1. Ako je $\mathbb{F}$ konačno polje, $|\mathbb{F}| = m$, tada svaki polinom $f(x) \in F[x]$, $f(x) = x^2 + bx + c$ ima koren u polju $\mathbb{E} \supseteq \mathbb{F}$, $|\mathbb{E}| = m^2$.

2. a. Neka je $\mathbb{A}$ polje algebarskih brojeva i $\theta : \mathbb{A} \to \mathbb{A}$. Tada $\theta : \mathbb{A} \cong \mathbb{A}$.

b. Navesti primer polja $\mathbb{F}$ takvo da postoji $\theta : \mathbb{F} \to \mathbb{F}$, ali $\theta F \subsetneq F$.

3. Neka je $f(x) \in \mathbb{Q}[x]$, $f(x) = x^6 - 3$. Odrediti Galoisovu grupu polinoma $f(x)$ nad: a) $\mathbb{Q}$, b) $\mathbb{Q}[\varepsilon]$, $\varepsilon = e^{\frac{2\pi i}{3}}$.
Ako je $\mathbb{E}$ korenско polje polinoma $f(x)$, dokazati da postoji međupolje $\mathbb{F}$, $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{E}$, takvo da je $|\mathbb{F} : \mathbb{Q}| = 4$.

4. Odrediti grupu datu prezentacijom

$$\Pi = \langle a, b, c ; a^3 = 1, b^2 = 1, c^2 = 1, ab = ba^2, ac = ca, bc = cb \rangle$$

Kolokvijum Algebra 2, Feb. 2005

1. Neka je $\mathbb{F} = \mathbb{Q}[\sqrt[3]{2} + \varepsilon]$, $\varepsilon = e^{\frac{2\pi i}{3}}$.
   a. Odrediti $|\mathbb{F} : \mathbb{Q}|_s$
   b. Odrediti $\mathrm{Aut}\,\mathbb{F}$.

2. Neka je $\mathbb{F} = \overline{\mathbb{Z}}_p$, $p \in \mathbb{P}rost$. Dokazati da je svaki element multiplikativne grupe $\mathbb{F}^*$ konačnog reda

3. Ispitati da li jednačina $f(x) = 0$ ima [redrawn] rešenje u $GF(2^6)$ ako je:
   a) $f(x) = x^5 + x + 1$
   b) $f(x) = x^8 + x^2 + 1$

4. ~~Dokazati~~ Neka je p prost broj i $\mathbb{F} = GF(p^n)$, $\mathbb{E} = GF(p^q)$. Dokazati da postoji $h : \mathbb{F} \to \mathbb{E}$ akko $n \mid q$.

5. Neka je $f(x) \in \mathbb{Z}_p[x]$ i $\mathbb{E} \supseteq \mathbb{Z}_p$ konačno proširenje. Dokazati da je $\prod_{a \in E} f(a) \in \mathbb{Z}_p$.

P1. Teorema o primitivnom elementu:
Ako je $\mathbb{E} \supseteq \mathbb{F}$ konačno separabilno proširenje tada postoji $a \in \mathbb{E}$ takvo da je $\mathbb{E} = \mathbb{F}[a]$.

P2. Ako je $\mathbb{E}$ algebarsko proširenje polja $\mathbb{F}$, tada postoji $h : \mathbb{E} \to \overline{\mathbb{F}}$ takvo da je $h|_{\mathbb{F}} = i_{\mathbb{F}}$.

$$\begin{array}{ccc} \mathbb{E} & \xrightarrow{h} & \overline{\mathbb{F}} \\ \cup & \nearrow & \\ \mathbb{F} & & \end{array}$$

Algebra II 1 Sept. 2005
Okt. 2005

1. Galoisova grupa polinoma $f(x) = x^5 - 2$, $f \in \mathbb{Q}[x]$.
2. Odrediti sva podpolja polja $GF(32)$.
3. Ako su H, K rešive podgrupe grupe G i $H \lhd G$, tada je HK rešiva (podgrupa).
4. Neka je $\mathfrak{B}_n$ slobodna Bulova algebra sa n slobodnih generatora. Dokazati da je $\mathfrak{B}_n \cong 2^{2^n}$. 2 je dvočlana Bulova algebra

Literatura: Algebarska proširenja polja

Други колоквијум из Алгебре 2

1. Нека је $\xi = e^{\frac{2\pi i}{15}}$.
а) Одредити $[\mathbf{Q}(\xi) : \mathbf{Q}]$ и минимални полином за ξ над $\mathbf{Q}$.
б) Нека је G група Галоа минималног полинома за ξ над $\mathbf{Q}$. Показати да је G изоморфна директном производу две цикличне групе. Описати елементе групе G и наћи њихове редове.

2. Нека је $L|F$ Галоаово раширење чија је Галоаова група $G = G(L|F)$. Нека су H_1, H_2 подгрупе од G и $H_1 \cap H_2 = \{e\}$. Нека је K_i фиксно поље за H_i. Доказати да је $K_1K_2 = L$, где је K_1K_2 најмање потпоље од L које садржи K_1 и K_2.

3. Нека су M и N нормалне подгрупе групе G и нека су G/M и G/N решиве групе.
а) Доказати да је $N/(M \cap N)$ решива група.
б) Доказати да је $G/(M \cap N)$ решива група.

4. Одредити групу задату презентацијом
$\Pi =< a, b, c \mid a^3 = 1, b^2 = 1, c^2 = 1, b^{-1}ab = a^{-1}, ac = ca, bc = cb >$.

Теорија:
1. Слободне алгебре

24. 9. 2004. u 9:00

ALGEBRA 2

1. Odrediti Galuaovu grupu polinoma $f(x) = x^4 - 5, f(x) \in \mathbb{Q}[x]$: nad $\mathbb{Q}, \mathbb{Q}(\sqrt{5}), \mathbb{Q}(i)$.

2. Neka je G grupa reda $2k$, $k \in 2\mathbb{N} + 1$. Dokazati da G nije prosta.

3. Ako je $\mathbb{C}$ polje kompleksnih brojeva, dokazati da postoji polje $E \subset \mathbb{C}$ tako da:

   i)$\mathbb{C}$ je algebarsko nad E,

   ii) svaki polinom $f(x) \in E[x]$ neparnog stepena ima koren u E,

   iii) $\sqrt{3} \notin E$.

4. Odrediti slobodnu algebru $\mathbf{A}$ jezika L, nad skupom K slobodnih generatora, klase zakona Z, gde je: $L = \{1, \cdot, ^{-1}\}$, Z: aksiome grupe, $x^2 = 1$, $K = \{a_1, a_2, \cdots, a_n\}$.

5. Teorema o primitivnom elementu.

Algebra II : I grupa zadataka

Rok: 28.12.2004

L 1. Neka je $f(x) \in \mathbb{F}[x]$, gde $\mathbb{F} = GF(2)$, $f(x) = x^4 + x + 1$. Dokazati da je f nesvodljiv nad $\mathbb{F}$ i navesti tablice aperacija Kroneckerove ekstenzije $\mathbb{F}[b]$.

L 2. Ako je $\mathbb{F} = GF(24)$, $\sqrt[n \in 2N+1,]{a}, b \in \mathbb{F}$ i $a^2 + ab + b^2 = 0$ u $\mathbb{F}$, dokazati da $a = 0, b = 0$.

L 3. a. Ako svaka kvadratna jednačina $x^2 + bx + c = 0$ ima rešenje u polju $\mathbb{F}$, dokazati da je $\mathbb{F}$ beskonačno polje.

b. Ako je $\mathbb{F}$ konačno polje, $|\mathbb{F}| = m$, dokazati da svaki polinom $f(x) \in \mathbb{F}[x]$ $f(x) = x^2 + bx + c$ ima koren u polju $\mathbb{E} \supseteq \mathbb{F}$, $|\mathbb{E}| = m^2$.

