Algebra 3

Hugo Trebše (hugo.trebse@gmail.com)

19. oktober 2024

Algebra is the offer made by the devil to
the mathematician. The devil says:
»I will give you this powerful machine, it
will answer any question you like.
All you need to do is give me your soul:
give up geometry and you will have this
marvelous machine.«

Michael Atiyah

Kazalo

1 Ponovitev Algebre 2

Definicija 1.1

Naj bo $\mathbb{F} \subseteq \mathbb{K}$

- $a \in \mathbb{K}$ je algebraičen nad $\mathbb{F}$, če je ničla nekega polinoma iz $\mathbb{F}[X]$.
- $\mathbb{K}$ je algebraična razširitev $\mathbb{F}$, če so vsi elementi $\mathbb{K}$ algebraični nad $\mathbb{F}$.
- $\mathbb{K}$ je končna razširitev $\mathbb{F}$, natanko tedaj, ko je $\mathbb{K}$ končnodimenzionalni vektorski prostor nad $\mathbb{F}$.

Trditev 1.2

- $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$. Če je $[\mathbb{L} : \mathbb{F}], [\mathbb{K} : \mathbb{L}] < \infty$, potem je $[\mathbb{K} : \mathbb{L}] < \infty$ ter velja
$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{L}][\mathbb{L} : \mathbb{F}].$$

Izrek 1.3: Boreico

Kvadratni koreni različnih naravnih števil, ki niso deljiva s kvadrati naravnih števil, so linearno neodvisni nad $\mathbb{Q}$.

Naloga 1.4

Naj sta a, b algebraična nad $\mathbb{F}$, ter $[\mathbb{F}(a) : \mathbb{F}]$ tuj $[\mathbb{F}(b) : \mathbb{F}]$. Potem je
$$[\mathbb{F}(a, b) : \mathbb{F}] = [\mathbb{F}(a) : \mathbb{F}][\mathbb{F}(b) : \mathbb{F}].$$

Oris dokaza. Očitno $[\mathbb{F}(a) : \mathbb{F}]$ deli $[\mathbb{F}(a, b) : \mathbb{F}]$, enako za b, sledi, da je $[\mathbb{F}(a, b) : \mathbb{F}] = c \cdot [\mathbb{F}(a) : \mathbb{F}][\mathbb{F}(b) : \mathbb{F}]$. Obenem je tudi $[\mathbb{F}(a, b) : \mathbb{F}(a)] \leq [\mathbb{F}(b) : \mathbb{F}]$, po opazovanju minimalnega polinoma b nad $\mathbb{F}$ in nad $\mathbb{F}(a)$. □

Naloga 1.5

Poišči razpadno polje $x^5 - 2$.

Oris dokaza. Trivialno je razpadno polje $\mathbb{Q}(\sqrt[5]{2}, e^{\frac{2i\pi}{5}})$. Ker je $[\mathbb{Q}(e^{\frac{2\pi i}{5}}) : \mathbb{Q}] = 4$ in $[\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 5$ je stopnja razpadnega polja nad $\mathbb{Q}$ enaka 20. □

Naloga 1.6

V $\mathbb{Z}_p$ ne velja izrek o primitivnem elementu: Pokaži, da razširitev $\mathbb{Z}_p(x, y)/\mathbb{Z}_p(X^p, Y^p)$ ni primitivna.

2 Razpadna polja

Izrek 2.1

Za vsako polje $\mathbb{F}$ in nerazcepen polinom $p \in \mathbb{F}[X]$ obstaja razširitev $\mathbb{F}$, ki jo imenujmo $\mathbb{K}$, da je za nek $a \in \mathbb{K}$ velja $p(a) = 0$.

Oris dokaza. $\mathbb{K} \cong \mathbb{F}[X]/\langle p(x) \rangle$. Očitno vsebuje podpolje izomorfno $\mathbb{F}$, element $x + \langle p(x) \rangle$ pa je ničla p. □

Definicija 2.2

Razpadno polje polinoma $p \in \mathbb{F}[X]$ je najmanjše polje, ki vsebuje $\mathbb{F}$ kot podpolje, ter v njem $p(x)$ razpade na linearne faktorje.

Definicija 2.3

Polje $\mathbb{F}$ je *algebraično zaprto*, če je razpadno polje vsakega polinoma $\mathbb{F}[X]$ enako $\mathbb{K}$. *Algebraično zaprtje* polja $\mathbb{F}$ je polje $\mathbb{K}$, ki je algebraično nad $\mathbb{F}$ in je algebraično zaprto.

Izrek 2.4

Do izomorfizma natančno obstaja samo eno razpadno polje.

