Algebra 3

Jan Pantner (jan.pantner@gmail.com)

30. oktober 2024

Kazalo

1 Galoisova teorija

1.1 Polja s karakteristiko 0

Izrek 1.1.1. Naj bo F polje s karakteristiko 0. Potem ima vsak nerazcepen polinom $p(x) \in F[x]$ v vsaki razširitvi same enostavne ničle. 2. oktober 2024

Izrek 1.1.2. Naj bo F polje s karakteristiko 0, naj bo $f(x) \in F[x]$ nekonstanten polinom, naj bo K razpadno polje $f(x)$ nad F, naj bo $\varphi\colon F \to F'$ izomorfizem in naj bo K' razpadno polje $f_\varphi(x)$ nad F'. Potem obstaja natanko $[K : F]$ razširitev izomorfizma φ do izomorfizma iz K v K'.

Definicija 1.1.3. Razširitev K polja F je ***enostavna***, če je $K = F(a)$ za neki $a \in K$. Tak a imenujemo ***primitivni elemen*** te razširitve.

Opomba 1.1.3.1. Primitivni element ni nujno enolično določen.

Izrek 1.1.4 (o primitivnem elementu)**.** Vsaka končna razširitev polja s karakteristiko 0 je enostavna.

1.2 Fundamentalni izrek Galoisove teorije

Definicija 1.2.1. Naj bo K razširitev polja F. Grupo avtomorfizmov K, ki fiksirajo F označimo z 16. oktober 2024

$$\mathrm{Aut}(K/F) := \{\sigma \in \mathrm{Aut}(K) \mid \forall\lambda \in F.\ \sigma(\lambda) = \lambda\}.$$

Definicija 1.2.2. Naj bo $H \leq \mathrm{Aut}(K/F)$. ***Polje fiksnih točk*** podgrupe H definiramo kot

$$K^H := \{x \in K \mid \forall\sigma \in H.\ \sigma(x) = x\}.$$

Lema 1.2.3. Naj bo polje K razširitev polja F s karakteristiko 0. Če je $\sigma \in \mathrm{Aut}(K/F)$ in $a \in K$ ničla $f(x) \in F[x]$, potem je $\sigma(a)$ ničla $f(x)$.

Opomba 1.2.3.1. Naj bo K končna razširitev polja F s karakteristiko 0. Po izreku o primitivnem elementu je $K = F(a)$. Vsak avtomorfizmem je tako enolično določen z delovanjem v a. Naj bo $p(x)$ minimalni polinom a nad F. Sledi, da vsak avtomorfizem, ki fiksira F, le permutira ničle $p(x)$, zato je takšnih avtomorfizmov kvečjemu $\deg(p(x))$. Po lemi (ref) pa vemo, da jih je natanko $\det(p(x)) = [K : F]$.

Lema 1.2.4. Naj bo $a \in K$ in naj bodo $a_1 = a, a_2, \ldots, a_m$ različni elementi množice $\{\sigma(a) \mid \sigma \in H\}$. Potem je 23. oktober 2024

$$p(x) = (x - a_1)(x - a_2)\cdots(x - a_m)$$

minimalni polinom a nad K^H.

Lema 1.2.5. Velja $|H| = [K : K^H]$ in $[K : F] = |H| \cdot [K^H : F]$.

Izrek 1.2.6. Naj bo K končna razširitev polja F s karakteristiko 0. Naslednji pogoji so ekvivalentni:

(i) $|\mathrm{Aut}(K/F)| = [K : F]$.

(ii) $K^{\mathrm{Aut}(K/F)} = F$.

(iii) Vsak nerazcepen polinom v $F[x]$ z ničlo v K, razpade v K.

(iv) K je razpadno polje nekega nerazcepnega polinoma iz $F[x]$.

(v) K je razpadno polje nekega polinoma iz $F[x]$.

Definicija 1.2.7. Končna razširitev K polja F s karakteristiko 0, se imenuje ***Galoisova razširitev***, če ustreza vsem pogojem izreka 1.2.6. Tedaj $\mathrm{Aut}(K/F)$ označujemo z $\mathrm{Gal}(K/F)$.

