Univerzitet u Beogradu – Matematički fakultet

Predavanja iz Algebre II

Žarko Mijajlović

Beograd 2001

Žarko Mijajlović

Ciklične grupe

Grupa $\mathbb{G}$ je ciklična ako je $\mathbb{G}$ generisana jednim elementom, tj. postoji $a \in G$ t.d. $\mathbb{G} = \langle a \rangle$.

<u>Primeri</u> 1° $\mathbb{Z} = (Z, +, -, 0) = \langle 1 \rangle$, $Z = \{\dots, -2, -1, 0, 1, 2, \dots\}$

2° $\mathbb{Z}_n = (Z_n, +_n, -, 0) = \langle 1 \rangle$, $Z_n = \{0, 1, \dots, n-1\}$,

3° $C_n = \{x \in C \mid x^n = 1\} = \langle \varepsilon \rangle$, $\varepsilon = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$

C = skup kompleksnih brojeva

$\mathbb{C}_n = (C_n, \cdot, ^{-1}, 1)$.

<u>Teorema 1.</u> Neka je $\mathbb{G} = \langle a \rangle$.

a) Ako je $red(a) = n$, onda $G = \{1, a, \dots, a^{n-1}\}$ i za $0 \le i < j < n$, $a^i \ne a^j$.

b) Ako je $red(a) = \infty$, onda $G = \{\dots, a^{-2}, a^{-1}, 1, a, a^2, \dots\} = \{a^n \mid n \in Z\}$, $i \ne j \Rightarrow a^i \ne a^j$.

<u>Dokaz</u> a) Neka je $\alpha \in Z$. Tada postoje $q, i \in Z$, t.d.

(1) $\alpha = nq + i$, $0 \le i < n$.

S druge strane $\langle a \rangle = \{a^\alpha \mid \alpha \in Z\}$ pa prema (1)

$G = \langle a \rangle = \{a^i \mid 0 \le i < n\} = \{1, a, a^2, \dots, a^{n-1}\}$.

Ako $0 \le i < j < n$ onda $a^i \ne a^j$, jer u suprotnom $a^{j-i} = 1$, $0 < j - i < n$, što je # prema $red(a) = n$.

b) Neka su $\alpha, \beta \in Z$, $\alpha < \beta$. Ako $a^\alpha = a^\beta$, onda $a^{\beta-\alpha} = 1$, $\beta - \alpha \ne 0$, # prema pretpostavci $red(a) = \infty$.

<u>Teorema 2.</u> Neka su $\mathbb{G}$ i $\mathbb{H}$ ciklične grupe istog reda. Tada $\mathbb{G} \cong \mathbb{H}$.

<u>Dokaz</u> Neka su $\mathbb{G} = \langle a \rangle$, $\mathbb{H} = \langle b \rangle$.

a) Ako je $red(a) = red(b) = n$ onda je $f = \begin{pmatrix} 1 & a & a^2 & \dots & a^{n-1} \\ 1 & b & b^2 & \dots & b^{n-1} \end{pmatrix}$

$f : \mathbb{G} \cong \mathbb{H}$.

Zaista, f je 1-1 i na jer $G = \{1, \dots, a^{n-1}\}$, $H = \{1, \dots, b^{n-1}\}$ i $|G| = |H| = n$. Takođe, f je homomorfizam:

Za $a^i, a^j \in G$, neka je $k = ost(i+j, n) = i +_n j$. Tada

$a^i \cdot a^j = a^{i+j} = a^{qn+k} = a^k = a^{i +_n j}$, pa

$f(a^i \cdot a^j) = f(a^{i+j}) = f(a^k) = b^k = b^{i+j} = b^i \cdot b^j = f(a^i) f(a^j)$.

b) $red(a) = red(b) = \infty$. Tada $f : \mathbb{G} \cong \mathbb{H}$, gde

$f : a^\alpha \mapsto b^\alpha$, $\alpha \in Z$.

Dakle sve cikličke grupe su:

$\mathbb{C}_1, \mathbb{C}_2, \mathbb{C}_3, \dots$ (konačne cikličke grupe)

$\mathbb{C}_\infty$ (beskonačna ciklička grupa)

i dakako $\mathbb{C}_n \cong (\mathbb{Z}_n, +_n, 0)$, $\mathbb{C}_\infty \cong (\mathbb{Z}, +, 0)$.

Teorema 3. a) Homomorfna slika cikličke grupe je ciklična grupa.

b) Podgrupa cikličke grupe je ciklička grupa.

c) Neka su $m, n \in N^+$. Tada $\mathbb{C}_{mn} \cong \mathbb{C}_m \times \mathbb{C}_n$ akko $(m,n)=1$.

Dokaz a) Neka je $\mathbb{G} = \langle a \rangle$ i $h: \mathbb{G} \xrightarrow{na} \mathbb{H}$, tj. $\mathbb{H} = h\mathbb{G}$.

Tada $\mathbb{H} = \langle h(a) \rangle$.

b) Neka je $\mathbb{G} = \langle a \rangle$ i $H < \mathbb{G}$. P.P. $\operatorname{red} \mathbb{H} > 1$. Neka je $k \in N^+$ najmanji (pozitivan prirodan broj) takav da $a^k \in H$. Kako je $H < \mathbb{G}$ to $\langle a^k \rangle \subseteq H$. Neka je $x \in H$. Tada postoji $i \in \mathbb{Z}$ t.d. $x = a^i$. Neka su $q, r \in \mathbb{Z}$ t.d.

$$i = k \cdot q + r, \quad 0 \leq r < k.$$

Tada $a^r = a^i \cdot (a^k)^{-q}$ pa $a^r \in H$ jer $a^i, a^k \in H$. S obzirom na izbor broja k, sledi da je $r = 0$, pa $x = a^i = (a^k)^q$ tj. $x \in \langle a^k \rangle$. Dakle $H = \langle a^k \rangle$, tj. H je ciklička.

c) Neka su $m, n \in N^+$, $(m,n)=1$. Prema teoremi o razlaganju prstena $\mathbb{Z}_{mn}$, važi $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$, tj.

$$(\mathbb{Z}_{mn}, +_{mn}, \cdot_{mn}, 0, 1) \cong (\mathbb{Z}_m, +_m, \cdot_m, 0, 1) \times (\mathbb{Z}_n, +_n, \cdot_n, 0, 1)$$

pa $(\mathbb{Z}_{mn}, +_{mn}, 0) \cong (\mathbb{Z}_m, +_m, 0) \times (\mathbb{Z}_n, +_n, 0)$.

Dakle $\mathbb{C}_{mn} \cong \mathbb{C}_m \times \mathbb{C}_n$ jer $\mathbb{C}_{mn} \cong (\mathbb{Z}_{mn}, +_m, 0)$, $\mathbb{C}_n \cong (\mathbb{Z}_n, +_n, 0)$.

Pretpostavimo $(m,n) \neq 1$, tj. za $d = (m,n)$, $d > 1$. Neka je $k = \frac{mn}{d}$. Dalje, $\mathbb{C}_m \times \mathbb{C}_n = \langle \bar{a}, \bar{b} \rangle$, gde $\bar{a} = (a, 1)$, $\bar{b} = (1, b)$ i $\operatorname{red}(a) = m$, $\operatorname{red}(b) = n$. Tada

$a^k = a^{m \cdot \frac{n}{d}} = (a^m)^{\frac{n}{d}} = 1$ i slično $b^k = b^{n \cdot \frac{m}{d}} = (b^n)^{\frac{m}{d}} = 1$, pa za proizvoljan $(a^i, b^j) \in \mathbb{C}_m \times \mathbb{C}_n$,

$(a^i, b^j)^k = ((a^k)^i, (b^k)^j) = (1,1)$, tj. za $x \in \mathbb{C}_m \times \mathbb{C}_n$,

$\operatorname{red}(x) \leq k < mn$, pa $\mathbb{C}_m \times \mathbb{C}_n \not\cong \mathbb{C}_{mn}$. ▨

Teorema 4. Neka su $k, n \in N^+$ i pretpostavimo da $k \mid n$. Tada postoji tačno jedna podgrupa $H < C_n$, $red(H) = k$.

Dokaz Neka je $C_n = \langle a \rangle$. Tada $H = \langle a^{\frac{n}{k}} \rangle$ je reda k i $H < C_n$. Dokažimo da je H jedina podgrupa reda k grupe C_n. Neka je $H' < C_n$, $|H'| = k$. Prema dokazu Teoreme 3 b, postoji $i \in N^+$ (uz uslov $k > 1$; za $k = 1$ tvrđenje trivijalno sledi) t.d. $H' = \langle a^i \rangle$, i pri tome i je najmanji pozitivan broj sa tom osobinom. Kako je $red(H') = k$, to $a^{ik} = 1$ pa $ik \equiv 0 \mod n$, tj. $n \mid ik$. Kako $k \mid n$, zatim i je najmanji pr. broj da $n \mid ik$, to $ik = n$, pa $i = \frac{n}{k}$, tj. $H' = \langle a^{\frac{n}{k}} \rangle = H$.

Teorema 5 Neka je $S = \{ b \in C_n \mid C_n = \langle b \rangle \}$. Tada $|S| = \varphi(n)$, gde je $\varphi(n)$ Eulerova f-ja.

Dokaz Neka je $C_n = \langle a \rangle$, i neka je $b \in S$. Tada $b = a^i$ za neki $i \in Z_n \setminus \{0\}$. Kako $C_n = \langle b \rangle$ to za neki k, $b^k = a$ tj. $a^{ik} = a$, odavde $ik \equiv 1 \mod n$ pa $i \in \Phi(n)$ (jer je i jedinica prstena Z_n). S druge strane, neka je $i \in \Phi(n)$. Tada za neki $k \in Z_n$, $ik \equiv 1 \mod n$, pa $ik = 1 + dn$ za neki $d \in Z$. Odavde $a^{ik} = a^{1+dn} = a^1 \cdot a^{dn} = a$, pa za proizvoljno $x \in C_n$ za odgovarajuće $j \in N$ imamo

$$x = a^j = (a^{ik})^j = (a^i)^{kj} \quad \text{tj.} \quad x \in \langle a^i \rangle, \text{ pa } C_n = \langle a^i \rangle.$$

Dakle, $C_n = \langle a^i \rangle$ akko $i \in \Phi_n$, pa $|S| = |\Phi(n)| = \varphi(n)$. ∎

Odavde imamo sledeće zanimljive primene:

1° Neka je $d \mid n$, $S_d = \{ x \in C_n \mid red(x) = d \}$. Prema Lagranževoj teoremi, $C_n = \bigcup_{d \mid n} S_d$ i to je disjunktna unija, pa

$$n = |C_n| = \sum_{d \mid n} |S_d|.$$

Ako je $H_d < C_n$ podgrupa (jedina prema Teoremi 4) grupe C_n reda d, to je S_d skup generatora grupe H_d pa prema Teoremi 5,

$$n = \sum_{d \mid n} \varphi(d).$$

Prema teoremi inverzije, onda $\varphi(n) = \sum_{d \mid n} \mu(d) \frac{n}{d} = n \sum_{d \mid n} \frac{\mu(d)}{d}$.

2° $Aut\, C_n \cong \Phi_n$.
Zaista, $f \in Aut\, C_n$ u potpunosti je određen vrednošću $f(a)$, gde $C_n = \langle a \rangle$, jer $f(a^i) = f(a)^i$. S druge strane ako $C_n = \langle a \rangle$ onda $C_n = f(C_n) = \langle fa \rangle$ pa je fa generator grupe C_n.

Takođe, ako $C_n = \langle a \rangle$ onda za $k \in \Phi(n)$, preslikavanje $f: C_n \to C_n$ definisano sa

$$f(a^i) = a^{ki}, \quad i = 0, 1, \ldots, n-1$$

jeste automorfizam grupe C_n:

$$f(a^i \cdot a^j) = f(a^{i+j}) = f(a^{i +_n j}) = a^{k(i +_n j)} = a^{k \cdot_n (i +_n j)}$$
$$= a^{k \cdot_n i +_n k \cdot_n j} = a^{k \cdot_n i} \cdot a^{k \cdot_n j} = a^{ki} \cdot a^{kj} = f(a^i) f(a^j)$$

tj. f je homomorfizam, a da je 1-1 sledi iz činjenice da je $f(C_n) = C_n$.

Dakle, $\mathrm{Aut}\, C_n = \{ f_k \mid k \in \Phi(n) \}$, gde je $f_k(a) = a^k$.

Neka je $F: \Phi(n) \to \mathrm{Aut}\, C_n$, $F: k \mapsto f_k$, $k \in \Phi(n)$.

Tada: a) F je 1-1 i na (prema prethodnom)

b) $F: \Phi(n) \to \mathrm{Aut}\, C_n$.

Neka su $l, k \in \Phi(n)$ i neka je $s = l \cdot_n k$.

Tada $(f_k \circ f_l)(a) = (a^l)^k = a^{lk} = a^{l \cdot_n k} = f_s(a)$

pa $f_s = f_k \circ f_l$ jer se f_s i $f_k \circ f_l$ poklapaju na generatoru a.

$a^{lk} = a^{l \cdot_n k}$ jer $a^{l \cdot_n k} = a^{lk + dn} = a^{lk} \cdot a^{dn} = a^{lk} \cdot 1$

Dakle, F je 1-1 i na homomorfizam grupe $\Phi(n)$ na grupu $\mathrm{Aut}\, C_n$ pa $\Phi(n) \cong \mathrm{Aut}\, C_n$.

<u>Primer</u> Odrediti grupu $\mathrm{Aut}\, C_{12}$.

<u>Rešenje</u> $\mathrm{Aut}\, C_{12} \cong \Phi(12) = \Phi(3 \cdot 4) \cong \Phi(3) \times \Phi(4) \cong C_2 \times C_2$.

<u>Zadatak</u> Odrediti $\mathrm{Aut}\, C_{100}$

<u>Zadatak</u> Dokazati da $C_\infty \times C_\infty \not\cong C_\infty$ i napište $C_\infty^m \cong C_\infty^n$ akko $m = n$.

<u>Zadatak</u> Da li klasa cikličnih grupa obrazuje algebarski varijetet? Obrazložiti.

<u>Zadatak</u> Dokazati da je svaka ciklična grupa homomorfna slika grupe C_∞.

Abelove grupe

April 2000
Žarko Mijajlović

Grupa $\mathbb{G}$ je Abelova ako je komutativna, tj. ako za sve $x, y \in G$, $x \cdot y = y \cdot x$. U slučaju Abelovih grupa često se koristi aditivna notacija:

multiplikativna notacija	aditivna notacija
$\mathbb{G} = (G, \cdot, ^{-1}, 1)$	$\mathbb{A} = (A, +, -, 0)$
$x \cdot y = z$	$x + y = z$
$y = x^{-1}$, $z = x y^{-1}$	$y = -x$, $z = x - y$
$y = x^n$, $n \in Z$	$y = nx$, $n \in Z$
$y = x_1^{d_1} x_2^{d_2} \cdots x_k^{d_k}$	$y = d_1 x_1 + d_2 x_2 + \cdots + d_k x_k$ $(d_1, \ldots, d_k \in Z)$
$y = \prod_{i=1}^{n} x_i$	$y = \sum_{i=1}^{n} x_i$

Identiteti koji važe u svim grupama

$(m, n \in Z)$

$(x^m)^n = x^{mn}$	$n(mx) = (mn)x$
$x^{m+n} = x^m \cdot x^n$	$(m+n)x = (mx) + (nx)$
$(xy)^{-1} = y^{-1} x^{-1}$	$-(x+y) = (-y) + (-x)$ odnosno u slučaju Ab. grupa $-(x+y) = (-x) + (-y)$

Identiteti koji važe u Abelovim grupama

$(xy)^{-1} = x^{-1} y^{-1}$	$-(x+y) = (-x) + (-y)$
$(xy)^m = x^m y^m$	$m(x+y) = mx + my$
$\prod_{i \in I} x_{p_i} = \prod_{i \in I} x_i$	$\sum_{i \in I} x_{p_i} = \sum_{i \in I} x_i$

$p \in S_n$, $I = \{1, \ldots, n\}$

Konstrukcije:

$G = H \cdot K$, $H, K < G$	$\mathbb{A} = B + C$, $B, C < \mathbb{A}$
$\mathbb{G}$ je unutrašnji proizvod podgrupa H, K; $G = HK$, $H \cap K = \langle 1 \rangle$	$\mathbb{A}$ je direktna suma podgrupa B i C; $\mathbb{A} = B \dot{+} C$, $B \cap C = \langle 0 \rangle$.

Primeri Abelovih grupa: $\mathbb{C}_n$, $(\mathbb{Z},+,0)$, $(\mathbb{Q},+,0)$, $(\mathbb{Q}\setminus\{0\},\cdot,1)$, ...
Primeri grupa koje nisu Abelove: $\mathbb{S}_n$ – grupa permutacija skupa $\{1,2,\dots,n\}$.
$\mathbb{D}_n$ – dijedarska grupa – grupa simetrija pravilnog n-tougla.

<u>Teorema</u> Abelove grupe čine algebarski varijetet.
Dakle, klasa Abelovih grupa zatvorena je za:
- podgrupe
- homomorfne slike
- operaciju proizvoda algebri
- konstrukciju količničke algebre.

<u>Napomena</u> Svaka podgrupa Abelove grupe G je normalna u G tj.,
$H < G \Rightarrow H \triangleleft G$. Dakle, ako je $H < G$, postoji i dobro je definisana količnička grupa G/H.

<u>Teorema o razlaganju konačno-generisanih Abelovih grupa</u>

Ciklične grupe su Abelove grupe. Dakle za sve koje $n_1,\dots,n_k \in \mathbb{N}^+$,
$\mathbb{C}_{n_1} \times \mathbb{C}_{n_2} \times \dots \times \mathbb{C}_{n_k}$ je Abelova grupa (i to konačna). Ima li drugih Abelovih grupa? Nema! O tome govori upravo sledeća teorema:

Svaka konačno generisana Abelova grupa je proizvod cikličnih grupa.

Pre no što izložimo dokaz ove teoreme, dokazaćemo nekoliko pomoćnih tvrđenja – lema koje su od nezavisnog interesa.

<u>Lema 1</u> Neka su $a_1, a_2, \dots, a_n \in \mathbb{Z}$, $n \geq 2$, takvi da je $(a_1, a_2, \dots, a_n) = 1$, tj. $NZD(a_1, a_2, \dots, a_n) = 1$. Tada postoji kvadratna matrica M reda n nad $\mathbb{Z}$ takva da je $\det M = 1$.

<u>Dokaz</u> izvodimo indukcijom po n.

<u>Slučaj $n=2$</u> Neka su $a_1, a_2 \in \mathbb{Z}$, $(a_1, a_2) = 1$. Prema Bezuovoj teoremi postoje $\alpha, \beta \in \mathbb{Z}$ takvi da je $\alpha a_1 + \beta a_2 = 1$. Odatle za
$M = \begin{bmatrix} a_1 & a_2 \\ -\beta & +\alpha \end{bmatrix}$ važi $\det M = 1$.

Pretpostavimo IH, da tvrđenje važi za $n-1$. Neka su $a_1, \dots, a_n \in \mathbb{Z}$ takvi da je $(a_1, a_2, \dots, a_n) = 1$. Neka je $d = (a_1, a_2, \dots, a_{n-1})$ i neka su $b_1, b_2, \dots, b_{n-1} \in \mathbb{Z}$ takvi da je $a_1 = b_1 d$, $a_2 = b_2 d, \dots, a_{n-1} = b_{n-1} d$. Tada $(b_1, b_2, \dots, b_{n-1}) = 1$, te prema induktivnoj hipotezi postoji matrica (nad $\mathbb{Z}$)

$$M = \begin{bmatrix} b_1 & b_2 & \cdots & b_{n-1} \\ & & * & \end{bmatrix}$$

reda $n-1$, t.d. $\det M = 1$.

Dalje, $(a_n, d) = 1$, te prema Bezuovoj teoremi postoje $s, t \in \mathbb{Z}$ takvi da je $a_n t + d \cdot s = 1$. Neka je matrica M' nad $\mathbb{Z}$ određena pomoću M na sledeći način:

$$M' = \begin{bmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ & & * & & 0 \\ & & & & \vdots \\ & & & & 0 \\ \varepsilon t b_1 & \varepsilon t b_2 & \cdots & \varepsilon t b_{n-1} & s \end{bmatrix}$$

gde je $\varepsilon \in \{1, -1\}$ i gde će se tačna vrednost za ε odrediti kasnije.

Dakle, M' je reda n i važi:

$$\det M' = \begin{vmatrix} d b_1 & d b_2 & \cdots & d b_{n-1} & a_n \\ & * & & & 0 \\ \varepsilon t b_1 & \varepsilon t b_2 & \cdots & \varepsilon t b_{n-1} & s \end{vmatrix} = (-1)^{n+1} a_n \begin{vmatrix} * \\ \varepsilon t b_1 \cdots \varepsilon t b_{n-1} \end{vmatrix} + s \begin{vmatrix} d b_1 \cdots d b_{n-1} \\ * \end{vmatrix} =$$

$$\pm \varepsilon t (-1)^{n+1} a_n \begin{vmatrix} b_1 \cdots b_{n-1} \\ * \end{vmatrix} + s d \begin{vmatrix} b_1 \cdots b_{n-1} \\ * \end{vmatrix} =$$

$$a_n t + d s = 1,$$ birajući ε tako da je $\pm \varepsilon (-1)^{n+1} = 1$. ▨

<u>Posledica 1</u> (uopštenje Bezuove teoreme) Neka su $a_1, \dots, a_n \in \mathbb{Z}$ takvi da je $(a_1, a_2, \dots, a_n) = 1$. Tada diofantovska jednačina

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = 1$$

ima rešenje (u $\mathbb{Z}$).

<u>Dokaz</u> Neka je prema prethodnoj teoremi $M = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ & * & & \end{bmatrix}$ matrica reda n nad $\mathbb{Z}$ takva da je $\det M = 1$.

Tada prema Laplasovoj teoremi, razvijajući $\det M$ po prvoj vrsti,

$$a_1 D_1 + a_2 D_2 + \cdots + a_n D_n = 1 \quad i \quad D_i \in \mathbb{Z},\ i = 1, 2, \dots, n.$$

Dakle, možemo uzeti da je $x_1 = D_1, \dots, x_n = D_n$.

Zadatak Naći opšte rešenje diofantovske jednačine $6x+10y+15z=1$.

Rešenje Kako $(6,10,15)=1$, ova jednačina ima rešenje.

Partikularno rešenje: Rešavanjem ove jednačine u $\mathbb{Z}_6$ nalazimo $4y+3z=1$, odakle, $y_0=1$, $z_0=-1$, te iz polazne jednačine, $x_0=1$, tj. partikularno rešenje je $x_0=1$, $y_0=1$, $z_0=-1$.

Sada rešavamo homogenu jednačinu

$6X+10Y+15Z=0$, uzimajući $X=x-x_0$, $Y=y-y_0$, $Z=z-z_0$.

odakle $6X+10Y=-15Z$. Ova jednačina ima rešenje (prema B.T.) akko $2|Z$. Neka je $Z=2\alpha$. Tada se poslednja jednačina svodi na $3X+5Y=-15\alpha$. Opšte rešenje ove jednačine je

$X=-30\alpha+5\beta$, $Y=15\alpha-3\beta$, $\alpha,\beta\in\mathbb{Z}$, pa je opšte rešenje polazne jednačine: $x=1-30\alpha+5\beta$, $y=1+15\alpha-3\beta$, $z=-1+2\alpha$. ▨

Lema 2 Neka je $\mathbb{A}=(A,+,0)$ Abelova grupa i pp da je $\mathbb{A}$ generisana sa n elemenata $(n\in N^+)$, tj. postoje $x_1,\dots,x_n\in A$ takvi da je $\mathbb{A}=\langle x_1,x_2,\dots,x_n\rangle$. Dalje, neka su $a_1,a_2,\dots,a_n\in\mathbb{Z}$ takvi da je $(a_1,a_2,\dots,a_n)=1$ i neka je $y_1=a_1x_1+a_2x_2+\dots+a_nx_n$. Tada postoje $y_2,\dots,y_n\in A$ takvi da je $\mathbb{A}=\langle y_1,y_2,\dots,y_n\rangle$.
(Lema o promeni baze).

Dokaz Neka je prema Lemi 1, $M=\begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ & * & \end{bmatrix}$, $\det M=1$ i neka je $\begin{bmatrix} y_1\\ y_2\\ \vdots\\ y_n\end{bmatrix}=M\cdot\begin{bmatrix} x_1\\ x_2\\ \vdots\\ x_n\end{bmatrix}$. Dalje, s obzirom da je $\det M=1$, $M^{-1}=\frac{1}{\det M}\cdot\operatorname{adj}(M)$ to je i matrica M^{-1} celobrojna! Otuda

$\begin{bmatrix} x_1\\ x_2\\ \vdots\\ x_n\end{bmatrix}=M^{-1}\begin{bmatrix} y_1\\ y_2\\ \vdots\\ y_n\end{bmatrix}$, pa kako $A=\langle x_1,\dots,x_n\rangle$, to je i $\mathbb{A}=\langle y_1,\dots,y_n\rangle$, jer za $x\in A$,

za neke cele $d_1,\dots,d_n$, $x=d_1x_1+\dots+d_nx_n$, te kako su linearne kombinacije zatvorene za supstituciju linearnih formi, to je za neke $\beta_1,\dots,\beta_n\in\mathbb{Z}$, $x=\beta_1y_1+\dots+\beta_ny_n$ tj. $x\in\langle y_1,\dots,y_n\rangle$. ▨

Neka je $\mathbb{A}$ konačno generisana Abelova grupa. Tada postoji najmanji prirodan broj n takav da je $\mathbb{A}$ generisana sa n elemenata. Ovaj broj n nazvaćemo rangom grupe $\mathbb{A}$ i pišemo $\operatorname{rang} \mathbb{A} = n$.
Dakle, ako je $\operatorname{rang} \mathbb{A} = n$, onda postoje $x_1, \ldots, x_n \in A$ takvi da je $\mathbb{A} = \langle x_1, \ldots, x_n \rangle$ i za sve $k < n$ i sve $y_1, \ldots, y_k \in A$, $\mathbb{A} \neq \langle y_1, \ldots, y_k \rangle$.

<u>Dokaz</u> teoreme o razlaganju konačno generisanih Abelovih grupa. Dokaz izvodimo indukcijom po rang A. Koristimo aditivnu notaciju, dakle dokazujemo da je konačno generisana Abelova grupa $\mathbb{A} = (A, +, 0)$ direktna (konačna) suma cikličnih grupa.

<u>$\operatorname{rang} \mathbb{A} = 1$</u> Tada $\mathbb{A} = \langle a \rangle$ pa je $\mathbb{A}$ ciklična.

<u>$\operatorname{rang} \mathbb{A} = n > 1$</u> Dakle $\mathbb{A}$ je generisana sa n elemenata ali ne i sa manjim brojem. Razlikujemo dva slučaja:

a) postoje $x_1, \ldots, x_n \in A$ takvi da $\mathbb{A} = \langle x_1, \ldots, x_n \rangle$ i bar jedan od elemenata $x_1, \ldots, x_n$ je konačnog reda.

b) Ako je $\mathbb{A} = \langle x_1, \ldots, x_n \rangle$, onda su svi elementi $x_1, \ldots, x_n$ beskonačnog reda.

Pretpostavimo najpre slučaj (a). Neka su $x_1, \ldots, x_n \in A$ takvi da je $\mathbb{A} = \langle x_1, \ldots, x_n \rangle$ i $\{x_1, \ldots, x_n\}$ sadrži element x najnižeg reda u odnosu na sve generatorske skupove $\{y_1, \ldots, y_n\}$ grupe $\mathbb{A}$, tj. ako $\mathbb{A} = \langle y_1, \ldots, y_n \rangle$ onda $\operatorname{red} x \leq \operatorname{red} y_1, \ldots, \operatorname{red} y_n$.
Možemo pretpostaviti da je $x = x_n$.
Neka je $H = \langle x_1, \ldots, x_{n-1} \rangle$ i $K = \langle x_n \rangle$. Tada je $\operatorname{rang} H = n-1$ jer bi u suprotnom bilo $\operatorname{rang} \mathbb{A} < n$. Dakle, po induktivnoj hipotezi $\mathbb{H}$ je direktna suma (konačna) cikličnih grupa, a takođe i grupa $\mathbb{K}$ je ciklična. Prema tome dosta je da dokažemo da je $\mathbb{A}$ direktna suma grupa $\mathbb{H}$ i $\mathbb{K}$, tj. $\mathbb{A} = \mathbb{H} \dot{+} \mathbb{K}$.
Jedino treba dokazati $H \cap K = \langle 0 \rangle$. PP suprotno, tj. neka je $u \in H \cap K$ i $\operatorname{red} u > 1$.

Tada $u = d_1 x_1 + \dots + d_{n-1} x_{n-1}$ za neke $d_1, \dots, d_{n-1} \in \mathbb{Z}$ jer $u \in \langle x_1, \dots, x_{n-1} \rangle$
$u = d_n x_n$ za neko $d_n \in \mathbb{Z}$, jer $u \in \langle x_n \rangle$.

Neka je $d = (d_1, d_2, \dots, d_{n-1}, d_n)$ i neka su $a_1, \dots, a_n \in \mathbb{Z}$ takvi da je
$d_1 = a_1 d, \dots, d_n = a_n d$
i neka je $v = a_1 x_1 + \dots + a_{n-1} x_{n-1} - a_n x_n$.

Tada $(a_1, \dots, a_n) = 1$, te prema Lemi 2 postoje $v_2, \dots, v_n$ takvi da je $\mathbb{A} = \langle v, v_2, \dots, v_n \rangle$.

S druge strane, $d \cdot v = d_1 x_1 + \dots + d_{n-1} x_{n-1} - d_n x_n = 0$, pa
red $v \le d \le d_n <$ red x_n
što je kontradikcija prema izboru elementa x_n: da je x_n najmanjeg reda u svim generatorskim skupovima od n elemenata grupe $\mathbb{A}$.

Dakle, $\mathbb{H} \cap \mathbb{K} = \langle 0 \rangle$ pa $\mathbb{A} = \mathbb{H} \dot{+} \mathbb{K}$, te je $\mathbb{A}$ konačna direktna suma cikličnih grupa, odnosno $\mathbb{A}$ je izomorfna konačnom proizvodu cikličnih grupa.

Slučaj b: Svaki element u svakom generatorskom skupu od n elemenata grupe $\mathbb{A}$ je beskonačnog reda. U tom slučaju dokazuje se da je $\mathbb{A} \cong \mathbb{Z}^n = (\mathbb{Z}, +, 0)^n$. ▨

Posledica 1 Svaka konačna Abelova grupa izomorfna je (konačnom) proizvodu cikličnih grupa.

Dokaz Ako je $\mathbb{A}$ konačna, onda je i konačno generisana jer $\mathbb{A} = \langle A \rangle$.

Primer Opisati do na izomorfizam sve Abelove grupe reda 100.

Rešenje: $100 = 2^2 \cdot 5^2$, pa uzimajući u obzir prethodnu teoremu, Lagranžeovu teoremu o podgrupama i Teoremu 3c kod cikličnih grupa, nalazimo sledeće Abelove grupe reda 100:
$\mathbb{C}_4 \times \mathbb{C}_{25} = \mathbb{C}_{100}$, $\mathbb{C}_4 \times \mathbb{C}_5^2 = \mathbb{C}_{20} \times \mathbb{C}_5$, $\mathbb{C}_2^2 \times \mathbb{C}_{25} = \mathbb{C}_2 \times \mathbb{C}_{50}$, $\mathbb{C}_2^2 \times \mathbb{C}_5^2 = \mathbb{C}_{10}^2$.

Napomena: $\mathbb{C}_4 \times \mathbb{C}_5^2 \not\cong \mathbb{C}_2^2 \times \mathbb{C}_{25}$ jer, na primer, $\mathbb{C}_2^2 \times \mathbb{C}_{25}$ ima element reda 25, dok grupa $\mathbb{C}_4 \times \mathbb{C}_5^2$ nema element reda 25.
Iz sličnog razloga i ostali parovi navedenih grupa nisu međusobno izomorfne.

Zadatak Opisati do na izomorfizam sve grupe reda 150.

Posledica 2. Neka je A konačna Abelova grupa reda n i neka je p prost broj, $p \mid n$. Tada A ima element reda n.

Dokaz Prema teoremi o dekompoziciji k.g. Abelovih grupa, A je proizvod cikličnih grupa: $A = C_{n_1} \times \dots \times C_{n_k}$. Tada za neki $1 \le i \le k$, $p \mid n_i$. Ako je $C_{n_i} = \langle a \rangle$, tada je $a^{\frac{n_i}{p}}$ element reda p u A. ▨

Posledica 3. Neka je $F = (F, +, \cdot, 0, 1)$ polje i neka je $G < (F \setminus \{0\}, \cdot, 1)$ konačna, tj. G je konačna podgrupa multiplikativne grupe $F^* = (F \setminus \{0\}, \cdot, 1)$ polja F. Tada je G ciklična grupa.

Dokaz Prema teoremi o reprezentaciji k.g. Abelovih grupa, G je kon. proizvod cikličnih grupa. Ako je G nije ciklična, onda postoje ciklične grupe $H, K < G$ t.d. $H \cap K = \langle 1 \rangle$ i redovi ovih grupa nisu uzajamno prosti, tj. $(|H|, |K|) > 1$. Neka je p prost broj t.d. $p \mid (|H|, |K|)$. Tada postoji $a \in H$, $b \in K$ t.d. red $a = p$, red $b = p$ i $\{1, a, \dots, a^{p-1}\} \cap \{1, b, \dots, b^{p-1}\} = \{1\}$, tj. $\langle a \rangle \cap \langle b \rangle = \langle 1 \rangle$. Neka je $S = \{1, a, \dots, a^{p-1}, b, b^2, \dots, b^{p-1}\}$. Tada za $x \in S$, $x^p = 1$, pa jednačina $x^p - 1 = 0$ ima $|S| = 2p-1 > p$ rešenja, suprotno činjenici da polinom stepena p u polju može imati najviše p rešenja. Dakle, G je ciklična. ▨

Posledica 4. Neka je p prost broj. Tada je $\mathbb{Z}_p^* = (\mathbb{Z}_p \setminus \{0\}, \cdot_p, 1)$ ciklična grupa, dakle, $\mathbb{Z}_p^* \cong C_{p-1}$.

Zadatak Neka grupni identitet $u = v$ važi u svim cikličnim grupama. Tada $u = v$ važi u svim Abelovim grupama.

Zadatak. Neka je p prost broj. Dokazati da je Ojlerova grupa $\Phi(p)$ ciklična.

Zadatak Neka je A Abelova grupa reda n i neka $k \mid n$, $k, n \in \mathbb{N}$. Dokazati da A sadrži podgrupu reda k.

Abelove grupe sa deljenjem

Def. Abelova grupa A je grupa sa deljenjem ako za svaki $n \in N^+$ i svaki $a \in A$ jednačina $n \cdot x = a$ ima rešenje (po x).

Primer 1° $(Q, +, 0)$ je Ab. grupa sa deljenjem.

2° $(R, +, 0)$ je Ab. grupa sa deljenjem.

Osobine Abelovih grupa sa deljenjem

1. Homomorfna slika Ab. grupe sa deljenjem je Ab. grupa sa deljenjem.

2. Proizvod dveju Ab. grupa sa deljenjem je Ab. grupa sa deljenjem.

Dokaz. 1. Neka je A Ab. grupa sa deljenjem, $h: A \xrightarrow{na} B$.
Da li je jednačina $n \cdot x = b$, $n \in N^+$, $b \in B$, moguće rešiti u B?
Neka je $a \in A$ t.d. $h(a) = b$ (h je na!), i neka je $d \in A$ t.d. $n \cdot d = a$ (A je Ab. grupa sa deljenjem!). Tada $h(nd) = h(a)$, tj. $n\,h(d) = b$, tj. $h(d)$ je rešenje jedn. $nx = b$.

2. Neka su A, B Ab. grupe sa deljenjem i neka su $(a, b) \in A \times B$.
Neka su $a' \in A$, $b' \in B$ takvi da $n \cdot a' = a$, $n \cdot b' = b$, $n \in N^+$.
Tada je (a', b') rešenje jedn. $n \cdot (x, y) = (a, b)$ u $A \times B$. ☒

Def. Grupa G je bez torzije, ako je svaki $x \in G \setminus \{1\}$ beskonačnog reda.

Teorema Neka je $A = (A, +, 0)$ Ab. grupa sa deljenjem i bez torzije.
Onda je A vektorski prostor nad poljem racionalnih brojeva $Q = (Q, +, \cdot, 0, 1)$.

Dokaz Neka je $\mathcal{A} = (A, Q, \cdot)$ gde je operacija množenja vektora $a \in A$ i skalara $t \in Q$, $t = \frac{p}{q}$, $p, q \in Z$, definisana na sledeći način:

$$b = \frac{p}{q} \cdot a \iff qb = p \cdot a,$$

tj. b je rešenje jednačine $qx = pa$.

Primetimo da je ovako određeno b jedinstveno. Naime, ako je $qb' = pa$, onda $q(b - b') = 0$ pa $b = b'$ jer je A grupa bez torzije. Dakle operacija množenja vektora i skalara je dobro definisana.
Ostalo je da se dokažu sledeće aksiome:

a) $1\cdot x = x$, b) $(\alpha+\beta)x = (\alpha x)+(\beta x)$ c) $\alpha(x+y) = (\alpha\cdot x)+(\alpha\cdot y)$

d) $(\alpha\beta)x = \alpha(\beta x)$.

Dokažimo, na primer, (d): Najpre primetimo da za $n \in Z\setminus\{0\}$ važi

$$nx = ny \Rightarrow x = y, \quad x,y\in A.$$

Dalje, neka je $z = \alpha(\beta x) = \frac{p}{q}\left(\frac{p'}{q'}x\right)$. Tada $qz = py$, gde je $y = \frac{p'}{q'}\cdot x$. Odavde $q'(qz) = q'(py)$, pa $(qq')z = p(q'y) = p(p'x)$ tj. $(qq')z = (pp')x$, odakle $z = \frac{pp'}{qq'}\cdot x = (\alpha\beta)x$ tj:

$$\alpha(\beta x) = (\alpha\beta)x \quad \text{za } \alpha,\beta\in Q,\ x\in A,\ \alpha=\frac{p}{q},\ \beta=\frac{p'}{q'},$$

$p,p'\in Z$, $q,q'\in N^+$. Ovde smo koristili da je za $m,n\in Z$

$$m(nx) = (mn)x,$$

na primer za $m,n\in N^+$: $m(nx) = (mn)x = \underbrace{x+x+\dots+x}_{mn \text{ sabiraka}}$.

Slično se dokazuju identiteti (b) i (c).

Dakle, zaista je $A = (\mathbb{A}, Q, \cdot)$ vektorski prostor. Ako je $\dim A = n$, onda $A \cong Q^n$, tj. ($n\in N^+$):

<u>Teorema</u> Neka je $\dim A = n$. Tada $\mathbb{A} \cong (Q^n,+,0)$, odnosno

$$\mathbb{A} = \mathbb{A}_1 \dot{+} \mathbb{A}_2 \dot{+} \dots \dot{+} \mathbb{A}_n, \text{ gde } \mathbb{A}_i \cong (Q,+,0),\ 1\le i\le n.$$

Važi i opštije, ako je $\dim A = \kappa$, $\kappa\in CARD$, onda

$$\mathbb{A} = \sum_{i\in I} \mathbb{A}_i, \quad |I| = \kappa, \quad \mathbb{A}_i\cong(Q,+,0),\ i\in I.$$

tj. svaka Abelova grupa sa deljenjem i bez torzije, direktna je suma izomorfnih kopija aditivne grupe racionalnih brojeva.

Na primer, $(R,+,0) = \sum_{i\in I} R_i$, $|I| = c = 2^{\aleph_0}$, $\mathbb{R}_i\cong(Q,+,0)$.

<u>Zadatak</u> Navesti primer Abelove grupe sa deljenjem u kojoj su svi elementi konačnog reda.

<u>Zadatak</u> a) Odrediti (opisati) $Aut(Q,+,0)$, b) $Aut(R,+,0)$.

<u>Zadatak</u> Neka je $\mathbb{A}$ Abelova grupa sa deljenjem. Tada je $\mathbb{A}$ beskonačna grupa.

6 Lema 1° Neka su A i B konačne podgrupe grupe G. Tada
$$|AB| = \frac{|A|\cdot|B|}{|A\cap B|}.$$

2° Neka je G grupa i $Z(G)$ centar grupe G, tj.
$Z(G) = \{x \in G \mid (\forall g \in G)\ xg = gx\}$. Tada

a) $H < Z(G) \Rightarrow H \triangleleft G$.

b) $H < Z(G)$ i G/H je ciklična $\Rightarrow$ G je Abelova.

3° Neka je G grupa takva da je $(\forall a \in G)\ a^2 = e$.
Tada je G Abelova.

4° $|G : H| = 2 \Rightarrow H \triangleleft G$. $(H < G)$.

5° Neka je grupa G generisana skupom S i neka je za sve $x, y \in S$, $xy = yx$. Tada je G Abelova.

Dokaz 1°. Neka je $f : A\times B \to AB$ definisano sa
$f : (a,b) \mapsto ab$, $(a,b) \in A\times B$.

Prema teoremi o razlaganju homomorfizma imamo sledeći komutativan dijagram (D)

$$\begin{tikzcd} A\times B \arrow[r, "na"', "f"] \arrow[d, "k"'] & AB \\ A\times B/\sim \arrow[ur, "\cong"'] & \end{tikzcd} \qquad (D)$$

Ovde je $\sim$ jezgro preslikavanja f, tj. relacija ekvivalencije skupa $A\times B$ definisana sa: $(a_1,b_1) \sim (a_2,b_2)$ akko $f(a_1,b_1) = f(a_2,b_2)$.

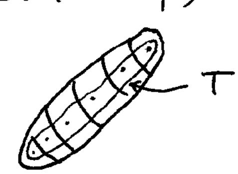
Kako je
$$\begin{aligned}(a_1,b_1) \sim (a_2,b_2) &\Leftrightarrow a_1 b_1 = a_2 b_2 \\ &\Leftrightarrow a_2^{-1}a_1 = b_2 b_1^{-1} \\ &\Leftrightarrow (\exists t \in A\cap B)(a_2^{-1}a_1 = t \wedge b_2 b_1^{-1} = t) \\ &\Leftrightarrow (\exists t \in A\cap B)(a_1 = a_2 t \wedge b_2 = t b_1),\end{aligned}$$

nalazimo $(a,b)/\sim\ = \{(at^{-1}, tb) \mid t \in A\cap B\}$. Odavde

(1) $|(a,b)/\sim| = |A\cap B|$ za proizvoljne $a\in A$, $b \in B$.

$A\times B$ je disjunktna unija klasa ekvivalencija, tj.

(2) $A\times B = \bigcup_{(a,b)\in T} (a,b)/\sim$, T je transverzala (izborni skup) particije $A\times B/\sim$.


T

Transverzala T ima tačno onoliko elemenata koliko ima klasa ekvivalencije, te prema (D), $|T| = |AB|$. Tada iz (2) nalazimo
$$|A|\cdot|B| = |A\times B| = \sum_{(a,b)\in T} (a,b)/\sim\ = |T|\cdot|A\cap B| = |AB|\cdot|A\cap B|. \blacksquare$$

2° a) Neka je $H < Z(G)$. Tada za proizvoljno $g \in G$,
$gH = \{gx \mid x \in H\} = \{xg \mid x \in H\} = Hg$
jer za proizvoljno $x \in Z(G)$, dakle i za $x \in H$, $xg = gx$.

b) Neka je $H < Z(G)$ i pretpostavimo da je G/H ciklička. Primetimo da je prema (a) G/H dobro definisana grupa. Kako je G/H ciklička postoji $a \in G$ tako da je $G/H = \langle aH \rangle$. Ako je G/H konačna ciklička grupa onda $G/H = \{H, aH, a^2H, \dots, a^{n-1}H\}$, gde su a^iH, $0 \le i < n$, disjunktni koseti grupe G i onda $G = H \cup aH \cup \dots \cup a^{n-1}H$. Neka su $x, y \in G$, Tada postoje $0 \le i, j \le n-1$, $h_1, h_2 \in H$ takvi da je $x = a^i h_1$, $y = a^j h_2$. S obzirom da h_1, h_2 komutiraju sa svim elementima grupe G i da je
$a^i \cdot a^j = a^{i+j} = a^{j+i} = a^j \cdot a^i$, nalazimo
$$xy = h_1 a^i h_2 a^j = \dots = h_2 a^j h_1 a^i = y \cdot x.$$
Ako je G/H beskonačna ciklička grupa, onda
$G/H = \{\dots, a^{-2}H, a^{-1}H, H, aH, a^2H, \dots\}$ i
$G = \bigcup_{n \in \mathbb{Z}} a^n H$, i dokaz da je za $x, y \in G$, $xy = yx$, izvodi se na isti način.

3° PP da je za sve $x \in G$, $x^2 = e$, e je jedinica grupe G.
Tada za proizvoljne $a, b \in G$, $(ab)^2 = e$, tj.
$abab = e$, odakle, $abab^2 = eb$ tj. $aba = b$, pa $aba^2 = ba$, tj.
$ab = ba$.

4° Pretpostavimo da je $|G : H| = 2$, $H < G$. Tada
a) za $x \in H$, $xH = Hx = H$.
b) za $x \in G \setminus H$, $xH = G \setminus H = Hx$
U svakom slučaju, za proizvoljno $x \in G$, $xH = Hx$, tj. $H \triangleleft G$.

5° Neka je $G=\langle S\rangle$ i pretpostavimo da je za sve $x,y\in S$, $xy=yx$. Tada:

a) za $x,y\in S$ i $m,n\in N$, važi $x^m y^n = y^n x^m$.
Ovo tvrđenje lako se dokazuje indukcijom po m,n.

b) Iz (a) sledi, množenjem sa x^{-m}, odnosno y^{-n}:

$$x^{-m}y^{n}=y^{n}x^{-m},\quad x^{m}y^{-n}=y^{-n}x^{m},\quad x^{-m}y^{-n}=y^{-n}x^{-m}$$

Dakle, za sve $x,y\in S$, $\alpha,\beta\in Z$

(1) $\quad x^{\alpha}y^{\beta}=y^{\beta}x^{\alpha}$.

Neka su $u,v\in G$. Tada $u,v\in\langle S\rangle$, te postoje $x_1,\dots,x_m\in S$, $\alpha_1,\dots,\alpha_m\in Z$ i $y_1,\dots,y_n\in S$, $\beta_1,\dots,\beta_n\in Z$ takvi da je

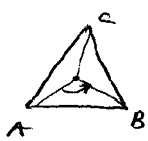
$$u=x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_m^{\alpha_m},\qquad v=y_1^{\beta_1}y_2^{\beta_2}\cdots y_n^{\beta_n}.$$

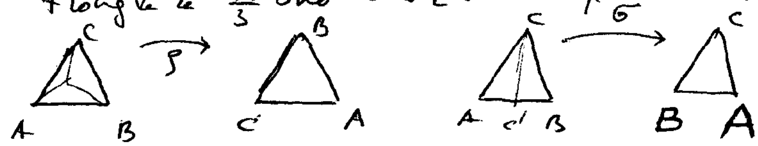
Tada, koristeći (1) nalazimo

$$xy=x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_m^{\alpha_m}y_1^{\beta_1}y_2^{\beta_2}\cdots y_n^{\beta_n}=\dots=y_1^{\beta_1}\cdots y_n^{\beta_n}x_1^{\alpha_1}\cdots x_m^{\alpha_m}=v\cdot u.$$

Primer 1. Postoji tačno jedna grupa (do na izomorfizam) $G=\langle a,b\rangle$ gde su: $red(a)=3$, $red(b)=2$, $ba=a^2b$.

Dokaz Postoji bar jedna takva grupa, to je $S_3\cong D_3$ (S_3 – grupa permutacija skupa $\{1,2,3\}$; D_3 – dijedarska grupa trougla). $D_3=\langle\rho,\sigma\rangle$, ρ = rotacija pravilnog trougla za $\frac{2\pi}{3}$ oko centra simetrije ΔABC.





σ – refleksija u odnosu na osu cc'

Takođe, $S_3=\langle a,b\rangle$, $a=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, $b=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$.

Jedinost: Neka je $G=\langle a,b\rangle$, $a^3=1$, $b^2=1$, $ba=a^2b$, $red(a)=3$, $red(b)=2$.

Kako je $ba^2=a^2ba=a^4b=ab$, to je

(1) $\langle a\rangle\triangleleft G$.

Otuda $G=AB$, gde $A=\langle a\rangle$, $B=\langle b\rangle$, te 4

$$|G|=|AB|=\frac{|A||B|}{|A\cap B|}=\frac{3\cdot 2}{1}=6$$

jer prema Lagrangeovoj teoremi $|A\cap B| \mid |A|, |B|$ tj. $|A\cap B|\mid 2,3$ pa $|A\cap B|=1$. Otuda

(2) $\quad G=\{1,a,a^2,b,ab,a^2b\}$, pa $G\cong S_3$, odnosno $G\cong D_3$

Dejstvo grupe na skup

Algebarska notacija slaganja funkcija:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, dashed, "g\circ f"'] & B \arrow[d, "g"] \\ & C \end{tikzcd} \qquad h = g\circ f, \quad (g\circ f)(x) = g(f(x))$$

skupovna notacija

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, dashed, "fg"'] & B \arrow[d, "g"] \\ & C \end{tikzcd} \qquad h = fg, \quad h(x) = (fg)(x) = g(f(x))$$

algebarska notacija

Neka je G grupa i S neki neprazan skup.

Dejstvo grupe G na skup S je svaki homomorfizam

$$\theta : G \longrightarrow \mathrm{Sym}(S)$$

gde je $\mathrm{Sym}(S) = (\mathrm{Sym}(S), \cdot, i_S)$ simetrična grupa (grupa permutacija) skupa S u algebarskoj notaciji. i_S je identičko preslikavanje skupa S. Dakle,

$\theta(e) = i_S$,

$\theta(gh) = \theta(g)\theta(h)$ za $g, h \in G$; i za $s \in S$;

$\theta(g) : S \xrightarrow[1-1]{na} S$; $\quad (\theta(g)\theta(h))(s) = \theta(h)(\theta(g)(s))$

Relacija ekvivalencije dejstva θ. Uobičajeno je u datom razmatranju dejstvo θ fiksirano, umesto $\theta(g)(s)$ pišemo s^g (ako je grupa data u multiplikativnoj notaciji), odnosno gs (ako je grupa G data u aditivnoj notaciji i, naravno, G je Abelova).

Lema 1 1° $s^e = s$, $\quad 2^\circ$ $(s^g)^h = s^{gh}$.

Dokaz 1° $s^e = \theta(e)(s) = i_S(s) = s$

2° $(s^g)^h = \theta(h)(\theta(g)(s)) = (\theta(g)\theta(h))(s) = \theta(gh)(s) = s^{gh}$.

Stabilizator elementa $s \in S$ (u odnosu na dejstvo θ) je

$G_s = \{ g \in G \mid s^g = s \}$.

Lema 2 $G_s < G$.

Dokaz 1° $e \in G_s$ jer $s^e = s$. 2° Ako $g, h \in G_s$ onda $s^{gh} = (s^g)^h = s^h = s$ pa $gh \in G_s$. Takođe, iz $s^g = s$ sledi $(s^g)^{g^{-1}} = s^{g^{-1}}$ tj. $s^{gg^{-1}} = s^{g^{-1}}$ pa $s^{g^{-1}} = s^e = s$, tj. $g^{-1} \in G_s$.

Relacija ekvivalencije dejstva θ. Neka je relacija $\sim$ skupa S definisana ovako:

$s \sim t$ akko postoji $g \in G$ tako da je $t = s^g$.

Lema 3 Relacija $\sim$ je relacija ekvivalencije skupa S.

Dokaz (R) $s \sim s$ jer $s^e = s$.

(S) PP $s \sim t$. Tada za neki $g \in G$, $t = s^g$, pa $s = t^{g^{-1}}$, tj. $t \sim s$.

(T) PP $s \sim t$, $t \sim u$. Tada za neke $g, h \in G$, $t = s^g$, $u = t^h$ pa

$$u = (s^g)^h = s^{gh} \quad \text{tj. } s \sim u.$$

Klasa ekvivalencije elementa $s \in S$ naziva se orbitom i obeležava se sa s^G. Dakle

$$s/_\sim = s^G = \{ s^g \mid g \in G \}.$$

Lema 4 Neka je $s \in S$. Tada $|s^G| = |G : G_s|$.

Dokaz Primetimo da je $|G : G_s| = |G/G_s|$, gde je $G/G_s = \{ G_s \cdot g \mid g \in G \}$ (Napomena: G/G_s ne mora biti grupa, ovaj skup nasleđuje biće grupa akko $G_s \triangleleft G$).

Dalje, za $g, h \in G$ važi:

$$s^g = s^h \iff s^{gh^{-1}} = s \iff gh^{-1} \in G_s \iff G_s gh^{-1} = G_s$$
$$\iff G_s g = G_s h$$

Dakle, preslikavanje $\Phi : s^G \to G/G_s$ definisano sa

$$\Phi : s^g \mapsto G_s \cdot g$$

je dobro definisano i jeste 1-1. Očigledno Φ je na, pa

$$|s^G| = |G/G_s| = |G : G_s|.$$

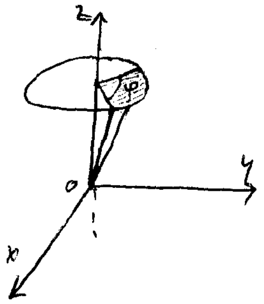
Klasovna jednakost Neka grupa G dejstvuje na skup S. Tada se S može predstaviti kao disjunktna unija orbita

$$S = \bigcup_{s \in T} s^G, \quad T \text{ je transverzala particije } \{ s^G \mid s \in S \}$$

pa $|S| = \sum_{s \in T} |s^G| = \sum_{s \in T} |G : G_s|$, tj.

$$|S| = \sum_{s \in T} |G : G_s| \quad \leftarrow \text{klasovna jednakost}$$

Primer 1. Neka je $G=(R,+,0)$, $S=R^3$.



Neka je za $\varphi\in R$, $\theta(\varphi): R^3\to R^3$ rotacija prostora R^3 oko z-ose za ugao φ.

Tada $\theta(\varphi_1+\varphi_2)=\theta(\varphi_1)\theta(\varphi_2)$, pa je θ dejstvo (očigledno $\theta(0)=i_{R^3}$).

Za $M\in R^3$, $G_M=\{2\pi k\mid k\in Z\}\cong\mathbb{Z}$, dok je orbita tačke M (ako $M\notin z$-osi) $M^G=$ kružnica sa centrom na z-osi; leži u ravni paralelnoj oxy-ravni.

$\ker\theta=\{2\pi k\mid k\in Z\}\cong\mathbb{Z}$.

Primer 2. $G=(R,+,0)$, $S=P(R^3)=\{X\mid X\subseteq R^3\}$

Za $\bar\theta: G\to Sym(S)$, $\bar\theta(X)=\theta[X]$, gde je θ preslikavanje iz prethodnog primera.

Za pogodno izabranu kružnicu $K\in P(R^3)$, orbita kružnice K biće torus (može biti i sfera).

Primer 3 Neka je G grupa, i $\sigma: G\to Sym(G)$ definisano sa $\sigma(g)(x)\overset{def}{=}\sigma_g(x)=g^{-1}xg$, $g,x\in G$. Tada

$\sigma(gh)(x)=(gh)^{-1}xgh=h^{-1}g^{-1}xgh=\sigma_h(\sigma_g(x))=(\sigma_g\sigma_h)(x)$

pa $\sigma(gh)=\sigma_g\sigma_h$ tj. σ je dejstvo grupe G na domen G te grupe. Tada

a) $G_x=\{g\in G\mid x^g=x\}=\{g\in G\mid g^{-1}xg=x\}=\{g\in G\mid xg=gx\}=C(x)$.
tj. stabilizator el. x je njegov centralizator.

b) $x^G=\{x^g\mid g\in G\}=\{y\in G\mid y$ je konjugovan sa $x\}$.

c) $\ker\theta=\{g\in G\mid\theta(g)=i_S\}=\{g\in G\mid(\forall s\in S)\ s^g=s\}$
$=\bigcap_{s\in S}G_s$ tj. za proizvoljno dejstvo $\theta: G\to Sym\,S$

$\ker\theta=\bigcap_{s\in S}G_s$. Specijalno za dejstvo σ

$\ker\sigma=\bigcap_{x\in G}C(x)=Z(G)$. Primetimo da $x\in Z(G)$ akko $C(x)=G$

d) Klasovna jednakost: $|G|=\sum_{x\in T}|G:G_x|=$

$$\sum_{\substack{x\in T\\ x\in Z(G)}}|G:C(x)|+\sum_{\substack{x\in T\\ x\notin Z(G)}}|G:C(x)|=\sum_{x\in Z(G)}1+\sum_{\substack{x\in T\\ x\notin Z(G)}}|G:C(x)|=|Z(G)|+\sum_{\substack{x\in T\\ x\notin Z(G)}}|G:C(x$$

Dakle, klasovna jednakost u ovom slučaju izgleda

$$|G| = |Z(G)| + \sum_{\substack{x\in T \\ x\notin Z(G)}} |G : C(x)| \quad , T \text{ je transverzala dejstva } G.$$

p-grupe

Konačna grupa G je p-grupa, gdje je p prost broj, ako je $red(G) = p^n$ za neki $n \in N^+$. Dakle, svaka grupa reda 8 je p-grupa (za $p=2$), svaka grupa reda 25 je p-grupa (za $p=5$) itd.