L 4. a. Polinom $f(x) = x^8 + x^7 + x^3 + x + 1$ je nesvodljiv nad $\mathbb{Z}_2$.

b. Polinom $f(x) = x^8 - 5x^7 + 3x^3 + x - 1$ je nesvodljiv nad $\mathbb{Q}$.

c. Polinom $f(x) = a_0 x^8 + a_1 x^7 + a_2 x^3 + a_4 x + a_5$, $a_0, \dots, a_5 \in 2\mathbb{Z}+1$, je nesvodljiv nad $\mathbb{Q}$.

L 5. Ako je $f(x) = 1 + x + x^2 + \dots + x^{n-1}$ nesvodljiv nad poljem $\mathbb{F}$, dokazati $n \in Pros$.

L 6. Ako je $x^n - 1 = (x - a_1)(x - a_2) \cdots (x - a_n)$ u polju $\mathbb{F}$, dokazati

$$a_1^k + a_2^k + \dots + a_n^k = 0, \quad k = 1, 2, \dots, n-1.$$

L 7. a. Ako je $\mathbb{A}$ polje algebarskih brojeva i $\theta : \mathbb{A} \to \mathbb{A}$, dokazati $\theta : \mathbb{A} \cong \mathbb{A}$.

b. Navesti primer polja $\mathbb{F}$ takvog da postoji $\theta : \mathbb{F} \to \mathbb{F}$, ali $\theta\mathbb{F} \subsetneq \mathbb{F}$.

8. Ako je $\mathbb{A}$ polje algebarskih brojeva, dokazati $|Aut\,\mathbb{A}| = 2^{\aleph_0}$.

L 9. a. Ispitati da li je $f(x) = x^4 - 5x^3 + 6x^2 + 4x - 8$ separabilan nad $\mathbb{Q}$.

b. Ispitati da li je $f(x) = x^6 + x^5 + x^4 + x^3 + 1$ separabilan nad $GF(2)$.

10. Neka je $\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$. Dokazati da je $\mathbb{Z}[\omega]$ euklidski prsten sa normom $\delta(a + b\omega) = a^2 - ab + b^2$. Odrediti jedinice (invertibilne elemente) u $\mathbb{Z}[\omega]$. Dokazati: Ako je $a + b\omega \in \mathbb{Z}[\omega]$, $a, b \neq 0$, tada $a + b\omega$ je prost u $\mathbb{Z}[\omega]$ akko $a^2 - ab + b^2$ prost u $\mathbb{Z}$. Prost $p \in \mathbb{Z}$ je prost u $\mathbb{Z}[\omega]$ akko $p = 2$ ili $p = 5 \pmod 6$.

11.* Naći primere polja $\mathbb{K}, \mathbb{L}$ takve da je $(K, +_K, 0_K) \cong (L, +_L, 0_L)$ i $\mathbb{K}^* \cong \mathbb{L}^*$ ali $\mathbb{K} \not\cong \mathbb{L}$

12.* Ako je $\mathbb{F}$ polje i $f : F^n \xrightarrow[1:1]{} F^n$ polinomijalno, onda $f : F^n \xrightarrow{na} F^n$.

13. Ako je $\mathbb{A}$ polje algebarskih brojeva, dokazati da postoji $\theta \in Aut(\mathbb{A})$ takvo da je $\theta(\sqrt{3} + \sqrt{5} + \sqrt{7}) = \sqrt{3} - \sqrt{5} + \sqrt{7}$.

6. $x^n-1=(x-a_0)\cdots(x-a_{n-1})$, $a_0=1$, $a_1=\varepsilon$, $a_k=\varepsilon^k$, $k=0,1,\dots,n-1$

$a_1^k+\dots+a_n^k = 1+\varepsilon^k+\varepsilon^{2k}+\dots+\varepsilon^{k(n-1)} = \frac{1-\varepsilon^{kn}}{1-\varepsilon} = \frac{1-1}{1-\varepsilon}=0$

3a. 1° $kF>2$, $f: F\to F$, $fx=x^2$. Ako je F konačno tada je f ne onda je 1-1, jer npr. $x^2=1$, $x\in\{1,-1\}$.

2° $kF=2$. pp. F konačno, $|F|=k$, $F=\{a_1,\dots,a_k\}$. Polin. x^2+bx+c ima k^2. Ako je $b=a_k$, red. i d je zbroj red. x^2+a_kx+c, tada d ima dugo zbroj ove vrste. Ako je

$S=\{d\in F \mid \bigvee_{b,c\in F} d^2+bd+c=0\}$, onda $|S|\le 2k$ a ima $k^2>2k$.

Tada neke vrste polin. $f(x)=x^2+bx+c$, $g(x)=x^2+b'x+c'$, koji imaju isti zbroj nula, za $f=g$, $\not\Leftarrow$.

6. $F=GF(p^k)$, $E=GF(p^{2k})$.
Ako $f(x)=x^2+bx+c$ nema nula u F, onda je $f(x)$ nesv. i $f(x)$ ima nula u $F(b)$, $|F(b):F|=2$, tj. $|F(b)|=n^2$. Znači $\exists$ nesvedljiv polinom $F(b)$ ove vrste (Dokaz).

5. $g(x)=f(x)(x-1)=x^n-1$. Ako n nije prost, $n=kl$, $k,l>1$, onda $g(x)=(x^k)^l-1=(x^k-1)(\dots)$ $\not\Rightarrow$ tj. $f(x)=(x^{k-1}+\dots+x+1)(\dots)$ tj. $f(x)$ nije nesvedljiv.

2. Ako $b\neq 0$, onda $d^2+d+1=0$, $d=a/b$ $d^3-1=0$, red $d=3$, $3\nmid 2^n-1$ ako je n neparan ($2^n=1=(-1)^n-1=-2\neq 0$)

4. $x^2+x+1=0$, $b^2+b+1=0$ u $\mathbb{Z}_2[b]$

$b^8+b^7+b^3+b+1 = b^7(b+1)+b^3+b^2 = b^8+b^2(b+1)=b^8+b^3=b^3(b^5+1)$

$=b^3(b+1)(b^4+b^3+b^2+b+1)=b^3(b+1)(b^4+b^3)=b(b+1)\,b^3\cdot b^2\cdot b^3(b+1)=b^3\cdot b^2b^3b^2\neq 0$

2: x^2+x+1 nesv. $x^2+x+1=x^4+x^2+1$

3: x^3+x+1, x^3+x^2+1

4: $x^4+1+q(x)$, $\deg q\le 3$, $x\nmid q(x)$ nep. $\Rightarrow$ nul. $\Rightarrow$ x, x^2, x^3, $x+x^2+x^3$

Algebra II : 1. kolokvijum (mart 2004)

Z1. Neka je $\mathbb{F}$ konačno polje. Izračunati u polju $\mathbb{F}$

$$S = \sum_{\substack{a \in F \\ a \neq \pm 1}} \frac{1}{1-a^2} \quad \left(= \sum_{a \in X} \frac{1}{1-a^2}, \; X = F \setminus \{1, -1\} \right)$$

Z2. Neka je $\mathbb{A} = (A, +, \cdot, 0, 1)$ polje algebarskih brojeva. Dokazati da je za svaki $n \in \mathbb{N}^+$

$$(A, +, 0)^n \cong (A, +, 0).$$

Z3. Neka je $\mathbb{E}$ proširenje polja $\mathbb{F}$ i neka je

$$L = \{x \in E \mid x \text{ je separabilan nad } \mathbb{F}\}.$$

Dokazati da je L potpolje polja $\mathbb{E}$.

