Univerzitet u Beogradu – Matematički fakultet

Predavanja iz
Algebre II

Žarko Mijajlović

Beograd 2001

ALGEBARSKA POLJA

OKTOBAR 2000

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 $x+y=0$, Odavde 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 $x^\alpha \overset{\text{def}}{=} (x^{-1})^n$. 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. $(x+y)^n=\sum_{i=0}^{n}\binom{n}{i}x^iy^{n-i}$, $n\in N$.

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 $x +_p y = \mathrm{rest}(x+y, p)$, $x \cdot_p y = \mathrm{rest}(xy, p)$, gde je $\mathrm{rest}(x, n)$ funkcija ostatka:
$$r = \mathrm{rest}(x, n) \overset{\text{def}}{\Longleftrightarrow} \exists q\,(x = qn + r \wedge 0 \le r < n), \quad r, x \in Z, n \in N^+.$$
Primetimo da je $\mathrm{rest}(x, n) \in \{0, 1, \ldots, n-1\}$, $n \in N^+$. 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 $g_p(x) = \mathrm{rest}(x, p)$ $g_p : \mathbb{Z} \xrightarrow{na} \mathbb{Z}_p$. 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 $g_p(ax + py) = g_p(1)$, tj. $a \cdot_p g_p(x) = 1$, te je $g_p(x) = a^{-1}$ 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

$\cdot$	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, $\mathbb{Z}_2 \subseteq \mathbb{F}$.

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

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

<u>2.3. 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 $1, a, \ldots, a^{p-1}, b, b^2, \ldots, b^{p-1}$ 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 $n^p = n \pmod p$, $n \in N$, $p \in Prost$.

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. $n^p = n \pmod p$. ∎

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

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

Dokaz Kako u $\mathbb{Z}_p$ važi $x^{p-1} = 1$ za $x \in \{1, \ldots, p-1\}$ to x^{p-1} Kako je x^{p-1}, su $1, 2, \ldots, p-1$ koreni polinoma $x^{p-1} - 1$. Kako je x^{p-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 $\mathbb{Z}_p$, $p = 0$, uvrštavajući $x = p$, 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 $(p-1)! = -1 \pmod p$.

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

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

2.10 Zadatak Neka je $\mathbb{F}$ polje. Dokazati: ako je $\mathbb{F}^*$ ciklična grupa, tada je $\mathbb{F}$ konačno (tj. $\mathbb{F}^* \ncong (\mathbb{Z}, +, 0)$).

3. <u>Karakteristika polja</u>. Polje F je <u>beskonačne karakteristike</u> akko za sve $n \in N^+$ sve $x \in F\setminus\{0\}$, $n \cdot x \neq 0$. Gde,
$n \cdot x \overset{\text{def}}{=} \underbrace{x + x + \dots + x}_{n}$. 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.
Neka je $\mathbb{F}$ polje konačne karakteristike. Dakle,
$S = \{n \in N^+ \mid \text{postoji } x \in F\setminus\{0\},\ n \cdot x = 0\}$ 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 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° $h(x+y) = (x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \cdots + \binom{p}{p-1} x y^{p-1} + y^p$.

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

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. Otuda, 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. $\mathrm{Aut}\, \mathbb{F} = (\mathrm{Aut}\, \mathbb{F}, \circ, i_F)$ 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 $\mathbb{F}$ akko 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. $x + y = x +' y$, $x \cdot y = x \cdot' y$, $x, y \in F$). Otuda podpolje identifikujemo sa njegovim domenom i koristimo iste oznake za operacije kao u ekstenziji.

5.3 Primer Postoji polje $\mathbb{F} = (\mathbb{Q}, +', \cdot', 0', 1')$, $\mathbb{Q}$ je skup racionalnih brojeva, tako da je $\mathbb{F} \cong \mathbb{Q}(\sqrt{2})$.
Dokaz Skupovi $\mathbb{Q}$ i $\mathbb{Q}(\sqrt{2})$ su prebrojivi, dakle postoji $f : \mathbb{Q} \xrightarrow[1-1]{na} \mathbb{Q}(\sqrt{2})$. Neka su $0' = f^{-1}(0)$, $1' = f^{-1}(1)$ i za $x, y \in \mathbb{Q}$
$x +' y = f^{-1}(f(x) + f(y))$, $x \cdot' y = f^{-1}(f(x) \cdot f(y))$. Tada je
$\mathbb{F} = (\mathbb{Q}, +', \cdot', 0', 1')$ 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 $\mathbb{Q}' = (\mathbb{Q}, +', \cdot', 0, 1)$ 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. <u>Teorema</u> Neka su $\mathbb{F}, \mathbb{E}, \mathbb{K}$ polja takva da je $\mathbb{F} \leq \mathbb{E} \leq \mathbb{K}$. Tada $|\mathbb{K}:\mathbb{F}| = |\mathbb{K}:\mathbb{E}| \cdot |\mathbb{E}:\mathbb{F}|$.

<u>Dokaz</u> 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,

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

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

<u>Napomena</u> 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 <u>Zadatak</u> Neka je dat lanac polja
$\mathbb{F}_1 \leq \mathbb{F}_2 \leq \cdots \leq \mathbb{F}_n$. 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. <u>Zadatak</u> Neka je $\mathbb{E}$ polje i $\sigma \in \mathrm{Aut}\,\mathbb{E}$ 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. <u>Teorema</u> Neka je $\mathbb{F}$ konačno polje. Tada za neki prost broj p i $n \in \mathbb{N}^+$, $|\mathbb{F}| = p^n$

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

5.14.[**] <u>Zadatak</u> 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

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

$S \subseteq N$ 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 otuda 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 6.8a.
Dalje, $\mathbb{O} = \langle 0, 0, 0, \dots \rangle$ i Sanaobe, 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:

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

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

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 imena 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 produžiti funkciju $f^F : F \to F$, uzimajući da je za $a \in F$, $f^F(a) \equiv$ vrednost polinoma f za $x=a$ u polju $\mathbb{F}$.

Pojmovi polinoma i polinomnih 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. Odade 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 $\mathbb{F}[x] \subseteq \mathbb{F}(x)$.
Utapanje je: $f \mapsto f/1$, $f \in F[x]$.

7.2. Na sličan način se definiše polje racionalnih izraza promenljivih $x_1, \ldots, x_n$ (ili induktivno: $F(x_1, \ldots, x_n) = (F(x_1, \ldots, x_{n-1}))(x_n)$).
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

(*) $$f = g \cdot q + r, \quad r = 0 \text{ ili } 0 \le \deg r < \deg g.$$

<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 $S = \{ n \in N^+ \mid n = \deg l,\ l \in R \}$ 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 $0 \le \deg r$ jer $0 \notin S$). PP suprotno, da je $m = \deg r \ge \deg g = n$. Tada za neki (dobro izabran) $c \in F$ i

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

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

Ovim je dokazana egzistencija razlaganja (*).

Dokažimo jedinost: Neka je

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

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

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 $f'(x) \overset{def}{=} a_1 + 2a_2 x + \dots + n \cdot a_n x^{n-1}$.
Umesto f' pišemo i Df. Ako je $c \in F$, onda $Dc = 0$.

9.1. Teorema $(x-a)^2 \mid f(x) \Leftrightarrow f(a) = 0, f'(a) = 0$.
($\Rightarrow$) 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 $f \in F[x]$, $\deg f \geq 1$, 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 $f \in F[x]$, $\deg f \geq 1$, 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. <u>Primer</u> 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 $a = \cos 20°$ jeste koren ovog polinoma.

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

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

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 <u>Teorema</u> Član r_n iz Euklidovog algoritma je polinom najvećeg stepena koji deli f i g.
<u>Dokaz</u> 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 monični polinom, to je $h \in (f, g)$, gde $h_n = 1$ (h je <u>moničan</u> polinom)

10.5. <u>Bezuova teorema za polinome</u> 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° $(f, g) = 1 \Rightarrow (f^m, g^n) = 1$

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

4° Neka je $M_n(F)$ skup kvadratnih matrica nad poljem $\mathbb{F}$. Tada je $(M_n(\mathbb{F}), +, \cdot, 0, E_n)$ 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 $(N, +, \cdot, 0, 1) \leq \mathbb{Z}$ ali $(N, +, \cdot, 0, 1)$ nije prsten ~~ukoliko~~.

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>.

U budućem 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 <u>domen</u>.
Prsten $\mathbb{Z}_6$ ima delitelje nule.

11.5. <u>Jedinica</u> prstena $\mathbb{P}$ je svaki invertibilan element $c \in P$. Dakle $c \in P$ je jedinica ako postoji $d \in P$ takav da je $c \cdot d = 1$. Skup svih jedinica prstena $\mathbb{P}$ označavamo sa $J(\mathbb{P})$.

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

11.7. <u>Zadatak</u> Dokazati da je $\mathbb{J}(\mathbb{Z}_n) = \mathbf{\Phi}_n$, gde je $\mathbf{\Phi}_n = (\Phi_n, \cdot_n, 1)$ 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. <u>Ideali prstena</u>

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

12.1. <u>Primer</u> 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 pp $I \neq \{0\}$. 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 $I = n\mathbb{Z}$.

2° Neka je $f \in F[x]$, 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 $f_1, \dots, f_n \in F[x]$. Tada je $I = \{f_1 g_1 + \dots + f_n g_n \mid g_1, \dots, g_n \in F[x]\}$ ideal prstena $\mathbb{F}[x]$.

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

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

Primer: 1° Ako je $p \in Prost$, tada je $p\mathbb{Z}$ maksimalan ideal prstena $\mathbb{Z}$. Zaista iz $p\mathbb{Z} \subsetneq n\mathbb{Z}$ 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 $\mathbb{F}[x]$, $(f) \subsetneq I$ i neka je $g \in I \setminus (f)$ polinom najmanjeg stepena. Prema lemi o ostatku za polinome postoje $q, r \in F[x]$ takvi da je $f = qg + r$, $\deg r < \deg f$ (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. <u>Zadatak</u> Neka je I ideal prstena $\mathbb{P}$ i $x \in P$. Dokazati da je $J = \langle I \cup \{x\} \rangle = \{i + xp \mid p \in P\}$ najmanji ideal prstena $\mathbb{P}$ koji sadrži I kao podskup i x.

13 <u>Količnički prsteni</u>

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 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 $x \sim z$.

Saglasnost sa operacijom $+$: 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 $x+x' \sim y+y'$.

Saglasnost sa operacijom $\cdot$: 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 $x/\sim + y/\sim \stackrel{\text{def}}{=} (x+y)/\sim$, $x/\sim \cdot y/\sim = (xy)/\sim$, $\mathbb{0} = \{x \in P \mid x \sim 0\} = I$

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

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

13.2. Teorema Neka je I maksimalni ideal prstena $\mathbb{P}$.

Tada je $\mathbb{P}/I$ polje.

Dokaz 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.

$1\!\!1 = 0 + (I+p)\cdot(I+x)$. Prema tome, inverzan za $I+x$ je $I+p$. ■ (19)

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 koreno 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 $\mathbb{E} \supseteq \mathbb{F}$ takvo 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 $\mathbb{F}[x]/\mathbb{F}$. ∎

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 $a_0 = I+1$, $a_1 = I+x, \dots, a_{n-1} = I + x^{n-1}$, $I = (g)$, 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 $k(g) = 0$, 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 $r_0 a_0 + r_1 a_1 + \dots + r_{n-1} a_{n-1} = 0$. Primetimo da je $0 = (g)\ (= I)$ i sobzirom 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 $I + (r_0 + r_1 x + \dots + r_{n-1} x^{n-1}) = I$.

Otuda sledi $r_0 + r_1 x + \dots + r_{n-1} x^{n-1} \in I = (g)$, 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. $a \in \mathbb{K}$ 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 $a \in \mathbb{K}$ algebarski element nad $\mathbb{F}$.

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

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 $1, \alpha, \alpha^2, \alpha^3, \dots$ je linearno zavisan niz vektora pa za neke $a_0, a_1, \dots, a_n \in F$, $a_n \neq 0$, $n \geq 1$, $a_0 \cdot 1 + a_1 \cdot \alpha + \dots + a_n \cdot \alpha^n = 0$. Dakle, α je koren polinoma $p(x) = a_0 + a_1 x + \dots + a_n x^n$, $p \in \mathbb{F}[x]$. ▨

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

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

<u>Dokaz</u> 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
$p = qm + r$, $\deg r < \deg m$, $q, r \in F[x]$.
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 $\mathbb{F} \subseteq \mathbb{F}(\alpha) \subseteq \mathbb{K}$, gde je $F(\alpha)$ polje (vrednosti) racionalnih izraza za $x = \alpha$. Dakle, elementi $F(\alpha)$ su oblika $p(\alpha)/q(\alpha)$, gde su $p, q \in F[x]$, $q(\alpha) \neq 0$.

(a) $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ su linearno nezavisni vektori prostora $(F(\alpha), +, \circ)$ 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 $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$.
Dakle, $p(\alpha) = 0$ gde $p(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ 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 $\alpha^n = -m_0 - m_1\alpha - \cdots - m_{n-1}\alpha^{n-1}$
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 $u \in F[\alpha]$, $u \neq 0$, $u = u_0 + u_1\alpha + \cdots + u_{n-1}\alpha^{n-1}$.
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) sledi $F(\alpha) = \mathcal{L}_F(1, \alpha, \dots, \alpha^{n-1})$, pa $|F(\alpha) : F| \leq n$, čime je dokazano 4°.