Oris dokaza. Beležimo dve opombi:
Opomba 1: Če je φ izomorfizem polj $\mathbb{F}$ in $\mathbb{F}'$, ga lahko razširimo do izomorfizma med $\mathbb{F}[X]$ in $\mathbb{F}'[X]$. Nerazcepni polinomi $\mathbb{F}[X]$ in $\mathbb{F}'[X]$ na trivialen način sovpadajo.
Opomba 2: Če je $a \in \mathbb{K}$ ničla nerazcepnega polinoma $p(X) \in \mathbb{F}[X]$, potem obstaja izomorfizem polj $\overline{\varepsilon}$, ki slika iz $\mathbb{F}[X]/\langle p(X) \rangle$ v $\mathbb{F}(a)$, ter je $\overline{\varepsilon}(X + \langle p(X) \rangle) = a$ in $\overline{\varepsilon}(\lambda + \langle p(X) \rangle) = \lambda$.
Če je $\varphi : \mathbb{F} \to \mathbb{F}'$ izomorfizem in a ničla nerazcepnega polinoma $p(X)$ ter a' ničla $p_\varphi(X)$, potem lahko φ na enoličen način raširimo do izomorfizma med $\mathbb{F}(a)$ in $\mathbb{F}'(a')$. Enoličnost je očitna. Definiramo lahko $\tilde{\varphi}$ kot naravni izomorfizmed med $\mathbb{F}[X]/\langle p(X) \rangle$ in $\mathbb{F}'[X]/\langle p_\varphi(X) \rangle$, ki kot kompozitum ostalih dokazanih izomorfizmov implicira izomorfnost $\mathbb{F}(a)$ in $\mathbb{F}'(a')$. Dobra definiranost $\tilde{\varphi}$ je očitna. □

2.1 Polja s karakteristiko 0

Lema 2.5

Naj bo $\mathbb{F}$ polje s karakteristiko 0. Potem ima vsak nerazcepen polinom nad $\mathbb{F}$ v vsaki razširitvi same enostavne ničle.

Oris dokaza. $\gcd(f(X), f'(X))$ je polinom v $\mathbb{F}[X]$, ki je nekonstanten in neničelen ter deli $f(X)$. □

Izrek 2.6

Naj bo $\mathbb{F}$ polje s karakteristiko 0, ter naj bo $f(X) \in \mathbb{F}[X]$ nekonstanten polinom. Naj bo $\mathbb{K}$ razpadno polje f, $\varphi : \mathbb{F} \to \mathbb{F}'$ izomorfizem polj ter $\mathbb{K}'$ razpadno polje $f_\varphi(X)$ nad $\mathbb{F}'[X]$. Potem obstaja natanko $[\mathbb{K} : \mathbb{F}]$ razširitev izomorfizmov φ na izomorfizem med $\mathbb{K}$ in $\mathbb{K}'$

Opazimo, da smo izreke zapisali v obliki razširitev izomorfizmov, ne pa v obliki razširitev polj (najpogosteje nas bo zanimalo le $\varphi = id_{\mathbb{F}}$). Če bi trditve zapisali na ta način, bi se dokazi otežili, saj bi s tem ošibili indukcijsko predpostavko.

Definicija 2.7

Razširitev polja $\mathbb{F}$ je *enostavna*, če je $K = F(a)$ za nek $a \in \mathbb{K}$. a tedaj imenujemo *primitivni element*.

Izrek 2.8: Izrek o primitivnem elementu

Vsaka končna razširitev polja s karakteristiko 0 je enostavna.

Oris dokaza. Zadosti pokazati, da če je $\mathbb{K} = \mathbb{F}(b, c)$, potem obstaja a, da je $\mathbb{K} = \mathbb{F}(a)$. b, c sta algebraična, saj je razširitev končna, zaporedoma imata minimalna polinoma $p(X)$ ter $q(X)$ nad $\mathbb{F}$. Naj bo $\mathbb{K}_1$ razširitev $\mathbb{K}$, v katerem $p(X)$ in $q(X)$ razpadeta. $b = b_1, \ldots, b_r$ naj bodo ničle $p(X)$ ter $c = c_1, \ldots, c_s$ ničle $q(X)$. Izberemo $\lambda \in \mathbb{F}$, ki ni enak $\frac{b_j - b}{c - c_k}$. Trdimo, da je $a = b + \lambda \cdot c$. Očitno je $\mathbb{F}(a) \subseteq F(b, c)$. Uvedimo $f(X) = p(a - \lambda X) \in \mathbb{F}(a)[X]$, velja $f(c) = 0$. Naj bo $\tilde{q}(X)$ minimalni polinom c nad $\mathbb{F}(a)$. Če bi bil $\tilde{q}(c_k) = 0$ za $k \neq 1$ bi bil $f(c_k) = 0 \implies p(a - \lambda c_k) = 0$, kar je nemogoče, po naši izbiri λ. Ker ima $\tilde{q}$ eno samo ničlo ter ima zgolj enostavne ničle pa je $\mathbb{F}(c) \subseteq \mathbb{F}(a)$, kar je bilo treba pokazati. □

3 Galoisova toerija

Dani sta polji $\mathbb{F}$ in $\mathbb{K}$, zanimala pa nas bodo »vmesna« polja $\mathbb{L}$, kjer je $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$.