Z4. Neka je $f(x) = x^4 + 1$. Odrediti: $f(x) \in \mathbb{Q}[x]$

a. Korensko polje polinoma $f(x)$. Objasniti zašto možemo uzeti $\mathbb{F} \subseteq \mathbb{C}$.
$\mathbb{F} \subseteq \mathbb{C}$

b. $|\mathbb{F} : \mathbb{Q}|_s$.

c. Primitivan element proširenja $\mathbb{F} \supseteq \mathbb{Q}$, tj. element $a \in F$ takav da je $\mathbb{F} = \mathbb{Q}(a)$.

d. Odrediti $\mathrm{Aut}\,\mathbb{F}$

Dokazati da je $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{F}$.

P1. Konačna polja

P2. Separabilan stepen.

21. R $\frac{1}{1-a^2} = \frac{1}{(1-a)(1+a)} = \frac{1}{2}\left(\frac{1}{1-a} + \frac{1}{1+a}\right)$ (kF ≠ 2)

$S = \sum_{a \in X} \frac{1}{1-a^2} = \frac{1}{2}\left(\sum_a \frac{1}{1-a} + \sum_a \frac{1}{1+a}\right)$ $\quad X = F \setminus \{1, -1\}$

$a \mapsto \frac{1}{1+a}$, $a \in X$, $\theta : X \xrightarrow[1-1]{} F$ $\quad \theta(X) = F \setminus \{0, 1/2\}$

$|X| = |F| - 2$

$\sum_{a \in X} \frac{1}{1+a} = \sum_{b \in F \setminus \{1/2\}} b = \sum_{b \in F} b - \frac{1}{2} = 0 - \frac{1}{2} = -\frac{1}{2}$ для $x \neq -x$ и $x \neq 0$

$\sum_{a \in X} \frac{1}{1-a} = \sum_{b \in \dots} \frac{1}{1-a} = \sum_{b \in F} b - \frac{1}{2} = -\frac{1}{2}$

$S = \frac{1}{2}\left[-\frac{1}{2} - \frac{1}{2}\right] = -\frac{1}{2}$

z_3: $S = \frac{1}{1-0^2} = \frac{1}{1-0} = 1$

z_5: $S = \frac{1}{1-0^2} + \frac{1}{1-2^2} + \frac{1}{1-3^2} = 1 + \frac{1}{3} - \frac{1}{3} = 1 - \frac{2}{3}$

$= 1 - 4 = -3$

1. kF = 2

$\frac{1}{1-a^2} = \frac{1}{1+a^2} = \left(\frac{1}{1+a}\right)^2$

$S = \sum_{a \in X} \frac{1}{1-a^2} = \sum_{a \in F \setminus \{1\}} \left(\frac{1}{1+a}\right)^2 = \sum_{i \in F^*} i^2 = \left(\sum_{i \in F^*} i\right)^2$

$0, 1, b, 1+b$

$i^2 = j^2 \Rightarrow i = j \vee i = -j$

$\Rightarrow i = j$

$S = \sum_{i \in F^*} i^2 = \sum_{i \in F^*} i$

$a \in S \setminus \{0, 1\}$

$aS = \sum_{i \in F^*} ai = \sum_{i \in F^*} i = S$

$aS = S$, $S(a-1) = 0$, $S = 0$

z_2: $S = 1$

$GF(2^n)$, $n \geq 2$: $S = \left(\sum_{0 \leq i \leq 2^n - 1} b^i\right)^2 = \left(1 + b + \dots + b^{2^n - 1}\right)^2 = \left(\frac{b^{2^n} - 1}{b - 1}\right)^2 = 0$

z_4: $F = z_3$

$\frac{1}{1-0^2} = 1$

2. kF > 2 $\quad x \neq -x$, $-(-x) = x$ $\quad F^* = \bigcup_{a \in T} \{a, -a\}$, $2|T| = |F| - 1 = |F^*|$

$\sum_{i \in F} i = 0$; $\sum_{i \in F} i = \sum_{a \in T} (a + (-a))$

22. R. $A_Q = ((A, +, 0), Q, \cdot)$, $\dim A_Q = \aleph_0$

$V_Q = A_Q \times A_Q$, $\dim V_Q = \aleph_0$ $\quad V_Q \cong A_Q$

$V_Q = ((A, +, 0)^2, Q, \cdot)$

Дальше, $(A, +, 0)^2 \cong (A, +, 0)$

$(A, +, 0)^3 = (A, +, 0) \times (A, +, 0)^2 \cong (A, +, 0) \times (A, +, 0) \cong (A, +, 0)$

Algebra 2 Domaći zadatak 11.04.2005

ponedeljak 25.04.2005, 16½

1. Odrediti grupu Galua za x^3-x-1 nad $\mathbb{Q}$. Ako je $\mathbb{E}$ korenско polje polinoma $f(x)=x^3-x-1$, odrediti sva međupolja i ispitati koja su od njih Galoisova.

2. Neka je $f(x)=x^6-2$, $f(x)\in\mathbb{Q}[x]$, i neka je $\mathbb{E}$ korenско polje polinoma $f(x)$. Odrediti $G=Aut(\mathbb{E}/\mathbb{Q})$ i sva međupolja i ispitati koja su od njih Galoisova.

3. Odrediti Galoisovu grupu polinoma $f(x)=x^6+x^3+1$ nad $\mathbb{Q}$.

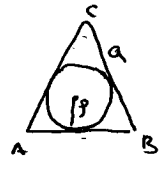
4. Neka je $\mathbb{E}/\mathbb{F}$ Galoisovo proširenje i $G=Aut(\mathbb{E}/\mathbb{F})$. Ako je $|G|=p^n$, p je prost broj, tada postoji međupolje L, $\mathbb{F}\subseteq\mathbb{L}\subseteq\mathbb{E}$, tako da je $|\mathbb{E}:\mathbb{F}|=p$ i $\mathbb{E}/\mathbb{F}$ je Galoisovo.

5. Neka je $\mathbb{E}$ korenско polje ~~polinoma~~ separabilnog polinoma $f(x)\in\mathbb{F}[x]$. Ako je $G=Aut(\mathbb{E}/\mathbb{F})$ i G ima element reda 7, tada je $\deg f\geq 7$.

6. Neka su m,n uzajamno prosti prirodni brojevi. Ako je $\varepsilon=e^{\frac{2\pi i}{m}}$, $\eta=e^{\frac{2\pi i}{n}}$ tada $\mathbb{Q}[\varepsilon]\cap\mathbb{Q}[\eta]=\mathbb{Q}$.

7. Neka je $\mathbb{F}$ polje karakteristike 2 i $f(x)\in\mathbb{Z}_2[x]$ separabilan polinom. Ako je $f(x)=\prod(x-x_i)$ rastavljen u $\overline{\mathbb{Z}_2}$, tada $\prod_{i<j}(x_i+x_j)=1$.

8. Da li je ravnokraki trougao sa krakom a i poluprečnikom upisanog kruga $\rho=1$ konstruktivan ako je: 1. $a=3$, 2. $a=4$.
* Za koje celе brojeve a je ovaj trougao konstruktivan?



9.* Neka je $n\in\mathbb{N}^+$. Dokazati da postoji galoisovo proširenje $\mathbb{E}$ polja racionalnih brojeva $\mathbb{Q}$ tako da je $Aut(\mathbb{E}/\mathbb{Q})=C_n$.

10. Dokazati da je jednačina $x^7-1=0$ rešiva u radikalima nad $\mathbb{Q}$. Rešiti tu jednačinu u radikalima (nad $\mathbb{Q}$) i izračunati u radikalima $\cos\frac{2\pi}{7}$.

11. Izračunati grupu Galua za $f(x)=x^4-5$, $f(x)\in\mathbb{Q}[x]$ nad $\mathbb{Q}$, $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[i]$.

