } n = 0, \\ \underbrace{(-a) + (-a) + \cdots + (-a)}_{-n}, & \text{ако } n < 0. \end{cases}$$

**Тврђење 6.** У сваком прстену  $R$  за све  $x, y \in R$  и све  $n \in \mathbb{Z}$ , важи:

- (1)  $x \cdot 0 = 0 \cdot x = 0$ ,
- (2)  $x \cdot (-y) = (-x) \cdot y = -xy$ ,
- (3)  $(-x)(-y) = xy$ ,
- (4)  $(nx) \cdot y = x \cdot (ny) = nxy$ ,

**Дефиниција 7.** Нека је  $R$  прстен и  $a \in R$ . Кажемо да је  $a$  *делитељ нуле* ако је  $a \neq 0$  и постоји  $b \in R \setminus \{0\}$  такав да је  $ab = 0$  или  $ba = 0$ . Кажемо да је  $a$  *нилпотентан* ако постоји  $n \geq 1$  такав да је  $a^n = 0$ .

Приметимо да је нула увек нилпотентан елемент, да је сваки нилпотентан елемент или нула или делитељ нуле, али да делитељ нуле не мора бити нилпотентан.

**Дефиниција 8.** Кажемо да је  $R$  *интегрални домен* ако је  $R$  комутативан прстен са јединицом без делитеља нуле.

**Тврђење 9.** Свако поље је интегрални домен.

**Пример 10.** Прстен Гаусових целих бројева  $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$  са стандардним операцијама сабирања и множења комплексних бројева јесте интегрални домен.

**Лема 11.** Нека је  $R$  комутативан прстен са јединицом. Тада је  $R$  интегрални домен ако за све  $a, b, c \in R$  из  $ab = ac$  следи да је  $a = 0$  или  $b = c$ .

**Тврђење 12.** У сваком комутативном прстену  $R$  за све  $x, y \in R$  и све *позитивне* целе бројеве  $n$  важи:

$$(x+y)^n = x^n + y^n + \sum_{i=1}^{n-1} \binom{n}{i} x^{n-i} y^i.$$

(Прстен  $R$  не мора да има јединицу, а ако је нема, онда изрази  $x^0$  и  $y^0$  немају смисла. Зато су у овом тврђењу издвојени чланови  $x^n$  и  $y^n$  из суме уместо да пишемо  $x^n y^0$ , односно  $x^0 y^n$ )

**Пример 13.** Ако је  $n$  природан број, са  $n\mathbb{Z}$  обележавамо скуп  $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ , дакле скуп свих целих бројева деливих са  $n$ . Приметимо да је онда  $(n\mathbb{Z}; +, \cdot)$  комутативан прстен где су  $+$  и  $\cdot$  уобичајене операције скупа целих бројева.

**Пример 14.** Ако је  $A$  скуп (може бити и празан), онда се на његовом партитивном скупу  $P(A)$  може дефинисати структура прстена на следећи начин: прстен је  $(P(A); \Delta, \cap)$ , где је  $X \Delta Y := (X \setminus Y) \cup (Y \setminus X)$  симетрична разлика.

Сада дефинишемо прстен остатака по модулу  $n$ , за цео број  $n \geq 2$ . Означимо  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ . Дефинишемо релацију  $\equiv_n$  на скупу целих бројева са: за  $k, m \in \mathbb{Z}$  је

$$k \equiv_n m \text{ ако постоји } q \in \mathbb{Z} \text{ такав да је } qn = m - k.$$

**Лема 15.**  $\equiv_n$  је релација еквиваленције на скупу  $\mathbb{Z}$ , има тачно  $n$  класа еквиваленције, а свака класа садржи тачно један елемент скупа  $\{0, \dots, n-1\}$ .

**Лема 16.** Нека су  $a, b, c$  и  $d$  цели бројеви. Ако је  $a \equiv_n b$  и  $c \equiv_n d$ , онда је

$$a + c \equiv_n b + d \quad \text{и} \quad ac \equiv_n bd.$$

**Дефиниција 17.** Пресликавање  $\pi_n : \mathbb{Z} \rightarrow \mathbb{Z}_n$  дефинишемо на следећи начин:

за  $m \in \mathbb{Z}$ ,  $\pi_n(m)$  је најмањи природан број који је у релацији  $\equiv_n$  са  $m$ .

Приметимо да из Леме 15 следи да је  $\pi_n(m) \in \mathbb{Z}_n$  за сваки цео број  $m$ , и да је заправо  $\pi_n(m)$  остатак при дељењу  $m$  са  $n$ .

**Дефиниција 18.** Дефинишемо операције  $+_n$  и  $\cdot_n$  на  $\mathbb{Z}_n$  на следећи начин: за  $m, k \in \mathbb{Z}_n$  је:

$$m +_n k = \pi_n(m+k) \quad \text{и} \quad m \cdot_n k = \pi_n(mk).$$

Приметимо да из Леме 15 и Леме 16 следи да су ове операције добро дефинисане. Увек ћемо подразумевати да су на  $\mathbb{Z}_n$  дате овако дефинисане операције  $+_n$  и  $\cdot_n$ .

**Теорема 19.**  $\mathbb{Z}_n$  је комутативан прстен са јединицом.

**Лема 20.** Нека су  $k$  и  $m$  цели бројеви различити од нуле и  $d$  њихов највећи заједнички делилац. Тада постоје цели бројеви  $a$  и  $b$  такви да је  $ak + bm = d$ .

**Теорема 21.** Сви инвертибилни елементи у прстену  $\mathbb{Z}_n$  су они који су узајамно прости са  $n$ . Сви делитељи нуле у прстену  $\mathbb{Z}_n$  су они који нису ни нула ни узајамно прости са  $n$ .

**Теорема 22.**  $\mathbb{Z}_n$  је поле ако и само је  $n$  прости број.

**Пример 23.** Нека је  $C[0, 1]$  скуп свих непрекидних функција  $f : [0, 1] \rightarrow \mathbb{R}$ . За  $f, g \in C[0, 1]$  и све  $x \in [0, 1]$ , дефинишемо  $(f \oplus g)(x) = f(x) + g(x)$  и  $(f \odot g)(x) = f(x) \cdot g(x)$ . Сада је  $(C[0, 1], \oplus, \odot)$  прстен, који зовемо прстен непрекидних функција над  $[0, 1]$ .

**Пример 24.** Нека је  $R$  комутативан прстен са јединицом 1. Тада скуп свих полинома над  $R$  са променљивом  $x$  чини прстен са стандардним операцијама сабирања и множења полинома. Овај прстен обележавамо са  $R[x]$ . Приметимо да је полином 1 јединица прстена  $R[x]$ . Прстен полинома више променљивих дефинишемо рекурзивно са  $R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}]) [x_n]$ .

**Дефиниција 25.** Нека је  $p$  прост број. Низ  $\bar{a} = \langle a_n : n \geq 1 \rangle$  називамо  $p$ -адички цео број ако:

- (1)  $0 \leq a_n < p^n$  за све  $n \geq 1$ ;
- (2)  $a_{n+1} \equiv_{p^n} a_n$  за све  $n \geq 1$ .

Скуп свих  $p$ -адичких целих бројева означавамо  $\mathbb{Z}_{[p]}$ .

**Дефиниција 26.** На  $\mathbb{Z}_{[p]}$  дефинишемо две операције  $\oplus$  и  $\odot$  на следећи начин: за  $\bar{a}, \bar{b} \in \mathbb{Z}_{[p]}$  је:

$$\bar{a} \oplus \bar{b} = \langle a_n +_{p^n} b_n \rangle \quad \text{и} \quad \bar{a} \odot \bar{b} = \langle a_n \cdot_{p^n} b_n \rangle.$$

**Лема 27.**  $\oplus$  и  $\odot$  су добро дефинисане операцije на  $\mathbb{Z}_{[p]}$ .

Увек подразумевамо да су на  $\mathbb{Z}_{[p]}$  дате овако дефинисане операције  $\oplus$  и  $\odot$ .

**Тврђење 28.** Нека је  $\bar{a} \in \mathbb{Z}_{[p]}$ . За све  $n, k \geq 1$  је искушено  $a_n \equiv_{p^n} a_{n+k}$ .

**Последица 29.** Ако је  $\bar{a} \in \mathbb{Z}_{[p]}$  такав да је  $a_1 \neq 0$ , онда је  $(a_n, p) = 1$  за све  $n \geq 1$ .

**Последица 30.** Ако је  $\bar{a} \in \mathbb{Z}_{[p]}$  такав да је  $a_1 \neq 0$ , онда је  $a_n \neq 0$  за све  $n \geq 1$ .

**Теорема 31.**  $\mathbb{Z}_{[p]}$  је интегрални домен, а елемент  $\langle a_n \rangle \in \mathbb{Z}_{[p]}$  је инвертибилан ако и само ако је  $a_1 \neq 0$ .

**Дефиниција 32.** Карактеристика прстена  $R$  је најмањи позитиван цео број  $n$  такав да је  $na = 0$  за све  $a \in R$ , ако такав позитиван цео број постоји. Ако такав број не постоји, онда кажемо да је  $R$  карактеристике нула. Карактеристику прстена  $R$  обележавамо са  $\text{char}(R)$ .

**Тврђење 33.** Ако је  $R$  прстен са 1, онда је  $\text{char}(R)$  једнак реду елемената 1 у прстену  $(R; +)$ , док  $\text{char}(R) = 0$  ако 1 нема коначан ред.

## 2. ПОТПРСТЕНИ, ХОМОМОРФИЗМИ ПРСТЕНА

**Дефиниција 34.** Нека је  $R$  прстен. Кажемо да је  $T \subseteq R$  подпрстен прстена  $R$ , ако и сам чини прстен са рестрикцијама  $+|_{T \times T}$  и  $\cdot|_{T \times T}$  операција из прстена  $R$ . Пишемо  $T \leq R$ .

Приметимо да према претходној дефиницији  $\mathbb{Q}$  јесте потпрстен прстена  $\mathbb{R}$  јер јесте  $\mathbb{Q} \subseteq \mathbb{R}$  и сабирање и множење у  $\mathbb{Q}$  су наслеђене из  $\mathbb{R}$ . Са друге стране  $\mathbb{Z}_n$  није потпрстен прстена  $\mathbb{Z}$  јер иако је  $\mathbb{Z}_n \subseteq \mathbb{Z}$ , операције у  $\mathbb{Z}_n$  су сабирање и множење по модулу  $n$ , а операције у  $\mathbb{Z}$  су класично сабирање и множење. Конечно,  $n\mathbb{Z}$  јесте потпрстен прстена  $\mathbb{Z}$  јер је  $n\mathbb{Z} \subseteq \mathbb{Z}$  и операције у  $n\mathbb{Z}$  су рестрикције операција из  $\mathbb{Z}$ .

Сваки прстен  $R$  има два привидна потпрстена, то су нула прстен  $\{0\}$  и цео прстен  $R$ .

**Пример 35.** Сви потпрстени прстена  $\mathbb{Z}$  су облика  $n\mathbb{Z}$  за  $n \geq 0$ .

**Лема 36.** Нека је  $R$  прстен. Тада је  $T \subseteq R$  подпрстен прстена  $R$  ако и само ако је:

- (1)  $x - y \in T$  за све  $x, y \in T$ ;
- (2)  $xy \in T$  за све  $x, y \in T$ .