15.7 <u>Posledice</u> 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 algebarski nad $\mathbb{K}$, tada $|\mathbb{F}(\alpha) : \mathbb{F}| < \infty$.

15.8 <u>Primer</u> 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° $1 + x + \cdots + x^{p-1}$, $p \in Prost$, 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.* <u>Zadatak</u> 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. <u>Zadatak</u>. a) Dokazati da je $a = 1 + \sqrt{2} + \sqrt{3}$ algebarski broj. b) Odrediti $|\mathbb{Q}(a) : \mathbb{Q}|$

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

16. <u>Kronekerova teorema</u> ("originalan" 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 $K = \{a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1} \mid a_0, \ldots, a_{n-1} \in F\}$ 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 $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. 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 $\varphi : \mathbb{F}[x] \longrightarrow K$, $\varphi(f) = \mathrm{rest}(f, p)(\xi)$, $f \in F[x]$.
Dokazujemo da je φ epimorfizam prstena $\mathbb{F}[x]$ na $\mathbb{K}$.

a) Očigledno je φ preslikavanje na.

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

Neka su $r_1, r_2 \in F[x]$ prema Lemi o ostatku takvi da je
$$f = q_1 p + r_1,\ \deg r_1 < \deg p\ ;\quad g = q_2 p + r_2,\ \deg r_2 < p.$$

Tada $r_1(\xi) = \varphi(f)$ i $r_2(\xi) = \varphi(g)$. Dalje,
$$f+g = (q_1+q_2)p + r_1 + r_2 \quad \text{i} \quad \deg(r_1+r_2) < \deg p,$$
te prema Lemi o ostatku, delu koji se odnosi na jedinstvenost ostatka, sledi $r_1(\xi) +_p r_2(\xi) = \mathrm{rest}(f+g, p)(\xi) = \varphi(f+g)$, dakle
$$\varphi(f+g) = r_1(\xi) +_p r_2(\xi) = \varphi(f) +_p \varphi(g).$$

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

Dokaz je sličan dokazu u (b). Uz iste oznake kao u (b) i uzimajući $r = \mathrm{rest}(r_1 r_2, p)$, 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, $r = \mathrm{rest}(fg, p)$, pa
$$\varphi(fg) = \mathrm{rest}(fg, p)(\xi) = r(\xi) = \mathrm{rest}(r_1 r_2, p)(\xi)$$
$$= r_1(\xi) \cdot_p r_2(\xi) = \varphi(f) \cdot_p \varphi(g).$$

Dakle, $\varphi : \mathbb{F}[x] \xrightarrow{na} \mathbb{K}$, 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) $\mathrm{rest}(x, p) = x$ jer $\deg p \geq 2$, pa $\varphi(x) = \xi$.

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

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

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

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

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 $(r(x), p(x)) = 1$. Otuda 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 $+_F, \cdot_F$ polja $\mathbb{F}$ i operacije $+_K, \cdot_K$ 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 $\mathbb{K}', \mathbb{K}''$ 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 $\mathbb{F}$).

$$\begin{array}{ccc} \mathbb{F}(\alpha)=\mathbb{K}' & \xrightarrow{\sigma} & K''=\mathbb{F}(\beta) \\ \rotatebox{90}{$\supseteq$} & & \rotatebox{90}{$\subseteq$} \\ & \mathbb{F} & \end{array}$$

– 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 $f(x)\in\mathbb{F}[x]$, $\deg f\leq n-1$.

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, $\mathbb{K}=\mathbb{F}(\xi)=\{f(\xi)\mid f(x)\in\mathbb{F}[x], \deg f\leq n-1\}$, 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 $f_i' = \sigma(f_i)$, $i \leq n$. 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 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 $\mathbb{K} = \mathbb{F}(\alpha)$, $\mathbb{K}' = \mathbb{F}'(\beta)$.

$$\begin{array}{ccc} \mathbb{F}(\alpha) = \mathbb{K} & \overset{\approx}{\underset{\theta}{\dashrightarrow}} & \mathbb{K}' = \mathbb{F}'(\beta) \\ \cup\!| & & \cup\!| \\ \mathbb{F} & \xrightarrow[\sigma]{\approx} & \mathbb{F}' \end{array}$$

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 $f \in \mathbb{F}[x]$, $\deg f \geq 1$.

$\mathbb{E}$ 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 $f \in \mathbb{F}[x]$, $\deg f \geq 1$. 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. induktivna hipoteza i neka je $\deg f = n \geq 2$. 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 $\mathbb{E} = \mathbb{F}(a_1, \ldots, a_n)$ i svaki a_{i+1} je algebarski nad $\mathbb{F}(a_1, \ldots, a_i)$, $0 \le i < n$, pa $|\mathbb{E} : \mathbb{F}| = |\mathbb{F}(a_1, \ldots, a_n) : \mathbb{F}(a_1, \ldots, a_{n-1})| \cdots |\mathbb{F}(a_1) : \mathbb{F}| < \infty$, 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 $\mathbb{F}(a_1, \ldots, a_n)$ korensko polje polinoma $p(x)$. Zaista:

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

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

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

Ali prema Teoremi 15.6.3° takođe
$\mathbb{F}(a_1, \ldots, a_n) = \{ f^{\mathbb{E}}(a_1, \ldots, a_n) \mid f(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]\}$.

17.5. __Zadatak__ 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. __Zadatak__ 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.* __Zadatak__ 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.

Lema 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 $p(b)=0$.

Dokaz 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 sve korene polinoma f, dakle $\beta \in E$. Prema tome možemo uzeti $b=\beta$. ∎

Teorema (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 $\theta|\mathbb{F} = i_F$.

Dokaz Prema dokazu Teoreme 17.2, možemo uzeti da je $\mathbb{E} = \mathbb{F}(a_1,\dots,a_n)$ 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

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

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

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. <u>Primer</u> Neka je p prost broj i $n \in N^+$. 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 $\mathbb{Z}_p \subseteq \mathbb{E}$.

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 $\mathbb{E}$, 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 $H = E$.

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

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 $p \in Prost$, $n \in N^+$ nad poljem $\mathbb{Z}_p$.

17.11. <u>Zadatak</u> Neka je p prost broj. Dokazati da postoji beskonačno polje karakteristike p.

18. Polje algebarskih brojeva.

Element $a \in \mathbb{C}$ je algebarski broj ako je a koren nekog polinoma $f \in \mathbb{Q}[X]$, $f \neq 0$. Skup algebarskih brojeva je
$A = \{a \in \mathbb{C} \mid a \text{ je algebarski broj}\}$.
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 $\mathbb{F} \leq \mathbb{E} \leq \mathbb{K}$ 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 $\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$ u K, $\alpha_0, \ldots, \alpha_n \in E$. Dakle, β je algebarski element nad $\mathbb{F}(\alpha_0, \ldots, \alpha_n) \subseteq \mathbb{E}$, pa prema Teoremi 15.6

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

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

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

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

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

Dalje, $|\mathbb{F}(\alpha_0, \ldots, \alpha_n, \beta) : \mathbb{F}| = |\mathbb{F}(\alpha_0, \ldots, \alpha_n, \beta) : \mathbb{F}(\alpha_0, \ldots, \alpha_n)| \cdot |\mathbb{F}(\alpha_0, \ldots, \alpha_n) : \mathbb{F}| < \infty$

te je $\mathbb{F}(\alpha_0, \ldots, \alpha_n, \beta)$ alg. raširenje polja $\mathbb{F}$. Kako je $\beta \in \mathbb{F}(\alpha_0, \ldots, \alpha_n, \beta)$ to je onda β algebarski nad $\mathbb{F}$. ∎

Iz dokaza prethodne leme vidimo da važi

18.2. Tvrđenje Neka je $\mathbb{F} \subseteq \mathbb{E}$ i neka su $\alpha_0, \ldots, \alpha_n \in \mathbb{E}$ algebarski nad $\mathbb{F}$. Tada je $\mathbb{F}(\alpha_0, \ldots, \alpha_n) \subseteq \mathbb{E}$ 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. $A \cap \mathbb{R}$ je takođe podpolje polja kompleksnih brojeva $\mathbb{C}$.
$A \cap \mathbb{R}$ je polje realnih algebarskih brojeva.

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

19. **Separabilnost** $\deg f > 0$

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

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

Dokaz 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. **Napomena** 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 **Teorema** Neka je $f \in \mathbb{F}[x]$, $\deg f \geq 1$, nesvodljiv. Tada je f separabilan akko $f' \neq 0$.

Dokaz $(\Rightarrow)$ 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. **Posledica** 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 $\alpha \in \mathbb{E}$ 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 $\alpha \in \mathbb{E}$ 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 $m(p)$ je minimalni polinom za $\alpha \in \mathbb{E}$ 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 $\alpha \in \mathbb{E}$. 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 $\varkappa \in E$ tako da je $\mathbb{E} = \mathbb{F}(\varkappa)$, tada kažemo da je $\mathbb{E}$ <u>prosto proširenje</u> polja $\mathbb{F}$. U tom slučaju je $\varkappa$ 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. $\mathbb{E}^* = \langle \varkappa \rangle$ za neki $\varkappa \in E^*$. Tada $\mathbb{E} = \mathbb{F}(\varkappa)$.
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, $\mathbb{E} = \mathbb{F}(\alpha_1, \dots, \alpha_n) = \mathbb{F}(\alpha_1, \dots, \alpha_{n-2}, \varkappa_1) = \mathbb{F}(\alpha_1, \dots, \alpha_{n-4}, \varkappa_2) = \dots = \mathbb{F}(\varkappa)$.
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. Posledica 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 $\mathbb{F}(\alpha_1, \dots, \alpha_n) = \mathbb{F}(\varkappa)$.

Napomena 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. Zadatak 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. Teorema (F. Gauss) Polje kompleksnih brojeva je algebarski zatvoreno polje.

20.2. Lanci polja 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. Z. 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. Zadatak 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 **Teorema** Polje algebarskih brojeva $\mathbb{A}$ je algebarski zatvoreno.

Dokaz Neka je $f \in \mathbb{A}[x]$, $\deg f \geq 1$ i neka je $\alpha \in C$ koren polinoma f u polju kompleksnih brojeva $\mathbb{C}$. Dalje, za neke $a_0, a_1, \ldots, a_n \in A$ $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ i s obzirom da su $a_0, \ldots, a_n$ algebarski nad Q to je $Q(a_0, \ldots, a_n)$ algebarsko raširenje polja $\mathbb{Q}$. α je algebarski nad $Q(a_0, \ldots, a_n)$, dakle $Q(a_0, \ldots, a_n, \alpha)$ je algebarsko raširenje polja $Q(a_0, \ldots, a_n)$. Prema Lemi 18.1, tada je $Q(a_0, \ldots, a_n, \alpha)$ algebarsko raširenje polja Q, pa kako je $\alpha \in Q(a_0, \ldots, a_n, \alpha)$, to je α algebarski nad $\mathbb{Q}$, tj. $\alpha \in A$. ∎

20.6. **Posledica** 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. **Teorema** 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.

Dokaz Neka je $\mathbb{F}$ prebrojivo polje. Tada je $\mathbb{F}[x]$ prebrojiv skup, tj:

(1) $\mathbb{F}[x] = \{p_0, p_1, \ldots\}$.

Dakle i $\mathcal{F} = \{f \in \mathbb{F}[x] \mid \deg f \geq 1\}$ je prebrojiv, tj:

(2) $\mathcal{F} = \{f_0, f_1, \ldots\}$.

Konstruišemo niz polja $\mathbb{F}_0 = \mathbb{F}, \mathbb{F}_1, \mathbb{F}_2, \ldots$ 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 $\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \cdots$, 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 $\mathbb{F}_{n+1}$, dakle i u $\mathbb{E}_1$ s obzirom da je $\mathbb{F}_{n+1} \subseteq \mathbb{E}_1$.

Dalje, konstruišemo niz polja $F = \mathbb{E}_0 \subseteq \mathbb{E}_1 \subseteq \mathbb{E}_2 \subseteq \cdots$ 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 $\mathbb{E}_n$, $n \in N$, $n > 2$. 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 $f \in \mathbb{E}[x]$, $\deg f \geq 1$, $f = f_0 + f_1 x + \cdots + f_n x^n$. Tada za neke k_i, osim n, $f_i \in \mathbb{E}_{k_i}$ 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 poređati u niz

$$f_0, f_1, \ldots, f_\alpha, \ldots, \quad \alpha < \kappa, \quad \kappa = card(F), \quad \alpha \text{ je ordinalni broj.}$$

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 $T =$ 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 $T' =$ 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.

$\blacksquare$

20.9. Polje $\mathbb{E}$ je <u>algebarsko zatvorenje</u> polja $\mathbb{F}$ ako je

1° $\mathbb{F} \leq \mathbb{E}$

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 <u>Teorema</u> Svako polje $\mathbb{F}$ ima algebarsko zatvorenje.

<u>Dokaz</u> Prema Teoremi 20.7. postoji algebarski zatvoreno polje $\mathbb{K} \geq \mathbb{F}$. Neka je $E = \{ \alpha \in K \mid \alpha \text{ je algebarski nad } \mathbb{F} \}$. Dokažemo da je $\mathbb{E}$ algebarsko zatvorenje polja $\mathbb{F}$. Primetimo najpre da je

1° $\mathbb{F} \leq \mathbb{E}$

2° $\mathbb{E}$ je algebarsko raširenje polja $\mathbb{F}$.