Teorema Svaka p-grupa ima netrivijalan centar.

Dokaz Ako $x \notin Z(G)$, onda je $C(x)$ prava podgrupa grupe G, pa je u tom slučaju $|G : C(x)| = p^\alpha$ za neki $\alpha \in N$, jer $|G : C(x)|$ dijeli $red(G) = p^n$. Otuda iz klasovne jednakosti nalazimo

$$|G| = |Z(G)| + \sum_{x\in T,\, x\notin Z(G)} |G : C(x)|$$

$$p^n = |Z(G)| + \lambda \cdot p \text{ , pa } p \mid |Z(G)| \text{ . Dakle}$$

$Z(G) \neq \langle 1 \rangle$, jer $Z(G)$ ima bar p elemenata. ☒

Posljedica Svaka p-grupa ima element reda p.

Dokaz $Z(G) < G$ je Abelova i netrivijalna, pa prema Košijevoj lemi za Abelove grupe, $Z(G)$ ima element a reda p. Naravno, a je element grupe G reda p.

Grupe reda p^2, $p \in$ Prost Postoje dve grupe reda p^2. To su C_{p^2} i $C_p^2 = C_p \times C_p$. Kao što ćemo vidjeti, drugih grupa reda p^2 nema. Neka je $red(G) = p^2$ i neka je $a \in Z(G)$, $red(a) = p$, taj element postoji prema prethodnoj posljedici. Tada $\langle a \rangle \triangleleft G$ te $|G/\langle a\rangle| = p$, pa je $G/\langle a \rangle$ ciklično. Prema 6 lema G je Abelova, tj. G je izomorfna C_{p^2} ili C_p^2. ☒

Sve grupe reda 4: C_4, $C_2^2 = K_4$ (Klajnova četvorna grupa)
9: C_9, $C_3^2 = C_3 \times C_3$.

Silovljeve teoreme

Def. 1. Za proizvoljnu grupu G, $H < G$ je p-podgrupa akko je H p-grupa, p je prost broj.

2. $H < G$ je Silovljeva p-podgrupa akko je H maksimalna p-podgrupa grupe G.

I Silovljeva teorema

Neka je G konačna grupa reda $p^n \cdot m$, $(p, m) = 1$. Tada postoji $H < G$ takva da je $|H| = p^n$.

Dakle, prema prvoj Silovljevoj teoremi i Langranževoj teoremi, ako je $|G| = p^n \cdot m$, $(p, m) = 1$, onda je Silovljeva podgrupa reda p^n. Silovljeve teoreme su strukturne teoreme teorije grupa i omogućavaju kombinatornu analizu strukture konačnih grupa, pre svega nekomutativnih.

Primer Neka je $|G| = 12 = 2^2 \cdot 3$. Tada G sadrži podgrupe H, K, $|H| = 2^2$, $|K| = 3$. Primetimo da je $H \cap K < H, K$ pa kako $(|H|, |K|) = 1$, prema Langranževoj teoremi, $|H \cap K| = 1$. Otuda i prema jednakosti $|HK| \cdot |H \cap K| = |H| \cdot |K|$, sledi $|HK| = 12$, tj. $G = HK$.

Dokaz Prve Silovljeve teoreme Dokaz izvodimo potpunom indukcijom po broju elemenata grupe $|G|$ i pri tome koristimo klasovnu jednakost:

$$(KJ) \qquad |G| = |Z(G)| + \sum_{x \in T,\, x \notin Z(G)} |G : C(x)|$$

Neka je $|G| = p^n \cdot m$, $(p, m) = 1$, $n \geq 1$, $p \in$ Prost i pretpostavimo

(IH) Silovljeva teorema važi za sve grupe $|H|$, $|H| < |G|$.

Razlikujemo dva slučaja:

(1) $p^n \mid |C(x)|$ za neki $x \in T$, $x \notin Z(G)$.

Tada je $C(x)$ prava podgrupa grupe G, dakle $|C(x)| < |G|$, pa prema IH $C(x)$ sadrži Silovljevu podgrupu H reda p^n. Naravno, tada je H Silovljeva podgrupa grupe G.

(2) Ni za jedno $x \in T$, $x \notin Z(G)$, $p^n \mid |C(x)|$ (negacija sl. (1)).
Kako važi $p^n |G| = |C(x)| \cdot |G : C(x)|$, to u ovom slučaju, tj. za $x \in T$, $x \notin Z(G)$, $p \mid |G : C(x)|$, pa
$p \mid \sum_{x \in T, x \notin Z(G)} |G : C(x)|$, te prema (KJ) sledi

$p^n m = |Z(G)| + \alpha p$ za neko $\alpha \in N$.

Otuda $p \mid |Z(G)|$ pa s obzirom da je $Z(G)$ konačna Abelova grupa prema Košijevoj lemi za Abelove grupe, postoji $a \in Z(G)$, $red(a) = p$.
Tada $\langle a \rangle < Z(G)$, pa $\langle a \rangle \lhd G$, te je $G/\langle a \rangle$ dobro definisana grupa i

$$red(G/\langle a \rangle) = |G| / |\langle a \rangle| = p^n \cdot m / p = p^{n-1} m.$$

Prema (IH), $G/\langle a \rangle$ ima Silovljevu podgrupu K reda p^{n-1}.
Neka je $k : G \to G/\langle a \rangle$ kanonski homomorfizam i neka je $H = k^{-1}(K)$. Tada je H Silovljeva podgrupa reda p^n grupe G. Zaista, neka je $K = \{ h_i \langle a \rangle \mid 1 \le i \le p^{n-1} \}$ gde su $h_i \langle a \rangle$ disjunktni koseti podgrupe $\langle a \rangle < G$.

$k : x \mapsto x\langle a \rangle$, $x \in G$

Dalje, $x \in H \Leftrightarrow x \in k^{-1}(K)$
$\Leftrightarrow k(x) \in K$
$\Leftrightarrow x\langle a \rangle = h_i \langle a \rangle$ za neki i
$\Leftrightarrow h_i^{-1} x \in \langle a \rangle$ za neki i
$\Leftrightarrow h_i^{-1} x = a^j$ za neke i, j
$\Leftrightarrow x = h_i a^j$ za neke i, j, tj.

$H = \bigcup_{1 \le i \le p^{n-1}} h_i \langle a \rangle$ i to je disjunktna unija, pa

$$|H| = \sum_{1 \le i \le p^{n-1}} |h_i \langle a \rangle| = \sum_{1 \le i \le p^{n-1}} |\langle a \rangle| = p^{n-1} \cdot |\langle a \rangle| = p^{n-1} \cdot p = p^n,$$

gde smo koristili činjenicu da svaki koset $h_i \langle a \rangle$ ima isti broj elemenata kao i podgrupa $\langle a \rangle$, tj. p.
Dakle, H je Silovljeva p-podgrupa grupe G reda p^n ▨

Primer 1. Opisati grupe reda 6.

Rešenje: Postoje bar dve međusobno neizomorfne grupe reda 6, to su $\mathbb{C}_6 = \mathbb{C}_2 \times \mathbb{C}_3$ i $\mathbb{S}_3 = \mathbb{D}_3$.

Dokažimo da je svaka grupa reda 6 izomorfna jednoj od ove dve grupe. Neka je G grupa reda 6. Prema Prvoj Silovljevoj teoremi, postoje $a, b \in G$, $red(a) = 2$, $red(b) = 3$. Kako je $|G : \langle b \rangle| = 6 : 3 = 2$, to je $\langle b \rangle \triangleleft G$, pa

$ab = b^i a$, $i \in \{0, 1, 2\}$. Tada $i \neq 0$ (jer inače $b = 1$, #),

pa (1) $ab = ba$ ili (2) $ab = b^2 a$.

Dalje $|\langle a \rangle \langle b \rangle| \cdot |\langle a \rangle \cap \langle b \rangle| = |\langle a \rangle| \cdot |\langle b \rangle|$, pa $|\langle a \rangle \langle b \rangle| = 6$, odakle $G = \langle a \rangle \langle b \rangle$ tj. G je generisana elementima a, b. Otuda u slučaju (1), G je Abelova, dok je u slučaju (2) $G \cong \mathbb{S}_3$ (vidi zadatak na ovu temu).

Primer 2. Opisati sve grupe reda $2p$, p je prost broj.

Rešenje (1) $p = 2$, tada $G \cong \mathbb{C}_4$ ili $G \cong \mathbb{C}_2^2$.

(2) Neka je $p > 2$. Tada imamo bar dve međusobno neizomorfne grupe reda $2p$, to su $\mathbb{C}_{2p} = \mathbb{C}_2 \times \mathbb{C}_p$ i $\mathbb{D}_p$.

Svaka grupa reda $2p$ izomorfna je jednoj od ovih dveju grupa. Zaista, neka je G grupa reda $2p$ i neka su $a, b \in G$, $red(a) = 2$, $red(b) = p$. Tada

(a) $G = \langle a \rangle \langle b \rangle$ prema jednakosti $|\langle a \rangle \langle b \rangle| \cdot |\langle a \rangle \cap \langle b \rangle| = |\langle a \rangle| \cdot |\langle b \rangle|$

(b) $\langle b \rangle \triangleleft G$ jer $|G : \langle b \rangle| = 2$.

Otuda $ab = b^i a$ za neko $i \in \{1, 2, \ldots, p-1\}$, tj. $\sigma_a(b) = b^i$,

pa $b = i(b) = \sigma_{a^2}(b) = \sigma_a^2(b) = \sigma_a(b^i) = (b^i)^i = b^{i^2}$, tj.

$i^2 = 1 \mod p$, odakle je $i \in \{1, -1\}$ (jer je $\mathbb{Z}_p$ polje!).

Slučaj $i = 1$: $ab = ba$, tj. G je Abelova pa $G \cong \mathbb{C}_{2p}$.

Slučaj $i = -1$: $ab = b^{-1} a = b^{p-1} a$, tj. $G \cong \mathbb{D}_p = \langle \rho, \sigma \rangle$ ∎

Dakle, grupe reda 10: $\mathbb{C}_{10}$, $\mathbb{D}_5$ i grupe reda 14: $\mathbb{C}_{14}$, $\mathbb{D}_7$.

U daljem izlaganju Silovljevih teorema koristićemo sledeću notaciju i terminologiju.

Neka je σ_x unutrašnji automorfizam grupe G, za $a \in G$ i $H \subseteq G$ umesto $\sigma_x(a)$ i $\sigma_x(H)$ koristićemo oznake a^x, odnosno H^x. Dakle, $a^x = x^{-1}ax$, $H^x = x^{-1}Hx$. Primetimo da je, s obzirom da je $\sigma_x \in Aut(G)$, za $H < G$ takođe $H^x < G$ i $|H^x| = |H|$.

Ako je $H \subseteq G$, $N(H) \overset{def}{=} \{x \in G \mid H^x = H\}$ i $N(H)$ nazivamo <u>normalizatorom</u> skupa H. Lako se proverava da je

<u>Lema 1.</u> $N(H) < G$.

Ako je H Silovljeva p-podgrupa grupe G, pisaćemo kraće da je H S_p-podgrupa grupe G. Tada s_p označava broj svih S_p-podgrupa grupe G. Ako je $Q < G$ i $red(Q)$ je stepen prostog broja p, rećićemo da je Q p-podgrupa grupe G.
Do daljeg pretpostavljamo da je G konačna grupa.

<u>Lema 2</u> Neka Q p-podgrupa grupe G i P S_p-podgrupa grupe G, p je prost broj. Ako $Q < N(P)$ tada $Q < P$.

<u>Dokaz</u> Prema poznatoj jednakosti

$$|QP| \cdot |Q \cap P| = |P| \cdot |Q|$$

i kako su $|Q \cap P|, |P|, |Q|$ stepeni prostog broja p (jer $Q \cap P < P$) to je $|QP| = p^{\alpha}$ za neki $\alpha \in N$. Dokažimo da je $QP < G$.
Kako je $Q < N(P)$, to $QP = \bigcup_{x \in Q} xP = \bigcup_{x \in Q} Px = PQ$, pa

- $(QP)^{-1} = P^{-1}Q^{-1} = PQ = QP$
- $(QP)(QP) = Q(PQ)P = Q(QP)P = (QQ)(PP) = QP$

pa $QP < G$. Primetimo da je $P < QP$. Dakle QP je p-podgrupa koja sadrži S_p-podgrupu P. Zbog maksimalnosti S_p podgrupe u skupu p-podgrupa grupe G, sledi $QP = P$, odakle $Q < P$ ▣

Neka je G konačna grupa, $|G| = mp^n$, $(m,p)=1$, p je prost.

<u>II Silovljeva teorema</u> 1. Ako je Q p-podgrupa grupe G, onda je Q sadržana u nekoj S_p-podgrupi grupe G.

2. Svake dve S_p-podgrupe su konjugovane, tj. ako su P, Q S_p-podgrupe grupe G, onda postoji $x \in G$ tako da $Q = P^x$.

<u>III Silovljeva teorema</u> 1. $s_p = 1 \pmod p$

2. $s_p = |G : N(P)|$, P je S_p-podgrupa grupe G.

3. $s_p \,\big|\, |G|$.

<u>Dokaz</u> Odjednom dokazujemo obe teoreme. Neka je ~~$A \leq G$~~

$S = \{ P^x \mid x \in G \}$ gde je P neka S_p-podgrupa grupe G.

Primetimo da je P^x S_p-pgrupa grupe G.

Neka je $\theta : G \longrightarrow Sym(S)$, gde je $\theta(g)(s) = s^x$, $g \in G$, $s \in S$, tj: $\theta(g)(P^x) = P^{xg}$. Tada je θ dejstvo grupe G na S. Zaista,

$\theta(e)(s) = s^e = s$; $\quad \theta(g_1 g_2)(s) = s^{g_1 g_2} = (s^{g_1})^{g_2} = \theta(g_2)(\theta(g_1)(s))$
$= (\theta(g_1)\theta(g_2))(s)$, tj.

$\theta(e) = i_S$, $\quad \theta(g_1 g_2) = \theta(g_1)\theta(g_2)$; pa je θ homomorfizam grupe G na skup S. Dalje za $s \in S$, orbita elementa s je

$s^G = \{ s^g \mid g \in G \} = \{ P^{xg} \mid g \in G \} = \{ P^x \mid x \in G \} = S$, tj.

(1) $s^G = S$.

Dakle pri ovom dejstvu postoji samo jedna orbita, neka je to orbita za P. Stabilizator el. $s \in S$ je

$G_s = \{ x \in G \mid s^x = s \} = N(s)$, tj.

(2) $G_s = N(s)$.

Klasovna jednakost dejstva glasi $|S| = \sum_{s \in T} |G : G_s|$, ali s obzirom da postoji samo jedna orbita i prema (2), sledi

(3) $|S| = |G : N(P)|$.

Cilj nam je da dokažemo da je $S = \{ Q \mid Q \text{ je } S_p\text{-podgrupa grupe } G \}$.

Neka je Q podgrupa grupe G i neka je $\theta_0 = \theta | Q$, tj. θ_0 je restrikcija dejstva θ na $Q < G$. Odmah vidimo da je θ_0 dejstvo grupe Q na skup S. Tada za $s \in S$

(4) θ_0-orbita elementa s : $s^Q = \{ s^g \mid g \in Q \}$

(5) θ_0-stabilizator elementa s : $Q_s = \{ g \in Q \mid s^g = s \}$

Kada je θ_0-orbita s^Q jednočlan skup? Kako $s \in s^Q$, to

$$s^Q = \{s\} \iff \{ s^g \mid g \in Q \} = \{s\}$$
$$\iff \text{Za sve } g \in Q,\ s^g = s$$
$$\iff Q < N(s).$$

Specijalno,

(6) $P^Q = \{P\} \iff Q < N(P)$ (P je neka S_p-pgrupa grupe G).

Te prema Lemi 2 (st-4) sledi

(7) $P^Q = \{P\} \iff Q < \underline{P}$.

Prema klasovnoj jednakosti za dejstvo θ_0 imamo

(8) $$|S| = \sum_{s \in T} |s^Q| = \sum_{\substack{s \in T \\ |s^Q| = 1}} 1 + \sum_{\substack{s \in T \\ |s^Q| \neq 1}} |Q : Q_s|$$

Setimo se da je $|s^Q| = |Q : Q_s|$

Kako $|Q : Q_s|$ deli $|Q|$ i $|Q|$ je stepen broja p, i za $|s^Q| \neq 1$, $Q_s \subsetneq Q$, to prema (7) i (8) imamo

(9) $$|S| = \sum_{\substack{s \in T \\ Q < s}} 1 + \alpha \cdot p \quad \text{za neki } \alpha \in N.$$

Ako je $Q = P$, onda, naravno, jedina S_p-podgrupa koja sadrži Q je ona sama, tj. P, dakle $\sum_{\substack{s \in T \\ Q < s}} 1 = 1$, pa prema (9)

(10) $|S| = 1 + \lambda p$ za neki $\lambda \in N$, tj. iz (9) i (10), ali za proizvoljnu p-podgrupu Q grupe G imamo

(11) $$\sum_{s \in T,\, Q < s} 1 = 1 \mod p.$$

Iz (11) sledi

(a) Postoji $s \in S$ tako da je $Q < s$, tj. postoji $x \in G$ t.d. $Q < P^x$, tj. Q je sadržana u nekoj S_p-podgrupi grupe G.

(b) Ako je Q S_p-pgra grupe G onda $Q < P^x$ za neko $x \in G$ ali tada $|Q| = |P^x| = p^n$, pa $Q = P^x$, tj. svake dve S_p-pgre grupe G su konjugovane, pa

(c) $S = \{ P \mid P$ je S_p-pgra grupe $G \}$, tj. $s_p = |S|$.
Prema (3) onda

(d) $s_p = |G : N(P)|$, odakle i

(e) $s_p \mid |G|$.
Prema (10)

(f) $s_p \equiv 1 \pmod p$. ∎

<u>Primer 1.</u> <u>Opis svih grupa reda 15.</u> Postoji bar jedna grupa reda 15, to je $C_{15} = C_5 \times C_3$. Dokažimo da drugih nema.
Neka je $|G| = 15 = 3 \cdot 5$ i neka su P, Q redom S_3, S_5 - pgre grupe G. Tada $|P| = 3$ i $|Q| = 5$, pa su obe ove grupe cikličke, tj. postoje $a \in P$, $b \in Q$ t.d. $P = \langle a \rangle$, $Q = \langle b \rangle$, $red(a) = 3$, $red(b) = 5$. Dalje $P \cap Q < P, Q$ pa $|P \cap Q| \mid 3, 5$ tj. $|P \cap Q| = 1$, pa $P \cap Q = \langle 1 \rangle$.
Otuda $|PQ| = |P| \cdot |Q| / |P \cap Q| = 3 \cdot 5 / 1 = 15$ pa

(1) $G = PQ$, $P \cap Q = \langle 1 \rangle$
Dalje, $s_3 \equiv 1 \bmod 3$, $s_5 \equiv 1 \bmod 5$ i $s_3, s_5 \mid 15$ odakle

(2) $s_3 = 1$, $s_5 = 1$.
Otuda za sve $x \in G$ $P^x = P$, $Q^x = Q$ tj.

(3) $P, Q \triangleleft G$.
Iz (1) i (3) sledi da je G unutrašnji proizvod podgrupa $P \cong C_3$, $Q \cong C_5$ pa $G \cong P \times Q \cong C_3 \times C_5 \cong C_{15}$. ∎

Zadatak Neka je θ dejstvo iz dokaza II i III Silovljeve teoreme. Dokazati da je $\ker\theta = \mathrm{core}(N(P))$, gde je P bilo koja S_p-grupa grupe G.

Zadatak Neka je $Q \lhd G$ p-podgrupa grupe G. Tada je Q sadržana u svakoj S_p-podgrupi grupe G.

Opis grupa reda $2p$, p je prost broj:

$p=2$ Tada postoje tačno dve grupe: C_4, C_2^2

$p \geq 3$ Tada postoje tačno dve grupe $C_{2p} = C_2 \times C_p$ i D_p.

Jedinost: Ako je $|G| = 2p$ neka su $P = \langle a \rangle$, $Q = \langle b \rangle$ redom S_2, S_p podgrupe grupe G. Tada $|Q| = p$ pa $|G:Q| = 2$ tj. $Q \lhd G$. Odatle $b^a \in \langle b \rangle$ tj. $b^a = b^i$ za neki i, $1 \leq i \leq p-1$. Tada $b = b^e = b^{a^2} = (b^a)^a = (b^i)^a = (b^a)^i = (b^i)^i = b^{i^2}$ pa $i^2 \equiv 1 \bmod p$, odakle $i \in \{1, -1\}$, pa imamo dva slučaja:

a) $i = 1$, i tada $G \cong C_2 \times C_p$ jer $ab = ba$

b) $i = -1$, i tada $G \cong D_p$ jer $ab = b^{-1}a$

Primetimo da je $G = \langle a, b \rangle = PQ$ (vidi opis grupa reda 15).

Dakle, jedine grupe reda 10 su C_{10} i D_5, i grupe reda 14 su C_{14} i D_7.

Zadatak Opisati grupe reda 1001. Postoji tačno jedna grupa reda 1001.

Jedinost: Neka je $|G| = 1001 = 7 \cdot 11 \cdot 13$ i neka su P, Q, R redom S_7, S_{11}, S_{13} podgrupe grupe G. Tada $s_7 \equiv 1 (\bmod 7)$, $s_{11} \equiv 1 (\bmod 11)$ i $s_{13} \equiv 1 \bmod 13$ i $s_7, s_{11}, s_{13} \mid 1001$. Neka $a \mid 1001$. Tada za $a < 1001$ $a-1 \in \{0, 6, 10, 12, 76, 90, 142\}$ i $7, 11, 13$ jedino dele 0 iz ovog skupa, pa $s_7 = 1$, $s_{11} = 1$, $s_{13} = 1$, pa $P, Q, R \lhd G$, da je G unutrašnji proizvod podgrupa P, Q, R, tj. $G \cong P \times Q \times R \cong C_7 \times C_{11} \times C_{13} = C_{1001}$.

ALGEBARSKA POLJA

1. Definicija polja i osnovna svojstva

Def. 1.1. Algebarsko polje je svaka algebra vida $\mathbb{F} = (F, +, \cdot, 0, 1)$ gde je $(F, +, 0)$ Abelova grupa, $(F \setminus \{0\}, \cdot, 1)$ takođe je Abelova grupa, $\mathbb{F}$ zadovoljava distributivni zakon i $0 \neq 1$.

Dakle, polje $\mathbb{F}$ zadovoljava sledeće aksiome:

a. $(x+y)+z = x+(y+z)$
$x+y = y+x$
$x+0 = x$
$\forall x \exists y \ (x+y=0)$

b. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
$x \cdot y = y \cdot x$
$x \cdot 1 = x$
$\forall x \ (x \neq 0 \Rightarrow \exists y \ (x \cdot y = 1))$

c. $x \cdot (y+z) = x \cdot y + x \cdot z$

d. $0 \neq 1$.

1.2. U polju $\mathbb{F}$ važi: a. $\forall x \exists_1 y \ (x+y=0)$ b. $\forall x (x \neq 0 \Rightarrow \exists_1 y \ (x \cdot y = 1))$

Dokažimo na primer (a): Neka su y, y' takvi da je $x+y=0$, $x+y'=0$. Tada, koristeći aksiome polja, važi sledeći niz jednakosti:
$y' + (x+y) = y' + 0$, $(y'+x)+y = y'$, $(x+y')+y = y'$, $0+y = y'$, $y = y'$,
te je ovim (a) dokazano. Svojstvo (b) dokazuje se na sličan način. Dakle, za svaki $x \in F$ postoji tačno jedan $y \in F$ tako da je $x+y=0$. Odatle u $\mathbb{F}$ možemo uvesti dve funkcije pomoću sledećih definicionih aksioma:

a. $y = -x \Leftrightarrow x+y=0$, b. $y = x^{-1} \Leftrightarrow x \cdot y = 1$, $x \neq 0$.

Obično se uzima da je 0^{-1} nedefinisana vrednost, ali po potrebi možemo uzeti za 0^{-1} bilo koju vrednost, na primer $0^{-1} = 0$.
Prema tome $x + (-x) = 0$, $x \neq 0 \Rightarrow x \cdot x^{-1} = 1$.

1.3. U polju $\mathbb{F}$ važi:

a. $a \cdot 0 = 0 = 0 \cdot a$, b. $(-1)a = -a$, c. $ab = 0 \Rightarrow (a=0 \vee b=0)$

Ako je $b \neq 0$, definišemo $a/b = ab^{-1}$. U tom slučaju imamo

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \quad b, d \neq 0.$$

Dokažimo, na primer, (a): $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$, odakle $a \cdot 0 = 0$.

Neka je $N = \{0, 1, 2, \dots\}$ skup prirodnih brojeva i $Z = \{\dots, -2, -1, 0, 1, 2, \dots\}$ skup celih brojeva. U $\mathbb{F}$ definišemo stepenu funkciju x^n, $n \in N$, induktivno na sledeći način: $x^0 = 1$, $x^{n+1} = x^n \cdot x$. Ako je α negativan ceo broj, tj. $\alpha = -n$, $n \in N$ i $x \neq 0$, onda $x^\alpha \overset{def}{=} (x^{-1})^n$. Tada važe uobičajeni identiteti: a. $x^{m+n} = x^m \cdot x^n$, $(x^m)^n = x^{mn}$, $x \in F$, $m, n \in N$,
b. $x^{\alpha+\beta} = x^\alpha \cdot x^\beta$, $(x^\alpha)^\beta = x^{\alpha\beta}$, $x \in F \setminus \{0\}$, $\alpha, \beta \in Z$, c. $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$, $n \in N$.

2. Primeri polja

a. $\mathbb{Q} = (Q, +, \cdot, 0, 1)$ - polje racionalnih brojeva

b. $\mathbb{R} = (R, +, \cdot, 0, 1)$ - polje realnih brojeva

c. $\mathbb{C} = (C, +, \cdot, 0, 1)$ - polje kompleksnih brojeva

d. $\mathbb{Z}_p$ - polje ostataka po modulu prostog broja p.
Ovde $\mathbb{Z}_p = (Z_p, +_p, \cdot_p, 0, 1)$, gde su $+_p, \cdot_p$ operacije sabiranja i množenja po modulu p. Na primer, $2 +_5 4 = 1$, $2 \cdot_5 4 = 3$.
Podsetimo se da je $x +_p y = rest(x+y, p)$, $x \cdot_p y = rest(xy, p)$, gde je $rest(x, n)$ funkcija ostatka:
$r = rest(x, n) \overset{def}{\Longleftrightarrow} \exists q\, (x = qn + r \wedge 0 \le r < n)$, $r, x \in Z$, $n \in N^+$.
Primetimo da je $rest(x, n) \in \{0, 1, \ldots, n-1\}$, $n \in N^+$. Skup $\{0, 1, \ldots, n-1\}$ označavamo sa Z_n.
Dokažimo da je $\mathbb{Z}_p$ polje: 1° $\mathbb{Z}_p$ je komutativan prsten s obzirom da je $\mathbb{Z}_p$ homomorfna slika prstena $\mathbb{Z}$. Naime za $\rho_p(x) = rest(x, p)$ $\rho_p : \mathbb{Z} \xrightarrow{na} \mathbb{Z}_p$. 2° Neka je $a \in Z_p \setminus \{0\}$. Tada $(a, p) = 1$, pa prema Bezuovoj teoremi postoje $x, y \in Z$ takvi da je $ax + py = 1$.
Tada $\rho_p(ax + py) = \rho_p(1)$, tj. $a \cdot_p \rho_p(x) = 1$, te je $\rho_p(x) = a^{-1}$ u $\mathbb{Z}_p$.

e. <u>Polje od četiri elementa:</u> Neka je $F = \{0, 1, a, b\}$ i neka su operacije $+$ i $\cdot$ definisane tablicama:

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

·	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

Tada je $\mathbb{F} = (F, +, \cdot, 0, 1)$ polje.
Primetimo da u $\mathbb{F}$ važi $2 \cdot x = 0$ i da jednačina $x^2 + x + 1 = 0$ ima rešenja a, b, dakle $x^2 + x + 1 = (x-a)(x-b)$.
Takođe, $\mathbb{Z}_2 \subseteq \mathbb{F}$.

2.1. <u>Zadatak</u> Konstruisati polje: a) od 9 elemenata b) od 8 elemenata.

2.2. <u>Definicija</u> Multiplikativni deo polja $\mathbb{F}$ je grupa $(F \setminus \{0\}, \cdot, 1)$. Ovu grupu označavamo sa $\mathbb{F}^*$. Dakle, $\mathbb{F}^* = (F \setminus \{0\}, \cdot, 1)$.

2.3. <u>Teorema</u> Neka je $\mathbb{F}$ polje i neka je G konačna podgrupa grupe $\mathbb{F}^*$. Tada je G ciklična grupa.

<u>Dokaz</u> Prema teoremi o razlaganju konačno generisanih Abelovih grupa, G je unutrašnji proizvod cikličnih grupa. Ako G nije ciklična onda postoje ciklične podgrupe $C_m, C_n < G$ i $A < G$, $m, n > 1$ takve da je

$G = C_m C_n A$ i $C_m \cap C_n = \langle 1 \rangle$ i prost broj p tako da $p \mid m, n$. Prema Košijevoj lemi postoje $a \in C_m$, $b \in C_n$, $red(a) = red(b) = p$. Tada su $1, a, \dots, a^{p-1}, b, b^2, \dots, b^{p-1}$ rešenja jednačine $x^p - 1$, pa polinom $x^p - 1 = 0$ ima $1 + 2(p-1) > p$ rešenja, što je kontradikcija. S obzirom na teoremu o cikličnim grupama: ako $(m, n) = 1$, onda $C_m \times C_n \cong C_{mn}$, sledi da je G ciklična. ∎

2.4. Posledica $\mathbb{Z}_p^* \cong C_{p-1}$ $(p \in Prost)$.

2.5. Zadatak Konstruisati izomorfizam $f : (\mathbb{Z}_{p-1}, +, 0) \cong \mathbb{Z}_p^*$.

2.6. Mala Fermaova teorema $n^p \equiv n \pmod p$, $n \in N$, $p \in Prost$.

Dokaz Kako u $\mathbb{Z}_p$ važi $x^{p-1} = 1$ za $x \neq 0$, to je $x^p = x$ za sve $x \in \mathbb{Z}_p$. Neka je $n \in N$, i $x = \rho_p(n) \equiv rest(n, p)$. Tada $\rho_p(n)^p = \rho_p(n)$ pa kako je $\rho_p : \mathbb{Z} \to \mathbb{Z}_p$ homomorfizam, to $\rho_p(n^p) = \rho_p(n)$ tj. $n^p \equiv n \pmod p$. ∎

Posledica $(n, p) = 1 \Rightarrow n^{p-1} \equiv 1 \bmod p$.

2.7. Vilsonova teorema Ako je $p \in Prost$, onda $(p-1)! \equiv -1 \bmod p$.

Dokaz Kako u $\mathbb{Z}_p$ važi $x^{p-1} = 1$ za $x \in \{1, \dots, p-1\}$ to su $1, 2, \dots, p-1$ koreni polinoma $x^{p-1} - 1$. Kako je $x^{p-1} - 1$ polinom stepena $p-1$, to važi faktorizacija u $\mathbb{Z}_p$:

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1)).$$

Kako je u $\mathbb{Z}_p$, $p = 0$, uzimajući $x = p$, nalazimo u $\mathbb{Z}_p$

$$(p-1) \cdot_p (p-2) \cdot_p \cdots \cdot_p 1 = -1$$

∎

pa $\rho_p((p-1)(p-2)\cdots 1) = \rho_p(-1)$, odakle $(p-1)! \equiv -1 \pmod p$.

2.8 Zadatak Neka je $n \in N^+$. Dokazati: ako je $(n-1)! \equiv -1 \pmod n$, onda je n prost broj.

2.9. Zadatak. Neka je p prost broj. Dokazati da je $(p-2)! \equiv 1 \bmod p$.

2.10 Zadatak Neka je $\mathbb{F}$ polje. Dokazati: ako je $\mathbb{F}^*$ ciklična grupa, tada je $\mathbb{F}$ konačno (tj. $\mathbb{F}^* \not\cong (\mathbb{Z}, +, 0)$).

3. <u>Karakteristika polja</u>. Polje F je <u>beskonačne karakteristike</u> ako za sve $n \in N^+$ sve $x \in F \setminus \{0\}$, $n \cdot x \neq 0$. Bude, $n \cdot x \stackrel{def}{=} \underbrace{x + x + \dots + x}_{n}$. Polje $\mathbb{F}$ je <u>konačne karakteristike</u> ako nije beskonačne karakteristike.

3.1. <u>Primer</u> 1° Brojevna polja, tj. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ su beskonačne karakteristike. Za polja beskonačne karakteristike koristi se i termin "polja karakteristike 0".
2° $\mathbb{Z}_p$ je polje konačne karakteristike. Dakle,
Neka je $\mathbb{F}$ polje konačne karakteristike.
$S = \{n \in N^+ \mid$ postoji $x \in F \setminus \{0\}$, $n \cdot x = 0\}$ je neprazan.
Prema principu najmanjeg broja za prirodne brojeve, S sadrži najmanji prirodni broj n_0. Tada je n_0 prost broj. Pretpostavimo suprotno da je $n_0 = k \cdot m$, $1 < k, m$, $k, m \in N$. Kako je za neki $x \in F \setminus \{0\}$ $n_0 \cdot x = 0$, to $(k \cdot m) \cdot x = 0$, tj. $(k \cdot 1)(m \cdot x) = 0$, odakle $k \cdot 1 = 0$ ili $m \cdot x = 0$, suprotno izboru broja n_0.
Broj n_0 nazivamo <u>karakteristikom</u> polja $\mathbb{F}$ i obeležavamo ga sa $k\mathbb{F}$. S obzirom da je $k\mathbb{F}$ prost broj, u tom slučaju kažemo da je $\mathbb{F}$ <u>proste karakteristike</u>.

3.2. Neka je $p = k\mathbb{F}$. Tada za sve $x \in F$, $p \cdot x = 0$.

<u>Dokaz</u> Za neki $a \in F \setminus \{0\}$, $p \cdot a = 0$, pa $(pa)a^{-1}x = 0$, tj. $p \cdot x = 0$.

3.3. <u>Teorema</u> 1° Polje $\mathbb{F}$ je beskonačne karakteristike akko $\mathbb{F}$ sadrži izomorfnu kopiju polja racionalnih brojeva.
2° Polje $\mathbb{F}$ je proste karakteristike akko $\mathbb{F}$ sadrži izomorfnu kopiju polja $\mathbb{Z}_p$.

<u>Dokaz</u> 1° Neka je $\mathbb{F}$ polje beskonačne karakteristike.
Tada $h : \mathbb{Q} \to \mathbb{F}$ definisano sa $h(\frac{m}{n}) = (m \cdot 1_F) \cdot (n \cdot 1_F)^{-1}$ jeste utapanje polja $\mathbb{Q}$ u $\mathbb{F}$ i $h\mathbb{Q} \subseteq \mathbb{F}$, $h\mathbb{Q} \cong \mathbb{Q}$.
2° Neka je $\mathbb{F}$ polje karakteristike p. Tada $h : \mathbb{Z}_p \to \mathbb{F}$ gde $h(x) = x \cdot 1_F$, $x \in \mathbb{Z}_p$.

4. Homomorfizmi polja. Neka su $\mathbb{F}$ i $\mathbb{E}$ polja. Preslikavanje $h : F \to E$ je homomorfizam polja $\mathbb{F}$ u polje $\mathbb{E}$, što zapisujemo $h : \mathbb{F} \to \mathbb{E}$, ako $h(0)=0$, $h(1)=1$, $h(x +_F y) = h(x) +_E h(y)$, $h(x \cdot_F y) = h(x) \cdot_E h(y)$.

4.1. Zadatak Neka je $h : \mathbb{F} \to \mathbb{E}$. Tada je h monomorfizam

4.2. Teorema Neka je $\mathbb{F}$ polje karakteristike p. Tada je $h(x) = x^p$ homomorfizam.

Dokaz 1° $h(xy) = (xy)^p = x^p y^p = h(x)\,h(y)$.

2° $h(x+y) = (x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \dots + \binom{p}{p-1} x y^{p-1} + y^p$.

Kako je za prost broj p, $p \mid \binom{p}{i}$, $1 \le i \le p-1$, pa $\binom{p}{i} = p \cdot k_i$, $k_i \in N$. Odatle $\binom{p}{i} a = (p \cdot k_i) a = p(k_i a) = 0$. ∎

Dakle, $(x+y)^p = x^p + y^p = h(x) + h(y)$.

Napomena Prema 4.1, sledi da je $x \mapsto x^p$, $x \in F$, utapanje. Odatle, prema Dirihleovom principu, ako je $\mathbb{F}$ konačno polje, onda je h i na, tj. h je automorfizam polja $\mathbb{F}$.

4.3. Definicija $h : \mathbb{F} \to \mathbb{F}$ je automorfizam ako je h 1-1 i na. Skup svih automorfizama polja $\mathbb{F}$ označava se sa $\mathrm{Aut}\,\mathbb{F}$.

4.4. $\mathbb{A}\mathrm{ut}\,\mathbb{F} = (\mathrm{Aut}\,\mathbb{F}, \circ, i_F)$ je grupa.

4.5 Zadatak Odrediti $\mathrm{Aut}\,\mathbb{Q}(\sqrt{2})$.

4.6. Zadatak Neka je f neprekidno rešenje Košijeve funkcionalne jednačine $h(x+y) = h(x) + h(y)$. Dokazati da tada postoji $a \in R$ tako da je $f(x) = ax$.

4.7.** Ako se uslov neprekidnosti sa ograničenošću ili merljivošću funkcije f, tada je isto $f(x) = ax$ za neki $a \in R$.

4.8. Dokazati da je $\mathrm{Aut}(\mathbb{R}) = \{i_R\}$.
Uputstvo Najpre dokažite da je $f \in \mathrm{Aut}(R)$ neprekidna funkcija, pa onda iskoristite 4.6.

5. Podpolje i ekstenzija polja

Neka su $\mathbb{F}$ i $\mathbb{E}$ polja. $\mathbb{F}$ je *podpolje* polja $\mathbb{E}$, odnosno $\mathbb{E}$ je *ekstenzija* polja $\mathbb{F}$ ako je $\mathbb{F}$ podalgebra polja $\mathbb{E}$.

Da je $\mathbb{F}$ podpolje polja $\mathbb{E}$, zapisujemo $\mathbb{F} \subseteq \mathbb{E}$.

Dakle, ako $\mathbb{F} \subseteq \mathbb{E}$ onda $0_F = 0_E$, $1_F = 1_E$, $x +_F y = x +_E y$, $x \cdot_F y = x \cdot_E y$, $x, y \in F$.

5.1 *Primer* $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. Svako podpolje polja $\mathbb{C}$ naziva se *brojevnim poljem*. Dakle $\mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\}$ je brojevno polje.

5.2. *Napomena* Svako podpolje jedinstveno je određeno svojim domenom, tj. ako $\mathbb{F}, \mathbb{F}' \subseteq \mathbb{E}$ i $F = F'$ onda $\mathbb{F} = \mathbb{F}'$ (tj. $x + y = x +' y$, $x \cdot y = x \cdot' y$, $x, y \in F$). Stoga podpolje identifikujemo sa njegovim domenom i koristimo iste oznake za operacije kao u ekstenziji.

5.3 *Primer* Postoji polje $\mathbb{F} = (Q, +', \cdot', 0', 1')$, Q je skup racionalnih brojeva, tako da je $\mathbb{F} \cong \mathbb{Q}(\sqrt{2})$.

Dokaz Skupovi Q i $Q(\sqrt{2})$ su prebrojivi, dakle postoji $f : Q \xrightarrow[1-1]{na} Q(\sqrt{2})$. Neka su $0' = f^{-1}(0)$, $1' = f^{-1}(1)$ i za $x, y \in Q$
$x +' y = f^{-1}(f(x) + f(y))$, $x \cdot' y = f^{-1}(f(x) \cdot f(y))$. Tada je
$\mathbb{F} = (Q, +', \cdot', 0', 1')$ polje i $\mathbb{F} \cong \mathbb{Q}(\sqrt{2})$.

5.4. *Zadatak* a) Pokažite da se u 5.3. može uzeti $0' = 0$, $1' = 1$.
b) Dokažite da postoji polje $\mathbb{Q}' = (Q, +', \cdot', 0, 1)$ tako da je $\mathbb{Q}' \cong \mathbb{Q}$ ali $\mathbb{Q}' \neq \mathbb{Q}$.

5.5 Neka je $\mathbb{F} \subseteq \mathbb{E}$, $\mathbb{F}$ i $\mathbb{E}$ su polja. Tada su $\mathbb{F}$ i $\mathbb{E}$ iste karakteristike.

5.6. Neka su $\mathbb{F}$ i $\mathbb{E}$ polja, $\mathbb{F} \subseteq \mathbb{E}$. Tada je
$\mathcal{E}_{\mathbb{F}} = ((E, +, 0), \mathbb{F}, \bullet)$, gde $\alpha \bullet x = \alpha x$, $\alpha \in F$, $x \in E$, vektorski prostor.

Definicija Ako je $\mathbb{F} \subseteq \mathbb{E}$, stepen polja $\mathbb{E}$ nad $\mathbb{F}$, u oznaci $|\mathbb{E} : \mathbb{F}|$ je $\dim \mathcal{E}_{\mathbb{F}}$. Dakle, $|\mathbb{E} : \mathbb{F}| = \dim \mathcal{E}_{\mathbb{F}}$.

Primer: $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$, $|\mathbb{C} : \mathbb{R}| = 2$, $|\mathbb{R} : \mathbb{Q}| = \infty$.

5.7. Teorema Neka su $\mathbb{F}, \mathbb{E}, \mathbb{K}$ polja takva da je $\mathbb{F} \leq \mathbb{E} \leq \mathbb{K}$. Tada $|\mathbb{K} : \mathbb{F}| = |\mathbb{K} : \mathbb{E}| \cdot |\mathbb{E} : \mathbb{F}|$.

Dokaz Neka je $\langle a_i \mid i \in I \rangle$ baza prostora $\mathcal{E}_{\mathbb{F}}$ i neka je $\langle b_j \mid j \in J \rangle$ baza prostora $\mathcal{K}_{\mathbb{E}}$. Dakle,

$\dim \mathcal{E}_{\mathbb{F}} = |I| = m$, $\dim \mathcal{K}_{\mathbb{E}} = n = |J|$.

Tada je $\langle a_i b_j \mid i \in I, j \in J \rangle$ baza prostora $\mathcal{K}_{\mathbb{F}}$ pa

$\dim \mathcal{K}_{\mathbb{F}} = |I \times J| = |I| \cdot |J| = m \cdot n = \dim \mathcal{E}_{\mathbb{F}} \cdot \dim \mathcal{K}_{\mathbb{E}}$,

odakle sledi $|\mathbb{K} : \mathbb{F}| = |\mathbb{K} : \mathbb{E}| \cdot |\mathbb{E} : \mathbb{F}|$. ⊠

Napomena u prethodnoj teoremi tvrdenje važi i ako je neki od stepena $|\mathbb{K} : \mathbb{F}|, |\mathbb{K} : \mathbb{E}|, |\mathbb{E} : \mathbb{F}|$ beskonačan kardinalan broj.

5.8 Zadatak Neka je dat lanac polja $\mathbb{F}_1 \leq \mathbb{F}_2 \leq \dots \leq \mathbb{F}_n$. Tada $|\mathbb{F}_n : \mathbb{F}_1| = |\mathbb{F}_n : \mathbb{F}_{n-1}| \cdot |\mathbb{F}_{n-1} : \mathbb{F}_{n-2}| \cdots |\mathbb{F}_2 : \mathbb{F}_1|$.

5.9. Zadatak Neka je $\mathbb{E}$ polje i $\sigma \in \operatorname{Aut} \mathbb{E}$ reda 2, tj. $\sigma^2 = i$, $\sigma \neq i$.

a) Neka je $F = \{ x \in E \mid \sigma x = x \}$. Dokazati da je $F \leq \mathbb{E}$.

b) Ako je $\mathbb{F}$ podpolje polja $\mathbb{E}$ iz (a), tada $|\mathbb{E} : \mathbb{F}| = 2$.

5.10. Ako je $\mathbb{F}$ beskonačne karakteristike, tada je $\mathbb{F}$ vektorski prostor nad $\mathbb{Q}$

5.11. Ako je $\mathbb{F}$ proste karakteristike p, onda je $\mathbb{F}$ vektorski prostor nad $\mathbb{Z}_p$.

5.12. Teorema Neka je $\mathbb{F}$ konačno polje. Tada za neki prost broj p i $n \in N^+$, $|\mathbb{F}| = p^n$

Dokaz $\mathbb{F}$ je konačne karakteristike, jer bi u suprotnom $\mathbb{F}$ sadržalo racionalne brojeve. Dakle, $\mathbb{F}$ je proste karakteristike p. Prema 5.11 tada je $\mathbb{F}$ vektorski prostor nad $\mathbb{Z}_p$. S obzirom da je $\mathbb{F}$ konačan, $\mathbb{F}$ je konačno dimenzionalan prostor, recimo $n = \dim \mathcal{F}_{\mathbb{Z}_p}$. Tada prema teoremi iz linearne algebre,

$\mathcal{F}_{\mathbb{Z}_p} \cong ((\mathbb{Z}_p, +_p, 0)^n, \mathbb{Z}_p, \cdot)$, pa $(F, +, 0) \cong (\mathbb{Z}_p, +_p, 0)^n$, odakle

$|F| = |\mathbb{Z}_p|^n = p^n$.

5.13. Zadatak U konačnom polju $\mathbb{F}$ važi $x^{p^n} = x$, $x \in F$, za neki p prost, $n \in N^+$.

5.14.** Zadatak Navesti primere polja $\mathbb{F}$ i $\mathbb{K}$ takve da je $(F, +, 0) \cong (K, +, 0)$, $\mathbb{F}^* \cong \mathbb{K}^*$ ali $\mathbb{F} \not\cong \mathbb{K}$.

6. Polinomi

6.1. Izrazi oblika $a_0 + a_1 x + \cdots + a_n x^n$, x je promenljiva x, $a_0, a_1, \ldots, a_n \in F$ nazivaju se polinomima promenljive x nad poljem $\mathbb{F}$. Skup ovih polinoma promenljive x nad poljem $\mathbb{F}$ označava se sa $\mathbb{F}[x]$. Dakle, $F[x] = \{ p(x) \mid p(x)$ je polinom nad $\mathbb{F} \}$.

6.2. Slična je definicija polinoma nad ma kojim prstenom $\mathbb{P}$. U ovom slučaju koeficijenti se biraju iz domena P prstena $\mathbb{P}$.

6.3. Skup polinoma više promenljivih definiše se induktivno. Ako su $x_1, x_2, \ldots, x_n$ promenljive tada, $(P[x_1, \ldots, x_{n-1}])[x_n] = P[x_1, \ldots, x_n]$. Primetimo da je $P[x_1, \ldots, x_n]$ prsten u odnosu na uobičajene operacije sabiranja i množenja polinoma. Ako je $p(x_1, \ldots, x_n) \in P[x_1, \ldots, x_n]$, tada

$$p(x_1, \ldots, x_n) = \sum_{\alpha \in S} a_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}, \quad \alpha = \langle \alpha_1, \ldots, \alpha_n \rangle$$

$S \subseteq N$ i S je konačan.

6.4. Nula polinom je polinom čiji su svi koeficijenti jednaki 0. Ovaj polinom označavamo sa $\mathbb{0}$. Sa $\mathbb{1}$ označavamo polinom kod kojeg je $a_1 = 1$, a ostali koeficijenti jednaki su 1.

6.5. Sabiranje $+$ i množenje $\cdot$ polinoma promenljive x nad poljem $\mathbb{F}$ (odnosno nad prstenom $\mathbb{P}$) definiše se na uobičajen način: Ako su $f, g \in F[x]$, $f(x) = \sum_{i=0}^{m} a_i x^i$, $g(x) = \sum_{j=0}^{n} b_j x^j$ i $k = \max(m, n)$,

$(f+g)(x) = \sum_{s=0}^{k} c_s x^s$, gde $c_s = a_s + b_s$, eventualno dopunjavajući koeficijente polinoma f i g nulama.

$$(f \cdot g)(x) = \sum_{s=0}^{mn} d_s x^s, \quad d_s = \sum_{i=0}^{s} a_i b_{s-i}, \quad 0 \le s \le mn.$$

6.6. U odnosu na ovako uvedene operacije sabiranja i množenja polinoma, $\mathbb{F}[x] = (F[x], +, \cdot, \mathbb{0}, \mathbb{1})$ je komutativan prsten sa jedinicom bez delitelja nule, tj. $f \cdot g = \mathbb{0} \Rightarrow (f = \mathbb{0} \vee g = \mathbb{0})$.

6.7. Stepen polinoma f je najveći indeks i takav da je $a_i \neq 0$. Stepen polinoma f označavamo sa $\deg(f)$. Važi

$$\deg \mathbb{0} = -1, \quad \deg(f+g) \le \max(\deg f, \deg g),$$

$$\deg(f \cdot g) = \deg f + \deg g, \quad f, g \neq \mathbb{0}.$$

6.8 Prethodna definicija polinoma može se učiniti preciznijom.

a. Prvi način. Jezik teorije polja je $L = \{+, \cdot, 0, 1\}$. Tada je svako polje $\mathbb{F} = (F, +_F, \cdot_F, 0_F, 1_F)$ jedna interpretacija ovog jezika. U praksi zanemarujemo indeks $_F$ u $+_F$, pa ostaje ista oznaka za operaciju sabiranja u polju $\mathbb{F}$ i simbol operacije jezika L. Uvedimo za svaki $a \in F$ simbol nove konstante $\underline{a}$. Ovaj novi znak nazivamo imenom elementa a. Neka je za domen F, $L_F = L \cup \{\underline{a} \mid a \in F\}$. Tada:
Polinom nad poljem $\mathbb{F}$ je algebarski izraz (term) vida

$$\underline{a}_0 + \underline{a}_1 x + \dots + \underline{a}_n x^n, \quad x \text{ je promenljiva.}$$

b. Drugi način. Polinom nad poljem $\mathbb{F}$ je svako preslikavanje $f : N \to F$, N je skup prirodnih brojeva, $f(n) = 0$ za sve $n \in N$ osim za konačno mnogo n.
Ako je $f = \langle f_0, f_1, f_2, \dots, f_n, 0, 0, \dots \rangle$, onda ovako definisanom polinomu f odgovara polinom $f(x) = \underline{f}_0 + \underline{f}_1 x + \dots + \underline{f}_n x^n$ u smislu definicije 6.8.a.
Dalje, $\mathbb{0} = \langle 0, 0, 0, \dots \rangle$ i također, polinomi f, g su jednaki akko ako su f i g jednaki kao preslikavanja, tj.

$$f = g \iff \bigwedge_{n \in N} f_n = g_n .$$

Dalje, operacije nad polinomima izgleda ovako u ovom slučaju:

$$(f+g)_n \overset{def}{=} f_n + g_n, \quad (f \cdot g)_n \overset{def}{=} \sum_{i=0}^{n} f_i g_{n-i}, \quad n \in N$$

$$\deg f \overset{def}{=} \max\{n \mid f_n \neq 0\} \text{ ako } f \neq \mathbb{0}, \quad \deg \mathbb{0} \overset{def}{=} -1 .$$

Polinomi više promenljivih mogu se uvesti na sličan način:
Polinom k-promenljivih je svako preslikavanje oblika

$$f : N^k \to F, \quad (k > 0).$$

Polinom f kao algebarski izraz tada izgleda $f = \sum_{\alpha} \underline{f}_\alpha x_1^{\alpha_1} \dots x_k^{\alpha_k}$.

Napomena Prema definiciji 6.8a polinom ne zavisi od operacija polja $\mathbb{F}$. Tek kad se uvodi prsten polinoma operacije polja $\mathbb{F}$ učestvuju u definicijama operacija prstena $\mathbb{F}[x]$. Na primer, ako je $h = f + g$, onda za $h = \sum \underline{h}_i x^i$, $h_i = f_i +_F g_i$.
Prema definiciji 6.8b, definicija polinoma ne zavisi ni od pojma promenljive.

6.9 Zadatak Definisati prstene polinoma $\mathbb{F}'[x]$, $\mathbb{F}''[x]$ nad poljem $\mathbb{F}$ redom prema definicijama polinoma 6.8a, 6.8b. Dokazati da je $\mathbb{F}'[x] \cong \mathbb{F}''[x]$.

6.10. Zadatak Neka je $\mathbb{F}$ podpolje polja $\mathbb{E}$. Dokazati:
1° Polje $\mathbb{F}$ utapa se u prsten $\mathbb{F}[x]$, dakle možemo uzeti $\mathbb{F} \subseteq \mathbb{F}[x]$.
2° $\mathbb{F}[x] \subseteq \mathbb{E}[x]$.

6.11. Polinomna funkcija Neka je $\mathbb{F}$ polje i $f \in \mathbb{F}[x]$. Polinom f možemo proširiti funkciju $f^F : F \to F$, uzimajući da je za $a \in F$, $f^F(a) =$ vrednost polinoma f za $x = a$ u polju $\mathbb{F}$.

Pojmovi polinoma i polinomne f-ja nisu isti, niti su ekvivalentni. Naime, može se desiti da različiti polinomi određuju istu polinomnu f-ju.

Primer 1° Polinomi x^p i x određuju istu polinomnu f-ju nad poljem $\mathbb{Z}_p$ s obzirom na identitet $x^p = x$ koji važi u $\mathbb{Z}_p$.

2° Ako je $\mathbb{F}$ konačno polje, $|F| = n$, onda svih f-ja iz F u F ima n^n, dakle konačno mnogo. Odatle i polinomnih f-ja ima konačno mnogo (nad $\mathbb{F}$), dok polinoma ima beskonačno mnogo.

6.12. Zadatak Neka je $\mathcal{F}$ skup polinomnih f-ja jedne promenljive nad $\mathbb{F}$.
1° Neka su operacije $+$ i $\cdot$ u $\mathcal{F}$ definisane pomoću
$$(f^F + g^F)(x) = f^F(x) + g^F(x), \quad (f^F \cdot g^F)(x) = f^F(x) \cdot g^F(x).$$
Dokazati da je $(\mathcal{F}, +, \cdot, 0^F, 1^F)$ komutativan prsten bez delitelja nule.
2° Dokazati da je $\sigma : f \mapsto f^{\mathbb{F}}$ homomorfizam iz $\mathbb{F}[x]$ u $\mathcal{F}$.
3° Ako je $\mathbb{F}$ konačno polje, $|F| = n$, tada je $\ker\sigma$ ideal generisan polinomom $x^n - x$, tj. $\ker\sigma = (x^n - x) = \{(x^n - x)h(x) \mid h \in F[x]\}$.
4° Ako je $\mathbb{F}$ beskonačno polje onda je σ monomorfizam.

7. Polje racionalnih izraza. Racionalni izrazi promenljive x nad poljem $\mathbb{F}$ su izrazi oblika $f(x)/g(x)$, $g \neq 0$. Skup svih racionalnih izraza obeležavamo sa $F(x)$. Dakle,
$F(x) = \{ f/g \mid f, g \in F[x]\}$. Operacije sabiranja i množenja u $F(x)$ uvodimo na uobičajeni način:
$$f/g + f'/g' \overset{\text{def}}{=} (fg' + f'g)/gg', \; g, g' \neq 0; \quad (f/g)\cdot(f'/g') \overset{\text{def}}{=} (ff')/(gg').$$

7.1. Teorema 1° $\mathbb{F}(x) = (F(x), +, \cdot, 0/1, 1/1)$ je polje.
2° $\mathbb{F}[x]$ se utapa u $\mathbb{F}(x)$, dakle možemo uzeti $F[x] \subseteq F(x)$.
Utapanje je : $f \mapsto f/1$, $f \in F[x]$.

7.2. Na sličan način se definiše polje racionalnih izraza promenljivih $x_1, \dots, x_n$ (ili induktivno : $F(x_1, \dots, x_n) = (F(x_1, \dots, x_{n-1}))(x_n)$).
Kao i kod polinoma, definišu se racionalne f-je nad $\mathbb{F}$ kao vrednosti racionalnih izraza.

8. <u>Deljivost polinoma</u> Relacija deljivosti polinoma definiše se na sledeći način: Za $f, g \in F[x]$, $g \neq 0$, $f \mid g$ akko postoji $q \in F[x]$ tako da $g = q \cdot f$.

8.1. Relacija $\mid$ nad $F[x]$ je refleksivna i tranzitivna. Ako $f, g \neq 0$ i $f \mid g$, $g \mid f$ onda postoji konstanta $c \in F$ tako da $f = c \cdot g$.

8.2. <u>Teorema o ostatku za polinome</u> Neka su $f, g \in F[x]$, $g \neq 0$. Tada postoje jedinstveni $q, r \in F[x]$ takvi da

(*) $f = g \cdot q + r$, $r = 0$ ili $0 \leq \deg r < \deg g$.

