4. Reprezentace grup

Uvědomme si, že množina regulárních čtvercových matic stupně n nad tělesem T je uzavřená na násobení, inverzní matice a obsahuje jednotkovou matici. Tuto množinu budeme v následujícím značit $\mathrm{GL}(n,T)$. Protože je násobení matic asociativní, tvoří $(\mathrm{GL}(n,T),\cdot,^{-1},\mathbf{E})$ grupu.

4.1. Nechť V je vektorový prostor dimenze n nad tělesem T a označme $\mathrm{Aut}(V)$ množinu všech automorfismů V (tj. bijektivních homomorfismů). Dokažte, že je $\mathrm{Aut}(V)$ podgrupou symetrické grupy $S(V)$ a dále ověřte, že jsou izomorfní grupy $(\mathrm{Aut}(V),\circ,^{-1},\mathrm{Id})$ a $(\mathrm{GL}(n,T),\cdot,^{-1},\mathbf{E})$.

V prvním případě si potřebujeme rozmyslet, že je složení automorfismů vektorové prostoru opět automorfismus a že inverzní zobrazení automorfismu je automorfismu, což bylo dokázáno na přednášce lineární algebry. Navíc Id je automorfismem zřejmě, proto $\mathrm{Aut}(V)\leq S(V)$.

Zvolme nyní nějakou bázi B vektorového prostoru V, označme $[f]_B$ matici endomorfismu $f\in\mathrm{Aut}(V)$ vzhledem k bázi B a definujme zobrazení $\psi:\mathrm{Aut}(V)\to\mathrm{GL}(n,T)$ předpisem $\psi(f)=[f]_B$. Tvrzení z linární algebry říkají, že zobrazení je dobře definované (tj. matice automorfismu je regulární) a že $\psi(f\circ g)=[f\circ g]_B=[f]_B\cdot[g]_B=\psi(f)\cdot\psi(g)$, tedy se jedná o grupový homomorfismus. Konečně protože každá regulární matice nám (v souřadnicích vzhledem k B) určuje izomorfismus a jediný automorfismus, jehož matice je jednotková, je identita, vidíme, že je ψ bijekce. $\square$

4.2. Dokažte, že množina všech matic z $\mathrm{GL}(n,T)$ s determinantem rovným 1 je normální podgrupou $(\mathrm{GL}(n,T),\cdot,^{-1},\mathbf{E})$.

Stačí si uvědomit, že determinant je homomorfismus grup $(\mathrm{GL}(n,T),\cdot,^{-1},E)$ a $(T\setminus\{0\},\cdot,^{-1},1)$, protože $\det(\mathbf{A}\cdot\mathbf{B})=\det(\mathbf{A})\cdot\det(\mathbf{B})$, a že $\{\mathbf{A}\in\mathrm{GL}(n,T)\mid\det(\mathbf{A})=1\}=\ker(\det)$. V Lemmatu 1.38 bylo dokázáno, že je každé jádro homomorfismu normální podgrupou, proto je i množina všech matic s determinantem rovným 1 normální podgrupou $(\mathrm{GL}(n,T),\cdot,^{-1},E)$. $\square$

Označme písmenem N nejmenší normální podgrupu grupy $(\mathrm{GL}(2,\mathbf{C}),\cdot,^{-1},E)$ obsahující matici $\mathbf{A}=\begin{pmatrix}3&1\\2&4\end{pmatrix}$.

4.3. Dokažte, že N obsahuje pro každé $x\in\mathbf{C}$ matice $\begin{pmatrix}2&x\\0&5\end{pmatrix}$, $\begin{pmatrix}2&0\\x&5\end{pmatrix}$, $\begin{pmatrix}5&x\\0&2\end{pmatrix}$ a $\begin{pmatrix}5&0\\x&2\end{pmatrix}$.

