Algebra 3

Hugo Trebše (hugo.trebse@gmail.com)

23. november 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 $\mathbb{F}(a)$. $\square$

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. $\square$

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 razširimo do izomorfizma med $\mathbb{F}(a)$ in $\mathbb{F}'(a')$. Enoličnost je očitna. Definiramo lahko $\tilde{\varphi}$ kot naravni izomorfizem 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. $b = b_1, \dots, b_r$ naj bodo ničle $p(X)$ ter $c = c_1, \dots, c_s$ 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 teorija

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 nerazcepen 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

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

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 $\omega \in \mathbb{C} \backslash \mathbb{R}$, 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 koeficient 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 izomorfna S_3.
Podgrupa 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 $\mathbb{F}$. Pogosto bomo $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$ označevali z G.

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 primitivnem 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 na 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 $\deg(p(X)) = [\mathbb{K} : \mathbb{F}]$.

Trditev 3.11

Avtomorfizmov $\mathbb{K}$, ki fiksirajo $\mathbb{F}$ je natanko $\deg(p)$, kjer je p minimalni polinom primitivnega elementa $\mathbb{K} : \mathbb{F}$, s koeficienti v $\mathbb{F}$.

Kot v prejšnjem podpoglavju definiramo za $H \leq G$ *polje fiksnih točk* H kot

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

Dve ključni lemi sta: (v obeh predpostavimo $\mathrm{char}(\mathbb{F}) = 0$)

Lema 3.12

Naj bo $H \leq G$ ter $[\mathbb{K} : \mathbb{F}] < \infty$. Naj bo $a \in \mathbb{K}$ in naj bodo $a = a_1, \ldots, a_m$ različni elementi množice $\{\sigma(a) \mid \sigma \in H\}$. Potem je

$$p(X) = (X - a_1) \ldots (X - a_m) \text{ minimalni polinom } a \text{ nad } \mathbb{K}^H.$$

Oris dokaza. Preverimo, da ima p koeficiente v $\mathbb{K}^H$. Če je $p(X) = \sum_{i=0}^m \alpha_i X^i$, potem je $p_\rho(X) = \sum_{i=0}^m \rho(\alpha_i) X^i$. Vsak a_i je oblike $\sigma_i(a)$ za nek $\sigma_i \in H$. Sledi, da je $\rho(a_i) \in \{\sigma(a) \mid \sigma \in H\}$, posledično ρ permutira to množico, saj je namreč injektiven. Sledi, da je $p_\rho(X) = p(X) \implies \rho(\alpha_i) = \alpha_i \implies \alpha_i \in \mathbb{K}^H$.

Naj bo $f(X) \in \mathbb{K}^H[X]$ tak, da je $f(a) = 0$, posledično so tudi vsi a_i ničle f. Sledi, da $p \mid f$. □

Lema 3.13

$$|H| = [\mathbb{K} : \mathbb{K}^H] \text{ ter } [\mathbb{K} : \mathbb{F}] = |H| \, [\mathbb{K}^H : \mathbb{F}].$$

Oris dokaza. Treba je pokazati le prvo trditev. Naj bo $\mathbb{K} = \mathbb{F}(a)$, zato velja tudi $\mathbb{K} = \mathbb{K}^H(a)$. Sledi, da je $[\mathbb{K} : \mathbb{K}^H] = m = \deg(m_a(X))$, kjer je $m_a(X)$ minimalni polinom a nad $\mathbb{K}^H$. Po zgornji lemi je $m = |\{\sigma(a) \mid \sigma \in H\}| = |H|$, kjer zadnja enakost velja, ker različna avtomorfizma iz H elementa a, kot primitivnega elementa, ne morata preslikati v isti element. □

Izrek 3.14

Naj bo $[\mathbb{K} : \mathbb{F}] < \infty$ ter $\mathrm{char}(\mathbb{F}) = 0$. Naslednje trditve so ekvivalentne:

- $|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| = [\mathbb{K} : \mathbb{F}]$.
- $\mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})} = \mathbb{F}$.
- Vsak nerazcepen polinom nad $\mathbb{F}$ z ničlo v $\mathbb{K}$ razpade v $\mathbb{K}$.
- $\mathbb{K}$ je razpadno polje nekega nerazcepnega polinoma iz $\mathbb{F}[X]$.
- $\mathbb{K}$ je razpadno polje nekega polinoma iz $\mathbb{F}[X]$.

