

# Algebra 3

Jan Pantner ([jan.pantner@gmail.com](mailto:jan.pantner@gmail.com))

10. november 2024

# Kazalo

<b>1</b>	<b>Galoisova teorija</b>	<b>3</b>
1.1	Polja s karakteristiko 0 . . . . .	3
1.2	Fundamentalni izrek Galoisove teorije . . . . .	3
1.3	Rešljivost polinomskih enačb z radikali . . . . .	4
<b>2</b>	<b>Moduli</b>	<b>6</b>
2.1	Vložitev kolobarja v kolobar endomorfizmov . . . . .	6
2.2	Definicija modula . . . . .	6
2.3	Osnovni pojmi teorije modulov . . . . .	7
<b>A</b>	<b>Naloge</b>	<b>9</b>

# 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.

**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  $\varphi: F \rightarrow F'$  izomorfizem in naj bo  $K'$  razpadno polje  $f_\varphi(x)$  nad  $F'$ . Potem obstaja natanko  $[K : F]$  razširitev izomorfizma  $\varphi$  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

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

**Definicija 1.2.2.** Naj bo  $H \leq \text{Aut}(K/F)$ . **Polje fiksni**h 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  $\sigma \in \text{Aut}(K/F)$  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 avtomorfizem 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  $\deg(p(x)) = [K : F]$ .

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

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

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

9. oktober 2024

16. oktober 2024

23. oktober 2024

- (ii)  $K^{\text{Aut}(K/F)} = F$ .
- (iii) Vsak nerazcepen polinom v  $F[x]$  z ničlo v  $K$ , razpade v  $K$ .
- (iv)  $K$  je razpadno polje nekega nerazcepne 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  $\text{Aut}(K/F)$  označujemo z  $\text{Gal}(K/F)$ .

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  $G := \text{Gal}(K/F)$ .

- (a) Preslikava

$$\alpha: \mathcal{B} \rightarrow \mathcal{F}, \quad \alpha(H) = K^H$$

je bijektivna z inverzom

$$\beta: \mathcal{F} \rightarrow \mathcal{B}, \quad \beta(L) = \text{Gal}(K/L).$$

- (b) Če  $H$  pripada  $L$  – torej  $H = \text{Gal}(K/L)$  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  $H \triangleleft G$  natanko tedaj, kadar je  $L$  Galoisova razširitev  $F$ . V tem primeru velja  $G/H \cong \text{Gal}(L/F)$ .

### 1.3 Rešljivost polinomskih enačb z radikali

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

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

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

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  $a_1, \dots, a_m$  neke razširitve  $F$ , da:

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

**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  $F = \mathbb{Q}(a, b, c)$ . 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.

## 2 Moduli

### 2.1 Vložitev kolobarja v kolobar endomorfizmov

Naj bo  $M$  aditivna grupa. Množica endomorfizmov  $\text{End}(M)$  skupaj z operacijama

$$\begin{aligned}(\varphi + \psi)(v) &= \varphi(v) + \psi(v) \quad \text{in} \\ (\varphi \cdot \psi)(v) &= \varphi(\psi(v))\end{aligned}$$

je kolobar.

**Izrek 2.1.1.** Vsak kolobar lahko vložimo v kolobar endomorfizmov neke aditivne grupe.

*Dokaz.* Naj bo  $K$  kolobar in  $\text{End}(K)$  kolobar endomorfizmov aditivne grupe  $(K, +)$ . definiramo

$$\begin{aligned}\varphi: K &\rightarrow \text{End}(K), \\ a &\mapsto l_a,\end{aligned}$$

kjer je  $l_a$  levo množenje:  $l_a(x) = ax$ . Velja

$$\begin{aligned}\varphi(a + b) &= l_{a+b} = l_a + l_b = \varphi(a) + \varphi(b), \\ \varphi(a \cdot b) &= l_{a \cdot b} = l_a \circ l_b = \varphi(a) \cdot \varphi(b), \\ \varphi(1) &= l_1 = \text{id}_K.\end{aligned}$$

Velja še

$$\varphi(a) = 0 \Rightarrow l_a = 0 \Rightarrow l_a(1) = 0 \Rightarrow a = 0,$$

torej je jedro trivialno in res imamo vložitev.  $\square$

**Izrek 2.1.2.** Vsako algebro lahko vložimo v algebro endomorfizmov  $\text{End}_F(V)$  za neki vektorski prostor  $V$ .

*Dokaz.* Dokaz je podoben dokazu izreka 2.1.1.  $\square$

**Posledica 2.1.2.1.** Vsako končnorazsežno algebro lahko vložimo v  $\text{End}_F(V) \cong M_n(F)$ , kjer je  $V$   $n$ -dimenzionalni vektorski prostor nad  $F$ .