12.* Neka je $\mathbb{E}$ polje dobijeno iz $\mathbb{Q}$ adjunkcijom svih n-tih korena iz jedinice, $n\in\mathbb{N}$.
a. Dokazati da za svaki $a\in\mathbb{Z}$ jednačina $x^2-a=0$ ima rešenje u $\mathbb{E}$.
b. Dokazati da je $Aut(\mathbb{E}/\mathbb{Q})$ merdi kontinuuma.

Algebra 2 (predrok, 2003)

1. Neka je G rešiva grupa i neka je $f: \mathbb{K} \longrightarrow G$ homomorfizam. Ako je $\ker f$ rešiva grupa, tada je i $\mathbb{K}$ rešiva grupa.

2. Neka je $\mathbb{E}$ galoisovo proširenje polja $\mathbb{F}$ i neka je $\mathrm{Aut}(\mathbb{E}|\mathbb{F})$ ciklička grupa reda n. Dokazati:
   a. Ako $d|n$ tada postoji tačno jedno međupolje $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{E}$ t.d. $|\mathbb{E}:\mathbb{L}| = d$.
   b. Ako su $\mathbb{F} \subseteq \mathbb{K}, \mathbb{L} \subseteq \mathbb{E}$ međupolja, tada $\mathbb{L} \subseteq \mathbb{K}$ akko $|\mathbb{E}:\mathbb{K}|$ deli $|\mathbb{E}:\mathbb{L}|$.

3. Odrediti grupu zadatu prezentacijom:
   $\Pi = \langle a, b, c;\ a^3=1,\ b^2=1,\ c^2=1,\ a^b = a^{-1},\ ac=ca,\ bc=cb \rangle$.

4. Odrediti Bulovu algebru zadatu prezentacijom
   $\Pi = \langle a, b, c;\ abc = a+b+c \rangle$.

Pitanja

1. Galoisove grupe kubne jednačine
2. Slobodne algebre.

Zadaci iz teorije polja

1. Odrediti Galuaovu grupu polinoma $f(x) = x^3 - x - 1$ nad poljem Q. Ako je E korensko polje polinoma f, odrediti sva međupolja i ispitati koja su od njih Galuaova.

2. Neka je $f(x) = x^6 - 2$ polinom nad poljem Q i neka je E korensko polje polinoma f. Odrediti grupu $\mathrm{Aut}\,(E|Q)$, sva međupolja F, $Q \subseteq F \subseteq E$, i ispitati koja su od njih Galuaova.

3. Odrediti Galuaovu grupu polinoma $f(x) = x^6 + x^3 + 1$ nad poljem Q.

4. Neka je $E|F$ Galuaovo raširenje polja F i $G = \mathrm{Aut}\,(E|F)$. Ako je p prost broj i $|G| = p^n$, $n \geq 1$, onda postoji međupolje L, $F \subseteq L \subseteq E$, takvo da je $L|F$ je Galuaovo raširenje polja F i $|L : F| = p$.

5. Neka je E korensko polje separabilnog polinoma $f \in F[x]$. Ako grupa $\mathrm{Aut}\,(E|F)$ ima element reda 7, onda je $\deg(f) \geq 7$.

6. Ako su m i n uzajamno prosti prirodni brojevi, $\varepsilon = e^{\frac{2\pi i}{m}}$ i $\eta = e^{\frac{2\pi i}{n}}$, onda je $Q(\varepsilon) \cap Q(\eta) = Q$.

7. Neka je $f \in Z_2[x]$ separabilan polinom i $\overline{Z}_2$ algebarsko zatvorenje polja Z_2. Ako je $\prod_i (x - x_i)$ razlaganje polinoma f u polju $\overline{Z}_2$, onda je

$$\prod_{i<j} (x_i + x_j) = 1.$$

8. Da li se može konstruisati ravnokraki trougao sa krakom a i poluprečnikom upisanog kruga $\varrho = 1$ ako je $a = 3$, odnosno, ako je $a = 4$. Za koje cele brojeve a je takav trougao konstruktibilan?

9*. Neka je $n \geq 1$. Dokazati da postoji Galuaovo raširenje E polja racionalnih brojeva Q tako da je $\mathrm{Aut}\,(E|Q) = C_n$.

10. Dokazati da je jednačina $x^7 - 1 = 0$ rešiva u radikalima nad poljem Q, rešiti tu jednačinu u radikalima nad Q i izračunati u radikalima $\cos\frac{2\pi}{7}$.

11. Naći Galuaovu grupu polinoma $f(x) = x^4 - 5$ nad Q, $Q[\sqrt{5}]$ i $Q[i]$.

12*. Neka je E polje dobijeno iz Q adjunkcijom svih korena jedinice. Pritom, ε je koren jedinice ako $\varepsilon^n = 1$, za neko $n \geq 1$. Dokazati da za svako $a \in Z$, jednačina $x^2 - a = 0$ ima rešenje u E. Dokazati da grupa $\mathrm{Aut}\,(E|Q)$ ima moć kontinuuma.

13. Neka je $q > 0$ racionalan broj. Odrediti Galuaovu grupu polinoma $f(x) = x^4 - q$.

14. Neka je $f(x) = x^4 + 1$ polinom nad poljem Q. Odrediti korensko polje F polinoma f. Odrediti primitivni element raširenja $F \supseteq Q$, odnosno element $a \in F$ takav da je $F = Q(a)$. Odrediti $\mathrm{Aut}\,(F)$. Dokazati da je $Q(\sqrt{2}) \subseteq F$.

15*. Neka je $f(x) = x^5 - 2$ polinom nad poljem Q i neka je E korensko polje polinoma f. Odrediti grupu $G = \mathrm{Aut}\,(E|Q)$. Odrediti sva Galuaova međupolja L, $Q \subseteq F \subseteq E$. Naći potpolja $L_1, L_2 \subseteq E$, takva da $|L_1 : Q| = 10$ i $|L_2 : Q| = 5$.

Ispitna pitanja iz teorije polja

1. Prsteni i ideali,
2. Stepen raširenja polja,
3. Algebarsko raširenje polja,
4. Osobine prstena polinoma nad datim poljem,
5. Kronekerova konstrukcija (egzistencija i jedinstvenost),
6. Korensko polje polinoma (egzistencija i jedinstvenost),
7. Konačne podgrupe grupe F^*,
8. Konačna polja,
9. Automorfizmi konačnih polja,
10. Algebarski zatvorena polja i algebarsko zatvorenje,
11. Teorema o primitivnom elementu separabilnih raširenja,
12. Kubna jednačina,
13. O rešivosti algebarskih jednačina pomoću radikala,
14. Galuaova raširenja,
15. Primer algebarske jednačine koja nije rešiva pomoću radikala.
16. Geometrijske konstrukcije lenjirom i šestarom
17. Separabilni stepen,
18. Ciklotomični polinomi i polja $Q[\varepsilon]$, $\varepsilon^n = 1$.
19. Gausova lema i kriterijumi nesvodljivosti polinoma.
20. Primene u teoriji brojeva (Mala Fermaova teorema, Vilsonova teorema, ojlerova funkcija $\varphi(n)$.

Uputstva za izradu zadataka iz teorije polja

Ključna teorema u svim zadacima jeste *Osnovna teorema teorije Galua:*

- Ako je E Galuaovo raširenje polja F i L međupolje, $F \subseteq L \subseteq E$, onda je E Galuaovo raširenje polja L i $Aut(E|L)$ je podgrupa grupe $Aut(E|F)$.

- Polje L je Galuaovo raširenje polja F ako i samo ako $Aut(E|L)$ je normalna podgrupa grupe $Aut(E|F)$.