Dokaz. Označujmo $G = \mathrm{Aut}(\mathbb{K}/\mathbb{F})$. Uporabimo drugo lemo v primeru $H = G$, sledi, da je $[\mathbb{K}^G : \mathbb{F}] = 1$, kar pokaže implikacijo.

Naj bo $p(X)$ minimalni polinom elementa $a \in \mathbb{K}$ nad $\mathbb{F}$. Po prvi lemi v primeru $H = G$ in upoštevajoč $\mathbb{K}^G = \mathbb{F}$ dobimo, da je $p(X) = \prod_{i=1}^m (X - \sigma_i(a))$, ter je $p(X) \in \mathbb{F}[X]$ ter so $\sigma_i(a) \in \mathbb{K}$.

Uporabimo izrek o primitivnem elementu, naj bo $\mathbb{K} = \mathbb{F}(a)$ ter $p(X)$ minimalni polinom a nad $\mathbb{F}$. $p(X)$ razpade na produkt linearnih faktorjev v $\mathbb{K}[X]$. K je najmanjše polje v katerem razpade p, saj je $\mathbb{K}$ najmanjše polje, ki vsebuje ničlo a.

Zadnja točka implicira prvo po izreku 2.1. □

Če razširitev $\mathbb{K}$ zadošča enemu izmed zgornjih pogojev jo imenujemo *Galoisova* razširitev. Tedaj označujemo $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$ tudi z $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$. Če je $\mathbb{K}$ razpadno polje polinoma f, potem $\mathbb{K}$ imenujemo tudi *Galoisova razširitev* polinoma f.

Opomba: Splošneje (zunaj karakteristike 0) Galoisovo razširitev vpeljemo preko pojma normalnosti in separabilnosti. Razširitev je *normalna*, če je algebraična in zadošča tretji točki zgornjega izreka Razširitev je *separabilna*, če je vsak nerazcepen polinom separabilen - ima vse ničle enostavne.

Opomba: $\mathbb{K}$ naj bo Galoisova razširitev $\mathbb{F}$ in $\mathbb{L}$ vmesno polje. Potem je $\mathbb{K}$ tudi Galoisova razširitev $\mathbb{L}$ (saj je razpadno polje istega polinoma nad $\mathbb{L}$ kot nad $\mathbb{F}$).

Izrek 3.15: Osnovni izrek Galoisove teorije

Naj bo $\mathbb{K}$ Galoisova razširitev polja $\mathbb{F}$ s katakteristiko 0. Označimo s $\mathcal{F}$ množico vseh vmesnih polj med $\mathbb{F}$ in $\mathbb{K}$ ter naj bo $\mathcal{G}$ množica vseh podgrup grupe $\mathrm{Gal}(\mathbb{K}/\mathbb{F}) = G$.

- Preslikava $\alpha : \mathcal{G} \to \mathcal{F}$, kjer je
$$\alpha(H) = \mathbb{K}^H$$
je *bijektivna* in njena inverzna preslikava je $\beta : \mathcal{F} \to \mathcal{G}$, kjer je
$$\beta(\mathbb{L}) = \mathrm{Gal}(\mathbb{K}/\mathbb{L}).$$
- Če H ustreza $\mathbb{L}$: $\mathbb{L} = \mathbb{K}^H$ ali ekvivalentno $\mathrm{Gal}(\mathbb{K}/\mathbb{L}) = H$, potem je
$$|H| = [\mathbb{K} : \mathbb{L}] \text{ ter } [G : H] = [\mathbb{L} : \mathbb{F}].$$
- Če H ustreza $\mathbb{L}$ in H' ustreza $\mathbb{L}'$, potem je
$$H \subseteq H' \iff \mathbb{L}' \subseteq \mathbb{L}.$$
- Če H ustreza $\mathbb{L}$, potem je
$$H \trianglelefteq G \iff \mathbb{L} \text{ je Galoisova razširitev } \mathbb{F}.$$
Tedaj velja tudi
$$G/H \cong \mathrm{Gal}(\mathbb{L}/\mathbb{F}).$$