3° Dokaz da je $\mathbb{E}$ algebarski zatvoreno izvodi se na isti način kao i dokaz da je $\mathbb{A}$ algebarski zatvoreno: Neka je $f \in E[x]$, $\deg f \geq 1$, i neka je $\alpha \in K$ takav da je $f^{K}(\alpha) = 0$. Dalje, neka je $f(x) = a_0 + a_1 x + \dots + a_n x^n$. Tada $a_0, \dots, a_n \in E$ i

$\mathbb{F}(a_0, \dots, a_n)$ je algebarsko raširenje polja $\mathbb{F}$ i

$\mathbb{F}(a_0, \dots, a_n, \alpha)$ je algebarsko raširenje polja $\mathbb{F}(a_0, \dots, a_n)$, dakle

$\mathbb{F}(a_0, \dots, a_n, \alpha)$ 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. <u>Zadatak</u> Neka je $\overline{\mathbb{F}}$ algebarsko zatvorenje polja $\mathbb{F}$. Ako je $\mathbb{F} \leq \mathbb{K} \leq \overline{\mathbb{F}}$, tada je $\overline{\mathbb{F}}$ algebarsko zatvorenje polja $\mathbb{K}$.

20.12. <u>Zadatak</u> Ako je $\mathbb{F}$ beskonačno polje tada, tada $|\overline{F}| = |F|$.

20.13. <u>Zadatak</u> Svako algebarski zatvoreno polje je beskonačno.

20.14. <u>Zadatak</u> Ako je $\mathbb{R} \leq \mathbb{K}$ i $|\mathbb{K} : \mathbb{R}| = 2$, tada je $\mathbb{K}$ algebarski zatvoreno.

20.15. <u>Zadatak</u> 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. <u>Teorema</u> 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 $\theta \restriction \mathbb{F} = \sigma$.

$$\begin{array}{ccc} \mathbb{K} & \overset{\theta}{\dashrightarrow} & \mathbb{K}' \\ \cup\!\mathrm{I} & & \cup\!\mathrm{I} \\ \mathbb{F} & \xrightarrow{\sigma} & \mathbb{F}' \end{array}$$

$\leftarrow$ komutativan dijagram

<u>Dokaz</u> Dokaz ćemo sprovesti u slučaju prebrojivog polja $\mathbb{F}$.
Tada je, naravno, i polje $\mathbb{F}'$ prebrojivo.
Neka $p_1, p_2, \ldots$ su polinomi promenljive x, $\deg p_i \geq 1$, nad poljem $\mathbb{F}$
i neka su $p_1', p_2', \ldots$, korespondentni polinomi nad $\mathbb{F}'$! Tada
je $p_1', p_2', \ldots$ tačno niz polinoma nad $\mathbb{F}'$ stepena ≥ 1.
Konstruišemo lanac polja i izomorfizama tako da sledeći beskonačan dijagram komutira:

$$\begin{array}{cccccccccccccc}
\mathbb{F} = \mathbb{F}_0 & \subseteq & \mathbb{F}_1 & \subseteq & \mathbb{F}_2 & \subseteq \cdots & \subseteq & \bigcup_n \mathbb{F}_n & = \mathbb{E}_1 & \subseteq & \mathbb{E}_2 & \subseteq \cdots & \subseteq \bigcup_n \mathbb{E}_n = \mathbb{H} & \subseteq \mathbb{K} \\
\sigma = \sigma_0 \downarrow & & \sigma_1 \downarrow & & \sigma_2 \downarrow & & & \downarrow \theta_1 & \downarrow \theta_1 & & \downarrow \theta_2 & & \downarrow \theta & \downarrow \theta \\
\mathbb{F}' = \mathbb{F}_0' & \subseteq & \mathbb{F}_1' & \subseteq & \mathbb{F}_2' & \subseteq \cdots & \subseteq & \bigcup_n \mathbb{F}_n' & = \mathbb{E}_1' & \subseteq & \mathbb{E}_2' & \subseteq \cdots & \subseteq \bigcup_n \mathbb{E}_n' = \mathbb{H}' & \subseteq \mathbb{K}'
\end{array}$$

Ako je $\{\alpha \in \mathbb{K} \mid \alpha \text{ je koren polin. } p_1 \text{ u } \mathbb{K}\} = \{\alpha_1, \ldots, \alpha_m\}$ i $\mathbb{F}_1 = \mathbb{F}_0(\alpha_1, \ldots, \alpha_m)$, 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) <u>postoji</u> $\sigma_1 : \mathbb{F}_1 \cong \mathbb{F}_1'$, $\sigma_1 \restriction \mathbb{F}_0 = \sigma_0$.
Ako je $\{\alpha \in \mathbb{K} \mid \alpha \text{ je koren polin. } p_2 \text{ u } \mathbb{K}\} = \{\beta_1, \ldots, \beta_l\}$ i $\mathbb{F}_2 = \mathbb{F}_1(\beta_1, \ldots, \beta_l)$ 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 $n \in N$, nalazimo lance polja $\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \ldots$, $\mathbb{F}' = \mathbb{F}_0' \subseteq \mathbb{F}_1' \subseteq \ldots$ 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 $\mathbb{F}_0 = \mathbb{E}_0 \subseteq \mathbb{E}_1 \subseteq \mathbb{E}_2 \subseteq \ldots$, $\mathbb{F}_0' = \mathbb{E}_0' \subseteq \mathbb{E}_1' \subseteq \mathbb{E}_2' \subseteq \ldots$ 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 $n \in N$, $n \geq 2$.

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 $\mathbb{F}_n$ algebarsko raširenje polja $\mathbb{F}$, dakle i $\mathbb{F}_n'$ je algebarsko raširenje polja $\mathbb{F}'$.

Lema 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 $\alpha \in E$, 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. Posledica $\overline{\mathbb{Q}} \cong \mathbb{A}$, $\overline{\mathbb{R}} \cong \mathbb{C}$

$\overline{\mathbb{Q}}$ je neko alg. zatv. polja $\mathbb{Q}$ i $\overline{\mathbb{R}}$ je alg. zatv. polja $\mathbb{R}$

20.18. Zadatak Neka su $\mathbb{K}$ i $\mathbb{K}'$ alg. zatvorenja polja $\mathbb{F}$. Tada postoji $\theta : \mathbb{K} \cong \mathbb{K}'$ tako da je $\theta \restriction F = i_F$.

$$\begin{tikzcd} \mathbb{K} \arrow[rr, "\theta", "\cong"'] & & \mathbb{K}' \\ & \mathbb{F} \arrow[ul, phantom, "\supseteq"] \arrow[ur, phantom, "\subseteq"] & \end{tikzcd}$$

20.19. Zadatak. Neka je $\mathbb{K}$ alg. zatvorenje polja $\mathbb{F}$ i neka je $\mathbb{E} \supseteq \mathbb{F}$ alg. zatvoreno polje. Tada postoji $\theta : \mathbb{K} \xrightarrow[1-1]{} \mathbb{E}$.

$$\begin{tikzcd} \mathbb{K} \arrow[rr, "\theta"] & & \mathbb{E} \\ & \mathbb{F} \arrow[ul, phantom, "\supseteq"] \arrow[ur, phantom, "\subseteq"] & \end{tikzcd}$$

20.20. Zadatak 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. $\lambda | \mathbb{F} = \theta$).

Dokaz Dokaz izvodimo primenom Zornove leme primenom na parcijalno uređen skup $(\mathcal{F}, \subseteq)$, gde je

$$\begin{tikzcd} \mathbb{L} \arrow[r, dashed, "\lambda"] & \mathbb{K} \\ \mathbb{F} \arrow[u, phantom, "\subseteq" rotate=90] \arrow[r, "\theta"] & \mathbb{E} \arrow[u, phantom, "\subseteq" rotate=90] \end{tikzcd}$$

$$\mathcal{F} = \{ \mu \mid \theta \subseteq \mu, \text{ za neko međupolje } \mathbb{F} \subseteq \mathbb{L}' \subseteq \mathbb{L},\ \mu : \mathbb{L}' \to \mathbb{K} \}$$

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 $\mathbb{F} \subseteq L'$ i takođe $\lambda : \mathbb{L}' \to \mathbb{K}$, $\theta \subseteq \lambda$. Dokazujemo 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 $\mathbb{L}'(a) \subseteq \mathbb{L}$ 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. **Posledica** 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 $\lambda : \mathbb{L} \to \mathbb{K}$, $\lambda \circ \tau = \sigma$.

$$\begin{tikzcd} \mathbb{L} \arrow[rr, dashed, "\lambda"] & & \mathbb{K} \\ & \mathbb{F} \arrow[ul, "\tau"] \arrow[ur, "\sigma"'] & \end{tikzcd}$$

Dokaz

$$\begin{array}{ccc} \mathbb{L} & \overset{\lambda}{\dashrightarrow} & \mathbb{K} \\ \cup\!| & & \cup\!| \\ \tau\mathbb{F} & \xrightarrow{\sigma \circ \tau^{-1}} & \sigma\mathbb{K} \end{array}$$

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 $\sigma^* \supseteq \sigma$, $\sigma^* : \mathbb{E} \to \mathbb{K}$.

$$\begin{tikzcd} \mathbb{E} \arrow[rr, dashed, "\sigma^*"] & & \mathbb{K} \\ \cup\!| & & \\ \mathbb{F} \arrow[urr, "\sigma"'] & & \end{tikzcd}$$

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. **Teorema.** 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

$$\begin{tikzcd} \mathbb{L} \arrow[r, dashed, "\lambda"] & \mathbb{K} \\ \cup & \cup \\ \sigma\mathbb{F} \arrow[r, "\tau\circ\sigma^{-1}"] & \tau\mathbb{F} \end{tikzcd}$$

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 $\Phi : \mathcal{F}_{\sigma,\mathbb{L}} \xrightarrow[1\text{-}1]{na} \mathcal{F}_{\tau,\mathbb{K}}$

$$\begin{tikzcd} \mathbb{L} \arrow[rr, "\lambda"] & & \mathbb{K} \\ \cup & \mathbb{E} \arrow[ul, "\sigma^*"] \arrow[ur, dashed, "\tau^*"'] & \cup \\ & \cup & \\ \sigma\mathbb{F} & \mathbb{F} \arrow[l, "\sigma"'] \arrow[r, "\tau"] & \tau\mathbb{F} \end{tikzcd}$$

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 1-1.
Za dato $\tau^* : \mathbb{E} \longrightarrow \mathbb{K}$, neka je $\sigma^* := \lambda^{-1}\circ\tau^*$. Tada $\Phi(\sigma^*) = \tau^*$
dakle Φ je na. ∎

Prema prethodnom za dato polje $\mathbb{F}$ i njegovu algebarsku ekstenziju $\mathbb{E}$, $|\mathcal{F}_{\sigma,\mathbb{L}}|$ je konstanta.

21.4 **Definicija** 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. **Teorema** Neka su $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ polja. Tada

$$|\mathbb{K} : \mathbb{F}|_s = |\mathbb{K} : \mathbb{E}|_s \cdot |\mathbb{E} : \mathbb{F}|_s .$$

Dokaz 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) $\quad |\{\tau \mid \tau : \mathbb{F}(a) \to \mathbb{K},\ \tau / F = \sigma / F\}| \leq |\mathbb{F}(a) : \mathbb{F}|.$

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> $\quad |\mathbb{F}(a) : \mathbb{F}|_s \leq |\mathbb{F}(a) : \mathbb{F}|.$ ∎

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 $\quad |\mathbb{E} : \mathbb{F}|_s \leq |\mathbb{E} : \mathbb{F}|.$ ∎

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 $\mathbb{F}$.

Dokaz ($\Rightarrow$) PP $|\mathbb{E}:\mathbb{F}|_s = |\mathbb{E}:\mathbb{F}|$. Neka je $a \in \mathbb{E}$. Dokazujemo 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 $|\mathbb{E}:\mathbb{F}(a)|_s \le |\mathbb{E}:\mathbb{F}(a)|$ i $|\mathbb{F}(a):\mathbb{F}|_s \le |\mathbb{F}(a):\mathbb{F}|$ 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.

$$\begin{array}{ccc} \mathbb{F}(a) & \xrightarrow{\sigma_i} & \overline{\mathbb{F}} \\ \cup\!| & & \\ \mathbb{F} & & \end{array}$$

Dakle, postoje n utapanja $\sigma_1, \dots, \sigma_n$ koja produžuju inkluziono preslikavanje $i_F : \mathbb{F} \to \overline{\mathbb{F}}$, $\sigma_i : \mathbb{F}(a) \hookrightarrow \overline{\mathbb{F}}$, $i = 1, \dots, n$.
S obzirom da je $\sigma_i|F = \sigma_j|F$ i $\mathbb{F}(a)$ je generisano sa $F \cup \{a\}$, to za $i \ne j$, $\sigma_i(a) \ne \sigma_j(a)$.

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 $b_i \ne b_j$, za $i \ne j$). Dakle, $|\mathbb{E}:\mathbb{F}|_s \ge n$. S druge strane $|\mathbb{E}:\mathbb{F}| = \deg f = n$, pa kako $|\mathbb{E}:\mathbb{F}|_s \le |\mathbb{E}:\mathbb{F}|$ sledi $|\mathbb{E}:\mathbb{F}|_s = |\mathbb{E}:\mathbb{F}|$. ∎

21.6. Primer (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. Zadatak 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. <u>Zadatak</u> 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. <u>Zadatak</u> Odrediti sva utapanja $\sigma : \mathbb{Q}(\varepsilon) \longrightarrow \mathbb{A}$, $\varepsilon = e^{\frac{2\pi i}{p}}$, $p \in Prost$

21.10. <u>Zadatak</u> 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. <u>Z.</u> Dokazati da postoji beskonačno mnogo prostih brojeva p takvih da $f(x) = x^2 + x + 1$ ima koren u $\mathbb{Z}_p$.