1. Pogledati šta je rečeno o jednačini trećeg stepena i dokazati da koreni polinoma $f(x) = x^3 - x - 1$ nisu svi realni. Dakle, neka su $b \in R$ i $\varepsilon, \overline{\varepsilon} \in C \backslash R$ koreni polinoma f, tj. $E = Q(b, \varepsilon)$.

Kako su koreni ε i $\overline{\varepsilon}$ su konjugovano kompleksni brojevi, njihov minimalni polinom m_ε je kvadratni polinom. Pritom polinom m_ε nije svodljiv nad $Q(b)$. Kako je polinom f nesvodljiv nad Q, minimalni polinom za b je $m_b = f$. Otuda sledi da grupa Aut $(E|Q)$ ima 6 elemenata (zašto?). Svi njeni elementi su redom:

$$\begin{aligned} e &: b \mapsto b, \varepsilon \mapsto \varepsilon, \overline{\varepsilon} \mapsto \overline{\varepsilon}, \\ \sigma &: b \mapsto b, \varepsilon \mapsto \overline{\varepsilon}, \overline{\varepsilon} \mapsto \varepsilon, \\ \varrho &: b \mapsto \varepsilon, \varepsilon \mapsto \overline{\varepsilon}, \overline{\varepsilon} \mapsto b, \\ \rho^2 &: b \mapsto \overline{\varepsilon}, \varepsilon \mapsto b, \overline{\varepsilon} \mapsto \varepsilon, \\ \sigma\rho &: b \mapsto \overline{\varepsilon}, \varepsilon \mapsto \varepsilon, \overline{\varepsilon} \mapsto b, \\ \sigma\rho^2 &: b \mapsto \varepsilon, \varepsilon \mapsto b, \overline{\varepsilon} \mapsto \overline{\varepsilon}, \end{aligned}$$

Očigledno se radi o grupi $D_3 \cong S_3$. Njene podgrupe reda 2 su redom $G_1 = \{e, \sigma\}$, $G_2 = \{e, \sigma\rho\}$ i $G_3 = \{e, \sigma\rho^2\}$. Nijedna od njih nije normalna podgrupa grupe D_3 pa nijedno od međupolja $L_1 = E^{G_1}$, $L_2 = E^{G_2}$, $L_3 = E^{G_1}$ nije Galuaovo. Pritom $L_1 = Q(b)$ jer $\sigma(b) = b$, $L_2 = Q(\varepsilon)$ jer $\sigma\rho(\varepsilon) = \varepsilon$, a $L_3 = Q(\varepsilon)$ jer $\sigma\rho(\overline{\varepsilon}) = \overline{\varepsilon}$.

Jedina podgrupa reda 3 je $G_4 = \{e, \rho, \rho^2\}$, ona je normalna u grupi D_3, a njeno fiksno polje je $L_4 = E^{G_4}$ jeste Galuaovo međupolje. Kako je

$$\rho(b + \varepsilon + \overline{\varepsilon}) = \rho^2(b + \varepsilon + \overline{\varepsilon}) = b + \varepsilon + \overline{\varepsilon},$$

to je konačno $L_4 = Q(b + \varepsilon + \overline{\varepsilon})$.

2. Ako je $b = \sqrt[6]{2}$, svi koreni polinoma f su b, εb, $\varepsilon^2 b$, $\varepsilon^3 b$, $\varepsilon^4 b$ i $\varepsilon^5 b$, gde je $\varepsilon = e^{\frac{2\pi i}{6}} = e^{\frac{\pi i}{3}}$ koren iz jedinice ($\varepsilon^6 = 1$). To znači da je $E = Q(b, \varepsilon)$

korensko polje polinoma f. Minimalni polinom elementa b nad poljem Q je upravo polinom f (objasniti zašto).

Kako je $x^6 - 1 = (x-1)(x+1)(x^2-x+1)(x^2+x+1)$ i kako su ε i $\varepsilon^5 = \bar{\varepsilon}$ koreni nesvodljivog polinoma $m_\varepsilon(x) = x^2 - x + 1$, to je m_ε minimalni polinom za ε nad poljem Q, odnosno i nad poljem $Q(b)$. Otuda sledi da je $[E : Q] = 12$ (zašto?), pa Galuaova grupa $G = \mathrm{Aut}\,(E|F)$ ima 12 elemenata. Pritom $12 = 3 \cdot 2^2$, pa možemo koristiti Silovljeve teoreme za određivanje njenih podgrupa.

Ako je $\sigma : b \mapsto b, \varepsilon \mapsto \varepsilon^5$ i $\rho : b \mapsto b\varepsilon, \varepsilon \mapsto \varepsilon$, gde je $\varepsilon^5 = \bar{\varepsilon}$, onda je Galuaova grupa automorfizama

$$\mathrm{Aut}\,(E|Q) = \{e, \sigma, \rho, \rho^2, \rho^3, \rho^4, \rho^5, \sigma\rho, \sigma\rho^2, \sigma\rho^3, \sigma\rho^4, \sigma\rho^5\} \cong D_6.$$

Strukturne jednakosti grupe D_6 su $\sigma^2 = 1$, $\rho^6 = 1$ i $\rho\sigma = \sigma\rho^5$. Ona ima sedam podgrupa reda dva: šest podgrupa oblika $H_i = (\sigma\rho^{i-1})$, za $i = 1, \ldots, 6$, koje nisu normalne jer $\rho H_i \rho^{-1} \neq H_i$ (proveriti!), kao i grupu $H_7 = (\rho^3)$, koja jeste normalna (proveriti!).

Podgrupa H_7 je normalna, pa su $V_1 = H_7 \cdot H_1$, $V_2 = H_7 \cdot H_2$ i $V_3 = H_7 \cdot H_3$ podgrupe reda 4 grupe D_6. Pritom, podgrupe $V_i \cong C_2 \times C_2$ nisu normalne podgrupe u D_6 (dokazati). Takođe, to su sve podgrupe (Klajnove grupe) reda 4 u grupi D_6 (zašto?).

Grupa $K_1 = (\rho^2) = \{e, \rho^2, \rho^4\}$ je jedina podgrupa reda 3 u grupi D_6 (zašto?), pa mora biti normalna (zašto?).

Grupe $G_1 = K_1 \cdot H_1$, $G_2 = K_1 \cdot H_2$ i $G_3 = K_1 \cdot H_7$ su sve podgrupe reda 6, pa su normalne u D_6.

Polje E^{H_1} je fiksno za automorfizam $\sigma : b \mapsto b$, pa je $E^{H_1} \supseteq Q(b)$, ali kako je $[E : E^{H_1}] = |H_1| = 2$, to mora biti $E^{H_1} = Q(b)$. Pritom, $Q(b)$, nije Galuaovo međupolje.

Dokazati da je $E^{H_2} = Q(b^4, \varepsilon)$ i $E^{H_3} = Q(b^3, b^2\varepsilon)$. Pritom, to nisu Galuaova međupolja.