Oris dokaza. $\alpha(\beta(\mathbb{L})) = \alpha(\mathrm{Gal}(\mathbb{K}/\mathbb{L}))$ ter $\beta(\alpha(H) = \mathrm{Gal}(\mathbb{K}/\mathbb{K}^H)$, želeli, bi pokazati $\mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{L})} = \mathbb{L}$ in $\mathrm{Gal}(\mathbb{K}/\mathbb{K}^H) = H$. Ker je $\mathbb{K}$ Galoisova razširitev $\mathbb{L}$ in zaradi druge točke izreka na prejšnji strani sledi prva enakost.

Očitno velja, da je $H \subseteq \mathrm{Gal}(\mathbb{K}/\mathbb{K}^H)$. Treba je dokazati le še, da imata grupi isti red. Po drugi lemi sledi, da je $|H| = [\mathbb{K} : \mathbb{L}]$ in po prvi točki izreka je $[\mathbb{K} : \mathbb{L}] = |\mathrm{Gal}(\mathbb{K}/\mathbb{L})|$.

Prva enakost druge točke sledi po lemi 2. Druga enakost druge točke pa sledi po uporabi Lagrangevega izreka.

Pokažimo četrto točko privzemši 1.. Naj H ustreza $\mathbb{L}$, $\mathbb{L} = \mathbb{K}^H$ in $H = \mathrm{Gal}(\mathbb{K}/\mathbb{L})$.

$$H \trianglelefteq G \iff \sigma^{-1}\rho\sigma \in H \; \forall\sigma \in H \land \forall\rho \in H.$$

Zato bi želeli pokazati, da je za vse $l \in \mathbb{L}$: $\rho(\sigma(l)) = \sigma(l)$, ker pa je $\mathbb{L} = \mathbb{K}^H$ pa je to ekvivalentno $\sigma(l) \in \mathbb{L}$, saj je $\sigma(l)$ fiksna točka ρ. Tako je $H \trianglelefteq G \iff \sigma(\mathbb{L}) \subseteq \mathbb{L} \iff \sigma(\mathbb{L}) = \mathbb{L}$, kjer zadnja ekvivalenca velja, ker je σ injektiven, ter ker je $\mathbb{L}$ končno-dimenzionalen vektorski prostor nad $\mathbb{F}$. Definirajmo $\varphi : G \to \mathrm{Aut}(\mathbb{L}/\mathbb{F}) \implies \phi(\sigma) = \sigma|_{\mathbb{L}}$. Ker je $G/\ker(\varphi) \cong \mathrm{im}(\varphi) \ldots$ □

Avtomorfizem polinomske razširitve je določen s slikami ničel (saj so generatorji) ter jih permutira.

3.3 Rešljivost polinomskih enačb z radikali

»Rešljive grupe so blizu Abelovih grup«.

Definicija 3.16

Grupa G je rešljiva, če obstajajo take edinke v G: $N_0 = \{1\} \leq N_1 \leq N_2 \leq \cdots \leq N_m = G$, da je N_{i+1}/N_i Abelova grupa za $i = 0, \ldots, m-1$.

Primer 3.17

S_3 ima edinko A_3: $N = A_3 \triangleleft S_3$. $N \cong \mathbb{Z}_3$ je Abelova ter $G/N \cong \mathbb{Z}_2$ je Abelova. S_3 je tako rešljiva grupa. Tudi S_4 je rešljiva, najmanjši primer je za $m = 3$.

Izrek 3.18: Feit-Thompson

Vsaka končna grupa lihega reda je rešljiva.