21.12. <u>Z</u> Ako je $|\mathbb{E} : \mathbb{F}| < \infty$ tada $|\mathbb{E} : \mathbb{F}|_s$ deli $|\mathbb{E} : \mathbb{F}|$.

21.13. <u>Z.</u> Ako je $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{C}$ tada $|\mathbb{F} : \mathbb{Q}|_s = |\mathbb{F} : \mathbb{Q}|$.

21.14. <u>Z</u> 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 $\mathbb{K} \leq \overline{\mathbb{F}}$ korensko polje minimalnog polinoma za a. Napomena: najpre dokažite da je a algebarski nad $\mathbb{F}$!

21.15. <u>Z.</u> 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. <u>Normalna raširenja algebarskih polja</u>

Neka je $\mathbb{E} \supseteq \mathbb{F}$ algebarsko raširenje polja $\mathbb{F}$. $\mathbb{E}$ je <u>normalno raširenje</u> 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. <u>Teorema</u> Neka je $\mathbb{F} \subseteq \mathbb{E} \leq \overline{\mathbb{F}}$. 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 $\mathbb{F}$.

<u>Napomena</u>: $\mathbb{E}$ 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 $f \in \mathcal{F}$.

$$\begin{tikzcd} \mathbb{E} \arrow[r, dashed, "\sigma"] & \overline{\mathbb{F}} \\ \mathbb{F}(a) \arrow[u, phantom, "\cup" rotate=90] \arrow[r, "\tau"] & \mathbb{F}(b) \arrow[u, phantom, "\cup" rotate=90] \\ & \mathbb{F} \arrow[ul, phantom, "\subseteq"] \arrow[u, phantom, "\subseteq"] \end{tikzcd}$$

Dokaz ($1^\circ \Rightarrow 3^\circ$) PP da važe uslovi u 1°. Dokazujemo 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 $\mathbb{E}$.

($3^\circ \Rightarrow 2^\circ$) PP da važi 3°. Dokazujemo 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 $S = \{a \in E \mid \bigvee_{f \in \mathcal{F}} f^{E}(a)=0\}$. 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°. Dokazujemo 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 $f(\sigma(a)) = 0$, 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 $p \in \mathbb{F}[x_1, \dots, x_n]$ i $a_1, \dots, a_n \in S$ takvi da $b = p^{E}(a_1, \dots, a_n)$ pa $\sigma b = p^{\overline{\mathbb{F}}}(\sigma a_1, \dots, \sigma a_n)$. S obzirom da $\sigma a_1, \dots, \sigma a_n \in E$ i $\mathbb{E} \subseteq \overline{\mathbb{F}}$ to

$$p^{\overline{\mathbb{F}}}(\sigma a_1, \dots, \sigma a_n) = p^{E}(\sigma a_1, \dots, \sigma a_n),$$

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 $\mathbb{C}$

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \varepsilon\sqrt[3]{2})(x - \varepsilon^2\sqrt[3]{2}), \text{ gde } \varepsilon = e^{\frac{2\pi i}{3}}.$$

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, Hiparh, 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 jednačinu 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 odslikava 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. <u>Definicija</u> 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 Teorema 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. Posledica 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. Primer 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 $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$, dakle leže u $\mathbb{Q}(\varepsilon)$. Odavde $\mathbb{Q}(\varepsilon)$ je korensko polje polinoma $f(x) = x^n - 1$.

23.5. Neka je $\mathbb{E}$ polje i $\sigma_1, \ldots, \sigma_n \in \mathrm{Aut}\,\mathbb{E}$.
Tada je $\mathbb{F} = \{a \in E \mid \sigma_1 x = \cdots = \sigma_n x = x\}$ podpolje polja $\mathbb{E}$ (proverite!). Ovo polje naziva se invarijantnim ili nepokretnim poljem automorfizama $\sigma_1, \ldots, \sigma_n$ i obeležavamo ga pomoću $\mathbb{F} = \mathbb{F}(\mathbb{E}, \sigma_1, \ldots, \sigma_n)$. Ako je $G = \{\sigma_1, \ldots, \sigma_n\}$ podgrupa grupe $\mathrm{Aut}\,\mathbb{E}$, koristimo oznaku $\mathbb{F} = \mathbb{F}(\mathbb{E}, G)$. Negde se koristi i oznaka $\mathbb{F} = \mathbb{E}^G$.

23.6. Galoaova grupa Neka su $\mathbb{F}$ i $\mathbb{E}$ polja i $\mathbb{F} \subseteq \mathbb{E}$ i neka je
$G = \{\sigma \in \mathrm{Aut}\,\mathbb{E} \mid \sigma \restriction F = i_F\} = \{\sigma \in \mathrm{Aut}\,\mathbb{E} \mid \bigwedge_{x \in F} \sigma x = x\}$.
Nije teško proveriti da je $G < \mathrm{Aut}\,\mathbb{E}$ (tj. G je podgrupa grupe $\mathrm{Aut}\,\mathbb{E}$).
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 $\mathbb{F} \leq \mathbb{E}$, $\mathbb{F} \leq \mathbb{K}$.

$\mathrm{Hom}(\mathbb{E} | \mathbb{F}, \mathbb{K}) = \{\sigma \mid \sigma : \mathbb{E} \longrightarrow \mathbb{K},\ \sigma | F = i_F\}$.

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 $\tau \leq \sigma$.

4° Pretpostavimo $\mathbb{F} \leq \mathbb{E}$, $\sigma : \mathbb{F} \longrightarrow \mathbb{K}$, $\mathbb{F}, \mathbb{E}, \mathbb{K}$ su polja.

$\mathrm{Hom}(\mathbb{E} |_\sigma \mathbb{F}, \mathbb{K}) = \{\tau \mid \tau : \mathbb{E} \longrightarrow \mathbb{K},\ \sigma \leq \tau\}$.

Dakle, $\mathrm{Hom}(\mathbb{E} |_\sigma \mathbb{F}, \mathbb{K})$ je skup homomorfizama τ takvih da dijagram (D) komutira.

(D)
$$\begin{tikzcd} \mathbb{E} \arrow[r, "\tau"] & \mathbb{K} \\ \mathbb{F} \arrow[u, phantom, sloped, "\leq"] \arrow[ur, "\sigma"'] & \end{tikzcd}$$

Ako je $\mathbb{F} \leq \mathbb{K}$, 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, $\mathbb{A}\mathrm{ut}\,\mathbb{F}$ je skup svih automorfizama polja $\mathbb{F}$.

6° Ako je $\mathbb{F} \leq \mathbb{E}$, 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 $\mathbb{F} \leq \mathbb{E}$ 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 $\mathbb{Q} \leq \mathbb{E}, \mathbb{K}$, tada $\mathrm{Hom}(\mathbb{E} | \mathbb{Q}, \mathbb{K}) = \mathrm{Hom}(\mathbb{E}, \mathbb{K})$ i slično ako $\mathbb{Z}_p \leq \mathbb{E}, \mathbb{K}$, $p \in \mathrm{Prost}$, $\mathrm{Hom}(\mathbb{E} | \mathbb{Z}_p, \mathbb{K}) = \mathrm{Hom}(\mathbb{E}, \mathbb{K})$.

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 $\mathrm{Hom}(\mathbb{E}|_\sigma \mathbb{F}, \mathbb{K}) \neq \emptyset$.

24.3. Zadatak Dokazati obrat od 24.2: Ako za svako algebarsko raširenje $\mathbb{E} \geq \mathbb{F}$ i svako $\sigma : \mathbb{F} \to \mathbb{K}$ važi $\mathrm{Hom}(\mathbb{E}|_\sigma \mathbb{F}, \mathbb{K}) \neq \emptyset$, 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 $\mathrm{Hom}(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}}) = \mathrm{Aut}(\mathbb{E}|\mathbb{F})$.

Primetimo da je u opštem slučaju $\mathrm{Aut}(\mathbb{E}|\mathbb{F}) \subseteq \mathrm{Hom}(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})$.

24.5. (Teorema 21.3). Neka su $\mathbb{K}$ i $\mathbb{L}$ algebarski zatvorena polja, $\mathbb{E}|\mathbb{F}$ algebarsko i $\sigma \in \mathrm{Hom}(\mathbb{F}, \mathbb{K})$, $\tau \in \mathrm{Hom}(\mathbb{F}, \mathbb{L})$.

Tada $|\mathrm{Hom}(\mathbb{E}|_\sigma \mathbb{F}, \mathbb{K})| = |\mathrm{Hom}(\mathbb{E}|_\tau \mathbb{F}, \mathbb{L})|$.

$$\begin{tikzcd}
\mathbb{K} & & & & \mathbb{L} \\
\mathbb{E} \arrow[u, dashed, "\sigma^*"] & \geq & \mathbb{F} \arrow[ull, "\sigma"'] \arrow[urr, "\tau"] & \leq & \mathbb{E} \arrow[u, dashed, "\tau^*"']
\end{tikzcd}$$

Specijalno, $|\mathrm{Hom}(\mathbb{E}|_\sigma \mathbb{F}, \mathbb{K})| = |\mathrm{Hom}(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})|$

Otuda, za definiciju separabilnog stepena možemo uzeti

24.6. $|\mathbb{E} : \mathbb{F}|_s = |\mathrm{Hom}(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})|$, 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. Teorema Neka je $\mathbb{E} \geq \mathbb{F}$ normalno raširenje polja $\mathbb{F}$.
Tada $|\mathrm{Aut}(\mathbb{E}|\mathbb{F})| = |\mathbb{E} : \mathbb{F}|_s$.

Dokaz. $\mathrm{Aut}(\mathbb{E}|\mathbb{F}) = \mathrm{Hom}(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})$ i $|\mathbb{E} : \mathbb{F}|_s = |\mathrm{Hom}(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})|$.

24.8. Teorema Neka je $\mathbb{E}$ konačno raširenje polja $\mathbb{F}$. Tada $|\mathrm{Aut}(\mathbb{E}|\mathbb{F})| = |\mathbb{E} : \mathbb{F}|$.
akko je $\mathbb{E}$ galoavo raširenje polja $\mathbb{F}$.

Dokaz 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 $|\mathrm{Aut}(\mathbb{E}|\mathbb{F})| = |\mathbb{E} : \mathbb{F}|_s$.
Kako je $\mathbb{E}|\mathbb{F}$ separabilno, $|\mathbb{E} : \mathbb{F}|_s = |\mathbb{E} : \mathbb{F}|$. Dakle $|\mathrm{Aut}(\mathbb{E}|\mathbb{F})| = |\mathbb{E} : \mathbb{F}|$.
2° Neka je $|\mathrm{Aut}(\mathbb{E}|\mathbb{F})| = |\mathbb{E} : \mathbb{F}|$. Dalje $\mathrm{Aut}(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}}) \subseteq \mathrm{Hom}(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})$ i $|\mathrm{Hom}(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}}| = |\mathbb{E} : \mathbb{F}|_s \leq |\mathbb{E} : \mathbb{F}|$, pa $|\mathbb{E} : \mathbb{F}|_s = |\mathbb{E} : \mathbb{F}|$, tj. $\mathbb{E}|\mathbb{F}$ je separabilno. Takođe $|\mathrm{Aut}(\mathbb{E}|\mathbb{F})| = |\mathrm{Hom}(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})|$ i $\mathrm{Hom}(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})$ je konačan, dakle $\mathrm{Aut}(\mathbb{E}|\mathbb{F}) = \mathrm{Hom}(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})$, tj. $\mathbb{E}|\mathbb{F}$ je normalno ∎

24.9. Prema prethodnom, ako je $\mathbb{E}|\mathbb{F}$ konačno, tada

$$|Aut(\mathbb{E}|\mathbb{F})| \le |\mathbb{E}:\mathbb{F}|.$$

Jednakost važi akko $\mathbb{E}|\mathbb{F}$ je galoavo!

24.10. <u>Teorema</u> Neka je $\mathbb{E}|\mathbb{F}$ algebarsko. Tada $Hom(\mathbb{E}|\mathbb{F}, \mathbb{E}) = Aut(\mathbb{E}|\mathbb{F})$.

<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 homomorfizama i monomorfizama 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 $Hom(\mathbb{E}, \mathbb{E}) = Aut\, \mathbb{E}$.

Zaista, $Hom(\mathbb{E}, \mathbb{E}) = Hom(\mathbb{E}|\mathbb{Q}, \mathbb{E}) = Aut(\mathbb{E}|\mathbb{Q}) = Aut\, \mathbb{E}$.
Specijalno, ako je $\mathbb{A}$ polje algebarskih brojeva, tada $Hom(\mathbb{A}, \mathbb{A}) = Aut\, \mathbb{A}$.

24.10.2. <u>Posledica</u> Ako je $\mathbb{E}$ algebarsko raširenje polja $\mathbb{Z}_p$, $p \in Prost$, tada $Hom(\mathbb{E}, \mathbb{E}) = Aut\, \mathbb{E}$.

24.11. <u>Teorema</u> Neka su $\sigma_1, \dots, \sigma_n \in Aut(\mathbb{E}|\mathbb{F})$ različiti i $|\mathbb{E}:\mathbb{F}| = n$. Tada je $\mathbb{E}$ galoavo 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 $Aut(\mathbb{E}|\mathbb{F})$.