Nejdříve určíme vlastní čísla matice $\mathbf{A}$, jimiž jsou 2 a 5. Připomeňme, že podle Jordanovy věty (dokázané na přednášce lineární algebry) je matice A podobná Jordanově matici $\mathbf{B}=\begin{pmatrix}2&0\\0&5\end{pmatrix}$, která je určena jednoznačně až na pořadí Jordanových buněk. Tedy existuje taková regulární matice $\mathbf{Q}$, že $\mathbf{B}=\mathbf{Q}\cdot\mathbf{A}\cdot\mathbf{Q}^{-1}$. Podgrupa N je ovšem normální, tedy je uzavřena na všechny konjugace (tj. v řeči lineární algebry podobnosti), proto obsahuje matici **B** i všechny matice podobné **B**. Všimneme-li si, že všechny matice $\begin{pmatrix}2 & x\\ 0 & 5\end{pmatrix}$, $\begin{pmatrix}2 & 0\\ x & 5\end{pmatrix}$, $\begin{pmatrix}5 & x\\ 0 & 2\end{pmatrix}$ a $\begin{pmatrix}5 & 0\\ x & 2\end{pmatrix}$ jsou podobné matici **B**, leží všechny rovněž v N. □

4.4. Dokažte, že N obsahuje pro každé $x \in \mathbf{C}$ matice $\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}$ a $\begin{pmatrix}1 & 0\\ x & 1\end{pmatrix}$.

Uvážíme-li, že v podgrupě N leží s každými dvěma maticemi i jejich součin a matice k nim inverzní, leží v N i součin

$$\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix} = \begin{pmatrix}2 & 5x\\ 0 & 5\end{pmatrix}\begin{pmatrix}2 & 0\\ 0 & 5\end{pmatrix}^{-1}.$$

Že N obsahuje i matice $\begin{pmatrix}1 & 0\\ x & 1\end{pmatrix}$ plyne opět například z Jordanovy věty. □

4.5. Dokažte, že $\begin{pmatrix}c^{-1} & 0\\ x & c\end{pmatrix} \in N$ pro každé $x \in \mathbf{C}$ a $c \in \mathbf{C} \setminus \{0\}$.

Z předchozí úlohy plyne, že N obsahuje pro libovolné $y \in \mathbf{C}$ matici

$$\begin{pmatrix}1 & 1\\ y & y+1\end{pmatrix} = \begin{pmatrix}1 & 0\\ y & 1\end{pmatrix} \cdot \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}.$$

Položíme-li $y = c - 1$ leží v N matice

$$\begin{pmatrix}1 & 1\\ c-1 & c\end{pmatrix}, \qquad \begin{pmatrix}c^{-1} & 0\\ c-1 & 1\end{pmatrix} = \begin{pmatrix}1 & -c^{-1}\\ 0 & 1\end{pmatrix} \cdot \begin{pmatrix}1 & 1\\ c-1 & c\end{pmatrix}.$$

Díky Jordanově větě tedy $\begin{pmatrix}c^{-1} & 0\\ x & c\end{pmatrix} \in N$ pro všechna $x \in \mathbf{C}\setminus\{0\}$ a $c \in \mathbf{C}\setminus\{0, -1, 1\}$ a navíc $\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix} \in N$. Přitom z předchozí úlohy víme, že N pbsahuje matice $\begin{pmatrix}1 & 0\\ x & 1\end{pmatrix}$ pro každé $x \in \mathbf{C}$, tedy zbývá nahlédnout, že

$$\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \cdot \begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix}.$$

□

4.6. Ověřte, že v N leží všechny matice s determinantem rovným jedné.

Opět využijeme Jordanovy věty. Stačí si uvědomit, že matice s determinantem 1 je podobná (tedy konjugovaná) matici $\begin{pmatrix}c^{-1} & 0\\ x & c\end{pmatrix}$ pro vhodné x a nenulové c, o níž už jsme dokázali, že leží v N. □

4.7. Nechť $f : G_1 \to G_2$ je homorfismus grup $(G_1, \cdot, ^{-1}, 1)$ a $(G_2, \cdot, ^{-1}, 1)$ a H je normální podgrupa grupy G_2. Dokažte, že je $f^{-1}(H)$ normální podgrupou grupy G_1.