Izrek 3.19: Burnside

Grupa reda $p^a \cdot q^b$, kjer sta $p, q \in \mathbb{P}$ ter $a, b \in \mathbb{Z}^+$ je rešljiva.

Trditev 3.20

Nekomutativna enostavna grupa ni rešljiva.

Zgornja trditev je očitna. Primer nerešljive grupe je A_5.

Trditev 3.21

- Podgrupa rešljive grupe je sama rešljiva.
- Naj bo $N \triangleleft G$. Potem je G rešljiva natanko tedaj, ko sta N in G/N rešljivi.

Iz druge točke sledi, da S_n za $n \geq 5$ ni rešljiva, saj vsebuje A_5.

Lema 3.22

Naj bo $\mathbb{F}$ podpolje $\mathbb{C}$ ter $\alpha \in \mathbb{F}$. Potem je Galoisova grupa polinoma $f(X) = X^n - \alpha$ rešljiva za vsak $n \in \mathbb{N}$.

Oris dokaza. $\mathbb{K} = \mathbb{F}(a, \omega)$, kjer je a poljubna rešitev $a^n = \alpha$ ter $\omega = e^{\frac{2\pi i}{n}}$, je razpadno polje f.

$\mathbb{F}(\omega)$ je razpadno polje $X^n - 1$, zato lahko govorimo o $\mathrm{Gal}(\mathbb{F}(\omega)/\mathbb{F})$ ter o generičnih avtomorfizmih σ, ρ iz slednje. σ ter ρ sta določena z vrednostjo v ω, zato velja $\sigma(\omega) = \omega^i$ ter $\rho(\omega) = \omega^j$. Vidimo, da je $\rho \circ \sigma = \sigma \circ \rho$, zato je $\mathrm{Gal}(\mathbb{F}(\omega)/\mathbb{F})$ Abelova.

$\mathrm{Gal}(\mathbb{K}/\mathbb{F}(\omega))$ je Galoisova, saj je $\mathbb{K}$ razpadno polje f tudi nad $\mathbb{F}(\omega)$. Če sta σ', ρ' avtomorfizma iz slednje grupe, ki sta seveda določena z vrednostjo v a. Po enakem postopku dokažemo, da je $\mathrm{Gal}(\mathbb{K}/\mathbb{F}(\omega))$ Abelova, saj σ' ter ρ' fiksirata $\mathbb{F}(\omega)$.

Po četrti točki osnovnega izreka Galoisove teorije sledi, da je $\mathrm{Gal}(\mathbb{K}/\mathbb{F}(\omega)) = H \lhd G = \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ ter, da je $G/H \cong \mathrm{Gal}(\mathbb{F}(\omega)/\mathbb{F})$, ki je Abelova. Zato sledi, da je $\mathrm{Gal}(\mathbb{F}(a, \omega)/\mathbb{F})$ rešljiva. □

Definicija 3.23

Naj bo $\mathbb{F}$ polje. Polinom $f(X) \in \mathbb{F}[X]$ je *rešljiv z radikali* nad $\mathbb{F}$, če obstajajo taki elementi $a_1, \dots, a_m$ iz neke razširitve $\mathbb{F}$, da:

- $f(X)$ razpade v $\mathbb{F}(a_1, \dots, a_m)$.
- Obstajajo $n_1, \dots, n_m \in \mathbb{N}$, da je $a_1^{n_1} \in \mathbb{F}$ ter $a_i^{n_i} \in \mathbb{F}(a_1, \dots, a_{i-1})$ za vse $1 < i \leq m$.

Intuitivno lahko preverimo, da pogoja dejansko predstavljata to, kar mislimo, ko rečemo, da je polinom rešljiv z radikali.

Primer 3.24

Naj bodo $a, b, c \in \mathbb{C}$ ter $f(X) = aX^2 + bX + c$ ter naj bo $\mathbb{F} = \mathbb{Q}(a, b, c)$. f je rešljiv z radikali nad $\mathbb{F}$.