**Лема 37.** Нека је  $R$  прстен. Тада важи:

- (1) Ако је  $\mathcal{A}$  фамилија подпрстена  $R$ , онда је  $\bigcap \mathcal{A}$  шакоће подпрстен од  $R$ ;
- (2) Ако је  $\mathcal{L}$  ланац подпрстена  $R$ , онда је  $\bigcup \mathcal{L}$  шакоће подпрстен прстена  $R$  (ланац значи да је за све  $T_1, T_2 \in \mathcal{L}$  исуђено  $T_1 \subseteq T_2$  или  $T_2 \subseteq T_1$  - приметимо да исуди доказ даје  $\bigcup \mathcal{D} \leq R$  и за првоизвољну на тај начин  $\mathcal{D}$  подпрстена од  $R$ , јер је фамилију шакву да за све  $T_1, T_2 \in \mathcal{D}$  постоји  $T_3 \in \mathcal{D}$  шакав да је  $T_1 \cup T_2 \subseteq T_3$ ).

**Дефиниција 38.** Нека су  $(R, +_R, \cdot_R)$  и  $(T, +_T, \cdot_T)$  прстени. Кажемо да је  $\varphi : R \rightarrow T$  хомоморфизам из  $R$  у  $T$  ако је:

- (1)  $\varphi(x +_R y) = \varphi(x) +_T \varphi(y)$  за све  $x, y \in R$ ;
- (2)  $\varphi(x \cdot_R y) = \varphi(x) \cdot_T \varphi(y)$  за све  $x, y \in R$ ;

**Лема 39.** Нека су  $R, S, T$  прстени и нека су  $\varphi : R \rightarrow S$  и  $\psi : S \rightarrow T$  хомоморфизми. Тада је  $\psi \circ \varphi : R \rightarrow T$  хомоморфизам.

**Дефиниција 40.** Нека су  $R$  и  $T$  прстени и  $\varphi : R \rightarrow T$  хомоморфизам. Кажемо да је  $\varphi$  подобарење ако је  $\varphi$  1-1 пресликавање. Кажемо да је  $\varphi$  изоморфизам ако је  $\varphi$  бијекција. Ако су прстени  $R$  и  $T$  изоморфни, пишемо  $R \cong T$ .

**Лема 41.** Нека су  $R$  и  $T$  прстени и нека је  $\varphi : R \rightarrow T$  изоморфизам прстена. Тада је  $\varphi^{-1}$  изоморфизам.

**Лема 42.** Нека су  $R$  и  $T$  прстени и  $\varphi : R \rightarrow T$  хомоморфизам који је 'на'. Тада:

- (1) Ако је  $R$  комутативан, онда је и  $T$  комутативан;
- (2) Ако  $R$  има јединицу, онда и  $T$  има јединицу;
- (3) Ако је  $\text{char}(R) \neq 0$ , онда је и  $\text{char}(T) \neq 0$  и  $\text{char}(T)$  делу  $\text{char}(R)$ .

**Пример 43.** Постоји континуум много различитих потпрстена  $C[0, 1]$ .

**Пример 44.** Постоји континуум много неизоморфних потпрстена  $\mathbb{Q}$ .

**Лема 45.** Нека су  $R$  и  $T$  прстени и  $\varphi : R \rightarrow T$  хомоморфизам. Тада је  $\varphi(R)$  подпрстен прстена  $T$ .

**Дефиниција 46.** Нека је  $R$  прстен и  $X \subseteq R$ . Дефинишемо  $\langle X \rangle_p$  као најмањи потпрстен прстена  $R$  који садржи  $X$  као подскуп. Ако је  $a \in R$  онда скраћено обележавамо  $\langle a \rangle_p = \langle \{a\} \rangle_p$ .

**Дефиниција 47.** Нека је  $R$  комутативан прстен са јединицом,  $S \leq R$  и  $Y \subseteq R$  непразан. Дефинишемо

$$S[Y] = \{f(y_1, \dots, y_n) : f \in S[x_1, \dots, x_n], n > 0, y_1, \dots, y_n \in Y\}.$$

**Лема 48.** Нека је  $R$  комутативан прстен са јединицом,  $S \leq R$ ,  $1 \in S$  и  $Y \subseteq R$  непразан подскуп. Тада је  $\langle S \cup Y \rangle_p = S[Y]$ .

### 3. ИДЕАЛИ

**Дефиниција 49.** Нека је  $R$  прстен. Кажемо да је потпрстен  $I \leq R$  идеал прстена  $R$  ако је  $ar \in I$  и  $ra \in I$  за све  $a \in I$  и  $r \in R$ . Пишемо  $I \triangleleft R$ .

У прстену  $R$  скупови  $\{0\}$  и цео прстен  $R$  су *тритивијални* идеали. За идеал  $I \triangleleft R$  кажемо да је *прави* ако је  $I \neq R$ .

**Лема 50.** Нека је  $R$  прстен. Тада је  $I \subseteq R$  идеал прстен ако и само ако је:

- (1)  $a - b \in I$  за све  $a, b \in I$ ;
- (2)  $ar \in I$  и  $ra \in I$  за све  $a \in I$  и  $r \in R$ .

**Лема 51.** Нека је  $R$  прстен. Тада:

- (1) Ако је  $\mathcal{A}$  фамилија идеала прстена  $R$ , онда је  $\bigcap \mathcal{A}$  тачкоје идеал у  $R$ ;
- (2) Ако је  $\mathcal{A}$  највећа усмерена фамилија идеала у  $R$ , онда је  $\bigcup \mathcal{A} \triangleleft R$  (приметимо да је специјалан случај овога када је  $\mathcal{A}$  ланац).

Ако су  $R$  и  $T$  прстени и  $\varphi : R \rightarrow T$  хомоморфизам, онда  $\ker(\varphi) = \{a \in R : \varphi(a) = 0\}$  називамо *језиро* хомоморфизма  $\varphi$ .

**Лема 52.** Нека су  $R$  и  $T$  прстени и  $\varphi : R \rightarrow T$  хомоморфизам. Тада је  $\ker(\varphi) \triangleleft R$ .

**Лема 53.** Нека су  $R$  и  $T$  прстени и  $\varphi : R \rightarrow T$  хомоморфизам. Тада је  $\varphi$  1-1 пресликавање ако је  $\ker(\varphi) = \{0\}$ .

**Лема 54.** Нека су  $R$  и  $T$  прстени и  $\varphi : R \rightarrow T$  хомоморфизам. Тада:

- (1) Ако је  $I \triangleleft T$ , онда је  $\varphi^{-1}[I] \triangleleft R$ .
- (2) Ако је  $\varphi$  'на' хомоморфизам и  $I \triangleleft R$ , онда је  $\varphi[I] \triangleleft T$ .

**Тврђење 55.** Нека је  $R$  прстен са јединицом. Тада је идеал  $I \triangleleft R$  прави ако и само ако је  $I \cap R^* = \emptyset$ .

**Дефиниција 56.** Нека је  $R$  прстен. Кажемо да је  $I$  максималан идеал прстена  $R$  ако је  $I \triangleleft R$  прави идеал и ако не постоји  $J \triangleleft R$  такав да је  $I \subsetneq J \subsetneq R$ .

**Пример 57.** Постоји континуум много максималних идеала у  $C[0, 1]$ .

**Тврђење 58.** Нека је  $R$  прстен и  $X \subseteq R$  такав да  $0 \notin X$ . Тада постоји  $I \triangleleft R$  који је максималан међу идеалима који су генерирани са  $X$ .

**Последица 59.** Нека је  $R$  прстен са јединицом који има више од једног елемената. Тада  $R$  има максималан идеал.

**Теорема 60.** Нека је  $R$  комутативан прстен са јединицом. Тада је  $R$  поле ако и само ако су једини чланови идеали тритивијални:  $\{0\}$  и  $R$ .

**Дефиниција 61.** Нека је  $R$  прстен и  $X \subseteq R$ . Дефинишемо  $\langle X \rangle_i$  као најмањи идеал прстена  $R$  који садржи  $I$  као подскуп. Ако је  $a \in R$  онда скраћено обележавамо  $\langle a \rangle_i = \langle \{a\} \rangle_i$ .

**Пример 62.** Ако посматрамо прстен  $\mathbb{Q}$ , онда је  $\langle 1 \rangle_p = \mathbb{Z}$  или  $\langle 1 \rangle_i = \mathbb{Q}$ .

**Дефиниција 63.** Нека је  $R$  прстен и  $I, J \triangleleft R$ . Дефинишемо  $I + J = \{a + b : a \in I, b \in J\}$ .

**Тврђење 64.** Нека је  $R$  прстен, и  $I, J \triangleleft R$ . Тада је  $I + J \triangleleft R$ .

**Тврђење 65.** Ако је  $R$  прстен и  $\mathcal{A}$  фамилија идеала прстена  $R$ , онда је

$$\left\langle \bigcup \mathcal{A} \right\rangle_i = \{a_1 + \cdots + a_n : n > 0, (\forall i \leq n)(\exists I \in \mathcal{A}) a_i \in I\}.$$

### 4. ГЛАВНИ И ПРОСТИ ИДЕАЛИ

**Дефиниција 66.** Нека је  $R$  прстен и  $I \triangleleft R$ . Кажемо да је  $I$  главни идеал ако постоји елемент  $a \in R$  такав да је  $I = \langle a \rangle_i$ .

Приметимо да у зависности од особина прстена, можемо потпуно описати главни идеал генерисан елементом:

- (1) Ако је  $R$  комутативан прстен са јединицом, онда је

$$\langle a \rangle_i = Ra = \{ra : r \in R\}.$$

- (2) Ако је  $R$  комутативан прстен без јединице, онда је

$$\langle a \rangle_i = \{ra + na : r \in R, n \in \mathbb{Z}\}.$$

(3) Ако је  $R$  прстен са јединицом који није комутативан, онда је

$$\langle a \rangle_i = \left\{ \sum_{i=1}^n r_i a s_i : n > 0, r_i, s_j \in R \right\}.$$

(4) Ако прстен  $R$  није комутативан и нема јединицу, онда је

$$\langle a \rangle_i = \left\{ \sum_{i=1}^m r_i a s_i + ra + as + na : m > 0, n \in \mathbb{Z}, r, s, r_i, s_j \in R \right\}.$$

**Дефиниција 67.** Нека је  $R$  прстен и  $I, J \triangleleft R$ . Дефинишемо  $IJ = \{\sum_{i=1}^n a_i b_i : n > 0, a_i \in I, b_j \in J\}$ .

**Тврђење 68.** Нека је  $R$  прстен и  $I, J \triangleleft R$ . Тада је  $IJ \triangleleft R$ .

**Теорема 69.** Нека је  $n \geq 2$  и нека је  $R$  прстен са јединицом. Тада је  $I \triangleleft M_n(R)$  ако и само ако  $\forall a \in I, a \in M_n(J)$ .