<u>Dokaz</u> Neka je $R = \{ f - gh \mid h \in F[x] \}$.

a. Ako je $0 \in R$, onda $r = 0$, i biramo q tako da $f - gh = 0$.

b. PP $0 \notin R$. Tada je $S = \{ n \in N^+ \mid n = \deg h,\ h \in R \}$ neprazan jer $\deg f \in S$ ili ako $\deg f = 0$ onda $\deg g \in S$. Neka je $m = \min S$ (prema Principu najmanjeg broja za prirodne brojeve). Tada $m = \deg r$ za neki $r \in R$ i postoji $q \in F[x]$ tako da je $r = f - g \cdot q$, tj. $f = gq + r$. Dokažimo da je $\deg r < \deg g$ (očigledno $0 \leq \deg r$ jer $0 \notin S$). PP suprotno, da je $m = \deg r \geq \deg g = n$. Tada za neki (dobro izabran) $c \in F$ i

$s(x) = r(x) - c \cdot x^{m-n} g(x) = f(x) - (q(x) + c \cdot x^{m-n}) g(x)$,

$\deg s \leq m - 1$ i $s \in R$, što je kontradikcija prema izboru polinoma r.

Ovim je dokazana egzistencija razlaganja (*).

Dokažimo jedinost: Neka je

$f = g \cdot q + r = g \cdot q' + r'$, $q \neq q'$. Tada $g(q - q') = r' - r$

odakle $\deg g > \deg r, \deg r' \geq \deg(r - r') = \deg g + \deg(q - q') \geq \deg g$, #.

Dakle $\deg(q - q') = 0$, pa $q = q'$ te i $r = r'$ ▨

8.3 <u>Posledica</u> Neka je $a \in F$. Tada postoji jedinstveni $r \in F$ tako da $f(x) = (x - a) q(x) + r$. Primetimo da je $r = f(a)$. Otuda $f(a) = 0 \Leftrightarrow (x - a) \mid f(x)$.

8.4. <u>Teorema</u> Neka je $n \in N$, $\deg f = n$. Tada $f(x)$ ima najviše n nula.
<u>Dokaz indukcijom</u>: Ako je a koren polinoma $f(x)$, onda $f(x) = (x - a) g(x)$, $\deg g = n - 1$ i prema induktivnoj hipotezi g ima najviše $n-1$ koren. ▨

8.5 Posledica Ako je $\deg f = n$ i $a_1, a_2, \dots, a_n$ su koreni polinoma f, onda $f(x) = c(x-a_1)(x-a_2)\cdots(x-a_n)$, za neki $c \in F$.
Primetimo da je $c = f_n$.

9. Izvod polinoma Neka je $\mathbb{F}$ bilo koje polje i neka je $f \in F$, $f(x) = a_0 + a_1 x + \dots + a_n x^n$. Tada $f'(x) \overset{\text{def}}{=} a_1 + 2a_2 x + \dots + n \cdot a_n x^{n-1}$.
Umesto f' pišemo i Df. Ako je $c \in F$, onda $Dc = 0$.

9.1. Teorema $(x-a)^2 \mid f(x) \iff f(a) = 0,\ f'(a) = 0$.
($\Rightarrow$) PP $(x-a)^2 \mid f(x)$. Tada $f(x) = (x-a)^2 g(x)$, $f'(x) = (x-a)(2g(x) + (x-a)g'(x))$
pa $f(a) = f'(a) = 0$.
($\Leftarrow$) PP $f(a) = 0$, $f'(a) = 0$. Tada prema 8.4. $f(x) = (x-a)g(x)$
za neki $g \in F$, pa $f'(x) = g(x) + (x-a)g'(x)$. Kako je $f'(a) = 0$,
to $g(a) = 0$ pa prema 8.4, $g(x) = (x-a)\,l(x)$ za neki $l \in F[x]$,
tj. $f(x) = (x-a)^2 l(x)$.

9.2. Lajbnicova formula $D^n(f \cdot g) = \sum_{i=0}^{n} \binom{n}{i} D^i f \cdot D^{n-i} g$.
Dokaz: indukcijom po n.

9.3. Njutnova formula. Neka je $k\mathbb{F} = 0$ (karakteristika polja $\mathbb{F} = 0$).
Tada za $f \in \mathbb{F}[x]$ važi
$$f(x) = f(a) + \frac{f'(a)}{1!}(x-a) + \dots + \frac{f^{(n)}(a)}{n!}(x-a)^n, \quad n \in N^+.$$
Dokaz: indukcijom po n.

9.4. Neka je $k\mathbb{F} = 0$. Tada $(x-a)^n \mid f(x)$, $(x-a)^{n+1} \nmid f(x)$ akko
$f(a) = 0$, $f'(a) = 0, \dots, f^{(n-1)}(a) = 0$, $f^{(n)}(a) \neq 0$, $n \in N^+$.

9.5. Zadatak $(f+g)' = f' + g'$, $(f \cdot g)' = f \cdot g' + f' g$.

9.6. Zadatak (Langranžev polinom). Neka su $(x_1, y_1), \dots, (x_n, y_n) \in F^2$, $x_i \neq x_j$ za $i \neq j$. Tada postoji tačno jedan polinom $f \in F[x]$ tako da $f(x_i) = y_i$, $1 \le i \le n$. Konstruisati taj polinom.

10. Euklidov algoritam za polinome. Polinom $f \in F[x]$, $\deg f \ge 1$, je svodljiv nad $\mathbb{F}$ ako postoje $g, h \in F[x]$ takvi da je
$$f = g \cdot h \quad \text{i} \quad \deg g,\ \deg h < \deg f.$$
Polinom $f \in F[x]$, $\deg f \ge 1$, je nesvodljiv nad $\mathbb{F}$ ako nije svodljiv nad $\mathbb{F}$.

10.1. Primer x^2+1 svodljiv nad $\mathbb{Z}_2$ jer $x^2+1 = (x+1)^2$ u $\mathbb{Z}_2$.
x^2+x+1 je nesvodljiv nad $\mathbb{Z}_2$ (jer x^2+x+1 nema nula u $\mathbb{Z}_2$).

10.2. Primer Polinom $4x^3 - 3x - 1/2$ je nesvodljiv nad $\mathbb{Q}$ (jer nema racionalnih korena, dakle niti linearnih faktora. Svaki svodljiv polinom trećeg stepena nad $\mathbb{Q}$ mora imati linearan faktor $(x-a) \in \mathbb{Q}[x]$, dakle i racionalan koren).
Primetimo da $a = \cos 20^\circ$ jeste koren ovog polinoma.

Euklidov algoritam Neka su $f, g \in F[x]$, $g \neq 0$. Tada prema 8.2 postoji sledeći niz jednakosti:

$$
\begin{aligned}
f &= g \cdot q_1 + r_1, \quad 0 \leq \deg r_1 < \deg g \\
g &= r_1 q_2 + r_2, \quad 0 \leq \deg r_2 < \deg r_1 \\
r_1 &= r_2 q_3 + r_3, \quad 0 \leq \deg r_3 < \deg r_2 \qquad n \in N \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 \leq \deg r_n < \deg r_{n-1} \\
r_{n-1} &= r_n q_{n+1}
\end{aligned}
$$

Ovaj niz je konačan s obzirom da u skupu prirodnih brojeva nema beskonačnih regresija, $\deg g > \deg r_1 > \deg r_2 > \cdots$

10.3 Teorema Član r_n iz Euklidovog algoritma je polinom najvećeg stepena koji deli f i g.
Dokaz Iz poslednje jednakosti, $r_n | r_{n-1}$, te iz pretposlednje $r_n | r_{n-2}$ i tako redom, $r_n | f, g$.
S druge strane ako $h | f, g$ onda prema prvoj jednakosti $h | r_1$, prema drugoj $h | r_2$ i tako redom, $h | r_n$.

10.4. Polinom najvećeg stepena koji deli polinome f i g naziva se najvećim zajedničkim deliocem polinoma f, g. Skup svih najvećih zajedničkih delilaca polinoma f i g označava se sa (f, g).
Ako su $h, h' \in (f, g)$ onda postoji $c \in F$ tako da $h' = c \cdot h$.
Primetimo da je (f, g) dobro definisan ako $f \neq 0$ ili $g \neq 0$, s obzirom da svaki $f \in F[x]$, $f | 0$.
U skupu (f, g), uz uslov $f \neq 0$ ili $g \neq 0$, postoji konačni polinom, to je $h \in (f, g)$, gde $h_n = 1$ (h je moničan polinom)

10.5. Bezuova teorema za polinome Polazeći od prve jednakosti u Euklidovom algoritmu vidimo da je r_1 linearna kombinacija polinoma f i g. Vršeći redom supstituciju polinoma r_k u $k+1$-jednakosti pomoću linearne kombinacije polinoma f i g, iz pretposlednje jednakosti nalazimo

za neke $p, q \in F[x]$, $p \cdot f + q \cdot g = r_n$.

Drugim rečima, ako je $d \in (f, g)$, onda postoje $\alpha, \beta \in F[x]$ tako da
$$\alpha f + \beta g = d.$$

10.6. Za polinome $f, g \in F[x]$ kažemo da su uzajamno prosti ako $1 \in (f, g)$. Ako su f i g uzajamno prosti tada pišemo $(f, g) = 1$

<u>Lema</u> 1° $(f, g) = 1 \Rightarrow \bigvee_{p, q \in F[x]} p \cdot f + q \cdot g = 1$

2° $(f, g) = 1 \Rightarrow (f^n, g^n) = 1$

3° $f \mid gh,\ (f, g) = 1 \Rightarrow f \mid h$

4° $(f, g) = 1,\ (f, h) = 1 \Rightarrow (f, gh) = 1.$

<u>Dokaz za 3°</u> PP $f \mid gh$, $(f, g) = 1$. Tada za neke $p, q \in F[x]$, $p \cdot f + q \cdot g = 1$, odakle $pfh + qgh = h$. Kako $f \mid pfh + qgh$ to $f \mid h$. ∎

10.7. <u>Teorema</u> o razlaganju polinoma na nesvodljive faktore
Neka je $f \in F[x]$, $\deg f \geq 1$. Tada postoje nesvodljivi polinomi $g_1, \dots, g_k$ takvi da je $f = g_1 g_2 \cdots g_k$. Ovo razlaganje je jedinstveno do na:
a) redosled faktora,
b) umnožak konstantama iz F članova razlaganja.
Drugim rečima ako je $f = g_1' \cdots g_l'$ razlaganje na nesvodljive faktore, tada $k = l$, postoji permutacija $(i_1, \dots, i_k) \in S_k$ i $c_1, \dots, c_k \in F$ tako da je $g_j' = c_i \cdot g_{i_j}$, $1 \leq j \leq k$.
<u>Dokaz</u>: Isto kao Osnovna teorema aritmetike.

10.8. <u>Zadatak</u> 1° Jedini nesvodljivi polinomi nad poljem kompleksnih brojeva $\mathbb{C}$ su polinomi $x - a$, $a \in \mathbb{C}$.
2° Ako su $a, b \in F$, $a \neq b$, onda za $m, n \in N^+$, $((x-a)^m, (x-a)^n) = 1$.
3° Ako je $f \in \mathbb{C}[x]$, onda postoje jedinstveni $a_1, \dots, a_k \in \mathbb{C}$, $a_i \neq a_j$ za $i \neq j$, $m_1, \dots, m_k \in N^+$ i $c \in \mathbb{C}$ takvi da je $f(x) = c \cdot (x - a_1)^{m_1} \cdots (x - a_k)^{m_k}$.

10.9. <u>Zadatak</u> 1° Ako je polje $\mathbb{F}$ konačno, onda postoji beskonačno mnogo nesvodljivih polinoma nad $\mathbb{F}$.
2° Za dati $n \in N^+$, postoji beskonačno mnogo nesvodljivih nad $\mathbb{Q}$ polinoma stepena n
<u>Uputstvo</u>: 1° slično dokazu da postoji beskonačno mnogo prostih brojeva.
2° $x^n - p$, $p \in Prost$.

10.10. <u>Gausova lema</u> Neka je $f \in \mathbb{Z}[x]$ (polinom sa celobrojnim koeficijentima). Tada, f je nesvodljiv nad $\mathbb{Q}$ akko je f nesvodljiv nad $\mathbb{Z}$.

10.11. <u>Ajzenštajnov kriterijum</u>. Neka je $f \in \mathbb{Z}[x]$. Pretpostavimo da postoji prost broj p takav da
1° $p \nmid f_n$, 2° $p \mid f_0, f_1, \dots, f_{n-1}$ 3° $p^2 \nmid f_0$.
Tada je f nesvodljiv nad $\mathbb{Z}$, dakle i nad $\mathbb{Q}$.

10.12. Ako je $p \in Prost$, tada je $1 + x + \dots + x^{p-1}$ nesvodljiv nad $\mathbb{Q}$.

11. PRSTENI

Algebra $\mathbb{P} = (P, +, \cdot, 0)$ je <u>prsten</u> ukoliko važi:

1° $(P,+,0)$ je Abelova grupa.

2° $(P,\cdot)$ je semigrupa.

3° $x\cdot(y+z) = (x\cdot y)+(x\cdot z)$

Prsten $\mathbb{P}$ je komutativan ako je $(P,\cdot)$ komutativna semigrupa.

$\mathbb{P} = (P,+,\cdot,0,1)$ je prsten sa jedinicom ako važe u P zakoni
$x\cdot 1 = x = 1\cdot x$.

11.1. <u>Primer</u> 1° $(\mathbb{Z},+,\cdot,0,1)$ je komutativan prsten.

2° Ako je $n\in N$, $n\geq 2$, $\mathbb{Z}_n = (Z_n, +_n, \cdot_n, 0, 1)$ je komutativan prsten. Primetimo da je preslikavanje $g_n : Z \to Z_n$, $g_n(x) = rest(x,n)$ homomorfizam prstena $\mathbb{Z}$ na $\mathbb{Z}_n$. S obzirom da homomorfizmi prenose algebarske zakone, ovo je istovremeno dokaz da je $\mathbb{Z}_n$ komutativan prsten sa jedinicom.

2° Svako polje je prsten.

3° $(2\mathbb{Z},+,\cdot,0)$ je prsten bez jedinice, $2\mathbb{Z}=\{\dots,-2,0,2,\dots\}$.

4° Neka je $M_n(F)$ skup kvadratnih matrica nad poljem $\mathbb{F}$. Tada je $(M_n(\mathbb{F}),+,\cdot,\mathbb{O},E_n)$ prsten sa jedinicom (nekomutativan za $n\geq 2$).

Za $A = \begin{bmatrix} 0 & 0 & \\ 1 & 0 & \\ & & * \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 & \\ 0 & 1 & \\ & & * \end{bmatrix}$ i $A, B \in M_n(\mathbb{F})$, $n\geq 2$

$AB = \begin{bmatrix} 0 & 0 & \\ 0 & 0 & \\ & & * \end{bmatrix}$, $BA = \begin{bmatrix} 0 & 0 & \\ 1 & 0 & \\ & & * \end{bmatrix}$, dakle $AB \neq BA$.

11.2. $x - y \overset{def}{=} x+(-y)$, $x,y\in P$, $\mathbb{P}$ je prsten.

Klasa $\mathcal{P}$ prstena zatvorena je za homomorfne slike i proizvode. $\mathcal{P}$ nije zatvorena za podalgebre jer, na primer,
$(N,+,\cdot,0,1)\subseteq \mathbb{Z}$ ali $(N,+,\cdot,0,1)$ nije prsten.

Neka je $\mathcal{P}'$ klasa proširenih algebri $(P,+,-,\cdot,0)$, gde je $\mathbb{P}=(P,+,\cdot,0)$ prsten. Tada je $\mathcal{P}'$ zatvorena za homomorfne slike, proizvode i podalgebre, tj. $\mathcal{P}'$ je <u>algebarski varijetet</u>.

Ubuduće implicitno pretpostavljamo da je simbol operacije oduzimanja element jezika prstena.

11.3. Od sada pa nadalje, ukoliko se drugačije ne kaže, pretpostavljamo da su prsteni komutativni i da imaju jedinicu.

11.4. Prsten $\mathbb{P}$ je bez delitelja nule ako u $\mathbb{P}$ važi:
$x \cdot y = 0 \Rightarrow (x = 0 \vee y = 0)$.
Prsteni $\mathbb{Z}$, $\mathbb{F}[x]$ (prsten polinoma nad poljem $\mathbb{F}$) i svako polje su primeri prstena bez delitelja nule. Za ove prstene koristi se i naziv domen.
Prsten $\mathbb{Z}_6$ ima delitelje nule.

11.5. Jednota prstena $\mathbb{P}$ je svaki invertibilan element $c \in P$. Dakle $c \in P$ je jednota ako postoji $d \in P$ takav da je $c \cdot d = 1$. Skup svih jednota prstena $\mathbb{P}$ označavamo sa $J(\mathbb{P})$.

11.6. Teorema $\mathcal{J} = (J(\mathbb{P}), \cdot, 1)$ je grupa.
Na primer, ako je $\mathbb{F}$ polje tada
$\mathcal{J}(\mathbb{F}) = \mathbb{F}^*$, $\mathcal{J}(\mathbb{F}[x]) = \mathbb{F}^*$, $\mathcal{J}(\mathbb{Z}) = (\{-1, 1\}, \cdot, 1)$.

11.7. Zadatak Dokazati da je $\mathcal{J}(\mathbb{Z}_n) = \Phi_n$, gde je $\Phi_n = (\Phi_n, \cdot_n, 1)$ Ojlerova grupa, $\Phi_n = \{x \in N^+ \mid (x, n) = 1\}$.
Red ove grupe je Ojlerova funkcija $\varphi(n)$.
Ako je $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ razlaganje broja n na proste faktore, onda $\varphi(n) = n \cdot (1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$.

12. Ideali prstena

Ideal prstena $\mathbb{P}$ je svaki $I \subseteq P$ koji ima ove osobine:
1° $(I, +, 0)$ je grupa.
2° $I P \subseteq I$, tj. $i \in I$, $x \in P \Rightarrow ix \in I$.

12.1. Primer 1° $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$, $n \in N$, su ideali prstena $\mathbb{Z}$.
Zapravo, to su jedini ideali prstena $\mathbb{Z}$: neka je I ideal prstena $\mathbb{Z}$ i pr. $I \neq \{0\}$. Tada postoji najmanji prirodan broj $n \in I$. Neka je $x \in I$ i $x = nq + r$, $0 \le r < n$. Kako $x, nq \in I$, to $x - nq \in I$ pa $r \in I$. Prema izboru broja n sledi $r = 0$, tj. $x = nq$, pa $I = n\mathbb{Z}$.

(17)

2° Neka je $f \in \mathbb{F}[x]$, gde je $\mathbb{F}$ polje. Tada je $(f) = \{fg \mid g \in \mathbb{F}[x]\}$ ideal prstena $\mathbb{F}[x]$.

3° Neka je $\mathbb{F}$ polje i $f_1, \dots, f_n \in \mathbb{F}[x]$. Tada je
$I = \{f_1 g_1 + \dots + f_n g_n \mid g_1, \dots, g_n \in \mathbb{F}[x]\}$ ideal prstena $\mathbb{F}[x]$.

4° Jedini ideal polja $\mathbb{F}$ je $\{0\}$.

12.2. Ideal $(0) = \{0\}$ je trivijalni ideal prstena $\mathbb{P}$.
Ako je ideal $I \neq \mathbb{P}$, onda se I naziva pravim idealom.
$\mathbb{P}$ je nepravi ideal prstena $\mathbb{P}$.
Pravi ideal I prstena $\mathbb{P}$ je maksimalan ako za svaki ideal J prstena $\mathbb{P}$ iz $I \subsetneqq J$ sledi $J = \mathbb{P}$.

Primer: 1° Ako je $p \in Prost$, tada je $p\mathbb{Z}$ maksimalan ideal prstena $\mathbb{Z}$. Zaista iz $p\mathbb{Z} \subsetneqq n\mathbb{Z}$ sledi $n \mid p$, $n \neq p$, pa $n=1$ tj: $n\mathbb{Z} = \mathbb{Z}$.

2° Ako je polinom f nesvodljiv nad $\mathbb{F}$, tada je (f) maksimalan ideal u $\mathbb{F}[x]$ ($\mathbb{F}$ je polje).
Zaista, neka je I ideal prstena $\mathbb{F}[x]$, $(f) \subsetneqq I$ i neka je $g \in I \setminus (f)$ polinom najmanjeg stepena. Prema lemi o ostatku za polinome postoje $q, r \in \mathbb{F}[x]$ takvi da je $f = qg + r$, $\partial \deg r < \deg f$ (primetimo da je $g \neq 0$, jer $0 \in (f)$).
Kako $f, q \cdot g \in I$, to $f - qg \in I$ tj. $r \in I$, suprotno izboru polinoma g.

12.3. Zadatak Neka je I ideal prstena $\mathbb{P}$ i $x \in \mathbb{P}$. Dokazati da je $J = \langle I \cup \{x\} \rangle = \{i + xp \mid p \in \mathbb{P}\}$ najmanji ideal prstena $\mathbb{P}$ koji sadrži I kao podskup i x.

13 Količnički prsteni

Neka je I ideal prstena $\mathbb{P}$. Tada se može definisati kongruencija $\sim$ prstena $\mathbb{P}$ na sledeći način:

$x \sim y \overset{def}{\Longleftrightarrow} x - y \in I.$

Relacija $\sim$ je relacija ekvivalencije domena $\mathbb{P}$:

(R) $x \sim x$ jer $x - x = 0$, $0 \in I$

(S) PP $x \sim y$. Tada $x - y \in I$, pa $-(x-y) \in I$ odakle $y \sim x$.

(T) PP $x \sim y$, $y \sim z$. Tada $x - y, y - z \in I$, odakle $(x-y)+(y-z) \in I$, tj. $x - z \in I$, te $x \sim z$.

<u>Saglasnost sa operacijom +</u>: PP $x \sim y$, $x' \sim y'$. Tada $x-y,\ x'-y' \in I$, pa $(x-y)+(x'-y') \in I$, tj. $(x+x')-(y+y') \in I$, dakle $x+x' \sim y+y'$.

<u>Saglasnost sa operacijom $\cdot$</u> PP $x \sim y$, $x' \sim y'$. Tada za neke $i,j \in I$ $x-y=i$, $x'-y'=j$, odakle $xx'-yy' = iy'+jy+ij$. S obzirom da je $iy'+jy+ij \in I$ sledi $xx'-yy' \in I$, tj. $xx' \sim yy'$.

Dakle, postoji količnički prsten $\mathbb{P}/\sim = (P/\sim, +, \cdot, \mathbb{0}, \mathbb{1})$ gde $x/\sim + y/\sim \overset{\text{def}}{=} (x+y)/\sim$, $x/\sim \cdot y/\sim = (xy)/\sim$, $\mathbb{0} = \{x \in P \mid x \sim 0\} = I$

$\mathbb{1} = \{x \in P \mid x \sim 1\} = \{x \in P \mid \text{za neki } i \in I,\ x = i+1\} = I+1$.

Pri tome, kanonsko preslikavanje $k : P \to P/\sim$, $k : x \mapsto x/\sim$, $x \in P$ je homomorfizam.

Primetimo da je za $x \in P$, $x/\sim = \{y \in P \mid y \sim x\} = \{y \in P \mid y-x \in I\} = \{y \in P \mid \bigvee_{i \in I} y-x=i\} = \{y \in P \mid \bigvee_{i\in I} y = i+x\} = I+x$.

Dakle, $x/\sim = I+x$, pa $P/\sim = \{I+x \mid x \in P\}$. Zato skup $P/\sim$ obeležavamo sa P/I, a prsten $\mathbb{P}/\sim$ sa $\mathbb{P}/I$.

Prema ovim oznakama, vidimo da je

$$(I+x)+(I+y) = I+(x+y), \quad (I+x)\cdot(I+y) = I+(xy),$$

$$k(x) = I+x, \ x \in P.$$

S obzirom da je algebra $\mathbb{P}/I$ homomorfna slika prstena $\mathbb{P}$, biće i $\mathbb{P}/\sim$ takođe prsten. Inače operacije u $\mathbb{P}/I$ (odnosno $\mathbb{P}/\sim$) dobro su definisane prema teoremi o kongruencijama i količničkim algebrama.

13.1. <u>Primer</u> $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. Izomorfizam je $\sigma : x \mapsto I+x$, $x \in \mathbb{Z}_n$.

13.2. <u>Teorema</u> Neka je I maksimalni ideal prstena $\mathbb{P}$. Tada je $\mathbb{P}/I$ polje.

<u>Dokaz</u> Neka je $I+x \in P/I$, $I+x \neq \mathbb{0}$, tj. $I+x \neq I$. Tada $x \notin I$, pa je $\langle I, x\rangle = \langle I \cup \{x\}\rangle = P$, tj. $1 \in \langle I, x\rangle$. Dakle, za neke $i \in I$, $p \in P$, $1 = i+px$, odakle $k(1) = k(i)+k(p)k(x)$, tj.

$1 = 0 + (I+p)\cdot(I+x)$. Prema tome, inverzan za $I+x$ je $I+p$. ■

13.3 Posledica Ako je $p \in Prost$, tada je $\mathbb{Z}_p$ polje.

13.4. Posledica Ako je $g \in \mathbb{F}[x]$ nesvodljiv ($\mathbb{F}$ je polje), tada je $\mathbb{F}[x]/(g)$ polje.

13.5 Zadatak Neka su $\mathbb{P}$ i $\mathbb{P}'$ prsteni i neka je $h : \mathbb{P} \to \mathbb{P}'$! Dalje neka je $\ker h \overset{def}{=} \{x \in P \mid hx = 0\}$. Dokazati da je $\ker h$ ideal prstena $\mathbb{P}$ i da $\mathbb{P}'$ sadrži izomorfnu sliku prstena $\mathbb{P}/\ker h$. (uputstvo: primeniti teoremu o razlaganju homomorfizma).

13.6. Zadatak. Neka je $\mathcal{K}$ skup svih kongruencija prstena $\mathbb{P}$ i $\mathcal{J}$ skup svih ideala prstena $\mathbb{P}$. Neka su $\alpha : \mathcal{K} \to \mathcal{J}$ i $\beta : \mathcal{J} \to \mathcal{K}$ definisani na sledeći način:

$\alpha(\sim) = \{x \in P \mid x \sim 0\}$,

$\beta(I) = \sim$, gde $x \sim y$ akko $x - y \in I$.

Dokazati da su α i β uzajamno inverzne bijekcije.

13.7. Zadatak Dokazati da je svaki pravi ideal I prstena $\mathbb{P}$ sadržan u nekom maksimalnom idealu.
Uputstvo: primeniti Zornovu lemu na parcijalno uređen skup $(\mathcal{P}, \subseteq)$, gde $\mathcal{P} = \{J \subseteq P \mid J$ je ideal prstena $\mathbb{P}, I \subseteq J\}$.

13.8. Zadatak 1° $\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}(\sqrt{2})$

2° $\mathbb{Z}_2/(x^2+x+1) = \mathbb{F}$, gde je $\mathbb{F}$ polje iz Primera 2.e.

13.9 Zadatak Dokazati da postoji polje od 8 elemenata.

14. Kronekerova teorema

Polinom x^2-2 nema korena u polju $\mathbb{Q}$, niti polinom x^2+x+1 nema korena u polju $\mathbb{Z}_2$. S druge strane (primeri 13.8) pokazuju da polja $\mathbb{Q}$ i $\mathbb{Z}_2$ imaju ekstenzije u kojima ovi polinomi imaju korene. Kronekerova teorema utvrđuje ovu činjenicu za proizvoljna polja i proizvoljne polinome stepena ≥ 1.

14.1. <u>Teorema</u> (Kronecker) Neka je $\mathbb{F}$ polje i $f \in \mathbb{F}[X]$, $\deg f \geq 1$. Tada postoji ekstenzija $\mathbb{E} \supseteq \mathbb{F}$ takva da polinom f ima koren u $\mathbb{E}$.

<u>Dokaz</u>: Prema teoremi 10.7 polinom f ima nesvodljiv faktor g, $\deg g \geq 1$, ili je f sam nesvodljiv (tada $g = f$). Dovoljno je da dokažemo da g ima koren u nekoj ekstenziji. Prema Posledici 13.4. $\mathbb{F}[X]/(g)$ je polje. Neka je $k : \mathbb{F}[X] \to \mathbb{F}[X]/(g)$ kanonski homomorfizam.

1° $k|_{\mathbb{F}}$ je utapanje polja $\mathbb{F}$ u $\mathbb{F}[X]$:

Zaista, neka su $c, c' \in \mathbb{F}$ i pp $k(c) = k(c')$.

Tada $(g)+c = (g)+c'$, odakle $c-c' \in (g)$, tj. $g \mid c-c'$.

Kako je $\deg g \geq 1 > \deg(c-c')$, to $c-c' = 0$, tj. $c = c'$.

Prema tome, bez gubljenja opštosti možemo smatrati da je $\mathbb{F}$ podpolje polja $\mathbb{F}[X]/(g)$, pa i da je svaki polinom nad $\mathbb{F}$ istovremeno polinom nad $\mathbb{F}[X]/(g)$.

2° Polinom $g(X)$ ima koren u polju $\mathbb{F}[X]/(g)$.

Neka je $g(X) = g_0 + g_1 X + \cdots + g_n X^n$. S obzirom na primedbu na kraju paragrafa 1°, $k(g_i) = g_i$.

Dalje, kako je $g \in (g)$, to $k(g) = 0$. Dakle, (k je hom.)

$$0 = k(g(x)) = k(g_0 + g_1 X + \cdots + g_n X^n) = g_0 + g_1 k(x) + \cdots + g_n k(x)^n$$

tj. $k(x)$ je koren polinoma $g(x)$ u $\mathbb{F}[X]/\mathbb{F}$. $\blacksquare$

Primetimo da je $k(x) = I + x$.

14.2. <u>Zadatak</u>. (Teorema o prenosu, odnosno identifikaciji struktura). Neka su $\mathbb{P}$ i $\mathbb{K}$ prsteni i neka je $\alpha : \mathbb{P} \to \mathbb{K}$ utapanje. Dokazati da postoje prsteni $\mathbb{P}'$ i $\mathbb{K}'$ i izomorfizmi β i γ takvi da sledeći dijagrami komutiraju:

(1)
$$\begin{tikzcd} \mathbb{K}' \arrow[d, phantom, "\cup"] & \\ \mathbb{P} \arrow[r, "\alpha"'] & \mathbb{K} \arrow[ul, "\beta"', "\cong"] \end{tikzcd}$$

(2)
$$\begin{tikzcd} & \mathbb{P}' \arrow[d, phantom, "\cap"] \\ \mathbb{P} \arrow[ur, "\gamma", "\cong"'] \arrow[r, "\alpha"'] & \mathbb{K} \end{tikzcd}$$

14.3. <u>Teorema</u> Neka je $g \in \mathbb{F}[x]$ nesvodljiv polinom, i neka je $\deg g = n$. Tada $|\mathbb{F}[x]/(g) : \mathbb{F}| = n$.

<u>Dokaz</u> Dokazujemo da $a_0 = I+1$, $a_1 = I+x$, ..., $a_{n-1} = I + x^{n-1}$, $I = (g)$, čine bazu vektorskog prostora $\mathcal{F} = ((\mathbb{F}[x]/(g), +, 0), \mathbb{F}, \cdot)$.
Proizvoljan vektor u ovom prostoru oblika je $k(f)$, gde $f \in \mathbb{F}[x]$, $k : \mathbb{F}[x] \longrightarrow \mathbb{F}[x]/(g)$ je kanonski homomorfizam. Prema Lemi o ostatku za polinome postoje $q, r \in \mathbb{F}[x]$ takvi da je $f = q \cdot g + r$, $\deg r < n$. Neka je $r(x) = r_0 + r_1 x + \dots + r_{n-1} x^{n-1}$.

S obzirom da je $g \in (g)$, imamo $k(g) = \mathbb{O}$, pa

$$k(f) = k(q \cdot g + r) = k(q)\, k(g) + k(r) = k(r)$$
$$= r_0 + r_1 k(x) + \dots + r_{n-1} k(x)^{n-1}$$

Kako je $k(x^i) = I + x^i = a_i$, to je $k(f) = a_0 r_0 + a_1 r_1 + \dots + a_{n-1} r_{n-1}$, tj. vektori $a_0, a_1, \dots, a_{n-1}$ generišu prostor $\mathcal{F}$, dakle

(1) $\dim \mathcal{F} \leq n$.

Dokažimo da su vektori $a_0, a_1, \dots, a_{n-1}$ linearno nezavisni
Neka su $r_0, r_1, \dots, r_{n-1} \in F$ i pp $r_0 a_0 + r_1 a_1 + \quad + r_{n-1} a_{n-1} = \mathbb{O}$.
Primetimo da je $\mathbb{O} = (g)\ (= I)$ i s obzirom da smo za $c \in F$ c identifikovali sa $I + c$, to je
$(I + r_0)(I+1) + \dots + (I + r_{n-1})(I + x^{n-1}) = I$, tj.
$(I + r_0) + \dots + (I + r_{n-1} x^{n-1}) = I$, pa $I + (r_0 + r_1 x + \quad + r_{n-1} x^{n-1}) = I$.
Odatle sledi $r_0 + r_1 x + \quad + r_{n-1} x^{n-1} \in I = (g)$, tj. $g \mid r_0 + r_1 x + \dots + r_{n-1} x^{n-1}$.

Ali $\deg g = n > \deg (r_0 + \dots + r_{n-1} x^{n-1})$, pa je $r_0 + r_1 x + \dots + r_{n-1} x^{n-1}$ 0-polinom, tj. $r_0 = r_1 = \dots = r_{n-1} = 0$.
Dakle, $a_0, a_1, \dots, a_{n-1}$ su linearno nezavisni vektori prostora $\mathcal{F}$, pa

(2) $\dim \mathcal{F} \geq n$.

Iz (1) i (2) sledi $\dim \mathcal{F} = n$, tj. $|\mathbb{F}[x]/(g) : \mathbb{F}| = n$.

14.4. <u>Primer</u> 1° $|\mathbb{Q}[x]/(x^2-2) : \mathbb{Q}| = 2$, 2° $|\mathbb{Z}_2[x]/(x^2+x+1) : \mathbb{Z}_2| = 2$
3° $|\mathbb{R}[x]/(x^2+1) : \mathbb{R}| = 2$.

15. Algebarska raširenja

Neka su $\mathbb{F}$ i $\mathbb{K}$ polja, $\mathbb{F} \subseteq \mathbb{K}$.

15.1. $\mathbb{K}$ je konačno raširenje polja $\mathbb{F}$ akko je $|\mathbb{K}:\mathbb{F}| < \infty$.

15.2. $a \in K$ je algebarski element nad $\mathbb{F}$ akko postoji $p \in \mathbb{F}[x]$ tako da je $p(a)=0$.

15.3. Raširenje $\mathbb{K}$ je algebarsko raširenje polja $\mathbb{F}$ akko je svaki $a \in K$ algebarski element nad $\mathbb{F}$.

Primer: 1° $\sqrt{2}$ je algebarski element nad $\mathbb{Q}$. Bude smo uzeli, naprimer, $\mathbb{F} = \mathbb{Q}$, $\mathbb{K} = \mathbb{R}$.

2° $\mathbb{Q}(\sqrt{2})$ je algebarsko raširenje polja $\mathbb{Q}$, jer je svaki $\alpha + \beta\sqrt{2}$, $\alpha, \beta \in \mathbb{Q}$, algebarski nad $\mathbb{Q}$ (jeste rešenje neke kvadratne jednačine).

3° $\mathbb{R}$ nije algebarsko raširenje polja $\mathbb{Q}$, jer $\pi \in \mathbb{R}$ nije algebarski broj nad $\mathbb{Q}$.

15.4. Teorema Ako je $\mathbb{K}$ konačno raširenje polja $\mathbb{F}$, onda je $\mathbb{K}$ algebarsko raširenje polja $\mathbb{F}$.

Dokaz P.P. $|\mathbb{K}:\mathbb{F}| < \infty$ i neka je $\alpha \in K$. $(K, +, 0)$ je vektorski prostor nad $\mathbb{F}$ i to konačne dimenzije. Dakle $1, \alpha, \alpha^2, \alpha^3, \ldots$ je linearno zavisan niz vektora pa za neke $a_0, a_1, \ldots, a_n \in F$, $a_n \neq 0$, $n \geq 1$, $a_0 \cdot 1 + a_1 \cdot \alpha + \cdots + a_n \cdot \alpha^n = 0$. Dakle, α je koren polinoma $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, $p \in \mathbb{F}[x]$. ▨

15.5. Minimalni polinom Neka je $\mathbb{F} \subseteq \mathbb{K}$, i pretpostavimo da je $\alpha \in K$ algebarski nad $\mathbb{F}$. Tada postoji $p \in \mathbb{F}[x]$ tako da je $p(\alpha)=0$. Prema Principu najmanjeg elementa za $\mathbb{N}$, postoji polinom $m \in \mathbb{F}[x]$ najmanjeg stepena tako da je $m(\alpha)=0$. Možemo pretpostaviti da je m moničan.
Primetimo da za m važi:

$\alpha \in F \Rightarrow m(x) = x - \alpha$

$\alpha \notin F \Rightarrow \deg m \geq 2$.

15.6 Teorema (Osobine minimalnog polinoma). Neka je $\mathbb{F} \subseteq \mathbb{K}$, $\alpha \in K$ je algebarski nad $\mathbb{F}$ i neka je m minimalni polinom za α. Tada:

1° m je nesvodljiv nad $\mathbb{F}$.

2° Ako je $p \in \mathbb{F}[x]$ i $p(\alpha)=0$, onda $m(x) | p(x)$

3° $F[\alpha] = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \dots, a_{n-1} \in F\}$, $n = \deg m$, je polje (podpolje polja K).

4° $|\mathbb{F}[\alpha] : \mathbb{F}| = n = \deg m$.

Dokaz 1° PP m je svodljiv. Tada postoje $g_1, g_2 \in \mathbb{F}[x]$, takvi da je $m = g_1 \cdot g_2$, $\deg g_1, \deg g_2 < \deg m$. Kako je $m(\alpha) = 0$, to $g_1(\alpha) = 0$ ili $g_2(\alpha) = 0$ što je kontradikcija prema izboru polin. m.

2° Neka je $p \in F[x]$, $p(\alpha) = 0$ i neka su prema lemi o ostatku
$p = q m + r$, $\deg r < \deg m$, $q, r \in F[x]$.
Tada $p(\alpha) = q(\alpha) m(\alpha) + r(\alpha)$, pa $r(\alpha) = 0$, pa je prema izboru polin. m i $\deg r < \deg m$, $r = 0$.

3° Neka je $\deg m = n$. Tada $\mathbb{F} \subseteq \mathbb{F}(\alpha) \subseteq \mathbb{K}$, gdje je $F(\alpha)$ polje (vrijednosti) racionalnih izraza za $x = \alpha$. Dakle, elementi $F(\alpha)$ su oblika $p(\alpha)/q(\alpha)$, gdje su $p, q \in F[x]$, $q(\alpha) \neq 0$.

(a) $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ su linearno nezavisni vektori prostora $(F(\alpha), +, \cdot)$ nad $\mathbb{F}$. Pretpostavimo suprotno, da su ovi vektori linearno zavisni. Tada postoje $a_0, a_1, \dots, a_{n-1} \in F$, nisu svi $a_0, \dots, a_{n-1}$ jednaki nuli, i $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} = 0$.
Dakle, $p(\alpha) = 0$ gdje $p(x) = a_0 + a_1 x + \dots + a_{n-1}x^{n-1}$ i $\deg p < \deg m$, #.

Otuda $|\mathbb{F}(\alpha) : \mathbb{F}| \geq n$.

(b) $F[\alpha]$ je polje, tj. $F[\alpha] = F(\alpha)$.
Očigledno $u, v \in F[\alpha] \Rightarrow u + v \in F[\alpha]$.
S obzirom da je $\alpha^n = -m_0 - m_1\alpha - \dots - m_{n-1}\alpha^{n-1}$
to $\alpha^n \in \mathcal{L}_F(1, \alpha, \dots, \alpha^{n-1})$. Množenjem ove jednakosti i supstitucijom α^n linearnom kombinacijom elemenata $1, \alpha, \dots, \alpha^{n-1}$ u novodobijenoj jednakosti, vidimo da je $\alpha^{n+1} \in \mathcal{L}_F(1, \alpha, \dots, \alpha^{n-1})$. Slično $\alpha^{n+2}, \alpha^{n+3}, \dots \in \mathcal{L}_F(1, \alpha, \dots, \alpha^{n-1})$.
Dakle, $u, v \in F[\alpha] \Rightarrow u \cdot v \in F[\alpha]$.
Neka je $u \in F[\alpha]$, $u \neq 0$, $u = u_0 + u_1\alpha + \dots + u_{n-1}\alpha^{n-1}$.
Tada $\deg u < \deg m$ i m je nesvodljiv, dakle $(u, m) = 1$.
Prema Bezuovoj teoremi postoje $p, q \in F[x]$ takvi da je
$$u(x) \cdot p(x) + m(x) \cdot q(x) = 1.$$
za $x = \alpha$ nalazimo $u(\alpha) \cdot p(\alpha) = 1$, pa je $p(\alpha) = u(\alpha)^{-1}$.

(c) Iz (b) slijedi $F(\alpha) = \mathcal{L}_F(1, \alpha, \dots, \alpha^{n-1})$, pa $|F(\alpha) : F| \leq n$, čime je dokazano 4°.

15.7 Posledice 1° Ako $p, q \in F[x]$, $\deg p, \deg q < \deg m$ i $p(\alpha) = q(\alpha)$ onda $p = q$ (m je min. polin. za α).

2° Ako je $\mathbb{F} \subseteq \mathbb{K}$, $\alpha \in K$ je algebarni nad $\mathbb{K}$, tada $|\mathbb{F}(\alpha) : \mathbb{F}| < \infty$.

15.8 Primer 1° Za $n \geq 2$, $x^n - 2$ je nesvodljiv nad $\mathbb{Q}$ (prema Ajzenštajnovom kriterijumu), dakle $x^n - 2$ je minimalni polinom za $\sqrt[n]{2}$ (zašto?). Otuda $|\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}| = n$.

2° $1 + x + \dots + x^{p-1}$, $p \in Prost$, je nesvodljiv, pa je ovaj polinom minimalan za $\varepsilon = e^{\frac{2\pi i}{p}}$. Otuda $|\mathbb{Q}(\varepsilon) : \mathbb{Q}| = p - 1$.

15.9.* Zadatak Neka je $\varepsilon = e^{\frac{2\pi i}{n}}$. Dokazati da je $|\mathbb{Q}(\varepsilon) : \mathbb{Q}| = \varphi(n)$, gde je $\varphi(n)$ Ojlerova funkcija.

15.10. Zadatak. a) Dokazati da je $a = 1 + \sqrt{2} + \sqrt{3}$ algebarni broj. b) Odrediti $|\mathbb{Q}(a) : \mathbb{Q}|$

c) Racionalisati izraz $\frac{1}{1+\sqrt{2}+\sqrt{3}}$ (tj: osloboditi se "korena" u imeniocu).

16. Kronekerova teorema ("originalni" Kronekerov dokaz).

Kroneker je bio motivisan u dokazu svoje teoreme izvođenjem iz prethodnog paragrafa.

16.1. Dakle, neka je $p \in F[x]$ nesvodljiv polinom. Treba konstruisati polje $\mathbb{K} \supseteq \mathbb{F}$ u kojem p ima koren. Pretpostavimo da je p moničan. Ako je $\deg p = 1$, onda $p(x) = x - \alpha$ za neki $\alpha \in F$, pa $\mathbb{K} = \mathbb{F}$.

Neka je $n = \deg p \geq 2$ i neka je ξ novi simbol konstante.

Dalje, neka je $K = \{a_0 + a_1\xi + \dots + a_{n-1}\xi^{n-1} \mid a_0, \dots, a_{n-1} \in F\}$

skup formalnih polinoma nad ξ.

U skupu K uvedimo operacije $+_p$ i $\cdot_p$ po modulu polinoma p, slično kako se uvode operacije $+_n$ i $\cdot_n$ u prstenu ostataka (mod n) u $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$. Dakle, za $f, g \in K$

$f +_p g \overset{def}{=} f + g$ (nema potrebe uzimati $rest(f+g, p)$, s obzirom da je $\deg(f+g) < n$).

$f \cdot_p g \overset{def}{=} rest(f(x)g(x), p(x))(\xi)$

16.2. Teorema (Kroneker) Neka su oznake kao u 16.1. $\mathbb{K}$ je polje i $\mathbb{K}$ je raširenje polja $\mathbb{F}$. ξ je koren polinoma $p(x)$ u polju $\mathbb{K}$.

Dokaz 1° $\mathbb{K} = (K, +_p, \cdot_p, 0, 1)$ je prsten.

Neka je $\varrho : \mathbb{F}[x] \longrightarrow K$, $\varrho(f) = \operatorname{rest}(f, p)(\xi)$, $f \in F[x]$.
Dokazujemo da je ϱ epimorfizam prstena $\mathbb{F}[x]$ na $\mathbb{K}$.

a) Očigledno je ϱ preslikavanje na.

b) $\varrho(f+g) = \varrho(f) +_p \varrho(g)$, $f, g \in F[x]$.

Neka su $r_1, r_2 \in F[x]$ prema Lemi o ostatku takvi da je

$$f = q_1 p + r_1, \ \deg r_1 < \deg p \ ; \ g = q_2 p + r_2, \ \deg r_2 < p.$$

Tada $r_1(\xi) = \varrho(f)$ i $r_2(\xi) = \varrho(g)$. Dalje,

$$f+g = (q_1 + q_2)p + r_1 + r_2 \quad i \quad \deg(r_1 + r_2) < \deg p,$$

te prema Lemi o ostatku, delu koji se odnosi na jedinstvenost ostatka, sledi $r_1(\xi) +_p r_2(\xi) = \operatorname{rest}(f+g, p)(\xi) = \varrho(f+g)$, dakle

$$\varrho(f+g) = r_1(\xi) +_p r_2(\xi) = \varrho(f) +_p \varrho(g).$$

c) $\varrho(fg) = \varrho(f) \cdot_p \varrho(g)$.

Dokaz je sličan dokazu u (b). Uz iste oznake kao u (b) i uzimajući $r = \operatorname{rest}(r_1 r_2, p)$, tj. $r_1 r_2 = qp + r$, $\deg r < \deg p$, nalazimo $fg = p(q_1 q_2 p + q_1 r_2 + q_2 r_1 + q) + r$, $\deg r < \deg p$.

Dakle, prema Lemi o ostatku, $r = \operatorname{rest}(fg, p)$, pa

$$\varrho(fg) = \operatorname{rest}(fg, p)(\xi) = r(\xi) = \operatorname{rest}(r_1 r_2, p)(\xi)$$
$$= r_1(\xi) \cdot_p r_2(\xi) = \varrho(f) \cdot_p \varrho(g).$$

Dakle, $\varrho : \mathbb{F}[x] \xrightarrow{na} \mathbb{K}$, tj. $\mathbb{K}$ je homomorfna slika prstena $\mathbb{F}[x]$, čime je, prema Teoremi o zatvorenosti algebarskih varijeteta za homomorfne slike, 1° dokazano.

2° $p(\xi) = 0$ u $\mathbb{K}$.

Najpre primetimo da je za $p(x) = p_0 + p_1 x + \cdots + p_n x^n$:

a) $\operatorname{rest}(x, p) = x$ jer $\deg p \geq 2$, pa $\varrho(x) = \xi$.

b) $x^n = 1 \cdot p(x) + (-p_0 - p_1 x - \cdots - p_{n-1} x^{n-1})$, $\deg(-p_0 - p_1 x - \cdots - p_{n-1} x^{n-1}) < \deg p$,
pa $\operatorname{rest}(x^n, p) = -p_0 - p_1 x - \cdots - p_{n-1} x^{n-1}$.

Koristeći da je ϱ homomorfizam, za $\xi^n = \xi \cdot_p \xi \cdot_p \cdots \cdot_p \xi$ nalazimo

$$\xi^n = \varrho(x)^n = \varrho(x^n) = \mathrm{rest}\,(x^n, p)(\xi) = -p_0 - p_1 \cdot_p \xi - \cdots - p_{n-1} \cdot_p \xi^{n-1}$$

odakle $\quad \xi^n +_p p_{n-1} \cdot_p \xi^{n-1} +_p \cdots +_p p_1 \cdot_p \xi +_p p_0 = 0.$

Ovim je 2° dokazano.

3° $\mathbb{K}$ je polje.

Neka je $r(\xi) \in K \setminus \{0\}$. Tada $\deg r(x) < \deg p(x)$.

Polinom $p(x)$ je nesvodljiv nad $\mathbb{F}$, te $(r(x), p(x)) = 1$. Odatle prema Bezuovoj teoremi postoje $u, v \in \mathbb{F}[x]$ tako da je $u(x)r(x) + v(x)p(x) = 1$, pa primenom homomorfizma ϱ na ovu jednakost, nalazimo $u(\xi) \cdot_p r(\xi) +_p v(\xi) \cdot_p p(\xi) = 1$.

Prema 2°, $p(\xi) = 0$ te $u(\xi) \cdot_p r(\xi) = 1$. Dakle $u(\xi)$ je inverzan element za $r(\xi)$, te je ovim 2° dokazano.

4° Ako je $c \in F$, onda $c = c + 0\cdot\xi + \cdots + 0\cdot\xi^{n-1}$, pa $c \in F$.

S obzirom da je za $a, b \in F$, $a +_F b = a +_p b$ i $a \cdot_F b = a \cdot_p b$, to je $\mathbb{K}$ raširenje polja $\mathbb{F}$. ∎

16.3. <u>Primer</u> 1° Kronekerova konstrukcija za polje $\mathbb{F} = \mathbb{Z}_2$ i polinom $p(x) = 1 + x + x^2$. $\deg p = 2$, pa $K = \{a + b\xi \mid a, b \in \mathbb{Z}_2\}$ tj.

$K = \{0, 1, \xi, 1+\xi\}$. Tada

$+_p$	0	1	ξ	$1+\xi$
0	0	1	ξ	$1+\xi$
1	1	0	$1+\xi$	ξ
ξ	ξ	$1+\xi$	0	1
$1+\xi$	$1+\xi$	ξ	1	0

$\cdot_p$	0	1	ξ	$1+\xi$
0	0	0	0	0
1	0	1	ξ	$1+\xi$
ξ	0	ξ	$1+\xi$	1
$1+\xi$	0	$1+\xi$	1	ξ

$1 +_p \xi +_p \xi^2 = 0$

$\mathbb{K} = \mathbb{Z}_2(\xi)$.

2° Kronekerova konstrukcija za polje $\mathbb{F} = \mathbb{R}$ i polinom $p(x) = 1 + x^2$. $\deg p = 2$, pa $C = K = \{a + bi \mid a, b \in R\}$, za novi simbol konstante i (umesto ξ biramo i). Tada $C = \{x + iy \mid x, y \in R\}$ i za $x_1, x_2, y_1, y_2 \in R$

$$(x_1 +_R y_1 i) +_p (x_2 +_R i y_2) = (x_1 +_R x_2) + i(y_1 +_R y_2)$$

$$(x_1 +_R i y_1) \cdot_p (x_2 +_R i y_2) = (x_1 x_2 - y_1 y_2) + i(x_1 \cdot_R y_2 +_R x_2 \cdot_R y_1), \quad i^2 +_p 1 = 0$$

Dakle, $\mathbb{C} = \mathbb{R}(i)$ je polje kompleksnih brojeva, odnosno $\mathbb{C}$ je izomorfno polju kompleksnih brojeva ako je polje kompl. brojeva drugačije definisano.

16.4. <u>Konvencija o oznakama</u>. 1° Ako je p nesvodljiv polinom nad $\mathbb{F}$ i $\mathbb{K}$ je polje određeno Kronekerovom konstrukcijom (odeljak 16) uz pomoć novog simbola konstante ξ, često koristimo oznaku $\mathbb{K}=\mathbb{F}(\xi)$.

2° U Kronekerovoj konstrukciji pojavljuju se operacije $+_{\mathbb{F}}, \cdot_{\mathbb{F}}$ polja $\mathbb{F}$ i operacije $+_p, \cdot_p$ polja $\mathbb{K}=\mathbb{F}(\xi)$ koje su ekstenzije operacija polja $\mathbb{F}$. Otuda se koriste jedinstvene oznake $+, \cdot$ za operacije i polja $\mathbb{F}$ i polja $\mathbb{K}$.

3° Ako je $\mathbb{F}$ podpolje polja $\mathbb{E}$, to znači da je $\mathbb{F}\subseteq\mathbb{E}$. Na mnogim mestima koristi se i oznaka $\mathbb{E}/\mathbb{F}$. Na primer fraza "Neka je $\mathbb{E}/\mathbb{F}$ algebarsko raširenje" znači da je $\mathbb{F}\subseteq\mathbb{E}$ i da je svaki $a\in E$ algebarski element nad $\mathbb{F}$.

16.5. <u>Teorema</u> Neka je $\mathbb{F}$ polje i neka je $p\in\mathbb{F}[x]$ nesvodljiv, $\deg p=n$. Dalje, neka su $\mathbb{K}'$ i $\mathbb{K}''$ raširenja polja $\mathbb{F}$ i neka su $\alpha\in K'$, $\beta\in K''$ takvi da je $\mathbb{K}'=\mathbb{F}(\alpha)$ i $\mathbb{K}''=\mathbb{F}(\beta)$, $p(\alpha)=0$ u $\mathbb{K}'$ i $p(\beta)=0$ u $\mathbb{K}''$. Tada postoji izomorfizam $\sigma:\mathbb{K}'\cong\mathbb{K}''$ tako da je $\sigma\restriction F=i_F$. (i_F je identično preslikavanje domena $\mathbb{F}$).

$$\begin{array}{ccc} \mathbb{F}(\alpha)=\mathbb{K}' & \xrightarrow{\sigma} & K''=\mathbb{F}(\beta) \\ \rotatebox{-45}{$\supseteq$} & & \rotatebox{-135}{$\supseteq$} \\ & \mathbb{F} & \end{array}$$

– komutativan dijagram

<u>Dokaz</u> Neka je $\mathbb{K}=\mathbb{F}(\xi)$ Kronekerovo polje za polinom p i neka je $\sigma:\mathbb{K}'\longrightarrow\mathbb{K}$ definisano pomoću

$$\sigma(f(\alpha))=f_0+f_1\xi+\cdots+f_{n-1}\xi^{n-1}, \quad f(x)\in F[x],\ \deg f<\deg p=n.$$

Dakle, $\sigma(f(\alpha))=f(\xi)$ za $f(x)\in\mathbb{F}[x]$, $\deg f\le n-1$.

a) Polinom p je minimalni polinom za α u K' i p je minimalni polinom za β u $\mathbb{K}''$. Dakle, prema Teoremi 15.6, preslikavanje σ je dobro

b) Prema Kronekerovoj konstrukciji, $\mathbb{K}=\mathbb{F}(\xi)=\{f(\xi)\mid f(x)\in\mathbb{F}[x],\ \deg f\le n-1\}$, dakle σ je preslikavanje <u>na</u>.

c) σ je 1-1 jer iz $\sigma(f(\alpha))=\sigma(g(\alpha))$ sledi $f(\alpha)=g(\alpha)$ ($\deg f, \deg g<n$) pa prema Posledici 15.7.1° sledi $f(x)=g(x)$.

d) σ je homomorfizam:

$\sigma(f(\alpha)+g(\alpha))=\sigma((f+g)(\alpha))=(f+g)(\xi)=f(\xi)+g(\xi)=\sigma(f)+\sigma(g)$.

Neka su $f,g\in\mathbb{F}[x]$, $r=\mathrm{rest}(fg,p)$. Tada $f(\alpha)g(\alpha)=p(\alpha)q(\alpha)+r(\alpha)$, $\deg r<n$, pa $f(\alpha)g(\alpha)=r(\alpha)$ jer $p(\alpha)=0$. Otuda

$\sigma(f(\alpha)g(\alpha))=\sigma((fg)(\alpha))=\sigma(r(\alpha))=r(\xi)=\mathrm{rest}(fg,p)(\xi)=f(\xi)\cdot_p g(\xi)=\sigma(f(\alpha))\cdot_p\sigma(g(\alpha))$.

Dakle, $\mathbb{F}(\alpha) \cong \mathbb{K} \cong \mathbb{F}(\beta)$.

Dalje, za $c \in F$, $\sigma(c) = c$, pa $\sigma \restriction F = i_F$. ∎

16.6. <u>Zadatak</u> Neka je $\sigma : \mathbb{F} \cong \mathbb{F}'$, $\mathbb{F}$ i $\mathbb{F}'$ su polja. Za $f \in \mathbb{F}[x]$, $f(x) = f_0 + f_1 x + \cdots + f_n x^n$, korespodentni polinom je $f' = \sigma(f)$, $f'(x) = f_0' + f_1' x + \cdots + f_n' x^n$, gde $f_i' = \sigma(f_i)$, $i \le n$. Tada je $f' \in F'[x]$. Dokazati:

1° f je nerastavljiv nad $\mathbb{F}$ akko je f' nerastavljiv nad $\mathbb{F}$!

2° Ako je $f = gh$ za neke $g, h \in F[x]$, tada je $f' = g' \cdot h'$!

16.7. <u>Zadatak</u> Neka je $\sigma : \mathbb{F} \cong \mathbb{F}'$, $\mathbb{F}$ i $\mathbb{F}'$ su polja. Dalje, neka je $p \in \mathbb{F}[x]$ nesvodljiv polinom nad $\mathbb{F}$ i neka je p' korespodentni nesvodljiv polinom nad $\mathbb{F}'$. Neka su $\mathbb{K} \supseteq \mathbb{F}$, $\mathbb{K}' \supseteq \mathbb{F}'$ raširenja takva

$$\begin{array}{ccc} \mathbb{F}(\alpha) = \mathbb{K} & \overset{\cong}{\underset{\theta}{\dashrightarrow}} & \mathbb{K}' = \mathbb{F}(\beta) \\ \cup & & \cup \\ \mathbb{F} & \overset{\cong}{\underset{\sigma}{\longrightarrow}} & \mathbb{F}' \end{array}$$

da je $\alpha \in K$ koren polin. $p(x)$ u $\mathbb{K}$ i $\beta \in K'$ je koren polin. $p(x)$ u $\mathbb{K}'$ i $\mathbb{K} = \mathbb{F}(\alpha)$, $\mathbb{K}' = \mathbb{F}'(\beta)$.