Oris dokaza. $a_1 = \sqrt{b^2 - 4ac}$. Seveda $f(X)$ razpade v $\mathbb{F}(a_1)$ ter $a_1^2 \in \mathbb{F}$. □

Izrek 3.25: Konsistenca rešljivosti

Naj bo $\mathbb{F}$ podpolje $\mathbb{C}$ in $f(X) \in \mathbb{F}[X]$. Če je polinom rešljiv z radikali nad $\mathbb{F}$, potem je Galoisova grupa polinoma f rešljiva.

Izrek pustimo brez dokaza. Pravzaprav pa celo velja, da je rešljivost polinoma z radikali **ekvivalentna** rešljivosti njegove Galoisove grupe.

Lema 3.26

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 $\mathbb{Q}$

Dokaz. Zaradi nerazcepnosti ima p pet različnih ničel $a_1, \dots, a_5$, naj bodo prve tri realne. Naj bo $\mathbb{K} = \mathbb{Q}(a_1, \dots, a_5)$ razpadno polje p. Želimo pokazati, da Galoisova grupa p ni rešljiva, saj smo uporabili izrek o konsistenci rešljivosti. Vsak avtomorfizem je določen s slikami ničel ter slednje permutira.

Imamo očitno vložitev $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ v S_5. Ker je konjugiranje avtomorfizem G gotovo vsebuje transpozicijo.

Naj bo $a \in \{a_1, \dots, a_5\}$. a je ničla nerazcepnega polinoma $p(X)$ stopnje 5, zato je a algebraično število stopnje 5, sledi $[\mathbb{Q}(a) : \mathbb{Q}] = 5$. Ker je $\mathbb{Q} \subset \mathbb{Q}(a) \subset \mathbb{K}$ sledi, da $5 \mid [\mathbb{K} : \mathbb{Q}] \implies 5 \mid G$. Po Cauchyjevem izreku ima G element reda 5, zato G vsebuje 5-cikel.

Kratek račun iz teorije grup pove, da če G vsebuje transpozicijo in 5-cikel, potem je $G = S_5$. Ker G vsebuje A_5 sledi, da ni rešljiva. $\square$

Izrek 3.27: Abel-Ruffini

Obstajajo polinomi v $\mathbb{Q}[X]$ stopnje 5, ki niso rešljivi z radikali nad $\mathbb{Q}$.

Dokaz. $f(X) = X^5 - 3X^4 + 3$ je nerazcepen po Eisensteinovem kriteriju ter ima tri realne ničle, saj je $f(-1) = -1$, $f(0) = 3$, $f(2) < 0$ ter $f(3) > 0$. Odvod $f'(X)$ ima le dve ničli, zato f nima petih realnih ničel po Rolleovem izreku. $\square$

3.4 Vaje

Naloga 3.28

Določi $\mathrm{Aut}(\mathbb{R})$.

Oris dokaza. Vemo, da je $f(x)+f(y)=f(x)+f(y)$ ter $f(xy)=f(x)f(y)$. Vemo, da je f na $\mathbb{Q}$ identiteta. Želimo pokazati zveznost f. Ker je $f(x^2)=f(x)^2$ hitro dobimo, da je $f(x)=f(y)+f(x-y)=f(y)+f(\sqrt{x-y})^2>f(y)$ za $x>y$, f je tako monotona. Velja, da je $f(x)-f(a)=f(x-a)<f(q)$ za neko racionalno število q, za katero velja, da je $|x-a|<q$. Zveznost sledi. $\square$

Nauk: Relacija urejenosti lahko izrazimo *algebraično*:

$$x>y \iff \exists\lambda\in\mathbb{R}\; x-y=\lambda^2.$$

Naloga 3.29

Določi zvezne elemente $\mathrm{Aut}(\mathbb{C})$.