Razmotrimo polje E^{H_4}. Kako je $E = Q(b, \varepsilon) = Q(b)(\varepsilon) = \{a + c\varepsilon\}$, gde je $a = a_1 + a_2 b + a_3 b^2 + a_4 b^3 + a_5 b^4 + a^6 b^5$, $c = c_1 + c_2 b + c_3 b^2 + c_4 b^3 + c_5 b^4 + c^6 b^5$, za $a_i, c_i \in Q$. Za svako $e \in E$, ako $e = \sigma\rho^3(\epsilon)$, onda zbog $\sigma\rho^3(b) = \varepsilon^3 b$ i $\sigma\rho^3(\varepsilon) = \varepsilon^5$ imamo da je $e = (a_1 + a_2 b + a_3 b^2 + a_4 b^3 + a_5 b^4 + a^6 b^5) + (c_1 + c_2 b + c_3 b^2 + c_4 b^3 + c_5 b^4 + c_6 b^5)\varepsilon = (a_1 + a_2\varepsilon^3 b + a_3 b^2 + a_4\varepsilon^3 b^3 + a_5 b^4 + a^6\varepsilon^3 b^5) + (c_1 + c_2\varepsilon^3 b + c_3 b^2 + c_4\varepsilon^3 b^3 + c_5 b^4 + c_6\varepsilon^3 b^5)\varepsilon^5$, pa mora biti $a_2, a_4, a_6 = 0$ i $c_1, \ldots, c_6 = 0$, tj. $e = a_1 + a_3 b^2 + a_5 b^4$, pa $e \in Q(b^2)$, tj $E^{H_4} \subseteq Q(b^2)$. Kako je minimalni polinom $m_{b^2}(x) = x^3 - 2$ elementa $b^2 = (\sqrt[6]{2})^2 = \sqrt[3]{2}$ nesvodljiv nad poljem

Q, mora biti $Q(b^2) \subseteq E^{H_4}$. Svakako, $Q(b^2)$, nije Galuaovo međupolje. Na isti način dokazuje se da je $E^{H_5} = Q(b^3, b\varepsilon)$, odnosno, da je $E^{H_6} = Q(b^2\varepsilon)$. Jasno, ta polja nisu Galuaovo međupolje.

Prvo međupolje koje jeste Galuaovo je $E^{H_7} = Q(b^2, \varepsilon)$, jer H_7 jeste normalna podgrupa grupe D_6. Takođe, polje $E^{K_1} = Q(b^3, \varepsilon)$, jeste Galuaovo međupolje.

Odrediti element $\alpha \in E$ tako da je $E^{V_1} = Q(\alpha)$, pa zatim isto za polja E^{V_2} i E^{V_3}. Nijedno od tih polja nije Galuaovo međupolje.

Međupolja $E^{G_1} = Q(\alpha)$ i $E^{G_2} = Q(\beta)$ (odrediti α i β) jesu Galuaova međupolja i konačno, $E^{G_3} = Q(\varepsilon)$, jeste Galuaovo međupolje za polja $Q \subseteq E$.

3. Koreni polinoma $f(x) = x^6 + x^3 + 1$ dobijaju se smenom $x^3 = t$ u jednačini $x^6 + x^3 + 1 = 0$, što daje jednačinu $t^2 + t + 1$, čija su rešenja $\rho = e^{\frac{2\pi i}{3}}$ i $\rho^2 = \bar{\varepsilon}$, pa su rešenja polinoma f redom $\varepsilon, \varepsilon^4, \varepsilon^7$ i $\varepsilon^2, \varepsilon^5, \varepsilon^8$, gde je $\varepsilon^9 = 1$. Kako je polinom f nesvodljiv nad Q (dokazati), i $\deg(f) = 6$, to je stepen $[E : Q]$, njegovog korenskog raširenja E nad poljem Q, jednak 6, a to znači da grupa $\mathrm{Aut}(E|Q)$ ima šest elemenata. Ako je $\sigma : \varepsilon \mapsto \varepsilon^2$, vodeći računa da je $\varepsilon^9 = 1$, dobijamo da je $\mathrm{Aut}(E|Q) = (\sigma) = C_6$.

4. Neka je $E|F$ Galuaovo raširenje i neka grupa $\mathrm{Aut}(E|Q)$ ima p^n elemenata, $n \geq 2$, za neki prost broj p. Prema Silovljevoj teoremi, $\mathrm{Aut}(E|Q)$ sadrži podgrupu H reda p^{n-1}, odnosno, indeksa $|\mathrm{Aut}(E|Q) : H| = p$. Kako je p najmanji prost broj koji deli red grupe $\mathrm{Aut}(E|Q)$, podgrupa H mora biti normalna. Sada ostaje da se primeni osnovna teorema.

5. Pretpostavimo da je $\deg(f) = n < 7$. Kako je E korensko polje separabilnog polinoma $f(x) \in F[x]$, raširenje $E|F$ je Galuaovo i grupa $\mathrm{Aut}(E|F)$ je Galuaova grupa polinoma f koja se utapa simetričnu grupu S_n, tj. postoji podgrupa H grupe S_n takva da je $H \cong \mathrm{Aut}(E|Q)$. Ako grupa $\mathrm{Aut}(E|Q)$ ima element reda 7, onda $7|n!$, a to nije moguće jer, $n < 7$ i 7 je prost broj.

7. Neka je $E \subseteq \overline{Z}_2$ korensko polje polinoma f. Kako je f separabilan i E njegovo korensko polje, to je $E|Z_2$ Galuaovo raširenje. Kako je G Galuaova grupa polinoma f, to je $Z_2 = E^G$. To znači da za svako $x \in E$, x pripada polju Z_2 ako i samo ako za svako $\sigma \in G$, $\sigma(x) = x$. Kako $\sigma \in G$ samo permutuje korene polinoma$f$ i kako je $\prod_{i<j}(x_i + x_j) \in E$,

$$\sigma\left(\prod_{i<j}(x_i + x_j)\right) = \prod_{i<j}(x_i + x_j),$$

za svaki automorfizam $\sigma \in G$. To znači da $\prod_{i<j}(x_i + x_j) \in Z_2$, odnosno, da $\prod_{i<j}(x_i+x_j) = 0$ ili $\prod_{i<j}(x_i+x_j) = 1$. Pretpostavimo da je $\prod_{i<j}(x_i+x_j) = 0$, onda postoji bar jedan par x_i, x_j, za koji je $x_i + x_j = 0$, tj. $x_i = -x_j = x_j$, budući da je E raširenje polja Z_2, pa je i samo karakteristike 2. To protivreči pretpostavci da je f separabilan polinom (svi koreni su različiti), pa mora biti $\prod_{i<j}(x_i + x_j) = 1$.

8. Neka je u jednakokrakom trouglu poluprečnik upisanog kruga 1, osnovica b i krak a. Površina takvog trougla je $P = S$, gde je $S = a + \frac{b}{2}$, pa kako je $P^2 = S(S-a)(S-a)(S-b)$, mora biti $b^3 - 2ab^2 + 4b + 8a = 0$. Sada treba raspraviti prirodu rešenja polinoma $f(x) = x^3 - 2ax^2 + 4x + 8a$ u zavisnosti od parametra $a \in Z$.

9*. Neka je $f(x) = x^{p-1} + \cdots + x + 1$, p prost, polinom nad poljem Q. Polinom f je nesvodljiv nad poljem Q i ako je $\varepsilon = e^{\frac{2\pi i}{p}}$, onda je njegovo korensko raširenje $E = Q(\varepsilon)$. Svi koreni polinoma f su ε^i, $i = 1, \ldots, p-1$.

Tvrdimo da je Galuaova grupa $\mathrm{Aut}\,(E|Q)$ ciklična grupa C_{p-1}. Naime, svaki automorfizam slika ε u ε^q, za neko q, pa ako je q primitivni koren $(\mathrm{mod}\, p)$, onda automorfizam $\sigma : \varepsilon \mapsto \varepsilon^q$ generiše grupu $\mathrm{Aut}\,(E|Q)$.

Neka je $n \geq 1$. Prema Dirišleovoj teoremi, svaka aritmetička progresija sadrži beskonačno mnogo prostih brojeva, pa neka je p prost broj oblika $p = k \cdot n + 1$, odnosno, prost broj p je takav da n deli $p-1$.

Za tako izabrano p, posmatrajmo polinom $f(x) = x^{p-1} + \cdots + x + 1$ nad poljem Q. Grupa automorfizama njegovog korenskog raširenja E je ciklična grupa C_{p-1}, pa kako n deli $p-1$, ona sadrži podgrupu G reda n, koja je takođe ciklična, tj. $G \cong C_n$. Kako je svaka podgrupa ciklične grupe normalna, međupolje $E^{C_n} = F$ je Galuaovo raširenje polja Q i $\mathrm{Aut}\,(F|Q) \cong C_n$.