**Дефиниција 70.** Нека је  $R$  прстен и  $I$  прави идеал прстена  $R$ . Кажемо да је  $I$  прости идеал ако за све идеале  $J, K \triangleleft R$ , из  $JK \subseteq I$  следи  $J \subseteq I$  или  $K \subseteq I$ .

**Лема 71.** Нека је  $R$  комутативан прстен и  $I$  прави идеал прстена  $R$ . Тада је  $I$  прости идеал ако и само ако за све  $a, b \in R$ , из  $ab \in I$  следи  $a \in I$  или  $b \in I$ .

Приметимо да је  $\{0\}$  прост идеал у сваком интегралном домену.

**Пример 72.** Претходна лема не важи у некомутативним прстенима.

**Теорема 73.** Нека је  $n > 1$ . Тада је идеал  $n\mathbb{Z}$  прости идеал прстена  $\mathbb{Z}$  ако и само ако је  $n$  прости број.

**Лема 74.** Нека је  $R$  прстен са јединицом и  $I \triangleleft R$  максималан идеал. Тада је  $I$  прости идеал.

**Лема 75.** Нека је  $R$  комутативан прстен са јединицом и  $S$  скуп делилаца нуле у  $R$ . Тада скуп  $S \cup \{0\}$  садржи бар један прости идеал.

**Пример 76.** Прост идеал који није максималан (у прстену полинома са целобројним коефицијентима).

## 5. ФАКТОР ПРСТЕН, КОЛИЧНИЧКО ПОЉЕ ИНТЕГРАЛНОГ ДОМЕНА

**Лема 77.** Нека је  $R$  прстен и  $T \leq R$ . Дефинишемо  $R/T = \{r + T : r \in R\}$  и сабирање  $(r + T) + (r' + T) = (r + r') + T$  и множење  $(r + T)(r' + T) = rr' + T$  кошета за  $r, r' \in R$ . Тада су сабирање и множење кошета добро дефинисане операције на  $R/T$  ако је  $T$  идеал прстена  $R$ . У том случају,  $(R/T; +, \cdot)$  је прстен.

**Лема 78.** Нека је  $R$  прстен и  $I \triangleleft R$ . Тада је пресликавање  $\varphi : R \rightarrow R/I$  гашто са  $\varphi(r) = r + I$  'на' хомоморфизам. Ово пресликавање зовемо природни хомоморфизам.

**Тврђење 79.** Нека је  $R$  комутативан прстен и  $I \triangleleft R$ . Тада  $R/I$  нема делилаче нуле ако и само ако је  $I$  прости идеал.

**Теорема 80.** Ако је  $R$  интегрални домен, онда постоји поље  $\tilde{R}$  такво да важе следећа два услова:

- (1)  $R \leq \tilde{R}$ ;
  - (2) ако је  $K$  поље и  $R \leq K$ , онда постоји јединствено поштање  $\theta : \tilde{R} \rightarrow K$  га је  $\theta(x) = x$  за све  $x \in R$ .
- Овакво поље  $\tilde{R}$  зовемо количничко поље интегралног домена  $R$ .

**Теорема 81.** Нека је  $F$  поље. Тада је  $F[x]$  интегрални домен, а

$$F(x) = \{f(x)/g(x) : f(x), g(x) \in F[x], g(x) \neq 0\}$$

је поље. Ово поље називамо поље рационалних функција над  $F$ .

## 6. X - МРЕЖЕ ПОТПРСТЕНА, ЛЕВИХ ИДЕАЛА, ДЕСНИХ ИДЕАЛА И ИДЕАЛА

**Дефиниција 82.** За структуру  $(L; \wedge, \vee)$  кажемо да је мрежса ако за све  $x, y, z \in L$  важе следећи услови:

- (1)  $x \wedge x = x = x \vee x$ ,
- (2)  $x \wedge y = y \wedge x$  и  $x \vee y = y \vee x$ ,
- (3)  $(x \wedge y) \wedge z = x \wedge (y \wedge z)$  и  $(x \vee y) \vee z = x \vee (y \vee z)$ ,
- (4)  $x \wedge (x \vee y) = x = x \vee (x \wedge y)$ .

**Лема 83.** Нека је  $L$  мрежса и релација  $\leq$  на  $L$  дефинисана са  $a \leq b \Leftrightarrow a \wedge b = a$ . Тада је  $(L, \leq)$  парцијално уређен скуп.

Убудуће, када год нам је дата мрежа  $L$ , подразумевамо да нам је дато и парцијално уређење  $\leq$  на  $L$ , дефинисано у претходној леми. Тада, за  $A \subseteq L$  дефинишемо  $\inf(A)$  као највеће доње ограничење скупа  $A$  у  $L$ , а  $\sup(A)$  као најмање горње ограничење скупа  $A$  у  $L$ , оба у уређењу  $\leq$ . Дефинишемо и  $\inf(\emptyset) = \max(L)$  и  $\sup(\emptyset) = \min(L)$

**Дефиниција 84.** Нека је  $(L; \wedge, \vee)$  мрежа. Кажемо да је  $L$  комилећна ако за сваки  $A \subseteq L$  постоје  $\inf(A) \in L$  и  $\sup(A) \in L$ . Кажемо да је  $L$  модуларна ако за све  $a, b, c \in L$  такве да је  $a \leq b$ , важи  $a \vee (c \wedge b) = (a \vee c) \wedge b$ .

**Лема 85.** Нека је  $L$  мрежа. Тада је  $L$  комилећна ако и само ако за сваки  $A \subseteq L$  постоји  $\inf(A) \in L$ .

**Теорема 86 (Без доказа).** Нека је  $R$  прстен и нека је  $L_p(R)$  скуп свих поштарских прстена  $R$ , а  $L_i(R)$  скуп свих идеала прстена  $R$ . На  $L_p(R)$  можемо посматрати операцију: за  $S, T \leq R$  је  $S * T = \langle S \cup T \rangle_p$ . Тада су структуре  $(L_p(R), *, \cap)$  и  $(L_i(R), +, \cap)$  комилећне мреже.

**Теорема 87.** Ако је  $R$  прстен, онда је мрежа  $L_i(R)$  модуларна.

**Пример 88.** Мрежа  $L_p(M_2(\mathbb{R}))$  није модуларна.

**Дефиниција 89.** Нека је  $R$  прстен. Релација  $\rho$  на  $R$  је конструенција на  $R$  ако је релација еквиваленције и ако за све  $a, b, c, d \in R$  из  $a\rho b$  и  $c\rho d$  следи  $(a+c)\rho(b+d)$  и  $(ac)\rho(bd)$ .

Композиција  $\circ$  две бинарне релације на скупу  $X$  дефинисана је са:  $a(\rho \circ \sigma)b \Leftrightarrow (\exists c \in X)(a\rho c \wedge c\sigma b)$ .

**Лема 90.** Нека су  $\rho$  и  $\sigma$  конструенције на прстену  $R$ . Тада је  $\rho \circ \sigma$  конструенција на прстену  $R$ .

**Лема 91.** Нека је  $R$  прстен. Тада је  $(\text{Con}(R), \circ, \cap) \cong (L_i(R), +, \cap)$ .

7. ЛЕМА ЦАСЕНХАУСА, ТЕОРЕМЕ О ИЗОМОРФИЗМУ И ТЕОРЕМА О КОРЕСПОНДЕНЦИЈИ У ПРСТЕНИМА

**Теорема 92 (I теорема о изоморфизму).** Нека су  $R$  и  $T$  прстени и  $\varphi : R \rightarrow T$  хомоморфизам који је 'на'. Тада је  $T \cong R/\ker(\varphi)$ .

**Пример 93.** Хомоморфне слике прстена  $\mathbb{Z}$ . Сви идеали прстена  $\mathbb{Z}$  су  $\{0\}$ ,  $n\mathbb{Z}$  за  $n \geq 2$ , и  $\mathbb{Z}$ . По првој теореми о изоморфизму, све хомоморфне слике прстена  $\mathbb{Z}$  су  $\mathbb{Z} \cong \mathbb{Z}/\{0\}$ ,  $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$  за  $n \in \mathbb{Z}$ , и  $\mathbb{Z}/\mathbb{Z} \cong \{0\}$ .

**Пример 94.** Поље реалних бројева је хомоморфна слика прстена  $C[0, 1]$ .

**Лема 95.** Нека је  $R$  прстен,  $T, S \leq R$  и  $I \triangleleft S$ , онда је  $I \cap T \triangleleft S \cap T$ .

**Теорема 96 (Лема Цасенхауса).** Нека је  $R$  прстен,  $A, B \leq R$ ,  $A_1 \triangleleft A$  и  $B_1 \triangleleft B$ . Тада је

- (1)  $A_1 + (A \cap B_1) \triangleleft A_1 + (A \cap B)$ ,
- (2)  $B_1 + (A_1 \cap B) \triangleleft B_1 + (A \cap B)$ ,
- (3)  $A_1 + (A \cap B)/A_1 + (A \cap B_1) \cong B_1 + (A \cap B)/B_1 + (A_1 \cap B)$ .

**Теорема 97 (II теорема о изоморфизму).** Нека је  $R$  прстен и  $A, B \leq R$  такав да је  $A \triangleleft \langle A \cup B \rangle_p$ . Тада је  $A + B/A \cong B/A \cap B$ .

**Теорема 98 (Теорема о кореспонденцији).** Нека су  $R$  и  $T$  прстени и нека је  $\varphi : R \rightarrow T$  'на' хомоморфизам. Тада је  $\{A \in L_p(R) : \ker(\varphi) \subseteq A \subseteq R\}$  посмрежа мрежа  $L_p(R)$  и бијекција  $\Phi$

$$\Phi : L_p(T) \rightarrow \{A \in L_p(R) : \ker(\varphi) \subseteq A \subseteq R\}$$

такав да су испуњена следећа три услова:

- (1)  $I \triangleleft T$  ако је  $\Phi(I)$  идеал у  $R$  који садржи  $\ker(\varphi)$ ,
- (2) ако је  $A \subseteq B$  за  $A, B \in L_p(T)$ , онда је  $\Phi(A) \subseteq \Phi(B)$ ,
- (3) ако је  $\ker(\varphi) \subseteq A \subseteq B$  за  $A, B \in L_p(R)$ , онда је  $\Phi^{-1}(A) \subseteq \Phi^{-1}(B)$ .

**Теорема 99 (III теорема о изоморфизму).** Нека је  $R$  прстен,  $T \leq R$ ,  $I \triangleleft R$  и  $I \subseteq T$ . Тада:

- (1)  $T/I \leq R/I$ ,
- (2) ако је још  $T \triangleleft R$ , онда је  $T/I \triangleleft R/I$  и  $R/T \cong (R/I)/(T/I)$ .

## 8. x - ДИРЕКТНИ ПРОИЗВОДИ И ДИРЕКТНЕ СУМЕ ПРСТЕНА. УНУТРАШЊЕ СУМЕ

**Дефиниција 100.** Нека је  $\mathcal{A} = \{R_j : j \in \mathcal{J}\}$  фамилија прстена. Тада је производ фамилије  $\mathcal{A}$  скуп

$$\prod_{j \in \mathcal{J}} R_j = \left\{ f : \mathcal{J} \rightarrow \bigcup_{j \in \mathcal{J}} R_j : (\forall j \in \mathcal{J}) f(j) \in R_j \right\},$$

са операцијама  $(f+g)(j) = f(j) + g(j)$  и  $(fg)(j) = f(j)g(j)$ .