Če je K razpadno polje polinoma $f(x) \in F[x]$, potem K imenujemo tudi ***Galoisova razširitev polinoma*** $f(x)$.

Opomba 1.2.7.1. Splošneje te pojme vpeljemo za polja s poljubno karakteristiko. Galoisova razširitev je normalna in separabilna razširitev.

Razširitev je ***normalna***, če zadošča pogoju (iii) iz izreka 1.2.6.

Razširitev K/F je ***separabilna***, če je vsak nerazcepen polinom iz $F[x]$ ***separabilen***, tj. vse njegove ničle so enostavne.

Izrek 1.2.8 (Fundamentalni izrek Galoisove teorije)**.** Naj bo K Galoisova razširitev polja F s karakteristiko 0. S $\mathcal{F}$ označimo množico vseh vmesnih polj med F in K, z $\mathcal{G}$ pa množico vseh podgrup grupe $G := \mathrm{Gal}(K/F)$.

(a) Preslikava

$$\alpha\colon \mathcal{B} \to \mathcal{F}, \qquad \alpha(H) = K^H$$

je bijektivna z inverzom

$$\beta\colon \mathcal{F} \to \mathcal{B}, \qquad \beta(L) = \mathrm{Gal}(K/L).$$

(b) Če H pripada L – torej $H = \mathrm{Gal}(K/L)$ oziroma $L = K^H$ – potem

$$|H| = [K : L] \quad \text{in} \quad [G : H] = [L : F].$$

(c) Če H in H' zaporedoma pripadata L in L', potem $H \subseteq H'$ natanko tedaj, kadar $L \supseteq L'$.

(d) Če H pripada L, potem je $H \triangle G$ natanko tedaj, kadar je L Galoisova razširitev F. V tem primeru velja $G/H \cong \mathrm{Gal}(L/F)$.

1.3 Rešljivost polinomskih enačb z radikali

Definicija 1.3.1. Grupa G je ***rešljiva***, če obstajajo take edinke

$$\{1\} = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_m = G,$$

da je N_{i+1}/N_i Abelova grupa za $i = 0, \ldots, m-1$.

Direktno iz definicije sledi, da enostavna nekomutativna grupa ne more biti rešljiva.

Primer 1.3.1.1. Grupa A_5 ni rešljiva.

Izrek 1.3.2 (Feit-Thompson)**.** Vsaka grupa lihega reda je rešljiva.

Trditev 1.3.3.

1. Podgrupa rešljive grupe je rešljiva.
2. Naj bo $N \triangleleft G$. Grupa G je rešljiva natanko tedaj, kadar sta rešljivi N in G/N.

Primer 1.3.3.1. Grupa S_n, kjer je $n \geq 5$, vsebuje A_5, torej ni rešljiva.

Lema 1.3.4. Naj bo $F \subseteq \mathbb{C}$ polje in $a \in F$. Potem je Galoisova grupa polinoma $f(x) = x^n - 1$ rešljiva.

Definicija 1.3.5. Naj bo F polje. Polinom $f(x) \in F[x]$ je ***rešljiv z radikali*** nad F, če obstajajo taki elementi $a_1, \ldots, a_m$ neke razširitve F, da:

- Polinom $f(x)$ razpade v $F(a_1, \ldots, a_m)$
- Obstajajo takšni $n_1, \ldots, n_m \in \mathbb{N}$, da velja $a_1^{n_1} \in F$ in $a_i^{n_i} \in F(a_1, \ldots, a_{i-1})$.

Opomba 1.3.5.1. Druga točka nam pove to, da imamo tudi korenjenje.

Primer 1.3.5.2. Naj bodo $a, b, c \in \mathbb{C}$ in $f(x) = ax^2 + bx + c$. Polinom $f(x)$ je rešljiv z radikali nad $F = Q(a, b, c)$. Njegovi ničli sta

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

torej ustreza $a_1 = \sqrt{b^2 - 4ac}$.

Podobno velja za polinome tretje in četrte stopnje.