**Primer 2.1.2.2.** Naj bo  $A$   $n$ -razsežna realna algebra. Ali obstajata takšna  $s, t \in A$ , da velja  $st - ts = 1$ ?

Po posledici je to ekvivalentno obstoju  $S, T \in M_n(\mathbb{R})$ , kjer velja  $ST - TS = I$ . To ni mogoče, saj velja

$$0 = \text{tr}(ST - TS) \neq \text{tr}(I) = n.$$

### 2.2 Definicija modula

**Definicija 2.2.1.** Naj bo  $K$  kolobar. Množica  $M$  skupaj z binarno operacijo seštevanja  $+$  in zunanjo binarno operacijo  $K \times M \rightarrow M$ ,  $(a, u) \mapsto au$  imenovano **modulsko množenje** (tudi skalarno množenje), se imenuje **(levi) modul** nad  $K$  ali  **$K$ -modul**, če velja:

- $(M, +)$  je Abelova grupa,
- $\forall a \in K. \forall u, v \in M. a(u + v) = au + av,$
- $\forall a, b \in K. \forall u \in M. (a + b)u = au + bu,$
- $\forall a, b \in K. \forall u \in M. (ab)u = a(bu),$
- $\forall u \in M. 1u = u.$

**Opomba 2.2.1.1.** Analogno lahko definiramo tudi **desni modul**.

**Opomba 2.2.1.2.** Če je  $M$   $K$ -modul, je  $\varphi: K \rightarrow \text{End}(M)$ ,  $\varphi(a)(u) = au$ , homomorfizem kolobarjev.

Obratno, če je  $\varphi: K \rightarrow \text{End}(M)$  homomorfizem kolobarjev, postane  $M$   $K$ -modul, če vpeljemo  $au := \varphi(a)(u)$ .

**Primer 2.2.1.3.** (1) Vektorski prostor nad poljem  $F$  je  $F$ -modul.

- (2) Vsaka Abelova (aditivna) grupa je  $\mathbb{Z}$ -modul. Obratno,  $\mathbb{Z}$ -modul je aditivna grupa.
- (3) Vsak kolobar  $K$  je  $K$ -modul, če za modulsko množenje vzamemo običajno množenje v kolobarju.
- (4) Če je  $I$  levi ideal  $K$ , ga lahko obravnavamo kot levi  $K$ -modul.
- (5) Če je  $K$  podkolobar  $K'$ , je  $K'$   $K$ -modul.
- (6) Naj bo  $K = M_n(F)$  in  $M = F^n$ . Potem je  $M$   $K$ -modul za običajno množenje matrike s stolpcem.

## 2.3 Osnovni pojmi teorije modulov

### Podmoduli

**Definicija 2.3.1.** Podmnožica  $N$   $K$ -modula  $M$  je **podmodul**, če je za isti operaciji tudi sama  $K$ -modul.

Ekvivalentno

$$\forall a, b \in K. \forall u, v \in N. au + bv \in N$$

oziroma

$$(\forall u, v \in N. u + v \in N) \wedge (\forall a \in K. \forall t \in N. at \in N).$$

**Primer 2.3.1.1.** (1) Če je  $K$  polje, so podmoduli podprostor.

- (2) Če je  $K = \mathbb{Z}$ , so podmoduli podgrupe.
- (3) Podmoduli  $K$ -modula  $K$  so levi ideali.

(4) Množici  $\{0\}$  in  $M$  sta vedno podmodula modula  $M$ .

**Trditev 2.3.2.** Če sta  $N_1$  in  $N_2$  podmodula, sta podmodula tudi

$$N_1 + N_2 = \{v_1 + v_2 \mid v_i \in N_i\}$$

in  $N_1 \cap N_2$ .

**Definicija 2.3.3.** Modul  $M \neq \{0\}$ , ki nima drugih podmodulov poleg  $\{0\}$  in  $M$ , se imenuje **enostavni modul**.

**Primer 2.3.3.1.** (1) Če je  $K$  polje, so enostavni moduli 1-razsežni prostori.

(2) Če je  $K = \mathbb{Z}$ , so enostavni moduli  $\mathbb{Z}_p$ , kjer je  $p$  praštevilo.

(3) Naj bo  $K = M_n(F)$  in  $M = F^n$ . Naj bo  $N \neq \{0\}$  podmodul  $M$  in  $x \in N$ . Velja

$$\forall y \in M. \exists A \in K. Ax = y.$$

Torej ni pravega podmodula –  $M$  je enostaven  $K$ -modul.