Dokazati da postoji $\theta : \mathbb{K} \cong \mathbb{K}'$, $\theta \restriction F = \sigma$.

17. <u>Korensko polje (faktorsko polje) polinoma.</u>

17.1. <u>Definicija</u> Neka su $\mathbb{F} \subseteq \mathbb{E}$ polja i neka je $f \in \mathbb{F}[x]$, $\deg f \ge 1$.

$\mathbb{E}$ je <u>korensko polje</u> polinoma f akko

1° f ima faktorizaciju na linearne faktore, tj. za neke $a_1, \dots, a_n \in E$
$f(x) = c \cdot (x - a_1) \dots (x - a_n)$, $c \in F$.

2° Ni u jednom međupolju $\mathbb{L}$ (tj. $\mathbb{F} \subsetneq \mathbb{L} \subsetneq \mathbb{E}$), $f(x)$ se ne može rastaviti na linearne faktore.

17.2. <u>Teorema</u> Neka je $\mathbb{F}$ polje i $f \in \mathbb{F}[x]$, $\deg f \ge 1$. Tada f ima korensko polje.

<u>Dokaz</u> Dokaz izvodimo indukcijom po $n = \deg f$. Ako je $\deg f = 1$, tada $f(x) = f_0 + f_1 x = f_1 \cdot (x - a_1)$ gde $a_1 = -f_0/f_1$.
P.P. induktivnu hipotezu i neka je $\deg f = n \ge 2$. Rastavimo polinom f na nesvodljive faktore: $f = p_1 \cdot p_2 \cdots p_k$, $p_1, \dots, p_k \in \mathbb{F}[x]$ su nesvodljivi. Prema Kronekerovoj teoremi postoji polje $\mathbb{K}$ i $a_1 \in K$, $\mathbb{K} = F(a_1)$ i a_1 je koren polinoma $p_1(x)$. Dakle $f(x) = (x - a_1) \cdot g(x)$, $g(x) \in \mathbb{K}[x]$.
$\deg g = n - 1 < n = \deg f$, te prema I.H. g ima korensko polje $\mathbb{E} \supseteq K$, tj. postoje $a_2, \dots, a_n \in E$ takvi da je $g(x) = c \cdot (x - a_2) \cdots (x - a_n)$. Tada $f(x) = c \cdot (x - a_1) \cdots (x - a_n)$ u $\mathbb{E}$ i $\mathbb{F}(a_1, \dots, a_n) \subseteq \mathbb{E}$ (podpolje generisano elementima $a_1, \dots, a_n$) je korensko polje za f. ∎

17.3 Neka je $\mathbb{E} \supseteq \mathbb{F}$ korensko polje polinoma $p \in F[x]$. Tada je $\mathbb{E}$ algebarsko raširenje polja $\mathbb{F}$. Zaista, ako je $p(x) = c \cdot (x-a_1) \cdots (x-a_n)$ faktorizacija polinoma $p(x)$ u $\mathbb{E}$, onda je $\mathbb{E} = \mathbb{F}(a_1, \dots, a_n)$ i svaki a_{i+1} je algebarski nad $\mathbb{F}(a_1, \dots, a_i)$, $0 \le i < n$, pa $|\mathbb{E} : \mathbb{F}| = |\mathbb{F}(a_1, \dots, a_n) : \mathbb{F}(a_1, \dots, a_{n-1})| \cdots |\mathbb{F}(a_1) : \mathbb{F}| < \infty$, dakle tvrđenje važi prema Teoremi 15.4.

17.4. Ako $p(x) \in \mathbb{F}[x]$ ima faktorizaciju $p(x) = c \cdot (x-a_1) \cdots (x-a_n)$ u polju $\mathbb{E} \supseteq \mathbb{F}$, tada je $\mathbb{F}(a_1, \dots, a_n)$ korensko polje polinoma $p(x)$. Zaista:

1° $\mathbb{F}(a_1, \dots, a_n)$ je raširenje polja $\mathbb{F}$ i $p(x)$ ima faktorizaciju u $\mathbb{F}(a_1, \dots, a_n)$ s obzirom da $a_1, \dots, a_n \in F(a_1, \dots, a_n)$

2° Ako je $\mathbb{K}$ međupolje, tj. $\mathbb{F} \le \mathbb{K} \le \mathbb{F}(a_1, \dots, a_n)$ i $p(x)$ ima faktorizaciju u $\mathbb{K}$, onda $a_1, \dots, a_n \in K$, pa s obzirom da je $\mathbb{K}$ polje koje je zatvoreno za vrednosti racionalnih funkcija kada se argumenti biraju K, to $\mathbb{F}(a_1, \dots, a_n) \le K$, dakle $K = \mathbb{F}(a_1, \dots, a_n)$.

Primetimo da je $\mathbb{F}(a_1, \dots, a_n) = \{ f^{\mathbb{E}}(a_1, \dots, a_n) \mid f(x_1, \dots, x_n) \in \mathbb{F}(x_1, \dots, x_n) \}$.

Ali prema Teoremi 15.6.3° takođe

$F(a_1, \dots, a_n) = \{ f^{\mathbb{E}}(a_1, \dots, a_n) \mid f(x_1, \dots, x_n) \in \mathbb{F}[x_1, \dots, x_n] \}$.

17.5. <u>Zadatak</u> Neka je $\mathbb{E}$ korensko polje polinoma $f(x) \in \mathbb{F}[x]$, $\deg f = n$. Dokazati da je $|\mathbb{E} : \mathbb{F}| \le n!$.

17.6. <u>Zadatak</u> Neka je $f(x) \in \mathbb{Q}[x]$ polinom neparnog stepena i neka je $f(x)$ nesvodljiv. Dokazati da se $\mathbb{Q}[x]/(f)$ utapa u polje realnih brojeva $\mathbb{R}$.

17.7.* <u>Zadatak</u> Za polinom $f \in \mathbb{F}[x]$ označimo sa $k(f, \mathbb{F})$ broj korena polinoma f u polju $\mathbb{F}$. Kao što znamo, ako je $f \ne 0$, onda $k(f, \mathbb{F}) \le \deg f$. Neka je $\mathbb{R}$ polje realnih brojeva, $n \in N^+$, $k \in N$, $k < n$ i neka je $h \in \mathbb{R}[x]$, $\deg h = k$, $h \ne 0$

Za polinom $f = x^n + h$ dokazati:

a) Ako je $n \in 2N$ onda $k(f, \mathbb{R}) \le 2[\frac{k}{2}] + 2$.

b) Ako je $n \in 2N+1$ onda $k(f, \mathbb{R}) \le 2[\frac{k+1}{2}] + 1$.

17.8. Odrediti stepen raširenja polja $\mathbb{E} \supseteq \mathbb{Q}$, ako je $\mathbb{E}$ korensko polje polinoma $f \in \mathbb{Q}[x]$: a) $f(x) = x^2 + 2$ b) $f(x) = x^5 - 1$ c) $f(x) = x^3 + x + 1$.

17.9. U ovom paragrafu dokazaćemo da je korensko polje polinoma jedinstveno određeno. Naime, svaka dva korenska polja datog polinoma međusobno su izomorfna. U dokazu ove teoreme koristićemo sledeću lemu.

<u>Lema</u> Neka je $\mathbb{E} \supseteq \mathbb{F}$ korensko polje polinoma $f \in \mathbb{F}[x]$ i neka je $p \in \mathbb{F}[x]$ nesvodljivi faktor polinoma f. Tada postoji $b \in E$ tako da je $p(b)=0$.

<u>Dokaz</u> Polinom p je faktor polinoma f, te postoji $h \in \mathbb{F}[x]$ tako da je $f = ph$. Tada je $p \in E[x]$ takođe, pa neka je $\mathbb{E}(\beta)$ Kroneckerovo raširenje polja $\mathbb{E}$ u kojem je $p(\beta)=0$. Tada $f(\beta)=p(\beta)h(\beta)=0$, te je β koren polinoma f. Ali $\mathbb{E}$ sadrži <u>sve</u> korene polinoma f, dakle $\beta \in E$. Prema tome možemo uzeti $b=\beta$. ☐

<u>Teorema</u> (o jedinstvenosti korenskog raširenja). Neka su $\mathbb{E}, \mathbb{K} \supseteq \mathbb{F}$ korenska polja polinoma $f \in \mathbb{F}[x]$. Tada postoji $\theta : \mathbb{E} \cong \mathbb{K}$ tako da je $\theta | \mathbb{F} = i_F$.

<u>Dokaz</u> Prema dokazu Teoreme 17.2, možemo uzeti da je $E = \mathbb{F}(a_1, \dots, a_n)$ gde su $a_1, \dots, a_n$ koreni polinoma f u $\mathbb{E}$ i da je a_{i+1}, $0 \le i < n$, koren nekog nesvodljivog faktora $p \in \mathbb{F}(a_1, \dots, a_i)$ polinoma f u polju $\mathbb{F}(a_1, \dots, a_i)$. Prema lemi postoji $b_1 \in K$ koji je koren nekog nesvodljivog faktora p_1 polin. f nad $\mathbb{F}$ za koji je $p_1(a_1)=0$ u $\mathbb{F}(a_1)$ i $p_1(b_1)=0$ u $\mathbb{K}$. Primetimo da je $\mathbb{F}(a_1) \subseteq E$ i $\mathbb{F}(b_1) \subseteq \mathbb{K}$. Prema Teoremi 16.5 (o jedinstvenosti Kroneckerove ekstenzije), postoji $\sigma_1 : \mathbb{F}(a_1) \cong \mathbb{F}(b_1)$, $\sigma_1 | \mathbb{F} = i_F$. Slično, a_2 je koren nekog nesvodljivog faktora p_2 polinoma f u $\mathbb{F}(a_1)$. Neka je p_2' korespodentni polinom u odnosu na izomorfizam σ_1, $p_2' \in \mathbb{F}(a_1)[x]$. Tada je p_2' nesvodljivi faktor polinoma f u polju $\mathbb{F}(a_1)$ (vidi Zadatak 16.6), te prema Lemi postoji $b_2 \in K$ tako da je $p_2'(b_2)=0$. Tada postoji $\sigma_2 : \mathbb{F}(a_1,a_2) \cong \mathbb{F}(b_1,b_2)$ s obzirom na Zadatak 16.7. i $\mathbb{F}(a_1,a_2) = \mathbb{F}(a_1)(a_2)$, i pri tome $\sigma_2 | \mathbb{F}(a_1) = \sigma_1$. Nastavljajući ovaj postupak dobijamo sledeći komutativan dijagram

$$\begin{tikzcd}
 & \mathbb{F}(a_1) \arrow[d, "\sigma_1", "\cong"'] & \subseteq & \mathbb{F}(a_1,a_2) \arrow[d, "\sigma_2", "\cong"'] & \subseteq \cdots \subseteq & \mathbb{F}(a_1,\dots,a_{n-1}) \arrow[d, "\sigma_{n-1}", "\cong"'] & \subseteq & \mathbb{F}(a_1,\dots,a_n) = \mathbb{E} \arrow[d, "\sigma_n", "\cong"'] \\
\mathbb{F} \arrow[ur, phantom, "\subseteq"] \arrow[r, phantom, "\subseteq"] & \mathbb{F}(b_1) & \subseteq & \mathbb{F}(b_1,b_2) & \subseteq \cdots \subseteq & \mathbb{F}(b_1,\dots,b_{n-1}) & \subseteq & \mathbb{F}(b_1,\dots,b_n) = \mathbb{K}
\end{tikzcd}$$

$$\sigma_1 \subseteq \sigma_2 \subseteq \dots \subseteq \sigma_n = \theta.$$

Kako je $f(x) = c \cdot (x-a_1) \cdots (x-a_n)$ faktorizacija polin. f u $\mathbb{E}$ i $\sigma_n : E \to \mathbb{K}$ je utapanje, $\sigma_n(a_i) = b_i$, $1 \le i \le n$, to će $f(x) = c'(x-b_1)\cdots(x-b_n)$, $c' = \sigma_n(c)$, biti faktorizacija polinoma f u polju $\mathbb{K}$. Dakle, $\mathbb{F}(b_1, \dots, b_n) \subseteq \mathbb{K}$ je korensko polje polinoma f, pa kako je to i $\mathbb{K}$, sledi $\mathbb{K} = \mathbb{F}(b_1, \dots, b_n)$. ☐

17.10. Primer Neka je p prost broj i $n \in \mathbb{N}^+$. Tada postoji tačno jedno polje (do na izomorfizam) $\mathbb{E}$, $|\mathbb{E}| = p^n$.

Zaista, neka je $f(x) = x^{p^n} - x$, $f \in \mathbb{Z}_p[x]$. Neka je $\mathbb{E}$ korensko polje polinoma f

1° $\mathbb{E}$ je karakteristike p jer $\mathbb{Z}_p \leq \mathbb{E}$.

Neka je $H = \{a \in \mathbb{E} \mid a^{p^n} = a\}$. Tada

2° $|H| = p^n$ jer je H tačno skup svih korena polin. f u $\mathbb{E}$.

3° $H \setminus \{0\}$ je podgrupa multiplikativnog dela $\mathbb{E}^*$ polja $\mathbb{E}$ jer $a, b \in H \Rightarrow ab \in H$, $a \in H, a \neq 0 \Rightarrow a^{-1} \in H$.

Prema Teoremi 4.2 preslikavanje $h(x) = x^p$ je endomorfizam polja E, dakle i $\theta = h^n$ je endomorfizam polja E, tj. u $\mathbb{E}$ važi: $(x+y)^{p^n} = x^{p^n} + y^{p^n}$. Specijalno za $a, b \in H$

$(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b$, tj.

4° $a, b \in H \Rightarrow a + b \in H$.

Prema prethodnom H je podpolje polja $\mathbb{E}$ koje sadrži sve korene polinoma f, tj. H je korensko polje polinoma f, pa $H = E$.

Time je dokazano da postoji polje $\mathbb{E}$ takvo da je $|E| = p^n$.

a) Neka je $\mathbb{K}$ bilo koje polje, $|K| = p^n$. Tada je multiplikativni deo K^* polja $\mathbb{K}$ konačna grupa, dakle $\mathbb{K}^*$ je ciklična (Teorema 2.3) i $|K^*| = p^n - 1$. Neka je $b \in K$ tako da je $\mathbb{K}^* = \langle b \rangle$. Tada važi $b^{p^n - 1} = 1$, tj. $b^{p^n} = b$ pa i za sve $a = b^i$ važi $a^{p^n} = a$. Dakle svaki $a \in K^*$ je koren polinoma $x^{p^n} - x$, a takođe, tj. K je tačno skup svih korena polinoma $x^{p^n} - x$. Kako je $\deg f = p^n$ i $|K| = p^n$ to je onda K korensko polje polinoma f. Prema tome na osnovu jedinstvenosti korenskog polja imamo

b) $\mathbb{K} \cong \mathbb{E}$.

S obzirom na Teoremu 5.12. ovim su opisana sva konačna polja, to su tačno korenska polja polinoma $x^{p^n} - x$ za $p \in Prost$, $n \in \mathbb{N}^+$ nad poljem $\mathbb{Z}_p$.

17.11. Zadatak Neka je p prost broj. Dokazati da postoji beskonačno polje karakteristike p.

18. Polje algebarskih brojeva.

Element $a\in C$ je algebarski broj ako je a koren nekog polinoma $f\in \mathbb{Q}[X]$, $f\neq 0$. Skup algebarskih brojeva je
$A=\{a\in C \mid a \text{ je algebarski broj}\}$.
Dokazaćemo da je A podpolje polja kompleksnih brojeva $\mathbb{C}$. I više od toga, tj. da svaki polinom $f\in A[X]$ ima koren u A.

18.1. Lema Neka su $\mathbb{F}\subseteq\mathbb{E}\subseteq\mathbb{K}$ polja. Ako je $\mathbb{E}$ algebarsko raširenje polja $\mathbb{F}$ i $\mathbb{K}$ je algebarsko raširenje polja $\mathbb{E}$, tada je $\mathbb{K}$ algebarsko raširenje polja $\mathbb{F}$.

Dokaz Neka je $\beta\in K$. Tada je β koren nekog polinoma $\alpha_0+\alpha_1X+\dots+\alpha_nX^n$ u K, $\alpha_0,\dots,\alpha_n\in E$. Dakle, β je algebarski element nad $\mathbb{F}(\alpha_0,\dots,\alpha_n)\subseteq\mathbb{E}$, pa prema Teoremi 15.6

a) $|\mathbb{F}(\alpha_0,\dots,\alpha_n,\beta):\mathbb{F}(\alpha_0,\dots,\alpha_n)| = |\mathbb{F}(\alpha_0,\dots,\alpha_n)(\beta):\mathbb{F}(\alpha_0,\dots,\alpha_n)|<\infty$

Dalje, s obzirom da su $\alpha_0,\dots,\alpha_n$ algebarski nad $\mathbb{F}$, to je α_i algebarski nad $\mathbb{F}(\alpha_0,\dots,\alpha_{i-1})$, $i=1,\dots,n$, pa prema Teoremi 15.6.

$|\mathbb{F}(\alpha_0,\dots,\alpha_n):\mathbb{F}| = |\mathbb{F}(\alpha_0,\dots,\alpha_n):\mathbb{F}(\alpha_0,\dots,\alpha_{n-1})|\cdots|\mathbb{F}(\alpha_0):\mathbb{F}|<\infty$

odakle je prema Teoremi 15.4 $\mathbb{F}(\alpha_0,\dots,\alpha_n)$ algebarsko raširenje polja $\mathbb{F}$ i

b) $|\mathbb{F}(\alpha_0,\dots,\alpha_n):\mathbb{F}|<\infty$.

Dalje, $|\mathbb{F}(\alpha_0,\dots,\alpha_n,\beta):\mathbb{F}| = |\mathbb{F}(\alpha_0,\dots,\alpha_n,\beta):\mathbb{F}(\alpha_0,\dots,\alpha_n)|\cdot|\mathbb{F}(\alpha_0,\dots,\alpha_n):\mathbb{F}|<\infty$
te je $\mathbb{F}(\alpha_0,\dots,\alpha_n,\beta)$ alg. raširenje polja $\mathbb{F}$. Kako je $\beta\in\mathbb{F}(\alpha_0,\dots,\alpha_n,\beta)$ to je onda β algebarski nad $\mathbb{F}$. ∎

Iz dokaza prethodne leme vidimo da važi

18.2. Tvrdnja Neka je $\mathbb{F}\subseteq\mathbb{E}$ i neka su $\alpha_0,\dots,\alpha_n\in\mathbb{E}$ algebarski nad $\mathbb{F}$. Tada je $\mathbb{F}(\alpha_0,\dots,\alpha_n)\subseteq\mathbb{E}$ algebarsko raširenje polja $\mathbb{F}$.

18.3. Teorema A je podpolje polja $\mathbb{C}$.

Dokaz Neka su $\alpha,\beta\in A$. Tada $\alpha+\beta,\ \alpha\beta\in Q(\alpha,\beta)$ i $\alpha^{-1}\in Q(\alpha,\beta)$ ako $\alpha\neq 0$. Elementi α,β su algebarski nad $\mathbb{Q}$, te je prema 18.2 $Q(\alpha,\beta)$ algebarsko raširenje polja $\mathbb{Q}$. Dakle, $\alpha+\beta$, $\alpha\beta$ i α^{-1} (za $\alpha\neq 0$) su algebarski nad $\mathbb{Q}$, prema tome $\alpha+\beta,\ \alpha\beta\in A$ i $\alpha^{-1}\in A$ ako $\alpha\neq 0$. ∎

18.4. Zadatak Neka su E i F podpolja polja $\mathbb{K}$. Tada je $E\cap F$ podpolje polja $\mathbb{K}$.

18.5. $A\cap R$ je također podpolje polja kompleksnih brojeva $\mathbb{C}$.
$A\cap R$ je polje realnih algebarskih brojeva.

18.6. Zadatak Skup celih algebarskih brojeva je $\bar{Z}=\{\alpha\in C \mid \alpha \text{ je koren polin. } f\in Z[X]\}$.
Dokazati da je $\bar{Z}$ podprsten polja A.

19. <u>Separabilnost</u> $\deg f > 0$

Polinom $f \in \mathbb{F}[x]$ je <u>separabilan</u> akko su svi koreni polinoma f u korenskom polju $\mathbb{E}$ polin. f međusobno različiti. Drugim rečima ako je $\deg f = n > 1$ i $\alpha_1, \dots, \alpha_n$ su koreni polinoma f, tada su $\alpha_1, \dots, \alpha_n$ međusobno različiti, tj. $f(x) = c\cdot(x-\alpha_1)\cdots(x-\alpha_n)$,

19.1 <u>Teorema</u> Neka je $f \in \mathbb{F}[x]$. Tada je f separabilan akko $(f, f') = 1$, gde je f' izvod polinoma f. Pretpostavljamo da je $\deg f > 0$.

<u>Dokaz</u> Tvrđenje teoreme očigledno je ekvivalentno sa:

$$(f, f') \neq 1 \iff f \text{ nije separabilan.}$$

($\Rightarrow$) PP $(f, f') \neq 1$. Tada postoji $g \in \mathbb{F}[x]$ tako da $g \mid f, f'$ i $\deg g \geq 1$. Neka je $\mathbb{E}$ korensko polje polinoma f. Dalje, imamo $f = g h_1$ i $f' = g h_2$ za neke $h_1, h_2 \in \mathbb{F}[x]$. Prema Lemi u 17.9 postoji $b \in \mathbb{E}$ tako da je $g(b) = 0$. Tada $f(b) = 0$ i $f'(b) = 0$, te je prema Teoremi 9.1 b višestruki koren polinoma f, tj. f nije separabilan.

($\Leftarrow$) PP $f(x)$ nije separabilan. Tada u korenskom proširenju $\mathbb{E} \supseteq \mathbb{F}$ polinoma f postoji α tako da je za neki $h \in E[x]$, $f(x) = (x-\alpha)^2 h(x)$. Tada $f^{\mathbb{E}}(\alpha) = 0$, $f'^{\mathbb{E}}(\alpha) = 0$ pa $(x-\alpha) \mid f, f'$. Neka je $r \in (f, f')$. Tada $(x-\alpha) \mid r(x)$ pa $\deg r \geq 1$ ili $\deg r = -1$ ($r = 0$).
U prvom slučaju sledi $(f, f') \neq 1$. Ako je $r = 0$, onda $f' \mid f$, pa kako je $\deg f \geq 1$ i f ima višestruke korene, to $\deg f \geq 2$, to $\deg f' \geq 1$, tj. $(f, f') \neq 1$. Primetimo da $f' \neq 0$ jer $f' \mid f$ i $\deg f \geq 1$. ∎

19.2. <u>Napomena</u> U poljima proste karakteristike postoje polinomi f takvi da je $\deg f \geq 1$ i $f' = 0$. Na primer za $p \in$ Prost, i $f(x) = x^{p^2} + x^p$ $f' = 0$ u svakom polju karakteristike p.
Ako je karakteristika polja $\mathbb{F} = 0$ i $f \in \mathbb{F}[x]$, $\deg f > 0$, tada $f' \neq 0$, preciznije $\deg f' = \deg f - 1$.

19.3 <u>Teorema</u> Neka je $f \in \mathbb{F}[x]$, $\deg f \geq 1$, nesvodljiv. Tada je f separabilan akko $f' \neq 0$.

<u>Dokaz</u> ($\Rightarrow$) PP f je separabilan. Prema Teoremi 19.1. tada je $(f, f') = 1$. Otuda $f' \neq 0$, jer u suprotnom $f \in (f, f') = (f, 0)$.
($\Leftarrow$) PP $f' \neq 0$. Tada $\deg f' \geq 0$ pa zbog nesvodljivosti polinoma f, $(f, f') = 1$.

19.4. <u>Posledica</u> Neka je $k\,\mathbb{F} = 0$ i neka je $f \in \mathbb{F}[x]$ nesvodljiv polinom nad $\mathbb{F}$. Tada je f separabilan polinom. Ako je f nesvodljiv polinom nad brojevnim poljem, tada je f separabilan, tj. nema višestruke kompleksne korene.

19.5. Neka su $\mathbb{E} \supseteq \mathbb{F}$ polja. Element $\alpha \in E$ je <u>separabilan</u> nad $\mathbb{F}$ ako je α koren separabilnog polinoma $f \in \mathbb{F}[x]$. $\mathbb{E}$ je <u>separabilno proširenje</u> polja $\mathbb{F}$ ako je svaki $\alpha \in E$ separabilan nad $\mathbb{F}$.
Primetimo da je separabilno proširenje polja $\mathbb{F}$ algebarsko proširenje polja $\mathbb{F}$. Dalje, svako algebarsko proširenje polja $\mathbb{F}$, $k\mathbb{F} = 0$, je separabilno. Ako je $\mathbb{E}$ separabilno proširenje polja $\mathbb{F}$ i $m(x)$ je minimalni polinom za $\alpha \in E$ nad $\mathbb{F}$, tada je $m(x)$ nesvodljiv, dakle i separabilan.

19.6. <u>Zadatak</u> Neka su $\mathbb{E} \supseteq \mathbb{F}$ polja proste karakteristike p i neka je $\alpha \in E$. Dokazati da je α separabilan nad $\mathbb{F}$ akko $F(\alpha^p) = F(\alpha)$.

19.7. <u>Zadatak</u> Neka su $\mathbb{E} \supseteq \mathbb{F}$ polja i $\alpha \in E$. Dokazati da je $\mathbb{F}(\alpha)$ separabilno proširenje polja $\mathbb{F}$ akko je α separabilan nad $\mathbb{F}$.

19.8. <u>Z</u> Dokazati da je relacija separabilnog raširenja tranzitivna: Ako je $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ i $\mathbb{E}/\mathbb{F}$ je separabilno, $\mathbb{K}/\mathbb{E}$ je separabilno, tada je $\mathbb{K}/\mathbb{F}$ separabilno.

19.9. <u>Z</u> Neka su $\mathbb{E} \supseteq \mathbb{F}$ polja i neka je $K = \{\alpha \in E \mid \alpha$ je separabilan nad $\mathbb{F}\}$. Tada je $\mathbb{K}$ podpolje polja $\mathbb{E}$.

19.10. Neka su $\mathbb{E} \supseteq \mathbb{F}$ polja. Ako postoji $\vartheta \in E$ tako da je $\mathbb{E} = \mathbb{F}(\vartheta)$, tada kažemo da je $\mathbb{E}$ <u>prosto proširenje</u> polja $\mathbb{F}$. U tom slučaju ϑ se naziva <u>primitivnim elementom</u> polja $\mathbb{E}$.
Na primer, $Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2} + \sqrt{3})$. Dakle $Q(\sqrt{2}, \sqrt{3})$ je prosto proširenje polja $\mathbb{Q}$ i $\sqrt{2} + \sqrt{3}$ je primitivni element polja $Q(\sqrt{2}, \sqrt{3})$.

19.11. <u>Teorema</u> (o primitivnom elementu). Neka je $\mathbb{E}$ konačno separabilno raširenje polja $\mathbb{F}$. Tada je $\mathbb{E}$ prosto proširenje polja $\mathbb{F}$.

<u>Dokaz</u> 1° <u>$\mathbb{F}$ je konačno polje</u>. Kako je $|\mathbb{E} : \mathbb{F}| < \infty$, to je onda $\mathbb{E}$ takođe konačno polje, pa je $\mathbb{E}^*$ ciklična grupa (Teorema 2.3), tj. $\mathbb{E}^* = \langle \vartheta \rangle$ za neki $\vartheta \in E^*$. Tada $\mathbb{E} = \mathbb{F}(\vartheta)$.
2° <u>$\mathbb{F}$ je beskonačno polje</u>. Dovoljno je da tvrđenje dokažemo za ekstenzije oblika $\mathbb{E} = \mathbb{F}(\alpha, \beta)$, jer ako je $\mathbb{E} = \mathbb{F}(\alpha_1, \dots, \alpha_n)$, onda ako tvrđenje važi za dva generatora, $\mathbb{E} = \mathbb{F}(\alpha_1, \dots, \alpha_n) = \mathbb{F}(\alpha_1, \dots, \alpha_{n-2}, \vartheta_1) =$

$\mathbb{F}(\alpha_1, \dots, \alpha_{n-4}, \vartheta_2) = \dots = \mathbb{F}(\vartheta)$.
Dalje, primetimo ako je $|\mathbb{E} : \mathbb{F}| < \infty$, onda postoje $\alpha_1, \dots, \alpha_n \in E$ takvi da je $\mathbb{E} = \mathbb{F}(\alpha_1, \dots, \alpha_n)$. Zaista neka je $\alpha_1 \in E \setminus F$, tada $|\mathbb{F}(\alpha_1) : \mathbb{F}| = n_1 > 1$.
Dalje neka je $\alpha_2 \in E \setminus F(\alpha_1)$ (ako $E \neq F(\alpha_1)$) i slično $|\mathbb{F}(\alpha_1, \alpha_2) : \mathbb{F}(\alpha_1)| = n_2 > 1$.

Postupak biranja elemenata α_i mora se završiti u konačno mnogo koraka, jer inače za neko $k \in N$ važi

$n = |\mathbb{E} : \mathbb{F}| = |\mathbb{E} : \mathbb{F}(\alpha_1, \dots, \alpha_k)| \cdot |\mathbb{F}(\alpha_1, \dots, \alpha_k) : \mathbb{F}(\alpha_1, \dots, \alpha_{k-1})| \cdots |\mathbb{F}(\alpha_1) : \mathbb{F}| \geq n_1 n_2 \cdots n_k > n$, #.

Dakle, dokazujemo tvrđenje teoreme za $\mathbb{E} = \mathbb{F}(\alpha, \beta)$.
Neka je $f \in \mathbb{F}[x]$ minimalni polinom za α i neka je $g \in \mathbb{F}[x]$ minimalni polinom za β. S obzirom da je $\mathbb{E}$ separabilno proširenje polja $\mathbb{F}$, f i g su separabilni polinomi. Najpre dokažimo

(1) Postoji algebarsko raširenje $\mathbb{K}$ polja $\mathbb{E}$ koje sadrži korensko polja polinoma f i g.
Polje $\mathbb{K}$ možemo dobiti na sledeći način. Kako je $\mathbb{F} \subseteq \mathbb{E}$, to je $f \in \mathbb{E}[x]$, neka je $\mathbb{E}_1 \supseteq \mathbb{E}$ korensko polje polinoma f nad $\mathbb{E}$. Slično $g \in \mathbb{E}_1[x]$, pa za $\mathbb{K}$ možemo uzeti korensko polje polinoma g nad $\mathbb{E}_1$.
Dakle u polju $\mathbb{K}$ polinomi f i g imaju linearnu faktorizaciju i zbog njihove separabilnosti f i g nemaju višestruke korene u K.
Neka su $\alpha = \alpha_1, \alpha_2, \dots, \alpha_m$ svi koreni polinoma f u K i neka su $\beta = \beta_1, \beta_2, \dots, \beta_n$ svi koreni polinoma g u $\mathbb{K}$. Kao što smo primetili, $\alpha_1, \dots, \alpha_m$ su međusobno različiti i slično, $\beta_1, \dots, \beta_n$ su međusobno različiti. Neka je $c \in F$ takav da je

$$c \notin \left\{ \frac{\alpha - \alpha_i}{\beta - \beta_j} \mid i = 2, \dots, m,\ j = 2, 3, \dots, n \right\}.$$

Ovakav c postoji s obzirom da je $\mathbb{F}$ beskonačno polje. Dalje, neka je $\varkappa = \alpha + c\beta$. Tada $F(\varkappa) \subseteq F(\alpha, \beta)$ i takođe

(2) $\varkappa = \alpha_i + c\beta_j$ akko $i = 1, j = 1$.
Neka je $h(x) = f(\varkappa - cx)$. Tada $h \in F(\varkappa)[x]$ i
$h(\beta) = f(\varkappa - c\beta) = f(\alpha) = 0$, tj. $\beta_1 = \beta$ je koren polinoma h.
Primetimo da ni jedan od elemenata $\beta_2, \dots, \beta_n$ nije koren polinoma h, jer ako je, na primer, $h(\beta_2) = 0$, onda $f(\varkappa - c\beta_2) = 0$, pa $\varkappa - c\beta_2 = \alpha_i$ za neki i, tj. $\varkappa = \alpha_i + c\beta_2$, suprotno (2).

(3) Prema tome $\beta_1 = \beta$ jedini je zajednički koren polinoma g i h.
Neka je $m(x)$ minimalni polinom za β nad $F(\varkappa)$. Tada $m / g, h$ jer $g(\beta) = 0$, $h(\beta) = 0$ (Teorema 15.6). Polje $\mathbb{K}$ sadrži faktorsko polje polinoma g i m / g, dakle $\mathbb{K}$ sadrži i korensko polje polinoma m.
Prema tome $m(x)$ ima linearnu faktorizaciju u K. S obzirom na (3) i $m / g, h$, β je jedini koren polinoma m. Kako je g separabilan i m / g, to je i m separabilan, tj. nema višestrukih korena u K.
Dakle, $m(x) = a(x - \beta)$ i $a, a\beta \in F(\varkappa)$ (jer $m \in F(\varkappa)[x]$), odakle sledi $\beta \in F(\varkappa)$ te i $\varkappa - c\beta \in F(\varkappa)$, tj. $\alpha \in F(\varkappa)$. Otuda $F(\alpha, \beta) \subseteq F(\varkappa)$, pa kako je $F(\varkappa) \subseteq F(\alpha, \beta)$, to $F(\alpha, \beta) = F(\varkappa)$. ▨

19.12. <u>Posledica</u> Neka je $\mathbb{F}$ brojevno polje i neka je $\mathbb{E} \doteq \mathbb{F}(\alpha_1, \dots, \alpha_n)$ algebarska ekstenzija polja $\mathbb{F}$. Tada postoji $\varkappa \in \mathbb{C}$ takav da je $\mathbb{F}(\alpha_1, \dots, \alpha_n) = \mathbb{F}(\varkappa)$.

<u>Napomena</u> Dokaz za 19.12. može se učiniti nešto jednostavnijim, s obzirom da nije potrebna konstrukcija polja $\mathbb{K}$ u 19.11.(1). S obzirom da je $\mathbb{C}$ algebarski zatvoreno, možemo uzeti $\mathbb{K} = \mathbb{C}$.

19.13. <u>Zadatak</u> Odrediti primitivne elemente za polja $\mathbb{Q}(i, \sqrt{2})$ i $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

20. Algebarski zatvorena polja

Polje $\mathbb{E}$ je algebarski zatvoreno ako svaki polinom $f \in E[x]$, $\deg f \geq 1$ ima koren u $\mathbb{E}$. Dakle, ako je $\mathbb{E}$ algebarski zatvoreno polje i $f \in E[x]$, $\deg f \geq 1$, tada f ima linearnu faktorizaciju u $\mathbb{E}$, tj. $\mathbb{E}$ sadrži korensko polje polinoma f.

20.1. <u>Teorema</u> Polje kompleksnih brojeva je algebarski zatvoreno polje.
(F. Gauss)

20.2. <u>Lanci polja</u> Neka je $\mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \dots$ prebrojiv niz polja, i neka je $E = \bigcup_n F_n$. Tada se nad domenom E može definisati struktura polja $\mathbb{E}$ tako da je $\bigwedge_n \mathbb{F}_n \subseteq \mathbb{E}$.

Neka su $\alpha, \beta \in E$. Tada za neke $m, n \in N$, $\alpha \in F_m$ i $\beta \in F_n$. Neka je $m \geq n$. Tada $\alpha +_E \beta \overset{\text{def}}{=} \alpha +_{F_m} \beta$ i $\alpha \cdot_E \beta \overset{\text{def}}{=} \alpha \cdot_{F_m} \beta$.

Operacije $+_E$ i $\cdot_E$ su dobro definisane s obzirom da za $i \leq j$ $\mathbb{F}_i \subseteq \mathbb{F}_j$, tj. za $x, y \in F_i$, $x +_{F_i} y = x +_{F_j} y$ i $x \cdot_{F_i} y = x \cdot_{F_j} y$.

Neposredno se proverava da je $\mathbb{E} = (E, +_E, \cdot_E, 0, 1)$ polje.

Ovo polje nazivamo unijom polja $\mathbb{F}_i$ i pišemo $\mathbb{E} = \bigcup_i \mathbb{F}_i$.

20.3. <u>Z.</u> Neka je $(I, \leq)$ linearno uređen skup i neka je $\mathcal{L} = \{\mathbb{F}_i \mid i \in I\}$ lanac polja, tj. za $i, j \in I$ važi:

$$i \leq j \Rightarrow \mathbb{F}_i \subseteq \mathbb{F}_j.$$

Dokazati da se na domenu $\mathbb{E} = \bigcup_{i \in I} F_i$ može definisati struktura polja $\mathbb{E}$ tako da je $\bigwedge_{i \in I} \mathbb{F}_i \subseteq \mathbb{E}$.

20.4. <u>Zadatak</u> 1° Neka je $\mathbb{F}$ najviše prebrojivo polje. Dokazati da je tada $\mathbb{F}[x]$ prebrojiv skup.

2°* Neka je $\mathbb{F}$ beskonačno polje. Dokazati da je $|F[x]| = |F|$, $|X|$ je kardinalni broj skupa X.

20.5 <u>Teorema</u> Polje algebarskih brojeva A je algebarski zatvoreno.

<u>Dokaz</u> Neka je $f \in A[x]$, $\deg f \geq 1$ i neka je $\alpha \in C$ koren polinoma f u polju kompleksnih brojeva $\mathbb{C}$. Dalje, za neke $a_0, a_1, \dots, a_n \in A$ $f(x) = a_0 + a_1 x + \dots + a_n x^n$ i s obzirom da su $a_0, \dots, a_n$ algebarski nad Q to je $Q(a_0, \dots, a_n)$ algebarsko raširenje polja $\mathbb{Q}$. α je algebarski nad $Q(a_0, \dots, a_n)$, dakle $Q(a_0, \dots, a_n, \alpha)$ je algebarsko raširenje polja $Q(a_0, \dots, a_n)$. Prema Lemi 18.1, tada je $Q(a_0, \dots, a_n, \alpha)$ algebarsko raširenje polja Q, pa kako je $\alpha \in Q(a_0, \dots, a_n, \alpha)$, to je α algebarski nad $\mathbb{Q}$, tj. $\alpha \in A$. ∎

20.6. <u>Posledica</u> Polje $A \cap R$ realnih algebarskih brojeva je realno zatvoreno, tj.:

1° Svaki polinom $f \in (A \cap R)[x]$ neparnog stepena ima koren u $A \cap R$.

2° Ako je $a \in A \cap R$ tada $\sqrt{a} \in A \cap R$ ili $\sqrt{-a} \in A \cap R$, tj. ili jednačina $x^2 + a = 0$ ili jednačina $x^2 - a = 0$ ima koren u $A \cap R$.

20.7. <u>Teorema</u> Svako polje $\mathbb{F}$ sadržano je u nekom algebarski zatvorenom polju.

Dokaz ovog tvrđenja za proizvoljna polja, odnosno neprebrojiva polja zasniva se velikim delom na teoriji skupova. Zato ćemo ovu teoremu dokazati u slučaju prebrojivog polja F.

<u>Dokaz</u> Neka je $\mathbb{F}$ prebrojivo polje. Tada je $\mathbb{F}[x]$ prebrojiv skup, tj:

(1) $\mathbb{F}[x] = \{p_0, p_1, \dots\}$.

Dakle i $\mathcal{F} = \{f \in \mathbb{F}[x] \mid \deg f \geq 1\}$ je prebrojiv, tj:

(2) $\mathcal{F} = \{f_0, f_1, \dots\}$.

Konstruišemo niz polja $\mathbb{F}_0 = \mathbb{F}, \mathbb{F}_1, \mathbb{F}_2, \dots$ na sledeći način.
$\mathbb{F}_1$ je korensko polje polinoma f_0 nad $\mathbb{F}_0$, $\mathbb{F}_2$ je korensko polje polinoma f_1 nad $\mathbb{F}_1$ i uopšte za proizvoljno $n \in N$, $\mathbb{F}_{n+1}$ je korensko polje polinoma f_n nad $\mathbb{F}_n$.
Tada $\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \dots$, pa neka je $\mathbb{E}_1 = \bigcup_n \mathbb{F}_n$. Za polje $\mathbb{E}_1$ važi

(3) Ako je $f \in \mathbb{F}[x]$, $\deg f \geq 1$, tada f ima koren u $\mathbb{E}_1$.

Zaista, $f = f_n$ za neki $n \in N$, pa f ima koren u $\mathbb{F}_{n+1}$ i dakle i u $\mathbb{E}_1$ s obzirom da je $\mathbb{F}_{n+1} \subseteq \mathbb{E}_1$.
Dalje, konstruišemo niz polja $F = \mathbb{E}_0 \subseteq \mathbb{E}_1 \subseteq \mathbb{E}_2 \subseteq \dots$ na sledeći način.
Polje $\mathbb{E}_2$ je konstruisano nad poljem $\mathbb{E}_1$ na isti način kako je polje $\mathbb{E}_1$ konstruisano nad poljem $\mathbb{E}_0$ $(=\mathbb{F})$, i na isti način konstruiše se polje $\mathbb{E}_{n+1}$ nad poljem $\mathbb{E}_n$, $n \in N$, $n \geq 2$. Neka je $\mathbb{E} = \bigcup_n \mathbb{E}_n$. Tada

(4) $\mathbb{E}$ je algebarski zatvoreno polje i $\mathbb{F} \subseteq \mathbb{E}$.

Očigledno $\mathbb{F} \subseteq \mathbb{E}$. Neka je $f \in \mathbb{E}[x]$, $\deg f \geq 1$, $f = b_0 + b_1 x + \dots + b_n x^n$. Tada za neke k_i, $i \leq n$, $b_i \in \mathbb{E}_{k_i}$ pa $f \in E_k$ za $k = \max_i k_i$, dakle f ima koren u $\mathbb{E}_{k+1}$, pa i u $\mathbb{E}$ jer $\mathbb{E}_{k+1} \subseteq \mathbb{E}$. Prema tome $\mathbb{E}$ je algebarski zatvoreno ∎

20.8 Napomena* Uz poznavanje ordinalnih brojeva, prethodni dokaz se lako može adaptirati u dokaz i za neprebrojiva polja. Zaista, u ovom slučaju sve polinome $f \in \mathbb{F}[x]$, $\deg f \geq 1$, možemo poredati u niz

$$f_0, f_1, \ldots, f_\alpha, \ldots, \quad \alpha < \kappa, \quad \kappa = card(F), \ \alpha \text{ je ordinalni broj.}$$

Tada se konstruiše niz polja $\mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_\alpha \subseteq \cdots$, $\alpha < \kappa$:

- ako je α sukcesor, tj. $\alpha = \beta + 1$, tada je $\mathbb{F}_\alpha$ korensko polje polinoma f_β nad $\mathbb{F}_\beta$,
- ako je α granični ordinal, neka je $\mathbb{K} = \bigcup_{\beta<\alpha} \mathbb{F}_\beta$. Tada je $\mathbb{F}_\alpha$ korensko polje polinoma f_α nad $\mathbb{K}$.

Najzad, $\mathbb{E}_1 = \bigcup_{\alpha<\kappa} \mathbb{F}_\alpha$. Dalje je dokaz isti kao u prebrojivom slučaju.

Drugi mogući dokaz pretpostavlja primenu Zornove leme. Na prvi pogled, u cilju primene Zornove leme, možemo uočiti "parcijalno uređen skup" $(\mathcal{F}, \subseteq)$, gde je $\mathcal{F} = \{\mathbb{K} \mid \mathbb{K} \supseteq \mathbb{F}\}$ i u njoj da posmatramo odgovarajuće lance. Problem je u tome što $\mathcal{F}$ nije skup, već prava klasa (na pr. u smislu NBG sistema), te se Zornova lema ne može primeniti. Ipak, kolekciju $\mathcal{F}$ možemo redukovati na skup, ali tako da novodobijeni skup ipak omogućava konstrukciju algebarski zatvorenog raširenja polja $\mathbb{F}$. Ako je $|\mathbb{F}| = \kappa$, neka je V_κ član kumulativne hijerarhije univerzuma V ($V_0 = \emptyset$, $V_{\alpha+1} = V_\alpha \cup \mathcal{P}(V_\alpha)$, $V_\alpha = \bigcup_{\beta<\alpha} V_\beta$, α je granični ordinal) i neka je $\mathcal{F}_\kappa = \{\mathbb{E} \in V_{\kappa^+} \mid \mathbb{F} \subseteq \mathbb{E}\}$. Tada možemo pretpostaviti da je $\mathbb{F} \in \mathcal{F}_\kappa$ i tada se može primeniti standardna konstrukcija uz pomoć Zornove leme.

Treći način dokaza ove teoreme u opštem slučaju može se sprovesti uz pomoć Teoreme kompaktnosti predikatskog računa i najbliži je duhu algebre: Neka je za svaki $f \in \mathbb{F}[x]$, c_f novi simbol konstante i neka je $T = \text{Teorija polja} + \Delta_{\mathbb{F}} + \{f(c_f) = 0 \mid f \in \mathbb{F}[x], \deg f \geq 1\}$ gde je $\Delta_{\mathbb{F}}$ dijagram modela (polja) $\mathbb{F}$. Ako je $S \subseteq \{f(c_f) = 0 \mid f \in \mathbb{F}[x], \deg f \geq 1\}$ konačan skup, tada teorija $T' = \text{Teorija polja} + \Delta_{\mathbb{F}} + S$ ima model, odnosno polje koje realizuje sve aksiome teorije T'. Dokaz ove činjenice sadržan je već u dokazu Teoreme 20.7 za prebrojiv slučaj, te prema teoremi kompaktnosti postoji polje $\mathbb{E}_1$ u kojem važe sve aksiome teorije T. U ovom polju $\mathbb{E}_1$, ako je $f \in \mathbb{F}[x]$, $\deg f \geq 1$, f ima koren, te se dalje sprovodi dokaz Teoreme 20.7 kao u prebrojivom slučaju. ■

20.9. Polje $\mathbb{E}$ je algebarsko zatvorenje polja $\mathbb{F}$ ako je

1° $\mathbb{F} \le \mathbb{E}$

2° $\mathbb{E}$ je algebarsko raširenje polja $\mathbb{F}$

3° $\mathbb{E}$ je algebarski zatvoreno.

Na primer polje kompleksnih brojeva $\mathbb{C}$ je algebarsko zatvorenje polja $\mathbb{R}$ (jer $|\mathbb{C} : \mathbb{R}| = 2$ i $\mathbb{C}$ je algebarski zatvoreno), dok je polje $\mathbb{A}$ algebarskih brojeva algebarsko zatvorenje polja $\mathbb{Q}$ (Teoreme 18.3, 20.5).

20.10 Teorema Svako polje $\mathbb{F}$ ima algebarsko zatvorenje.

Dokaz Prema Teoremi 20.7. postoji algebarski zatvoreno polje $\mathbb{K} \ge \mathbb{F}$. Neka je $E = \{\alpha \in \mathbb{K} \mid \alpha$ je algebarski nad $\mathbb{F}\}$. Dokažimo da je $\mathbb{E}$ algebarsko zatvorenje polja $\mathbb{F}$. Primetimo najpre da je

1° $\mathbb{F} \le \mathbb{E}$

2° $\mathbb{E}$ je algebarsko raširenje polja $\mathbb{F}$.

3° Dokaz da je $\mathbb{E}$ algebarski zatvoreno svodi se na isti način kao i dokaz da je $\mathbb{A}$ algebarski zatvoreno: Neka je $f \in E[x]$, $\deg f \ge 1$, i neka je $\alpha \in K$ takav da je $f^{K}(\alpha) = 0$. Dalje, neka je $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Tada $a_0, \ldots, a_n \in E$ i

$\mathbb{F}(a_0, \ldots, a_n)$ je algebarsko raširenje polja $\mathbb{F}$ i

$\mathbb{F}(a_0, \ldots, a_n, \alpha)$ je algebarsko raširenje polja $\mathbb{F}(a_0, \ldots, a_n)$, dakle

$\mathbb{F}(a_0, \ldots, a_n, \alpha)$ je algebarsko raširenje polja $\mathbb{F}$, pa $\alpha \in E$. ☒

Ovim smo nezavisno od činjenice da je polje $\mathbb{C}$ algebarski zatvoreno dokazali da polje $\mathbb{R}$ ima neko algebarsko zatvorenje $\overline{\mathbb{R}}$ i slično da polje racionalnih brojeva $\mathbb{Q}$ ima neko algebarsko zatvorenje $\overline{\mathbb{Q}}$. Da li su polja $\overline{\mathbb{R}}$ i $\mathbb{C}$ ista, odnosno da li je $\overline{\mathbb{R}} \cong \mathbb{C}$, i slično, da li je $\overline{\mathbb{Q}} \cong \mathbb{A}$?

20.11. Zadatak Neka je $\overline{\mathbb{F}}$ algebarsko zatvorenje polja $\mathbb{F}$. Ako je $\mathbb{F} \le \mathbb{K} \le \overline{\mathbb{F}}$, tada je $\overline{\mathbb{F}}$ algebarsko zatvorenje polja $\mathbb{K}$.

20.12. Zadatak Ako je $\mathbb{F}$ beskonačno polje tada, tada $|\overline{F}| = |F|$.

20.13. Zadatak Svako algebarski zatvoreno polje je beskonačno.

20.14. Zadatak Ako je $\mathbb{R} \le \mathbb{K}$ i $|\mathbb{K} : \mathbb{R}| = 2$, tada je $\mathbb{K}$ algebarski zatvoreno.

20.15. Zadatak Dokazati da je polje $\mathbb{K}$ algebarski zatvoreno akko $\mathbb{K}$ nema pravo algebarsko raširenje.

Dokazaćemo da je algebarsko zatvorenje polja $\mathbb{F}$ do na izomorfizam jedinstveno određeno.

20.16. Teorema Neka su $\mathbb{F}$ i $\mathbb{F}'$ polja, $\sigma : \mathbb{F} \cong \mathbb{F}'$ i neka su $\mathbb{K}$ i $\mathbb{K}'$ algebarska zatvorenja redom polja $\mathbb{F}$ i $\mathbb{F}'$. Tada postoji $\theta : \mathbb{K} \cong \mathbb{K}'$ tako da $\theta \restriction \mathbb{F} = \sigma$.

$$\begin{array}{ccc} \mathbb{K} & \overset{\theta}{\dashrightarrow} & \mathbb{K}' \\ \cup\!\vert & & \cup\!\vert \\ \mathbb{F} & \overset{\sigma}{\longrightarrow} & \mathbb{F}' \end{array}$$ ← komutativan dijagram

Dokaz Dokaz ćemo sprovesti u slučaju prebrojivog polja $\mathbb{F}$. Tada je, naravno, i polje $\mathbb{F}'$ prebrojivo.

Neka $p_1, p_2, \dots$ su polinomi promenljive x, $\deg p_i \geq 1$, nad poljem $\mathbb{F}$ i neka su $p_1', p_2', \dots$ korespondentni polinomi nad $\mathbb{F}'$! Tada je $p_1', p_2', \dots$ takođe niz polinoma nad $\mathbb{F}'$ stepena ≥ 1.

Konstruišemo lanac polja i izomorfizama tako da sledeći beskonačan dijagram komutira:

$$\begin{array}{ccccccccccccccccc} \mathbb{F} = \mathbb{F}_0 & \subseteq & \mathbb{F}_1 & \subseteq & \mathbb{F}_2 & \subseteq & \cdots & \subseteq & \bigcup_n \mathbb{F}_n = \mathbb{E}_1 & \subseteq & \mathbb{E}_2 & \subseteq & \cdots & \subseteq & \bigcup_n \mathbb{E}_n = \mathbb{H} & \subseteq & \mathbb{K} \\ \sigma = \sigma_0 \downarrow & & \sigma_1 \downarrow & & \sigma_2 \downarrow & & & & \downarrow \theta_1 & & \downarrow \theta_2 & & & & \downarrow \theta & & \downarrow \theta \\ \mathbb{F}' = \mathbb{F}_0' & \subseteq & \mathbb{F}_1' & \subseteq & \mathbb{F}_2' & \subseteq & \cdots & \subseteq & \bigcup_n \mathbb{F}_n' = \mathbb{E}_1' & \subseteq & \mathbb{E}_2' & \subseteq & \cdots & \subseteq & \bigcup_n \mathbb{E}_n' = \mathbb{H}' & \subseteq & \mathbb{K}' \end{array}$$

Ako je $\{\alpha \in \mathbb{K} \mid \alpha \text{ je koren polin. } p_1 \text{ u } \mathbb{K}\} = \{\alpha_1, \dots, \alpha_m\}$ i $\mathbb{F}_1 = \mathbb{F}_0(\alpha_1, \dots, \alpha_m)$, tada je $\mathbb{F}_1$ korensko polje polinoma p_1 nad $\mathbb{F}_0$ i tada je $\mathbb{F}_1'$ korensko polje polinoma p_1' nad $\mathbb{F}_0'$ jer $\sigma_0 : \mathbb{F} \cong \mathbb{F}_0'$ i $p_1' = \sigma_0 p_1$ i prema Teoremi 4.17.9 (teorema o jedinstvenosti korenskog proširenja) postoji $\sigma_1 : \mathbb{F}_1 \cong \mathbb{F}_1'$, $\sigma_1 \restriction \mathbb{F}_0 = \sigma_0$.

Ako je $\{\alpha \in \mathbb{K} \mid \alpha \text{ je koren polin. } p_2 \text{ u } \mathbb{K}\} = \{\beta_1, \dots, \beta_\ell\}$ i $\mathbb{F}_2 = \mathbb{F}_1(\beta_1, \dots, \beta_\ell)$ tada je $\mathbb{F}_2$ korensko polje polinoma p_2 nad $\mathbb{F}_1$ i tada je $\mathbb{F}_2'$ korensko polje polinoma p_2' nad $\mathbb{F}_1'$. Kao malopre, postoji $\sigma_2 : \mathbb{F}_2 \cong \mathbb{F}_2'$, $\sigma_1 \subseteq \sigma_2$.

Nastavljajući ovaj postupak za sve $n \in \mathbb{N}$, nalazimo lance polja $\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \dots$, $\mathbb{F}' = \mathbb{F}_0' \subseteq \mathbb{F}_1' \subseteq \dots$ i $\sigma_n : \mathbb{F}_n \cong \mathbb{F}_n'$ tako da $\sigma_{n+1} \restriction \mathbb{F}_n = \sigma_n$. Neka je $\mathbb{E}_1 = \bigcup_n \mathbb{F}_n$, $\mathbb{E}_1' = \bigcup_n \mathbb{F}_n'$ i $\theta_1 = \bigcup_n \sigma_n$.

Tada $\theta_1 : \mathbb{E}_1 \cong \mathbb{E}_1'$ i svaki $f \in \mathbb{F}_0[x]$, $\deg f \geq 1$, ima koren u $\mathbb{E}_1$ i svaki $f \in \mathbb{F}_0'[x]$ ima koren u $\mathbb{E}_1'$.

Zatim konstruišemo lance polja $\mathbb{F}_0 = \mathbb{E}_0 \subseteq \mathbb{E}_1 \subseteq \mathbb{E}_2 \subseteq \dots$, $\mathbb{F}_0' = \mathbb{E}_0' \subseteq \mathbb{E}_1' \subseteq \mathbb{E}_2' \subseteq \dots$ i niz izomorfizama $\theta_n : \mathbb{E}_n \cong \mathbb{E}_n'$.

Polje $\mathbb{E}_2$ konstruiše se nad poljem $\mathbb{E}_1$ isto tako kao i polje $\mathbb{E}_1$ nad $\mathbb{E}_0$ ($= \mathbb{F}_0 = \mathbb{F}$) i slično polje $\mathbb{E}_2'$ nad $\mathbb{E}_1'$ kao i izomorfizam $\theta_2 : \mathbb{E}_2 \cong \mathbb{E}_2'$ (kao što je konstruisan izomorfizam $\theta_1 : \mathbb{E}_1 \cong \mathbb{E}_1'$). Postupak se nastavlja za sve $n \in \mathbb{N}$, $n \geq 2$.

Neka je $\mathbb{H} = \bigcup_n \mathbb{E}_n$, $\mathbb{H}' = \bigcup_n \mathbb{E}_n'$ i $\theta = \bigcup_n \theta_n$.
θ je dobro definisan jer $\theta_1 \subseteq \theta_2 \subseteq \dots$ i tada $\theta : \mathbb{H} \cong \mathbb{H}'$.
Koristeći činjenicu da je relacija algebarskog raširenja tranzitivna (L.18.1) indukcijom odmah nalazimo da je svako polje $\mathbb{E}_n$ algebarsko raširenje polja $\mathbb{F}$, dakle i $\mathbb{E}_n'$ je algebarsko raširenje polja $\mathbb{F}'$.