Oris dokaza. f fiksira $\mathbb{Q}$. Ker je $\mathbb{Q}$ gosta v $\mathbb{R}$ sledi, da f fiksira tudi $\mathbb{R}$.
$i^2+1=0 \implies f(i)\in\{i,-i\}$ $\square$

Nauk: Pri algebraičnih razširitvah iščemo minimalne polinome generatorjev razširitve, nato pa vemo, da avtomorfizem permutira ničle.

Kaj pa nezvezni elementi $\mathrm{Aut}(\mathbb{C})$? Te konstruiramo s pomočjo izbire.

Splošna uporaba *Zornove leme* $\{(K,\pi)\mid \mathbb{F}\subseteq K\subseteq\mathbb{C},\pi:\mathbb{K}\to\mathbb{C}\}$. Uvedemo delno urejenost: $(K,\pi)\subseteq(K',\pi') \iff K\subseteq K'$ ter $\pi'|_K=\pi$. Obstaja zgornja meja verige, zato imamo maksimum.

Pomnimo, da je $\mathbb{K}/\mathbb{F}$ *Galoisova razširitev*, če je K razpadno polje nekega polinoma nad $\mathbb{F}$. V Galoisovi razširitvi vsak nerazcepen polinom nad $\mathbb{F}$, ki ima ničlo v $\mathbb{K}$, razpade v $\mathbb{K}$.

Naloga 3.30

Vsaka kvadratična razširitev $\mathbb{K}/\mathbb{F}$ je Galoisova.

Oris dokaza. Po Vietu je vsota ničel v $\mathbb{F}$, če vsebuje eno seveda tudi drugo. $\square$

Naloga 3.31

Ali je $\mathbb{Q}(\sqrt[4]{2}/\mathbb{Q})$ Galoisova razširitev? Poišči $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$.

Oris dokaza. Ako bi bila Galoisova bi vsebovala vse ničle polinoma $X^4 - 2$, kompleksnih ničel pa seveda ne vsebuje. Po klasičnem argumentu o permutaciji ničel dobimo, da sta edina avtomorfizma identiteta ter »konjugiranje«. $\square$

Naloga 3.32

Če sta $\mathbb{K}/\mathbb{F}$ in $\mathbb{L}/\mathbb{K}$ Galoisova, ali sledi, da je $\mathbb{L}/\mathbb{F}$ Galoisova?

Oris dokaza. Vse kvadratične razširitve so Galoisove, pogledamo $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[2]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ $\square$

Naloga 3.33

Pokaži, da lahko Galoisovo grupo polinoma stopnje n vložimo v S_n.

Oris dokaza. Galoisova grupa polinoma je tu mišljena kot Galoisovo grupo razpadnega polja polinoma. Ničle oštevilčimo, nato imamo naravno vložitev. $\square$

3.4.1 Drugi pregled Galoisove teorije

Naj bo razširitev $\mathbb{K}/\mathbb{F}$ Galoisova ter $G = \mathrm{Gal}(\mathbb{K}/\mathbb{F})$. Velja, da je $|G| = [\mathbb{K} : \mathbb{F}]$ ter obstaja bijektivna korespondenca med vmesnimi polji med $\mathbb{K}$ in $\mathbb{F}$ ter med podgrupami G. Korespondenca slika podgrupo v polje fiksnih točk avtomorfizmov te grupe. Če je eno izmed vmesnih polj Galoisova razširitev drugega vmesnega polja, potem je pripadajoča grupa edinka v grupi drugega podpolja (»normalne« razširitve ustrezajo »normalnim« podgrupam.)

Naloga 3.34

Naj bo $\mathbb{K} = \mathbb{F}(\sqrt{a}, \sqrt{b})$, kjer sta $a, b \in \mathbb{F}$ ter je $[\mathbb{K} : \mathbb{F}] = 4$. Pokaži, da je $\mathbb{K}/\mathbb{F}$ Galoisova ter določi strukturo podpolj.