Приметимо да је у овој ситуацији  $\left( \prod_{j \in \mathcal{J}} R_j; +, \cdot \right)$  прстен.

**Дефиниција 101.** Нека је  $\mathcal{A} = \{R_j : j \in \mathcal{J}\}$  фамилија прстена. Тада је *директна сума фамилије  $\mathcal{A}$* :

$$\bigoplus \sum_{j \in \mathcal{J}} R_j = \left\{ f \in \prod_{j \in \mathcal{J}} R_j : |\{j \in \mathcal{J} : f(j) \neq 0\}| < \infty \right\} \leq \prod_{j \in \mathcal{J}} R_j.$$

**Напомена 102.** Приметимо:

- (1) Ако сви прстени  $R_j$  ( $j \in \mathcal{J}$ ) имају јединицу, онда и  $\prod_{j \in \mathcal{J}} R_j$  има јединицу, док  $\bigoplus \sum_{j \in \mathcal{J}} R_j$  има јединицу ако је  $\{j \in \mathcal{J} : |R_j| > 1\}$  коначан скуп.

- (2) Ако бар два, нпр.  $R_{j_1}$  и  $R_{j_2}$  имају више од једног елемента, онда  $\prod_{j \in \mathcal{J}} R_j$  и  $\bigoplus \sum_{j \in \mathcal{J}} R_j$  имају делитеље нуле.
- (3) Ако је  $\{j \in \mathcal{J} : |R_j| > 1\}$  бесконачан, онда је сваки елемент  $\bigoplus \sum_{j \in \mathcal{J}} R_j$  делитељ нуле.

**Лема 103.** Нека је  $\{R_j : j \in \mathcal{J}\}$  фамилија прстена и  $f \in \bigoplus \sum_{j \in \mathcal{J}} R_j$ . Елеменат  $f$  је нилпотентан ако и само ако је  $f(j)$  нилпотентан за свако  $j \in \mathcal{J}$ .

**Пример 104.** Тврђење претходне леме не важи за директне производе.

**Лема 105.** Нека је  $R_j$  прsten за све  $j \in \mathcal{J}$ . Нека  $T_j \leq R_j$  за све  $j \in \mathcal{J}$ . Тада је

- (1)  $\prod_{j \in \mathcal{J}} T_j \leq \prod_{j \in \mathcal{J}} R_j$ ;
- (2)  $\bigoplus \sum_{j \in \mathcal{J}} T_j \leq \bigoplus \sum_{j \in \mathcal{J}} R_j$ ;

**Лема 106.** Нека је  $R_j$  прsten за све  $j \in \mathcal{J}$ . Нека  $T_j \triangleleft R_j$  за све  $j \in \mathcal{J}$ . Тада је

- (1)  $\prod_{j \in \mathcal{J}} T_j \triangleleft \prod_{j \in \mathcal{J}} R_j$ ;
- (2)  $\bigoplus \sum_{j \in \mathcal{J}} T_j \triangleleft \bigoplus \sum_{j \in \mathcal{J}} R_j$ ;
- (3)  $\prod_{j \in \mathcal{J}} R_j / \prod_{j \in \mathcal{J}} T_j \cong \prod_{j \in \mathcal{J}} (R_j / T_j)$ ;
- (4)  $\bigoplus \sum_{j \in \mathcal{J}} R_j / \bigoplus \sum_{j \in \mathcal{J}} T_j \cong \bigoplus \sum_{j \in \mathcal{J}} (R_j / T_j)$ ;

Ако нам је дата фамилија прстена  $\{R_j : j \in \mathcal{J}\}$  и ако посматрамо  $\bigoplus \sum_{j \in \mathcal{J}} R_j$  онда можемо дефинисати:

$$\widehat{R}_j = \left\{ f \in \bigoplus \sum_{j \in \mathcal{J}} R_j : (\forall k \in \mathcal{J} \setminus \{j\}) f(k) = 0 \right\}.$$

Јасно је да је тада  $R_j \cong \widehat{R}_j$ .

**Лема 107.** Нека је дата фамилија прстена  $\{R_j : j \in \mathcal{J}\}$ . Тада:

- (1)  $\widehat{R}_j \triangleleft \bigoplus \sum_{j \in \mathcal{J}} R_j$  за све  $j \in \mathcal{J}$ ,
- (2)  $\widehat{R}_j \cap \left\langle \bigcup_{k \in \mathcal{J} \setminus \{j\}} \widehat{R}_k \right\rangle_i = \{0\}$  за све  $j \in \mathcal{J}$ ,
- (3)  $\left\langle \bigcup_{j \in \mathcal{J}} \widehat{R}_j \right\rangle_i = \bigoplus \sum_{j \in \mathcal{J}} R_j$ .

**Дефиниција 108.** Нека је  $R$  прsten и  $\mathcal{A} = \{A_j : j \in \mathcal{J}\}$  фамилија потпрстена прстена  $R$ . Тада кажемо да је  $R$  унутрашња сума фамилије  $\mathcal{A}$  ако је

- (1)  $A_j \triangleleft R$  за све  $j \in \mathcal{J}$ ,
- (2)  $A_j \cap \left\langle \bigcup_{k \in \mathcal{J} \setminus \{j\}} A_k \right\rangle_i = \{0\}$  за све  $j \in \mathcal{J}$ ,
- (3)  $\left\langle \bigcup_{j \in \mathcal{J}} A_j \right\rangle_i = R$ .

**Лема 109.** Нека је  $R$  прsten и  $\mathcal{A} = \langle A_j : j \in \mathcal{J} \rangle$  фамилија поштрустена прстена  $R$ . Следећи услови су еквивалентни:

- (1)  $R$  је унутрашња сума фамилије  $\mathcal{A}$ ;
- (2) (a) за све  $k \neq j$  из  $\mathcal{J}$ , све  $a \in R_k$  и све  $b \in R_j$  је  $ab = 0$ .
- (b) сваки  $r \in R$  различит је од нуле, може се на јединствен начин приказати као сума  $r = a_1 + \dots + a_n$  за неке  $a_m \in R_{j_m}$  ( $m \leq n$ ), при чему је  $j_m \neq j_l$  за  $m \neq l$ .

**Лема 110.** Нека је прsten  $R$  унутрашња сума фамилије идеала  $\{A_j : j \in \mathcal{J}\}$ . Тада је  $R \cong \bigoplus \sum_{j \in \mathcal{J}} A_j$ .

**Лема 111.** Нека је  $\{R_j : j \in \mathcal{J}\}$  фамилија прстена са јединицом и  $A \subseteq \bigoplus \sum_{j \in \mathcal{J}} R_j$ . Тада је  $A \triangleleft \bigoplus \sum_{j \in \mathcal{J}} R_j$  ако је облика  $A = \bigoplus \sum_{j \in \mathcal{J}} A_j$  за неке  $A_j \triangleleft R_j$  ( $j \in \mathcal{J}$ ).

## 9. КИНЕСКА ТЕОРЕМА О ОСТАЦИМА

**Тврђење 112.** Нека је  $R$  прsten и  $\{A_j : j \in \mathcal{J}\}$  фамилија идеала прстена  $R$ . Нека је пресликавање  $\psi : R \mapsto \prod_{j \in \mathcal{J}} R/A_j$  гашо са  $(\psi(r))(j) = r + A_j$  за  $j \in \mathcal{J}$ . Тада је  $\psi$  хомоморфизам из  $R$  у  $\prod_{j \in \mathcal{J}} R/A_j$  и важи  $\ker(\psi) = R / \bigcap_{j \in \mathcal{J}} A_j$ . Даље,  $R / \bigcap_{j \in \mathcal{J}} A_j$  је изоморфан поштрустену ог  $\prod_{j \in \mathcal{J}} R/A_j$ .

**Теорема 113** (Кинеска теорема о остацима). Нека је  $R$  прsten са јединицом и  $\{A_1, A_2, \dots, A_n\}$  фамилија идеала прстена  $R$  таква да за све  $k \neq j$  важи  $A_k + A_j = R$ . Нека су  $r_1, \dots, r_n \in R$  произвољни елементи. Тада постоји  $r \in R$  такав да је

$$r + A_1 = r_1 + A_1$$

$$r + A_2 = r_2 + A_2$$

⋮

$$r + A_n = r_n + A_n.$$

**Последица 114** (Кинеска теорема о остацима у  $\mathbb{Z}$ ). Нека су  $a_1, \dots, a_n \in \mathbb{N}$  ненећасници цели бројеви такви да за све  $i \neq j$  важи  $\text{NZD}(a_i, a_j) = 1$ . Тада за све  $r_1, r_2, \dots, r_n \in \mathbb{Z}$  постоји  $r \in \mathbb{Z}$  такав да је

$$\begin{aligned} r &\equiv r_1 \pmod{a_1} \\ r &\equiv r_2 \pmod{a_2} \\ &\vdots \\ r &\equiv r_n \pmod{a_n}. \end{aligned}$$

## 10. ИДЕАЛИ КОМУТАТИВНИХ ПРСТЕНА

**Лема 115.** Нека је  $R$  комутативан прстен са јединицом и  $I$  прави идеал прстена  $R$ . Тада су следећи услови еквивалентни:

- (1)  $I$  је максимални идеал;
- (2) за сваки елемент  $a \in R \setminus I$  постоји елемент  $b \in R$  такав да је  $1 - ab \in I$ .
- (3)  $R/I$  је поље.

**Лема 116.** Нека је  $R$  комутативан прстен са јединицом у ком је сваки прави идеал прстена  $R$  прост. Тада је  $R$  поље.

**Дефиниција 117.** Нека је  $R$  комутативан прстен и  $I$  прави идеал у  $R$ . Кажемо да је  $I$  примиран ако за све  $a, b \in R$  из  $ab \in I$  следи да је  $a \in I$  или да постоји  $n > 0$  такав да је  $b^n \in I$ .

Приметимо да је сваки прост идеал примаран.

**Лема 118.** Нека је  $n > 1$ . Идеал  $n\mathbb{Z}$  је примиран ако и само ако је  $n$  стелен неког простог броја.

**Лема 119.** Нека је  $I$  прави идеал комутативног прстена  $R$ . Тада је  $I$  примиран ако је сваки делитељ нуле у  $R/I$  нилпотентан.

**Дефиниција 120.** Нека је  $R$  комутативан прстен и  $I \triangleleft R$ . Радикал од  $I$  је

$$\sqrt{I} = \{a \in R : (\exists n > 0) a^n \in I\}.$$

Приметимо да је  $\sqrt{I}$  такође идеал прстена  $R$ .

**Лема 121.** Нека је  $R$  комутативан прстен, а  $I$  и  $J$  идеали у  $R$ . Тада је:

- (1)  $(\exists k \in \mathbb{N}) I^k \subseteq J \Rightarrow \sqrt{I} \subseteq \sqrt{J}$ ;
- (2)  $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ ;
- (3)  $\sqrt{\sqrt{I}} = \sqrt{I}$ ;
- (4)  $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$ .