Postupujeme přímo podle definice. Protože $f(1) = 1 \in H$, je $1 \in f^{-1}(H)$. Zvolme $h_1, h_2 \in f^{-1}(H)$. Potom $f(h_1^{-1}) = f(h_1)^{-1} \in H$ a $f(h_1 \cdot h_2) = f(h_1) \cdot f(h_2) \in H$, a proto $h_1^{-1}, h_1 \cdot h_2 \in f^{-1}(H)$. Konečně, vezmeme-li $h \in f^{-1}(H)$ a $g \in G_1$, pak $f(g \cdot h \cdot g^{-1}) = f(g) \cdot f(h) \cdot f(g)^{-1} \in H$, tedy $g \cdot h \cdot g^{-1} \in f^{-1}(H)$. $\square$

4.8. Dokažte, že $N = \{B \in \mathrm{GL}(2, \mathbf{C}) | \ \exists k \in \mathbf{Z} : \det(B) = 10^k\}$.

Připomeňme, že determinat tvoří homomorfismus grupy $\mathrm{GL}(2, \mathbf{C})$ na multiplikativní grupu $\mathbf{C} \setminus \{0\}$. Vezmeme-li cyklickou podgrupu $\langle 10 \rangle$ komutativní grupy $(\mathbf{C} \setminus \{0\}, \cdot, ^{-1}, 1)$, půjde o normální podgrupu, jejíž úplný vzor $\det^{-1}(\langle 10 \rangle)$ je podle 4.7 normální podgrupa grupy $(\mathrm{GL}(2, \mathbf{C}), \cdot, ^{-1}, \mathbf{E})$. Protože $\mathbf{A} \in \det^{-1}(\langle 10 \rangle)$ a N je nejmenší normální podgrupu obsahující $\mathbf{A}$, platí, že $N \subseteq \det^{-1}(\langle 10 \rangle)$.

Nyní si uvědomme, že pro libovolné $k \in \mathbf{Z}$ je $\det(\mathbf{A}^k) = 10^k$ a že $\mathbf{A}^k \in N$. Protože $\ker(\det) \subseteq N \subseteq \det^{-1}(\langle 10 \rangle)$ a $\ker(\det)$ je normální podgrupa N, vidíme, že všechny rozkladové třídy $\mathbf{A}^k \ker(\det)$ leží v N. Ovšem podle 1. věty o izomorfismu $\det^{-1}(\langle 10 \rangle) = \bigcup_{k \in k \in \mathbf{Z}} \mathbf{A}^k \ker(\det)$, a proto $\det^{-1}(\langle 10 \rangle) = N$. $\square$

30.11./3.12.

4.9. Existuje pro každou cyklickou grupu její věrná reprezentace stupně 1?

Nejprve si všimněme, že je grupa $(\mathrm{GL}(1, T), \cdot, ^{-1}, \mathbf{E})$ regulárních matic stupně 1 izomorfní grupě nenulových prvků tělesa s násobením $(T \setminus \{0\}, \cdot, ^{-1}, 1)$. Nyní stačí, abychom pro nekonečnou cyklickou grupu $\mathbf{Z}$ uvažovali zobrazení $g(k) = c^k$, kde c je takové nenulové komplexní číslo, že $|c| \neq 1$. Potom g je prostý homomorfismus.

Pro konečnou cyklickou grupu $\mathbf{Z}_n$ označme ξ_n primitivní n-tou odmocninu z jedné, tj $\xi_n = \cos(\frac{2\pi}{n}) + i \sin(\frac{2\pi}{n})$ a definujme zobrazení $g_n(k) = \xi_n^k$. Snadno nahlédneme, že i tentokrát se jedná o prostý grupový homomorfismus. $\square$

4.10. Najděte pro každou cyklickou grupu její věrnou reprezentaci stupně 3 nad tělesem komplexních čísel.

Využijeme-li úvahy předchozí úlohy, stačí pro pro nekonečnou cyklickou grupu $\mathbf{Z}$ vzít zobrazení $g(k) = \begin{pmatrix} c & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^k$ pro nenulové $|c| \neq 1$. Podobně pro konečnou cyklickou grupu $\mathbf{Z}_n$ definujmu zobrazení $g_n(k) = \begin{pmatrix} \xi_n & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^k = \begin{pmatrix} \xi_n^k & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, kde $\xi_n = \cos(\frac{2\pi}{n}) + i \sin(\frac{2\pi}{n})$. Obdobně jako v předchozím příkladě uvážíme, že jde o prosté homomorfismy, tedy o věrné reprezentace. $\square$