Oris dokaza. $f(X) = (X^2 - a)(X^2 - b)$ je polinom, katerega razpadno polje je $\mathbb{K}$. Sledi, da je razširitev Galoisova. Očitni so štirje kandidati za avtomorfizme, ker je razširitev Galoisova in ker je $[\mathbb{K} : \mathbb{F}] = 4$ sledi, da je $\mathrm{Gal}(\mathbb{K}/\mathbb{F}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ po preprostem argumentu z redi. $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ ima tri prave netrivialne podgrupe, ki jih generirajo elementi reda 2. Tri vmesna polja med $\mathbb{K}$ in $\mathbb{F}$ so tako $\mathbb{F}(\sqrt{a})$, $\mathbb{F}(\sqrt{b})$ ter $\mathbb{F}(\sqrt{ab})$. $\square$

Naloga 3.35

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

Oris dokaza. Naj bo $\zeta = e^{\frac{2i\pi}{7}}$. Velja $[\mathbb{K} : \mathbb{Q}] = 6$, saj je $m_\zeta(X) = X^6 + \cdots + 1$. Sledi, da je $\mathbb{K}/\mathbb{Q}$ Galoisova. Vemo, da je $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \in \{S_3, \mathbb{Z}_2 \times \mathbb{Z}_3\}$. Ker je $[\mathbb{K} : \mathbb{Q}] = 6$ velja, da so atomorfizmi ravno $\sigma_i : x \mapsto x^i$ za $i \in \{1, \ldots, 6\}$. Ker avtomorfizmi komutirajo (očitno) sledi, da je $\mathrm{Gal}(\mathbb{K}/\mathbb{F}) = \mathbb{Z}_2 \times \mathbb{Z}_3$. Ustrezni podgrupi reda 2 ter reda 3 generirata $\rho : x \mapsto x^3$ ter $\psi : x \mapsto x^2$.

Kako določimo polje fiksnih točk ρ?. Vemo, da je $\mathbb{K}^\rho = \langle \sum_{i=0}^5 a_i\zeta^i \mid \rho(x) = x\rangle$. Zapišemo izraz $\sum_{i=0}^5 a_i\zeta^i = \sum_{i=0}^5 a_i\rho(\zeta^i) = \sum_{i=0}^5 a_i\zeta^{2i}$ ter primerjamo koeficiente. Z nekaj računske spretnosti ugotovimo, da je element $\zeta^5+\zeta^2$ generator enega izmed podpolj, namreč tistega s stopnjo razširitve 3, saj je njegov minimalni polinom $X^3 + X^2 - 2X - 1$, ki je očitno nerazcepen.

Enak posopek ponovimo na $\mathbb{K}^\psi$, ter ugotovimo, da je generator $\zeta + \zeta^2 + \zeta^4$. Ker ima ta minimalni polinom $X^2 + X + 2$ lahko s kvadratno formulo dobimo, da $\mathbb{K}^\psi$ generira $\sqrt{-7}$. □

3.4.2 Kaj se zgodi, če razširitev ni Galoisova?

Odgovor: *Razširimo polje, dokler ne pridemo do Galoisove razširitve, nato pa uporabimo našo teorijo.*

Naloga 3.36: Galoisovo zaprtje

Določi podpolja $\mathbb{K} = \mathbb{Q}(\sqrt[4]{2})$.

Oris dokaza. Opazujemo $\mathbb{K}(i)$, ki je razpadno polje nerazcepnega polinoma $X^4 - 2$. Ker je $[\mathbb{K} : \mathbb{Q}] = 4$ in je $[\mathbb{K}(i) : \mathbb{K}] = 2$ velja, da je za $G = \mathrm{Gal}(\mathbb{K}(i)/\mathbb{Q})$, $|G| = 8$. Za generični avtomorfizem σ velja, da je $\sigma(\sqrt[4]{2}) \in \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$, ter da je $\sigma(i) \in \{\pm i\}$. Sestavimo:

$$\sigma_{k,l} = \begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2} \cdot i^k, & k \in \mathbb{Z}_4 \\ i \mapsto (-1)^l i, & l \in \mathbb{Z}_2 \end{cases}$$

Naj bo $\omega = \sqrt[4]{2}$. Opazimo, da je

$$\sigma_{0,1} \circ \sigma_{1,0} = -i\omega$$

ter

$$\sigma_{1,0} \circ \sigma_{0,1} = i\omega,$$

zato G ni komutativna.