Izrek 1.3.6. Naj bo $F \subseteq \mathbb{C}$ in $f(x) \in F[x]$. Polinom $f(x)$ je rešljiv z radikali nad F natanko tedaj, kadar je Galoisova grupa $f(x)$ nad F rešljiva.

Lema 1.3.7. Naj bo $p(x) \in \mathbb{Q}[x]$ nerazcepen polinom stopnje 5 z natanko tremi realnimi ničlami. Potem $p(x)$ ni rešljiv z radikali nad $\mathbb{Q}$.

Izrek 1.3.8. Obstajajo polinomi iz $\mathbb{Q}[x]$ stopnje 5, ki niso rešljivi z radikali.

A Naloge

Vaje 1

1. Dokaži, da je število $\sqrt{2} + i\sqrt{3}$ algebraično. Poišči njegov minimalni polinom. 7. oktober 2024
2. Določi $[\mathbb{Q}(\sqrt{2} + \sqrt[3]{2}) : \mathbb{Q}]$, $[\mathbb{Q}(\sqrt{2} + \sqrt[4]{2}) : \mathbb{Q}]$ in $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})]$.
3. Naj bo $K/\mathbb{Q}$ kvadratična razširitev (tj. razširitev stopnje 2). Dokaži, da obstaja enolično določeno celo število $a \in \mathbb{Z}, a \neq 1$, brez kvadratov, za katerega je $K \cong \mathbb{Q}(\sqrt{a})$.
4. Naj bo $p \in \mathbb{N}$ praštevilo in $\zeta = e^{2\pi i/p}$ primitivni p-ti koren enote. Dokaži, da je ζ algebraično število, in določi stopnjo $[\mathbb{Q}(\zeta) : \mathbb{Q}]$.

Vaje 2

1. Naj bosta a in b algebraična elementa nad poljem F. Denimo, da sta stopnji $[F(a) : F]$ in $[F(b) : F]$ tuji si števili. Dokaži, da je 14. oktober 2024
$$[F(a, b) : F] = [F(a) : F][F(b) : F].$$
2. Določi razpadno polje K polinoma $x^5 - 2$ in izračunaj $[K : \mathbb{Q}]$.
3. Poišči primitiven element za razširitev $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.
4. Izračunaj $[\mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5}) : \mathbb{Q}]$.
5. Naj bo ω transcendenten element nad $\mathbb{Z}_2$. Dokaži, da je polinom $f(x) = x^2 - \omega$ nerazcepen nad $\mathbb{Z}_2(\omega)$, a ima dvakratno ničlo.
6. Naj bo p neko praštevilo. Dokaži, da razširitev $\mathbb{Z}_p(X, Y)/\mathbb{Z}_p(X^p, Y^p)$ ni enostavna.

Vaje 3

1. Pokaži, da je grupa avtomorfizmov realnih števil $\mathbb{R}$, $\mathrm{Aut}(\mathbb{R})$, trivialna. 21. oktober 2024
2. Dokaži, da sta edina zvezna avtomorfizma kompleksnih števil $\mathbb{C}$ identiteta in konjugiranje.
3. Naj bo $[K : F] = 2$. Dokaži, da je K Galoisova razširitev F. Določi tudi grupo avtomorfizmov polja K, ki fiksirajo vse elemente iz F.
4. Ali je $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ Galoisova razširitev? Poišči grupo $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$.
5. Če sta K/F in L/K Galoisovi razširitvi, ali je nujno tudi L/F Galoisova razširitev?
6. Dokaži, da lahko Galoisovo grupo polinoma stopnje n vložimo v S_n in zato red te Galoisove grupe deli $n!$.

Vaje 4

1. Razširitev K/F imenujemo ***bikvadratična***, če je $K = F(\sqrt{a}, \sqrt{b})$ za neka $a, b \in F$ in je $[K : F] = 4$. Poišči Galoisovo grupo bikvadratične razširitve K/F in določi vsa polja L, ki ležijo med F in K.

2. Določi vsa podpolja polja $\mathbb{Q}(e^{2\pi i/7})$.

3. Določi vsa podpolja polja $\mathbb{Q}(\sqrt[4]{2})$.

Stvarno kazalo