Te bomo analizirali z opazovanjem grup avtomorfizmov polja $\mathbb{K}$, ki fiksirajo $\mathbb{F}$. Ponovno opomnimo, da bomo opazovali le tiste avtomorfizme, za katere je restrikcija na $\mathbb{F}$ identiteta. Da je ta množica grupa je očitno.

Naj bo G množica avtomorfizmov $\mathbb{K}$, ki fiksirajo $\mathbb{F}$ ter $\mathcal{G}$ množica podgrup grupe G. $\mathcal{G}$ bomo povezali s $\mathcal{F}$ - množico vmesnih polj med $\mathbb{F}$ in $\mathbb{K}$. Taka povezava je koristna, saj znamo o grupah povedati mnogo več kot o poljih, zato lahko vprašanja o poljih prevedemo na vprašanja o grupah, jih v grupah rešimo, ter odgovorimo na začetno vprašanje.

Najprej brez dokaza navedemo ključne trditve ter obravnavamo nekaj primerov.

3.1 Pregled Galoisove teorije

Primer 3.1

Naj bo $\mathbb{F} = \mathbb{R}$ ter $\mathbb{K} = \mathbb{C}$. Denimo, da bi obstajalo vmesno polje $\mathbb{L}$ med $\mathbb{R}$ in $\mathbb{C}$. Bodisi protislovje po stopnjah razširitev, bodisi ugotovimo, da če je $\ell \in \mathbb{L}$, potem je $\ell - \Re(\ell) \in \mathbb{L}$, posledično je $i \in \mathbb{L}$, sledi $\mathbb{L} = \mathbb{C}$, ali pa $\mathbb{L} = \mathbb{R}$, če so vsi elementi $\mathbb{L}$ realni.
Kaj pa vemo o avtomorfizmih $\mathbb{C}$, ki fiksirajo $\mathbb{R}$? Očitno je $\sigma(z) = \overline{z} \in G$. Ker velja $i^2 + 1 = 0$ je $\sigma'(i)^2 + \sigma'(1) = 0 \implies \sigma'(i)^2 = -1$, posledično je $\sigma'(i) \in \{-i, i\}$. Sledi, da je $\sigma' \in \{\mathrm{id}, \bar{\cdot}\}$.

Trditev 3.2

Za razširitev $\mathbb{K}$ polja $\mathbb{F}$ so ekvivalentni naslednji pogoji. Če velja eden izmed naslednjih pogojev je razširitev *Galoisova*.

- K je razpadno polje nekega polinoma iz $\mathbb{F}[X]$.
- Če ima nerzcepen polinom $p(X) \in \mathbb{F}[X]$ neko ničlo v $\mathbb{K}$, potem p razpade v $\mathbb{K}$.
- $|G| = [\mathbb{K} : \mathbb{F}]$.

Primer 3.3

Naj bo $\mathbb{F} = \mathbb{Q}$ ter $\mathbb{K} = \mathbb{Q}(\sqrt{2})$. Z enostavnim razmislekom o stopnjah razširitve dobimo $\mathcal{F} = \{\mathbb{Q}, \mathbb{Q}(\sqrt{2})\}$. Ponovno vidimo, da je $G = \{1, \sigma\}$, kjer je $\sigma(a + \sqrt{2}b) = a - \sqrt{2}b$. Z uporabo enačbe $\sqrt{2}^2 - 2 = 0$ ugotovimo, da smo našli vse avtomorfizme, ki fiksirajo $\mathbb{Q}$.

Primer 3.4

Naj bo $\mathbb{F} = \mathbb{Q}$ ter $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2})$. Ponovno je potrebno ugotoviti le kako generični avtomorfizem $\sigma \in G$ deluje na elementu $\sqrt[3]{2}$. Vemo, da je $\sqrt[3]{2}^3 - 2 = 0$, sledi, da je $\sigma(\sqrt[3]{2})^3 = 2$. Ker σ slika v $\mathbb{Q}(\sqrt[3]{2})$, v posebnem primeru v $\mathbb{R}$, pa obstaja le ena rešitev te enačbe, sledi, da je $\sigma = \text{id}$. Dobimo, da je $|G| = 1 = |\mathcal{G}|$, obenem pa je $\mathcal{F} = \{\mathbb{F}, \mathbb{K}, \dots\}$, kar se zdi v protislovju z zgornjo trditvijo. Seveda to ni protislovje, le ugotovili smo, da tudi prvi dve točki ne moreta veljati.