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 $\mathbb{L}$.

$$n\left[\begin{array}{l}\left.\begin{array}{c}\mathbb{E}\\ \cup|\\ \mathbb{L}\end{array}\right]n\\ \;\cup|\\ \;\mathbb{F}\end{array}\right.$$

<u>Dokaz</u> Kako je $\mathbb{E} \supseteq \mathbb{F}$ normalno, to je $Hom(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}}) = Aut(\mathbb{E}|\mathbb{F})$.
Dalje, $Hom(\mathbb{E}|\mathbb{L}, \overline{\mathbb{F}}) \subseteq Hom(\mathbb{E}|\mathbb{F}, \overline{\mathbb{F}})$ jer $\mathbb{F} \subseteq \mathbb{L}$ pa
$Hom(\mathbb{E}|\mathbb{L}, \overline{\mathbb{F}}) \subseteq Aut(\mathbb{E}|\mathbb{F})$, odakle $Hom(\mathbb{E}|\mathbb{L}, \overline{\mathbb{F}}) = Aut(\mathbb{E}|\mathbb{L})$.
Dakle, prema 24.4 $\mathbb{E}|\mathbb{L}$ je normalno. ∎

25.2. Teorema 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.

$$\begin{tikzcd} \mathbb{E} \arrow[d, dash, "s"] \arrow[dd, dash, bend right, "s"'] \\ \mathbb{L} \arrow[d, dash, "s"] \\ \mathbb{F} \end{tikzcd}$$

Dokaz $|\mathbb{E} : \mathbb{F}| = |\mathbb{E} : \mathbb{L}| \cdot |\mathbb{L} : \mathbb{F}|$, $|\mathbb{E} : \mathbb{F}|_s = |\mathbb{E} : \mathbb{L}|_s \cdot |\mathbb{L} : \mathbb{F}|_s$

$|\mathbb{E} : \mathbb{F}|_s = |\mathbb{E} : \mathbb{F}|$ (zbog separabilnosti), pa

$|\mathbb{E} : \mathbb{L}|_s \cdot |\mathbb{L} : \mathbb{F}|_s = |\mathbb{E} : \mathbb{L}| \cdot |\mathbb{L} : \mathbb{F}|$

$|\mathbb{E} : \mathbb{L}|_s \leq |\mathbb{E} : \mathbb{L}|$, $|\mathbb{L} : \mathbb{F}|_s \leq |\mathbb{L} : \mathbb{F}|$, odakle

$(m \cdot n = m' \cdot n',\ m \leq m',\ n \leq n' \Rightarrow m = m',\ n = n',\ m, n, m', n' \in N^+)$

$|\mathbb{E} : \mathbb{L}|_s = |\mathbb{E} : \mathbb{L}|$, $|\mathbb{L} : \mathbb{F}|_s = |\mathbb{L} : \mathbb{F}|$, tj.

$\mathbb{E}|\mathbb{L}$ je separabilno i $\mathbb{L}|\mathbb{F}$ je separabilno. ∎

25.3. Teorema 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.

$$\begin{tikzcd} \mathbb{E} \arrow[d, dash, "g"] \arrow[dd, dash, bend right, "g"'] \\ \mathbb{L} \arrow[d, dash] \\ \mathbb{F} \end{tikzcd}$$

Dokaz Prema 25.1 i 25.2.

25.4. Teorema Neka je $\mathbb{E}|\mathbb{F}$ galoava ekstenzija i $G = Aut(\mathbb{E}|\mathbb{F})$.

Tada $\mathbb{F} = \mathbb{E}^G \left(= \mathcal{F}(\mathbb{E}, G) = \{ x \in E \mid \bigwedge_{\sigma \in G} \sigma x = x \}\right)$.

Dokaz 1° Očigledno $F \subseteq \mathbb{E}^G$.

2° $\mathbb{E}^G \subseteq \mathbb{F}$. 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:

$$\begin{tikzcd} \mathbb{E} \arrow[r, dashed, "\tau"] & \overline{\mathbb{F}} \\ \mathbb{F}(a) \arrow[u, phantom, sloped, "\subseteq"] \arrow[ur, "\sigma"'] & \\ \mathbb{F} \arrow[u, phantom, sloped, "\subseteq"] & \end{tikzcd}$$

$\sigma | F = i_F$, $\sigma(a) = a$, te $\sigma = i_{F(a)}$.

Ovim smo dokazali da je $Hom(\mathbb{F}(a)|\mathbb{F}, \overline{\mathbb{F}}) = \{ i_{F(a)} \}$, te $|\mathbb{F}(a) : \mathbb{F}|_s = 1$. Kako je $\mathbb{F}(a) \supseteq \mathbb{F}$ separabilna ekstenzija (25.2) to je $|\mathbb{F}(a) : \mathbb{F}| = |\mathbb{F}(a) : \mathbb{F}|_s = 1$, tj. $\mathbb{F}(a) = \mathbb{F}$ odakle $a \in F$. 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 $\mathcal{G} = \{ H \mid H < Aut(\mathbb{E}|\mathbb{F}) \}$.

Prema Teoremi 25.3 preslikavanje $\Phi : \mathcal{M} \longrightarrow \mathcal{G}$, $\Phi : \mathbb{L} \mapsto Aut(\mathbb{E}|\mathbb{L})$, $\mathbb{L} \in \mathcal{M}$, je dobro definisano.

25.5. **Teorema** $\Phi : \mathcal{M} \xrightarrow[1-1]{} \mathcal{G}$.

$$\begin{tikzcd}[column sep=small] & \mathbb{E} & \\ \mathbb{L} \arrow[ur, phantom, "\subsetneq"] & & \mathbb{L}' \arrow[ul, phantom, "\supseteq"] \\ & \mathbb{F} \arrow[ul, phantom, "\supseteq"] \arrow[ur, phantom, "\subseteq"] & \end{tikzcd}$$

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 $\bigwedge_{a \in E} |\mathbb{F}(a):\mathbb{F}| \le n$. Tada $|\mathbb{E}:\mathbb{F}| \le n$.

Dokaz Neka je m najveći prirodan broj takav da je za neki $a \in E$ $|\mathbb{F}(a):\mathbb{F}| = m$. Tada, naravno, $m \le n$. 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 $a \in \mathbb{E}$ je koren nekog separabilnog polinoma f stepena $\leq n$, $f \in F[x]$.
Neka je $a \in \mathbb{E}$ 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 $\sigma f_i = f_i$, $0 \leq i < m$

⌜ 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 $\deg f = m \leq n$ ($m \leq n$ je $m = |S| \leq |G| = n$), $f(a) = 0$, te je ovim 1° dokazano.
Prema Lemi 25.8 važi

2° $\mathbb{E}|\mathbb{F}$ je separabilna ekstenzija i $|\mathbb{E} : \mathbb{F}| \leq n$. Takođe

3° $\mathbb{E}|\mathbb{F}$ je normalna jer je svaki $a \in \mathbb{E}$ koren nekog polinoma $(**)$ koji se razlaže na linearne faktore. Dakle

4° $\mathbb{E}|\mathbb{F}$ je Galoaova ekstenzija.
Najzad, $n = |G|$, $G \subseteq Aut(\mathbb{E}|\mathbb{F})$, $n \leq |Aut(\mathbb{E}|\mathbb{F})| \underset{\text{zbog normalnosti}}{=} |\mathbb{E} : \mathbb{F}|_s \leq |\mathbb{E} : \mathbb{F}| \leq n$

pa $Aut(\mathbb{E}|\mathbb{F}) = G$. ∎

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 $G = Aut(\mathbb{E}|\mathbb{F})$, 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 $Sym(S)$ (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)

$$\begin{tikzcd} \mathbb{E} \arrow[r, "\sigma"] & \mathbb{E} & & \mathbb{E}' \arrow[r, "\sigma'"] & \mathbb{E}' \\ & \mathbb{F} \arrow[ul, phantom, "\subseteq" sloped] \arrow[u, phantom, "\subseteq" sloped] \arrow[rr, squiggly] & & & \mathbb{F}' \arrow[ul, phantom, "\subseteq" sloped] \arrow[u, phantom, "\subseteq" sloped] \end{tikzcd}$$

(D2)

Pretpostavke o ekstenzijama $\mathbb{E}|\mathbb{F}$ i $\mathbb{E}'|\mathbb{F}'$ predstavljene su dijagramom (D1). Možemo postaviti prirodno pitanje o korespodenciji između $Aut(\mathbb{E}|\mathbb{F})$ i $Aut(\mathbb{E}'|\mathbb{F}') = Aut(\lambda\mathbb{E}|\lambda\mathbb{F})$, vidi dijagram (D2).

Neka je $\sigma \in Aut(\mathbb{E}|\mathbb{F})$ i $\sigma' = \lambda \circ \sigma \circ \lambda^{-1}$.

Neposredno se proverava da dijagram (D3) komutira, i da je $\sigma' \in Aut(\mathbb{E}'|\mathbb{F}')$.

$$\begin{tikzcd} \mathbb{E}' \arrow[rr, "\sigma'"] \arrow[dd, "\lambda^{-1}"', "\cong"] & & \mathbb{E}' \\ & \mathbb{F}' \arrow[ul, phantom, "\subseteq" sloped] \arrow[ur, phantom, "\subseteq" sloped] & \\ & \mathbb{F} \arrow[u, "\lambda|\mathbb{F}"'] \arrow[dl, phantom, "\subseteq" sloped] \arrow[dr, phantom, "\subseteq" sloped] & \\ \mathbb{E} \arrow[rr, "\sigma"] & & \mathbb{E} \arrow[uuu, "\lambda"', "\cong"] \end{tikzcd}$$

(D3).

Otuda, preslikavanje
$$h : \sigma \mapsto \lambda \circ \sigma \circ \lambda^{-1}, \quad \sigma \in Aut(E|\mathbb{F})$$
preslikava $Aut(\mathbb{E}|\mathbb{F})$ u $Aut(\mathbb{E}'|\mathbb{F}')$.

Uz prethodno uvedene oznake važi sledeće tvrđenje:

26.1. Lema $h : Aut(\mathbb{E}|\mathbb{F}) \cong Aut(\mathbb{E}'|\mathbb{F}')$.

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 $\sigma' \in Aut(\mathbb{E}'|\mathbb{F}')$ i $\sigma = \lambda^{-1} \circ \sigma' \circ \lambda$. Tada $\sigma \in Aut(\mathbb{E}|\mathbb{F})$ 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
$$Aut(\lambda\mathbb{E}|\lambda\mathbb{F}) = \lambda \circ Aut(\mathbb{E}|\mathbb{F}) \circ \lambda^{-1}.$$

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. $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{E}$. Dalje, neka je $\lambda : \mathbb{L} \to \mathbb{E}$, $\lambda|\mathbb{F} = i_{\mathbb{F}}$. Prema Posledici 21.2.

$$\begin{tikzcd} \mathbb{E} \arrow[r, dashed, "\bar{\lambda}"] & \mathbb{E} \\ \mathbb{L} \arrow[u, phantom, "\subseteq" sloped] \arrow[r, "\lambda", "\approx"'] & \mathbb{L}' \arrow[u, phantom, "\subseteq" sloped] \\ & \mathbb{F} \arrow[ul, phantom, "\subseteq" sloped] \arrow[u, phantom, "\subseteq" sloped] \end{tikzcd}$$

(D4)

postoji $\bar{\lambda} \in \mathrm{Hom}(\mathbb{E}, \bar{\mathbb{F}})$ tako da dijagram (D4) komutira, tj. $\lambda \leq \bar{\lambda}$. S obzirom da je raširenje $\mathbb{E}|\mathbb{F}$ galoaovo, ono je normalno, dakle $\bar{\lambda} \in \mathrm{Aut}(\mathbb{E}|\mathbb{F})$, te je prema Teoremi 26.2, $\mathrm{Aut}(\mathbb{E}|\lambda\mathbb{L}) = \bar{\lambda} \circ \mathrm{Aut}(\mathbb{E}|\mathbb{L}) \circ \bar{\lambda}^{-1}$. Ovim smo dokazali

26.3. <u>Teorema</u> Neka je $\mathbb{E}|\mathbb{F}$ galoaova ekstenzija, $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{E} \subseteq \bar{\mathbb{F}}$ i $\lambda \in \mathrm{Hom}(\mathbb{L}, \mathbb{E})$. Tada su podgrupe $\mathrm{Aut}(\mathbb{E}|\lambda\mathbb{L})$ i $\mathrm{Aut}(\mathbb{E}|\mathbb{L})$ galoaove grupe $\mathrm{Aut}(\mathbb{E}|\mathbb{F})$ konjugovane, preciznije, postoji $\bar{\lambda} \in \mathrm{Aut}(\mathbb{E}|\mathbb{F})$ tako da je $\lambda \leq \bar{\lambda}$ i

$$\mathrm{Aut}(\mathbb{E}|\lambda\mathbb{L}) = \bar{\lambda} \circ \mathrm{Aut}(\mathbb{E}|\mathbb{L}) \circ \bar{\lambda}^{-1}. \qquad \blacksquare$$

sledeće tvrđenje je posledнji deo teoreme o korespodenciji između međupolja galoaove ekstenzije $\mathbb{E}|\mathbb{F}$ i podgrupa galoaove grupe $\mathrm{Aut}(\mathbb{E}|\mathbb{F})$.

26.4. <u>Teorema</u> Neka je $\mathbb{E}|\mathbb{F}$ galoaova ekstenzija, $\mathrm{Aut}(\mathbb{E}|\mathbb{F}) = \mathbb{G}$, $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{E}$, $H = \mathrm{Aut}(\mathbb{E}|\mathbb{L})$. Tada

1° $\mathbb{L}|\mathbb{F}$ je normalno raširenje akko $H \trianglelefteq \mathbb{G}$.