4.11. Existuje věrná reprezentace cyklické grupy $(\mathbf{Z}_3, +, -, 0)$ stupně 1 nad tělesem reálných čísel?

Protože $(\mathrm{GL}(1, \mathbf{R}), \cdot, ^{-1}, \mathbf{E}) \cong (\mathbf{R} \setminus \{0\}, \cdot, ^{-1}, 1)$ a protože je obraz prostého homomorfismu podle 1. věty o izomorfismu izomorfní vzoru, můžeme otázku přeformulovat a zeptat se, zda existuje v grupě $(\mathbf{R} \setminus \{0\}, \cdot, ^{-1}, 1)$ prvek řádu 3 (tj. generátor cyklické grupy izomorfní $(\mathbf{Z}_3, +, -, 0)$). Protože rovnici $x^3 = 1$ řeší nad $\mathbf{R}$ pouze hodnota 1, jejíž řád je 1, žádný prvek řádu 3 v $(\mathbf{R} \setminus \{0\}, \cdot, ^{-1}, 1)$ neleží, a proto věrná reprezentace cyklické grupy $(\mathbf{Z}_3, +, -, 0)$ stupně 1 nad $\mathbf{R}$ neexistuje. $\square$

4.12. Najděte nějakou věrnou reprezentaci grupy symetrií čtvrece D_8 stupně 4 nad libovolným tělesem.

Předně poznamenejme, že nalezení množiny všech symetrií čtverce je geometricky velmi názorné a nevyžaduje další formální důkaz. Tato množina obsahuje identitu, otočení o $\frac{\pi}{2}$, π a $\frac{3\pi}{2}$, osové symetrie podle dvou diagonál a dvě osové symetrie podle spojnice středů dvou protilehlých stran. Tedy $|D_8| = 8$.

Protože jde vlastně o permutaci vrcholů s jistými dodatečnými podmínkami (nesmíme „zkroutit” ani „přelámat” strany), můžeme tuto grupu chápat jako podgrupu grupy všech permutací čtyř vrcholů, které si například po směru hodinových ručiček označíme čísly 1, 2, 3, 4. Přesněji řečeno definujeme takový prostý homomorfismus naší grupy do S_4, že každé symetrii přiřadíme právě tu permutaci, jakou provede daná symetrie na vrcholech. Grupa D_8 je tedy izomorfní například s podgrupou $\{\mathrm{Id}, (1234), (13)(24), (1432),\ (14)(23), (12)(34), (13), (24)\}$ grupy S_4.

Nyní stačí využít prostého homomorfismu $\phi : D_8 \to S_4$ a poté pobdobně jako při konstrukci regulární reprezentce (Věta 1.77) vzít prostý homomorfismus ψ grupy S_4 do grupy permutačních matic. Hledanou věrnou reprezentací je potom složení $\psi\phi$. $\square$

5. Okruhy

5.1. Nechť $(A, +, -, 0)$ je komutativní grupa. Definujme $\mathrm{End}(A)$ jako množinu všech homomorfismů komutativní grupy A do sebe, a na ní zaveďmě operace $+$ a $-$ předpisem $[f+g](a) = f(a)+g(a)$, $[-f](a) = -f(a)$ pro každé $a \in A$. Označíme-li 0 nulový endomorfismus na $(A, +, -, 0)$, dokažte, že $(\mathrm{End}(A), +, -, 0, \circ, \mathrm{Id})$ je okruh.

Zvolíme $f, g, h \in \mathrm{End}(A)$ a $a \in A$ a postupujme podle definice. $[(f+g)+h](a) = [f+g](a) + h(h) = (f(a)+g(a)) + h(a) = f(a) + (g(a)+h(a) = [f+(g+h)](a))$ a $[f+g](a) = f(a)+g(a) = g(a)+f(a) = [g+f](a)$ díky asociativitě a komutativitě operace $+$ na A. Dále $[f+0](a) = f(a)+0 = f(a)$ a $[-f+f](a) = -f(a) + f(a) = 0$. Tím jsme ověřili, že $(\mathrm{End}(A), +, -, 0)$ je komutativní grupa. Protože je $\mathrm{End}(A)$ podmonoidem transformačního monoidu $(T(A), \circ, \mathrm{Id})$, je $(\mathrm{End}(A), \circ, \mathrm{Id})$ opět monoid. Konečně $[(f+g)\circ h](a) = [f+g](h(a)) = fh(a) + gh(a) = [f \circ h + g \circ h](a))$ a $[f \circ (g+h)](a) = f(g(a)+h(a)) = fg(a) + fh(a) = [f \circ g + f \circ h](a))$, čímž jsme dokončili důkaz. $\square$

5.2. Buď V vektorový prostor nad tělesem T. Definujme na množině všech endiomorfismů $\mathrm{End}(A)$ operace $+$ a $-$ stejně jako v předchozí úloze každé $\mathbf{v} \in V$. Dokažte, že $(\mathrm{End}(V), +, -, 0, \circ, \mathrm{Id})$ je okruh.

