A

1. Ak A a B sú normálne podgrupy G, $a \in A$ a $b \in B$, tak $aba^{-1}b^{-1} \in A \cap B$.

2. Ak I_1, I_2 sú ideály v okruhu $(R, +, \cdot)$, tak aj
a) $I_1 + I_2 = \{a + b; a \in I_1, b \in I_2\}$ je ideál v R.
b) $I_1.I_2 = \{a_1b_1 + \dots + a_nb_n; n \in \mathbb{N}, a_i \in I_1, b_i \in I_2\}$ je ideál v R.

3. Nájdite izomorfizmus medzi poľami $\mathbb{Z}_3[x]/(x^2 + 1)$ a $\mathbb{Z}_3[x]/(x^2 + x + 2)$.

4. Nájdite rozklad polynómu $x^4 + 4x^2 + 8$ $(x^4 + 4x^2 + 16)$[1] na ireducibilné polynómy v $\mathbb{C}[x]$, v $\mathbb{R}[x]$ a v $\mathbb{Q}[x]$.

A

3. Oba polynómy vystupujúce v zadaní sú ireducibilné (polynómy stupňa 2 bez koreňov), pre sú to skutočne polia. Pole $K = \mathbb{Z}_3[x]/(x^2 + 1)$ pozostáva z prvkov tvaru $au + b$, kde $a, b \in \mathbb{Z}_3$ a $u = x + (x^2 + 1)$ je trieda rozkladu obsahujúca polynóm x. Podobne $L = \mathbb{Z}_3[x]/(x^2 + x + 2)$ pozostáva z prvkov tvaru $av + b$, kde v označuje triedu rozkladu x v rozklade podľa ideálu $(x^2 + x + 2)$.

Všimnime si, že v $\mathbb{Z}_3[x]$ platí $(x + 2)^2 = x^2 + x + 1$, čiže $(x + 2)^2 + 1 = x^2 + x + 2$. To nám hovorí, že v $\mathbb{Z}_3[x]/(x^2 + x + 2)$ platí $(v + 2)^2 + 1$ je koreň polynómu $x^2 + 1$. Skúsme voliť náš izomorfizmus f tak, že u (koreň polynóm $x^2 + 1$ v K) zobrazíme na $v + 2$ (koreň polynómu $x^2 + 1$ v L) a f nemení prvky zo $\mathbb{Z}_3$. (Každý izomorfizmus zobrazí jednotku na jednotku, z čoho vyjde, že musí zachovávať prvky $\mathbb{Z}_3$ a aj to, že zachováva korene – riešenia polynomiálnych rovníc – ak koeficienty sú zo $\mathbb{Z}_3$. Čiže pre f sme vlastne ani veľmi nemali inú možnosť – nanajvýš sme za $f(u)$ mohli zvoliť druhý koreň polynómu $x^2 + 1$.)

$$f \colon K \to L$$
$$f \colon a + bu \mapsto a + b(v + 2) = a + 2b + bv$$

To, že f je izomorfizmus, môžeme overiť viacerými spôsobmi:
a) Priamym overením definície, pričom okrem overenia, že f zachováva súčin sú ostatné časti ľahké.[2]

$$f(a + bu)f(c + du) = [(a + 2b) + bv][(c + 2d) + dv] =$$
$$= (a + 2b)(c + 2d) + [(a + 2b)d + b(c + 2d)]v + bd[2v + 2] = (ac + 2bc + 2ad + 2bd) + (ad + bc)v$$
$$f((a + bu)(c + du)) = f(ac + 2bd + (ad + bc)u) = (ac + 2bd + 2ad + 2bc) + (ad + bc)v$$

b) Overením, že zobrazenie $g(x) \mapsto g(x + 2)$ je izomorfizmus $\mathbb{Z}_3[x]$, ktorý zobrazí ideál $(x^2 + 1)$ na ideál $(x^2 + x + 1)$ – potom musia byť aj faktorové okruhy izomorfné.

Fakt, že dané polia sú izomorfné, vyplýva aj z toho, že existuje jediné pole, ktoré má 3^2 prvkov – to je v časti, ktorú som už nestihol odprednášať (nepovinne si ju môžete prečítať).

4. Prvý spôsob riešenia je tak trochu trikový – prinajmenšom ak človek niečo také vidí po prvýkrát. Nad $\mathbb{Q}$ aj nad $\mathbb{R}$ máme rozklad $x^4 + 4x^2 + 16 = (x^2 + 4)^2 - 4x^2 = (x^2 + 2x + 4)(x^2 - 2x + 4)$. V $\mathbb{C}$ dostaneme rozklad na koreňové činitele, korene polynómov $(x \pm 1)^2 + 3$ sú $\pm 1 \pm \sqrt{3}i$.

Štandardný postup by bol: substitúcia $t = x^2$, riešim kvadratickú rovnicu $t^2 + 2t + 16 = 0$ a dostanem 2 komplexné korene $-2 \pm 2\sqrt{3}i$. Prevediem na gonimetrický tvar $4(-\frac{1}{2} \pm \frac{\sqrt{3}}{2}i)$, čo zodpovedá veľkosti 4 a uhlom $\frac{2}{3}\pi$, $\frac{4}{3}\pi$. Číslo v goniometrickom tvare viem odmocniť (pozri príslušnú kapitolu v poznámkach z minulého semestra), vyjdú pekné uhly – po prevedení späť na algebraický tvar dostanem tie isté korene, ktoré mi vyšli hore.