<u>Lema</u> Ako je $\mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \dots$ i svako $\mathbb{F}_n$ je alg. raširenje polja $\mathbb{F}_0$, tada je i $\mathbb{E} = \bigcup_n \mathbb{F}_n$ alg. raširenje polja $\mathbb{F}_0$.
Zaista, ako je $\alpha \in \mathbb{E}$, tada $\alpha \in \mathbb{F}_n$ za neki n, pa je α alg. nad $\mathbb{F}_0$. ∎

Dakle, Polje $\mathbb{E}_1$ je alg. raširenje polja $\mathbb{E}_0 = \mathbb{F}_0 = \mathbb{F}$, $\mathbb{E}_2$ je alg. raširenje polja $\mathbb{F}$ i slično za svaki $n \in N$, $\mathbb{E}_n$ je alg. raširenje polja $\mathbb{F}$, pa i $\mathbb{E}_n'$ je alg. raširenje polja $\mathbb{F}'$, $n \in N$. Dakle, $\mathbb{H}$ je alg. raš. polja $\mathbb{F}$ i $\mathbb{H}'$ je alg. raširenje polja $\mathbb{F}'$. Otuda

1° $\mathbb{F} \subseteq \mathbb{H} \subseteq \mathbb{K}$ 2° $\mathbb{H}$ je alg. raširenje polja $\mathbb{F}$

3° $\mathbb{H}$ je alg. zatvoreno polje (vidi dokaz za Teoremu 20.5), i

1'. $\mathbb{F}' \subseteq \mathbb{H}' \subseteq \mathbb{K}'$

2'. $\mathbb{H}'$ je algebarsko raširenje polja $\mathbb{F}'$

3'. $\mathbb{H}'$ je alg. zatvoreno.

Ako je $\alpha \in K$ tada je prema pp teoreme α algebarski nad $\mathbb{F}$ dakle α je koren nekog $f \in \mathbb{F}[x]$, pa zbog 3°, $\alpha \in H$.
Prema tome $H = K$ i slično $H' = K'$. ∎

Dakle, $\theta : \mathbb{K} \cong \mathbb{K}'$, $\theta \restriction F = \sigma$

20.17. <u>Posledica</u> $\overline{\mathbb{Q}} \cong \mathbb{A}$, $\overline{\mathbb{R}} \cong \mathbb{C}$
$\overline{\mathbb{Q}}$ je neko alg. zatv. polja $\mathbb{Q}$ i $\overline{\mathbb{R}}$ je alg. zatv. polja $\mathbb{R}$

20.18. <u>Zadatak</u> Neka su $\mathbb{K}$ i $\mathbb{K}'$ alg. zatvorenja polja $\mathbb{F}$. Tada postoji $\theta : \mathbb{K} \cong \mathbb{K}'$ tako da je $\theta \restriction F = i_F$.

$$\begin{tikzcd} \mathbb{K} \arrow[r, "\theta"', "\cong"] & \mathbb{K}' \\ \mathbb{F} \arrow[u, phantom, "\cup"] \arrow[ur, phantom, "\subseteq"] & \end{tikzcd}$$

20.19. <u>Zadatak.</u> Neka je $\mathbb{K}$ alg. zatvorenje polja $\mathbb{F}$ i neka je $\mathbb{E} \supseteq \mathbb{F}$ alg. zatvoreno polje. Tada postoji $\theta : \mathbb{K} \xrightarrow[1-1]{} \mathbb{E}$.

$$\begin{tikzcd} \mathbb{K} \arrow[r, "\theta"] & \mathbb{E} \\ \mathbb{F} \arrow[u, phantom, "\cup"] \arrow[ur, phantom, "\subseteq"] & \end{tikzcd}$$

20.20. <u>Zadatak</u> Dokazati da svako polje ima beskonačno mnogo neizomorfnih algebarski zatvorenih raširenja.

21. Utapanja algebarskih polja

21.1. Teorema Neka je $\mathbb{L}$ algebarsko raširenje polja $\mathbb{F}$ i neka je $\mathbb{K}$ algebarski zatvoreno polje koje sadrži polje $\mathbb{E}$. Ako je $\theta : \mathbb{F} \to \mathbb{E}$ utapanje, tada postoji utapanje $\lambda : \mathbb{L} \to \mathbb{K}$, $\theta \subseteq \lambda$ (tj. $\lambda | F = \theta$).

Dokaz Dokaz izvodimo primenom Zornove leme primenom na parcijalno uređen skup $(\mathcal{F}, \subseteq)$, gde je

$$\mathcal{F} = \{ \mu \mid \theta \subseteq \mu, \text{ za neko međupolje } \mathbb{F} \subseteq \mathbb{L}' \subseteq \mathbb{L}, \ \mu : \mathbb{L}' \to \mathbb{K} \}$$

$$\begin{tikzcd} \mathbb{L} \arrow[r, dashed, "\lambda"] & \mathbb{K} \\ \mathbb{F} \arrow[u, phantom, "\cup" rotate=90] \arrow[r, "\theta"] & \mathbb{E} \arrow[u, phantom, "\cup" rotate=90] \end{tikzcd}$$

Dakle, $\mathcal{F}$ se sastoji iz svih utapanja podpolja $L' \subseteq L$ koja sadrže $\mathbb{F}$ i pritom μ produžuje θ. Primetimo da je $\theta \in \mathcal{F}$, dakle $\mathcal{F} \neq \emptyset$.

Neka je $\mathcal{L}$ neprazan lanac u $(\mathcal{F}, \subseteq)$ i neka je $\tau = \bigcup \mathcal{L}$ i $\mathbb{L}' = \bigcup_{\sigma \in \mathcal{L}} \operatorname{dom} \sigma$. Nije teško proveriti da je L' međupolje, $\mathbb{F} \subseteq \mathbb{L}' \subseteq \mathbb{L}$ i da $\tau : \mathbb{L} \to \mathbb{K}$.

Dakle, svaki neprazan lanac u $(\mathcal{F}, \subseteq)$ ima gornju granicu, te prema Zornovoj lemi postoji maksimalan član λ u $\mathcal{F}$. Neka je $L' = \operatorname{dom} \lambda$. Tada je L' podpolje polja $\mathbb{L}$ i $F \subseteq L'$ i takođe $\lambda : \mathbb{L}' \to \mathbb{K}$, $\theta \subseteq \lambda$. Dokažimo da je $L' = L$. PP suprotno, da je $L' \subsetneq L$. Tada postoji $a \in L \setminus L'$ i s obzirom da je $\mathbb{L}$ algebarsko raširenje polja $\mathbb{F}$, a je algebarski nad $\mathbb{L}'$. Neka je $f \in L'[x]$ minimalni polinom za a. Tada je f nesvodljiv nad $\mathbb{L}$, te je $\mathbb{L}'(a) \leq \mathbb{L}$ Kronekerova ekstenzija polja $\mathbb{L}'$.

Dalje, $\lambda L' = \operatorname{Im} \lambda$ je izomorfna slika polja L' i $\lambda L' \subseteq \mathbb{K}$. Neka je f' korespodentan polinom polinomu f u odnosu na λ, tj. ako je $f(x) = \sum_i a_i x^i$, onda $f'(x) = \sum_i \lambda(a_i) x^i$. S obzirom da je $\mathbb{K}$ algebarski zatvoreno polje, postoji $b \in K$ tako da je $f'(b) = 0$. f' je nesvodljiv (jer je f nesvodljiv), pa je $(\lambda L')(b)$ Kronekerova ekstenzija polja $\lambda L'$.
Prema Teoremi 16.5 (Zadatak 16.7) postoji $\lambda' : \mathbb{L}'(a) \cong (\lambda L')(b)$, $\lambda \subsetneq \lambda'$ i $\lambda' \in \mathcal{F}$, suprotno izboru monomorfizma λ (da je maksimalan).

Dakle, $L = L'$. ■

21.2. <u>Posledica</u> Neka su $\mathbb{F}$, $\mathbb{L}$ i $\mathbb{K}$ algebarska polja i neka su $\sigma : \mathbb{F} \to \mathbb{K}$ i $\tau : \mathbb{F} \to \mathbb{L}$. Ako je $\mathbb{K}$ algebarski zatvoreno i ako je $\mathbb{L}$ algebarsko raširenje polja $\tau\mathbb{F}$, tada postoji $\lambda : \mathbb{L} \to \mathbb{K}$, $\lambda \circ \tau = \sigma$.

$$\begin{tikzcd} \mathbb{L} \arrow[rr, dashed, "\lambda"] & & \mathbb{K} \\ & \mathbb{F} \arrow[ul, "\tau"] \arrow[ur, "\sigma"'] & \end{tikzcd}$$

<u>Dokaz</u>

$$\begin{tikzcd} \mathbb{L} \arrow[r, dashed, "\lambda"] & \mathbb{K} \\ \tau\mathbb{F} \arrow[u, phantom, "\subseteq" description] \arrow[r, "\sigma\circ\tau^{-1}"] & \sigma\mathbb{K} \arrow[u, phantom, "\subseteq" description] \end{tikzcd}$$

Primenimo prethodnu lemu na $\theta = \sigma \circ \tau^{-1}$.

■

Primetimo da je Teorema 20.16. posledica Teoreme 21.1. Naime, ako uz ostale uslove u Teoremi 21.1. pretpostavimo da je θ izomorfizam, da je $\mathbb{K}$ algebarsko raširenje polja $\mathbb{E}$ i da je $\mathbb{L}$ algebarski zatvoreno, onda λ mora biti izomorfizam.

Neka je $\mathbb{E}$ algebarsko raširenje polja $\mathbb{F}$ i neka je $\mathbb{K}$ algebarski zatvoreno polje. Ako je $\sigma : \mathbb{F} \to \mathbb{K}$, onda prema prethodnoj posledici (birajući $\tau = i_{\mathbb{F}}$ - inkluziono preslikavanje) postoji ekstenzija $\sigma^* \supseteq \sigma$, $\sigma^* : \mathbb{E} \to \mathbb{K}$

$$\begin{tikzcd} \mathbb{E} \arrow[r, dashed, "\sigma^*"] & \mathbb{K} \\ \mathbb{F} \arrow[u, phantom, "\subseteq" description] \arrow[ur, "\sigma"'] & \end{tikzcd}$$

Primetimo da je $\sigma\mathbb{F} \leq \mathbb{K}$, $\sigma^*\mathbb{E} \leq \mathbb{K}$ i da je $\sigma^*\mathbb{E}$ algebarsko raširenje polja $\sigma\mathbb{F}$. Dakle, $\sigma^*\mathbb{E}$ sadržano je u algebarskom zatvorenju $\overline{\sigma \mathbb{F}} \leq \mathbb{K}$ polja $\sigma\mathbb{F}$. Otuda u daljem razmatranju pretpostavljamo da je $\mathbb{K}$ algebarsko zatvorenje polja $\sigma\mathbb{F}$. Neka je

$\mathcal{F}_{\sigma,\mathbb{K}} = \{ \lambda \mid \lambda : \mathbb{E} \to \mathbb{K},\ \sigma \leq \lambda \}$. Dokazaćemo da broj ekstenzija utapanja σ na $\mathbb{E}$ ne zavisi od izbora utapanja σ niti od polja $\mathbb{K}$.

21.3. <u>Teorema.</u> Neka je $\mathbb{E}$ algebarsko raširenje polja $\mathbb{F}$ i neka su $\tau : \mathbb{F} \to \mathbb{K}$, $\sigma : \mathbb{F} \to \mathbb{L}$, gde $\mathbb{K} = \overline{\tau\mathbb{F}}$, $\mathbb{L} = \overline{\sigma\mathbb{F}}$.

Tada $|\mathcal{F}_{\tau,\mathbb{K}}| = |\mathcal{F}_{\sigma,\mathbb{L}}|$.

Dokaz

$$\begin{tikzcd}
\mathbb{L} \arrow[r, dashed, "\lambda"] & \mathbb{K} \\
\sigma\mathbb{F} \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, "\tau\circ\sigma^{-1}"] & \tau\mathbb{F} \arrow[u, phantom, sloped, "\subseteq"]
\end{tikzcd}$$

Prema teoremi 20.16. postoji izomorfizam $\lambda : \mathbb{L} \xrightarrow{\approx} \mathbb{K}$ koji produžuje $\tau\circ\sigma^{-1}$.
Neka je $\Phi : \sigma^* \longmapsto \lambda\circ\sigma^*$, $\sigma^* \in \mathcal{F}_{\sigma,\mathbb{L}}$.
Dokazujemo da $\Phi : \mathcal{F}_{\sigma,\mathbb{L}} \xrightarrow[1-1]{na} \mathcal{F}_{\tau,\mathbb{K}}$

$$\begin{tikzcd}
\mathbb{L} \arrow[rr, "\lambda"] & & \mathbb{K} \\
& \mathbb{E} \arrow[ul, "\sigma^*"'] \arrow[ur, dashed, "\tau^*"] & \\
\sigma\mathbb{F} \arrow[uu, phantom, sloped, "\subseteq"] & \mathbb{F} \arrow[l, "\sigma"'] \arrow[r, "\tau"] \arrow[u, phantom, sloped, "\subseteq"] & \tau\mathbb{F} \arrow[uu, phantom, sloped, "\subseteq"]
\end{tikzcd}$$

Neka je $\tau^* = \lambda\circ\sigma^*$.
Uzimajući restrikcije na $\mathbb{F}$ dobijamo $\tau^*|_{\mathbb{F}} = (\lambda\circ\sigma^*)|_{\mathbb{F}} = (\tau\circ\sigma^{-1})\circ\sigma = \tau$, tj. τ^* je utapanje polje $\mathbb{E}$ u $\mathbb{K}$ koje produžuje τ. Dakle, $\Phi : \mathcal{F}_{\sigma,\mathbb{L}} \to \mathcal{F}_{\tau,\mathbb{K}}$.

Dalje, ako $\Phi(\sigma_1^*) = \Phi(\sigma_2^*)$ onda $\lambda\circ\sigma_1^* = \lambda\circ\sigma_2^*$, tj.
$\lambda^{-1}\circ(\lambda\circ\sigma_1^*) = \lambda^{-1}\circ(\lambda\circ\sigma_2^*)$ tj. $\sigma_1^* = \sigma_2^*$. Dakle Φ je $\underline{1-1}$.
Za dato $\tau^* : \mathbb{E} \longrightarrow \mathbb{K}$, neka je $\sigma^* := \lambda^{-1}\circ\tau^*$. Tada $\Phi(\sigma^*) = \tau^*$
dakle Φ je <u>na</u>. ■

Prema prethodnom za dato polje $\mathbb{F}$ i njegovu algebarsku ekstenziju $\mathbb{E}$, $|\mathcal{F}_{\sigma,\mathbb{L}}|$ je konstanta.

21.4 <u>Definicija</u> Neka je $\mathbb{E}$ algebarska ekstenzija polja $\mathbb{F}$. Separabilni stepen polja $\mathbb{E}$ nad $\mathbb{F}$ je
$$|\mathbb{E} : \mathbb{F}|_s = |\mathcal{F}_{\sigma,\mathbb{L}}| .$$

21.5. <u>Teorema</u> Neka su $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ polja. Tada
$$|\mathbb{K} : \mathbb{F}|_s = |\mathbb{K} : \mathbb{E}|_s \cdot |\mathbb{E} : \mathbb{F}|_s .$$

<u>Dokaz</u> Neka je $\sigma : \mathbb{F} \longrightarrow \mathbb{L}$ utapanje polja $\mathbb{F}$ u algebarski zatvoreno polje $\mathbb{L}$ i neka je $\mathcal{F}_{\sigma,\mathbb{L}} = \{\sigma_i \mid i\in I\}$ skup svih produženja σ na $\mathbb{E}$. Dalje neka je za svako $i\in I$, $\mathcal{F}_{\sigma_i,\mathbb{L}} = \{\tau_{ij} \mid j\in J\}$ skup svih produženja utapanja σ_i na $\mathbb{K}$. Za svako i mogli smo uzeti isti skup indeksa J s obzirom na Teoremu 21.3 i prema istom tvrđenju $|J| = |\mathcal{F}_{\sigma_i,\mathbb{L}}| = |\mathbb{K}:\mathbb{E}|_s$. Takođe $|I| = |\mathcal{F}_{\sigma,\mathbb{L}}| = |\mathbb{E}:\mathbb{F}|_s$.
Otuda $|\{\tau_{ij} \mid i\in I, j\in J\}| = |I\times J| = |\mathbb{K}:\mathbb{E}|_s \cdot |\mathbb{E}:\mathbb{F}|_s$.
Očigledno $\{\tau_{ij} \mid i\in I, j\in J\} \subseteq \{\tau \mid \sigma\subseteq\tau,\ \tau:\mathbb{K}\to\mathbb{L}\}$. S druge strane, ako $\tau:\mathbb{K}\to\mathbb{L}$, $\sigma\subseteq\tau$, onda $\sigma|_{\mathbb{E}} = \sigma_i$ za neki $i\in I$ pa za neki $j\in J$ $\tau=\tau_{ij}$.
Dakle, $\{\tau_{ij} \mid i\in I, j\in J\} = \{\tau \mid \sigma\subseteq\tau,\ \tau:\mathbb{K}\to\mathbb{L}\}$, te $|\mathbb{K}:\mathbb{F}|_s = |I\times J| = |\mathbb{K}:\mathbb{E}|_s \cdot |\mathbb{E}:\mathbb{F}|_s$. ■

21.6. Neka je $\mathbb{E} \supseteq \mathbb{F}$ algebarsko raširenje polja $\mathbb{F}$ i pretpostavimo da je $\mathbb{E} = \mathbb{F}(a)$. Dalje, neka su $\sigma, \tau : \mathbb{F}(a) \to \mathbb{K}$ utapanja polja $\mathbb{F}(a)$ u $\mathbb{K}$ takva da je $\sigma/F = \tau/F$. S obzirom da je a algebarski element nad $\mathbb{F}$, postoji $f \in \mathbb{F}[x]$ tako da je $f(a)=0$. Označimo sa σf korespodentni polinom u odnosu na σ, tj. ako je $f(x) = \sum_i f_i x^i$, tada $(\sigma f) x = \sum_i (\sigma f_i) x$. Tada je očigledno $\sigma f = \tau f$ (jer $\sigma/F = \tau/F$). S obzirom da je σ homomorfizam biće $(\sigma f)(\sigma(a)) = 0$, dakle $\sigma(a)$ je koren polinoma σf. Dakle, ako je $n = \deg f$, tada je broj mogućih vrednosti za $\sigma(a)$ manji ili jednak n. S druge strane ako $\sigma(a) = \tau(a)$ onda $\sigma = \tau$ jer je $\mathbb{F}(a)$ generisano skupom $F \cup \{a\}$ i $\sigma/F = \tau/F$. Dakle

$$|\{\tau \mid \tau : \mathbb{F}(a) \to \mathbb{K},\ \tau/F = \sigma/F\}| \leq n = \deg f.$$

Ako za f izaberemo minimalan polinom onda $|\mathbb{F}(a):\mathbb{F}| = n$, pa

(1) $$|\{\tau \mid \tau : \mathbb{F}(a) \to \mathbb{K},\ \tau/F = \sigma/F\}| \leq |\mathbb{F}(a):\mathbb{F}|.$$

Otuda, ako je $\theta : \mathbb{F}(a) \to \mathbb{K}$ i $\mathbb{K}$ je algebarski zatvoreno polje, s obzirom da je $\mathcal{F}_{\theta\mathbb{K}} = \{\tau \mid \tau : \mathbb{F}(a) \to \mathbb{K},\ \theta \leq \tau\} = \{\tau \mid \tau : \mathbb{F}(a) \to \mathbb{K}, \tau/F = \sigma/F = \theta\}$ gde je $\theta \leq \sigma$. Dakle, prema (1) imamo

21.7. <u>Teorema</u> $|\mathbb{F}(a):\mathbb{F}|_s \leq |\mathbb{F}(a):\mathbb{F}|$. ∎

Ako je $\mathbb{E} \supseteq \mathbb{F}$ konačno algebarsko raširenje polja $\mathbb{F}$, onda za neke $a_1, \dots, a_n \in E$, $\mathbb{E} = F(a_1, \dots, a_n)$ i kako je

$$|\mathbb{E}:\mathbb{F}| = |\mathbb{E} : \mathbb{F}(a_1, \dots, a_{n-1})| \cdots |\mathbb{F}(a_1):\mathbb{F}|$$

i prema 21.7. $|\mathbb{F}(a_1, \dots, a_i) : \mathbb{F}(a_1, \dots, a_{i-1})|_s \leq |\mathbb{F}(a_1, \dots, a_i) : \mathbb{F}(a_1, \dots, a_{i-1})|$ to imamo

21.8. <u>Teorema</u> Ako je $\mathbb{E}$ konačno algebarsko raširenje polja $\mathbb{F}$ onda $|\mathbb{E}:\mathbb{F}|_s \leq |\mathbb{E}:\mathbb{F}|$. ∎

Razmotrimo granični slučaj, kada je $|\mathbb{E}:\mathbb{F}|_s = |\mathbb{E}:\mathbb{F}|$.

21.9. <u>Teorema</u> Neka je $\mathbb{E} \supseteq \mathbb{F}$ konačno algebarsko raširenje polja $\mathbb{F}$. Tada $|\mathbb{E}:\mathbb{F}|_s = |\mathbb{E}:\mathbb{F}|$ akko je $\mathbb{E}$ separabilna ekstenzija polja $\mathbb{F}$.

<u>Dokaz</u> ($\Rightarrow$) PP $|\mathbb{E}:\mathbb{F}|_s = |\mathbb{E}:\mathbb{F}|$. Neka je $a \in \mathbb{E}$. Dokažimo da je a koren nekog separabilnog polinoma $f \in \mathbb{F}[x]$ (tj. f nema višestruke korene). Kako je

$$|\mathbb{E}:\mathbb{F}| = |\mathbb{E}:\mathbb{F}(a)| \cdot |\mathbb{F}(a):\mathbb{F}| \quad i$$
$$|\mathbb{E}:\mathbb{F}|_s = |\mathbb{E}:\mathbb{F}(a)|_s \cdot |\mathbb{F}(a):\mathbb{F}|_s \quad \text{to}$$
$$|\mathbb{E}:\mathbb{F}(a)| \cdot |\mathbb{F}(a):\mathbb{F}| = |\mathbb{E}:\mathbb{F}(a)|_s \cdot |\mathbb{F}(a):\mathbb{F}|_s$$

S obzirom da je $|\mathbb{E}:\mathbb{F}(a)|_s \leq |\mathbb{E}:\mathbb{F}(a)|$ i $|\mathbb{F}(a):\mathbb{F}|_s \leq |\mathbb{F}(a):\mathbb{F}|$ sledi $|\mathbb{F}(a):\mathbb{F}|_s = |\mathbb{F}(a):\mathbb{F}| = n$,

gde je $n = \deg f$, $f \in \mathbb{F}[x]$ je minimalni polinom za a.

$$\begin{tikzcd} \mathbb{F}(a) \arrow[r, "\sigma_i"] & \overline{\mathbb{F}} \\ \mathbb{F} \arrow[u, phantom, "\cup" description] \arrow[ur, hook] & \end{tikzcd}$$

Dakle, postoje n utapanja $\sigma_1, \dots, \sigma_n$ koja produžuju inkluziono preslikavanje $i_{\mathbb{F}}: \mathbb{F} \to \overline{\mathbb{F}}$, $\sigma_i : \mathbb{F}(a) \hookrightarrow \overline{\mathbb{F}}$, $i = 1, \dots, n$. S obzirom da je $\sigma_i|\mathbb{F} = \sigma_j|\mathbb{F}$ i $\mathbb{F}(a)$ je generisano sa $\mathbb{F} \cup \{a\}$, to za $i \neq j$, $\sigma_i(a) \neq \sigma_j(a)$.

S druge strane, $\sigma_i(a)$ je koren polinoma f (jer $f(a) = 0$), pa f ima n različitih korena i $\deg f = n$, pa je f separabilan.

($\Leftarrow$) Neka je $\mathbb{E}$ konačna separabilna ekstenzija polja $\mathbb{F}$. Prema Teoremi 19.11 (teorema o primitivnom elementu) postoji $b \in \mathbb{E}$ tako da je $\mathbb{E} = \mathbb{F}(b)$. Ako je $f \in \mathbb{F}[x]$ minimalan polinom za b, tada je f nesvodljiv pa kako je b separabilan, to je f separabilan (vidi 19.5), tj. f ima n različitih korena $b_1, \dots, b_n$ u $\overline{\mathbb{F}}$, $n = \deg f$. Tada je $\mathbb{F}(b_i) \subseteq \overline{\mathbb{F}}$ Kroneckerova ekstenzija polja $\mathbb{F}$ i postoji $\sigma_i : \mathbb{F}(b) \cong \mathbb{F}(b_i)$, dakle $\sigma_i : \mathbb{E} \to \overline{\mathbb{F}}$, $i = 1, \dots, n$, i pritom $\sigma_i(b) = b_i$. Dakle $\sigma_1, \dots, \sigma_n$ su različita utapanja polja $\mathbb{F}(b)$ u $\overline{\mathbb{F}}$ (jer $b_i \neq b_j$, za $i \neq j$). Dakle, $|\mathbb{E}:\mathbb{F}|_s \geq n$. S druge strane $|\mathbb{E}:\mathbb{F}| = \deg f = n$, pa kako $|\mathbb{E}:\mathbb{F}|_s \leq |\mathbb{E}:\mathbb{F}|$ sledi $|\mathbb{E}:\mathbb{F}|_s = |\mathbb{E}:\mathbb{F}|$. ∎

21.6. <u>Primer</u> (rešenje zadatka 19.7). Ako je $\mathbb{E} = \mathbb{F}(a)$ i a je separabilan nad $\mathbb{F}$ tada je $\mathbb{F}(a)$ separabilno raširenje polja $\mathbb{F}$ (tj. svaki $f \in \mathbb{F}[x]$ minimalni polinom za $b \in \mathbb{E}$ je separabilan). Zaista ako je a i $b_1, \dots, b_n \in \overline{\mathbb{F}}$ su različiti koreni polinoma f u $\overline{\mathbb{F}}$, tada postoje $\sigma_i : \mathbb{F}(a) \to \overline{\mathbb{F}}$, $\sigma_i(a) = b_i$ (vidi preth. dokaz ($\Leftarrow$)), te $|\mathbb{F}(a):\mathbb{F}|_s = |\mathbb{F}(a):\mathbb{F}|$.

21.7. <u>Zadatak</u> Neka je $\mathbb{F}(a_1, \dots, a_n) \supseteq \mathbb{F}$ algebarska ekstenzija polja $\mathbb{F}$. Ako su $a_1, \dots, a_n$ separabilni nad $\mathbb{F}$, tada je $\mathbb{F}(a_1, \dots, a_n)$ separabilna ekstenzija polja $\mathbb{F}$.

21.8. Zadatak Odrediti sva utapanja $\sigma : \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{A}$, $\mathbb{A}$ je polje algebarskih brojeva. Odrediti $|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}|_s$.

21.9. Zadatak Odrediti sva utapanja $\sigma : \mathbb{Q}(\varepsilon) \longrightarrow \mathbb{A}$, $\varepsilon = e^{\frac{2\pi i}{p}}$, $p \in Prost$

21.10. Zadatak Neka je $\varepsilon = e^{\frac{2\pi i}{p}}$, $p \in Prost$. Ako $\sigma : \mathbb{Q}(\varepsilon) \longrightarrow \mathbb{C}$, $\mathbb{C}$ je polje kompleksnih brojeva, tada $\sigma : \mathbb{Q}(\varepsilon) \longrightarrow \mathbb{A}$, $\mathbb{A}$ je polje algebarskih brojeva.

21.11. Z. Dokazati da postoji beskonačno mnogo prostih brojeva p takvih da $f(x) = x^2 + x + 1$ ima koren u $\mathbb{Z}_p$.

21.12. Z Ako je $|\mathbb{E} : \mathbb{F}| < \infty$ tada $|\mathbb{E} : \mathbb{F}|_s$ deli $|\mathbb{E} : \mathbb{F}|$.

21.13. Z. Ako je $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{C}$ tada $|\mathbb{F} : \mathbb{Q}|_s = |\mathbb{F} : \mathbb{Q}|$.

21.14. Z Ako je $\sigma : \mathbb{E} \longrightarrow \overline{\mathbb{F}}$, $\sigma / \mathbb{F} = i_{\mathbb{F}}$, $\mathbb{E} \supseteq \mathbb{F}$, $\mathbb{E} = \mathbb{F}(a)$, tada $\sigma(\mathbb{E}) \subseteq \mathbb{K}$ gde je $\mathbb{K} \subseteq \overline{\mathbb{F}}$ korensko polje minimalnog polinoma za a. Napomena: najpre dokažite da je a algebarski nad $\mathbb{F}$!

21.15. Z. Ako $|\mathbb{F}(a) : \mathbb{F}|_s < |\mathbb{F}(a) : \mathbb{F}|$ tada je $\mathbb{F}$ proste karakteristike p i za neki n $|\mathbb{F}(a) : \mathbb{F}| = p^n \cdot |\mathbb{F}(a) : \mathbb{F}|_s$.

22. Normalna raširenja algebarskih polja

Neka je $\mathbb{E} \supseteq \mathbb{F}$ algebarsko raširenje polja $\mathbb{F}$. $\mathbb{E}$ je normalno raširenje polja $\mathbb{F}$ ukoliko za svaki nesvodljivi polinom $f \in \mathbb{F}[x]$ važi: ako f ima koren u $\mathbb{E}$ tada se f razlaže na linearne faktore u $\mathbb{E}$. Drugim rečima, ako $\mathbb{E}$ sadrži bar jedan koren polinoma f, tada $\mathbb{E}$ sadrži korensko polje polinoma f.

22.1. Teorema Neka je $\mathbb{F} \subseteq \mathbb{E} \subseteq \overline{\mathbb{F}}$. Tada su sledeći uslovi ekvivalentni:

1° Ako $\sigma : \mathbb{E} \longrightarrow \overline{\mathbb{F}}$, $\sigma / \mathbb{F} = i_{\mathbb{F}}$, tada $\sigma \in Aut\, \mathbb{E}$.

2° $\mathbb{E}$ je faktorsko polje neke familije polinoma nad $\mathbb{F}$.

3° $\mathbb{E}$ je normalno raširenje polja $\mathbb{F}$.

Napomena: $\mathbb{E}$ je faktorsko polje familije polinoma $\mathcal{F} \subseteq \mathbb{F}[x]$ ako:
- svaki $f \in \mathcal{F}$ ima linearnu faktorizaciju u $\mathbb{E}$
- $\mathbb{E}$ je generisano nad korenima polinoma $f \in \mathcal{F}$.

Dokaz $(1^\circ \Rightarrow 3^\circ)$ PP da važe uslovi u 1°. Dokažimo da je $\mathbb{E}$ normalno raširenje polja $\mathbb{F}$. Neka je $f \in \mathbb{F}[x]$ nesvodljiv nad $\mathbb{F}$ i pp da je $f(a)=0$ za neki $a \in E$. Neka je $b \in \overline{F}$ bilo koji koren polinoma f u $\overline{\mathbb{F}}$. S obzirom da su $\mathbb{F}(a)$ i $\mathbb{F}(b)$ prosta (Kroneckerova) proširenja istog nesvodljivog polinoma, postoji $\tau : \mathbb{F}(a) \cong \mathbb{F}(b)$, $\tau(a)=b$ i $\tau | F = i_F$. Kako je $\mathbb{E}$ algebarsko raširenje polja $\mathbb{F}(a)$, τ se produžuje do utapanja $\sigma : \mathbb{E} \to \overline{\mathbb{F}}$ (vidi Teoremu 21.1). Ali prema uslovima 1°, $\sigma : \mathbb{E} \cong \mathbb{E}$, tj. $\sigma(a) \in E$, dakle $b \in E$. Dakle svi koreni polinoma f koji leže u $\overline{\mathbb{F}}$ nalaze se i u $\mathbb{E}$. S obzirom da f ima linearnu faktorizaciju u $\overline{\mathbb{F}}$ to onda f ima linearnu faktorizaciju i u $\mathbb{E}$.

$$\begin{tikzcd}
\mathbb{E} \arrow[rr, dashed, "\sigma"] & & \overline{\mathbb{F}} \\
\mathbb{F}(a) \arrow[u, phantom, "\cup" description] \arrow[rr, "\tau"] & & \mathbb{F}(b) \arrow[u, phantom, "\cup" description] \\
& \mathbb{F} \arrow[ul, phantom, "\subseteq" description] \arrow[ur, phantom, "\subseteq" description] &
\end{tikzcd}$$

$(3^\circ \Rightarrow 2^\circ)$ PP da važi 3°. Dokažimo da važi 2°. Neka je

$$\mathcal{F} = \{ f \in \mathbb{F}[X] \mid f \text{ je nesvodljiv nad } \mathbb{F},\ f \text{ ima koren u } \mathbb{E} \}$$

Neka je $S = \{ a \in E \mid \bigvee_{f \in \mathcal{F}} f^{\mathbb{E}}(a) = 0 \}$. Očigledno $S \subseteq E$. S druge strane, ako $a \in E$ s obzirom da je $\mathbb{E}$ algebarsko raširenje polja a je koren nekog nesvodljivog (minimalnog) polinoma $f \in \mathbb{F}[X]$ i prema 3° f ima linearnu faktorizaciju u $\mathbb{E}$, dakle $f \in \mathcal{F}$ i $a \in S$.

$(2^\circ \Rightarrow 1^\circ)$ PP da važi 2°. Dokažimo da važi 1°. Neka je $\mathbb{E} = \mathbb{F}(S)$ gde je S skup korena polinoma iz familije $\mathcal{F} \subseteq \mathbb{F}[X]$ takve da $\mathbb{E}$ sadrži korensko polje svakog polinoma $f \in \mathcal{F}$. Neka je $\sigma : \mathbb{E} \to \overline{\mathbb{F}}$. Ako $a \in S$ tada $f^{\mathbb{E}}(a) = 0$ gde $f \in \mathcal{F}$, te $f^{\overline{\mathbb{F}}}(\sigma(a)) = 0$, tj. $\sigma(a)$ je koren polinoma f u polju $\overline{\mathbb{F}}$. S obzirom da je $\mathbb{E} \subseteq \overline{\mathbb{F}}$, polinom f ima istu linearnu faktorizaciju u $\mathbb{E}$ i $\overline{\mathbb{F}}$, dakle $\sigma a \in E$, odnosno $\sigma a \in S$ jer σa je koren polin. f i $f \in \mathcal{F}$. Neka je $b \in \mathbb{F}(S)$. Tada postoji $p \in \mathbb{F}[x_1, \ldots, x_n]$ i $a_1, \ldots, a_n \in S$ takvi da $b = p^{E}(a_1, \ldots, a_n)$ pa $\sigma b = p^{\overline{\mathbb{F}}}(\sigma a_1, \ldots, \sigma a_n)$. S obzirom da $\sigma a_1, \ldots, \sigma a_n \in E$ i $\mathbb{E} \subseteq \overline{\mathbb{F}}$ to $p^{\overline{\mathbb{F}}}(\sigma a_1, \ldots, \sigma a_n) = p^{E}(\sigma a_1, \ldots, \sigma a_n)$, tj. $\sigma b \in E$.

22.2. Primer 1° Ako je b koren polin. $f(x) = x^2 - a$, $a \in \mathbb{Q}$, $b \in \mathbb{C}$ tada je $\mathbb{Q}(b)$ normalno proširenje polja $\mathbb{Q}$ jer je $\mathbb{Q}(b)$ korensko polje za $\mathcal{F} = \{f\}$. Primetimo da je u $\mathbb{Q}(b)$ $f(x) = (x-b)(x+b)$.

2° $\mathbb{Q}(\sqrt[3]{2})$ nije normalno proširenje polja $\mathbb{Q}$ jer $\sqrt[3]{2}$ je koren polinoma $f(x) = x^3 - 2$ i $f(x)$ nema linearnu faktorizaciju u $\mathbb{Q}(\sqrt[3]{2})$. Primetimo da je u $\mathbb{C}$ $x^3 - 2 = (x - \sqrt[3]{2})(x - \varepsilon\sqrt[3]{2})(x - \varepsilon^2\sqrt[3]{2})$, gde $\varepsilon = e^{\frac{2\pi i}{3}}$.

23. Galoava proširenja algebarskih polja

Évariste Galois (1811-1832) razvio je svoju teoriju radi rešenja starog problema iz algebre: da se za datu algebarsku jednačinu nađe "formula" koja opisuje rešenja te jednačine. Kvadratnu jednačinu umeli su da rešavaju već matematičari antičke Grčke (Euklid, Hipark, Heron, Diofant), zatim u Indiji Brahmagupta (6 v.), i to sa negativnim koeficijentima. Metoda kako se danas koristi potiče od Baskare (12 v.). Opšta jednačina $f(x)=0$ stepena 3 i 4 rešena je tokom 16. veka od strane italijanskih matematičara. Zanimljiv istorijat rešavanja ovog problema može se naći u knjizi "Viša algebra" Đure Kurepe.
Galoa je uz pomoć svoje teorije dokazao da u opštem slučaju nije moguće rešiti jednačin 5. stepena uz pomoć osnovnih aritmetičkih operacija i korenovanja (radikala). Osnovna ideja njegove teorije je da se raširenjima datog polja (na pr. $\mathbb{Q}$) pridruži određena grupa. Ako je raširenje korensko polje polinoma f onda ova grupa određuje rešivost ove jednačine. U slučaju $f \in \mathbb{Q}[x]$, $f(x)=0$ biće rešiva pomoću radikala akko je pridružena grupa rešiva. Teoriju Galoa razvijali su i drugi matematičari, Kroneker, Kumer, Hilbert, Artin.

23.1. Definicija Raširenje $\mathbb{E} \supseteq \mathbb{F}$ je Galoaovo ukoliko je ono
1° konačno,
2° separabilno,
3° normalno.

Ako je $\mathbb{E} \supseteq \mathbb{F}$ galoaovo raširenje vidimo da je ono algebarsko s obzirom da je $|\mathbb{E} : \mathbb{F}| < \infty$ (Teorema 15.4.)
Ako je $\mathbb{E}$ korensko polje polinoma $f \in \mathbb{F}[x]$, tada je prema T. 22.1 normalno i konačno, vidi 17.5).
Ako je $\mathbb{E}$ algebarsko raširenje brojevnog polja $\mathbb{F}$ (opštije polja karakteristike 0) tada je ono separabilno (videti 19.5).

Otuda, važi sledeće tvrđenje

23.2 <u>Teorema</u> Neka je $\mathbb{F}$ polje karakteristike nula i neka je $\mathbb{E} \supseteq \mathbb{F}$ korensko polje polinoma f. Tada je $\mathbb{E}$ Galoaova raširenje polja $\mathbb{F}$.

23.3. <u>Posledica</u> 1° Neka je $\mathbb{F}$ brojevno polje i $f \in \mathbb{F}[x]$. Tada je korensko polje polinoma f Galoaovo raširenje polja $\mathbb{F}$.
2° Neka je $f \in \mathbb{Q}[x]$. Tada je korensko polje polinoma f Galoaovo.

23.4. <u>Primer</u> 1° $\mathbb{Q}(\sqrt{2})$ je Galoaovo raširenje polja $\mathbb{Q}$ (Primer 22.2.1°)
2° $\mathbb{Q}(\sqrt[3]{2})$ nije Galoaovo raširenje polja $\mathbb{Q}$ (v. Primer 22.2.2°).
Za $\varepsilon = e^{\frac{2\pi i}{3}}$, $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ je korensko polje polinoma $x^3 - 2$, dakle $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ je Galoaovo raširenje polja $\mathbb{Q}$. Primetimo da je $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ takođe Galoaovo raširenje polja $\mathbb{Q}(\sqrt[3]{2})$.
3° Ako je $n \in N^*$ i $\varepsilon = e^{\frac{2\pi i}{n}}$ (primitivni koren n-tog stepena iz jedinice), tada je $\mathbb{Q}(\varepsilon)$ Galoaovo raširenje polja $\mathbb{Q}$. Naime, svi koreni n-tog stepena iz jedinice su $1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}$, dakle leže u $\mathbb{Q}(\varepsilon)$. Odatle $\mathbb{Q}(\varepsilon)$ je korensko polje polinoma $f(x) = x^n - 1$.

23.5. Neka je $\mathbb{E}$ polje i $\sigma_1, \dots, \sigma_n \in \operatorname{Aut} \mathbb{E}$.
Tada je $\mathbb{F} = \{ a \in E \mid \sigma_1 x = \dots = \sigma_n x = x \}$ podpolje polja $\mathbb{E}$ (proverite!). Ovo polje naziva se <u>invarijantnim</u> ili <u>nepokretnim</u> poljem automorfizama $\sigma_1, \dots, \sigma_n$ i obeležavamo ga pomoću $\mathbb{F} = \mathbb{F}(\mathbb{E}, \sigma_1, \dots, \sigma_n)$. Ako je $G = \{\sigma_1, \dots, \sigma_n\}$ podgrupa grupe $\operatorname{Aut} \mathbb{E}$, koristimo oznaku $\mathbb{F} = \mathbb{F}(\mathbb{E}, G)$. Negde se koristi i oznaka $\mathbb{F} = \mathbb{E}^G$.

23.6. <u>Galoaova grupa</u> Neka su $\mathbb{F}$ i $\mathbb{E}$ polja i $\mathbb{F} \subseteq \mathbb{E}$ i neka je
$G = \{ \sigma \in \operatorname{Aut} \mathbb{E} \mid \sigma \restriction F = i_F \} = \{ \sigma \in \operatorname{Aut} \mathbb{E} \mid \bigwedge_{x \in F} \sigma x = x \}$.
Nije teško proveriti da je $G < \operatorname{Aut} \mathbb{E}$ (tj. G je podgrupa grupe $\operatorname{Aut} \mathbb{E}$).
Ovu grupu obeležavamo sa $G = G(\mathbb{E}/\mathbb{F})$.
Ako je $\mathbb{E}$ Galoaovo raširenje polja $\mathbb{F}$, tada grupu $G(\mathbb{E}/\mathbb{F})$ nazivamo Galoaovom grupom polja $\mathbb{E}$ nad $\mathbb{F}$.

24. O notaciji

Neka su $\mathbb{A}$ i $\mathbb{B}$ algebre istog jezika (iste signature) L. Tada $\sigma : \mathbb{A} \longrightarrow \mathbb{B}$ označava činjenicu da je σ homomorfizam iz algebre $\mathbb{A}$ u algebru $\mathbb{B}$. U sledećim definicijama $\mathbb{E}$ i $\mathbb{F}$ su algebarska polja, mada se deo tih definicija može preneti na proizvoljne algebre.

24.1. <u>Definicija</u> 1° $\mathrm{Hom}(\mathbb{F}, \mathbb{E}) = \{\sigma \mid \sigma : \mathbb{F} \longrightarrow \mathbb{E}\}$.

2° $\mathrm{Mon}(\mathbb{F}, \mathbb{E}) = \{\sigma \mid \sigma : \mathbb{F} \longrightarrow \mathbb{E},\ \sigma \text{ je } 1\text{-}1\}$.

Dakle, elementi skupa $\mathrm{Mon}(\mathbb{F}, \mathbb{E})$ su monomorfizmi, odnosno utapanja polja $\mathbb{F}$ u polje $\mathbb{E}$.

3° Neka su $\mathbb{F}, \mathbb{E}$ i $\mathbb{K}$ algebarska polja i pretpostavimo $\mathbb{F} \le \mathbb{E}$, $\mathbb{F} \le \mathbb{K}$.

$\mathrm{Hom}(\mathbb{E} \mid \mathbb{F}, \mathbb{K}) = \{\sigma \mid \sigma : \mathbb{E} \longrightarrow \mathbb{K},\ \sigma|F = i_F\}$.

Ovde je $i_F : F \to F$ inkluziono preslikavanje, tj. $\bigwedge_{a \in F} i_F(a) = a$.

$\sigma|F$ je restrikcija preslikavanja σ na F. Da je $\sigma|F = \tau$, drugačije možemo zapisati $\tau \le \sigma$.

4° Pretpostavimo $\mathbb{F} \le \mathbb{E}$, $\sigma : \mathbb{F} \longrightarrow \mathbb{K}$, $\mathbb{F}, \mathbb{E}, \mathbb{K}$ su polja.

$\mathrm{Hom}(\mathbb{E}|_\sigma \mathbb{F}, \mathbb{K}) = \{\tau \mid \tau : \mathbb{E} \longrightarrow \mathbb{K},\ \sigma \le \tau\}$.

$$(D)\quad \begin{tikzcd} \mathbb{E} \arrow[r, "\tau"] & \mathbb{K} \\ \mathbb{F} \arrow[u, phantom, "\cup" rotate=90] \arrow[ur, "\sigma"'] & \end{tikzcd}$$

Dakle, $\mathrm{Hom}(\mathbb{E}|_\sigma \mathbb{F}, \mathbb{K})$ je skup homomorfizama τ takvih da dijagram (D) komutira.

Ako je $\mathbb{F} \le \mathbb{K}$, tada $\mathrm{Hom}(\mathbb{E} | \mathbb{F}, \mathbb{K}) = \mathrm{Hom}(\mathbb{E}|_{i_F} \mathbb{F}, \mathbb{K})$.

5° $\mathrm{Aut}\,\mathbb{F} = \{\sigma \mid \sigma : \mathbb{F} \cong \mathbb{F}\}$. Dakle, $\mathrm{Aut}\,\mathbb{F}$ je skup svih automorfizama polja $\mathbb{F}$.

6° Ako je $\mathbb{F} \le \mathbb{E}$, tada $\mathrm{Aut}(\mathbb{E} | \mathbb{F}) = \{\sigma \in \mathrm{Aut}\,\mathbb{E} : \sigma|F = i_F\}$.

Dakle, $\mathrm{Aut}(\mathbb{E}|\mathbb{F})$ je skup svih automorfizama polja $\mathbb{E}$ u odnosu na koje je polje $\mathbb{F}$ <u>nepokretno</u> (invarijantno).

Neke od teorema koje smo već dokazali mogu se iskazati koristeći ove nove oznake, na sledeći način:

24.2. (4.4) a) $\mathbb{A}\mathrm{ut}\,\mathbb{F} = (\mathrm{Aut}\,\mathbb{F}, \circ, i_F)$ je grupa.

b) Ako je $\mathbb{F} \le \mathbb{E}$ tada je $\mathbb{A}\mathrm{ut}(\mathbb{E}|\mathbb{F}) = (\mathrm{Aut}(\mathbb{E}|\mathbb{F}), \circ, i_F)$ podgrupa grupe $\mathbb{A}\mathrm{ut}\,\mathbb{E}$, tj. $\mathbb{A}\mathrm{ut}(\mathbb{E}|\mathbb{F}) < \mathbb{A}\mathrm{ut}\,\mathbb{E}$.

24.1. (4.1) $\mathrm{Hom}(\mathbb{F}, \mathbb{E}) = \mathrm{Mon}(\mathbb{F}, \mathbb{E})$.

Drugim rečima, kod polja se pojmovi homomorfizma i utapanja poklapaju.

Prema Teoremi 3.3. važi:

Ako je $\mathbb{Q} \le \mathbb{E}, \mathbb{K}$, tada $\mathrm{Hom}(\mathbb{E}|\mathbb{Q}, \mathbb{K}) = \mathrm{Hom}(\mathbb{E}, \mathbb{K})$ i slično ako $\mathbb{Z}_p \le \mathbb{E}, \mathbb{K}$, $p \in \mathrm{Prost}$, $\mathrm{Hom}(\mathbb{E}|\mathbb{Z}_p, \mathbb{K}) = \mathrm{Hom}(\mathbb{E}, \mathbb{K})$.

24.2. (Teorema 21.1) Ako je $\mathbb{E} \geq \mathbb{F}$ algebarsko raširenje, $\mathbb{K}$ je algebarski zatvoreno polje i $\sigma: \mathbb{F} \to \mathbb{K}$, tada $Hom(\mathbb{E}|_\sigma \mathbb{F}, \mathbb{K}) \neq \emptyset$.

24.3. <u>Zadatak</u> Dokazati obrat od 24.2: Ako za svako algebarsko raširenje $\mathbb{E} \geq \mathbb{F}$ i svako $\sigma: \mathbb{F} \to \mathbb{K}$ važi $Hom(\mathbb{E}|_\sigma \mathbb{F}, \mathbb{K}) \neq \emptyset$, tada $\mathbb{K}$ sadrži algebarsko zatvorenje $\overline{\mathbb{F}}$ polja $\mathbb{F}$.

24.4. (Teorema 22.1) Neka je $\mathbb{E} \geq \mathbb{F}$ algebarsko raširenje. Tada:
$\mathbb{E}$ je normalno raširenje polja $\mathbb{F}$ akko $Hom(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}}) = Aut(\mathbb{E}|\mathbb{F})$.

Primetimo da je u opštem slučaju $Aut(\mathbb{E}|\mathbb{F}) \subseteq Hom(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})$.

24.5. (Teorema 21.3). Neka su $\mathbb{K}$ i $\mathbb{L}$ algebarski zatvorena polja, $\mathbb{E}|\mathbb{F}$ algebarsko i $\sigma \in Hom(\mathbb{F}, \mathbb{K})$, $\tau \in Hom(\mathbb{F}, \mathbb{L})$.

Tada $|Hom(\mathbb{E}|_\sigma \mathbb{F}, \mathbb{K})| = |Hom(\mathbb{E}|_\tau \mathbb{F}, \mathbb{L})|$.

$$\begin{tikzcd}
\mathbb{K} & & & & \mathbb{L} \\
\mathbb{E} \arrow[u, dashed, "\sigma^*"] & \geq & \mathbb{F} \arrow[ull, "\sigma"'] \arrow[urr, "\tau"] & \leq & \mathbb{E} \arrow[u, dashed, "\tau^*"']
\end{tikzcd}$$

Specijalno, $|Hom(\mathbb{E}|_\sigma \mathbb{F}, \mathbb{K})| = |Hom(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})|$

Otuda, za definiciju separabilnog stepena možemo uzeti

24.6. $|\mathbb{E}:\mathbb{F}|_s = |Hom(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})|$, gde je $\mathbb{E} \geq \mathbb{F}$ algebarska ekstenzija.

Podsećamo na osobine algebarskog stepena i separabilnog stepena:
Neka je $\mathbb{E} \geq \mathbb{F}$ algebarska ekstenzija. Tada

1° Ako je $\mathbb{K}|\mathbb{E}$ i $\mathbb{E}|\mathbb{F}$ algebarsko tada $|\mathbb{K}:\mathbb{F}|_s = |\mathbb{K}:\mathbb{E}|_s \cdot |\mathbb{E}:\mathbb{F}|_s$

2° Ako je $\mathbb{E}|\mathbb{F}$ konačna ekstenzija, tada $|\mathbb{E}:\mathbb{F}|_s \leq |\mathbb{E}:\mathbb{F}|$.

3° $|\mathbb{E}:\mathbb{F}|_s = |\mathbb{E}:\mathbb{F}|$ akko je $\mathbb{E} \geq \mathbb{F}$ separabilna ekstenzija (uz uslov da je $\mathbb{E} \geq \mathbb{F}$ konačna ekstenzija).

24.7. <u>Teorema</u> Neka je $\mathbb{E} \geq \mathbb{F}$ normalno raširenje polja $\mathbb{F}$.

Tada $|Aut(\mathbb{E}|\mathbb{F})| = |\mathbb{E}:\mathbb{F}|_s$.

<u>Dokaz</u>. $Aut(\mathbb{E}|\mathbb{F}) = Hom(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})$ i $|\mathbb{E}:\mathbb{F}|_s = |Hom(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})|$.

24.8. <u>Teorema</u> Neka je $\mathbb{E}$ konačno raširenje polja $\mathbb{F}$. Tada $|Aut(\mathbb{E}|\mathbb{F})| = |\mathbb{E}:\mathbb{F}|$ akko je $\mathbb{E}$ galoavo raširenje polja $\mathbb{F}$.

<u>Dokaz</u> Neka je $\mathbb{E} \geq \mathbb{F}$ konačno.

1° Pretpostavimo da je $\mathbb{E}$ galoavo raširenje polja $\mathbb{F}$.

Kako je $\mathbb{E}|\mathbb{F}$ normalno, prema 24.7 $|Aut(\mathbb{E}|\mathbb{F})| = |\mathbb{E}:\mathbb{F}|_s$.
Kako je $\mathbb{E}|\mathbb{F}$ separabilno, $|\mathbb{E}:\mathbb{F}|_s = |\mathbb{E}:\mathbb{F}|$. Dakle $|Aut(\mathbb{E}|\mathbb{F})| = |\mathbb{E}:\mathbb{F}|$.

2° Neka je $|Aut(\mathbb{E}|\mathbb{F})| = |\mathbb{E}:\mathbb{F}|$. Dalje $Aut(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}}) \subseteq Hom(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})$ i $|Hom(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})| = |\mathbb{E}:\mathbb{F}|_s \leq |\mathbb{E}:\mathbb{F}|$, pa $|\mathbb{E}:\mathbb{F}|_s = |\mathbb{E}:\mathbb{F}|$, tj. $\mathbb{E}|\mathbb{F}$ je separabilno. Takođe $|Aut(\mathbb{E}|\mathbb{F})| = |Hom(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})|$ i $Hom(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})$ je konačan, dakle $Aut(\mathbb{E}|\mathbb{F}) = Hom(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})$, tj. $\mathbb{E}|\mathbb{F}$ je normalno $\blacksquare$

24.9. Prema prethodnom, ako je $\mathbb{E}|\mathbb{F}$ konačno, tada

$$|\mathrm{Aut}(\mathbb{E}|\mathbb{F})| \le |\mathbb{E}:\mathbb{F}|.$$

Jednakost važi akko $\mathbb{E}|\mathbb{F}$ je galoovo!

24.10. <u>Teorema</u> Neka je $\mathbb{E}|\mathbb{F}$ algebarsko. Tada $\mathrm{Hom}(\mathbb{E}|\mathbb{F}, \mathbb{E}) = \mathrm{Aut}(\mathbb{E}|\mathbb{F})$.

<u>Dokaz</u> Neka je $\sigma: \mathbb{E} \to \mathbb{E}$, $\sigma|\mathbb{F} = i_{\mathbb{F}}$. σ je 1-1 jer se kod polja pojmovi homomorfizma i monomorfizma poklapaju.

σ je <u>na</u>: Neka je $a \in \mathbb{E}$ i $p(x) \in \mathbb{F}[x]$ minimalan polinom za a. Tada je $p(x)$ nesvodljiv nad $\mathbb{F}$. Dalje, neka su $a_1, a_2, \dots, a_n$ <u>svi</u> međusobno različiti koreni polinoma $p(x)$ u $\mathbb{E}$, $a = a_1$. Kako je $p(a_i) = 0$ to $p(\sigma_i(a_i)) = 0$, te su i $\sigma a_1, \dots, \sigma a_n$ međusobno različiti, dakle $\{\sigma a_1, \dots, \sigma a_n\} = \{a_1, \dots, a_n\}$, pa $a = a_1 = \sigma a_i$ za neki i. ∎

<u>Posledica</u> 24.10.1 Ako je $\mathbb{E}$ brojevno algebarsko polje, tada $\mathrm{Hom}(\mathbb{E}, \mathbb{E}) = \mathrm{Aut}\,\mathbb{E}$.

Zaista, $\mathrm{Hom}(\mathbb{E}, \mathbb{E}) = \mathrm{Hom}(\mathbb{E}|\mathbb{Q}, \mathbb{E}) = \mathrm{Aut}(\mathbb{E}|\mathbb{Q}) = \mathrm{Aut}\,\mathbb{E}$. Specijalno, ako je $\mathbb{A}$ polje algebarskih brojeva, tada $\mathrm{Hom}(\mathbb{A}, \mathbb{A}) = \mathrm{Aut}\,\mathbb{A}$.

24.10.2. <u>Posledica</u> Ako je $\mathbb{E}$ algebarsko raširenje polja $\mathbb{Z}_p$, $p \in$ Prost, tada $\mathrm{Hom}(\mathbb{E}, \mathbb{E}) = \mathrm{Aut}\,\mathbb{E}$.

24.11. <u>Teorema</u> Neka su $\sigma_1, \dots, \sigma_n \in \mathrm{Aut}(\mathbb{E}|\mathbb{F})$ različiti i $|\mathbb{E}:\mathbb{F}| = n$. Tada je $\mathbb{E}$ galoovo raširenje polja $\mathbb{F}$.

<u>Dokaz</u> Neposredno prema 24.9.

25. <u>Teorema galoave korespodencije</u>

U ovom odeljku dokazaćemo da postoji obostrano jednoznačna korespodencija između međupolja Galoave ekstenzije $\mathbb{E} \supseteq \mathbb{F}$ i podgrupa pridružene Galoave grupe $\mathrm{Aut}(\mathbb{E}|\mathbb{F})$.

25.1. <u>Teorema</u> Ako je $\mathbb{E} \supseteq \mathbb{F}$ normalno raširenje i $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{E}$, tada je $\mathbb{E}$ normalno raširenje polja $\mathbb{L}$.

$$\begin{array}{c} \mathbb{E} \\ \cup \\ \mathbb{L} \\ \cup \\ \mathbb{F} \end{array}$$

n n

<u>Dokaz</u> Kako je $\mathbb{E} \supseteq \mathbb{F}$ normalno, to je $\mathrm{Hom}(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}}) = \mathrm{Aut}(\mathbb{E}|\mathbb{F})$. Dalje, $\mathrm{Hom}(\mathbb{E}|\mathbb{L}, \overline{\mathbb{F}}) \subseteq \mathrm{Hom}(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})$ jer $\mathbb{F} \subseteq \mathbb{L}$ pa $\mathrm{Hom}(\mathbb{E}|\mathbb{L}, \overline{\mathbb{F}}) \subseteq \mathrm{Aut}(\mathbb{E}|\mathbb{F})$, odakle $\mathrm{Hom}(\mathbb{E}|\mathbb{L}, \overline{\mathbb{F}}) = \mathrm{Aut}(\mathbb{E}|\mathbb{L})$. Dakle, prema 24.4 $\mathbb{E}|\mathbb{L}$ je normalno. ∎

25.2. <u>Teorema</u> Ako je $\mathbb{E} \geq \mathbb{F}$ konačna i separabilna ekstenzija i $\mathbb{E} \geq \mathbb{L} \geq \mathbb{F}$, tada je $\mathbb{E}|\mathbb{L}$ i $\mathbb{L}|\mathbb{F}$ separabilno.