10. Kako je $x^7 - 1 = (x-1) \cdot x^3 \cdot (x^3 + x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2} + \frac{1}{x^3})$, smenom $x + \frac{1}{x} = t$, jednačina $(x^3 + x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2} + \frac{1}{x^3}) = 0$ svodi se na jednačinu trećeg stepena $t^3 + t^2 - 2t - 1 = 0$. Poslednja jednačina jeste rešiva u radikalima, pa je $x^7 - 1 = 0$ rešiva u radikalima.

Smenom $t = y - \frac{1}{3}$, jednačina $t^3 + t^2 - 2t - 1 = 0$ svodi se na jednačinu $y^3 - \frac{7}{3}y - \frac{7}{27} = 0$, tj. na jednačinu oblika $y^3 + px + q = 0$, za koju je $-\Delta = 27q^2 + 4p^3$. Otuda se dobija da je $\Delta = 49$, pa su rešenja jednačine $y^3 - \frac{7}{3}y - \frac{7}{27} = 0$ redom

$$y_1 = u + v,\ y_2 = \varepsilon u + \varepsilon^2 v,\ y_3 = \varepsilon^2 u + \varepsilon v,\ \varepsilon = e^{\frac{2\pi i}{3}},$$

gde je

$$u = \sqrt[3]{\frac{\frac{7}{27} + \sqrt{-\frac{49}{27}}}{2}}, \quad v = \sqrt[3]{\frac{\frac{7}{27} - \sqrt{-\frac{49}{27}}}{2}}.$$

Pritom, kako je $\Delta = 49$, jednačina $x^2 - \Delta = 0$ ima rešenje u R, pa su sva rešenja jednačine $y^3 - \frac{7}{3}y - \frac{7}{27} = 0$ realna. Rešenja jednačine $t^3 + t^2 - 2t - 1 = 0$ su sada redom

$$t_1 = u + v - \frac{1}{3}, \; t_2 = \varepsilon u + \varepsilon^2 v - \frac{1}{3}, \; t_3 = \varepsilon^2 u + \varepsilon v - \frac{1}{3}.$$

Kako je $x + \frac{1}{x} = t$, to je $x^2 - tx + 1 = 0$, tj. $x_{1/2} = \frac{t \pm \sqrt{t^2-4}}{2}$, pa konačno dobijamo da je

$$x_{1/2} = \frac{t_1 \pm \sqrt{t_1{}^2 - 4}}{2}, \; x_{3/4} = \frac{t_2 \pm \sqrt{t_2{}^2 - 4}}{2}, \; x_{5/6} = \frac{t_3 \pm \sqrt{t_3{}^2 - 4}}{2}.$$

Ako je $\varepsilon = e^{\frac{2\pi i}{7}}$, onda $\varepsilon + \overline{\varepsilon} = 2\cos\frac{2\pi i}{7}$. Izaberimo $t_i > 0$ (jer $\cos\frac{2\pi i}{7} > 0$), pa zbog $x^2 - t_i x + 1 = 0$, imamo da je $x_1 + x_2 = t_i = 2\cos\frac{2\pi i}{7}$, pa se konačno dobija da je

$$\cos\frac{2\pi i}{7} = \frac{1}{2}\left(\sqrt[3]{\frac{\frac{7}{27} + \sqrt{-\frac{49}{27}}}{2}} + \sqrt[3]{\frac{\frac{7}{27} - \sqrt{-\frac{49}{27}}}{2}} - \frac{1}{3}\right).$$

11. Neka je E korensko polje polinoma $f(x) = x^4 - 5$. Kako su koreni polinoma f redom b, $-b$, ib i $-ib$, gde je $b = \sqrt[4]{5}$, to je $E = Q(b, i)$. Pritom,

$$|\mathrm{Aut}\,(E|Q)| = [E : Q] = [Q(b)(i) : Q(b)] \cdot [Q(b) : Q] = 2 \cdot 4 = 8,$$

jer polinom $f(x) = x^4 - 5$ je nesvodljiv nad Q, pa je minimalni polinom $m_b = f$, a polinom $x^2 + 1$ je nesvodljiv nad poljem $Q(b)$ zbog $i \notin Q(b)$.

Neka je $\sigma : i \mapsto -i, b \mapsto b$ i $\rho : i \mapsto i, b \mapsto ib$. Jasno je da $\sigma^2 = e$, $\rho^4 = e$ i $\rho\sigma = \sigma\rho^3$, pa je

$$\mathrm{Aut}\,(E|Q) = \{e, \sigma, \rho, \rho^2, \rho^3, \sigma\rho, \sigma\rho^2, \sigma\rho^3\} = D_2.$$

Sve podgrupe reda 2 su oblika $H_i = \sigma\rho^{i-1}$, $i = 1, \ldots, 4$ i grupa $H_0 = (\rho^2)$. Kako je $\rho H_i \rho^{-1} \neq H_i$, za sve $i = 1, \ldots, 4$, nijedna od grupa H_i, $i \neq 0$,

nije normalna podgrupa u D_2. Jedina normalna podgrupa reda 2 jeste H_0. Sve podgrupe reda 4 su; $G_0 = (\rho)$, $G_1 = H_0 \cdot H_1$ i $G_1 = H_0 \cdot H_2$. Kako su podgrupe G_i indeksa 2 u grupi D_4, sve grupe G_i su normalne. Pritom, $G_0 \cong C_4$, a grupe G_1 i G_2 izomorfne su grupi $C_2 \times C_2$, tj. Klajnovoj grupi. Dakle, međupolja oblika E^{H_i}, $i = 1, \ldots, 4$, nisu Galoaova, dok međupolja oblika E^{G_i}, $i = 0, 1, 2$, kao i međupolje E^{H_0}, jesu Galoaova.

Neka je $e \in E$. Kako je $E = Q(b)(i) = \{a + ci : a, c \in Q(b)\}$, to je

$$e = (a_1 + a_2 b + a_3 b^2 + a_4 b^3) + (c_1 + c_2 b + c_3 b^2 + c_4 b^3)i,$$

za neke $a_i, c_i \in Q$. Budući da automorfizmi $\sigma\rho$ i ρ^2 generišu grupu G_2, $e \in E^{G_2}$ ako i samo ako $e = \rho^2(e)$ i $e = \sigma\rho(e)$. Iz prve jednakosti dobijamo da $a_2, a_4, c_2, c_4 = 0$, tj. da je $e = a_1 + a_3 b^2 + (c_1 + c_3 b^2)i$. Iz druge jednakosti dobijamo $a_3, c_1 = 0$, pa je $e = a_1 + c_3 b^2 i$. Dakle, dobijamo da je Galuaovo međupolje E^{G_2} zapravo polje $Q(ib^2)$. Treba još odrediti međupolja E^{G_0} i E^{G_1}. Kako ρ generiše grupu G_0, $e \in E^{G_0}$ ako i samo ako $e = \rho(e)$. Iz te jednakosti dobija se da je $a_2, c_2, a_3, c_3, a_4, c_4 = 0$, pa je $e = a_1 + c_1 i$, gde se $a_1, c_1 \in Q$. To znači da je Galuaovo međupolje E^{G_0} zapravo polje $Q(i)$. Preostaje još međupolje E^{G_1}. Automorfizmi σ i ρ^2 generišu G_1, pa se iz jednakosti $e = \rho^2(e)$ dobija da je $e = a_1 + a_3 b^2 + (c_1 + c_3 b^2)i$, pa primenom jednakosti $e = \sigma(e)$ dobijamo $e = a_1 + a_2 b^2$, tj. međupolje E^{G_1} je polje $Q(b^2) = Q(\sqrt{5})$. Treba još odrediti primitivni element polja E.