**Лема 122.** Нека је  $R$  комутативан прстен са јединицом, а  $I$  примиран идеал у  $R$ . Тада је  $\sqrt{I}$  најмањи прост идеал који садржи  $I$ .

## 11. ЕУКЛИДОВИ ДОМЕНИ И ДОМЕНИ ГЛАВНИХ ИДЕАЛА

**Дефиниција 123.** Нека је  $R$  интегрални домен. Кажемо да је  $R$  Еуклидов домен ако постоји функција  $\varphi : R \setminus \{0\} \rightarrow \mathbb{N} \cup \{0\}$  таква да:

- (1)  $(\forall a, b \in R \setminus \{0\}) \varphi(ab) \geq \varphi(a)$ ,
- (2) за све  $a \in R$  и  $b \in R \setminus \{0\}$  постоје  $q, r \in R$  такви да је  $a = bq + r$  и још је  $r = 0$  или  $\varphi(r) < \varphi(b)$ .

Приметимо да је  $\varphi(a) \geq \varphi(1)$  за све  $a \in R \setminus \{0\}$  и да је  $\varphi(1) = \varphi(a)$  ако је  $a$  инвертибилан.

**Пример 124.** Ако је  $F$  поље, онда је  $F[x]$  Еуклидов домен

**Пример 125.** Прстен Гаусових целих бројева  $\mathbb{Z}[i]$  је Еуклидов домен.

**Пример 126.** Прстен  $\mathbb{Q}_p = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b > 0, p \nmid b \right\}$  је Еуклидов домен (када се посматра као потпрстен  $\mathbb{Q}$ ).

**Дефиниција 127.** Нека је  $R$  интегрални домен. Кажемо да је  $R$  домен главних идеала ако је сваки идеал у  $R$  главни идеал.

**Теорема 128.** Сваки Еуклидов домен је домен главних идеала.

## 12. ДОМЕНИ ЈЕДНОЗНАЧНЕ ФАКТОРИЗАЦИЈЕ 1

**Дефиниција 129.** Нека је  $R$  интегрални домен и  $a, b \in R$ . Кажемо да  $a$  дели  $b$  (пишемо  $a | b$ ) ако постоји неки  $c \in R$  такав да је  $b = ac$ . Кажемо да су  $a$  и  $b$  асоцирани (пишемо  $a \sim b$ ) ако  $a | b$  и  $b | a$ .

**Лема 130.** Нека је  $R$  интегрални домен. Тада је  $|$  рефлексивна и транзишивна релација, а  $\sim$  је релација еквиваленције.

**Лема 131.** Нека је  $R$  интегрални домен и  $a, b \in R$ . Тада је  $a \sim b$  ако постоји  $u \in R^*$  такав да је  $a = ub$ .

**Лема 132.** Нека је  $R$  интегрални домен и  $a, b \in R$ . Тада  $a | b$  ако  $a' | b'$  за све  $a' \in [a]_\sim$  и све  $b' \in [b]_\sim$ .

**Дефиниција 133.** Нека је  $R$  интегрални домен и  $a \in R$ .

- (1) Кажемо да је  $a$  несводљив ако  $a \notin R^*$  и још за све  $b, c \in R$  из  $a = bc$  следи да је или  $a \sim b$  или  $a \sim c$ .
- (2) Кажемо да је  $a$  прости ако  $a \notin R^*$  и још за све  $b, c \in R$  из  $a | bc$  следи да  $a | b$  или  $a | c$ .

Приметимо да је  $a$  несводљив ако  $a \notin R^*$  и за све  $b, c \in R$  из  $a = bc$  следи  $b \in R^*$  или  $c \in R^*$ .

**Лема 134.** Нека је  $R$  интегрални домен. Тада је сваки прости елеменат у  $R$  несводљив.

**Лема 135.** Нека је  $R$  интегрални домен. Ако је  $a$  прости онда је сваки елеменат у  $[a]_\sim$  шакође прости. Ако је  $a$  несводљив, онда је сваки елеменат у  $[a]_\sim$  шакође несводљив.

**Дефиниција 136.** Нека је  $R$  интегрални домен и  $a, b_1, \dots, b_n \in R$ . Кажемо да је  $a = \text{NZD}(b_1, \dots, b_n)$  ако  $a | b_k$  за све  $k \leq n$  и још за све  $c \in R$  такве да  $c | b_k$  ( $k \leq n$ ) важи  $c | a$ .

**Лема 137.** Нека је  $R$  интегрални домен и  $a, b_1, \dots, b_n \in R$ . Тада ако је  $a = \text{NZD}(b_1, \dots, b_n)$  и  $u \in R^*$ , онда је  $au = \text{NZD}(b_1, \dots, b_n)$

**Лема 138.** Нека је  $R$  интегрални домен и  $a, b \in R \setminus \{0\}$ . Тада:

- (1)  $a | b$  ако  $\langle b \rangle_i \subseteq \langle a \rangle_i$ ,
- (2)  $a \sim b$  ако  $\langle b \rangle_i = \langle a \rangle_i$ ,
- (3)  $a$  је прости ако је  $\langle a \rangle_i$  ненула прости идеал,
- (4)  $a$  је несводљив ако је  $\langle a \rangle_i$  ненула идеал који је максималан међу главним идеалима у  $R$ .

## 13. ДОМЕНИ ЈЕДНОЗНАЧНЕ ФАКТОРИЗАЦИЈЕ 2

**Дефиниција 139.** Нека је  $R$  интегрални домен и  $a \in R$ . Кажемо да је  $a = up_1 \cdots p_n$  разлагање елемената  $a$  на несводљиве факторе (или факторизација) ако је  $u \in R^*$  и ако су  $p_1, \dots, p_n$  несводљиви. Кажемо и да су два разлагања елемента  $a = up_1 \cdots p_n = vq_1 \cdots q_m$  еквивалентна ако је  $n = m$  и постоји пермутација  $\sigma$  скупа  $\{1, \dots, n\}$  таква да је  $p_k \sim q_{\sigma(k)}$  за све  $k \leq n$ .

**Дефиниција 140.** Нека је  $R$  интегрални домен. Кажемо да је  $R$  домен једнозначне факторизације ако за сваки елеменат  $a \in R \setminus \{0\}$  постоји разлагање на несводљиве факторе и свака два таква разлагања су еквивалентна.

**Напомена 141.** Нека је  $R$  интегрални домен,  $S$  скуп несводљивих елемената у  $R$ , а  $P$  скуп такав да  $(\forall a \in S) |P \cap [a]_\sim| = 1$  и  $(\forall a \in S) (\exists b \in P) a \sim b$ .  $R$  је домен једнозначне факторизације ако за све  $a \in R \setminus \{0\}$  постоји факторизација  $a = up_1 \cdots p_n$  при чему је  $u \in R^*$  и  $p_1, \dots, p_n \in P$  и још за сваке две такве факторизације  $a = up_1 \cdots p_n = vq_1 \cdots q_m$  важи да је  $m = n$  и да постоји пермутација  $\sigma$  скупа  $\{1, \dots, n\}$  таква да је  $(\forall k \leq n) p_k = q_{\sigma(k)}$ . Тада, ако  $a | b$  и  $a = up_1^{\alpha_1} \cdots p_n^{\alpha_n}$  и  $b = vq_1^{\beta_1} \cdots q_m^{\beta_m}$  (где су факторизације као у првом делу запажања и сви  $p$ -ови су по паровима различити и сви  $q$ -ови су по паровима различити), онда је  $n \leq m$  и  $(\forall k \leq n) (\exists l_k \leq m) (p_k = q_{l_k} \wedge \alpha_k \leq \beta_{l_k})$ .

**Теорема 142.** Интегрални домен  $R$  је домен једнозначне факторизације ако важе следећа два услова:

- (1) (услов стационарности) ако је  $(a_n : n \geq 1)$  низ у  $R$  за који  $(\forall n \geq 1) a_{n+1} | a_n$ , онда постоји  $m \geq 1$  такво да је  $a_m \sim a_{m+k}$  за све  $k \geq 0$ .
- (2) сваки несводљив елеменат у  $R$  је прости.

**Пример 143.**  $\mathbb{Z}$  јесте домен једнозначне факторизације, а  $\mathbb{Z}[i\sqrt{5}]$  није домен једнозначне факторизације.

**Лема 144.** Ако је  $R$  домен једнозначне факторизације, онда за све елементе  $b_1, \dots, b_n \in R \setminus \{0\}$  постоји  $\text{NZD}(b_1, \dots, b_n)$ .

**Теорема 145.** Сваки домен главних идеала је домен једнозначне факторизације.

**Пример 146.**  $\mathbb{Z}[x]$  јесте домен једнозначне факторизације (према теореми 154), али није домен главних идеала.

**Теорема 147.** Нека је  $R$  интегрални домен и  $a = \text{NZD}(b_1, \dots, b_n)$ . Тада

- (1) Ако је  $R$  домен једнозначне факторизације, онда је  $aR$  најмањи главни идеал који садржи идеал  $\langle b_1, \dots, b_n \rangle_i$ .
- (2) Ако је  $R$  домен главних идеала, онда је  $aR = \langle b_1, \dots, b_n \rangle_i$ .

#### 14. x - \*ДОМЕНИ ЈЕДНОЗНАЧНЕ ФАКТОРИЗАЦИЈЕ 3

**Дефиниција 148.** Нека је  $R$  домен једнозначне факторизације и  $p(x) = a_nx^n + \dots + a_1x + a_0 \in R[x]$ . Дефинишемо меру полинома  $p(x)$  као

$$m(p(x)) = \text{NZD}(a_0, \dots, a_n).$$

Кажемо да је  $p(x)$  примиштан ако је  $m(p(x)) \sim 1$ .

**Теорема 149** (Гаусова лема 1). Нека је  $R$  домен једнозначне факторизације, а  $f(x)$  и  $g(x)$  примиштани полиноми у  $R[x]$ . Тада је и полином  $f(x)g(x)$  примиштан.

**Лема 150.** Нека је  $R$  домен једнозначне факторизације и  $\tilde{R}$  његово количничко поље. Ако је  $f(x) \in \tilde{R}[x]$ , онда постоји  $\alpha \in \tilde{R}$  и примиштан полином  $g(x) \in R[x]$  такви да важе следећа два услова:

- (1)  $f(x) = \alpha g(x)$ ,
- (2)  $g(x)$  је јединствен до на производ са инвертибилним елементом из  $R$ .

**Теорема 151** (Гаусова лема 2). Нека је  $R$  интегрални домен,  $\tilde{R}$  количничко поље  $R$ , а  $f(x) \in R[x]$ . Тада се  $f(x)$  не може расставити на производ неконстантних полинома у  $R[x]$  ако се не може расставити у производ неконстантних полинома у  $\tilde{R}[x]$ .

**Пример 152.** Несводљив полином у  $\mathbb{Q}[x]$  који је сводљив у  $\mathbb{Z}[x]$ .

**Последица 153.** Нека је  $R$  домен једнозначне факторизације,  $\tilde{R}$  количничко поље  $R$ , а  $f(x) \in R[x]$  примиштан полином степена  $n \geq 1$ . Тада је  $f(x)$  несводљив у  $R[x]$  ако је несводљив у  $\tilde{R}[x]$ .