2° Ako je $\mathbb{L}|\mathbb{F}$ normalna ekstenzija, tada je $h : \sigma \mapsto \sigma|\mathbb{L}$, $\sigma \in \mathbb{G}$, $h : \mathbb{G} \to \mathrm{Aut}(\mathbb{L}|\mathbb{F})$ i $\ker h = H$.

3° Pod uslovima u 2°, $\mathrm{Aut}(\mathbb{L}|\mathbb{F}) \cong \mathbb{G}/H$.

<u>Dokaz</u> Neka je $\mathbb{G}' = \mathrm{Aut}(\mathbb{L}|\mathbb{F})$. 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 $\bar{\lambda} \in \mathrm{Aut}(\mathbb{E}|\mathbb{F}) (= \mathbb{G})$,

1° ($\Rightarrow$) Neka je $\mathbb{L}|\mathbb{F}$ normalno raširenje. Tada $\lambda : \mathbb{L} \to \mathbb{E} \subseteq \bar{\mathbb{F}}$, te proizvoljno. Dalje, neka je $\lambda = \bar{\lambda}|\mathbb{L}$. 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 $\mathrm{Aut}(\mathbb{E}|\mathbb{L}) = \mathrm{Aut}(\mathbb{E}|\lambda\mathbb{L}) = \bar{\lambda} \circ \mathrm{Aut}(\mathbb{E}|\mathbb{L}) \circ \bar{\lambda}^{-1}$,

tj. $\bigwedge_{\sigma \in G} \sigma H \sigma^{-1} = H$, dakle $H \trianglelefteq \mathbb{G}$.

($\Leftarrow$) 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 $\lambda \in \mathrm{Hom}(\mathbb{L}|\mathbb{F}, \mathbb{E})$ tako da $\lambda \notin \mathrm{Aut}(\mathbb{L}|\mathbb{F})$, 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 $\mathbb{E} \subseteq \bar{\mathbb{F}}$, dakle $\bar{\lambda} \in \mathrm{Aut}(\mathbb{E}|\mathbb{F})$, s obzirom da je $\mathbb{E}|\mathbb{F}$ normalno. Otuda prema T26.3 $\mathrm{Aut}(\mathbb{E}|\lambda\mathbb{L}) = \bar{\lambda}\, \mathrm{Aut}(\mathbb{E}|\mathbb{L})\, \bar{\lambda}^{-1}$. S druge strane $\mathrm{Aut}(\mathbb{E}|\lambda\mathbb{L}) \neq \mathrm{Aut}(\mathbb{E}|\mathbb{L})$ jer u suprotnom (T. 25.5) $\lambda\mathbb{L} = \mathbb{L}$, kontradikcija. Dakle $H \neq \bar{\lambda} H \bar{\lambda}^{-1}$,

tj. $H \ntrianglelefteq \mathbb{G}$.

2° a. $h : G \to G'$: Ako $\sigma \in G$, tada $\sigma|L : L \to \mathbb{E} \subseteq \overline{\mathbb{F}}$, dakle $\sigma|L \in Hom(\mathbb{L}|\mathbb{F}, \overline{\mathbb{F}})$, a 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).

$$\begin{tikzcd} \mathbb{E} \arrow[r, "\sigma"] & \mathbb{E} \\ \mathbb{L} \arrow[u, phantom, "\cup" rotate=90] \arrow[r, "\sigma|_L"] & \mathbb{L} \arrow[u, phantom, "\cup" rotate=90] \\ & \mathbb{F} \end{tikzcd} \quad (D5) \qquad \begin{tikzcd} G \arrow[r, "h", "na"'] \arrow[d, "h"] & G' \\ G/H = G/\ker h \arrow[ur, dashed, "\approx"'] & \end{tikzcd} \quad (D6)$$

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 $G' = Aut(\mathbb{L}|\mathbb{F})$.

$$\begin{tikzcd} \mathbb{E} \arrow[r, dashed, "\sigma"] & \mathbb{E} \\ \mathbb{L} \arrow[u, phantom, "\cup" rotate=90] \arrow[r, "\tau"] & \mathbb{L} \arrow[u, phantom, "\cup" rotate=90] \\ & \mathbb{F} \end{tikzcd}$$

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, $h\sigma = \sigma|_L = \tau$.
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 Galoaova ekstenzija polja $\mathbb{F}$. Osnovni zadatak teorije Galoa je da se odredi Galoaova 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 Galoaove nad $\mathbb{Q}$, tj. ako je G konačna grupa da li je $G \cong Aut(\mathbb{E}|\mathbb{Q})$ za neku Galoaovu ekstenziju $\mathbb{E}|\mathbb{Q}$. Poznato je da su konačne ciklične grupe i konačne Abelove grupe Galoaove nad $\mathbb{Q}$. U tom pogledu ističe se sledeće tvrđenje:

Teorema (Šafarevič) Svaka konačna rešiva grupa je Galoaova nad $\mathbb{Q}$.

Otvoren problem Da li je svaka konačna grupa Galoaova 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 $|H| = p^n$, $n \in N$.
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 $G = Aut(\mathbb{E}|\mathbb{F})$ 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.
$Im\,\Phi = \{ H < G \mid H$ je zatvorena u Krulovoj topologiji$\}$.

27.4. Galoaovo preslikavanje Neka je $G < Aut\,E$ konačna grupa automorfizama polja $\mathbb{E}$, i neka je $\mathbb{F} \subseteq E$ nepokretno polje u odnosu na G, tj.
$F = \{a \in E \mid \bigwedge_{\sigma \in G} \sigma a = a\}$. Tada je prema Artinovoj teoremi (T. 25.9) $\mathbb{E}|\mathbb{F}$ galoaova ekstenzija i $G = Aut(\mathbb{E}/\mathbb{F})$. Neka su $X \subseteq E$ i $Y \subseteq G$ i
$X^* \overset{\text{def}}{=} \{\sigma \in G \mid \bigwedge_{a \in X} \sigma a = a\}$, $Y^* = \{a \in E \mid \bigwedge_{\sigma \in Y} \sigma a = a\}$.
Dakle, uvedena su dva preslikavanja sa istom oznakom $*$:
$* : \mathbb{P}(E) \longrightarrow \mathbb{P}(G)$, $* : \mathbb{P}(G) \longrightarrow \mathbb{P}(E)$ ($\mathbb{P}(A)$ = 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 $H = Aut(\mathbb{E}|H^*)$.
S druge strane, prema definiciji preslikavanja $*$, $H^{**} = Aut(\mathbb{E}|H^*)$, 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 Galoaovog preslikavanja (vidi P. M. Cohn, "Universal Algebra").

Primene teorije Galoa

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 $|F(d) : F| = 2$, i Galoaova grupa $\mathbb{G}$ ove jednačine je reda 2, pa $\mathbb{G} = C_2$. $\mathbb{G} = \{i, \sigma\}$, 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) $\mathbb{Z}_p \models \exists x\,(x^2 = a)$ ako $a^{\frac{p-1}{2}} = 1 \bmod p$, $a \in \mathbb{Z}_p \setminus \{0\}$.

Dokaz. Koristićemo činjenicu da je $\mathbb{Z}_p^* = (\mathbb{Z}_p \setminus \{0\}, \cdot, 1)$ ciklička grupa, dakle $\mathbb{Z}_p^* = \mathbb{C}_{p-1} = \langle b \rangle$, $b^i \neq 1$ za $1 \leq i < p-1$, $b^{p-1} = 1$.

($\Rightarrow$) 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 ako $a^{\frac{p-1}{2}} = 1 \pmod p$.

28.1d. U vezi sa ovom jednačinom nad konačnim poljima je Ležandrov (Legendre) simbol: ako $(a, p) = 1$, $\left(\frac{a}{p}\right) \overset{\text{def}}{=} a^{\frac{p-1}{2}}$ (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 $\left(-\frac{1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$, $p \in Prost$, $p \geq 3$. Dakle, x^2+1 ima rešenje u $\mathbb{Z}_p$ $(p \geq 3)$ ako $p = 1 \pmod 4$.

28.2. $kF = 2$ 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 $kF \geq 3$, 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 tvrdnji 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 $p | h_0, \dots, p | h_n$, $n = \deg h$. 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.

$$h_k = \underbrace{f_0 g_k + f_1 g_{k-1} + \dots + f_{i-1} g_{j+1}}_{\text{deljivo sa } p} + f_i g_j + \underbrace{f_{i+1} g_{j-1} + \dots + f_{k-1} g_1 + f_k g_0}_{\text{deljivo sa } p}$$

$p | h_k$ i p deli označene zbirove u h_k, dakle $p | f_i g_j$ pa $p | f_i$ ili $p | g_j$, #.
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 $ab' g(x) = a'b g'(x) \equiv h(x)$. 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 $f \in \mathbb{F}[x]$ <u>moničan</u> ako je $f_n = 1$, $\deg f = n$.

29.5 <u>Lema</u> 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 $g, h \in \mathbb{Z}[x]$.

<u>Dokaz</u> 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 $a \mid b$, 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. <u>Zadatak</u> Neka su $a, b, c, d \in \mathbb{Z}$. Dokazati da su sva racionalna rešenja sistema (S) (operacijem 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. <u>Z.</u> Dokazati Ajzenštajnov kriterijum nesvodljivosti za polinome sa celobrojnim koeficijentima.

29.8 $x^n - 1 = 0$ nad poljem $\mathbb{F}$, $\kappa\mathbb{F} = p$, $p \in Prost$.

1° a <u>Slučaj $n = p$.</u> Tada $x^p - 1 = (x-1)^p$, te ova jednačina ima tačno jedno rešenje, $x = 1$.

1° b <u>Slučaj $n = p^k$.</u> Tada $x^{p^k} - 1 = (x-1)^{p^k}$, pa kao u prethodnom slučaju, jedino rešenje je $x = 1$.

2° <u>$(n, p) = 1$.</u> Tada $f'(x) = nx^{n-1}$, $(f, f') = 1$, te je polinom $f(x) = x^n - 1$ separabilan.

29.9. <u>$x^n - 1 = 0$ nad $\mathbb{Q}$.</u> 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 $\mathbb{E} \le \mathbb{C}$, 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.

<u>Lema</u> 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 ($\Rightarrow$) Neka je $C_n = \langle b \rangle$. Tada za neki $x \in \mathbb{Z}$, $b^x = a$, tj. $a^{ix} = a$. Otuda (prema Langranžovoj teoremi) $ix \equiv 1 \pmod n$, te za neki $y \in \mathbb{Z}$, $ix - yn = 1$. Otuda $(i, n) = 1$.

($\Leftarrow$) 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 $\sigma(a) = b$: $\sigma(a^i) \overset{\text{def}}{=} b^i$, $0 \le i \le n-1$.
Otuda, $|\mathrm{Aut}\, C_n| =$ 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 $\sigma \mid H_n$ je automorfizam grupe $(H_n, \cdot, 1) = \mathbb{H}_n$. Neka je

(0) $h : \mathrm{Aut}(\mathbb{Q}(\varepsilon) \mid \mathbb{Q}) \longrightarrow \mathrm{Aut}\, \mathbb{H}_n \cong \mathrm{Aut}\, C_n \cong \Phi_n$, $h(\sigma) = \sigma \mid H_n$.

h je 1-1: Neka je $h(\sigma) = h(\tau)$, tj. $\sigma \mid H_n = \tau \mid H_n$. Tada $\sigma(\varepsilon) = \tau(\varepsilon)$, pa kako je $\mathbb{Q}(\varepsilon)$ generisano sa ε nad $\mathbb{Q}$ i σ, τ fiksiraju $\mathbb{Q}$, to $\sigma = \tau$. Otuda

(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, $g \in \mathbb{Q}[X]$. Kako je $f(\varepsilon)=0$, to za neki $h \in \mathbb{Q}[X]$

$$x^n - 1 = g(x)\,h(x)$$

Mogli smo pretpostaviti da je g moničan, odakle $1 = g_n h_n \equiv 1 \cdot h_n$, tj. i h je moničan. Prema Lemi 29.5 tada su g, h celobrojni polinomi, tj. $g, h \in \mathbb{Z}[X]$. 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 $(i,n)=1$, $i = p_1^{k_1} \cdots p_l^{k_l}$, $(p_j, n) = 1$, $j = 1, \dots, l$; onda je i $g(\varepsilon^i) = 0$.

<u>Dokaz za (3):</u> Pretpostavimo suprotno, da nije $g(\varepsilon^p)=0$, tj. $g(\varepsilon^p) \ne 0$. 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 $h_1 \in \mathbb{Q}[X]$. Polinomi g i h su monični, pa je i h_1 moničan, te prema Lemi 29.5 $h_1 \in \mathbb{Z}[X]$. Dakle, $h(x^p), g(x), h_1(x) \in \mathbb{Z}[X]$.