12. Neka je E polje dobijeno iz polja Q adjunkcijom svih n-tih korena iz jedinice ε_n, $n \geq 3$, tj. $E = Q(\varepsilon_3, \varepsilon_4, \ldots)$. Za svako $n \geq 3$, minimalni polinom m_{ε_n} elementa ε_n je stepena $\varphi(n)$, gde je φ Ojlerova funkcija. Otuda, ako je $\sigma \in \mathrm{Aut}\,(E|Q)$, $\sigma(\varepsilon_n)$ može imati $\varphi(n)$ različitih vrednosti, za svako $n \geq 3$. Otuda sledi da je

$$|\mathrm{Aut}\,(E|Q)| = \prod_{n \geq 3} \varphi(n) \geq \prod_{n \geq 3} 2 = 2^{\aleph_0},$$

jer $\varphi(3) = 2$ i $\varphi(n) \geq 2$, za svako $n > 3$.

13. Koreni polinoma $f(x) = x^4 - q$, $q \in Q^+$, su $\sqrt[4]{q}, i\sqrt[4]{q}, i^2\sqrt[4]{q}, i^3\sqrt[4]{q}$, gde je $i^2 = -1$. Razlikuju se tri mogućnosti: $\sqrt[4]{q} \in Q$, postoji $r \in Q^+$, $q = r^2$ i konačno, ne postoji $r \in Q^+$, takvo da je $q = r^2$.

U prvom slučaju, korensko raširenje E polinoma f je polje $Q(i)$ i njegova Galuaova grupa $\mathrm{Aut}\,(E|Q)$ je C_2 (objasniti).

U drugom slučaju, ako $\sqrt{r}$ nije racionalan, korensko raširenje E polinoma f je polje $Q(\sqrt{r}, i)$, pa kako je

$$[Q(\sqrt{r}, i) : Q] = [Q(\sqrt{r}, i) : Q(\sqrt{r})] \cdot [Q(\sqrt{r}) : Q] = 2 \cdot 2 = 4,$$

Galuaova grupa $\mathrm{Aut}\,(E|Q)$ je reda 4. Njeni generatori su automorfizmi $\sigma : i \mapsto -i, \sqrt{r} \mapsto \sqrt{r}$ i $\rho : i \mapsto i, \sqrt{r} \mapsto -\sqrt{r}$, tj.

$$\mathrm{Aut}\,(E|Q) = \{e, \sigma, \rho, \sigma\rho\},$$

sa strukturnim jednakostima $\sigma^2 = e, \rho^2 = e$ i $\sigma\rho = \rho\sigma$. To zapravo znači da je $\mathrm{Aut}\,(E|Q) \cong C_2 \times C_2$.

Ako ne postoji $r \in Q^+$ takvo da je $q = r^2$, onda je $E = Q(\sqrt[4]{q}, i)$ korensko raširenje polinoma f. Stepen tog raširenja je (objasniti)

$$[Q(\sqrt[4]{q}, i) : Q] = [Q(\sqrt[4]{q}, i) : Q(\sqrt[4]{q})] \cdot [Q(\sqrt[4]{q}) : Q] = 2 \cdot 4 = 8,$$

pa grupa $\mathrm{Aut}\,(E|Q)$ ima osam elemenata (objasniti). Dokazati da je grupa automorfizama $\mathrm{Aut}\,(E|Q)$ izomorfna grupi D_4.

14. Polinom $f(x) = x^4 + 1$ nije svodljiv nad poljem Q i njegovi koreni su redom

$$x_1 = \frac{\sqrt{2} + i\sqrt{2}}{2}, \quad x_2 = \frac{-\sqrt{2} + i\sqrt{2}}{2}, \quad x_3 = \frac{-\sqrt{2} - i\sqrt{2}}{2}, \quad x_4 = \frac{\sqrt{2} - i\sqrt{2}}{2}.$$

Ako je $u = \sqrt{-1}$, polje $Q(u)$ sadrži $i = u^2$, ali ne sadrži sve korene polinoma f. Stoga je neophodno da to polje proširimo sa $\sqrt{2}$, pa tako dobijamo da je $E = Q(u, \sqrt{2})$ korensko proširenje polinoma E. Jasno, stepen tog proširenja je 8.

Ako je $\sigma = \begin{pmatrix} \sqrt{2} & i \\ \sqrt{2} & -i \end{pmatrix}$ i $\rho = \begin{pmatrix} \sqrt{2} & i \\ i\sqrt{2} & i \end{pmatrix}$, onda je $\sigma^2 = e$, $\rho^4 = e$ i $\rho\sigma = \sigma\rho^3$. Pritom, na korenima polinoma f, σ deluje kao permutacija $(14)(23)$, a ρ kao permutacija, odnosno, ciklus (1234). Otuda se dobija da je D_4 Galoaova grupa korenskog raširenja polinoma f. Podgrupa $G_0 = (\rho)$ je reda 4 i normalna u D_4, pa je E^{G_0} Galuaovo međupolje. Kao u 11. zadatku, dobijamo da je $E^{G_0} = Q(\sqrt{2})$.

15*. Polinom $f(x) = x^5 - 2$ nije svodljiv nad poljem Q. Ako je $b = \sqrt[5]{2}$, svi njegovi koreni su $b, \varepsilon b, \varepsilon^2 b, \varepsilon^3 b, \varepsilon^4 b$, gde je $\varepsilon = e^{\frac{2\pi i}{5}}$. Kako je polinom f nesvodljiv nad Q, a polinom $g(x) = 1 + x + x^2 + x^4$ nad poljem $Q(u)$, korensko

raširenje polinoma f je $E = Q(\varepsilon, u)$. Pritom je $[E : Q] = 4 \cdot 5 = 20$ i grupa $G = \mathrm{Aut}\,(E|Q)$ je reda 20.

Ako je $\tau = \begin{pmatrix} b & \varepsilon \\ \varepsilon b & \varepsilon \end{pmatrix}$ i $\sigma = \begin{pmatrix} b & \varepsilon \\ b & \varepsilon^2 \end{pmatrix}$, onda je $\tau^5 = e$, $\sigma^4 = e$ i $\sigma\tau = \tau^2\sigma$, pa je $G = (\sigma, \tau)$ i grupa G zadovoljava navedene strukturne jednakosti. Treba primetiti da je presek podgrupa $K = \{e, \tau, \tau^2, \tau^3, \tau^4\}$ i $H = \{e, \sigma, \sigma^2, \sigma^3\}$ jednak (e), pa kako je H normalna u G, to je $H \cdot K$ grupa reda 20, odnosno, $H \cdot K = G$. Otuda sledi da je $G = \{\tau^k\sigma^l : 0 \leq k \leq 4,\ 0 \leq l \leq 3\}$. Kako K nije normalna podgrupa u G, grupa G nije komutativna.

Ispitivanje strukture podgrupa grupe G nije lako. Kako je $G \subseteq S_6$, $6 = \deg f$, red svakog elementa u G je ≤ 6, pa je $r_1 + r_2 + r_4 + r_5 = 20$, gde je r_k broj elemenata reda k u grupi G. Elemenata reda pet ima četiri i svi su sadržani u H. Elemenata reda četiri ima deset, pa $r_2 = 5$. Dakle, grupa G ima pet podgrupa reda dva, od kojih ni jedna nije normalna. Podgrupa reda četiri ima pet i nijedna od njih nije normalna. Jedina podgrupa reda pet je H i ona jeste normalna. Konačno, postoji samo jedna grupa reda deset, to je dijedarska grupa D_5. Kao podgrupa indeksa 2, ona jeste normalna. Odrediti fiksna podpolja za H, K i D_5.