Definicija 3.5

Za vsak $H \in \mathcal{G}$ definirajmo *polje fiksnih točk podgrupe* H

$$\mathbb{K}^H = \{x \in \mathbb{K} \mid \sigma(x) = x \;\; \forall \sigma \in H\}$$

Opazimo, da je

$$\mathbb{K}^G = \mathbb{F} \quad \text{ter} \quad \mathbb{K}^{\{1\}} = \mathbb{K}.$$

Trditev 3.6

- Preslikava $H \to \mathbb{K}^H$ je bijekcija iz $\mathcal{G}$ v $\mathbb{F}$.
- $H \leq H'$ natanko tedaj, ko je $\mathbb{K}^{H'} \subseteq \mathbb{K}^H$
- $|H| = [\mathbb{K} : \mathbb{K}^H]$.

Primer 3.7

Naj bo $\mathbb{F} = \mathbb{Q}$ in $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Mar je $\mathbb{K}$ Galoisova razširitev? Seveda je K razpadno polje $(X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$. Sledi, da je $[\mathbb{K} : \mathbb{F}] = 4$, štiri podpolja pa so generirana z $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. Vidimo, da je $\sigma(\sqrt{2})^2 = 2$ ter $\sigma(\sqrt{3})^2 = 3$, kar poda le 4 možnosti za avtomorfizem σ, sledi $|G| = 4$. Ker imajo vsi avtomorfizmi red 2 je $G \cong \mathbb{Z}_2 \bigoplus \mathbb{Z}_2$.

Primer 3.8

Naj bo $\mathbb{F} = \mathbb{Q}$ ter za $\omega \in \mathbb{C} \setminus \mathbb{R}$, ki zadošča $\omega^3 = 1$ naj bo $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}, \omega)$. K je razpadno polje polinoma $X^3 - 2$. Velja, da je $[K : F] = 6$, zato pričakujemo, da je $|G| = 6$. Minimalni polinom ω je $X^2 + X + 1$. Seveda velja, da je vsak avtomorfizem, ki fiksira $\mathbb{F}$, določen s svojimi vrednostmi na $\sqrt[3]{2}$ ter ω. Izberemo bazo $1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega$, da je ta množica baza preverimo na standarden način, upoštevajoč, da je koefcient ω kot kompleksnega števila nujno 0.
Vemo, da je $\sigma(\sqrt[3]{2})^3 = 2$ ter, da je $\sigma(\omega)^3 = 1$, za sliko vsakega izmed $\sqrt[3]{2}$ in ω imamo tri možnosti za sliko. Opazimo lahko, da avtomorfizem σ, ki fiksira ω in slika $\sqrt[3]{2}$ v $\sqrt[3]{2}\omega$ ne komutira z avtomorfizmom ρ, ki fiksira $\sqrt[3]{2}$ ter slika ω v $\sqrt[3]{2}\omega$. Ker je G nekomutativna in reda 6 je izmorfna S_3.
Pogrupa S_3 s 3 elementi je A_3, sledi, da to generira σ. Ostale podgrupe generirajo transpozicije, namreč $\sigma, \sigma \cdot \rho$ ter $\sigma \cdot \rho^2$.

Izrek 3.9

$H \trianglelefteq G$ natanko tedaj, ko je $\mathbb{K}^H$ *Galoisova* razširitev $\mathbb{F}$ in je $G/H \cong \mathrm{Aut}(\mathbb{K}^H/\mathbb{F})$.

3.2 Legitimizacija Galoisove teorije

Naj bo $\mathbb{F}$ podpolje $\mathbb{K}$. $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$ naj bo grupa avtomorfizmov $\mathbb{K}$, ki fiksirajo $\mathbb{F}$.

Lema 3.10

Če je $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{F})$ in je $a \in \mathbb{K}$ ničla $f(X) \in \mathbb{F}[X]$, potem je $\sigma(a)$ ničla $f(X)$.

Avtomorfizmi, ki fiksirajo bazno polje, tako permutirajo ničle polinomov.

Po izreku o primitvnem elementu lahko vsako končno razširitev $\mathbb{K}$ polja $\mathbb{F}$ zapišemo kot razširitev v elementu $a \in \mathbb{K}$. Vsak avtomorfizem je tako enolično določen z delovanjem v a. Naj bo $p(X)$ minimalni polinom a nad $\mathbb{F}$. Sledi, da vsak avtomorfizem, ki fiksira $\mathbb{F}$, le permutira ničle $p(X)$, zato je avtomorfizmov največ $\deg(p)$. Po eni izmed lem iz prejšnjega predavanja (komutativni diagram) pa vemo, da je avtomorfizmov natanko $\deg(p(X)) = [\mathbb{K} : \mathbb{F}]$.

Literatura

[1] prof. dr. Matej Brešar. *Predavanja Algebre 3*. 2025.