<u>Dokaz</u> $|\mathbb{E} : \mathbb{F}| = |\mathbb{E} : \mathbb{L}| \cdot |\mathbb{L} : \mathbb{F}|$, $|\mathbb{E} : \mathbb{F}|_s = |\mathbb{E} : \mathbb{L}|_s \cdot |\mathbb{L} : \mathbb{F}|_s$

$$\begin{tikzcd} \mathbb{E} \arrow[d, dash, "s"] \\ \mathbb{L} \arrow[d, dash, "s"] \\ \mathbb{F} \end{tikzcd} \quad (\mathbb{E}|\mathbb{F} : s)$$

$|\mathbb{E} : \mathbb{F}|_s = |\mathbb{E} : \mathbb{F}|$ (zbog separabilnosti), pa

$|\mathbb{E} : \mathbb{L}|_s \cdot |\mathbb{L} : \mathbb{F}|_s = |\mathbb{E} : \mathbb{L}| \cdot |\mathbb{L} : \mathbb{F}|$

$|\mathbb{E} : \mathbb{L}|_s \leq |\mathbb{E} : \mathbb{L}|$, $|\mathbb{L} : \mathbb{F}|_s \leq |\mathbb{L} : \mathbb{F}|$, odavde

$(m \cdot n = m' \cdot n',\ m \leq m',\ n \leq n' \Rightarrow m = m',\ n = n',\ m, n, m', n' \in \mathbb{N}^+)$

$|\mathbb{E} : \mathbb{L}|_s = |\mathbb{E} : \mathbb{L}|$, $|\mathbb{L} : \mathbb{F}|_s = |\mathbb{L} : \mathbb{F}|$, tj.

$\mathbb{E}|\mathbb{L}$ je separabilno i $\mathbb{L}|\mathbb{F}$ je separabilno. ∎

25.3. <u>Teorema</u> Neka je $\mathbb{E} \geq \mathbb{F}$ galoava ekstenzija i $\mathbb{E} \geq \mathbb{L} \geq \mathbb{F}$. Tada je $\mathbb{E}|\mathbb{L}$ galoava ekstenzija.

$$\begin{tikzcd} \mathbb{E} \arrow[d, dash, "g"] \\ \mathbb{L} \arrow[d, dash] \\ \mathbb{F} \end{tikzcd} \quad (\mathbb{E}|\mathbb{F} : g)$$

<u>Dokaz</u> Prema 25.1 i 25.2.

25.4. <u>Teorema</u> Neka je $\mathbb{E}|\mathbb{F}$ galoava ekstenzija i $G = Aut(\mathbb{E}|\mathbb{F})$.

Tada $\mathbb{F} = \mathbb{E}^G \left(= \mathcal{F}(\mathbb{E}, G) = \{ x \in E \mid \bigwedge_{\sigma \in G} \sigma x = x \}\right)$.

<u>Dokaz</u> 1° Očigledno $F \subseteq \mathbb{E}^G$.

2° <u>$\mathbb{E}^G \subseteq \mathbb{F}$</u>. Neka je $a \in \mathbb{E}^G$ i $\sigma : \mathbb{F}(a) \longrightarrow \overline{\mathbb{F}}$, $\sigma|F = i_F$, proizvoljno. Tada postoji $\tau : \mathbb{E} \longrightarrow \overline{\mathbb{F}}$, $\sigma \leq \tau$ (Teorema 24.2, odnosno 21.1). Tada τ fiksira $\mathbb{F}$ pa kako je $\mathbb{E}|\mathbb{F}$ normalno, to $\tau \in Aut(\mathbb{E}|\mathbb{F})$, tj. $\tau \in G$. Kako $a \in E^G$, to $\tau(a) = a$, dakle i $\sigma(a) = a$ jer $\sigma \leq \tau$. Prema tome imamo:

$$\begin{tikzcd} \mathbb{E} \arrow[r, dashed, "\tau"] & \overline{\mathbb{F}} \\ \mathbb{F}(a) \arrow[u, phantom, "\cup"] \arrow[ur, "\sigma"] \\ \mathbb{F} \arrow[u, phantom, "\cup"] \end{tikzcd}$$

$\sigma | F = i_F$, $\sigma(a) = a$, te $\sigma = i_{F(a)}$.

Ovim smo dokazali da je $Hom(\mathbb{F}(a)|\mathbb{F}, \overline{\mathbb{F}}) = \{ i_{\mathbb{F}(a)} \}$, te $|\mathbb{F}(a) : \mathbb{F}|_s = 1$. Kako je $\mathbb{F}(a) \geq \mathbb{F}$ separabilna ekstenzija (25.2) to je $|\mathbb{F}(a) : \mathbb{F}| = |\mathbb{F}(a) : \mathbb{F}|_s = 1$, tj. $\mathbb{F}(a) = \mathbb{F}$ odavde $a \in F$. Prema tome $\mathbb{E}^G \subseteq \mathbb{F}$, što zajedno sa 1° daje $\mathbb{F} = \mathbb{E}^G$. ∎

Neka je $\mathbb{E} \geq \mathbb{F}$ galoava ekstenzija i
$\mathcal{M} = \{ \mathbb{L} \mid \mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{E} \}$ i $\mathcal{H} = \{ H \mid H < Aut(\mathbb{E}|\mathbb{F}) \}$.
Prema Teoremi 25.3 preslikavanje $\Phi : \mathcal{M} \longrightarrow \mathcal{H}$, $\Phi : \mathbb{L} \mapsto Aut(\mathbb{E}|\mathbb{L})$, $\mathbb{L} \in \mathcal{M}$, je dobro definisano.

25.5. **Teorema** $\Phi : \mathcal{M} \xrightarrow[1-1]{} \mathcal{G}$.

$$\begin{array}{ccc} & \mathbb{E} & \\ \subsetneq & & \supsetneq \\ \mathbb{L} & & \mathbb{L}' \\ \supsetneq & & \subsetneq \\ & \mathbb{F} & \end{array}$$

Dokaz Ako je $\mathbb{F} \subseteq \mathbb{L}, \mathbb{L}' \subseteq \mathbb{E}$, tada je $\mathbb{E}$ Galoavo proširenje polja $\mathbb{L}, \mathbb{L}'$. Odavde, ako $\Phi(\mathbb{L}) = \Phi(\mathbb{L}')$, tj. $Aut(\mathbb{E}|\mathbb{L}) = Aut(\mathbb{E}|\mathbb{L}') \equiv H$ prema T. 25.4. $\mathbb{L} = \mathbb{E}^H = \mathbb{L}'$. ∎

25.6. **Primer**. Ako je $\mathbb{E}$ konačna separabilna ekstenzija polja $\mathbb{F}$, tada postoji konačno mnogo međupolja $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{E}$, tj. $|\mathcal{M}| < \infty$.

Dokaz Najpre proširimo polje $\mathbb{E}$ do Galoave ekstenzije $\mathbb{E}' \supseteq \mathbb{F}$:
Kako je $\mathbb{E}$ konačna separabilna ekstenzija polja $\mathbb{F}$, prema Teoremi o primitivnom elementu, postoji $b \in E$ tako da je $\mathbb{E} = \mathbb{F}(b)$.
Neka je $p(x) \in F[x]$ minimalan polinom za a. Tada je $p(x)$ separabilan jer je a separabilan. Neka je $\mathbb{E}'$ korensko polje polinoma p, tj. $\mathbb{E}' = F(a_1, \dots, a_n)$ gde $p(x) = c(x-a_1)\cdots(x-a_n)$ (u $\mathbb{E}'$). Kako su $a_1, \dots, a_n$ koreni separabilnog polinoma $p(x)$, to je $\mathbb{E}' \supseteq \mathbb{F}$ separabilno proširenje. Dakle, $\mathbb{E}'|\mathbb{F}$ je galoavo. Prema Teoremi 25.5 Φ je 1-1, dakle $\mathcal{M}'$ je konačno (jer je $\mathcal{G}$ konačno), pa je i $\mathcal{M}$ konačno. ∎

25.7*. **Zadatak** (Obrat za 25.6) Ako je $\mathbb{E} \supseteq \mathbb{F}$ i $\mathcal{M}$ je konačno, tada je $\mathbb{E} \supseteq \mathbb{F}$ separabilna ekstenzija.

25.8. **Lema** Neka je $\mathbb{E} \supseteq \mathbb{F}$ separabilna ekstenzija (tj. $\mathbb{E} \supseteq \mathbb{F}$ je algebarsko i svaki $a \in F$ je separabilan nad $\mathbb{F}$). Dalje, neka je $n \in N^+$ i pretpostavimo $\bigwedge_{a \in E} |\mathbb{F}(a) : \mathbb{F}| \leq n$. Tada $|\mathbb{E} : \mathbb{F}| \leq n$.

Dokaz Neka je m najveći prirodan broj takav da je za neki $a \in E$ $|\mathbb{F}(a) : \mathbb{F}| = m$. Tada, naravno, $m \leq n$. Dokazujemo da je $\mathbb{E} = \mathbb{F}(a)$. Pretpostavimo suprotno, da postoji $b \in E \setminus F(a)$. Prema teoremi o primitivnom elementu postoji $c \in E$ tako da $F(a,b) = F(c)$ (jer je $\mathbb{F}(a,b) \supseteq \mathbb{F}$ separabilno). Tada $\mathbb{F} \subseteq \mathbb{F}(a) \subsetneq \mathbb{F}(c)$, pa $|\mathbb{F}(c) : \mathbb{F}| > m$, suprotno izboru broja m. ∎

25.9. **Teorema** (E. Artin) Neka je $\mathbb{E}$ algebarsko polje, $G < Aut\,\mathbb{E}$ konačnog reda n i neka je $\mathbb{F} = \mathbb{E}^G = \{x \in E \mid \bigwedge_{\sigma \in G} \sigma(x) = x\}$.
Tada je $\mathbb{E}|\mathbb{F}$ galoava ekstenzija, $|\mathbb{E} : \mathbb{F}| = n$ i $Aut(\mathbb{E}|\mathbb{F}) = G$.

25.10 **Posledica** Ako je $\mathbb{E}|\mathbb{F}$ galoavo, tada $\Phi : \mathcal{M} \xrightarrow{na} \mathcal{G}$.
Dokaz Neka je $H \in \mathcal{G}$, tj. $H < Aut(\mathbb{E}|\mathbb{F})$, i neka je $L = E^H$. Tada je prema 25.9 $\mathbb{E}|\mathbb{L}$ galoavo i $Aut(\mathbb{E}|\mathbb{L}) = H$, tj. $H = \Phi(\mathbb{L})$. ∎

Dokaz T. 25.9. Najpre dokazujemo

1° Svaki $a \in E$ je koren nekog separabilnog polinoma f stepena $\le n$, $f \in F[x]$.
Neka je $a \in E$ i $S = \{\sigma_1, \dots, \sigma_m\} \subseteq G$ maksimalan skup automorfizama takvih da su $\sigma_1 a, \dots, \sigma_m a$ različiti. Neka je $\tau \in G$. Tada

(*) $\{\tau\sigma_1 a, \dots, \tau\sigma_m a\} = \{\sigma_1 a, \dots, \sigma_m a\}$ jer:

a. $\tau \circ \sigma_i \in G$ b. τ je 1-1   c. S je maksimalan sa navedenim svojstvom.

Dakle, $\tau\sigma_1 a, \dots, \tau\sigma_m a$ je jedna permutacija niza $\sigma_1 a, \dots, \sigma_m a$.
Ako izaberemo $\tau = \sigma_1^{-1}$ (prema tome takođe $\tau \in G$), onda $a = \tau\sigma_1 a$ pa prema (*), $a \in \{\sigma_1 a, \dots, \sigma_m a\}$, te je a koren polinoma

(**) $$f(x) = (x - \sigma_1 a) \cdots (x - \sigma_m a).$$

Ako je $\sigma \in G$, onda prema prethodnom σ permutuje korene polinoma f, tj. $f(x)$ je invarijantan u odnosu na σ:

ako je $f(x) = x^m + f_{m-1}x^{m-1} + \dots + f_1 x + f_0$, onda $\sigma f_i = f_i$, $0 \le i < m$

⌈U to se možemo uveriti i ovako: prema Vijetovim pravilima, f_i su simetrične funkcije korena polin. $f(x)$, tj. $f_i = F(\sigma_1 a, \dots, \sigma_m a)$, gde $F(x_{p_1}, \dots, x_{p_m}) = F(x_1, \dots, x_m)$, $p \in S_m$ (skup permutacija skupa $\{1, \dots, m\}$) pa $\sigma f_i = F(\sigma\sigma_1 a, \dots, \sigma\sigma_m a) = F(\sigma_{p_1} a, \dots, \sigma_{p_m} a) = F(\sigma_1 a, \dots, \sigma_m a) = f_i$ ⌋

Dakle, prema definiciji polja $\mathbb{F}$, $f_0, \dots, f_{m-1} \in F$, tj. $f(x) \in F[x]$.
Dalje, $f(x)$ je separabilan jer su mu koreni $\sigma_1 a, \dots, \sigma_m a$ različiti i $\deg f = m \le n$ ($m \le n$ je $m = |S| \le |G| = n$), $f(a) = 0$, te je ovim 1° dokazano.
Prema Lemi 25.8 važi

2° $\mathbb{E}|\mathbb{F}$ je separabilna ekstenzija i $|\mathbb{E} : \mathbb{F}| \le n$. Takođe

3° $\mathbb{E}|\mathbb{F}$ je normalna jer je svaki $a \in E$ koren nekog polinoma (**) koji se razlaže na linearne faktore. Dakle

4° $\mathbb{E}|\mathbb{F}$ je Galoaova ekstenzija.
Najzad, $n = |G|$, $G \subseteq \mathrm{Aut}(\mathbb{E}|\mathbb{F})$, $n \le |\mathrm{Aut}(\mathbb{E}|\mathbb{F})| \underset{\text{zbog normalnosti}}{=} |\mathbb{E} : \mathbb{F}|_s \le |\mathbb{E} : \mathbb{F}| \le n$
pa $\mathrm{Aut}(\mathbb{E}|\mathbb{F}) = G$. ∎

25.11. Neka je $f \in \mathbb{F}[x]$ separabilan i neka je $\mathbb{E} = \mathbb{F}(a_1, \dots, a_n)$ korensko polje polinoma $f(x) = c \cdot (x - a_1) \cdots (x - a_n)$. Tada je $\mathbb{E}|\mathbb{F}$ Galoaova ekstenzija.

Ako je $S = \{a_1, \dots, a_n\}$ i $G = \mathrm{Aut}(\mathbb{E}|\mathbb{F})$, tada se G naziva <u>Galoaovom grupom polinoma f</u>. Ako je $\sigma \in G$, tada σ permutuje korene polin. f i za $\sigma, \tau \in G$, $(\sigma \circ \tau)|S = \sigma|S \circ \tau|S$, dakle $\Psi : \sigma \longmapsto \sigma|S$ je utapanje grupe G u $\mathrm{Sym}(S)$ (grupa permutacija skupa S), tj. G je izomorfna podgrupi grupe S_n. Primetimo da $\sigma|S = \tau|S \Rightarrow \sigma = \tau$, tj. Ψ je 1-1.

26. Svojstva izomorfnih međupolja galoaovih ekstenzija

Neka je $\mathbb{E}|\mathbb{F}$ galoaova ekstenzija i neka je $\mathbb{E}'|\mathbb{F}'$ galoaova ekstenzija. Dalje, neka je $\lambda : \mathbb{E} \cong \mathbb{E}'$ tako da je $\lambda|\mathbb{F} : \mathbb{F} \cong \mathbb{F}'$, tj. $\lambda \mathbb{F} = \mathbb{F}'$.

$$\begin{tikzcd} \mathbb{E} \arrow[r, "\lambda", "\approx"'] & \mathbb{E}' \\ \mathbb{F} \arrow[u, phantom, "\subseteq" sloped] \arrow[r, "\lambda|\mathbb{F}", "\approx"'] & \mathbb{F}' \arrow[u, phantom, "\subseteq" sloped] \end{tikzcd}$$

(D1)

$$\begin{tikzcd} \mathbb{E} \arrow[rr, "\sigma"] & & \mathbb{E} & & \mathbb{E}' \arrow[rr, "\sigma'"] & & \mathbb{E}' \\ & \mathbb{F} \arrow[ul, phantom, "\subseteq" sloped] \arrow[ur, phantom, "\subseteq" sloped] & & \rightsquigarrow & & \mathbb{F}' \arrow[ul, phantom, "\subseteq" sloped] \arrow[ur, phantom, "\subseteq" sloped] & \end{tikzcd}$$

(D2)

Pretpostavke o ekstenzijama $\mathbb{E}|\mathbb{F}$ i $\mathbb{E}'|\mathbb{F}$ predstavljene su dijagramom (D1). Možemo postaviti prirodno pitanje o korespodenciji između $\mathrm{Aut}(\mathbb{E}|\mathbb{F})$ i $\mathrm{Aut}(\mathbb{E}'|\mathbb{F}') = \mathrm{Aut}(\lambda\mathbb{E}|\lambda\mathbb{F})$, vidi dijagram (D2).

Neka je $\sigma \in \mathrm{Aut}(\mathbb{E}|\mathbb{F})$ i $\sigma' = \lambda \circ \sigma \circ \lambda^{-1}$.

Neposredno se proverava da dijagram (D3) komutira, i da je $\sigma' \in \mathrm{Aut}(\mathbb{E}'|\mathbb{F}')$.

$$\begin{tikzcd} \mathbb{E}' \arrow[rr, "\sigma'"] \arrow[dd, "\lambda^{-1}"', "\cong"] & & \mathbb{E}' \\ & \mathbb{F}' \arrow[ul, phantom, "\supseteq" sloped] \arrow[ur, phantom, "\subseteq" sloped] & \\ & \mathbb{F} \arrow[u, "\lambda|\mathbb{F}"'] \arrow[dl, phantom, "\subseteq" sloped] \arrow[dr, phantom, "\supseteq" sloped] & \\ \mathbb{E} \arrow[rr, "\sigma"] & & \mathbb{E} \arrow[uuu, "\lambda"', "\cong"] \end{tikzcd}$$

(D3).

Otuda, preslikavanje

$$h : \sigma \longmapsto \lambda \circ \sigma \circ \lambda^{-1}, \quad \sigma \in \mathrm{Aut}(\mathbb{E}|\mathbb{F})$$

preslikava $\mathrm{Aut}(\mathbb{E}|\mathbb{F})$ u $\mathrm{Aut}(\mathbb{E}'|\mathbb{F}')$.

Uz prethodno uvedene oznake važi sledeće tvrđenje:

26.1. Lema $h : \mathrm{Aut}(\mathbb{E}|\mathbb{F}) \cong \mathrm{Aut}(\mathbb{E}'|\mathbb{F}')$.

Dokaz 1° h je homomorfizam: $h(\sigma \circ \tau) = \lambda \circ (\sigma \circ \tau) \circ \lambda^{-1} = (\lambda \circ \sigma \circ \lambda^{-1}) \circ (\lambda \circ \tau \circ \lambda^{-1}) = h(\sigma) \circ h(\tau)$.

2° h je 1-1: Pretpostavimo $h(\sigma) = h(\tau)$. Tada $\lambda \circ \sigma \circ \lambda^{-1} = \lambda \circ \tau \circ \lambda^{-1}$, odakle $\lambda^{-1} \circ \lambda \circ \sigma \circ \lambda^{-1} \circ \lambda = \lambda^{-1} \circ \lambda \circ \tau \circ \lambda^{-1} \circ \lambda$, tj. $\sigma = \tau$.

3° h je na: Neka je $\sigma' \in \mathrm{Aut}(\mathbb{E}'|\mathbb{F}')$ i $\sigma = \lambda^{-1} \circ \sigma' \circ \lambda$. Tada $\sigma \in \mathrm{Aut}(\mathbb{E}|\mathbb{F})$ i $h(\sigma) = \sigma'$. ▨

Prethodno tvrđenje možemo zapisati i na sledeći način:

26.2. Teorema Neka je $\lambda : \mathbb{E} \cong \mathbb{E}'$ i $\mathbb{F} \subseteq \mathbb{E}$. Tada

$$\mathrm{Aut}(\lambda\mathbb{E}|\lambda\mathbb{F}) = \lambda \circ \mathrm{Aut}(\mathbb{E}|\mathbb{F}) \circ \lambda^{-1}.$$

Primetimo da prethodno tvrđenje važi zapravo za bilo koju ekstenziju $\mathbb{E}|\mathbb{F}$. Pretpostavimo sada da je $\mathbb{E}|\mathbb{F}$ galoaova ekstenzija. S obzirom da je $\mathbb{E}|\mathbb{F}$ algebarsko raširenje, možemo pretpostaviti da je $\mathbb{E} \subseteq \overline{\mathbb{F}}$. Dalje, neka je $\mathbb{L}$ međupolje polja $\mathbb{F} \subseteq \mathbb{E}$, tj. $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{E}$.

$$\begin{tikzcd} \mathbb{E} \arrow[r, dashed, "\bar{\lambda}"] & \mathbb{E} \\ \mathbb{L} \arrow[u, phantom, "\subseteq" sloped] \arrow[r, "\lambda", "\approx"'] & \mathbb{L}' \arrow[u, phantom, "\subseteq" sloped] \\ & \mathbb{F} \arrow[ul, phantom, "\subseteq" sloped] \arrow[u, phantom, "\subseteq" sloped] \end{tikzcd}$$

(D4)

Dalje, neka je $\lambda : \mathbb{L} \longrightarrow \mathbb{E}$, $\lambda|\mathbb{F} = i_{\mathbb{F}}$. Prema Posledici 21.2.

postoji $\bar\lambda \in Hom(\mathbb{E}, \bar{\mathbb{F}})$ tako da dijagram (D4) komutira, tj. $\lambda \leq \bar\lambda$. S obzirom da je raširenje $\mathbb{E}|\mathbb{F}$ galoaovo, ono je normalno, dakle $\bar\lambda \in Aut(\mathbb{E}|\mathbb{F})$, te je prema Teoremi 26.2, $Aut(\mathbb{E}|\lambda\mathbb{L}) = \bar\lambda \circ Aut(\mathbb{E}|\mathbb{L}) \circ \bar\lambda^{-1}$ 6vim smo dokazali

26.3. Teorema Neka je $\mathbb{E}|\mathbb{F}$ galoava ekstenzija, $\mathbb{F} \leq \mathbb{L} \leq \mathbb{E} \leq \bar{\mathbb{F}}$ i $\lambda \in Hom(\mathbb{L}, \mathbb{E})$. Tada su podgrupe $Aut(\mathbb{E}/\lambda\mathbb{L})$ i $Aut(\mathbb{E}|\mathbb{L})$ galoaove grupe $Aut(\mathbb{E}|\mathbb{F})$ konjugovane, preciznije, postoji $\bar\lambda \in Aut(\mathbb{E}|\mathbb{F})$ tako da je $\lambda \leq \bar\lambda$ i

$$Aut(\mathbb{E}|\lambda\mathbb{L}) = \bar\lambda \circ Aut(\mathbb{E}|\mathbb{L}) \circ \bar\lambda^{-1}. \qquad \blacksquare$$

sledeće tvrđenje je poslednji deo teoreme o korespodenciji između međupolja galoaove ekstenzije $\mathbb{E}|\mathbb{F}$ i podgrupa galoaove grupe $Aut(\mathbb{E}|\mathbb{F})$.

26.4. Teorema Neka je $E|\mathbb{F}$ galoaova ekstenzija, $Aut(\mathbb{E}|\mathbb{F}) = \mathbb{G}$, $\mathbb{F} \leq \mathbb{L} \leq \mathbb{E}$, $H = Aut(\mathbb{E}|\mathbb{L})$. Tada

1° $\mathbb{L}|\mathbb{F}$ je normalno raširenje akko $H \triangleleft \mathbb{G}$.

2° Ako je $\mathbb{L}|\mathbb{F}$ normalna ekstenzija, tada je $h : \sigma \mapsto \sigma|L$, $\sigma \in \mathbb{G}$, $h : \mathbb{G} \to Aut(\mathbb{L}|\mathbb{F})$ i $\ker h = H$.

3° Pod uslovima u 2°, $Aut(\mathbb{L}|\mathbb{F}) \cong \mathbb{G}/H$.

Dokaz Neka je $\mathbb{G}' = Aut(\mathbb{L}|\mathbb{F})$. S obzirom da je $\mathbb{E}|\mathbb{F}$ galoaovo, to je $\mathbb{E}|\mathbb{F}$ separabilno, dakle $\mathbb{L}|\mathbb{F}$ je separabilna ekstenzija (T. 25.2). Dakle, $\mathbb{L}|\mathbb{F}$ je galoaova ekstenzija akko je $\mathbb{L}|\mathbb{F}$ normalno raširenje. i neka je $\bar\lambda \in Aut(E|\mathbb{F}) (= \mathbb{G})$,

1° ($\Rightarrow$) Neka je $\mathbb{L}|\mathbb{F}$ normalno raširenje. Tada $\lambda : \mathbb{L} \to \mathbb{E} \leq \bar{\mathbb{F}}$, te proizvoljno. Dalje, neka je $\lambda = \bar\lambda|L$. Tada $\lambda : \mathbb{L} \to \mathbb{L}$, tj. $\lambda\mathbb{L} = \mathbb{L}$. Otuda, prema zbog normalnosti ekstenzije $\mathbb{L}|\mathbb{F}$, $\lambda : \mathbb{L} \to \mathbb{L}$, tj. $\lambda \mathbb{L} = \mathbb{L}$. Otuda, prema T. 26.2 odnosno T. 26.3 važi $Aut(\mathbb{E}|\mathbb{L}) = Aut(\mathbb{E}|\lambda\mathbb{L}) = \bar\lambda \circ Aut(\mathbb{E}|\mathbb{L}) \circ \bar\lambda^{-1}$,

tj. $\bigwedge_{\sigma \in G} \sigma H \sigma^{-1} = H$, dakle $H \triangleleft \mathbb{G}$.

($\Leftarrow$) Dokazujemo kontrapoziciju (tj. $\neg q \Rightarrow \neg p$ umesto $p \Rightarrow q$). Pretpostavimo da $\mathbb{L}|\mathbb{F}$ nije normalno. Tada prema definiciji normalnosti, postoji $\lambda \in Hom(\mathbb{L}|\mathbb{F}, \mathbb{E})$ tako da $\lambda \notin Aut(\mathbb{L}|\mathbb{F})$, tj. $\lambda\mathbb{L} \neq \mathbb{L}$, $\lambda|\mathbb{F} = i_{\mathbb{F}}$. Tada se λ produžuje do $\bar\lambda : \mathbb{E} \to \bar{\mathbb{F}}$, te uz pretpostavku $\mathbb{E} \leq \bar{\mathbb{F}}$, dakle $\bar\lambda \in Aut(\mathbb{E}|\mathbb{F})$, s obzirom da je $\mathbb{E}|\mathbb{F}$ normalno. Otuda prema T26.3 $Aut(\mathbb{E}|\lambda\mathbb{L}) = \bar\lambda\, Aut(\mathbb{E}|\mathbb{L})\, \bar\lambda^{-1}$. S druge strane $Aut(\mathbb{E}/\lambda\mathbb{L}) \neq Aut(\mathbb{E}/\mathbb{L})$ jer u suprotnom (T. 25.5) $\lambda\mathbb{L} = \mathbb{L}$, kontradikcija. Dakle $H \neq \bar\lambda H \bar\lambda^{-1}$,

tj. $H \ntriangleleft \mathbb{G}$.

2° a. $h : G \to G'$: Ako $\sigma \in G$, tada $\sigma|L : \mathbb{L} \to \mathbb{E} \leq \overline{\mathbb{F}}$, dakle $\sigma|L \in Hom(\mathbb{L}|\mathbb{F}, \overline{\mathbb{F}})$, te kako je $\mathbb{L}|\mathbb{F}$ normalno, to $\sigma|L \in Aut(\mathbb{L}|\mathbb{F})$. Primetimo da je $(\sigma|_L)|_F = i_F$ jer $\sigma \in Aut(\mathbb{E}|\mathbb{F})$, dakle $\sigma|_F = i_F$ i $\sigma|_L \leq \sigma$. Vidi dijagram (D5).

$$\begin{tikzcd} \mathbb{E} \arrow[r, "\sigma"] & \mathbb{E} \\ \mathbb{L} \arrow[u, phantom, "\cup" rotate=90] \arrow[r, "\sigma|_L"] & \mathbb{L} \arrow[u, phantom, "\cup" rotate=90] \\ & \mathbb{F} \arrow[ul, phantom, "\subseteq"] \arrow[u, phantom, "\subseteq"] \end{tikzcd} \qquad (D5)$$

$$\begin{tikzcd} G \arrow[r, "h", "na"'] \arrow[d, "h"] & G' \\ G/H = G/\ker h \arrow[ur, dashed, "\approx"'] & \end{tikzcd} \qquad (D6)$$

b. h je homomorfizam: Za $\sigma_1, \sigma_2 \in G$,

$$h(\sigma_1 \circ \sigma_2) = (\sigma_1 \circ \sigma_2)|_L = \sigma_1|_L \circ \sigma_2|_L = h(\sigma_1) \circ h(\sigma_2).$$

c. $\ker h = \{\sigma \in G : h\sigma = i_L\} = \{\sigma \in G : \sigma|_L = i_L\} = Aut(\mathbb{E}|L) = H.$

3° Pretpostavimo uslove i oznake kao u 2°. Tada $h : G \to G'$.
Dokazujemo da je h epimorfizam (homomorfizam na).
Neka je $\tau \in G'$, gde $G' = Aut(\mathbb{L}|\mathbb{F})$.
Tada postoji $\sigma \supseteq \tau$, $\sigma \in Hom(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})$,
pa zbog normalnosti ekstenzije $\mathbb{E}|\mathbb{F}$,
$\sigma \in Aut(\mathbb{E}|\mathbb{F})$ i pri tome, naravno, $h\sigma = \sigma|_L = \tau$.

$$\begin{tikzcd} \mathbb{E} \arrow[r, dashed, "\sigma"] & \mathbb{E} \\ \mathbb{L} \arrow[u, phantom, "\cup" rotate=90] \arrow[r, "\tau"] & \mathbb{L} \arrow[u, phantom, "\cup" rotate=90] \\ & \mathbb{F} \arrow[ul, phantom, "\subseteq"] \arrow[u, phantom, "\subseteq"] \end{tikzcd}$$

Dakle $h : G \xrightarrow{na} G'$. Prema Teoremi o razlaganju homomorfizma, onda $G' \cong G/\ker H$ (vidi dijagram D6). ∎

Ovim je dokazana glavna teorema teorije galoa, teorema korespodencije.

27. Napomene.

27.1. Osnovni zadatak teorije Galoa. Neka je $f(x)$ separabilan polinom nad poljem $\mathbb{F}$. Tada je korensko polje $\mathbb{E}$ polinoma f galoava ekstenzija polja $\mathbb{F}$. Osnovni zadatak teorije galoa je da se odredi galoava grupa $G = Aut(\mathbb{E}|\mathbb{F})$. Primetimo da je G izomorfna podgrupi grupe S_n, gde je $n = \deg f$. Ponegde se u ovom slučaju $Aut(\mathbb{E}|\mathbb{F})$ obeležava sa $Aut(f|\mathbb{F})$.

27.2 Inverzni zadatak teorije galoa. U ovom zadatku pitanje je koje su konačne grupe galoave nad $\mathbb{Q}$, tj. ako je G konačna grupa da li je $G \cong Aut(\mathbb{E}|\mathbb{Q})$ za neku galoavu ekstenziju $\mathbb{E}|\mathbb{Q}$. Poznato je da su konačne ciklične grupe i konačne Abelove grupe galoave nad $\mathbb{Q}$. U tom pogledu ističe se sledeće tvrđenje:

Teorema (Šafarevič) Svaka konačna rešiva grupa je galoava nad $\mathbb{Q}$.

Otvoren problem Da li je svaka konačna grupa galoava grupa nad $\mathbb{Q}$?

Zadatak Podsetimo se da je konačna grupa G nilpotentna ako je ona unutrašnji proizvod svojih Silovskih podgrupa, tj. G je izomorfna konačnom proizvodu konačnih p-grupa, $p \in Prost$. H je p-grupa ako je $|H| = p^n$, $n \in \mathbb{N}$. Dokazati da je nilpotentna grupa rešiva.

27.3 Infinitarna teorija Galoa. Neka je $\mathbb{E}|\mathbb{F}$ algebarsko, normalno i separabilno raširenje. Ako je $|\mathbb{E}:\mathbb{F}| < \infty$ tada je $\mathbb{E}$ Galoaova raširenje polja $\mathbb{F}$. Ako je $|\mathbb{E}:\mathbb{F}| = \infty$ tada kažemo da je $\mathbb{E}|\mathbb{F}$ infinitarna Galoaova ekstenzija. Ova teorija složenija je od klasične teorije Galoa i za nju važi samo deo tvrđenja iz klasične (konačne) teorije Galoa. Na primer važi Teorema 25.5, tj. $\Phi : \mathcal{M} \xrightarrow[1-1]{} \mathcal{G}$, ali Φ ne mora biti na.

U slučaju beskonačnog Galoaovog raširenja $\mathbb{E}|\mathbb{F}$ na Galoaovoj grupi $G = \mathrm{Aut}(\mathbb{E}|\mathbb{F})$ uvodi se Krulova (W. Krull) topologija, uzimajući za okolinu jedinice (u G) mnoštvo podgrupa koje odgovaraju konačnim raširenjima $\mathbb{L} \supseteq \mathbb{F}$, $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{E}$. Pokazuje se da su zatvorene podgrupe grupe G tačno Galoave grupe međupolja $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{E}$, tj.

$\mathrm{Im}\,\Phi = \{ H < G \mid H$ je zatvorena u Krulovoj topologiji$\}$.

27.4. Galoaovo preslikavanje Neka je $G < \mathrm{Aut}\,\mathbb{E}$ konačna grupa automorfizama polja $\mathbb{E}$, i neka je $\mathbb{F} \subseteq \mathbb{E}$ nepokretno polje u odnosu na G, tj.

$\mathbb{F} = \{a \in \mathbb{E} \mid \bigwedge_{\sigma \in G} \sigma a = a\}$. Tada je prema Artinovoj teoremi (T. 25.9) $\mathbb{E}|\mathbb{F}$ galoaova ekstenzija i $G = \mathrm{Aut}(\mathbb{E}|\mathbb{F})$. Neka su $X \subseteq \mathbb{E}$ i $Y \subseteq G$ i

$X^* \overset{def}{=} \{\sigma \in G \mid \bigwedge_{a \in X} \sigma a = a\}$, $Y^* = \{a \in \mathbb{E} \mid \bigwedge_{\sigma \in Y} \sigma a = a\}$.

Dakle, uvedena su dva preslikavanja sa istom oznakom $*$:

$* : \mathbb{P}(\mathbb{E}) \longrightarrow \mathbb{P}(G)$, $* : \mathbb{P}(G) \longrightarrow \mathbb{P}(\mathbb{E})$ ($\mathbb{P}(A)$ = partitivni skup skupa A).

a. Neposredno se proverava da je $X^* < G$, dok je Y^* međupolje, tj. Y^* je polje i $\mathbb{F} \subseteq Y^* \subseteq \mathbb{E}$.

b. Neka je $H < G$. Tada je prema Artinovoj teoremi (25.9) H^* nepokretno polje u odnosu na H, $\mathbb{E}|H^*$ je Galoaova ekstenzija i $H = \mathrm{Aut}(\mathbb{E}|H^*)$.
S druge strane, prema definiciji preslikavanja $*$, $H^{**} = \mathrm{Aut}(\mathbb{E}|H^*)$, tj. $H^{**} = H$.
Otuda i prema Teoremi 25.4 odmah nalazimo

c. $X^{***} = X^*$, $Y^{***} = Y^*$.

Postoji uopštenje koje se takođe naziva Galoaovo preslikavanje:
Neka su A i B skupovi i R binarna relacija iz A u B, tj. $R \subseteq A \times B$.
Za $X \subseteq A$ i $Y \subseteq B$ definiše se:

$X^* = \{ y \in B \mid \bigwedge_{x \in X} (x,y) \in R\}$, $Y^* = \{ x \in A \mid \bigwedge_{y \in Y} (x,y) \in R\}$.

Ovim je definisan par preslikavanja

$$X \mapsto X^*,\ X \in \mathbb{P}(A);\quad Y \mapsto Y^*,\ Y \in \mathbb{P}(B).$$

Galoavo preslikavanje u slučaju polja dobija se uzimajući $R = \{(a, \sigma) \in E \times G \mid \sigma a = a\}$. Dakle, $R \subseteq E \times G$.
U slučaju opšteg Galoavog preslikavanja za $X \subseteq A$ i $Y \subseteq B$ takođe važi:

$$X^{***} = X^*,\quad Y^{***} = Y^*.$$

Postoje mnoge zanimljive osobine uopštenog Galoovog preslikavanja (vidi P. M. Cohn, "Universal Algebra").

Primene teorije Galua

28. Kvadratna jednačina $x^2 + bx + c = 0$.
Razmotrimo ovu jednačinu nad poljem $\mathbb{F}$. Neka je $f(x) = x^2 + bx + c$, $b, c \in F$.

28.1. Neka je $kF \geq 3$. Kako je $x^2 + bx + c = (x + \frac{b}{2})^2 - \frac{b^2 - 4c}{4}$, uz smenu $y = x + \frac{b}{2}$ i $a = \frac{b^2-4c}{4}$, dobijamo jednačinu $y^2 - a = 0$.

28.1a Lema Neka je $g(x) \in F[x]$ i $c \in F$. Tada polinomi $g(x)$ i $g(x+c)$ imaju ista korenska polja. Ako je $g(x)$ separabilan, tada je i $g(x+c)$ separabilan i Galoave grupe polinoma $g(x)$ i $g(x+c)$ su jednake.

Dokaz Neka je $\mathbb{F}(a_1, \dots, a_n)$ korensko polje polinoma $g(x)$. Tada je $F(a_1+c, \dots, a_n+c)$ korensko polje polinoma $g(x+c)$. S obzirom da $a_1+c, \dots, a_n+c \in F(a_1, \dots, a_n)$, to $F(a_1+c, \dots, a_n+c) \subseteq F(a_1, \dots, a_n)$. Slično $F(a_1, \dots, a_n) \subseteq F(a_1+c, \dots, a_n+c)$, pa $F(a_1+c, \dots, a_n+c) = F(a_1, \dots, a_n)$.
Što se tiče drugog dela tvrđenja, s obzirom da $g(x)$ i $g(x+c)$ imaju ista korenska polja, to imaju i iste Galoaove grupe. ∎

Prema prethodnom umesto opšte kvadratne jednačine, dovoljno je razmatrati jednačinu $x^2 - a = 0$.

Ako jednačina $x^2 - a = 0$ nema korena u $\mathbb{F}$, tada je polinom $f(x) = x^2 - a$ nesvodljiv nad $\mathbb{F}$, $f'(x) = 2x$, i u tom slučaju $(f, f') = 1$ te je separabilan.
Dakle, ako je $\mathbb{F}(d)$ korensko polje tog polinoma, tada je $\mathbb{F}(d)/\mathbb{F}$ Galoaova ekstenzija $|\mathbb{F}(d) : \mathbb{F}| = 2$, i Galoaova grupa $\mathcal{G}$ ove jednačine je reda 2, pa $\mathcal{G} = C_2$. $\mathcal{G} = \{i, \sigma\}$, gde $\sigma(d) = -d$. $\mathbb{F}(d) = \{x + yd \mid x, y \in F\}$,
$\sigma : x + yd \mapsto x - yd$, $x, y \in F$.

Razmotrimo ovu jednačinu nad konačnim poljima $\mathbb{Z}_p$, $p \geq 3$.

28.1b **Teorema** (Ojler) $\mathbb{Z}_p \models \exists x (x^2 = a)$ akko $a^{\frac{p-1}{2}} = 1 \bmod p$, $a \in \mathbb{Z}_p \setminus \{0\}$.

Dokaz Koristićemo činjenicu da je $\mathbb{Z}_p^* = (\mathbb{Z}_p \setminus \{0\}, \cdot, 1)$ ciklična grupa, dakle $\mathbb{Z}_p^* = \mathbb{C}_{p-1} = \langle b \rangle$, $b^i \neq 1$ za $1 \le i < p-1$, $b^{p-1} = 1$.

($\Rightarrow$) Neka je $d \in \mathbb{Z}_p$ rešenje jednačine $x^2 = a$ u $\mathbb{Z}_p$, dakle $d^2 = a$. Neka je $d = b^i$. Tada u $\mathbb{Z}_p$ $a = b^{2i}$, pa $a^{\frac{p-1}{2}} = b^{2i\frac{p-1}{2}} = b^{(p-1)i} = 1$, odakle $a^{\frac{p-1}{2}} = 1 \pmod p$.

($\Leftarrow$) Računamo u $\mathbb{Z}_p$. Pretpostavimo $a^{\frac{p-1}{2}} = 1$. Za neko i, $a = b^i$, te $1 = a^{\frac{p-1}{2}} = b^{\frac{i(p-1)}{2}}$, odakle $\frac{i(p-1)}{2} = 0 \pmod{(p-1)}$, tj. $p-1 \mid i\frac{p-1}{2}$, pa $\frac{i}{2} \in N$, odakle je $i = 2k$, tj. $a = b^{2k}$, te su rešenja ove jednačine u $\mathbb{Z}_p$ b^k i $-b^k$.

28.1.c. **Posledica** Neka je $a \in \mathbb{Z}$, $(a,p) = 1$. Tada kongruencijska jednačina $x^2 = a \pmod p$ ima rešenje akko $a^{\frac{p-1}{2}} = 1 \pmod p$.

28.1d. U vezi sa ovom jednačinom nad konačnim poljima je Ležandrov (Legendre) simbol: ako $(a,p) = 1$, $\left(\frac{a}{p}\right) \overset{def}{=} a^{\frac{p-1}{2}}$ (stepenovanje u $\mathbb{Z}_p$).
S obzirom da je u $\mathbb{Z}_p$ $a^{p-1} = 1$, to je $\left(\frac{a}{p}\right) \in \{1,-1\}$, preciznije

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ako } x^2 = a \text{ ima rešenje u } \mathbb{Z}_p \\ -1, & \text{inače} \end{cases}.$$

Odmah dobijamo sledeće multiplikativno svojstvo Ležandrovog simbola: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, $(a,p)=1$, $(b,p)=1$.
U vezi sa ovom funkcijom čuven je Gausov zakon reciprociteta:
Ako su p, q različiti neparni prosti brojevi, tada $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)(q-1)}$.

28.1e. **Zadatak** $\left(-\frac{1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$, $p \in Prost$, $p \ge 3$. Dakle, x^2+1 ima rešenje u $\mathbb{Z}_p$ ($p \ge 3$) akko $p = 1 \pmod 4$.

28.2. **$\mathrm{k}F = 2$** Tada se jednačina $x^2 + bx + c$ ne može smenom $x = y + c$ svesti na jednačinu $y^2 - a$. Ako je $b \neq 0$, tada $f'(x) = b$, $b \neq 0$, $(f, f') = 1$, pa je $f(x)$ separabilan, te je kao i u slučaju $\mathrm{k}F \ge 3$, Galoaova grupa ove jednačine $\mathbb{C}_2$. Primetimo, da ako je α koren ove jednačine da je tada i $\alpha + b$ koren iste jednačine. Razmotrimo u ovim poljima jednačinu $x^2 - a = 0$. Preslikavanje $h(x) = x^2$, $h: F \to F$ je homomorfizam (Frobeniusov homomorfizam), dakle h je utapanje. Ako je F algebarsko nad $\mathbb{Z}_2$, tada je prema Teoremi 24.10, $h \in Aut\,\mathbb{F}$, pa jednačina $x^2 - a = 0$ u tom slučaju ima rešenje u $\mathbb{F}$ za sve $a \in F$. Ako je $F \subseteq E$, $a \in E$ i a je transcedentan nad $\mathbb{F}$, tada $x^2 = a$ nema rešenje u $\mathbb{F}(a)$ ($\cong \mathbb{F}(X)$): uzmimo da je a = promenljiva X i pp da za neki $p(X)/q(X) \in F(X)$ važi $(p/q)^2 = X$. Možemo pp da je $(p,q) = 1$. Kako je polinom X nesvodljiv, to $X \mid p(x)$, pa $p = Xp_1$, tj: $p_1^2 X = q$, odakle $X \mid q$, # prema $(p,q) = 1$.

29. Galoaova grupa polinoma $f(x)=x^n-1$.

U ovom odeljku razmotrićemo polinom $f(x)=x^n-1$ i Galoaovu grupu ovog polinoma nad poljem racionalnih brojeva $\mathbb{Q}$. Nekoliko sledećih tvrđenja biće nam od koristi u toj raspravi.

29.1 Definicija Polinom $f(x)\in \mathbb{Z}[x]$, $f(x)=\sum_i f_i x^i$ je primitivan ukoliko je najveći zajednički delilac koeficijenata f_i polinoma f jednak 1, tj. $(f_0, f_1, \dots, f_n)=1$.

Na primer, $f(x)=4x^2-6x+9$ je primitivan. Primetimo da je svaki moničan $f\in \mathbb{Z}[x]$, tj. kod kojeg je $f_n=1$, primitivan.

29.2. Lema Proizvod dva primitivna polinoma $f, g\in \mathbb{Z}[x]$ je primitivan.

Dokaz Neka je $h=f\cdot g$ i pretpostavimo da h nije primitivan. Tada postoji $p\in$ Prost tako da $p\mid h_0, \dots, p\mid h_n$, $n=\deg h$. Kako je f po pretpostavci primitivan, to postoji prvi u nizu koeficijenata $f_0, f_1, \dots, f_r$, $r=\deg f$, koji nije deljiv sa p. Neka je to f_i. Slično, neka je h_j prvi u nizu koeficijenata polin. h koji nije deljiv sa p. Neka je $k=i+j$ i h_k koeficijent polin. h uz x^{i+j}, tj.

$$h_k = \underbrace{f_0 g_k + f_1 g_{k-1} + \dots + f_{i-1} g_{j+1}}_{\text{deljivo sa } p} + f_i g_j + \underbrace{f_{i+1} g_{j-1} + \dots + f_{k-1} g_1 + f_k g_0}_{\text{deljivo sa } p}$$

$p\mid h_k$ i p deli označene zbirove u h_k, dakle $p\mid f_i g_j$ pa $p\mid f_i$ ili $p\mid g_j$, #.
Dakle, $h(x)$ je primitivan. ∎

29.3. Lema Neka je $f\in \mathbb{Q}[x]$, $\deg f>0$. Tada postoji jedinstveni $c\in \mathbb{Q}^+$ i primitivan $g\in \mathbb{Z}[x]$ tako da je $f(x)=c\cdot g(x)$. Otuda pišemo i $f(x)=c_f\cdot \tilde{f}$.

Dokaz 1° Egzistencija $f(x)=\frac{1}{b}h(x)$ gde je b zajednički imenilac koeficijenata polinoma f i $h(x)\in \mathbb{Z}[x]$. Tada $f(x)=\frac{a}{b}g(x)$, gde je a najveći zajednički delilac koeficijenata polinoma $h(x)$, pa $c=\frac{a}{b}$.

2° Jedinost Pretpostavimo da je $f(x)=\frac{a}{b}g(x)$, $f(x)=\frac{a'}{b'}g'(x)$, $\frac{a}{b}, \frac{a'}{b'}\in \mathbb{Q}^+$ i $g, g'\in \mathbb{Z}[x]$ su primitivni. Tada $ab'g(x)=a'bg'(x)\equiv h(x)$. Tada $h(x)\in \mathbb{Z}[x]$ i $ab'=(h_0, h_1, \dots, h_n)=a'b$, tj. $ab'=a'b$ i $g=g'$. ∎

29.4 Gausova lema. Neka je $f\in \mathbb{Z}[x]$, $\deg f>0$. Tada je f rastavljiv nad $\mathbb{Q}$ akko je f rastavljiv nad $\mathbb{Z}$.

Dokaz ($\Rightarrow$) Pretpostavimo da je f rastavljiv nad $\mathbb{Q}$, tj. $f(x)=g(x)\cdot h(x)$, $g, h\in \mathbb{Q}[x]$. Tada $f=c_g c_h \tilde{g}\cdot\tilde{h}$, $\tilde{g}$ i $\tilde{h}$ su primitivni. S druge strane $f=c_f\cdot\tilde{f}$, $\tilde{f}$ je primitivan, te zbog jedinstvenosti rastavljanja (L. 29.3) $c_g\cdot c_h=c_f$, tj. $c_g c_h\in \mathbb{Z}$ (jer f ima celobrojne koeficijente i $c_f=(f_0, \dots, f_n)$). Tada je $f=(c_f\tilde{g})\tilde{h}$ jedno rastavljanje polinoma f nad $\mathbb{Z}$.

($\Leftarrow$) Trivijalno.

Podsetimo se da je $f \in F[x]$ moničan ako je $f_n = 1$, $\deg f = n$.

29.5 Lema Neka je $f \in \mathbb{Z}[x]$ moničan i neka je $f = gh$ jedno rastavljanje polinoma f nad $\mathbb{Q}$, gde su g i h monični. Tada $g, h \in \mathbb{Z}[x]$.

Dokaz Neka je $g = c_g \tilde{g} \equiv \frac{a}{b} \tilde{g}$, $h = c_h \tilde{h} \equiv \frac{a'}{b'} \tilde{h}$ gde su $\tilde{g}$ i $\tilde{h}$ primitivni polinomi. Možemo pretpostaviti da su $a, b, a', b' \in N^+$ i $(a,b) = 1$, $(a', b') = 1$. Tada $f = c_g c_h \tilde{g}\tilde{h}$, te kako je $\tilde{g}\tilde{h}$ primitivan, prema Lemi 29.3, $c_g c_h = c_f \equiv 1$, tj. $ab' = a'b$. Kako je $g_m = 1$, $\deg g = m$, to $\frac{a}{b}\tilde{g}_m = 1$, tj. $a\tilde{g}_m = b$. Dakle $a | b$, ali $(a,b) = 1$ pa $a = 1$ i slično $a' = 1$. Otuda $\frac{1}{bb'} = 1$. Kako $b, b' \in N^+$, to $b = b' = 1$. ☒

29.6. Zadatak Neka su $a, b, c, d \in \mathbb{Z}$. Dokazati da su sva racionalna rešenja sistema (S) (operacije u polju $\mathbb{Q}$) cela.

$$\left.\begin{aligned} x+y &= a \\ zu &= b \\ xu + yz &= c \\ xy + z + u &= d \end{aligned}\right\} (S)$$

29.7. Z. Dokazati Ajzenštajnov kriterijum nesvodljivosti za polinome sa celobrojnim koeficijentima.

29.8 $x^n - 1 = 0$ nad poljem F, $kF = p$, $p \in Prost$

1° a Slučaj $n = p$. Tada $x^p - 1 = (x-1)^p$, te ova jednačina ima tačno jedno rešenje, $x = 1$.

1° b slučaj $n = p^k$. Tada $x^{p^k} - 1 = (x-1)^{p^k}$, pa kao u prethodnom slučaju, jedino rešenje je $x = 1$.

2° $(n, p) = 1$. Tada $f'(x) = nx^{n-1}$, $(f, f') = 1$, te je polinom $f(x) = x^n - 1$ separabilan.

29.9. $x^n - 1 = 0$ nad $\mathbb{Q}$. Neka je $\mathbb{E}$ korensko polje polinoma $f(x) = x^n - 1$. $f'(x) = nx^{n-1} \neq 0$, $(f, f') = 1$, pa je $f(x)$ separabilan. Dakle, $\mathbb{E}/\mathbb{Q}$ je Galoaovo raširenje. Dalje, $H_n = \{\varepsilon \in E \mid \varepsilon^n = 1\}$ je grupa u odnosu na množenje, te je kao konačna podgrupa multiplikativnog dela polja $\mathbb{E}$ ciklična, tj. postoji $\varepsilon \in E$ tako da je $H_n = \langle \varepsilon \rangle = \{1, \varepsilon, \dots, \varepsilon^{n-1}\}$. Primetimo da je $|H_n| = n$ jer je H_n skup svih korena polinoma $f(x)$ sadržanih u korenskom polju tog polinoma.

Ako je $\mathbb{E} \leq \mathbb{C}$, što možemo pretpostaviti, onda $H_n = \{ e^{\frac{2k\pi i}{n}} \mid k = 0, \dots, n-1\}$.

Ovde, $e^{i\varphi} = \cos\varphi + i\sin\varphi$ (Ojlerova notacija).

Ako $H_n = \langle \varepsilon \rangle$, onda kažemo da je ε primitivan koren ove jednačine.

Lema Neka je C_n ciklična grupa reda n, $C_n = \langle a \rangle$. Tada je $b \in C_n$, $b = a^i$ generator grupe C_n akko $(i, n) = 1$.

Dokaz (⇒) Neka je $C_n = \langle b \rangle$. Tada za neki $x \in \mathbb{Z}$, $b^x = a$, tj. $a^{ix} = a$.
Odavde (prema Lagranžovoj teoremi) $ix \equiv 1 \pmod n$, te za neki $y \in \mathbb{Z}$, $ix - yn = 1$.
Odavde $(i,n) = 1$.
(⇐) Pretpostavimo $(i,n) = 1$, $b = a^i$. Tada za neke $x, y \in \mathbb{Z}$ $ix + yn = 1$ (prema Bezuovoj teoremi), odakle $b^x = a^{ix} = a^{1-yn} = a \cdot (a^n)^{-y} = a$, te kako a generiše C_n, to i b generiše C_n. ∎

Napomena 1° Iz prethodnog odmah sledi $|\{a \in C_n \mid a \text{ je generator grupe } C_n\}| = \varphi(n)$, $\varphi(n)$ je Ojlerova funkcija.

2° Ako je $\sigma \in \mathrm{Aut}\, C_n$, tada

a. Ako $C_n = \langle a \rangle$ onda $C_n = \langle \sigma a \rangle$, tj. σ generatore grupe C_n prevodi u generatore grupe C_n

b. Ako je $C_n = \langle a \rangle$, tada je σ u potpunosti određen vrednošću $\sigma(a)$, tj. ako $\tau \in \mathrm{Aut}\, C_n$ i $\sigma(a) = \tau(a)$, onda $\sigma = \tau$: $\sigma(a^i) = \sigma(a)^i = \tau(a)^i = \tau(a^i)$.

c. Ako su a, b generatori grupe C_n tada postoji jedinstven $\sigma \in \mathrm{Aut}\, C_n$ tako da je $\sigma(a) = b$: $\sigma(a^i) \overset{\text{def}}{=} b^i$, $0 \le i \le n-1$.
Odavde, $|\mathrm{Aut}\, C_n|$ = broj generatora grupe $C_n = \varphi(n)$. Važi i više:
$\mathrm{Aut}\, C_n \cong \Phi_n = (\Phi_n, \cdot_n, 1)$, $\Phi_n = \{ i \in \mathbb{Z}_n \mid (i,n) = 1\} = \mathbb{Z}_n^*$.
Zaista, $h : \Phi_n \cong \mathrm{Aut}\, C_n$, gde $h(i) = \sigma_i$, $i \in \Phi_n$,
$\sigma_i(a) = a^i$ (a je generator grupe C_n).

d. $(m,n) = 1 \Rightarrow \Phi(mn) \cong \Phi(m) \times \Phi(n)$: Ako $(m,n) = 1$, tada je
$\rho : \Phi(mn) \cong \Phi(m) \times \Phi(n)$, $\rho(i) \overset{\text{def}}{=} (\mathrm{rest}(i,m), \mathrm{rest}(i,n))$, $i \in \Phi(mn)$.
Ovde, $\mathrm{rest}(x,n)$ = ostatak dobijen deljenjem x sa n, $x \in \mathbb{Z}$.

Vratimo se našoj jednačini $x^n - 1 = 0$ nad $\mathbb{Q}$. Ako je $\varepsilon \in E$ primitivan koren jednačine $x^n - 1$, tada je $E = \mathbb{Q}(\varepsilon)$ i $\mathbb{Q}(\varepsilon) \mid \mathbb{Q}$ je Galoaovo.

Teorema 1° $|\mathbb{Q}(\varepsilon) : \mathbb{Q}| = \varphi(n)$. 2° $\mathrm{Aut}(\mathbb{Q}(\varepsilon) : \mathbb{Q}] \cong \Phi(n)$!

Dokaz Primetimo da je prema prethodnom $H_n \cong C_n$. Ako je $\sigma \in \mathrm{Aut}(\mathbb{Q}(\varepsilon) \mid \mathbb{Q})$, tada $\sigma | H_n$ je automorfizam grupe $(H_n, \cdot, 1) = H_n$. Neka je

(0) $h : \mathrm{Aut}(\mathbb{Q}(\varepsilon) \mid \mathbb{Q}) \longrightarrow \mathrm{Aut}\, H_n \cong \mathrm{Aut}\, C_n \cong \Phi_n$, $h(\sigma) = \sigma | H_n$.

h je 1-1: Neka je $h(\sigma) = h(\tau)$, tj. $\sigma | H_n = \tau | H_n$. Tada $\sigma(\varepsilon) = \tau(\varepsilon)$, pa kako je $\mathbb{Q}(\varepsilon)$ generisano sa ε nad $\mathbb{Q}$ i σ, τ fiksiraju $\mathbb{Q}$, to $\sigma = \tau$. Odavde

(1) $|\mathrm{Aut}(\mathbb{Q}(\varepsilon) \mid \mathbb{Q})| \le \varphi(n)$, i s obzirom da je $|\mathbb{Q}(\varepsilon) : \mathbb{Q}| = |\mathrm{Aut}(\mathbb{Q}(\varepsilon) \mid \mathbb{Q})|$

(2) $|\mathbb{Q}(\varepsilon) : \mathbb{Q}| \le \varphi(n)$.