**Теорема 154** (Гаусова теорема). Ако је  $R$  домен једнозначне факторизације, онда је и  $R[x]$  домен једнозначне факторизације.

#### 15. x - ДОМЕНИ ЈЕДНОЗНАЧНЕ ФАКТОРИЗАЦИЈЕ 4

**Тврђење 155.** Нека је  $R$  интегрални домен. Тада су следећи услови еквивалентни:

- (1)  $R$  је поље.
- (2) Сваки ненула прост идеал у  $R[x]$  је максималан.

**Пример 156.** Домен једнозначне факторизације који није домен главних идеала ( $F[x, y]$  за  $F$  поље).

**Пример 157.** Примери интегралног домена који није домен једнозначне факторизације. Један пример када не важи услов (1) теореме 142, и један пример када не важи услов (2) из исте теореме.

#### 16. НЕСВОДЉВОСТ ПОЛИНОМА

**Теорема 158** (Ајзенштајнов критеријум). Нека је  $R$  домен једнозначне факторизације и  $f(x) = a_nx^n + \dots + a_1x + a_0 \in R[x]$ . Ако постоји несводљив  $p \in R$  такав да  $p \nmid a_n$ ,  $p^2 \nmid a_0$  и  $(\forall k < n) p \mid a_k$ , онда  $f(x)$  није производ неконстантних полинома у  $R[x]$ .

**Теорема 159.** Нека је  $p$  прост број. Онда је полином  $x^{p-1} + x^{p-2} + \dots + x + 1$  несводљив у  $\mathbb{Z}[x]$ .

**Дефиниција 160.** Нека су  $R$  и  $T$  комутативни прстени са јединицом и  $\varphi : R \rightarrow T$  хомоморфизам прстена. Дефинишемо  $\varphi^* : R[x] \rightarrow T[x]$  на следећи начин:

$$\varphi^*(a_nx^n + \dots + a_1x + a_0) = \varphi(a_n)x^n + \dots + \varphi(a_1)x + \varphi(a_0).$$

Приметимо да је у ситуацији из претходне дефиниције пресликање  $\varphi^*$  хомоморфизам. Подсетимо се и да је  $\pi_m : \mathbb{Z} \rightarrow \mathbb{Z}_m$  хомоморфизам који за  $a \in \mathbb{Z}$  као резултат даје остатак при дељењу броја  $a$  са  $m$ .

**Лема 161.** Нека је  $f(x) \in \mathbb{Z}[x]$ . Ако је  $a_n = 1$  и постоји  $m > 0$  такав да је  $\pi_m^*(f(x))$  несводљив у  $\mathbb{Z}_m[x]$ , онда је  $f(x)$  несводљив у  $\mathbb{Z}[x]$ .

Подсетимо се да за полином  $f(x)$  кажемо да је  $\alpha$  његова нула ако је  $f(\alpha) = 0$ .

**Тврђење 162.** Нека је  $F$  поље,  $f(x) \in F[x]$  и  $a \in F$ . Тада  $x - a \mid f(x)$  у  $F[x]$  ако је  $f(a) = 0$ . Такође, ако је  $f(x)$  степена  $n$ , може имати највише  $n$  нула у  $F$ .

**Теорема 163.** Ако је  $F$  поље и  $G$  коначна поструга мултипликативне трупе  $(F^*; \cdot)$ , онда је  $G$  циклична.

**Последица 164.** За свако коначно поље  $F$ , мултипликативна трупа поља  $(F^*; \cdot)$  је циклична.

**Лема 165.** Ако је  $p > 2$  прост број, онда је  $-1, 2$  или  $-2$  квадратни остатак по модулу  $p$  (што је неки  $a \in \mathbb{Z}$  је  $a^2 \equiv_p -1$  или  $a^2 \equiv_p 2$  или  $a^2 \equiv_p -2$ ).

**Пример 166.** Полином  $x^4 + 1$  несводљив је у  $\mathbb{Z}[x]$ , али за сваки прост број  $p$ ,  $x^4 + 1$  је сводљив у  $\mathbb{Z}_p[x]$ .

## 17. ОСНОВНЕ ОСОБИНЕ ПОЉА

**Лема 167.** Нека је  $R$  интегрални домен. Тада је  $\text{char}(R)$  или 0 или прости број. Специјално, карактеристика сваког поља је или нула или прости број.

**Напомена 168.** Нека су  $F$  и  $K$  поља и  $F \leq K$ . Кажемо да је тада  $K$  проширење поља  $F$ . Приметимо и да је тада  $K$  векторски простор над  $F$ .

**Дефиниција 169.** Нека је  $K$  проширење поља  $F$ . Дефинишемо степен проширења  $K$  над  $F$ , у означи  $[K : F]$ , као димензију векторског простора  $K$  над  $F$ . Кажемо да је проширење коначно, у означи  $[K : F] < \infty$ , ако је  $[K : F]$  природан број.

**Лема 170.** Нека су  $L$  и  $F$  поља са  $L \leq F$ . Тада је  $[L : F] < \infty$  ако и само ако је  $[L : K] < \infty$  и  $[K : F] < \infty$ , а у том случају је  $[L : F] = [L : K] \cdot [K : F]$ .

**Дефиниција 171.** Нека је  $K$  проширење поља  $F$ . Кажемо да је елемент  $\alpha \in K$  алгебарски над  $F$  ако постоји ненула полином  $f(x) \in F[x]$  такав да је  $f(\alpha) = 0$ . Ако елемент није алгебарски над  $F$ , онда кажемо да је трансцендентан над  $F$ .

**Дефиниција 172.** Нека је  $K$  проширење поља  $F$ . Кажемо да је  $K$  алгебарско проширење поља  $F$  ако је сваки елемент  $\alpha \in K$  алгебарски над  $F$ .

**Теорема 173.** Нека је  $K$  проширење поља  $F$  и  $\alpha \in K$ . Тада:

- (1) Ако је  $\alpha$  трансцендентан над  $F$ , онда је  $F[\alpha] \cong F[x]$ .
- (2) Ако је  $\alpha$  алгебарски онда:
  - (a)  $F[\alpha]$  поштоље од  $K$  и
  - (b)  $[F[\alpha]] : F = \deg(f(x))$  где је  $f(x)$  полином из  $F[x]$  минималног степена такав да је  $f(\alpha) = 0$ .

Подсетимо се да за полином  $f(x) = a_nx^n + \dots + a_1x + a_0 \in F[x]$  кажемо да је монички ако је  $a_n = 1$ .

**Дефиниција 174.** Нека је  $K$  проширење поља  $F$  и  $\alpha \in K$ . Минимални полином за  $\alpha$  над  $F$ , у означи  $p_\alpha^F(x)$ , је монички полином из  $F[x]$  минималног степена чија је једна нула  $\alpha$ .

**Лема 175.** Нека је  $K$  проширење поља  $F$  и  $\alpha \in K$ . Тада је минимални полином за  $\alpha$  над  $F$  јединствен и сваки несводљив полином у  $F[x]$  чија је једна нула  $\alpha$  асоциран је са  $p_\alpha^F(x)$ .

**Тврђење 176.** Ако је  $K$  коначно проширење поља  $F$ , онда је  $K$  алгебарско проширење  $F$ .

## 18. КРОНЕКЕРОВА ТЕОРЕМА

**Лема 177.** Нека  $K$  проширење поља  $F$  и  $f(x) \in F[x]$  несводљив полином над  $F$  стечена већет од 1 који има нулу у  $K$ . Следећи услови су еквивалентни:

- (1)  $K$  је минимално проширење  $F$  које садржи бар једну нулу полинома  $f(x)$ .
- (2)  $K = F[\alpha]$  за свако  $\alpha \in K$  такво да је  $f(\alpha) = 0$ .
- (3)  $K = F[\alpha]$  за неко  $\alpha \in K$  такво да је  $f(\alpha) = 0$ .

**Теорема 178** (Кронекерова теорема). Нека је  $F$  поље и  $f(x) \in F[x]$  несводљив над  $F$ . Тада постоји минимално проширење  $K$  поља  $F$  које садржи бар једну нулу полинома  $f(x)$ . То проширење је јединствено до на изоморфизам.

**Последица 179.** Нека је  $F$  поље и  $f(x) \in F[x]$ . Тада постоји минимално проширење поља  $F$  у ком се  $f(x)$  разлаže на производ линеарних фактора. Овајко поље називамо поље разлагања полинома  $f(x)$  над  $F$ . Ако је  $K$  једно поље разлагања полинома  $f(x)$  над  $F$  и  $f(x) = a_n(x - \alpha_1) \cdots (x - \alpha_n)$  у  $K[x]$ , онда је  $K = F[\alpha_1, \dots, \alpha_n]$ .

## 19. АЛГЕБАРСКИ ЗАТВОРЕНА ПОЉА

**Дефиниција 180.** Кажемо да је поље  $F$  алгебарски затворено ако за свако алгебарско проширење  $K$  поља  $F$  важи да је  $K = F$ .

**Лема 181.** Нека су  $F, K, L$  поља,  $K$  алгебарско проширење  $F$  и  $\alpha \in L$ . Ако је  $\alpha$  алгебарски елемент над  $K$ , онда је  $\alpha$  алгебарски и над  $F$ . Специјално, ако је  $L$  алгебарско проширење поља  $K$ , онда је  $L$  и алгебарско проширење поља  $F$ .

**Лема 182.** Нека је  $F$  поље. Следећи услови су еквивалентни:

- (1)  $F$  је алгебарски затворено.
- (2) Сваки полином у  $F[x]$  стечена већет од 1 има бар једну нулу у  $F$ .
- (3) Сваки несводљив полином у  $F[x]$  је стечена 1.
- (4) Сваки полином у  $F[x]$  стечена већет од нуле производ је линеарних фактора из  $F[x]$ .

**Тврђење 183.** Не постоји коначно алгебарски затворено поље.

**Теорема 184.** Ако је  $F$  поље, онда постоји алгебарски затворено алгебарско проширење поља  $F$ .

## 20. x - \*ЛЕМА О ПРОШИРЕЊУ УТАПАЊА ПОЉА

Подсетимо се да сваки хомоморфизам који је 1-1 називамо *поштавање*, а да за скуп  $X$  идентичко пресликање на  $X$  означавамо  $\text{id}_X$  (дакле  $\text{id}_X(x) = x$  за све  $x \in X$ ).

**Лема 185.** Нека је  $F$  поље,  $K$  алгебарско проширење  $F$  и  $L$  неко алгебарски затворено поље. Тада за свако поштавање  $\varphi : F \rightarrow L$  постоји поштавање  $\psi : K \rightarrow L$  такво да је  $\varphi(x) = \psi(x)$  за све  $x \in F$ .

**Последица 186.** Ако је  $K$  алгебарско проширење поља  $F$  и  $L$  алгебарски затворено проширење  $F$ , онда постоји поштавање  $\varphi : K \rightarrow L$  такво да је  $\varphi(x) = x$  за све  $x \in F$  (уј.  $\varphi \upharpoonright F = \text{id}_F$ ).

**Последица 187.** Нека је  $F$  поље, а  $K$  и  $M$  алгебарски затворена алгебарска проширења  $F$ . Тада постоји изоморфизам  $\varphi : K \rightarrow M$  такав да је  $\varphi(x) = x$  за све  $x \in F$ .