V prípade druhého zadania to vyjde „škaredšie“: $x^4 + 4x^2 + 8 = (x^2 + 2\sqrt{2})^2 - 4(\sqrt{2} - 1)x^2 = (x^2 + 2\sqrt{2})^2 - (2\sqrt{\sqrt{2} - 1}x)^2 = (x^2 + 2\sqrt{\sqrt{2} - 1}x + 2\sqrt{2})(x^2 - 2\sqrt{\sqrt{2} - 1}x + 2\sqrt{2})$. To bude rozklad nad $\mathbb{R}$, nad $\mathbb{Q}$ bude polynóm ireducibilné (lebo tam máme iracionálny koeficient).

[1] V zadaní som omylom nechal 8 namiesto 16 – zabudol som to opraviť, opravu som povedal až kdesi v polovici písomky, keď som si to všimol. Dolu v návodoch na riešenia píšem o oboch.

[2] Toto už je úloha, v ktorej ste „trénovaní“ – zadané zobrazenie a predpisy operácií, zistiť, či to je homomorfizmus. Dôležité bolo prísť na to, že toto je vhodný kandidát na izomorfizmus. A samozrejme vedieť ako sa počíta v poliach K a L – t.j. že násobenie tam funguje tak, ako je to napísané v nasledujúcich rovniciach.

Postupom cez bikvadratickú rovnicu (cez substitúciu) sa dostaneme ku koreňom $\pm\sqrt[4]{8}\left(\cos\frac{\pi}{8} \pm i\sin\frac{\pi}{8}\right)$. Z toho vieme nájsť dvojice komplexne združených koreňov a rozklad v tvare

$$(x^2 - 2\sqrt[4]{8}\cos\frac{\pi}{8} + \sqrt{8})(x^2 + 2\sqrt[4]{8}\cos\frac{\pi}{8} + \sqrt{8}).$$

Koeficient $\sqrt{8}$ je iracionálny, takže to nie je rozklad nad $\mathbb{Q}$. Ak by niekomu vadilo, že nemáme nijako vyjadrený $\cos\frac{\pi}{8}$, môže si spomenúť na vzorec zo strednej školy

$$\left|\cos\frac{\alpha}{2}\right| = \sqrt{\frac{1+\cos\alpha}{2}},$$

dosadiť a skúsiť dorátať – mal by výjsť presne ten istý rozklad ako prvým postupom.

B

1. Dokážte, že každá jednoduchá podgrupa grupy S_n, ktorá má viac ako 2 prvky, je obsiahnutá v podgrupe A_n. (Grupa sa nazýva jednoduchá, ak nemá žiadne normálne podgrupy okrem seba samej a triviálnej podgrupy. S_n=grupa permutácií $\{1, 2, \dots, n\}$ s operáciou skladania, A_n=párne permutácie).

2. Dokážte, že pole komplexných čísel $(\mathbb{C}, +, \cdot)$ je izomorfné s okruhom všetkých matíc tvaru $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $a, b \in \mathbb{R}$ s operáciami obvyklého sčitovanie a násobenia matíc.

3. Rozložte nad $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ polynóm $x^4 + 4x^3 + 2x^2 - 4x - 2$. (Hint: Možno by mohla pomôcť vhodná substitúcia alebo Taylorov rozvoj v bode -1.)

4. Nájdite minimálny polynóm prvku $u = \sqrt{2} + 1$ nad $\mathbb{Q}$.

B

1. Ak H je podgrupa S_n, tak $H \cap A_n$ je podgrupa grupy H. Predpokladajme, že by H bola jednoduchá podgrupa s aspoň 3 prvkami a neplatilo by $H \subseteq A_n$. Potom $K := H \cap A_n$ je vlastná podgrupa H. Všimnime si, že je to podgrupa indexu 2, t.j. $[H : K] = 2$. Skutočne, máme iba 2 triedy rozkladu – párne permutácie ležia v triede K, ak φ, ψ sú 2 nepárne permutácie z K, tak $\varphi^{-1}\psi$ je párna permutácia, teda ľubovoľné 2 nepárne permutácie ležia v rovnakej triede rozkladu (čo znamená, že nepárne permutácie vytvoria druhú triedu rozkladu). Z toho, že je to podgrupa indexu 2 vyplýva, že je normálna. (Mali sme na cvičeniach, použili sme fakt, že ľavý a pravý rozklad je taký istý.) Ak H je jednoduchá a K je jej vlastná normálna podgrupa, tak K je jednoprvková. Ale keďže $[H : K] = 2$, znamenalo by to

3. Stačilo si všimnúť, že $x^4 + 4x^3 + 2x^2 - 4x - 2 = (x + 1)^4 - 4(x + 1)^2 + 1$ a potom (po substitúcii $t = x + 1$) už len rozložiť $t^4 - 4t^2 + 1$. (To je veľmi podobný príklad ako v skupine A, dostaneme $(t^2 + \sqrt{2}t - 1)(t^2 - \sqrt{2}t - 1) = (x^2 + (2 + \sqrt{2})x + \sqrt{2})(x^2 + (2 - \sqrt{2})x - \sqrt{2})$.)

4. Stačí si všimnúť, že $u(u - 2) = (\sqrt{2} + 1)(\sqrt{2} - 1) = 0$, teda u je koreň polynómu $x^2 - 2x - 1$. Vieme, že minimálny polynóm je aspoň stupňa 2 (keďže $\sqrt{2} \notin \mathbb{Q}$), preto je to skutočne tento polynóm. (Bez „hádania“ sa to dá vyjadrením $1, x, x^2$ v báze $1, \sqrt{2}$ a hľadaním lineárnej závislosti – pozri riešený príklad v poznámkach k prednáške.)