Protože je $(V, +, -, \mathbf{0})$ komutativní grupa, je okruh $(\mathrm{End}(V), +, -, 0, \circ, \mathrm{Id})$ podokruhem okruhu endomorfismů komutativní grupy $(V, +, -, \mathbf{0})$, tedy jde opět o okruh. $\square$

7.12./10.12.

5.3. Nechť je V vektorový prostor dimenze n nad tělesem T. Ověřte, že jsou okruhy $(\mathrm{End}(V), +, -, 0, \circ, \mathrm{Id})$ a $(M_n(T), +, -, 0, \cdot, \mathbf{E})$ izomorfní.

Zvolme nějakou bázi $B = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ prostoru V a definujme zobrazení $\phi : \mathrm{End}(V) \to M_n(T)$ tak, že $\phi(f) = [f]_B$ je matice endomorfismu f vzhledem k bázi B. Ze základních tvrzení pro matice homomorfismů z přednášky lineární algebry plyne, že je zobrazení ϕ bijekce a že $\phi(f \circ g) = [f]_B \cdot [g]_B$ pro všechna $f, g \in \mathrm{End}(V)$. Dále okamžitě vidíme, že $\phi(\mathrm{Id}) = \mathbf{E}$ a snadno spočítáme, že

$$\begin{aligned}\phi(f+g) = [f+g]_B = (\{(f+g)(\mathbf{b}_1)\}_B^T, \dots, \{(f+g)(\mathbf{b}_n)\}_B^T) = \\ = (\{f(\mathbf{b}_1) + g(\mathbf{b}_1)\}_B^T, \dots, \{f(\mathbf{b}_n) + g(\mathbf{b}_n)\}_B^T) = \\ = (\{f(\mathbf{b}_1)\}_B^T + \{g(\mathbf{b}_1)\}_B^T, \dots, \{f(\mathbf{b}_n)\}_B^T + \{g(\mathbf{b}_n)\}_B^T) = \\ = [f]_B + [g]_B = \phi(f) + \phi(g).\end{aligned}$$

Tím jsme ověřili, že ϕ je hledaným okruhovým izomorfismem. □

5.4. Nechť je I podmnožina množiny celých čísel. Dokažte, že je I ideálem okruhu $(\mathbf{Z}, +, -, 0, \cdot, 1)$ (respektive $(\mathbf{Z}_n, +, -, 0, \cdot, 1)$), právě když je I je podgrupa grupy $(\mathbf{Z}, +, -, 0)$ (respektive $(\mathbf{Z}_n, +, -, 0)$).

Přímá implikace plyne přímo z definice ideálu. Vezmeme-li I podgrupu grupy $(\mathbf{Z}, +, -, 0)$, pak víme, že je tvaru $I = \langle n \rangle = n\mathbf{Z}$ pro vhodné n, tedy jde o (hlavní) ideál. Pro $\mathbf{Z}_n$ je argument totožný. □

5.5. Rozhodněte, kolik obsahuje okruh $(\mathbf{Z}_{50}, +, -, 0, \cdot, 1)$ (s počítáním modulo 50) ideálů. Jak tyto ideály vypadají?

V předchozím příkladě jsme si uvědomili, že každá podgrupa (cyklické) grupy $(\mathbf{Z}_{50}, +, -, 0)$ je ideálem okruhu $(\mathbf{Z}_{50}, +, -, 0, \cdot, 1)$, proto zbývá spočítat všechny podgrupy cyklické grupy řádu 50. Aplikujeme-li pozorování 3.13, vidíme, že máme spočítat přirozené dělitele čísla 50. Protože existuje celkem 6 dělitelů čísla 50, obsahuje okruh $(\mathbf{Z}_{50}, +, -, 0, \cdot, 1)$ právě 6 ideálů.