За поље  $F$ , убудуће ћемо његово алгебарски затворено алгебарско проширење означавати  $\overline{F}$  и звати алгебарско затворење  $F$ .

**Теорема 188.** Нека су  $F$  и  $M$  поља,  $M$  алгебарски затворено,  $F \leq M$  и  $A = \{\alpha \in M : \alpha$  алгебарски над  $F\}$ . Тада је  $A = \overline{F}$ .

## 21. МИНИМАЛНО ПОТПОЉЕ И ПОЉЕ РАЗЛАГАЊА

**Теорема 189.** Нека је  $F$  поље и  $f(x) \in F[x]$ . Тада:

- (1) У сваком пољу  $K$ , за које је  $F \leq K$  и  $F(x) = a_n(x - \alpha_1) \cdots (x - \alpha_n) \in K[x]$  постоји јединствено поље разлађања  $f(x)$  над  $F$ , уј. ако је  $F \leq L \leq K$  и  $F \leq M \leq K$  и  $L$  и  $M$  су поља разлађања  $f(x)$  над  $F$  онда је  $L = M$ .
- (2) Ако су  $L$  и  $M$  нека два поља разлађања  $f(x)$  над  $F$ , онда постоји изоморфизам  $\varphi : L \rightarrow M$  такав да је  $\varphi(x) = x$ .

Нека је  $F$  поље. Приметимо да је  $L = \bigcap \{K \leq F : K$  је поље} поље чије је проширење поље  $F$ . Поље  $L$  садржи 1 и изоморфно је са  $\mathbb{Z}_p$  ако је  $\text{char}(F) = p$  прост број, а изоморфно је са  $\mathbb{Q}$  ако је  $\text{char}(F) = 0$ . Овакво поље  $L$  називамо *минимално поље*  $F$ . Приметимо да је сваки хомоморфизам поља или константан или релативно потапање над минималним пољем.

**Дефиниција 190.** Нека су  $F, K, L$  поља, а  $K$  алгебарско проширење поља  $F$ . Кажемо да је  $\varphi : K \rightarrow L$  релативно поштавање над  $F$  ако је  $\varphi$  хомоморфизам који је 1-1 и још је  $\varphi(x) = x$  за све  $x \in F$ .

Скуп свих релативних потапања  $K$  у  $L$  над пољем  $F$  означавамо  $\text{Pot}_F(K, L)$ .

Групу свих аутоморфизама поља  $K$  означавамо  $\text{Aut}(K)$ .

Групу свих релативних изоморфизама  $K$  у  $K$  над  $F$  (тј. релативних аутоморфизама  $K$  над  $F$ ) означавамо  $\text{Gal}(K/F)$  и зовемо група Галоа  $K$  над  $F$ .

**Пример 191.** Једини аутоморфизам поља  $\mathbb{R}$  је идентичко пресликање.

## 22. НОРМАЛНА ПРОШИРЕЊА

**Лема 192.** Нека су  $F \leq K \leq L$  поља, нека је  $K$  алгебарско проширење поља  $F$  и  $\varphi \in \text{Pot}_F(K, L)$ . Ако је  $\varphi[K] \subseteq K$ , онда је  $\varphi[K] = K$ .

**Лема 193.** Нека је  $K$  алгебарско проширење поља  $F$ . Следећи услови су еквивалентни:

- (1) за свако  $\varphi \in \text{Pot}_F(K, \overline{K})$  је  $\varphi[K] = K$ .
- (2) за свако поље  $L \geq K$  и свако  $\varphi \in \text{Pot}_F(K, L)$  је  $\varphi[K] = K$ .

**Дефиниција 194.** Нека је  $K$  алгебарско проширење поља  $F$ . Кажемо да је  $K$  нормално проширење  $F$  ако за све  $\varphi \in \text{Pot}_F(K, \overline{K})$  важи  $\varphi[K] = K$  (тј.  $\varphi \in \text{Aut}(K)$ ).

## 23. x - КАРАКТЕРИЗАЦИЈА НОРМАЛНИХ ПРОШИРЕЊА

**Теорема 195.** Нека је  $K$  алгебарско проширење поља  $F$ . Тада су следећи услови еквивалентни:

- (1)  $K$  је нормално проширење  $F$ .
- (2) Ако је  $f(x) \in F[x]$  несводљив у  $F[x]$  и постоји  $\alpha \in K$  такав да је  $f(\alpha) = 0$ , онда се у  $K[x]$  полином  $f(x)$  разлајзе на производ линеарних фактора.
- (3)  $K$  је поље разлађања над  $F$  неке фамилије полинома из  $F[x]$  (уј.  $K$  је минимално проширење поља  $F$  у ком се сви полиноми из  $F$  разлајзу на линеарне факторе).

**Пример 196.** Пример алгебарског проширења поља које није нормално.

**Теорема 197.** Нека је  $K$  коначно проширење поља  $F$ . Тада је  $K$  нормално проширење  $F$  ако је поље разлађања неког полинома  $f(x) \in F[x]$  над  $F$ .

**Пример 198.** Пример три поља  $F \leq K \leq L$  таквих да је  $K$  нормално проширење  $F$  и  $L$  нормално проширење  $K$ , али да није  $L$  нормално проширење  $F$ .

## 24. СЕПАРАБИЛНА ПРОШИРЕЊА

**Дефиниција 199.** Нека је  $K$  алгебарско проширење поља  $F$ . За  $\alpha \in K$  кажемо да је *сепарабилан* над  $F$  ако  $p_\alpha^F(x)$  нема вишеструке нуле у  $\bar{K}$ . Кажемо да је  $K$  *сепарабилно* *проширење*  $F$  ако су сви елементи у  $K$  сепарабилни над  $F$ .

**Лема 200.** Нека је  $L$  алгебарско *проширење*  $F$ , а  $K$  алгебарско *проширење*  $L$ . Тада је

$$|\text{Pot}_F(L, \bar{K})| \cdot |\text{Pot}_L(K, \bar{K})| = |\text{Pot}_F(K, \bar{K})|.$$

**Теорема 201.** Нека је  $K$  коначно *проширење* поља  $F$ . Тада

- (1)  $|\text{Pot}_F(K, \bar{K})| \leq [K : F]$ ,
- (2)  $|\text{Pot}_F(K, \bar{K})| = [K : F]$  ако је  $K$  *сепарабилно* *проширење*  $F$ .

## 25. ТЕОРИЈА ГАЛОА

Приметимо да ако је  $K$  проширење поља  $F$  и  $H \leq \text{Gal}(K/F)$  онда је  $\{\alpha \in K : (\forall \varphi \in H) \varphi(\alpha) = \alpha\}$  потпоље поља  $K$  (овде  $\leq$  означава подгрупу).

**Дефиниција 202.** Нека је  $K$  проширење поља  $F$  и  $H$  подгрупа групе  $\text{Gal}(K/F)$ . Тада поље

$$K_H = \{\alpha \in K : (\forall \varphi \in H) \varphi(\alpha) = \alpha\}$$

зовемо *поље инваријаната* подгрупе  $H$ .

Приметимо и да ако је  $F$  минимално потпоље од  $K$ , онда је  $\text{Gal}(K/F) = \text{Aut}(K)$ . Конкретно, то се дешава увек када је  $F \cong \mathbb{Q}$  или  $F \cong \mathbb{Z}_p$  за неки прост број  $p$ .

**Теорема 203** (Без доказа). Нека је  $K = F[\alpha_1, \dots, \alpha_n]$  алгебарско *проширење* поља  $F$ , шакво да су  $\alpha_1, \dots, \alpha_n$  *сепарабилни* над  $F$ . Тада је  $K$  *просечно* *проширење*  $F$ , тј. јоскоји  $\beta \in K$  шакав да је  $K = F[\beta]$ .

**Теорема 204.** Нека је  $K$  алгебарско *проширење* поља  $F$  и  $G$  коначна *подгрупа* *трупе*  $\text{Gal}(K/F)$ . Тада:

- (1)  $K$  је коначно, нормално и *сепарабилно* *проширење* поља  $K_G$ ,
- (2)  $[K : K_G] = |G|$ ,
- (3)  $\text{Gal}(K/K_G) = G$ .

**Последица 205.** Ако је  $K$  коначно, нормално и *сепарабилно* *проширење* поља  $F$ , онда:

- (1)  $|\text{Gal}(K/F)| = [K : F]$ ,
- (2)  $F = K_{\text{Gal}(K/F)}$ .

**Теорема 206** (Без доказа). Нека је  $L$  коначно, нормално и *сепарабилно* *проширење* поља  $F$ . Тада јоскоје *пресликања*

$$\{K : F \leq K \leq L\} \xrightarrow[\Phi]{\psi} \{H : H \leq \text{Gal}(L/F)\}$$

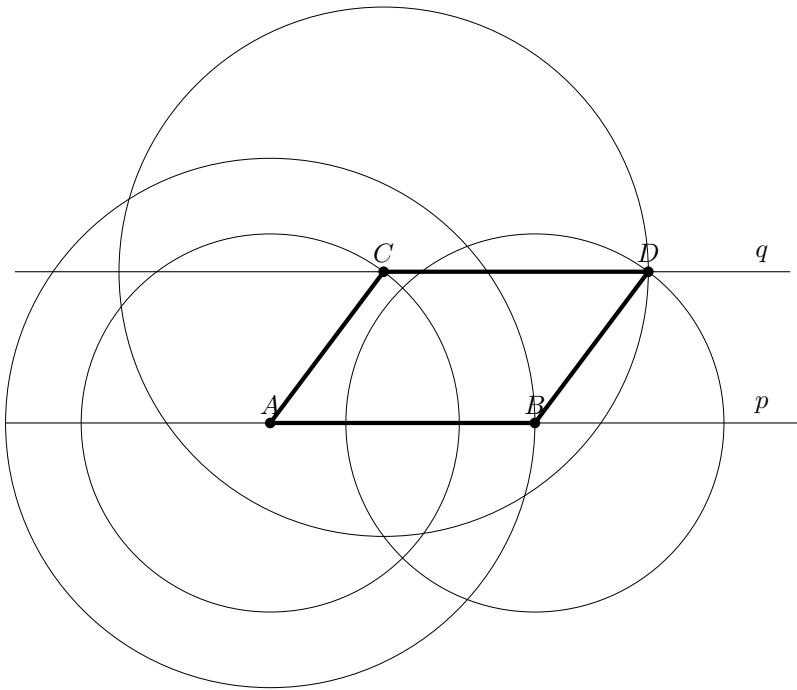
шаква да је  $\Phi(H) = L_H$  и  $\psi(K) = \text{Gal}(L/K)$  и да за њих важи:

- (1)  $\Phi$  и  $\psi$  су међусобно инверзне бијекције,
- (2)  $\Phi$  и  $\psi$  су аниши-изоморфизми мрежса,
- (3)  $H$  је нормална *подгрупа*  $\text{Gal}(L/F)$  ако је  $L_H$  нормално *проширење*  $F$ ,
- (4) ако је  $H$  нормална *подгрупа*  $\text{Gal}(L/F)$ , онда је  $\text{Gal}(L_H/F) \cong \text{Gal}(L/F)/\text{Gal}(L/L_H)$ .