Nekomutativni grupi reda 8 sta $D_8 = \langle r, z \,|\, r^4 = 1, zrz = r^{-1}\rangle$ ter $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. Za Q_8 vemo, da je vsaka podgrupa edinka, kar ni mogoče, saj razširitev $\mathbb{K}/\mathbb{Q}$ ni Galoisova, zato je $G \cong D_8$.

Očitno velja, da sta $\langle \sigma_{0,1}\rangle$ ter $\mathbb{K}$ v korespondenci, zato nas zanimajo podgrupe D_8 vsebujoč z. Te podgrupe določimo s standardnim postopkom. □

Naloga 3.37

Naj bo $\mathbb{K}$ razpadno polje $x^5 - 2$. Določi vse $a \in \mathbb{Z}$, za katere je $\sqrt{a} \in \mathbb{K}$.

Oris dokaza. Naj bo $\mathbb{K} = \mathbb{Q}(\omega = e^{\frac{2\pi i}{5}}, \sqrt[5]{2})$. Sledi, da je $[\mathbb{K} : \mathbb{Q}] = 20$. Želeli bi pokazati, da obstaja podpolje reda 2. Določimo najprej $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. Gotovo je $\bar{\cdot}$ avtomorfizem. Vemo, da je $\sigma(\sqrt[5]{2}) \in \{\sqrt[5]{2}\omega^b \mid j \in \{0, 1, 2, 3, 4\}\}$ ter $\sigma(\omega) \in \{\omega^a \mid a \in \{1, 2, 3, 4\}\}$. Vsaka izbira para (a, b) poda enolično določen avtomorfizem, ker je $|G| = 20$ sledi, da so to vsi avtomorfizmi v G po naslednjem razmisleku.

$\sigma_{a,b}(\sqrt[5]{2}\omega^i) = \sqrt[5]{2}\omega^{ai+b}$. Z analizo komponiranja preslikav ugotovimo, da je $G \cong \mathbb{Z}_5 \rtimes \mathbb{Z}_4$. Zanimajo nas podgrupe reda 10 grupe $\mathbb{Z}_5 \rtimes \mathbb{Z}_4$. Po Cauchyjevem izreku mora taka podgrupa vsebovati element reda 5 in element reda 2.

Ker je $\mathbb{Q}(\omega)$ razširitev $\mathbb{Q}$ stopnje 4 vemo iz enega izmed prejšnjih primerov ($\mathbb{Q}(e^{\frac{2\pi i}{7}})$), da je razširitev reda 2 ravno $\mathbb{Q}(\sqrt{5}) \cong \mathbb{Q}(\omega + \omega^{-1})$. Velja, da $\omega + \omega^{-1} \notin \mathbb{Q}$, hkrati pa tudi ni v $\mathbb{C}$. $\square$

3.4.3 Komutativne Galoisove grupe

Naloga 3.38

Kako vidimo, da je $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ komutativna iz strukture podpolj?

Ker so vse podgrupe komutativne grupe edinke, sledi, da so vsa podpolja Abelove Galoisove razširitve Galoisova.

Ali velja tudi obratno? Odgovor je ne, saj ima Q_8 vse podgrupe za edinke, a ni komutativna grupa. Velja, saj je $\langle 1 \rangle < \langle -1 \rangle < \langle i \rangle, \langle j \rangle, \langle k \rangle < Q_8$.

Če so vse podgrupe edinke, potem pravimo grupi *Dedekindova*. Dedekindove grupe so komutativne ali pa so G, kjer je $G/N \cong Q_8$.

Trditev 3.39

$G = \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ je komutativno natanko tedaj, ko je vsako vmesno podpolje Galoisovo ter v strukturi polj ni diamantnega uhana, ki ga tvori diagram podgrup Q_8.

Literatura

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