Všechny ideály seřadíme podle počtu prvků do seznamu: $0\mathbf{Z}_{50} = \{0\}$, $25\mathbf{Z}_{50}$, $10\mathbf{Z}_{50}$, $5\mathbf{Z}_{50}$, $2\mathbf{Z}_{50}$, $1\mathbf{Z}_{50} = \mathbf{Z}_{50}$. □

5.6. Buď $n > 1$. Rozhodněte, kolik podokruhů obsahují okruhy $(\mathbf{Z}, +, -, 0, \cdot, 1)$ a $(\mathbf{Z}_n, +, -, 0, \cdot, 1)$.

Protože podokruh musí obsahovat prvek 1 a zároveň musí být pogrupou aditivní grupy okruhu, obsahuje $(\mathbf{Z}, +, -, 0, \cdot, 1)$ a $(\mathbf{Z}_n, +, -, 0, \cdot, 1)$ pouze jediný podokruh (tedy celé $\mathbf{Z}$, resp. $\mathbf{Z}_n$). □

5.7. Uvažujme okruh reálných polynomů $(\mathbf{R}[x], +, -, 0, \cdot, 1)$ a množinu $C \subset \mathbf{R}$. Dokažte, že je množina $I_C = \{p \in \mathbf{R}[x] |\ p(C) = 0\}$ ideál okruhu $(\mathbf{R}[x], +, -, 0, \cdot, 1)$.

Vezměme libovolně $f, g \in I_C$ a $p \in \mathbf{R}[x]$. Potom pro každé $c \in C$ máme $(f + g)(c) = f(c) + g(c) = 0$, $(-f)(c) = 0$ a $(f \cdot p)(c) = f(c) \cdot p(c) = 0 \cdot p(c) = 0$. Protože zřejmě $0 \in I_C$, dokázali jsme, že je I_C ideál. □

5.8. Nechť T je komutativní těleso a X nějaká neprázdná množina. Dokažte, že $(T^X, +, -, \mathbf{0}, \cdot, \mathbf{1})$ je komutativní okruh, jsou-li operace $+$, $-$ a $\cdot$ definovány po složkách a $\mathbf{0}(x) = 0$ a $\mathbf{1}(x) = 1$ pro všechna $x \in X$.

Ověření faktu, že je $(T^X, +, -, \mathbf{0})$ komutativní grupa se provádí v lineární algebře, když se mluví o stejně konstruovaném vektorovém prostoru nad tělesem T. Zbývá ověřit distributivitu a to, že $(T^X, \cdot, \mathbf{1})$ je monoid. Nechť f, g, $h \in T^X$, pak díky asociativitě násobení v tělese máme, že $(f \cdot (g \cdot h))(x) = f(x) \cdot g(x) \cdot h(x) = ((f \cdot g) \cdot h)(x)$. Dále $(f \cdot 1)(x) = f(x) \cdot 1(x) = f(x) \cdot 1 = f(x)$ pro každé $x \in T$. Komutativita $\cdot$ a distributivita, které jsou opět důsledkem komutativity násobení a distributivity v tělese, se ověří obdobně. $\square$

5.9. Buď $C = \{c_1, \dots, c_n\} \subset \mathbf{R}$, kde $n = |C| \in \mathbf{N}$. Definujme zobrazení $\psi : \mathbf{R}[x] \to \mathbf{R}^n$ předpisem $\psi(f) = (f(c_1), \dots, f(c_n))$. Ověřte, že je ψ homomorfismus okruhu $(\mathbf{R}[x], +, -, 0, \cdot, 1)$ na okruh $(\mathbf{R}^n, +, -, \mathbf{0}, \cdot, \mathbf{1})$. Jak vypadá jádro $\ker \psi$?

Ověření podmínek homomorfismu je zcela přímočaré, a že jde o zobrazení na dokazuje interpolační argument. Konečně okamžitě z definice vidíme, že $\ker \psi$ je právě rovno ideálu I_C z úlohy 5.7. $\square$

14.12./17.12.

5.10. Nechť T je těleso a $n \in \mathbf{N}$. Dokažte, že je okruh $(M_n(T), +, -, 0, \cdot, \mathbf{E})$ jednoduchý, tj. že obsahuje pouze triviální ideály.