## 26. КОНСТРУКЦИЈЕ ШЕСТАРОМ И ЛЕЊИРОМ

Нека су дате две тачке у равни које ће бити координатни почетак и тачка  $(1, 0)$ . Све тачке које се могу конструисати шестаром и лењиром су конструабилне тачке. Шестар узима као отвор неку познату дужину  $r$  (раздаљину између две претходно конструисане тачке) и описује кружницу полупречника  $r$  око неке претходно конструисане тачке као центра. Лењир узима неке две претходно конструисане тачке и повлачи праву која је њима одређена. Нове тачке се конструишу кад се права или кружница коју смо конструисали пресече са неком правом или кружницом коју смо претходно конструисали. Све тачке које можемо конструисати после коначно много таквих корака зову се *конструабилне* тачке.

Прво конструишимо праву која пролази кроз тачку  $C$  паралелну правој  $p(A, B)$ . Илустрација ове конструкције дата је на слици 1 доле:



СЛИКА 1. Конструкција праве  $q$  кроз тачку  $C$  паралелно са правом  $p = p(A, B)$ .

Сад је јасно да је тачка конструкцијилна ако су јој пројекције на координатне осе  $x$  и  $y$  конструкцијилне: У једном смеру пројектујемо на координате, тако што повлачимо паралелу из тачке са сваком координатном осом (таква паралела је нормала на другу координатну осу и тако добијамо нормалну пројекцију на ту другу осу). У супротном смеру, конструишемо правоугаоник коме су три темена координатни почетак, пројекција тачке на  $x$  и пројекција тачке на  $y$  осу.

Скуп свих конструкцијилних тачака на  $x$  оси дат је својим  $x$ -координатама и нека је тај скуп координата  $G$ . Онда је  $G \subseteq R$  и  $G$  је такође и скуп свих конструкцијилних тачака на  $y$ -оси (шестаром се лако пребацују са осе на осу). На основу претходног пасуса, скуп свих конструкцијилних тачака у равни је  $G \times G$ .

**Лема 207.**  $G$  је поштоље поља реалних бројева.

Дакле,  $G$  је поље и очигледно важи  $\mathbf{Q} \leq G \leq \mathbf{R}$ .

**Лема 208.** Ако је  $a \in G$ , онда је  $u \sqrt{a} \in G$ .

Даље, ако је тачка конструкцијилна, онда је могуће конструисати је у коначно много елементарних корака од почетне две тачке, где су елементарни кораци детаљно описани са:

- (1) ако су дате две праве (тиме што свака садржи по две претходно конструисане тачке), онда можемо конструисати њихов пресек,
- (2) ако су дате права и кружница (кружница је дата ако је претходно конструисан њен центар и ако је полупречник  $r$  такав да је претходно конструисана тачка  $(r, 0)$ ), онда можемо конструисати њихов пресек, и коначно
- (3) ако су дата два круга, онда можемо конструисати њихов пресек.

**Лема 209** (Без доказа). Нека су све тачке које су конструисане после неколико елементарних корака неке конструкције у  $F \times F$ . Тада следећим елементарним кораком конструишимо тачке које су или у  $F \times F$ , или у  $F[\alpha] \times F[\alpha]$ , где је  $\alpha$  елеменат који је алгебарски наг  $F$  и такав да је  $p_\alpha^F(x)$  полином симетричен 2.

**Теорема 210.** Нека  $\alpha \in \mathbf{R}$ . Онда  $\alpha \in G$  ако постоји коначан низ поља  $\mathbf{Q} = \mathbf{F}_0 \leq \mathbf{F}_1 \leq \dots \leq \mathbf{F}_m \leq \mathbf{R}$  посвећен  $\alpha \in F_m$  и за све  $i < m$  важи  $[\mathbf{F}_{i+1} : \mathbf{F}_i] = 2$ .

**Последица 211.** Сваки  $\alpha \in G$  је алгебарски елеменат наг  $\mathbf{Q}$  и  $\deg(p_\alpha^{\mathbf{Q}}(x)) = 2^k$  за неко природно  $k$ .

**Последица 212.** Нека је  $z \in \mathbf{C}$  конструкцијилан. Онда је  $z$  алгебарски елеменат наг  $\mathbf{Q}$  и  $\deg(p_\alpha^{\mathbf{Q}}(x)) = 2^k$  за неко природно  $k$ .

Сад прелазимо на три класична проблема из конструкције шестаром и лењиром.

**Делски проблем** тражи да шестаром и лењиром одредимо страну која ће имати дупло већу запремину од задате коцке.

Грчки бот Аполон је обећао да ће скинуши шроклештво са града Делоса ако трађани усређу да конструишу двоспратуко већи храм од већ постојећег, али истог облика. Постојећи храм је био облика саврешене коцке.

У Старој Грчкој су математичари (наводно, ученици Платона) уселили да реше проблем механички, шако што су најправили справе које иртају криве које нису само праве и кругнице. Међутим, штитање је осјало да ли је било могуће да се конструише страна које користећи "числу теометрију", дакле, шестаром и лењиром.

Садашњим речником, питање је да ли је број  $\sqrt[3]{2}$  конструктибилан. Тада је корен полинома  $x^3 - 2$ , који је несводљив над  $Q$  на основу Ајзенштајновог критеријума. Дакле,  $p_{\sqrt[3]{2}}^Q(x) = x^3 - 2$ , и стога  $\sqrt[3]{2}$  није конструкцибилан број на основу последице 211. Дакле, да су житељи Делоса располагали само шестаром и лењиром, град би и дан-данас био проклет.

**Трисекција угла** тражи да, користећи само шестар и лењир, конструишу угао који је три пута мањи од датог. Проблем је постављен кад су у Старој Грчкој математичари открили конструкцију произвљеног рационалног умношка дате дужи (конструкцијама које доказују да је  $G$  поље у доказу леме 207), као и да преполове произвљан угао. Доказе да се Делски проблем и трисекција угла не могу решити дао је Пјер Вантел<sup>1</sup> 1837.

Доказаћемо да је немогућа конструкција угла од  $20^\circ$ , мада је угао од  $60^\circ$  (тривијално) конструкцибилан. Ако би угао од  $20^\circ$  био конструкцибилан, онда бисмо могли да конструишу тачку на јединичној кругници која је под тим углом са позитивним смером  $x$  осе. То је тачка са координатама  $(\cos 20^\circ, \sin 20^\circ)$ . За косинус троструког угла важи формула  $\cos 3x = 4\cos^3 x - 3\cos x$ , па кад заменимо  $x = 20^\circ$  и  $\cos 60^\circ = 1/2$  и помножимо са 2, добијамо  $1 = 8\cos^3 20^\circ - 6\cos 20^\circ$ . Ако заменимо  $\beta = 2\cos 20^\circ$ , добијамо да је  $\beta$  конструкцибилан ако је  $\cos 20^\circ$  конструкцибилан, и да  $\beta^3 - 3\beta - 1 = 0$ . Кад би полином  $p(x) = x^3 - 3x - 1$  био сводљив над  $Q$ , како је  $p(x)$  кубни полином, онда би један од нетривијалних фактора морао бити линеаран. Дакле,  $p(x)$  би морао имати рационалну нулу, а то би по критеријуму за рационалне нуле морао бити неки број из скупа  $\{1, -1\}$ . Међутим,  $p(1) = -3$  и  $p(-1) = -1$ , па је  $p(x)$  несводљив над  $Q$ . Дакле,  $p_\beta^Q(x) = x^3 - 3x - 1$ , и стога  $\beta$  није конструкцибилан број на основу последице 211.

**Квадратура круга** је проблем да се шестаром и лењиром конструише квадрат који има исту површину као дати круг. Ако је полупречник круга 1, онда је потребно конструисати квадрат повешице  $\pi$ . Дакле, квадратура круга је могућа ако је  $\sqrt{\pi}$  конструкцибилан број ако је (на основу теореме 210)  $\pi$  конструкцибилан. Међутим, Линдеман<sup>2</sup> је 1882. доказао (а Вајерштрас<sup>3</sup> уопштио резултат 1885.) да је  $\pi$  трансцендентан број, (то је нешто дужи доказ који не радимо у овом курсу, мада га можда укључим у неку каснију верзију ових белешки), па није конструкцибилан. Дакле, ни квадратура круга није могућа.

Проблем којем се у наставку посвећујемо је конструкцибилност правилног  $n$ -тоугла. Историјски, стари Грци су знали да конструишу правилни троугао, четвороугао, петоугао, петнаестоугао и, ако им је дат конструисан правилни  $n$ -тоугао, умели су да конструишу правилни  $2n$ -тоугао. Гаус<sup>4</sup> је 1796., када је имао само 19 година, конструисао правилни седамнаестоугао и, одушевљен лепотом те конструкције, определио се да постане математичар. Његова је и формулација теореме која даје потребан и довољан услов за  $n$  да би била могућа конструкција правилног  $n$ -тоугла. Тврдио је да је имао доказ да је тај услов потребан и довољан, мада је објавио само доказ довољности 1801. Иначе, Гаус је био изразито стидљив и објавио је много мање резултата него што је доказао, после ригорозних дугогодишњих провера. Без сумње је имао и доказ потребности, али први објављени доказ потребности је заслуга Пјера Вантела, и објављен је у истом раду у ком је решио дупликацију које и трисекцију угла. Доказе који следе адаптирали смо из књиге [10] и из белешки професора Милана Груловића.

<sup>1</sup>Pierre Laurent Wantzel (1814-1848), француски математичар

<sup>2</sup>Carl Louis Ferdinand von Lindemann (1852-1939), немачки математичар

<sup>3</sup>Karl Theodor Wilhelm Weierstrass (1815-1897), немачки математичар

<sup>4</sup>Johann Carl Friedrich Gauss (1777-1855), славни немачки математичар

## ЛИТЕРАТУРА

- [1] Siniša Crvenković, Igor Dolinka, Rozalia Sz. Madarasz: Odabrane teme opšte algebre, PMF u Novom Sadu, 1998.
- [2] Milan Grulović (beleške Ivane Djurdjević), Beleške iz Algebре 3, dostupno na moodle stranici kursa, 2014.
- [3] Milan Grulović, Predavanja iz Algebре 4, link dostupan na moodle stranici kursa, 2017.
- [4] Milan Grulović, Pismeni zadaci iz Algebarskih struktura, 2018.
- [5] Boriša Kuzeljević, Petar Marković, Zbirka zadataka iz Prstena, polja i teorije Galoa (Algebре 3), PMF u Novom Sadu, 2023.
- [6] Martin Isaacs, Algebra: a graduate course, American Mathematical Society, 1994.
- [7] Serge Lang, Algebra, Springer, 2002.
- [8] Petar Marković, Dodaci iz PPTG, dostupno na moodle stranici kursa, 2017.
- [9] Joseph Silverman, Abstract Algebra, American Mathematical Society, 2022.
- [10] Ian Stewart, Galois Theory, Chapman & Hall, 2003.
- [11] Jovana Tomik Ognjenović, Ciklotomični polinomi, Master rad na DMI - dostupan na moodle stranici kursa, 2020.