Neka je $\rho: \mathbb{Z} \longrightarrow \mathbb{Z}_p$, $\rho: x \longmapsto \mathrm{rest}(x,p)$. 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 $\bar{h}(x^p), \bar{g}(x), \bar{h}_1(x) \in \mathbb{Z}_p[X]$. Primetimo da je za ovu redukciju ispunjen bitan uslov, $h(x^p), g(x), h_1(x) \in \mathbb{Z}[X]$ (da bi se ρ uopšte primenilo). S obzirom da je $x \longmapsto x^p$, $x \in \mathbb{Z}_p$, automorfizam polja $\mathbb{Z}_p$ (Frobeniusov automorfizam), to iz identiteta $h(x^p) = g(x)\,h_1(x)$ koji važi u $\mathbb{Z}[X]$ dobijamo $\bar{h}(x)^p = \bar{g}(x)\,\bar{h}_1(x)$ u $\mathbb{Z}_p[X]$, 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 $\mathbb{Z}_p$, mada je $(n,p)=1$, što je kontradikcija prema 29.8.2°. Prema tome $\deg g \ge |\{i \in \mathbb{Z}_n \mid (i,n)=1\}| = \varphi(n)$, te je ovim 1° dokazano.

2° Preslikavanje $h: \mathrm{Aut}(\mathbb{Q}(\varepsilon) \mid \mathbb{Q}) \longrightarrow \mathrm{Aut}\, H_n \cong \Phi(n)$ je 1-1, pa kako $|\mathrm{Aut}(\mathbb{Q}(\varepsilon) \mid \mathbb{Q})| = \varphi(n)$, h je <u>na</u>, pa $\mathrm{Aut}(\mathbb{Q}(\varepsilon) \mid \mathbb{Q}) \cong \Phi(n) \cong \mathbb{Z}_n^* \cong \mathrm{Aut}\, C_n$.

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 $a^r=a^{i-qd}=a^i(a^d)^{-q}=xb^{-q}$, 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 $kd\equiv 0 \bmod n$, 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. $\quad C_n=\bigcup_{d|n} S_d$ je disjunktna unija; $S_d=\{b \mid b \text{ je generator cikličke grupe } C_d\}$.

30.4. Zadatak $\quad \sum_{d|n}\varphi(d)=n.$ (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 $n \in N^+$ $\Phi_n(x) = \prod_{\substack{\xi \in C_n \\ \mathrm{red}\,\xi = n}} (x-\xi)$, 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

$$x^n - 1 = \prod_{\xi \in C_n} (x-\xi) = \prod_{d|n} \prod_{\substack{\xi \in C_d \\ \mathrm{red}\,\xi = d}} (x-\xi) = \prod_{d|n} \Phi_d(x), \text{ tj.}$$

30.5. $x^n - 1 = \prod_{d|n} \Phi_d(x)$, $\deg \Phi_d(x) = \varphi(d)$.

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. Primer 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. $\Phi_{p^k}(x) = \sum_{i=0}^{p-1} x^{i p^{k-1}}$

30.7. Möbiusova funkcija: $\mu(n) = \begin{cases} (-1)^k, & n = p_1 \cdot p_2 \cdots p_k, \ p_1, \dots, p_k \text{ prosti} \\ 1, & n = 1 \\ 0, & \text{inače}. \end{cases}$

Teorema $\mu(n)$ je multiplikativna funkcija, tj. $(m,n) = 1 \Rightarrow \mu(mn) = \mu(m)\mu(n)$. ▨

30.8 Teorema Ako je $f(n)$ multiplikativna aritmetička funkcija tada je i $g(n) = \sum_{d|n} f(d)$ multiplikativna aritmetička funkcija.

Dokaz Najpre primetimo da važi

(1) Ako $(m,n) = 1$ tada $d \mid mn \Leftrightarrow \exists d, d' \ (d = dd' \wedge d|m \wedge d'|n)$

Otuda, za $(m,n) = 1$

$$g(mn) = \sum_{d|mn} f(d) = \sum_{d|m, d'|n} f(dd') = \sum_{d|m, d'|n} f(d) f(d') = \Big(\sum_{d|m} f(d)\Big) \cdot \Big(\sum_{d'|n} f(d')\Big) = g(m)\, g(n).$$

Primer $\nu(n) = \sum_{d|n} \mu(d)$ je multiplikativna aritmetička funkcija.

Kao što znamo, vrednosti multiplikativnih funkcija određene su vrednostima u potencijama prostih brojeva. Dakle, za $p \in Prost$, $k \in N$

$$\nu(p^k) = \sum_{d|p^k} \mu(d) = \sum_{i \le k} \mu(p^i) = \mu(1) + \mu(p) + \dots + \mu(p^k) = \begin{cases} \mu(1), & k = 0 \\ \mu(1) + \mu(p), & k \geq 1 \end{cases}, \text{ odakle}$$

$\nu(1) = 1$, $\nu(n) = 0$ za $n > 1$. (Primetimo da je $\nu(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \nu(p_1^{\alpha_1}) \cdots \nu(p_k^{\alpha_k})$ $p_1, \dots, p_k$ različiti prosti brojevi).

30.9. Möbiusova teorema inverzije. Neka je $\mathbb{F}$ polje i $f: N^+ \to F$.
Ako je $g(n) = \sum_{d|n} f(d)$, tada $f(n) = \sum_{d|n} \mu(d)\, g(\frac{n}{d})$, $n \in N^+$.

Dokaz. Najpre primetimo da za $d, d', n \in N^+$ važi:

(1) $d|n \wedge d'|\frac{n}{d} \Leftrightarrow d'|n \wedge d|\frac{n}{d'}$. Odatle

$$\sum_{d|n} \mu(d) g(\tfrac{n}{d}) = \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') = \sum_{d|n,\, d'|\frac{n}{d}} \mu(d) f(d') = \sum_{d'|n,\, d|\frac{n}{d'}} \mu(d) f(d')$$

$$= \sum_{d'|n} f(d') \cdot \sum_{d|\frac{n}{d'}} \mu(d) = \sum_{d'|n} f(d') \nu(\tfrac{n}{d'}) = f(n)\nu(1) = f(n)$$ ▨

30.10. Zadatak. Dokazati da je $\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$ (gauss)

30.11* Zadatak. Dokazati da je $\{ \frac{\varphi(n)}{n} \mid n \in N^+ \}$ gust u $[0,1]_R$.

30.12. Teorema $$\Phi_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}.$$

Dokaz. Iz $x^n - 1 = \prod_{d|n} \Phi_d(x)$ nalazimo $\ln(x^n-1) = \sum_{d|n} \ln \Phi_d(x)$ za one $x \in R$ za koje identitet ima smisla, u svakom slučaju za beskonačno mnogo $x \in R$.

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 $x \in R$, pa s obzirom da se radi o polinomima onda i za svako $x \in R$. ▨

30.13. Zadatak Ponovo uraditi zadatak 30.6. c.

30.14. Zadatak $$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}.$$

30.15. Primer $\sum_{\substack{\xi \in C_n \\ \text{red}\, \xi = n}} \xi = \mu(n)$. 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. $x^n - 1 = 0$.

Dokaz. 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 $\mathbb{C}_n = \{x \in C \mid x^n - 1 = 0\}$, $s_d = \sum_{\xi \in S_d} \xi$. Tada

$\nu(n) = \sum_{k=0}^{n-1} \varepsilon^k = \sum_{\xi \in C_n} \xi = \sum_{d|n} \sum_{\xi \in S_d} \xi = \sum_{d|n} s_d$, te prema Möbiusovoj teoremi inverzije,

$$s_n = \sum_{d|n} \mu(d) \nu(\tfrac{n}{d}) = \mu(n)\nu(1) = \mu(n)$$ ▨

30.16. Ramanujanova suma Dokazati za $m, n \in N^+$ $((m,n) = NZD(m,n))$:

$$\sum_{d|(m,n)} d\mu(\tfrac{n}{d}) = \frac{\mu(\frac{n}{(m,n)})\, \varphi(n)}{\varphi(\frac{n}{(m,n)})}.$$

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 širu i važnu klasu polja, realno zatvorena polja.

31.1. Formalno-realna polja. Polje $\mathbb{F}$ je formalno realno ukoliko u njemu važi:

$$x_1^2+x_2^2+\dots+x_n^2=0 \Rightarrow x_1,\dots,x_n=0, \quad n\in N.$$

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 $\le$ domena $\mathbb{F}$ tako da je $(\mathbb{F},\le)$ uređeno polje, tj. $\le$ je linearno uređenje i saglasno je sa operacijama polja $\mathbb{F}$: $x\le y \Rightarrow x+z\le y+z$; $x\le y,\ 0\le z \Rightarrow xz\le yz$, $x,y,z\in F$.

31.1b Zadatak Neka je $\pi=3.14\ldots$ i $\mathbb{F}=\mathbb{Q}(\pi)$. Dakle, $\pi\in F$.

1° Dokazati da postoji uređenje $\le$ polja $\mathbb{F}$ tako da je $\pi\le 0$.

2° Dokazati da postoji uređenje $\le$ 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 $\underbrace{1^2+\dots+1^2}_{p}=0$, 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 $\mathbb{R}$, $\mathbb{A}\cap\mathbb{R}$ su primeri realno-zatvorenih polja.

31.2a. Zadatak Dokazati da postoji realno-zatvoreno polje $\mathbb{F}$, $\mathbb{F}\not\cong\mathbb{R}$, $\mathbb{F}\not\cong\mathbb{A}\cap\mathbb{R}$.

Realno-zatvorena polja u mnogo čemu slična su polju 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

$$\bigwedge_{\bar{x}\in R} \left(h(\bar{x})\neq 0 \Rightarrow q(\bar{x})\geq 0 \right);$$

ovde je $\bar{x}=x_1,\dots,x_n$ 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 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. Zadatak Dokazati da postoji nearhimedovsko realno-zatvoreno polje.

Od ovog mesta pa do kraja odeljka 31, R će označavati bilo koje realno-zatvoreno polje, dok je $\mathbb{C} = R(i)$, gde je i koren polinoma x^2+1.

31.3. Uređenje polja R. Prema zadatku 31.1a R ima proširenje do uređenog polja. U slučaju polja R dokaz ove činjenice je jednostavan.

31.3a. Lema $\bigwedge_{a,b\in R} \bigvee_{c\in R} a^2+b^2=c^2$.

Dokaz 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. Teorema Neka je $\leq$ relacija domena R definisana sa: $a\leq b$ akko $\bigvee_{c\in R} b=a+c^2$. Tada je $(R,\leq)$ uređeno polje. (U dokazu koji sledi; $a,b,c,d\in R$)

Dokaz 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. Lema 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 Teorema Na $\mathbb{R}$ postoji tačno jedno uređenje tako da je $(R,\leq)$ uređeno polje.

Dokaz Prema 31.3b tako uređenje postoji, to je $(R,\leq)$ gde je $\leq$ konstruisano u 31.3b. Neka je $(R,\preceq)$ bilo koje uređeno polje, i neka su $a,b\in R$. PP $a\preceq b$. Za neki $c\in R$ $a-b=c^2$ ili $b-a=c^2$. Ako je $a-b=c^2$, tada $c^2\preceq 0$, te prema 31.3c 4°, $c=0$, tj. $a=b$. Dakle, $a\preceq b \Rightarrow \bigvee_{c\in R} b=a+c^2$, tj. $a\preceq b\Rightarrow a\leq b$. PP da nije $a\preceq b$. Zbog linearnosti, onda $a\neq b$, $b\preceq a$. Prema već dokazanom onda $b\leq a$. Dakle:

$\bigwedge_{a,b\in R}(a\preceq b \Leftrightarrow a\leq b)$. ∎

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 korenu funkciju:

31.3c <u>Definicija</u> $y = \sqrt{x} \Leftrightarrow x \geq 0 \wedge y \geq 0 \wedge x^2 = y$.

Ovim je f-ja $\sqrt{x}$ dobro definisana na pozitivnom segmentu R^+, $\sqrt{0} = 0$.

31.3d. <u>Zadatak</u> 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 $f: R^+ \cup \{0\} \to R$ tako 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. <u>$\mathbb{C} = R(i)$</u>

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. <u>Lema</u> Za svaki $z \in C$ jednačina $x^2 = z$ ima rešenje u $\mathbb{C}$.

<u>Dokaz</u> 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 <u>Posledica</u> Kvadratne jednačine sa koeficijentima u $\mathbb{C}$ imaju rešenja u $\mathbb{C}$.

31.4d. <u>Zadatak</u> Rešiti jednačinu $x^2 = i$ u $\mathbb{C}$.

31.4e. <u>Zadatak</u> Kako biste uveli funkciju $\sqrt[n]{x}$ za $x \in R$, $x \geq 0$, $n \in N^+$?

31.5. <u>Teorema</u> (Gaus; Artinov dokaz). $\overline{\mathbb{R}} = \mathbb{C}$.

U dokazu ove teoreme koristićemo sledeće tvrđenje.

31.5a. <u>Lema</u> Neka je G konačna p-grupa, tj. $|G| = p^n$, gde je $p \in Prost$, $n \in N^+$.

Tada postoji $H \triangleleft G$ tako da je $|G/H| = p$.

<u>Dokaz</u> Dokaz izvodimo indukcijom po n gde je $|G| = p^n$. Za $n=1$, tvrđenje je trivijalno.

PP $n \geq 2$. Iz klasovne jednakosti $|G| = |Z(G)| + \sum_{\substack{x \in \Gamma \\ x \notin Z(G)}} |G : C(x)|$ 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 $\langle a \rangle \triangleleft G$. Dakle, $G/\langle a \rangle$ je grupa reda $n-1$. Kako je $n \geq 2$, po induktivnoj hipotezi postoji $K \triangleleft G/\langle a \rangle$, $|K| = p^{n-2}$. Neka je $k: G \to G/\langle a \rangle$ kanonski homomorfizam. Tada je $H = k^{-1}(K)$, $H \triangleleft G$, $|H| = p^{n-1}$, dakle, $|G : H| = p$.