## Homomorfizmi modulov

**Definicija 2.3.4.** Naj bosta  $M$  in  $M'$   $K$ -modula. Preslikava  $\varphi: M \rightarrow M'$  je **homomorfizem modulov**, če velja  $\varphi(u + v) = \varphi(u) + \varphi(v)$  in  $\varphi(au) = a\varphi(u)$ . Homomorfizme modulov imenujemo tudi **linearne preslikave** oziroma  $K$ -linearne preslikave.

Ekvivalentno mora veljati  $\varphi(au + bv) = a\varphi(u) + b\varphi(v)$ .

Seveda velja, da je inverz izomorfizma izomorfizem in da je kompozitum homomorfizmov homomorfizem. Na standarden način definiramo **jedro** in **slika** homomorfizma. Jedro in slika sta podmodula.

**Primer 2.3.4.1.** 1. Če je  $K$  polje, so homomorfizmi “običajne” linearne preslikave.

2. Če je  $K = \mathbb{Z}$ , so homomorfizmi aditivne preslikave – homomorfizmi aditivnih grup.

3. Naj bo  $I$  levi ideal  $K$ . Naj bo  $c \in I$ . Preslikava  $\varphi: I \rightarrow I, u \mapsto uc$ , je homomorfizem.

## Kolobarji endomorfizmov in Schurova lema

Naj bo  $M$   $K$ -modul. Potem je množica vseh endomorfizmov  $M, \text{End}_K(M)$ , kolobar za običajno seštevanje in komponiranje kot množenje.

Velja, da je  $\varphi \in \text{End}_K(M)$  bijektivna preslikava natanko tedaj, kadar je avtomorfizem oziroma natanko tedaj, kadar je  $\varphi$  obrnljiv element  $\text{End}_K(M)$ .

**Lema 2.3.5** (Schur). Če je  $M$  enostaven  $K$ -modul, je  $\text{End}_K(M)$  obseg.

*Dokaz.* Naj bo  $\varphi \in \text{End}_K(M)$ . Upoštevamo, da sta  $\ker \varphi$  in  $\text{im } \varphi$  podmodula enostavnega modula. Torej je  $\varphi = 0$  ali pa je  $\varphi$  bijektiven endomorfizem.  $\square$



# A Naloge

## Vaje 1

1. Dokaži, da je število  $\sqrt{2} + i\sqrt{3}$  algebraično. Poišči njegov minimalni polinom.
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  $\zeta$  algebraično število, in določi stopnjo  $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ .

7. oktober 2024

## 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

$$[F(a, b) : F] = [F(a) : F][F(b) : F].$$

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  $\omega$  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.

14. oktober 2024

## Vaje 3

1. Pokaži, da je grupa avtomorfizmov realnih števil  $\mathbb{R}$ ,  $\text{Aut}(\mathbb{R})$ , trivialna.
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  $\text{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$ .
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  $n!$ .

21. oktober 2024

## 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  $\mathbb{Q}(\sqrt[4]{2})$ .

28. oktober 2024

## Vaje 5

1. Naj bo  $K$  razpadno polje polinoma  $x^5 - 2$  nad  $\mathbb{Q}$ . Določi vse  $a \in \mathbb{Z}$ , za katere je  $\sqrt{a} \in K$ .
2. Naj bo  $K/F$  Galoisova razširitev z  $[K : F] = 14$ . Dokaži, da so vsa vmesna polja  $L$ , za katere je  $[L : F] = 7$ , med seboj izomorfna. Določi tudi, koliko takih vmesnih polj obstaja.
3. Naj bo  $K/F$  Galoisova razširitev. Denimo, da je  $\text{Gal}(K/F)$  komutativna grupa. Pokaži, da je vmesno polje  $L$  Galoisova razširitev.
4. Grupi  $G$ , v kateri je vsaka podgrupa tudi edinka, rečemo **Dedekindova grupa**. Taka grupa  $G$  je bodisi komutativna bodisi obstaja epimorfizem  $\pi: G \rightarrow Q_8$ , kjer je  $Q_8$  kvaternionska grupa. Premisli, kako lahko iz strukture vmesnih polj neke Galoisove razširitve  $K/F$  vidimo, da je  $\text{Gal}(K/F)$  komutativna grupa.

4. november 2024

## Stvarno kazalo

bikvadratična razširitev, [10](#)

Dedekindova grupa, [10](#)

desni modul, [7](#)

enostavni modul, [8](#)

Galoisova razširitev, [4](#)

Galoisova razširitev polinoma, [4](#)

homomorfizem modulov, [8](#)

$K$ -linearna preslikava, [8](#)

levi modul, [6](#)

linearna preslikava, [8](#)

modul, [6](#)

modulsko množenje, [6](#)

normalna razširitev, [4](#)

podmodul, [7](#)

rešljiva grupa, [4](#)

rešljivost z radikali, [5](#)

separabilen polinom, [4](#)

separabilna razširitev, [4](#)