Nechť I je nenulový ideál, tedy I obsahuje nějakou nenulovou čtvercovou matici $\mathbf{A}$. Označme $\mathbf{D}_{ij}$ čtvercovou matici, která má všude nuly, kromě pozice na i-tém řádku a j-tém sloupci. Nechť má matice $\mathbf{A}$ v i-tém řádku a j-tém sloupci nenulovou hodnotu $a \in T$. Potom $a^{-1}\mathbf{D}_{ki} \cdot \mathbf{A} \cdot \mathbf{D}_{jk} = \mathbf{D}_{kk} \in I$, neboť I je oboustranný ideál, tj. je uzavřený na násobení z leva i z prava libovolným prvkem okruhu. Zároveň i součet $\mathbf{D}_{11} + \mathbf{D}_{22} + ... + \mathbf{D}_{nn} = \mathbf{E}$ leží v I. Tedy I obsahuje jednotkovou matici $\mathbf{E}$, proto $I = \mathbf{E}M_n(T)$. Ověřili jsme, že Maticový okruh obsahuje pouze dva oboustranné ideály $\{\mathbf{0}\}$ a $M_n(T)$. $\square$

5.11. Najděte nejmenší ideál a nejmenší pravý ideál okruhu $(M_3(\mathbf{Q}), +, -, 0, \cdot, \mathbf{E})$ obsahující matici $\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Podle tvrzení předchozí úlohy je nejmenší ideál obsahující nenulovou matici roven celému $M_3(\mathbf{Q})$.

Nejmenší pravý ideál obsahující matici $\mathbf{A}$ je právě hlavní pravý ideál $\mathbf{A}M_3(\mathbf{Q})$, můžeme ho popsat také jako množiny všech matic $M_3(\mathbf{Q})$ jejichž sloupce jsou lineární kombinací sloupců matice $\mathbf{A}$, tedy

$$\mathbf{A}M_3(\mathbf{Q}) = \{\mathbf{C} = (\mathbf{c}_1^T, \mathbf{c}_2^T, \mathbf{c}_3^T) \in M_3(\mathbf{Q}) |\ \mathbf{c}_i \in \langle (1,2,0), (0,0,1) \rangle \}.$$

$\square$

5.12. Určete kolik prvků obsahuje nejmenší ideál a nejmenší levý ideál okruhu $(M_2(\mathbf{Z}_3), +, -, 0, \cdot, \mathbf{E})$ obsahující matici $\mathbf{B} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$.

Tak jako v předchozím případě uvážíme, že nejmenší ideál I obsahující matici $\mathbf{B}$ je roven celému okruhu $M_2(\mathbf{Z}_3)$, snadno tehdy nahlédneme, že $|I| = |M_2(\mathbf{Z}_3)| = 3^4 = 81$.

Podobně užijeme argument předchozí úlohy, abychm viděli, že nejmenší levý ideál J obsahující matici $\mathbf{B}$ obsahuje právě matice, jejichž řádky jsou lineární kombinací řádkových vektorů matice $\mathbf{B}$, tedy násobky vektoru $(1, 2)$. To znamená, že

$$J = \mathbf{M}_2(\mathbf{Z}_3)B = \{\mathbf{C} = \begin{pmatrix} \mathbf{c}_1 \\ \mathbf{c}_2 \end{pmatrix} \in \mathbf{M}_2(\mathbf{Z}_3)|\ \mathbf{c}_i \in \langle(1, 2)\rangle\}.$$

Zbývá tedy spočítat, že existuje 3^2 dvojic vektorů z podprostoru $\langle(1, 2)\rangle$, proto $|J| = 3^2 = 9$. □

5.13. Nechť n je přirozené číslo, p prvočíslo a $\mathbf{D}$ matice hodnosti k maticového okruhu $(M_n(\mathbf{Z}_p), +, -, 0, \cdot, \mathbf{E})$. Porovnejte počet prvků pravého a levého ideálu generovaných maticí $\mathbf{D}$.

Úvaha je stejná jako v předchozích dvou příkladech: levý (pravý) ideál je tvořen právě maticemi jejichž řádky (sloupce) jsou lineární kombinací řádkových (sloupcových) vektorů matice $\mathbf{D}$. Dimenze příslušných vektorových prostorů je ovšem v obou případech rovna hodnosti matice, tedy k. Vektorový prostor, z nějž řádky (sloupce vybíráme) bude mít p^k prvků a z n takových vektorů umíme sestavit právě $(p^k)^n$ matic. Zjistili jsme, že $|\mathbf{D}M_n(\mathbf{Z}_p)| = p^{kn} = |M_n(\mathbf{Z}_p)\mathbf{D}|$. □

5.14. Buď X množina. Označme $\mathcal{P}(X)$ její potenční množinu, tj. množinu včech podmnožin X, a $\triangle$ buď symetrická dieference (t.j. $A \triangle B = A \cup B \setminus A \cap B$). Ověřte, že $(\mathcal{P}(X), \triangle, \mathrm{Id}_{P(X)}, \emptyset, \cap, X)$ tvoří komutativní okruh.