∎

<u>Dokaz Teoreme 31.5</u> 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 $a \in E$ 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 $\mathbb{R}$.

$$\mathbb{G}\left(\begin{array}{c} \mathbb{E} \\ \cup\!\!\mathrm{I} \\ \mathbb{C} \\ \cup\!\!\mathrm{I} \\ \mathbb{R} \end{array}\right. \qquad \begin{array}{c} \mathbb{E} \supseteq \mathbb{F} \\ H \end{array}$$

Neka je $\mathbb{G}$ galoaova grupa $\mathbb{E}|\mathbb{R}$, tj. $\mathbb{G} = \mathrm{Aut}(\mathbb{E}|\mathbb{R})$, i neka je $|\mathbb{G}| = 2^n(2m+1)$. Prema Silovljevoj teoremi, postoji 2-podgrupa $H < \mathbb{G}$. 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 $b \in F$ 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 $|\mathbb{G}| = 2^n$.

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 $\mathbb{G}' = \mathrm{Aut}(\mathbb{E}|\mathbb{C})$. Kako je $\mathbb{G}' < \mathbb{G}$ (jer svaki $\sigma \in \mathrm{Aut}\,\mathbb{E}$ koji fiksira $\mathbb{C}$, takođe fiksira i $\mathbb{R}$), to je $\mathbb{G}'$ takođe 2-grupa.

$$\mathbb{G}'\left[\begin{array}{c} \mathbb{E} \\ \cup\!\!\mathrm{I} \\ \mathbb{F}' \\ \cup\!\!\mathrm{I} \\ \mathbb{C} \end{array}\right. \begin{array}{l} \left.\begin{array}{c} \\ \\ \end{array}\right] H' \\ \left.\begin{array}{c} \\ \\ \end{array}\right] \text{gal.} \end{array}$$

Pretpostavimo da je $\mathbb{G}'$ netrivijalna, tj. $|\mathbb{G}'| \geq 2$. Tada prema Lemi 31.5b postoji $H' \triangleleft \mathbb{G}'$, $|\mathbb{G}:H'| = 2$. 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 $H' \triangleleft \mathbb{G}'$, to je i $\mathbb{F}'|\mathbb{C}$ galoaova ekstenzija i $\mathrm{Aut}(\mathbb{F}'|\mathbb{C}) \cong \mathbb{G}'/H'$, 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 $a \in F'$ 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, $\mathbb{G}'$ je trivijalna grupa, pa $|\mathbb{E}:\mathbb{C}| = |\mathbb{G}'| = 1$, tj. $\mathbb{E} = \mathbb{C}$ ■

31.5b* <u>zadatak</u> 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 simetričan 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. Primer Sledeći polinomi su simetrični:

1° $x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2$

2° $\sigma_0 = 1$, $\sigma_1 = -\sum\limits_{1\le i\le n} x_i$, $\sigma_2 = \sum\limits_{1\le i<j\le n} x_ix_j$, $\dots$, $\sigma_k = (-1)^k \sum\limits_{1\le i_1<\dots<i_k\le n} x_{i_1}x_{i_2}\cdots x_{i_k}$, $\sigma_n = (-1)^n\prod\limits_{i=1}^n x_i$.

3° $s_k = \sum\limits_{i=1}^n x_i^k$.

Na isti način definiše se pojam simetričnog racionalnog izraza.

32.2. Osnovna teorema o simetričnim polinomima. 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 $f(x_1,\dots,x_n) = g(\sigma_1,\dots,\sigma_n)$.

Dokaz 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:

1° L i S su podpolja polja K i $\mathbb{F} \subseteq \mathbb{S} \subseteq \mathbb{L} \subseteq \mathbb{K}$.

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 $\mathbb{G} = n!$

Dalje, očevidno je $L = K^{\mathbb{G}}$, te je prema Artinovoj teoremi $\mathbb{K}$ Galoaovo raširenje polja $\mathbb{L}$ i $\mathbb{G} = Aut(\mathbb{K}|\mathbb{L})$. Dakle,

3° $|\mathbb{K} : \mathbb{L}| = n! = \text{red } \mathbb{G}$.

Tvrđenje 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)

$$p_{k-1}(t) = \frac{p_n(t)}{(t-x_k)(t-x_{k+1})\cdots(t-x_n)} = \frac{p_k(t)}{t-x_k}, \quad k = n, n-1,\dots, 2.$$

Dalje, neka je $S_{k-1} = S_k(x_k) = S(x_k, x_{k+1}, \dots, x_n)$, $k = n, n-1, \dots, 1$, $S_n = S$.
Nije teško proveriti sledeće osobine polinoma $p_k(t)$ i polja S_k:

$S = S_n \subseteq S_{n-1} \subseteq \dots \subseteq S_1 \subseteq S_0 = K$.

$p_k(t) \in S_k(t)$, $\deg p_k(t) = k$, $p_k(x_k) = 0$ 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 $p_n(x_k)=0, \dots, p_n(x_n)=0$, pa odatle $p_k(t) \in S(x_{k+1}, \dots, x_n)(t) = S_k(t)$.

Otuda $|S_{k-1} : S_k| \le \deg p_k = k$, odakle je

$|K : S| = |S_0 : S_1| \cdot |S_1 : S_2| \cdots |S_{n-1} : S_n| \le 1 \cdot 2 \cdots n = n!$, tj.

$|K : S| \le n!$, pa $L = S$.

Odavde odmah nalazimo da je zapravo $|K : S| = n!$ i $|S_{k-1} : S_k| = k$.

Neka je $g(x_1, \dots, x_n) \in \mathbb{F}[x_1, \dots, x_n]$ (dakle g je polinom). Ako je g simetričan onda, kako je $L = S$, za neki $\varrho \in S$, $g = \varrho\epsilon$, tj.

$g(x_1, \dots, x_n) = \varrho(\sigma_1, \dots, \sigma_n)$ gde je $\varrho(x_1, \dots, x_n) \in F(x_1, \dots, x_n)$.

Treba dokazati da je $\varrho(x_1, \dots, x_n)$ polinom, za sada imamo samo da je $\varrho(x_1, \dots, x_n)$ racionalan izraz. Neka je $g(x_1, \dots, x_n)$ proizvoljan polinom, dakle ne mora biti simetričan. Prema prethodnom, $p_1(t) \in S(x_2, \dots, x_n)(t) = S_1(t)$, $\deg p_1 = 1$ 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 $\sigma_1, \dots, \sigma_n, x_2, \dots, x_n$, preciznije, $x_1 = g_1(s_1, \dots, s_n, x_2, \dots, x_n)$, gde $g_1(y_1, \dots, y_n, x_2, \dots, x_n) \in F(y_1, \dots, y_n, x_2, \dots, x_n)$. Zamenimo x_1 sa $g_1(s_1, \dots, s_n, x_2, \dots, x_n)$ u $g(x_1, \dots, x_n)$.
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 $x_3, \dots, x_n$ i $\sigma_1, \dots, \sigma_n$ (taj polinom ima koeficijente u $\mathbb{F}$).
Kako je $p_3(x_3) = 0$, x_3^3 i viši stepeni od x_3 mogu se izraziti pomoću polinoma (sa koeficijentima u $\mathbb{F}$) od $x_4, \dots, x_n$ i $\sigma_1, \dots, \sigma_n$.
Vršeći supstituciju x_i sa ovim polinomima vidimo da se $g(x_1, \dots, x_n)$ može izraziti kao polinom od x_i, σ_i tako da je u kanonskom polinomu stepen $x_i \le i-1$, tj.

(*) $$g(x_1, \dots, x_n) = \sum_{\alpha} a_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}, \quad \alpha_i \le i-1, \quad a_\alpha \in S,$$

a_α su polinomi od $\sigma_1, \dots, \sigma_n$.

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
$g = g \cdot x_1^0 \cdots x_n^0$, pa prema (*) i jedinstvenosti reprezentacije (*),
$g(x_1,\dots,x_n) = a_\alpha(\sigma_1,\dots,\sigma_n)$ 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. <u>Zadatak</u> Dokazati da je prema oznakama prethodne teoreme

$$K = S(x_1 + x_2^2 + \dots + x_n^n).$$

32.4. <u>Zadatak</u> 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. <u>Zadatak</u> Izraziti polinom 32.1.1° pomoću polinoma simetričnih funkcija $\sigma_1, \sigma_2, \sigma_3$.

32.6. <u>Zadatak</u> 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 $f(x) = \frac{1}{2}(g(x) + g(a-x))$ $(\mathrm{char}\,\mathbb{F} \neq 2)$
c. $\bigvee_{g \in F[x]} f(x) = g(x(a-x))$.

<u>Napomena</u> posmatrati grupu $G = \{i, \theta_a\}$, $G < \mathrm{Aut}\,\mathbb{F}(x)$, i je identičko preslikavanje, $\theta_a : f(x) \longmapsto f(a-x)$, $f \in F(x)$, primeniti Artinovu teoremu.

32.9. Neka je $f \in C(R)$ (tj. neprekidna f-ja na $\mathbb{R}$). Dokazati

$$\bigwedge_{x \in R} f(x) = f(a-x) \quad \text{akko} \quad \bigvee_{g \in C(R)} f(x) = g(x(a-x))$$

<u>Nap.</u> Primeniti Vajerštrasovu teoremu o aproksimaciji neprekidnih f-ja polinomima.

33. Konstrukcije lenjirom i šestarom

Neka je OA jedinična duž u kompleksnoj ravni $\mathbb{P}$ 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 uvodeće:

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

A4. Presek dve konstruktivne prave je konstruktivna tačka.

A5. Preseci dve konstruktivne kružnice su konstruktivne tačke.

A6. Presek konstruktivne prave i konstr. kružnice je konst. tačka.

Skup konstruktivnih tačaka $\mathbb{P}$ naziva se Pitagorejskom ravni.
Ako je $M(x,y)\in\mathbb{P}$ tada se x, y nazivaju konstruktivnim realnim brojevima.

33.1. Zadatak Dokazati da je $\mathbb{P}$ prebrojiv skup.

Neposredno se proverava.

33.2. Teorema Neka je $\mathbb{K}_R$ skup konstruktivnih realnih brojeva. Tada
$1°$ $\mathbb{K}_R$ je podpolje polja $\mathbb{R}$. $2°$ $\mathbb{P}$ je podpolje polja $\mathbb{C}$, $3°$ $\mathbb{K}_R\subseteq\mathbb{P}\subseteq\mathbb{A}$, $\mathbb{A}$ je polje alg. brojeva.

Neka je $r\in\mathbb{K}_R$ dobije elementarnom konstrukcijom u jednom ~~koraku~~, tj. 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 $r\in\mathbb{K}_R$, tada za neki n $|\mathbb{Q}(r):\mathbb{Q}|=2^n$.

Dokaz Ako je $\mathbb{Q}=\mathbb{F}_0\subseteq\mathbb{F}_1\subseteq\ldots\subseteq\mathbb{F}_m$ 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 $|\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}|=3\neq2^n$ za $n\in\mathbb{N}^+$, $\sqrt[3]{2}$ je dužina ivice veće kocke $(x^3=2\cdot1^3)$.

3° <u>Problem trisekcije ugla</u>: Podeliti ugao na tri jednaka ugla. <u>Konstrukcija nije uvek moguća</u>, 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 Q (jer nema racionalnih korena), dakle $|Q(\cos 20°) : Q| = 3 \neq 2^n$, $n \in N^+$, tj. $\cos 20° \notin \mathcal{K}_R$.

33.5. <u>O konstrukciji pravilnih poligona</u> (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 $|Q(\varepsilon) : Q| = 2^m$ za neki m. S druge strane, vidi odeljak 29, $|Q(\varepsilon) : Q| = \varphi(n) = p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1)(p_2 - 1)\cdots(p_k - 1)$.
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 primalna 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

<u>Teorema</u> Ako je pravilan poligon sa n temena konstruktivan, onda je n proizvod stepena dvojke i Fermaovih prostih brojeva.

<u>Primer</u> Pravilan sedmougao nije konstruktivan, jer $7 \neq 2^{2^n} + 1$ za $n \in N$.

2° Važi i obrat: Ako je n proizvod dvojke i Fermaovih prostih brojeva, onda je pravilan poligon sa n temena konstruktivan.

<u>Dokaz</u> U ovom slučaju $|Q(\varepsilon) : Q| = \varphi(n) = 2^m$. S druge strane, vidi odeljak 29, $Aut(Q(\varepsilon)|Q) = \Phi(n)$ i $\Phi(n)$ je Abelova grupa, dakle rešiva (prema teoremi o dekompoziciji konačnih Abelovih grupa na cikličke) i $Q(\varepsilon)|Q$ je Galoaova. Dakle postoji kompozicioni niz $\langle e \rangle = G_0 \leq G_1 \leq \cdots \leq G_m = Aut(Q(\varepsilon)|Q)$ tako da je $red\, G_i = 2^i$, tj. $|G_{i+1} : G_i| = 2$. Neka su $E_i = Q(\varepsilon)^{G_{m-i}}$. Tada $Q = E_0 \leq E_1 \leq \cdots \leq E_m = Q(\varepsilon)$ 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 $E_0 = Q$, to (indukcijom po i) $E_i \leq \mathcal{K}_R$, tj. $\varepsilon \in \mathcal{K}_R$.

33.6. <u>Zadatak</u> Dokazati da jednakokraki trougao, kod koga je krak $a = 3$, poluprečnik upisanog kruga $\underline{\rho = 1}$, nije konstruktivan.