Da bi dokazali da je $|\mathbb{Q}(\varepsilon) : \mathbb{Q}| \ge \varphi(n)$ (dakle i $|\mathbb{Q}(\varepsilon) : \mathbb{Q}| = \varphi(n)$), dovoljno je da dokažemo da je stepen minimalnog polinoma $q \in \mathbb{Q}[x]$ za ε baš $\varphi(n)$.

Neka je $g(x)$ minimalni polinom za ε, $g \in Q[X]$. Kako je $f(\varepsilon)=0$, to za neki $h \in Q[X]$

$$x^n - 1 = g(x)\, h(x)$$

Mogli smo pretpostaviti da je g moničan, odakle $1 = g_n h_n = 1 \cdot h_n$, tj. i h je moničan. Prema Lemi 29.5 tada su g, h celobrojni polinomi, tj. $g, h \in Z[X]$. Dokazujemo:

(2) Ako je η primitivan koren jednačine $x^n - 1 = 0$, tada $g(\eta) = 0$.

S obzirom da su primitivni koreni oblika ε^i, $(i,n)=1$, dovoljno je dokazati da je $g(\varepsilon^i)=0$ za $(i,n)=1$, $1\le i\le n$. Poslednje tvrđenje posledica je od

(3) Ako je $p \in$ Prost, $(p,n)=1$, tada $g(\varepsilon^p)=0$.

Zaista, uz uslove u (3), onda $g(\varepsilon^{p^k})=0$ za sve k takve da $p^k \le n$ te kako je svaki $(i,n)=1$, $i = p_1^{k_1}\cdots p_\ell^{k_\ell}$, $(p_j, n)=1$, $j=1,\dots,\ell$; onda je i $g(\varepsilon^i)=0$.

Dokaz za (3): Pretpostavimo suprotno, da nije $g(\varepsilon^p)=0$, tj. $g(\varepsilon^p)\neq 0$. Kako je ε^p koren jednačine $x^n=1$, to je onda $h(\varepsilon^p)=0$, tj. ε je koren polinoma $h(x^p)$. Kako je $g(x)$ nesvodljiv i $g(\varepsilon)=0$, to onda $g(x) \mid h(x^p)$, tj. $h(x^p) = g(x)\, h_1(x)$ za neki $h_1 \in Q[X]$. Polinomi g i h su monični, pa je i h_1 moničan, te prema Lemi 29.5 $h_1 \in Z[X]$. Dakle, $h(x^p), g(x), h_1(x) \in Z[X]$.

Neka je $\rho: Z \longrightarrow Z_p$, $\rho: x \longmapsto \mathrm{rest}(x,p)$. Kao što znamo, ρ je epimorfizam. Neka je $\bar g = \rho g$, tj. ako $g(x) = \sum_i g_i x^i$, tada $\bar g(x) = \sum_i \bar g_i x^i$, gde $\bar g_i = \rho(g_i)$ ($\bar g_i$ = redukcija koeficijenta g_i mod p).

Tada su $\bar h(x^p), \bar g(x), \bar h_1(x) \in Z_p[X]$. Primetimo da je za ovu redukciju ispunjen bitan uslov, $h(x^p), g(x), h_1(x) \in Z[X]$ (da bi se ρ uopšte primenilo). S obzirom da je $x \longmapsto x^p$, $x \in Z_p$, automorfizam polja Z_p (Frobeniusov automorfizam), to iz identiteta $h(x^p) = g(x) h_1(x)$ koji važi u $Z[X]$ dobijamo $\bar h(x)^p = \bar g(x)\, \bar h_1(x)$ u $Z_p[X]$, odakle neki nesvodljivi faktor m od $\bar g(x)$

deli $\bar h(x)$, tj. $\bar g = g_1 \cdot m$, $\bar h = h_2 \cdot m$, te kako je $x^n - 1 = \bar g \bar h$ to $m^2(x) \mid x^n - 1$, tj. $x^n - 1$ ima višestruki koren u Z_p, mada je $(n,p)=1$, što je kontradikcija prema 29.8.2°. Prema tome $\deg g \ge |\{i \in Z_n \mid (i,n)=1\}| = \varphi(n)$, te je ovim 1° dokazano.

2° Preslikavanje $h: \mathrm{Aut}(Q(\varepsilon)\mid Q) \longrightarrow \mathrm{Aut}\, H_n \cong \Phi(n)$ je 1-1, pa kako $|\mathrm{Aut}(Q(\varepsilon)\mid Q)| = \varphi(n)$, h je na, pa $\mathrm{Aut}(Q(\varepsilon)\mid Q) \cong \Phi(n) \cong Z_n^* \cong \mathrm{Aut}\, C_n$.

30. Ciklotomični polinomi

U ovom odeljku opisaćemo svojstva minimalnih polinoma primitivnih korena polinoma $x^n - 1$. U tome ćemo koristiti sledeća tvrđenja.

30.1. Teorema Neka je C_n ciklična grupa reda n i neka je $C_n = \langle a \rangle$. Tada $C_n = \langle a^k \rangle$ akko $(k,n) = 1$, $1 \le k < n$. Dakle, ako je S_n skup generatora grupe C_n, tada $S_n = \{a^k \mid (k,n) = 1\}$. Takođe, podgrupa ciklične grupe je ciklična.

Dokaz: vežba

30.2. Teorema Neka su $k, n \in N^+$. Tada za cikličnu grupu C_n važi:

1° Ako $k|n$ tada postoji $H < C_n$, red $H = k$.

2° Ako su $H, K < C_n$ i $|H| = |K|$ tada $H = K$.

Dokaz: 1° Ako $C_n = \langle a \rangle$, tada je $H = \langle a^{\frac{n}{k}} \rangle$ podgrupa reda k.

2° Neka su $H, K < C_n$, $C_n = \langle a \rangle$, $|H| = |K| = k$. Ako je $k = 1$, tada $H = \langle 1 \rangle = K$. Pretpostavimo $k > 1$. Neka je $H = \langle a^{\frac{n}{k}} \rangle$, tada $|H| = k$. Dokazujemo da je $K = H$. Za to je dosta da dokažemo da je $a^{\frac{n}{k}} \in K$, jer tada $H \subseteq K$, pa $H = K$ jer $|H| = |K|$.
Neka je $d \in N^+$ najmanji takav da je $a^d \in K$. Takav d postoji jer $|K| > 1$.
Neka je $b = a^d$ i neka je $x \in K$. Tada za neki i, $x = a^i$. Neka je $i = qd + r$, $0 \le r < d$.
Tada $a^r = a^{i-qd} = a^i (a^d)^{-q} = x b^{-q}$, pa $a^r \in K$. S obzirom na izbor broja d, $r = 0$, tj. $i = qd$, odakle $K = \langle b \rangle = \{1, b, \dots, b^{k-1}\}$ jer $|K| = k$ i za $0 \le i, j < k$, $i \ne j$, $b^i \ne b^j$. Dokažimo

(*) $\quad 0 \le i \le k \Rightarrow id \le n$.

Neka je $i \in N$ najmanji takav da je $id > n$. Tada $0 < id - n \le d$. Dalje $a^{id-n} = b^i$, pa $a^{id-n} \in K$, te s obzirom na izbor broja d, $d \le id - n$, tj. $id - n = d$, odakle $n = (i-1)d$. Dalje, $a^n = a^{(i-1)d} = b^{i-1}$, pa $b^{i-1} = 1$.
S obzirom da je $id > n$ i $d \le n$, to $i \ge 2$, tj. $i - 1 > 0$, odakle $i - 1 \ge k$ jer je red $K = k$ i $b^{i-1} = 1$. Prema tome (*) važi, a odatle sledi

(1) $\quad kd \le n$.

Dalje $b^k = 1$, tj. $a^{kd} = 1$, odakle $kd \equiv 0 \mod n$, pa $n \mid kd$ tj.

(2) $\quad n \le kd$

odakle $n = kd$, pa $b = a^d = a^{\frac{n}{k}}$.

Neka je $S_d = \{b \in C_n \mid \text{red } b = d\}$, gde $d|n$. Ako $b \in S_d$ tada b generiše podgrupu reda d grupe C_n. Prema T. 30.2 elementi iz S_d generišu jednu te istu podgrupu, cikličnu grupu $C_d \subseteq C_n$. S obzirom na T. 30.1, $|S_d| = \varphi(d)$, i

30.3. $C_n = \bigcup_{d|n} S_d$ je disjunktna unija; $S_d = \{b \mid b \text{ je generator cikličke grupe } C_d\}$.

30.4. Zadatak $\sum_{d|n} \varphi(d) = n$. (Gaus).

Neka je $C_n = \{x \in C \mid x^n - 1 = 0\}$. $C_n = (C_n, \cdot, 1)$ je ciklična grupa reda n, te neka je ε primitivan koren jednačine $x^n - 1 = 0$, tj. generator ove grupe.

Neka je za $n\in N^+$ $\Phi_n(x)=\prod_{\substack{\xi\in C_n\\ \text{red}\,\xi=n}}(x-\xi)$, tj. koreni polinoma $\Phi_n(x)$ tačno su primitivni koreni polinoma x^n-1. Dakle, $\Phi_n(x)=\prod_{(k,n)=1}(x-\varepsilon^k)$. Dalje, prema 30.3

$$x^n-1=\prod_{\xi\in C_n}(x-\xi)=\prod_{d|n}\prod_{\substack{\xi\in C_d\\ \text{red}\,\xi=d}}(x-\xi)=\prod_{d|n}\Phi_d(x),$$ tj.

30.5. $$x^n-1=\prod_{d|n}\Phi_d(x),\quad \deg\Phi_d(x)=\varphi(d).$$

Ako je $\sigma\in Aut(Q(\varepsilon)|Q)$ tada za $\sigma'=\sigma|C_n$, $\sigma'\in Aut\,C_n$, te ako je $\xi\in C_n$ element reda n, tada je i $\sigma(\xi)=\sigma'(\xi)$ element reda n, tj. σ permutuje korene polinoma $\Phi_n(x)$, pa koeficijenti polinoma $\Phi_n(x)$ pripadaju fiksnom polju grupe $G=Aut(Q(\varepsilon)|Q)$, tj. $\Phi_n(x)\in Q[x]$. Dakle, $\Phi_n(x)$ je moničan polinom sa racionalnim koeficijentima. Indukcijom se neposredno dokazuje da zapravo $\Phi_d(x)\in Z[x]$. Zaista, $x^n-1=\Phi_n(x)\cdot\prod_{\substack{d|n\\ d<n}}\Phi_d(x)$, pa po induktivnoj hipotezi $\prod\Phi_d(x)\in Z[x]$

Prema lemi 29.5 onda $\Phi_n(x)\in Z[x]$. Dakle, $\Phi_n(\varepsilon)=0$, $\deg\Phi_n(x)=\varphi(n)$ i $|Q(\varepsilon):Q|=\varphi(n)=\deg$ (minimalni polinom za x), odakle sledi da je $\Phi_n(x)$ minimalan polinom za ε, dakle i nesvodljiv. Ove polinome možemo odrediti pomoću rekurzivne formule 30.5:

30.6. <u>Primer</u> a. $\Phi_1(x)=x-1$, $\Phi_2(x)=x+1$, $\Phi_3(x)=1+x+x^2$; $x^6-1=\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)$ pa $\Phi_6(x)=x^2-x+1$.

b. $\Phi_p(x)=1+x+\dots+x^{p-1}$, $p\in$ Prost

c. $\Phi_{p^k}(x)=\sum_{i=0}^{p-1}x^{ip^{k-1}}$

30.7. Möbiusova funkcija: $$\mu(n)=\begin{cases}(-1)^k, & n=p_1\cdot p_2\cdots p_k,\ p_1,\dots,p_k \text{ prosti}\\ 1, & n=1\\ 0, & \text{inače}.\end{cases}$$

<u>Teorema</u> $\mu(n)$ je multiplikativna funkcija, tj. $(m,n)=1\Rightarrow\mu(mn)=\mu(m)\mu(n)$. ∎

30.8 <u>Teorema</u> Ako je $f(n)$ multiplikativna aritmetička funkcija tada je i $g(n)=\sum_{d|n}f(d)$ multiplikativna aritmetička funkcija.

<u>Dokaz</u> Najpre primetimo da važi

(1) Ako $(m,n)=1$ tada $d|mn\Leftrightarrow\exists d,d'\,(d=dd'\wedge d|m\wedge d'|n)$

Otuda, za $(m,n)=1$

$$g(mn)=\sum_{d|mn}f(d)=\sum_{d|m,d'|n}f(dd')=\sum_{d|m,d'|n}f(d)f(d')=\Big(\sum_{d|m}f(d)\Big)\cdot\Big(\sum_{d'|n}f(d')\Big)=g(m)g(n).$$

<u>Primer</u> $\nu(n)=\sum_{d|n}\mu(d)$ je multiplikativna aritmetička funkcija.

Kao što znamo, vrednosti multiplikativnih funkcija određene su vrednostima u potencijama prostih brojeva. Dakle, za $p\in$ Prost, $k\in N$

$$\nu(p^k)=\sum_{d|p^k}\mu(d)=\sum_{i\le k}\mu(p^i)=\mu(1)+\mu(p)+\dots+\mu(p^k)=\begin{cases}\mu(1), & k=0\\ \mu(1)+\mu(p), & k\ge1\end{cases},$$ odakle

$\nu(1)=1$, $\nu(n)=0$ za $n>1$. (Primetimo da je $\nu(p_1^{d_1}\cdots p_k^{d_k})=\nu(p_1^{d_1})\cdots\nu(p_k^{d_k})$, $p_1,\dots,p_k$ različiti prosti brojevi).

30.9. <u>Möbiusova teorema inverzije.</u> Neka je $\mathbb{F}$ polje i $f: \mathbb{N}^+ \to \mathbb{F}$. Ako je $g(n) = \sum_{d|n} f(d)$, tada $f(n) = \sum_{d|n} \mu(d)\, g(\frac{n}{d})$, $n \in \mathbb{N}^+$.

<u>Dokaz</u> Najpre primetimo da za $d, d', n \in \mathbb{N}^+$ važi:

(1) $d|n \wedge d'|\frac{n}{d} \Leftrightarrow d'|n \wedge d|\frac{n}{d'}$. Otuda

$$\sum_{d|n} \mu(d)\, g(\tfrac{n}{d}) = \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') = \sum_{d|n,\, d'|\frac{n}{d}} \mu(d) f(d') = \sum_{d'|n,\, d|\frac{n}{d'}} \mu(d) f(d')$$

$$= \sum_{d'|n} f(d') \cdot \sum_{d|\frac{n}{d'}} \mu(d) = \sum_{d'|n} f(d')\, \nu(\tfrac{n}{d'}) = f(n)\,\nu(1) = f(n) \quad ∎$$

30.10. <u>Zadatak.</u> Dokazati da je $\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$ (Gauss)

30.11* <u>Zadatak</u> Dokazati da je $\{ \frac{\varphi(n)}{n} \mid n \in \mathbb{N}^+ \}$ gust u $[0,1]_{\mathbb{R}}$.

30.12. <u>Teorema</u> $\Phi_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}$.

<u>Dokaz</u> Iz $x^n - 1 = \prod_{d|n} \Phi_d(x)$ nalazimo $\ln(x^n - 1) = \sum_{d|n} \ln \Phi_d(x)$ za one $x \in \mathbb{R}$ za koje identitet ima smisla, u svakom slučaju za beskonačno mnogo $x \in \mathbb{R}$.

Prema Möbiusovoj teoremi inverzije, nalazimo

$\ln \Phi_n(x) = \sum_{d|n} \mu(d) \ln(x^{\frac{n}{d}} - 1)$, tj. $\Phi_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}$ za beskonačno mnogo $x \in \mathbb{R}$, pa obzirom da se radi o polinomima onda i za svako $x \in \mathbb{R}$. ∎

30.13. <u>Zadatak</u> Ponovo uraditi zadatak 30.6.c.

30.14. <u>Zadatak</u> $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}$.

30.15. <u>Primer</u> $\sum_{\substack{\xi \in C_n \\ \text{red}\, \xi = n}} \xi = \mu(n)$. Tj. zbir primitivnih korena jednačine $x^n - 1 = 0$ jednak je $\mu(n)$, odnosno $\sum_{(k,n)=1} \varepsilon^k = \mu(n)$, ε je prim. koren jedn. $x^n - 1 = 0$.

<u>Dokaz</u> Neka je ε primitivan koren jednačine $x^n - 1 = 0$. Tada

(1) $\sum_{k=0}^{n-1} \varepsilon^k = (\varepsilon^n - 1)/(\varepsilon - 1) = 0$ za $n > 1$ i $\sum_{k=0}^{n-1} \varepsilon^k = 1$ za $n = 1$, tj.

(2) $\sum_{k=0}^{n-1} \varepsilon^k = \nu(n)$.

Prema oznakama u 30.3 neka je za $\mathbb{C}_n = \{x \in \mathbb{C} \mid x^n - 1 = 0\}$, $s_d = \sum_{\xi \in S_d} \xi$. Tada

$\nu(n) = \sum_{k=0}^{n-1} \varepsilon^k = \sum_{\xi \in \mathbb{C}_n} \xi = \sum_{d|n} \sum_{\xi \in S_d} \xi = \sum_{d|n} s_d$, te prema Möbiusovoj teoremi inverzije je

$$s_n = \sum_{d|n} \mu(d)\, \nu(\tfrac{n}{d}) = \mu(n)\,\nu(1) = \mu(n) \quad ∎$$

30.16. <u>Ramanujanova suma</u> Dokazati za $m, n \in \mathbb{N}^+$ ($(m,n) = NZD(m,n)$):

$$\sum_{d|(m,n)} d\, \mu(\tfrac{n}{d}) = \frac{\mu(\frac{n}{(m,n)})\, \varphi(n)}{\varphi(\frac{n}{(m,n)})}.$$

31. $\overline{\mathbb{R}} = \mathbb{C}$

U ovom odeljku dokazaćemo metodama teorije Galoa da je polje kompleksnih brojeva $\mathbb{C}$ algebarsko zatvorenje polja realnih brojeva $\mathbb{R}$. Ispostavlja se da slično tvrđenje važi za široku i važnu klasu polja, realno zatvorena polja.

31.1. Formalno-realna polja. Polje $\mathbb{F}$ je formalno realno ukoliko u njemu važi:

$$x_1^2 + x_2^2 + \cdots + x_n^2 = 0 \Rightarrow x_1, \ldots, x_n = 0 \quad , \quad n \in N.$$

Na primer, svako podpolje polja $\mathbb{R}$ je formalno realno. Polje racionalnih izraza $\mathbb{R}(x)$ nad $\mathbb{R}$ je takođe formalno realno.

31.1a* Zadatak Neka je $\mathbb{F}$ formalno realno polje. Dokazati da postoji uređenje $\leq$ domena $\mathbb{F}$ tako da je $(\mathbb{F}, \leq)$ uređeno polje, tj. $\leq$ je linearno uređenje i saglasno je sa operacijama polja $\mathbb{F}$: $x \leq y \Rightarrow x+z \leq y+z$; $x \leq y,\ 0 \leq z \Rightarrow xz \leq yz$, $x, y, z \in F$.

31.1b Zadatak Neka je $\pi = 3.14\ldots$ i $\mathbb{F} = \mathbb{Q}(\pi)$. Dakle, $\pi \in F$.

1° Dokazati da postoji uređenje $\leq$ polja $\mathbb{F}$ tako da je $\pi \leq 0$.

2° Dokazati da postoji uređenje $\leq$ polja $\mathbb{F}$ tako da je $\bigwedge_{n \in N^+} 0 < \pi < \frac{1}{n}$.

3° Dokazati da postoji $c = 2^{\aleph_0}$ uređenja polja $\mathbb{F}$.

4° Dokazati da postoji tačno jedno arhimedovsko uređenje polja $\mathbb{F}$.

Ako je $\mathbb{F}$ formalno-realno polje, odmah vidimo da je $k\mathbb{F} = 0$, jer ako bi $\mathbb{F}$ bilo proste karakteristike p, onda bi u $\mathbb{F}$ važilo $\underbrace{1^2 + \cdots + 1^2}_{p} = 0$, suprotno definiciji formalno-realnih polja. Primetimo da polje $\mathbb{C}$ nije formalno realno: $1^2 + i^2 = 0$.

31.1c. Zadatak Dokazati da polje $\mathbb{C}$ nema dopunu do uređenog polja.

31.2 Realno-zatvorena polja. Polje $\mathbb{F}$ je realno-zatvoreno ukoliko ~~zadovoljava~~ uslove:

1° $\mathbb{F}$ je formalno-realno polje.

2° Ako je $p \in \mathbb{F}[x]$ neparnog stepena, tada p ima koren u $\mathbb{F}$.

3° Ako je $a \in F$ tada (tačno) jedna od jednačina $x^2 = a$, $x^2 = -a$ ima koren u $\mathbb{F}$.

Polja $\mathbb{R}$, $A \cap \mathbb{R}$ su primeri realno-zatvorenih polja.

31.2a. Zadatak Dokazati da postoji realno-zatvoreno polje $\mathbb{F}$, $\mathbb{F} \not\cong \mathbb{R}$, $\mathbb{F} \not\cong A \cap \mathbb{R}$.

Realno-zatvorena polja su mnogo čemu slična sa poljem realnih brojeva $\mathbb{R}$. To je posledica, između ostalog, činjenice da se teorija prvog reda realno-zatvorenih polja poklapa sa teorijom prvog reda realnih brojeva. Polazno mesto u izučavanju ovih polja je Artin-Šrajerova teorija realno-zatvorenih polja. Artin je uz pomoć ove teorije rešio:

17. Hilbertov problem: $q(\bar{x}) \in R(\bar{x})$, $q(\bar{x}) = f(\bar{x})/h(\bar{x})$ je pozitivno definitna ako

$$\bigwedge_{\bar{x} \in R} (h(\bar{x}) \neq 0 \Rightarrow q(\bar{x}) \geq 0)\ ;$$ ovde je $\bar{x} = x_1, \ldots, x_n$ niz promenljivih. Tada 17HP glasi:

Ako je $q(\bar{x}) \in R(\bar{x})$ pozitivno definitna, tada je $q(\bar{x})$ suma kvadrata nekih racionalnih izraza nad $\mathbb{R}$.

31.2b. Zadatak Neka je $p(x) \in R[x]$ pozitivno definitan. Dokazati da postoje $q_1, q_2 \in R[x]$ tako da je $p = q_1^2 + q_2^2$.

Spomenimo da realno-zatvorena polja imaju važno mesto u nearhimedovskoj (nestandardnoj, Lajbnicovoj) analizi. Uz pomoć ove teorije i teorije modela, Abraham Robinson šezdesetih godina 20. veka zasnovao je infinitezimalni račun, tj. analizu sa aktuelnim beskonačno malim i beskonačno velikim veličinama, onako kako ga je zamišljao Lajbniz.

31.2c. <u>Zadatak</u> Dokazati da postoji nearhimedovsko realno-zatvoreno polje.

Od ovog mesta pa do kraja odeljka 31, $\mathbb{R}$ će označavati bilo koje realno-zatvoreno polje, dok je $\mathbb{C} = \mathbb{R}(i)$, gde je i koren polinoma x^2+1.

31.3. <u>Uređenje polja $\mathbb{R}$</u>. Prema zadatku 31.1a $\mathbb{R}$ ima proširenje do uređenog polja. U slučaju polja $\mathbb{R}$ dokaz ove činjenice je jednostavan.

31.3a. <u>Lema</u> $\bigwedge_{a,b\in R} \bigvee_{c\in R} a^2+b^2=c^2$.

<u>Dokaz</u> Neka su $a,b\in R$. Ako je $a=0$, $b=0$, možemo uzeti $c=0$. PP $a\neq 0$ ili $b\neq 0$. Prema 31.2.3° postoji $c\in R$ tako da je $a^2+b^2=c^2$ ili $a^2+b^2=-c^2$. Ako je $a^2+b^2=-c^2$ onda $a^2+b^2+c^2=0$, te prema 31.2.1° $a=0, b=0, c=0$, kontradikcija. Dakle $a^2+b^2=c^2$ ■

31.3b. <u>Teorema</u> Neka je $\leq$ relacija domene R definisana sa: $a\leq b$ akko $\bigvee_{c\in R} b=a+c^2$. Tada je $(\mathbb{R},\leq)$ uređeno polje. (U dokazu koji sledi; $a,b,c,d\in R$)

<u>Dokaz</u> 1° $a\leq a$ jer $a=a+0^2$ (R)

2° (AS) Neka je $a\leq b$, $b\leq a$. Tada za neke c,d, $a=b+c^2$, $b=a+d^2$, odakle $c^2+d^2=0$ tj. $c=0, d=0$, pa $a=b$.

3° (T) Neka je $a\leq b$, $b\leq c$. Tada za neke $d_1,d_2\in R$, $b=a+d_1^2$, $c=b+d_2^2$ tj. $c=a+d_1^2+d_2^2$. Prema Lemi 31.3a onda za neki d $c=a+d^2$ tj. $a\leq c$.

4° (L) Prema 31.2.3° postoji c tako da je $a-b=c^2$ ili $b-a=c^2$, dakle $a\leq b$ ili $b\leq a$.

Prema R + AS + T + L, $(R,\leq)$ je linearno uređenje.

5° (Saglasnost uređenja $\leq$ sa operacijom sabiranja $+_R$). PP $a\leq b$. Tada za neki d $b=a+d^2$, odakle $b+c=a+c+d^2$, tj. $a+c\leq b+c$.

6° (Saglasnost uređenja $\leq$ sa operacijom $\cdot_R$). PP $a\leq b$, $0\leq c$. Tada za neke $d_1,d_2\in R$ $b=a+d_1^2$, $c=0+d_2^2$, tj. $c=d_2^2$. Otuda $bc=(a+d_1^2)c=ac+(d_1d_2)^2$, pa $ac\leq bc$. ■

31.3c. <u>Lema</u> Neka je $(\mathbb{F},\leq)$ uređeno polje. Tada u $\mathbb{F}$ važi:

1° $x\geq 0 \Rightarrow -x\geq 0$, 2° $x\leq y \Rightarrow -y\leq -x$, 3° $x\leq y$, $z\leq 0 \Rightarrow yz\leq xz$, 4° $x^2\geq 0$. ■

31.3d <u>Teorema</u> Na $\mathbb{R}$ postoji tačno jedno uređenje tako da je $(\mathbb{R},\leq)$ uređeno polje.

<u>Dokaz</u> Prema 31.3b takvo uređenje postoji, to je $(\mathbb{R},\leq)$ gde je $\leq$ konstruisano u 31.3b. Neka je $(\mathbb{R},\preccurlyeq)$ bilo koje uređeno polje, i neka su $a,b\in R$. PP $a\preccurlyeq b$. Za neki $c\in R$ $a-b=c^2$ ili $b-a=c^2$. Ako je $a-b=c^2$, tada $c^2\preccurlyeq 0$, te prema 31.3c 4°, $c=0$, tj. $a=b$. Dakle, $a\preccurlyeq b \Rightarrow \bigvee_{c\in R} b=a+c^2$, tj. $a\preccurlyeq b \Rightarrow a\leq b$. PP da nije $a\preccurlyeq b$. Zbog linearnosti, onda $a\neq b$, $b\preccurlyeq a$. Prema već dokazanom onda $b\leq a$. Dakle:

$$\bigwedge_{a,b\in R}(a\preccurlyeq b \Leftrightarrow a\leq b).$$ ■

Prema prethodnom možemo pretpostaviti da je na $\mathbb{R}$ uvedeno uređenje, neka je to $\leq$, tako da je $(\mathbb{R}, \leq)$ uređeno polje. S obzirom na jedinstvenost tog uređaja možemo uvesti korenusku funkciju:

31.3c Definicija $y = \sqrt{x} \Leftrightarrow x \geq 0 \wedge y \geq 0 \wedge x^2 = y$.

Ovim je f-ja $\sqrt{x}$ dobro definisana na pozitivnom segmentu R^+, $\sqrt{0} = 0$.

31.3d. Zadatak Neka je $f: R^+ \to R$, $f(x) = \sqrt{x}$, $f(0) = 0$. Dokazati:

1° $f(x)^2 = x$, $f(xy) = f(x)f(y)$, $x, y \in R^+ \cup \{0\}$

2° Dokazati da postoji beskonačno mnogo f-ja $f: R^+ \cup \{0\} \to R$ takvih da je $f(x)^2 = x$.

3° Dokazati da je $\sqrt{x}$ jedina f-ja koja zadovoljava uslove 1°

U $\mathbb{R}$ se mogu uvesti i druge f-je, na primer $|x| = sgn(x) \cdot x$ gde je $sgn(x) = \begin{cases} 1, & x > 0 \\ 0, & x = 0 \\ -1, & x < 0 \end{cases}$.

31.4. $\mathbb{C} = \mathbb{R}(i)$

Najpre primetimo da je

31.4a $|\mathbb{C} : \mathbb{R}| = 2$ i $\mathbb{C}|\mathbb{R}$ je Galoaovo raširenje, takođe $\mathbb{C} = \{a + bi \mid a, b \in R\}$.

31.4b. Lema Za svaki $z \in C$ jednačina $x^2 = z$ ima rešenje u $\mathbb{C}$.

Dokaz Neka je $\underset{a,b \in R}{z = a + bi}$, $r = \sqrt{a^2+b^2}$, $u = \frac{a}{\sqrt{a^2+b^2}}$, $v = \frac{b}{\sqrt{a^2+b^2}}$, gde $z \neq 0$.

1° $1 - u^2 \geq 0$. Zaista, $1 - u^2 = \left(\frac{b}{\sqrt{a^2+b^2}}\right)^2 \geq 0$

2° $1-u, 1+u \geq 0$. Zaista, prema 1°, $1-u \geq 0, 1+u \geq 0$ ili $1-u \leq 0, 1+u \leq 0$. U ovom drugom slučaju, $0 < 1^2 + 1^2 = 2 = (1-u) + (1+u) \leq 0$, kontradikcija. Dakle, $1-u \geq 0$, $1+u \geq 0$.

Neposredno se proverava da su $x_{1,2} = \pm\sqrt{r}\left(\sqrt{\frac{1+u}{2}} + i\, sgn(v)\sqrt{\frac{1-u}{2}}\right)$ rešenja jednačine $x^2 = z$ ∎

31.4c Posledica Kvadratne jednačine sa koeficijentima u $\mathbb{C}$ imaju rešenja u $\mathbb{C}$.

31.4d. Zadatak Rešiti jednačinu $x^2 = i$ u $\mathbb{C}$.

31.4e. Zadatak Kako bi ste uveli funkciju $\sqrt[n]{x}$ za $x \in R$, $x \geq 0$, $n \in N^+$?

31.5. Teorema (Gaus; Artinov dokaz). $\overline{\mathbb{R}} = \mathbb{C}$.

U dokazu ove teoreme koristićemo sledeće tvrđenje.

31.5a. Lema Neka je G konačna p-grupa, tj. $|G| = p^n$, gde je $p \in$ Prost, $n \in N^+$. Tada postoji $H \lhd G$ tako da je $|G/H| = p$.

Dokaz Dokaz izvodimo indukcijom po n gde je $|G| = p^n$. Za $n=1$, tvrđenje je trivijalno.

PP $n \geq 2$. Iz klasovne jednakosti $|G| = |Z(G)| + \sum_{\substack{x \in T \\ x \notin Z(G)}} |G : C(x)|$ sledi da postoji $k \in N$ tako da je $p^n = |Z(G)| + kp$. Dakle, $p \mid |Z(G)|$, te prema Košijevoj lemi postoji $a \in Z(G)$, $red(a) = p$. Kako je $a \in Z(G)$, to je $\langle a \rangle \lhd G$. Dakle, $G/\langle a \rangle$ je grupa reda $n-1$. Kako je $n \geq 2$, po induktivnoj hipotezi postoji $K \lhd G/\langle a \rangle$, $|K| = p^{n-2}$. Neka je $k: G \to G/\langle a \rangle$ kanonski homomorfizam. Tada je $H = k^{-1}(K)$, $H \lhd G$, $|H| = p^{n-1}$, dakle, $|G : H| = p$.

∎

Dokaz Teoreme 31.5 Dovoljno je da dokažemo da se svako konačno raširenje polja $\mathbb{C}$ poklapa sa $\mathbb{C}$. Naime, ako je $f\in\mathbb{C}[x]$, $\deg f\geq 1$, tada f ima koren u nekom konačnom raširenju polja $\mathbb{C}$, te bi u ovom slučaju f imalo koren u $\mathbb{C}$.
Dakle, neka je $\mathbb{E}$ konačno raširenje polja $\mathbb{C}$.

Možemo pretpostaviti da je $\mathbb{E}|\mathbb{R}$ galoaovo. Najpre primetimo da je $\mathbb{E}$ konačno i separabilno raširenje polja $\mathbb{R}$ pa postoji $a\in\mathbb{E}$ tako da je $\mathbb{E}=\mathbb{R}(a)$. Ako je $f\in\mathbb{R}[x]$ minimalni polinom, tada je korensko polje $\mathbb{E}'\supseteq\mathbb{E}$ polin. f galoaovo raširenje polja $\mathbb{R}$.

$$G\left(\begin{array}{c}\mathbb{E}\\ \cup\!\mid\\ \mathbb{C}\\ \cup\!\mid\\ \mathbb{R}\end{array}\right.\qquad \mathbb{E}\overset{H}{\supseteq}\mathbb{F}\supseteq\mathbb{R}$$

Neka je G galoaova grupa $\mathbb{E}|\mathbb{R}$, tj. $G=\mathrm{Aut}(\mathbb{E}|\mathbb{R})$, i neka je $|G|=2^n(2m+1)$. Prema Silovljevoj teoremi postoji 2-podgrupa $H<G$. Neka je $\mathbb{F}=\mathbb{E}^H$ – fiksno polje grupe H. Tada je prema Artinovoj teoremi $H=\mathrm{Aut}(\mathbb{E}|\mathbb{F})$, dakle $|\mathbb{E}:\mathbb{F}|=|H|=2^n$, pa iz

$2^n(2m+1)=|\mathbb{E}:\mathbb{R}|=|\mathbb{E}:\mathbb{F}|\cdot|\mathbb{F}:\mathbb{R}|$ sledi $|\mathbb{F}:\mathbb{R}|=2m+1$. $\mathbb{F}$ je konačna separabilna ekstenzija polja $\mathbb{R}$, te postoji $b\in\mathbb{F}$ tako da je $\mathbb{F}=\mathbb{R}(b)$. Neka je g minimalni polinom elementa b, $g\in\mathbb{R}[x]$. Tada $\deg g=|\mathbb{F}:\mathbb{R}|=2m+1$, tj. g je neparnog stepena. Polinom g je nesvodljiv dok, s druge strane, svaki polin. neparnog stepena nad $\mathbb{R}$ ima koren u $\mathbb{R}$; dakle g je linearan polinom, tj. $m=0$.
Dakle $|G|=2^n$.

Kako je $\mathbb{C}$ međupolje polja $\mathbb{R}\subseteq\mathbb{C}$ i $\mathbb{E}|\mathbb{R}$ je galoaovo, to je prema osnovnoj teoremi 26.4 teorije Galoa $\mathbb{E}|\mathbb{C}$ galoaova ekstenzija. Neka je $G'=\mathrm{Aut}(\mathbb{E}|\mathbb{C})$. Kako je $G'<G$ (jer svaki $\sigma\in\mathrm{Aut}\,\mathbb{E}$ koji fiksira $\mathbb{C}$, takođe fiksira i $\mathbb{R}$), to je G' takođe 2-grupa.

$$G'\left[\begin{array}{c}\mathbb{E}\\ \cup\!\mid\\ \mathbb{F}'\\ \cup\!\mid\\ \mathbb{C}\end{array}\right.\qquad \mathbb{E}\overset{H'}{\supseteq}\mathbb{F}'\overset{\text{gal.}}{\supseteq}\mathbb{C}$$

Pretpostavimo da je G' netrivijalna, tj. $|G'|\geq 2$. Tada prema Lemi 31.5b postoji $H'\lhd G'$, $|G':H'|=2$. Neka je $\mathbb{F}'=\mathbb{E}^{H'}$ – fiksno polje grupe H'. Tada je $\mathbb{E}|\mathbb{F}'$ galoaova ekstenzija i $H'=\mathrm{Aut}(\mathbb{E}|\mathbb{F}')$. Kako je $H'\lhd G'$, to je i $\mathbb{F}'|\mathbb{C}$ galoaova ekstenzija i $\mathrm{Aut}(\mathbb{F}'|\mathbb{C})\cong G'/H'$, tj.

$|\mathbb{F}':\mathbb{C}|=|\mathrm{Aut}(\mathbb{F}'|\mathbb{C})|=2$, pa je $\mathbb{F}'|\mathbb{C}$ kvadratno raširenje, tj. $\mathbb{F}'=\mathbb{C}(a)$ gde je $a\in\mathbb{F}'$ koren nekog kvadratnog polinoma $h\in\mathbb{C}[x]$. Ali, prema 31.4c, $a\in\mathbb{C}$, dakle $\mathbb{F}'=\mathbb{C}$, kontradikcija prema $|\mathbb{F}':\mathbb{C}|=2$.
Dakle, G' je trivijalna grupa, pa $|\mathbb{E}:\mathbb{C}|=|G'|=1$, tj. $\mathbb{E}=\mathbb{C}$ ∎

31.5b*. zadatak Neka je $\mathbb{F}$ formalno-realno polje. Dokazati da postoji realno zatvoreno polje $\mathbb{E}\supseteq\mathbb{F}$ tako da je $\mathbb{E}|\mathbb{F}$ algebarsko raširenje.

32. Simetrične funkcije

Neka je $\mathbb{F}$ polje i $f(x_1,\dots,x_n) \in F[x_1,\dots,x_n]$ polinom promenljivih $x_1,\dots,x_n$. Polinom $f(x_1,\dots,x_n)$ je <u>simetričan</u> ako za svaku permutaciju $p \in S_n$ važi $f(x_{p_1},\dots,x_{p_n}) = f(x_1,\dots,x_n)$.

32.1. <u>Primer</u> Sledeći polinomi su simetrični:

1° $x_1^2 x_2 x_3 + x_1 x_2^2 x_3 + x_1 x_2 x_3^2$

2° $\sigma_0 = 1$, $\sigma_1 = -\sum\limits_{1\le i\le n} x_i$, $\sigma_2 = \sum\limits_{1\le i<j\le n} x_i x_j$, ..., $\sigma_k = (-1)^k \sum\limits_{1\le i_1<\dots<i_k\le n} x_{i_1} x_{i_2}\cdots x_{i_k}$, $\sigma_n = (-1)^n \prod\limits_{i=1}^n x_i$.

3° $s_k = \sum\limits_{i=1}^n x_i^k$.

Na isti način definiše se pojam simetričnog racionalnog izraza.

32.2. <u>Osnovna teorema o simetričnim polinomima.</u> Neka su $\sigma_1,\dots,\sigma_n$ polinomi definisani u 32.1.2°. Svaki simetričan polinom $f \in F[x_1,\dots,x_n]$ jednak je nekom polinomu nad $\mathbb{F}$ od simetričnih funkcija $\sigma_1,\dots,\sigma_n$, tj. postoji $g \in F[x_1,\dots,x_n]$ tako da je $f(x_1,\dots,x_n) = g(\sigma_1,\dots,\sigma_n)$.

<u>Dokaz</u> Neka je $\mathbb{K} = F(x_1,\dots,x_n)$ polje racionalnih izraza, $L = \{ f \in K \mid f \text{ je simetričan}\}$, $S = \{ g(\sigma_1,\dots,\sigma_n) \mid g(x_1,\dots,x_n) \in K\}$. Tada:

<u>1°</u> L i S su podpolja polja K i $\mathbb{F} \subseteq S \subseteq \mathbb{L} \subseteq \mathbb{K}$.

Neka je za permutaciju $p \in S_n$, $\theta_p \in Aut(\mathbb{K})$ definisan sa
$\theta_p : f(x_1,\dots,x_n) \longmapsto f(x_{p_1},\dots,x_{p_n})$, $f \in K$.
Tada je $G = \{\theta_p \mid p \in S_n\}$ podgrupa grupe $Aut(\mathbb{K})$ i očigledno

2° red $G = n!$

Dalje, očevidno je $L = K^G$, te je prema Artinovoj teoremi $\mathbb{K}$ Galoaovo raširenje polja $\mathbb{L}$ i $G = Aut(\mathbb{K}|\mathbb{L})$. Dakle,

3° $|\mathbb{K} : \mathbb{L}| = n! =$ red G.

Tvrdenje teoreme za racionalne izraze, tj. da je $L = S$, možemo sada lako dokazati. Naime dovoljno je da dokažemo da je $|\mathbb{K} : S| \le n!$, s obzirom da iz $n! \ge |\mathbb{K} : S| = |\mathbb{K} : L| \cdot |L : S| = n! \cdot |L : S|$ sledi $|\mathbb{L} : S| = 1$, tj. $L = S$. Dakle, dokazujemo da je $|\mathbb{K} : S| \le n!$.

Neka je $S_n, S_{n-1}, \dots, S_1$ niz polja i $p_n, \dots, p_1$ niz polinoma definisani na sledeći način, uzimajući da je t promenljiva koja se razlikuje od $x_1,\dots,x_n$:

$p_n(t) = (t-x_1)(t-x_2)\cdots(t-x_n) = \sum\limits_{i=0}^{n} \sigma_{n-i} x^i$ (prema Vijetovim formulama)

$p_{k-1}(t) = \dfrac{p_n(t)}{(t-x_k)(t-x_{k+1})\cdots(t-x_n)} = \dfrac{p_k(t)}{t-x_k}$, $k = n, n-1, \dots, 2$.

Dalje, neka je $S_{k-1} = S_k(x_k) = S(x_k, x_{k+1}, \ldots, x_n)$, $k = n, n-1, \ldots, 1$, $S_n = S$.
Nije teško proveriti sledeće osobine polinoma $p_k(t)$ i polja S_k:

$S = S_n \subseteq S_{n-1} \subseteq \cdots \subseteq S_1 \subseteq S_0 = K$.

$p_k(t) \in S_k(t)$, $\deg p_k(t) = k$, $p_k(x_k) = 0$ i
koeficijent uz t^k u $p_k(t)$ jednak je 1.

Primetimo da je $p_k(t)$ deljiv sa $(t - x_k)\cdots(t-x_n)$ jer $p_n(x_k) = 0, \ldots, p_n(x_n) = 0$,
pa odatle $p_k(t) \in S(x_{k+1}, \ldots, x_n)(t) = S_k(t)$.
Otuda $|S_{k-1} : S_k| \leq \deg p_k \leq k$, odakle je

$|K : S| = |S_0 : S_1| \cdot |S_1 : S_2| \cdots |S_{n-1} : S_n| \leq 1 \cdot 2 \cdots n = n!$, tj.

$|K : S| \leq n!$, pa $L = S$.

Odavde odmah nalazimo da je zapravo $|K : S| = n!$ i $|S_{k-1} : S_k| = k$.

Neka je $g(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ (dakle g je polinom). Ako je g simetričan onda, kako je $L = S$, za neki $q \in S$, $g = q\epsilon$, tj.

$g(x_1, \ldots, x_n) = q(\sigma_1, \ldots, \sigma_n)$ gde je $q(x_1, \ldots, x_n) \in F(x_1, \ldots, x_n)$.

Treba dokazati da je $q(x_1, \ldots, x_n)$ polinom, za sada imamo samo da je $q(x_1, \ldots, x_n)$ racionalan izraz. Neka je $g(x_1, \ldots, x_n)$ proizvoljan polinom, dakle ne mora biti simetričan. Prema prethodnom, $p_1(t) \in S(x_2, \ldots, x_n)(t) = S_1(t)$, $\deg p_1 = 1$ i $p_1(x_1) = 0$ i $S_0 = S_1(x_1)$, $|S_0 : S_1| = 1$, te $x_1 \in S_1$, tj. x_1 je polinom od $\sigma_1, \ldots, \sigma_n, x_2, \ldots, x_n$, preciznije, $x_1 = g_1(s_1, \ldots, s_n, x_2, \ldots, x_n)$, gde $g_1(y_1, \ldots, y_n, x_2, \ldots, x_n) \in F(y_1, \ldots, y_n, x_2, \ldots, x_n)$. Zamenimo x_1 sa $g_1(s_1, \ldots, s_n, x_2, \ldots, x_n)$ u $g(x_1, \ldots, x_n)$.
Slično nastavljamo dalje, pri čemu koristeći Kroneckerovu teoremu:
Kako je $p_2(x_2) = 0$, x_2^2 i viši stepeni od x_2 mogu se izraziti pomoću polinoma od $x_3, \ldots, x_n$ i $\sigma_1, \ldots, \sigma_n$ (taj polinom ima koeficijente u F).
Kako je $p_3(x_3) = 0$, x_3^3 i viši stepeni od x_3 mogu se ~~iz~~ izraziti pomoću polinoma (sa koeficijentima u F) od $x_4, \ldots, x_n$ i $\sigma_1, \ldots, \sigma_n$.
Vršeći supstituciju x_i sa ovim polinomima vidimo da se $g(x_1, \ldots, x_n)$ može izraziti kao polinom od x_i, σ_i tako da je u navedenom polinomu stepen $x_i \leq i-1$, tj.

$$(*) \qquad g(x_1, \ldots, x_n) = \sum_{\alpha} a_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}, \qquad \alpha_i \leq i-1, \quad a_\alpha \in S,$$

a_α su polinomi od $\sigma_1, \ldots, \sigma_n$.

Ovaj zapis polinoma g je jedinstven, tj. koeficijenti a_α su jedinstveno određeni s obzirom da je $|S_{i-1} : S_i| = i$ i prema 15.7.1°.
Specijalno, ako je $g(x_1,\dots,x_n)$ simetričan polinom, onda $g \in S$ i $g = g \cdot x_1^0 \cdots x_n^0$, te prema (*) i jedinstvenosti reprezentacije (*),
$g(x_1,\dots,x_n) = q_\alpha(\sigma_1,\dots,\sigma_n)$ za $\alpha_1 = \dots = \alpha_n = 0$, a_α ima koeficijente u $\mathbb{F}$, čime je teorema o simetričnim polinomima dokazana.
Primetimo da je (*) uopštenje teoreme o simetričnim polinomima i da važi za proizvoljne polinome promenljivih $x_1,\dots,x_n$

32.3. __Zadatak__ Dokazati da je prema oznakama prethodne teoreme

$$K = S(x_1 + x_2^2 + \dots + x_n^n).$$

32.4. __Zadatak__ Pretpostavimo oznake kao u 32.1. Dokazati da za $n,k \in N$ važi:

$$s_{n+k} + \sigma_1 s_{n+k-1} + \dots + \sigma_k s_n = 0.$$

32.5. __Zadatak__ Izraziti polinom 32.1.1° pomoću polinoma simetričnih funkcija $\sigma_1, \sigma_2, \sigma_3$.

32.6. __Zadatak__ Uz oznake kao u 32.1. dokazati

$$s_k = -\begin{vmatrix} \sigma_0 & 0 & 0 & \cdots & \sigma_1 \\ \sigma_1 & \sigma_0 & 0 & \cdots & 2\sigma_2 \\ \sigma_2 & \sigma_1 & \sigma_0 & \cdots & 3\sigma_3 \\ \vdots & & & & \\ \sigma_{k-1} & \sigma_{k-2} & & & k\sigma_k \end{vmatrix}$$

32.7. Diskriminanta polinoma $p(x) \in F[x]$ je
$D(p) = \prod_{i<j} (x_i - x_j)^2$, gde su $x_1,\dots,x_n$ koreni polinoma $p(x)$, $\deg p = n$.
Dokazati da je $D(p)$ simetrična funkcija i $D(p) = V(x_1,\dots,x_n)^2$ gde je $V(x_1,\dots,x_n)$ Vandermondova determinanta.
Odrediti $D(p)$ za $p(x) = x^3 + px + q$.

32.8. Funkcionalna jednačina $f(x) = f(a-x)$, $a \in F$, $\mathbb{F}$ je polje.
Dokazati da su sledeći uslovi ekvivalentni za $f(x) \in F[x]$:
a. $f(x) = f(a-x)$, b. postoji polinom $g(x) \in F[x]$ tako da je $f(x) = \frac{1}{2}(g(x) + g(a-x))$ ($\operatorname{kar} \mathbb{F} \neq 2$)
c. $\bigvee_{g \in F[x]} f(x) = g(x(a-x))$.

__Napomena__ posmatrati grupu $G = \{i, \theta_a\}$, $G < \operatorname{Aut} \mathbb{F}(x)$, i je identično preslikavanje, $\theta_a : f(x) \mapsto f(a-x)$, $f \in F(x)$, primeniti Artinovu teoremu.

32.9. Neka je $f \in C(R)$ (tj. neprekidna f-ja na $\mathbb{R}$). Dokazati

$$\bigwedge_{x \in R} f(x) = f(a-x) \quad \text{akko} \quad \bigvee_{g \in C(R)} f(x) = g(x(a-x))$$

__Nap.__ Primeniti Vajerštrasovu teoremu o aproksimaciji neprekidnih f-ja polinomima.

33. Konstrukcije lenjirom i šestarom

Neka je OA jedinična duž u kompleksnoj ravni $\mathbb{C}$ određena tačkama $O(0,0)$, $A(0,1)$. Tačka $M(x,y)\in \mathbb{C}$ je konstruktivna ako se može dobiti elementarnom konstrukcijom pomoću lenjira i šestara u konačno mnogo koraka polazeći od duži OA. Precizirajmo, konstruktivne tačke, duži, prave i kružnice uvode se:

A1. Tačke O, A su konstruktivne.

A2. Ako su B i C konstruktivne tačke i $B\neq C$, onda je prava (duž) određena tačkama B i C konstruktivna.

A3. Kružnica koja ima konstruktivan centar i konstruktivan poluprečnik je konstruktivna. A6. Presek konstruktivne prave i konst. kružnice je konst. tačka.

A4. Presek dve konstruktivne prave je konstruktivna tačka.

A5. Preseci dve konstruktivne kružnice su konstruktivne tačke.

Skup konstruktivnih tačaka $\mathcal{P}\subset\mathbb{C}$ naziva se Pitagorejskom ravni.

Ako je $M(x,y)\in\mathcal{P}$ tada se x, y nazivaju konstruktivnim realnim brojevima.

33.1. Zadatak Dokazati da je $\mathcal{P}$ prebrojiv skup.

Neposredno se proverava.

33.2. Teorema Neka je K_R skup konstruktivnih realnih brojeva. Tada

1° K_R je podpolje polja $\mathbb{R}$. 2° $\mathcal{P}$ je podpolje polja $\mathbb{C}$, 3° $K_R\subseteq\mathcal{P}\subseteq\mathbb{A}$, $\mathbb{A}$ je polje alg. brojeva.

Neka je $r\in K_R$ dobije elementarnom konstrukcijom u jednom ~~koraku~~, koji pomoću aksioma A1–A6 iz tačaka koje pripadaju polju $\mathbb{F}$. Tada je r rešenje sistema linearnih jednačina ili neke kvadratne jednačine, dakle $|\mathbb{F}(r):\mathbb{F}|\in\{1,2\}$.

Otuda

33.3. Ako je $r\in K_R$, tada za neki n $|\mathbb{Q}(r):\mathbb{Q}|=2^n$.

Dokaz Ako je $\mathbb{Q}=\mathbb{F}_0\subseteq\mathbb{F}_1\subseteq\dots\subseteq\mathbb{F}_m$ niz polja koja prati elementarnu konstrukciju broja $r\in\mathbb{F}_m$, tada.

$$|\mathbb{F}_m:\mathbb{Q}|=|\mathbb{F}_m:\mathbb{F}_{m-1}|\cdots|\mathbb{F}_1:\mathbb{F}_0| = 1\cdot2\cdot1\cdot2\cdot2\cdot1\cdots2=2^n.$$

33.4. Delski problemi

1° Problem kvadrature kruga: Konstruisati kvadrat koji ima površinu jednaku površini kruga poluprečnika 1.
Konstrukcija nije moguća: obzirom da je π transcedentan broj, te rešenje jednačine $x^2=\pi$ $(=\pi r^2)$ nije algebarski broj.

2° Problem udvajanja kocke: Konstruisati kocku dvostruko veće zapremine od jedinične kocke.
Konstrukcija nije moguća: Konstrukcija nije moguća obzirom da je $|\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}|=3\neq 2^n$ za $n\in\mathbb{N}$, $\sqrt[3]{2}$ je dužina ivice veće kocke $(x^3=2\cdot1^3)$.

3° Problem trisekcije ugla : Podeliti ugao na tri jednaka ugla.
Konstrukcija nije uvek moguća, na primer za $\alpha = 60°$. Ugao $\beta = 20°$ nije konstruktivan jer bi u tom slučaju i $\cos 20°$ bio konstruktivan (gledaj jedinični krug). Naime, kako je $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$, tada bi $\cos 20°$ zadovoljavao jednačinu $4x^3 - 3x - 1/2 = 0$. Polinom $4x^3 - 3x - 1/2$ je nesvodljiv nad $\mathbb{Q}$ (jer nema racionalnih korena), dakle
$|\mathbb{Q}(\cos 20°) : \mathbb{Q}| = 3 \neq 2^n,\ n \in \mathbb{N}^+$, tj. $\cos 20° \notin \mathcal{K}_R$.

33.5. O konstrukciji pravilnih poligona (Gauss). Konstrukcija pravilnog (regularnog) poligona sa n temena očigledno je ekvivalentna konstrukciji n-tih korena iz jedinice, tj. ε gde je ε primitivan koren jedinice, $\varepsilon^n = 1$, $\varepsilon = e^{\frac{2\pi i}{n}}$.

1° PP da je pravilan poligon sa n temena konstruktivan. Tada je prema prethodnom $|\mathbb{Q}(\varepsilon) : \mathbb{Q}| = 2^m$ za neki m. S druge strane, vidi odeljak 29, $|\mathbb{Q}(\varepsilon) : \mathbb{Q}| = \varphi(n) = p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1)(p_2 - 1)\cdots(p_k - 1)$.
Dakle, mora biti $p_1 = 2$ (ili $\alpha_1 = 1$) i $p_i - 1 = 2^{k_i}$, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ je primarna faktorizacija broja n.
Neka je $p \in$ Prost i $p = 2^k + 1$. Ako je $k = 2^s(2l+1)$, $l \neq 0$, onda $2^k + 1 = 2^{2^s(2l+1)} = (2^{2^s} + 1)(\cdots)$, tj. p nije prost. Dakle $l = 0$ i $k = 2^s$ tj. $p = 2^{2^s} + 1$, Fermaov prost broj (jedino poznati: 3, 5, 17, 257, $2^{2^5}+1$).
Dakle

Teorema Ako je pravilan poligon sa n temena konstruktivan, onda je n proizvod stepena dvojke i Fermaovih prostih brojeva.

Primer Pravilan sedmougao nije konstruktivan, jer $7 \neq 2^{2^n} + 1$ za $n \in \mathbb{N}$.

2° Važi i obrat: Ako je n proizvod dvojke i Fermaovih prostih brojeva, onda je pravilan poligon sa n temena konstruktivan.

Dokaz U ovom slučaju $|\mathbb{Q}(\varepsilon) : \mathbb{Q}| = \varphi(n) = 2^m$. S druge strane, vidi odeljak 29, $\mathrm{Aut}(\mathbb{Q}(\varepsilon) | \mathbb{Q}) = \Phi(n)$ i $\Phi(n)$ je Abelova grupa, dakle rešiva (prema teoremi o dekompoziciji konačnih Abelovih grupa na cikličke) i $\mathbb{Q}(\varepsilon)|\mathbb{Q}$ je Galoaova. Dakle postoji kompozicioni niz $\langle e \rangle = G_0 \leq G_1 \leq \cdots \leq G_m = \mathrm{Aut}(\mathbb{Q}(\varepsilon)|\mathbb{Q})$ tako da je $\mathrm{red}\, G_i = 2^i$, tj. $|G_{i+1} : G_i| = 2$. Neka su $E_i = \mathbb{Q}(\varepsilon)^{G_{m-i}}$. Tada $\mathbb{Q} = E_0 \leq E_1 \leq \cdots \leq E_m = \mathbb{Q}(\varepsilon)$ i $E_{i+1}|E_i$ je Galoaova ekstenzija, dakle $|E_i : E_{i-1}| = |G_{m+1-i} : G_{m-i}| = 2$, tj. $E_i | E_{i-1}$ je kvadratno proširenje (tj. $E_i = E_{i-1}(\sqrt{a})$, $a \in E_{i-1}$), pa kako je $E_0 = \mathbb{Q}$, to (indukcijom po i) $E_i \leq \mathcal{K}_R$, tj. $\varepsilon \in \mathcal{K}_R$.

33.6. Zadatak Dokazati da jednakokraki trougao, kod koga je krak $a = 3$, poluprečnik upisanog kruga $\varrho = 1$, nije konstruktivan.

1. Polja

Teorija polja predstavlja osnovu za teoriju algebarskih jednačina. Ispitivanje rešivosti neke algebraske jednačine pretpostavlja polje nad kojim se ta jednačina izučava. Na primer, za algebarsku jednačinu $x^2 - x + 1 = 0$ ne možemo reći ništa određeno o njenoj rešivosti dok ne izaberemo osnovno polje nad kojim je ta jednačina postavljena. U polju realnih brojeva ova jednačina nema rešenja, dok u polju kompleksnih brojeva ima rešenja. Otuda se teorija algebarskih jednačina svodi na izučavanje algebarskih polja. Glavno mesto u tome ima teorija Galua.

1.1 Definicija i osnovna svojstva polja

Polje je algebarska struktura u kojoj se mogu izvoditi osnovne racionalne operacije: sabiranje, oduzimanje, množenje i deljenje. U aksiomatskoj formulaciji, pored simbola konstanata $0, 1$ učestvuju jedino simboli operacija sabiranja i množenja, dakle jezik teorije polja je $L = \{+, \cdot, 0, 1\}$. Ostale operacije su izvedene, tj. mogu se definisati u okviru ove teorije.

1.1.1 Definicija *Algebarsko polje je svaka algebra vida* $\mathbf{F} = (F, +, \cdot, 0, 1)$ *gde su* $(F, +, 0)$ *i* $(F \backslash \{0\}, \cdot, 1)$ *Abelove grupe,* $\mathbf{F}$ *zadovoljava distributivni zakon i* $0 \neq 1$.

Dakle, svako polje $\mathbf{F}$ zadovoljava sledeće aksiome:

1.	$x + (y + z) = (x + y) + z$	asocijativnost sabiranja
2.	$x + y = y + x$	komutativnost sabiranja
3.	$x + 0 = x$	neutralni element sabiranja
4.	$\exists y(x + y = 0)$	suprotni element
5.	$x \cdot (y \cdot z) = (x \cdot y) \cdot z$	asocijativnost množenja
6.	$x \cdot y = y \cdot x$	komutativnost množenja
7.	$1 \cdot x = x$	neutralni element množenja
9.	$x \neq 0 \rightarrow \exists y(x \cdot y = 1)$	inverzni element
8.	$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$	distributivnost
10.	$0 \neq 1$	netrivijalnost polja

Primetimo da su aksiome polja zapravo univerzalna zatvorenja navedenih formula. Ovaj potpuni oblik aksioma dobija se vezivanjem slobodnih promenljivih u formuli stavljajući univerzalni kvantor ispred formule, Na primer, potpuni oblici Druge i Četvrte aksiome redom glase $\forall x \forall y(x+y=y+x)$, $\forall x \exists y(x+y=0)$. Univerzalni kvantori se u ovakvim situacijama (na početku predikatskih formula) dogovorno mogu izostaviti radi jednostavnije notacije, ali se ipak podrazumevaju.

1.1.2 Tvrđenje *U polju* **F** *važi:*

a. $\forall x \exists_1 y(x+y=0)$, **b.** $\forall x(x \neq 0 \Rightarrow \exists_1 y(x \cdot y=1))$.

Dokažimo, na primer, tvrđenje (**a**): Neka su y, y' takvi da je $x+y=0, x+y'=0$. Tada, prema aksiomama polja, važi sledeći niz jednakosti:

$$y'+(x+y)=y'+0,\ (y'+x)+y=y',\ (x+y')+y=y',\ 0+y=y',\ y=y',$$

čime je tvrđenje (**a**) dokazano. Svojstvo (**b**) se dokazuje na sličan način. □

Dakle, za svaki $x \in F$ postoji tačno jedan $y \in F$ tako da je $x+y=0$ i ako je $x \neq 0$ tačno jedno z tako da je $x \cdot z=1$. Otuda u **F** možemo uvesti dve nove operacije pomoću sledećih definicionih aksioma:

a. $y=-x \Leftrightarrow x+y=0$, **b.** $x \neq 0 \Rightarrow (y=x^{-1} \Leftrightarrow x \cdot y=1)$.

Za ovako uvedene opecije u polju **F** važi: $x+(-x)=0$, $x \neq 0 \Rightarrow x \cdot x^{-1}=1$. Obično se uzima da je 0^{-1} nedefinasana vrednost, ali po potrebi može se uzeti za 0^{-1} bilo koja vrednost iz F, na primer $0^{-1}=0$. Aksiome polja i dalje vrede!

1.1.3 Tvrđenje *U polju* **F** *važi:* **a.** $x \cdot 0=0=0 \cdot x$, **b.** $(-1) \cdot x=-x$ **c.** $x \cdot y=0 \Rightarrow (x=0 \vee y=0)$.

Dokažimo, na primer, tvrđenje (**a**): $a \cdot 0=a \cdot (0+0)=a \cdot 0+a \cdot 0$, odakle je $a \cdot 0=0$. □

Ako su $a, b \in F$ i $b \neq 0$, definišemo $a/b=a \cdot b^{-1}$. U tom slučaju za $c, d \in F$, $d \neq 0$, važi:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}.$$

Multiplikativnu grupu $(F \backslash \{0\}, \cdot, 1)$ polja **F** obeležavamo pomoću $\mathbf{F}^*$. Dakle, $\mathbf{F}^*=(F^*, \cdot, 1)$, gde $F^*=F \backslash \{0\}$.

U polju **F** definišemo stepenu funkciju x^n, $n \in N$ na sledeći način: $x^0=1$, $x^{n+1}=x^n \cdot x$. Ako je α negativan ceo broj, tj. $\alpha=-n$, $n \in N^+$, i ako je $x \neq 0$, onda uzimamo da je $x^\alpha=(x^{-1})^n$. Tada u **F** važe uobičajeni identiteti: **a.** $x^{m+n}=x^m \cdot x^n$, $(x^m)^n=x^{mn}$, $x \in F$, $m, n \in N$, **b.** $x^{m+n}=x^m \cdot x^n$, $(x^m)^n=x^{mn}$, $x \in F^*$, $m, n \in Z$, **c.** $(x+y)^n=\sum_{i=0}^n \binom{n}{i} x^i y^{n-i}$, $n \in N$.

1.2 Primeri polja

Sledeća polja su glavni primeri ovih algebraskih struktura:

a.	$\mathbf{Q}=(Q,+,\cdot,0,1)$,	polje racionalnih brojeva.
b.	$\mathbf{R}=(R,+,\cdot,0,1)$,	polje realnih brojeva.
c.	$\mathbf{C}=(C,+,\cdot,0,1)$,	polje kompleksnih brojeva.
d.	$\mathbf{Z}_p=(Z_p,+_p,\cdot_p,0,1)$,	polje ostataka po prostom modulu p.

Pretpostavljamo da je čitalac upoznat sa konstrukcijom polja $\mathbf{Q}, \mathbf{R}$ i $\mathbf{C}$ i dokazima da dobijene algebre zaista jesu polja. Razmotrimo poslednji primer. U ovom primeru $+_p$ i $\cdot_p$ su redom operacije sabiranja i množenja po prostom modulu p. Na primer, $2 +_5 4 = 1$, $2 \cdot_5 4 = 3$. Podsetimo se da je $x +_p y = \mathrm{rest}(x +_p y, p)$, $x \cdot_p y = \mathrm{rest}(xy, p)$, gde je $\rho_n(x) = \mathrm{rest}(x, n)$ funkcija ostatka:

$$r = \mathrm{rest}(x, n) \Leftrightarrow \exists q \in Z\,(x = qn + r \wedge 0 \leq r < n), \quad x \in Z, n \in N^+.$$

Primetimo da je $\mathrm{rest}(x, n) \in Z_n$, $n \in N^+$, gde je $Z_n = \{0, 1, \dots, n-1\}$ skup ostataka po modulu n. Za svako fiksno $n \in N^+$, preslikavnje $\mathrm{rest}(x, n)$ je homomorfizam iz prstena celih brojeva $\mathbf{Z}$ na prsten $\mathbf{Z}_n$ ostataka po modulu n, tj. $\rho_n : \mathbf{Z} \to \mathbf{Z}_n$, gde $\rho_n : x \mapsto \mathrm{rest}(x, n), x \in Z$.

1.2.1 Teorema *Neka je p prost broj. Tada je $\mathbf{Z}_p$ polje.*

Dokaz S obzirom da je $\mathbf{Z} = (Z, +, \cdot, 0, 1)$ je komutativan prsten sa jedinicom i $\rho_p : \mathbf{Z} \xrightarrow{\text{na}} \mathbf{Z}_p$, tj. $\mathbf{Z}_p$ je homomorfna slika prstena $\mathbf{Z}$, to je $\mathbf{Z}_p$ takodje komutativan prsten sa jedinicom. Dalje, neka je $a \in Z_p^*$. Tada $(a, p) = 1$, te prema Bezuovoj teoremi postoje $x, y \in Z$ takvi da je $ax + py = 1$. Otuda $\rho_p(ax + py) = \rho_p(1)$, tj. $a \cdot_p \rho_p(x) = 1$, odakle sledi da je $\rho_p(x) = a^{-1}$ u $\mathbf{Z}_p$. U $\mathbf{Z}_p$ važi $0 \neq 1$ jer je $p \geq 2$. □

1.2.2 Primer *Polje od četiri elementa.*
Neka je $F = \{0, 1, a, b\}$ i neka su operacije $+$ i $\cdot$ nad domenom F definisane tablicama:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

Direktnom proveroma aksioma utvrđujemo da je $\mathbf{F} = (F, +, \cdot, 0, 1)$ zaista polje. Primetimo da u $\mathbf{F}$ važi $2 \cdot x = 0$. Takođe, jednačina $x^2 + x + 1 = 0$ ovde ima rešenja a, b, dakle $x^2 + x + 1 = (x - a)(x - b)$. Najzad, primetimo da je $\mathbf{Z}_2 \subseteq \mathbf{F}$.

Sledećih nekoliko tvrđenja predstavljaju primenu teorije konačnih polja u elementarnoj teoriji brojeva.

1.2.3 Teorema *Neka je $\mathbf{F}$ polje i neka je $\mathbf{G}$ konačna podgrupa grupe $\mathbf{F}^*$. Tada je $\mathbf{G}$ ciklična grupa.*

Dokaz Podsetimo se sledećeg tvrđenja: ako su $\mathbf{C}_m$, $\mathbf{C}_n$ ciklične grupe redom redova m, n i $m, n \in N^+$ su uzajamno prosti, onda $\mathbf{C}_m \times \mathbf{C}_n \cong \mathbf{C}_{mn}$. Ovde koristimo sledeću varijantu ovog tvrđenja, i to za slučaj unutrašnjeg proizvoda podgrupa kod komutativnih grupa:

(1) *Ako je $\mathbf{G} = (G.\cdot, 1)$ konačna Abelova grupa i $H, K < \mathbf{G}$ su ciklične podgrupe uzajamno prostih redova, onda je podgrupa $HK < \mathbf{G}$ ciklična.*

Prema teoremi o razlaganju konačno-generisanih Abelovih grupa, $\mathbf{G}$ je unutrašnji proizvod cikličnih grupa. Ako u tom razlaganju sve ciklične podgrupe u parovima imaju uzajamno proste redove, onda uzastopnom primenom tvrđenja (1) nalazimo da je G ciklična. Otuda, ako $\mathbf{G}$ nije ciklična, onda u tom razlaganju postoje dve ciklične podgrupe, neka su to $H, K < G$, koje nisu uzajamno prostih redova. Dakle postoji prost broj p takav da $p|m, n$, gde je $m = \mathrm{red}H$ i $n = \mathrm{red}K$. Prema Košijevoj lemi, postoje $a \in H$ i $b \in K$ takvi da je $\mathrm{red}(a) = p = \mathrm{red}(b)$. Tada su $1, a, a^2, \ldots, a^{p-1}, b, b^2, \ldots, b^{p-1}$ različita rešenja algebarske jednačine $x^p - 1 = 0$ nad poljem $\mathbf{Z}_p$, dakle polinom $x^p - 1$ ima $1 + 2(p-1) > p$ različitih korena. To je kontradikcija činjenici da polinom stepena $p > 0$ nad nekim poljem ima najviše p različitih korena. Dakle $\mathbf{G}$ je ciklična grupa. □

1.2.4 Posledica Neka je p prost broj. Tada $\mathbf{Z}_p^* \cong \mathbf{C}_{p-1}$. □

1.2.5 Teorema *(Mala Fermaova teorema). Neka je p prost broj i neka je $a \in Z$, $(a, n) = 1$. Tada $a^{p-1} = 1 \bmod p$.*

Dokaz Prema Langranžeovoj teoremi za podgrupe, i kako je $\mathrm{red}(\mathbf{Z}_p^*) = p - 1$, za $x \neq 0$ u $\mathbf{Z}_p^*$, dakle i u $\mathbf{Z}_p$ važi $x^{p-1} = 1$. S obzirom da je $(a, p) = 1$, to $x = \rho_p(a) \neq 0$, prema tome $x^{p-1} = 1$ u $\mathbf{Z}_p$, gde je ρ_p funkcija ostatka po modulu p. S obzirom da je $\rho_p : \mathbf{Z} \to \mathbf{Z}_p$, imamo jednakosti $\rho_p(1) = 1 = x^{p-1} = \rho_p(a)^{p-1} = \rho_p(a^{p-1})$, odakle $\rho_p(1) = \rho_p(a^{p-1})$, tj. $a^{p-1} = 1 \bmod p$. □

1.2.6 Posledica Neka je p prost broj i a ceo broj. Tada $a^p = a \bmod p$.

Koristeći ideje kao u dokazu prethodne teoreme i algebarska svojstva funkcije ostatka, na sličan način se može dokazati ova čuventa teorema elementarne teorije brojeva.

1.2.7 Teorema *(Vilsonova teorema). Neka je p prost broj. Tada važi sledeća kongruencijska jednakost: $(p-1)! = -1 \bmod p$.*

Dokaz Kako smo videli u prethodnom dokazu, u $\mathbf{Z}_p$ važi identitet $x^{p-1} = 1$ za $x \in \{1, 2, \ldots, p-1\}$. Dakle, $1, 2, \ldots, p-1$ su (međusobno različiti) koreni polinoma $x^{p-1} - 1$. Kako je ovaj polinom stepena $p-1$ i pobrojanih korena takođe ima $p-1$, to onda u $\mathbf{Z}_p$ važi sledeća faktorizacija:

$$x^{p-1} - 1 = (x-1)(x-2) \cdot \ldots \cdot (x - (p-1)).$$

S obzirom da je $p = 0$ u $\mathbf{Z}_p$, dodeljujući vrednost p promenljivoj x u navedenom identitetu, dobijamo da u $\mathbf{Z}_p$ važi:

$$(p-1) \cdot_p (p-2) \cdot_p \ldots \cdot_p 1 = -1.$$

Otuda $\rho_p((p-1) \cdot (p-2) \cdot \ldots \cdot 1) = \rho_p(-1)$, odakle sledi Vilsonova teorema. □

U sledećem primeru pokazuje se kako se mogu primeniti Mala Fermaova teorema i Vilsonova teorema u rešavanju kvadratne jednačine $x^2 + 1 = 0$ u polju $\mathbf{Z}_p$, odnosno kongruencijeske jednačine $x^2 = -1 \bmod p$. Dokaz istovremeno daje rešenje ove jednačine u slučaju kada ono postoji.

1.2.8 Primer Neka je $p > 2$ prost broj. Tada jednačina $x^2 + 1 = 0$ ima rešenje u $\mathbf{Z}_p$ akko $p \in 4N + 1$.

Rešenje. S obzirom da je p neparan prost broj, to onda postoji $k \in N$ takav da je $p = 4k+1$ ili $p = 4k+3$. Neka je $m = (p-1)/2$. Sledeći račun izvodi se u $\mathbf{Z}_p$, tj. $+$ i $\cdot$ odnose se na operacije sabiranja i množenja po modulu p.

$\mathbf{1}^0$. Pretpostavimo da je $p = 4k+1$. Dakle m je paran i Prema Vilsonovoj teoremi važi

(1) $\quad 1 \cdot 2 \cdot \ldots \cdot (m-1)m(m+1)(m+2) \cdot \ldots \cdot (p-1) = -1.$

Kako je $p = 0$ u $\mathbf{Z}_p$, očigledno $m+i+1 = -(m-i)$, $i = 0, 1, \ldots, m-1$. Otuda, prema (1), nalazimo da je $-1 = (p-1)! = (-1)^m (m!)^2 = (m!)^2$, tj. $(m!)^2$ je rešenje jednačine $x^2+1 = 0$ u $\mathbf{Z}_p$. Prema tome $x^2+1 = 0$ ima rešenje u $\mathbf{Z}_p$ za p=1 mod 4.

$\mathbf{2}^0$. Pretpostavimo da je $p = 4k+3$. Dakle m je neparan. Pretpostavimo da je $b \in Z_p$ koren polinoma x^2+1, tj. da je $b^2 = -1$. Otuda i prema Maloj Fermaovoj teoremi sledi $1 = b^{p-1} = b^{2m} = (-1)^m = -1$, tj. $1 = -1$, što je kontradikcija pretpostavci da je $p > 2$. Prema tome jednačina $x^2+1 = 0$ nema rešenje u $\mathbf{Z}_p$ za p=3 mod 4.

1.3 Karakteristika polja

Prva i najjednostavnija klasifikacija polja je prema njihovoj karakteristici. U tom pogledu razlikovaćemo polja konačne i polja beskonačne karakteristike. U uvođenju ovog pojma koristćemo činjenicu da je svako polje $\mathbf{F} = (F, +_F, \cdot_F, 0_F, 1_F)$ modul nad prstenom celih brojeva $\mathbf{Z}$ ($\mathbf{F}$ je $\mathbf{Z}$-modul). Drugim rečima, može se uvesti spoljašnja operacija množenja između celih brojeva i elemenata polja $\mathbf{F}$: ako je $n \in N^+$ i $x \in F$, definišemo $n \cdot x = x + x + \ldots + x$ (n sabiraka), $(-n) \cdot x = -_F(n \cdot x)$, $0 \cdot x = 0_F$. Dakle, vrednosti ove spoljašnje operacije leže u polju $\mathbf{F}$. Tada za $m, n \in Z$ i $x, y \in F$ u strukturi $((F, +_F, 0_F), \mathbf{Z}, \cdot)$ važe sledeće jednakosti:

$$m(x +_F y) = (m \cdot x) +_F (m \cdot y), \quad (m+n) \cdot x = (m \cdot x) +_F (n \cdot x),$$
$$(mn)x = m \cdot (n \cdot x), \quad 1 \cdot x = x.$$

Primetiom da u ovoj definiciji i navedenim identitetima učestvuju dve operacije sabiranja (u $\mathbf{Z}$ i $\mathbf{F}$) i tri operacije množenja (u $\mathbf{Z}$, $\mathbf{F}$ i uvedena operacija spoljašnjeg množenja). Mada su to različite operacije, radi jednostavnije notacije u svim slučajevima koriste se iste oznake. Tako, umesto $x +_F y$ pisaćemo $x + y$, umesto $m \cdot x$ pisaćemo mx, i kontekst će određivati na koju se operaciju odnosi simbol $+$, odnosno $\cdot$ u izabranom algebarskom izrazu.

1.3.1 Definicija *Polje* $\mathbf{F}$ *je beskonačne karakteristike ako za svaki pozitivan prirodan broj* n *i sve* $x \in F^*$ *važi* $n \cdot x = 0$. *Polje* $\mathbf{F}$ *je konačne karakteristike ako ono nije beskonačne karakteristike.*

1.3.2 Primer 1^0. Brojevna polja $\mathbf{Q}$, $\mathbf{R}$ i $\mathbf{C}$ su beskonačne karakteristike. Za polje $\mathbf{F}$ beskonačne karakteristike takođe kažemo da je $\mathbf{F}$ *karakteristike* 0 i tada pišemo $k\mathbf{F} = 0$.
2^0. Polje $\mathbf{Z}_p$ ostataka po prostom modulu p je polje konačne karakteristike, s obzirom da u njemu važi $p \cdot x = 0$, $x \in Z_p$.

Neka je $\mathbf{F}$ polje konačne karakteristike. Dakle skup

$$S = \{n \in N^+ | \bigvee_{x \in F^*} n \cdot x = 0\}$$

je neprazan. Prema Principu najmanjeg broja za prirodne brojeve, S sadrži najmanji prirodan broj, neka je to p. Dakle za neki $a \in F^*$, $p \cdot a = 0$. Očigledno $p > 1$. Dokazaćemo da je p prost broj. Pretpostavimo suprotno, da je $p = km$, $1 < k, m$, $k, m \in N$. Otuda $(km) \cdot a = 0$, tj. $(k \cdot 1_F)(m \cdot a) = 0$, odakle sledi $k \cdot 1_F = 0$ ili $m \cdot a = 0$, suprotno izboru broja p. Dakle, p je prost broj. Ovaj broj nazivamo *karakteristikom* polja $\mathbf{F}$ i pišemo $k\mathbf{F} = p$.

Prema prethodnom, svakom polju $\mathbf{F}$ dodeljena je karkteristika $k\mathbf{F}$ i $k\mathbf{F} \in N$. Ako je $k\mathbf{F} = 0$ onda je $\mathbf{F}$ karakteristike 0 (beskonačne karakteristike). Ako je $k\mathbf{F} > 0$ onda je $k\mathbf{F}$ prost broj i tada kažemo da je $\mathbf{F}$ proste karakteristike. Prema tome, polje $\mathbf{Z}_p$ je proste karakeristike p. Ako je $\mathbf{F}$ proste karaketristike p, onda za sve $x \in F$ važi $p \cdot x = 0$. Zaista, pretpostavimo $k\mathbf{F} = p$. Tada za neki $a \in F^*$, $p \cdot a = 0$, odakle je $(p \cdot a) \cdot (a^{-1}x) = 0$, te $p \cdot x = 0$.

1.3.3 Teorema 1^0. *Polje* $\mathbf{F}$ *je karakteristike* 0 *akko* $\mathbf{F}$ *sadrži izomorfnu kopiju polja racionalnih brojeva* $\mathbf{Q}$.

2^0. Polje $\mathbf{F}$ je proste karakteristike p akko $\mathbf{F}$ sadrži izomorfnu kopiju polja $\mathbf{Z}_p$.

Dokaz 1^0. Neka je $k\mathbf{F}$ polje karakteristike 0 i neka je $h\colon Q \to F$ definisano sa $h(m/n) = (m \cdot 1_F) \cdot_F (n \cdot 1_F)^{-1}$, $m \in Z$, $n \in N^+$. Tada $h : \mathbf{Q} \xrightarrow[\text{1-1}]{} \mathbf{F}$, dakle $h\mathbf{Q} \subseteq \mathbf{F}$ i $h\mathbf{Q} \cong \mathbf{Q}$. Prema tome $\mathbf{F}$ zaista sadrži izomorfnu kopiju polja racionalnih brojeva, to je $h\mathbf{Q}$.
2^0. Neka je $\mathbf{F}$ proste karakteristike p i neka je $h\colon Z_p \to F$ definisano sa $h\colon x \mapsto x \cdot 1_F$, $x \in Z_p$. Tada $h : \mathbf{Z}_p \xrightarrow[\text{1-1}]{} \mathbf{F}$, dakle $h\mathbf{Z}_p \subseteq \mathbf{F}$ i $h\mathbf{Z}_p \cong \mathbf{Z}_p$. □

1.4 Homomorfizmi polja

Kao i kod drugih algebarskih struktura, pojam homomorfizma, a posebno automorfizma, ima ključno mesto u teoriji polja. Ispostaviće se da se analiza rešivosti algebraskih jednačina svodi na izučavanje strukture grupe automorfizama odgovarajućeg polja. Podsetimo se da su homomorfizmi preslikavanja između domena koja održavaju struktura polja.

1.4.1 Definicija *Neka su* $\mathbf{F}$ *i* $\mathbf{E}$ *polja. Preslikavanje* $h\colon F \to E$ *je homomorfizam polja* $\mathbf{F}$ *u polje* $\mathbf{E}$*, što zapisujemo* $h\colon \mathbf{F} \to \mathbf{E}$*, ako važi:*

$$h(x +_F y) = x +_E y,\ h(x \cdot_F y) = x \cdot_E y,\ h(0_F) = 0_E,\ h(1_F) = 1_F,\ x, y \in F.$$

Pojmovi utapanja (monomorfizma), homomorfizma *na* (epimorfizma), izomorfizma i autormorfizma kod polja definišu se na uobičajen način kao i kod ostalih algebarskih struktura. Naravno, važe osnovne teoreme kao i kod opštih algebri, na primer, da je funkcijski proizvod homomorfizama takođe homomorfizam, ili da skup svih automorfizama Aut$\mathbf{F}$ polja $\mathbf{F}$ čini grupu $\mathbf{AutF} = (\mathrm{Aut}\mathbf{F}, \circ, i_F)$ u odnosu na slaganje funkcija $\circ$. Sledeće tvrđenje odnosi se na važno i karakteristično svojstvo homomorfizama kod polja. Ono je posledica aksiome $0 \neq 1$ teorije polja i ukazuje na određenu rigidnost ovih struktura.

1.4.2 Teorema *Neka su* **F**, **E** *polja i neka je* $h\colon \mathbf{F} \to \mathbf{E}$. *Tada je* h *utapanje.*

Dokaz Neka je $a \in F$ i pretpostavimo da je $h(a) = 0$ i $a \neq 0$. Tada $1 = h(1) = h(aa^{-1}) = h(a)h(a^{-1}) = 0$, što je kontradikcija. Dakle, važi implikacija:

$$h(a) = 0 \Rightarrow a = 0,\ a \in F.$$

Otuda za $x, y \in F$ iz $hx = hy$ sledi $h(x - y) = 0$, tj. $x - y = 0$. Dakle h je $1-1$. □

S obzirom na prethodnu teoremu, prema kojoj se pojmovi homomorfizma u utapanja kod polja poklapaju, ubuduće ova dva pojma kod polja nećemo razlikovati.

1.4.3 Tvrđenje *Neka je* **Q** *potpolje polja* **F** *i polja* **K** *i neka je* $h\colon \mathbf{F} \to \mathbf{E}$. *Tada je* $h|Q = i_Q$. *Slično, ako je* p *prost broj i* $\mathbf{Z}_p$ *je potpolje polja* **F** *i polja* **K** *i ako je* $h\colon \mathbf{F} \to \mathbf{E}$, *tada* $h|Z_p = i_{Z_p}$.

Dokaz Zaista, ako je $n \in N^+$ onda: $h(n) = h(1+1+\ldots+1) = h(1)+h(1)+\ldots+h(1) = nh(1) = n$. Dalje, $0 = h0 = h(n+(-n)) = h(n)+h(-n)$, tj. $h(-n) = -h(n)$. Otuda za $m \in Z$, $h(m/n) = n^{-1}(h(n)h(m/n)) = n^{-1}(h(n(m/n)) = n^{-1}h(m) = m/n$. Dakle, $h|Q = i_Q$. Drugi deo tvrđenja dokazuje se na sličan način. □

Navodimo nekoliko primera homorfizama, odnosno automorfizama kod polja.

1.4.4 Primer 1^0. Neka je $Q(\sqrt{2}) = \{x + y\sqrt{2} \mid x, y \in Q\}$. Tada je algebra $\mathbf{Q}(\sqrt{2}) = (Q(\sqrt{2}), +, \cdot, 0, 1)$ polje i $\mathrm{Aut}\mathbf{Q}(\sqrt{2}) = \{\sigma, i\}$, $\sigma\colon x + y\sqrt{2} \mapsto x - y\sqrt{2}$, $x, y \in Q$, dok je i je identičko preslikavanje domena $Q(\sqrt{2})$. Zaista, neka je $h \in \mathrm{Aut}\mathbf{Q}(\sqrt{2})$, neka su $x, y \in Q$ i neka je $b = \sqrt{2}$. Tada, prema prethodnom tvrđenju, $hx = x, hy = y$ i $2 = h(2) = h(b^2) = h(b)^2$, tj. $h(b) \in \{\sqrt{2}, -\sqrt{2}\}$. Dakle,

$$\bigwedge_{x,y\in Q} h(x + y\sqrt{2}) = x + y\sqrt{2} \quad \text{ili} \quad \bigwedge_{x,y\in Q} h(x + y\sqrt{2}) = x - y\sqrt{2}.$$

pa $h \in \{i, \sigma\}$, tj. $\mathrm{Aut}\mathbf{Q}(\sqrt{2}) = \{i, \sigma\}$.
$\mathbf{2}^0$. Neka je p prost broj i neka je **F** polje karakteristike p. Ako je $\sigma_p\colon F \to F$ definisano pomoću $\sigma_p(x) = x^p$, $x \in F$, tada je σ_p utapanje polja **F** u samog sebe. Zaista, očigledno je $\sigma_p(0) = 0$, $\sigma_p(1) = 1$ i $\sigma_p(xy) = \sigma_p(x)\sigma_p(y)$. Dalje, kako je p prost broj, to je za sve $i \in N$, $1 \leq i < p$, $(i, p) = 1$, te je za isto i, $(i!, p) = 1$. Otuda, kako je $\binom{p}{i}$ ceo broj i $\binom{p}{i} = p(p-1)(p-2)\cdot\ldots\cdot(p-i+1)/i!$, sledi da p deli $(p-1)(p-2)\cdot\ldots\cdot(p-i+1)$, tj. p deli $\binom{p}{i}$, pa $\binom{p}{i} = 0$ u polju $\mathbf{Z}_p$. Ovim smo dokazali:

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

Dakle, σ_p je saglasan sa svim operacijam polja **F**, te je σ_p utapanje. Ako je polje **F** konačno, s obzirom da je σ_p $1-1$, prema Dirihleovom principu sledi da je σ_p presikavanje *na*, tj. u ovom slučaju $\sigma_p \in \mathrm{Aut}\mathbf{F}$. Ovaj automorfizam naziva se *Frobeniusovim automorfizmom.* Kompozicijom preslikavanja σ_p, nalazimo i ove homomorfizme (odnosno automorfizme u konačnom slučaju) polja **F**: $\sigma_{p^k}(x) = x^{p^k}$, $x \in F$, $k \in N$. Primetimo da ako je **F** konačno polje, tada je $\{\sigma_{p^k} \mid k \in N\}$ konačan skup, s obzirom da u tom slučaju preslikavanja iz F u F ima samo konačno mnogo.

Sledeći primer pokazuje da bez obzira što domen polja može biti veoma prostran skup, broj automorfizama tog polja može biti jako mali.

1.4.5 Primer Neka je $\mathbf{R}$ polje realnih brojeva. Tada je Aut$\mathbf{R} = \{i_R\}$. Dokaz ove činjenice razlaže se na nekoliko koraka. Neka je $h \in$ Aut$\mathbf{R}$.

1^0 Prema Tvrđenju 1.4.3 važi $h|Q = i_Q$.

2^0 h je monotono rastuće preslikavanje. Zaista, neka je $x < y$, $x, y \in R$. Tada postoji $b \in R\backslash\{0\}$ takav da je $y = x + b^2$, odakle $hy = h(x) + h(b^2) = h(x) + h(b)^2$. Kako je $h(b)^2 > 0$, sledi $hx < hy$.

3^0 $h \in C(R)$, tj. h je neprekidna funkcija na R: Neka je $\varepsilon \in R^+$, neka su $x, y \in R$ takvi da je $|x - y| < \varepsilon$ i neka je $q \in Q^+$ takav da je $|x - y| < q < \varepsilon$. Recimo da je $y < x$. Tada $y < x < y+q$, odakle prema 1^0 i 2^0 sledi $hy < hx+hq = hx+q$, pa $|hx-hy| < q < \varepsilon$. Slično razmatranje imamo i za $y < x$, te nalazimo: $\bigwedge_{\varepsilon\in R^+} \bigwedge_{x,y\in R}(|x - y| < \varepsilon \Rightarrow |hx - hy| < \varepsilon)$. Odavde sledi da je zaista $h \in C(R)$.

4^0 S obzirom da je Q gust u R, prema poznatoj činjenici iz realne analize imamo: Ako su $f, g \in C(R)$ i $f|Q = g|Q$ tada $f = g$.

5^0 Prema 3^0 h je neprekidna funkcija. Prema 1^0, $h|Q = i_R|Q$, odakle, prema 4^0 odmah sledi $h = i_R$.

1.5 Potpolja i raširenja polja

Videli smo da svako polje $\mathbf{F}$ sadrži potpolje $\mathbf{Q}$ (ako je $k\mathbf{F} = 0$) odnosno potpolje $\mathbf{Z}_p$ (ako je $\mathbf{F}$ proste karakteristike p). Drugim rečima svako polje je natpolje nekog od ova dva polja. U kasnijim lekcijama videćemo da je problem rešavanja algebarskih jednačina povezan sa izgradnjom ekstenizija baznog polja nad kojim je jednačina postavljena. Tada bazno polje postaje potpolje ekstenzije.

1.5.1 Definicija *Neka su* $\mathbf{F}$ *i* $\mathbf{E}$ *polja. Polje* $\mathbf{F}$ *je potpolje polja* $\mathbf{E}$, *odnosno* $\mathbf{E}$ *je raširenje (ekstenzija) polja* $\mathbf{F}$ *akko je* $\mathbf{F}$ *podalgebra polja* $\mathbf{E}$. *Činjenicu da je* $\mathbf{F}$ *potpolje polja* $\mathbf{E}$ *zapisujemo* $\mathbf{F} \subseteq \mathbf{E}$. *Dakle, ako je* $\mathbf{F} \subseteq \mathbf{E}$ *onda:* $0_\mathbf{F} = 0_\mathbf{E}$, $1_\mathbf{F} = 1_\mathbf{E}$, $x +_\mathbf{F} y = x +_\mathbf{E} y$, $x \cdot_\mathbf{F} y = x \cdot_\mathbf{E} y$, $x, y \in F$.

Na primer $\mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$. Svako potpolje polja $\mathbf{C}$ naziva se *brojevnim poljem.* Dakle $\mathbf{Q}(\sqrt{2})$ je primer brojevnog polja.

Primetimo da je svako potpolje jedinstveno određeno svojim domenom. Drugim rečima, ako su $\mathbf{F}, \mathbf{F}'$ potpolja polja $\mathbf{E}$ i $\mathbf{F}$ i $\mathbf{F}'$ imaju jednake domene, onda $\mathbf{F} = \mathbf{F}'$, tj. odgovarajuće operacije u ovim poljima se poklapaju. Otuda potpolje nekog polja identifikujemo sa njegovim domenom, pa umesto $\mathbf{F} \subseteq \mathbf{E}$ možemo pisati $F \subseteq \mathbf{E}$. Takođe, koristimo iste oznake za operacije i konstante u baznom polju $\mathbf{F}$ kao i u ekstenziji $\mathbf{E} \supseteq \mathbf{F}$.

Sledeća konstrukcija omogućava uvođenje stepena raširenja polja, važne numeričke konstante za dato raširenje $\mathbf{F} \subseteq \mathbf{E}$.

1.5.2 Teorema *Neka je* $\mathbf{F}$ *potpolje polja* $\mathbf{E}$. *Tada je* $\mathcal{E}_\mathbf{F} = ((E, +, 0), \mathbf{F}, \cdot)$ *vektorski prostor, gde se za proizvod skalara* $\alpha \in F$ *i vektora* $x \in E$ *uzima proizvod* $\alpha \cdot_\mathbf{E} x$.

Dokaz ove činjenice je očigledan i jednostavan, pa dokaz izostavljamo.

1.5.3 Definicija *Neka je* $\mathbf{E}$ *raširenje polja* $\mathbf{F}$*. Stepen (raširenja) polja* $\mathbf{E}$ *nad poljem* $\mathbf{F}$ *je dimenzija vektorskog prostora* $\mathcal{E}_{\mathbf{F}}$*. Za stepen raširenja polja* $\mathbf{E}$ *nad poljem* $\mathbf{F}$ *koristimo oznaku* $|\mathbf{E} : \mathbf{F}|$*. Dakle* $|\mathbf{E} : \mathbf{F}| = \dim \mathcal{E}_{\mathbf{F}}$*.*

1.5.4 Primer 1^0 $|\mathbf{Q}(\sqrt{2}) : \mathbf{Q}| = 2$; baza prostora $\mathcal{Q}(\sqrt{2})_{\mathbf{Q}}$ je $\{1, \sqrt{2}\}$.
2^0 $|\mathbf{C} : \mathbf{R}| = 2$; baza prostora $\mathcal{C}_{\mathbf{R}}$ je $\{1, i\}$.
3^0 $|\mathbf{R} : \mathbf{Q}| = \infty$. Da neka baza $\mathcal{H}$ prostora $\mathcal{R}_{\mathbf{Q}}$ postoji dokazuje se uz pomoć aksiome izbora i svaka takva baza naziva se *Hamelovom bazom.* Svaki vektor – realan broj – je konačna linearna kombinacija elemenata iz $\mathcal{H}$ sa skalarima u Q. Otuda, ako bi $\mathcal{H}$ bio prebrojiv skup, onda bi i tih linearnih kombinacija bilo prebrojivo mnogo, s obzirom da je Q prebrojiv. S druge strane R je neprebrojiv, dakle $\mathcal{H}$ je ne samo beskonačan već neprebrojiv skup. Može se dokazati da $\mathcal{H}$ ima moć kontinuuma, c.

1.5.5 Teorema *Neka su* $\mathbf{F}$*,* $\mathbf{E}$*,* $\mathbf{K}$ *polja takva da je* $\mathbf{F} \subseteq \mathbf{E} \subseteq \mathbf{K}$*. Tada važi jednakost* $|\mathbf{K} : \mathbf{F}| = |\mathbf{K} : \mathbf{E}| \cdot |\mathbf{E} : \mathbf{F}|$*.*

Dokaz Neka je $\langle a_i |\ i \in I\rangle$ baza prostora $\mathcal{E}_{\mathbf{F}}$ i neka je $\langle b_j |\ j \in J\rangle$ baza prostora $\mathcal{K}_{\mathbf{E}}$. Dakle, $|\mathbf{E} : \mathbf{F}| = \dim \mathcal{E}_{\mathbf{F}} = |I| = m$ i $|\mathbf{K} : \mathbf{E}| = \dim \mathcal{K}_{\mathbf{E}} = |J| = n$. Dokažimo da je $\langle a_i b_j |\ i \in I, j \in J\rangle$ baza prostora $\mathcal{K}_{\mathbf{F}}$:

1^0. Vektori $a_i b_j$, $i \in I$, $j \in J$, prostora $\mathcal{K}_{\mathbf{F}}$ su linearno nezavisni. Zaista, pretpostavimo da je neka konačna linearna kombiacija nekih od ovih vektora jednaka nuli, tj. da je za neke $r, s \in N^+$, različite $a_1, a_2, \ldots, a_r \in \{a_i |\ i \in I\}$, različite $b_1, b_2, \ldots, b_s \in \{b_j |\ j \in J\}$ i $\alpha_{ij} \in F$, $1 \le i \le r$, $1 \le j \le s$, $\sum_{i,j} \alpha_{ij} a_i b_j = 0$. Otuda

$$\sum_{j=1}^{s} \left(\sum_{i=1}^{r} \alpha_{ij} a_i \right) b_j = 0,$$

pa kako $\beta_j \in E$, $j = 1, 2, \ldots, s$, gde $\beta_j = \sum_{i=1}^{r} \alpha_{ij} a_i$, to su β_j skalari prostora $\mathcal{K}_{\mathbf{E}}$ i pritom $\sum_j \beta_j b_j = 0$. S obzirom da su $b_1, b_2, \ldots, b_s$ vektori iz baze istog prostora, dakle linearno nezavisni, sledi $\beta_1 = 0, \ldots, \beta_s = 0$. Otuda važe jednakosti $\sum_{i=1}^{r} \alpha_{ij} a_i = 0$, $j = 1, 2, \ldots, s$. S obzirom da su $a_1, a_2, \ldots, a_r$ bazni vektori prostora $\mathcal{E}_{\mathbf{F}}$ i da su α_{ij} skalari istog prostora, sledi $\alpha_{ij} = 0$, $i = 1, 2, \ldots, r$, $j = 1, 2, \ldots, s$, čime je tvrđenje 1^0 dokazano.

2^0. Vektori $a_i b_j$, $i \in I$, $j \in J$, prostora $\mathcal{K}_{\mathbf{F}}$ generišu ovaj prostor. Zaista, neka je $x \in K \backslash \{0\}$ proizvoljan vektor prostora $\mathcal{K}_{\mathbf{E}}$. S obzirom da je $\langle b_j |\ j \in J\rangle$ baza prostora $\mathcal{K}_{\mathbf{E}}$, to je za neki $s \in N^+$, neke $b_1, b_2, \ldots, b_s \in \{b_j |\ j \in J\}$ i neke skalare $e_1, e_2, \ldots, e_s \in E$, $x = \sum_{j=1}^{s} e_j b_j$. Kako su e_j vektori prostora $\mathcal{E}_{\mathbf{F}}$ i $\langle a_i |\ i \in I\rangle$ je baza istog prostora, postoji $r \in N^+$, postoje $\alpha_{ij} \in F$, $i = 1, 2, \ldots, r$, $j = 1, 2, \ldots, s$, i $a_1, a_2, \ldots, a_r \in \{a_i |\ i \in I\}$ takvi da je $e_j = \sum_{i=1}^{r} \alpha_{ij} a_i$, $j = 1, 2, \ldots, s$. Otuda $x = \sum_{j=1}^{s} e_j b_j = \sum_{ij} \alpha_{ij} a_i b_j$, čime je tvrđenje 2^0 dokazano.

Prema prethodnom $\langle a_i b_j |\ (j, i) \in J \times I\rangle$ je baza prostora $\mathcal{K}_{\mathbf{F}}$, tj.

$$|\mathbf{K} : \mathbf{F}| = \dim \mathcal{K}_{\mathbf{F}} = |J \times I| = |J| \cdot |I| = nm = |\mathbf{K} : \mathbf{E}| \cdot |\mathbf{E} : \mathbf{F}|. \qquad \square$$

Primetimo da u prethodnom dokazu nismo pretpostavljali da su stepeni raširenja konačni. Dakle, prethodno tvrđenje važi za proizvoljna raširenja polja, prema tome neki od kardinalnih brojeva $|\mathbf{K} : \mathbf{F}|$, $|\mathbf{K} : \mathbf{E}|$, $|\mathbf{E} : \mathbf{F}|$ mogu biti beskonačni. Naravno, $|\mathbf{K} : \mathbf{F}| = \infty$ akko $|\mathbf{K} : \mathbf{E}| = \infty$ ili $|\mathbf{E} : \mathbf{F}| = \infty$.

1.5.6 Posledica Neka je $\mathbf{F}_1 \subseteq \mathbf{F}_2 \subseteq \ldots \subseteq \mathbf{F}_n$, $n \in N^+$, lanac polja. Tada,

$$|\mathbf{F}_n : \mathbf{F}_1| = |\mathbf{F}_n : \mathbf{F}_{n-1}| \cdot |\mathbf{F}_{n-1} : \mathbf{F}_{n-2}| \cdot \ldots \cdot |\mathbf{F}_2 : \mathbf{F}_1|.$$ □

1.5.7 Primer Neka je $\mathbf{R}$ polje realnih i neka je $\mathbf{C}$ polje kompleksnih brojeva. Raširenje $\mathbf{R} \subseteq \mathbf{C}$ ne sadrži međupolje, tj. ako je $\mathbf{R} \subseteq \mathbf{E} \subseteq \mathbf{C}$, onda

$$2 = |\mathbf{C} : \mathbf{R}| = |\mathbf{C} : \mathbf{E}| \cdot |\mathbf{E} : \mathbf{R}|,$$

odakle $|\mathbf{C} : \mathbf{E}| = 1$ i tada $\mathbf{E} = \mathbf{C}$, ili $|\mathbf{E} : \mathbf{R}| = 1$ i tada $\mathbf{E} = \mathbf{R}$. Primetimo da slično tvrđenje ne važi za grupno raširenje $(R, +, 0) \subseteq (C, +, 0)$. Na primer, za skup celih brojeva Z i $\mathbf{A} = (R + iZ, +, 0)$ važi $(R, +, 0) \subseteq \mathbf{A} \subseteq (C, +, 0)$, $\mathbf{A} \neq (R, +, 0)$, $(C, +, 0)$.

Sledeće tvrđenje pokazuje koji su prirodni brojevi mogući kardinalni brojevi konačnih polja.

1.5.8 Teorema *Neka je* $\mathbf{E}$ *konačno polje. Tada za neki prost broj* p *i* $n \in N^+$ *važi* $|E| = p^n$.

Dokaz Neka je $\mathbf{E}$ konačno polje. Ono je karakteristike p za neki prost broj p, inače bi sadržalo potpolje racionalnih brojeva koje je beskonačno. Dakle $\mathbf{E}$ je vektorski prostor nad $\mathbf{Z}_p$. S obzirom da je $\mathbf{E}$ konačno, to je vektorski prostor $\mathcal{E}_{\mathbf{Z}_p}$ konačno-dimenzionalan, recimo dimenzije $n \in N^+$. Tada je $\mathcal{E}_{\mathbf{Z}_p}$ izomorfan vektorskom prostoru n-torki elemenata iz Z_p sa skalarima u $\mathbf{Z}_p$, odakle sledi $(E, +, 0) \cong (Z_p^n, +, \mathbf{0})$, te $|E| = |Z_p^n| = |Z_p|^n = p^n$. □

Zadaci

1.1 Neka je p prost broj. Dokazati da u polju $\mathbf{Z}_p$ važe identiteti

a. $\binom{p-1}{k} = (-1)^k$, $k \in Z_p$. **b.** $\sum_{i=1}^{p-1} \frac{1}{i} = 0$. **c.** $\sum_{i=1}^{p-1} \frac{1}{i^2} = 0$, $p > 3$.

1.2 Dokazati da važi obrat Vilsonove teoreme:
Ako je $n \in N^+$ i $(n-1)! = -1 \bmod n$, tada je n prost broj.

1.3 Navesti primer polja: **a.** od devet elemenata, **b.** od 8 elemenata.

1.4 Neka je $\mathbf{F}$ polje. Dokazati: Ako je $\mathbf{F}^*$ ciklična grupa, onda je $\mathbf{F}$ konačno.

1.5 Jednačine u kojima se kao nepoznate javljaju funkcije nad nekim domenom nazivaju se *funkcionalnim jednačinama.* Funkcionalna jednačina (f. j.)

(C) $f(x + y) = f(x) + f(y)$,

sa nepoznatom funkcijom f nad poljem realnih brojeva R naziva se *Košijevom funkcionalnom jednačinom.* Dokazati:

a. Ako je f neprekidno rešenje f. j. (C), tada postoji $a \in R$ tako da je $f(x) = ax$.
b. Postoji rešenje f. j. (C) koje nije neprekidno.
c*. Funkcija $f\colon R \to R$ je *ograničena* ako važi: $\bigvee_{M \in R^+} \bigwedge_{x \in R} |f(x)| \leq M$. Ograničena rešneja f. j. (C) su neprekidna na R.
d*. Lebeg-merljiva rešenja f. j. (C) su neprekidna na R.

1.6 Dokazati da postoje operacije $+'$, $\cdot'$ na skupu racionalnih brojeva Q takve da je $(Q(\sqrt{2}), +, \cdot, 0, 1) \cong (Q, +', \cdot', 0, 1)$.

1.7 Neka je $\mathbf{E}$ polje, $\sigma \in \mathrm{Aut}\mathbf{E}$ i neka je $F = \{x \in E \mid \sigma(x) = x\}$. Dokazati:
a. F je potpolje polja $\mathbf{E}$.
b. Ako je σ drugog reda, tj. $\sigma^2 = i_F$, $\sigma \neq i_F$, onda $|\mathbf{E} : \mathbf{F}| = 2$.

1.8 Dokazati: ako je $\mathbf{F}$ konačno polje, onda postoji prost broj p i $n \in N$ tako da za sve $x \in F$ važi $x^{p^n} = x$.

1.9 Dokazati da polja $\mathbf{Q}(\sqrt{2})$ i $\mathbf{Q}(\sqrt{3})$ nisu izomorfna.

1.10* Dokazati da postoje neizomorfna polja $\mathbf{F}$ i $\mathbf{E}$ takva da je $F^* \cong \mathbf{E}^*$ i $(F, +, 0) \cong (E, +, 0)$.

1.11 *Telo* je svaka algebarska struktura $\mathbf{K} = (K, +, \cdot, 0, 1)$ koja zadovoljava sve aksiome polja osim eventualno komutativnog zakona $xy = yx$. Ukoliko u nekom telu nije zadovoljen zakon $xy = yx$, onda se ono naziva i *nekomutativnim poljem.*
a. Neka je $\mathbf{K}_8 = (K_8, \cdot, 1)$, $K_8 = \{1, -1, i, -i, j, -j, k, -k\}$, grupa kvaterniona i neka je $\mathbf{K} = (K, +, \cdot, 0, 1)$, $K = \{x + yi + zj + uk \mid x, y, z, u \in R\}$ grupni prsten nad poljem realnih brojeva $\mathbf{R}$. Dokazati da je $\mathbf{K}$ nekomutativno polje (*telo kvaterniona*).
b. Dokazati da je svako konačno telo polje.

1.12 Neka je $\mathbf{R}$ polje realnih brojeva. Dokazati da potpolja polja $\mathbf{R}$ ima neprebrojivo mnogo, preciznije 2^c, $c = 2^{\aleph_0}$ je moć kontinuuma.

1.13* Neka je $\mathbf{F}$ prebrojivo polje i neka je $\mathcal{F}$ skup svih potpolja polja $\mathbf{F}$. Dokazati da je $|\mathcal{F}| \leq \aleph_0$ ili $|\mathcal{F}| = 2^{\aleph_0}$.

2. Polinomi

Ključno mesto u teoriji algebarskih polja imaju polinomi, posebna vrsta algebarskih izraza. O tome svedoče stariji i možemo reći, alternativni nazivi za teoriju polja: teorija jednačina, odnosno teorija polinoma. Postoje razne teorije u kojima su predmet izučavanja polinomi. Pojam algebarske jednačine ima glavno mesto u svim ovim teorijama.

1.1 Definicija polinoma

Neka je $\mathbf{F}$ polje i neka su $a_0, a_1, a_2, \ldots, a_n$, $n \in N$, elementi domena F. Izraze oblika

$$f(x) = f_0 + f_1x + f_2x^2 + \ldots + f_nx^n$$

uobičajeno nazivamo *polinomima* promenljive x nad poljem $\mathbf{F}$. Mada na prvi pogled izgleda da su ovim opisom polinomi definisani kao specijalni algebarski izrazi teorije polja, sa stanovišta savremene algebre ova definicija nije sasvim korektna. Naime, ako je $f(x)$ zaista algebarski izraz, onda je $f(x)$ term nekog algebarskog jezika L. S obzirom da u navedenom opisu ušestvuju elementi polja $\mathbf{F}$ koji nisu simboli jezika $L = \{+, \cdot, 0, 1\}$ teorije polja, postavlja se pitanje nad kojim se to algebarskim jezikom polinomi zapravo uvode. Ovaj problem notacije, odnosno korektnog definisanja polinoma može se razrešiti na nekoliko načina.

2.1.1 Prva definicija polinoma. Kao što je pomenuto, jezik teorije polja je $L = \{+, \cdot, 0, 1\}$. Tada je svako polje $\mathbf{F} = (F, +_{\mathbf{F}}, \cdot_{\mathbf{F}}, 0_{\mathbf{F}}, 1_{\mathbf{F}})$ jedna interpretacija ovog jezika. Radi jednostavnije notacije ispuštamo indek $_{\mathbf{F}}$ u zapisima operacija i konstanata strukture $\mathbf{F}$, pa otuda imamo iste oznake, na primer, za operaciju sabiranja u polju $\mathbf{F}$ i *simbol* operacije sabiranja jezika L. Dalje, uvedimo za svaki $a \in F$ novi simbol konstante $\underline{a}$. Ovaj novi znak nazivamo *imenom* elementa a. Neka je za domen F, $L_F = \{\underline{a} \mid a \in F\}$. Tada, polinome promenljive X nad poljem $\mathbf{F}$ definišemo kao algebarske izraze (terme) vida

$$a(x) = \underline{a}_0 + \underline{a}_1x + \underline{a}_2x^2 + \ldots + \underline{a}_nx^n, \quad a_0, a_1, \ldots, a_n \in F$$

Simbole $\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_n$ nazivamo koeficijentima polinoma $a(x)$. Radi jednostavnije notacije, i kada to kontekst dozvoljava, donju crtu u simbolu $\underline{a}_i$ ispuštamo.

Tako dolazimo do uobičajenog načina zapisivanja polinoma. Polinom $a(x)$ takođe zapisujemo $a(x) = \sum_{i=0}^{n} a_i x^i$. Ako je $a_n \neq 0$ kažemo da je $a(x)$ stepena n, i tu činjenicu zapisujemo pomoću $\deg a(x) = n$. Ako je $n = 0$ i $a_0 = 0$ (nula polinom), onda uzimamo da je $\deg a(x) = -1$. Za polinome važi sledeći

2.1.2 *Princip identiteta.* Neka su $f, g \in F[x]$, $f(x) = \sum_{i=0}^{m} f_i x^i$, $g(x) = \sum_{i=0}^{n} g_i x^i$. Tada, $f = g$ akko $m = \deg f = \deg g = n$ i za sve $0 \leq i \leq n$, $f_i = g_i$.

Skup svih polinoma promenljive x obeležavamo sa $F[x]$, dakle (N je skup prirodnih brojeva):

$$\begin{aligned} F[x] &= \{f(x) \mid f(x) \text{ je polinom promenljive } x \text{ nad } F\} \\ &= \{\sum_{i=0}^{n} a_i x^i \mid a_1, a_2, \ldots, a_n \in F, n \in N\}. \end{aligned}$$

Na sličan način se uvode polinomi nad ma kojim komutativnim prstenom $\mathbf{P}$. U tom slučaju, koeficijanti se biraju u domenu P prstena $\mathbf{P}$, dok $P[x]$ označava polinome nad $\mathbf{P}$. Na primer, $Z[x]$ označava polinome sa celobrojnim koeficijentima. Primetimo da u definiciji polinoma učestvuje zapravo samo domen strukture (polja, prstena), dakle u principu možemo govoriti o polinomima nad bilo kojim skupom. Polinome više promenljivih uvodimo na sledeći način.

2.1.3 Definicija *Skup polinoma $P[x_1, x_2, \ldots, x_n]$ promenljivih $x_1, x_2, \ldots, x_n$ nad poljem (komutativnim prstenom) $\mathbf{F}$ je skup izraza vida*

$$f(x_1, x_2, \ldots, x_n) = \sum_{\alpha \in S} a_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}, \quad \alpha = \langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle$$

gde $S \subseteq N^n$ i S je konačan, $a_\alpha \in F$, $\alpha \in S$.

U definiciji prstena polinoma nad poljem $\mathbf{F}$ značajnu ulogu imaju sledeći polinomi: *nula* polinom, $\mathbf{0} = \underline{0}$, i *jedinični* polinom, $\mathbf{1} = \underline{1}$.

Sabiranje $+$ i množenje $\cdot$ polinoma promenljive x definiše se na uobičajen način. Neka su $f, g \in F[x]$, $f(x) = \sum_{i=0}^{m} f_i x^i$, $g(x) = \sum_{j=0}^{n} g_j x^j$ i neka je $k = \max(m, n)$. Tada

$$(f+g)(x) = f(x) + g(x) = \sum_{s=0}^{k} \underline{a}_s x^s, \text{ gde } a_s = f_s +_{\mathbf{F}} g_s, \ 0 \leq s \leq k,$$

eventualno dopunjujući nizove koeficijenata polinoma f i g nulama. Proizvod polinoma f i g definišemo ovako:

$$(f \cdot g)(x) = \sum_{s=0}^{m+n} \underline{b}_s x^s, \text{ gde } b_s = \sum_{i+j=s} f_i g_j x^s, \ 0 \leq s \leq m+n.$$

2.1.4 Tvrđenje *Neka je $\mathbf{F}$ polje i neka su $f, g \in F[x]$. Tada:*

1^0 $\deg(f+g) \leq \max\{\deg f, \deg g\}$ 2^0 $f, g \neq 0 \Rightarrow \deg(f \cdot g) = \deg f + \deg g$. $\square$

Pomoću ovako uvedenih operacija sa polinomima promenljive x nad poljem $\mathbf{F}$, možemo uvesti algebrasku strukturu $\mathbf{F}[x] = (F[x], +, \cdot, \mathbf{0}, \mathbf{1})$.

2.1.5 Teorema *Neka je* $\mathbf{F}$ *polje. Tada je* $\mathbf{F}[x]$ *domen, tj. komutativan prsten sa jedinicom bez delitelja nule.*

Dokaz Dokažimo, na primer, da $\mathbf{F}[x]$ zadovoljava asocijativni zakon za množenje. Neka su za proizvoljan polinom $u \in F[x]$, $u_i = (u)_i$ koeficijenti polinoma u, tj. $u(x) = \sum_{i=0}^{n} (u)_i x^i$ i neka su $f, g, h \in F[x]$. Tada, koristeći činjenicu da važe odgovarajući zakoni u polju $\mathbf{F}$, za $0 \leq s \leq p+q+r$, $p = \deg f$, $q = \deg g$, $r = \deg h$, nalazimo

$$\begin{aligned}((fg)h)_s &= \sum_{t+k=s} (fg)_t h_k = \sum_{t+k=s} \sum_{i+j=t} (f_i g_j) h_k = \sum_{i+j+k=s} f_i g_j h_k \\ &= \sum_{i+t=s} \sum_{j+k=t} f_i (g_j h_k) = \sum_{i+t=s} f_i (gh)_t = (f(gh))_s\end{aligned}$$

odakle sledi $(fg)h = f(gh)$. Na sličan ili jednostavniji način dokazuje se da u $\mathbf{F}[x]$ važe ostale aksiome komutativnih prstena.

Pretpostavimo da je $f, g \neq 0$. Tada $f_p \neq 0$ i $g_q \neq 0$, odakle sledi $(fg)_{p+q} \neq 0$, tj. $fg \neq \mathbf{0}$. Dakle, $\mathbf{F}[x]$ je domen. $\square$