Okamžitě vidíme, že jsou operace $\triangle$ a $\cap$ komutativní, navíc $\cap$ je asociativní a pro každé $Y \in \mathcal{P}(X)$ máme $Y \triangle \emptyset = Y$, $Y \triangle Y = \emptyset$ a $Y^{\cap} X = Y$. Zbývá tedy ověřit asociativitu operace $\triangle$ a distributivitu. Vezměme $A, B, C \in \mathcal{P}(X)$ Nejprve uvažme, že $x \in A \triangle (B \triangle C)$, právě když $x \in A \setminus (B \cup C)$ nebo $x \in B \setminus (A \cup C)$ nebo $x \in C \setminus (B \cup C)$ nebo $x \in A \cap B \cap C$, což zjevně nezávisí na uzávorkování, proto $A \triangle (B \triangle C) = (A \triangle B) \triangle C)$. Podobně uvážíme, že $x \in A \cap (B \triangle C)$, právě když $x \in A$ a $x \in B \triangle C$, což nastává právě tehdy, když $x \in (A \cap B) \triangle (A \cap C)$. □

5.15. Uvažujme okruh $(\mathcal{P}(X), \triangle, \mathrm{Id}_{\mathcal{P}(X)}, \emptyset, \cap, X)$ a I jeho ideál. Dokažte, že

(a) I je hlavní, právě když $I = \mathcal{P}(A)$ pro nějaké $A \subseteq X$,
(b) I je uzavřeno na konečná sjednocení svých prvků,
(c) I je hlavní ideál, je-li X konečná,
(d) je-li X nekonečná množina, existuje ideál, který není hlavní.

(a) Nejprve si uvědomíme, že je $\mathcal{P}(A) = A\mathcal{P}(X) = \{A \cap Y|\ A \subseteq X\}$, tedy, že jde o hlavní ideál. Zvolíme-li $B \in \{A \cap Y|\ A \subseteq X\}$, potom $B \in \mathcal{P}(A)$ a vezmeme-li $B \in \mathcal{P}(A)$, potom $B = A \cap B \in A\mathcal{P}(X)$. Tedy skutečně $A\mathcal{P}(X) = \mathcal{P}(A)$ a máme dokázáno, že $\mathcal{P}(A)$ je hlavní ideál. Je-li naopak ideál I hlavní, existuje množina $A \subseteq X$, pro kterou $I = A\mathcal{P}(X) = \{A \cap Y|\ A \subseteq X\}$, tudíž $I = \mathcal{P}(A)$.

(b) Díky indukčnímu argumentu nám stačí ověřit, že $A \cup B \in I$ pro každé $A, B \in I$. Ovšem $A \cup B = (A^{\triangle} B)^{\triangle}(A \cap B) \in I$, protože $A^{\triangle} B, A \cap B \in I$.

(c) Je-li X konečná, pak i množiny $\mathcal{P}(X)$ a I jsou konečné, proto $A = \bigcup I \in I$ podle (b). Zřejmě pro každé $B \in I$ je $B \in \mathcal{P}(A)$ a naopak $\mathcal{P}(A) \subseteq I$ podle (a), tedy $\mathcal{P}(A) = I$

(d) Vezměme jako J množinu všech konečných podmnožin X. Snadno nahlédneme, že je J nekonečný ideál, ovšem $\mathcal{P}(F)$ je pro každé $F \in J$ konečný ideál, tedy díky (a) J není hlavní. □

5.16. Buď $A = \{1, 2, 4, 7\}$ a $B = \{2, 3, 4, 9\}$ dvě podmnožiny množiny $X = \{1, 2, \dots, 9\}$. Najděte generátor hlavního ideálu J generovaného množinou $\{A, B\}$ okruhu $(\mathcal{P}(X), ^{\triangle}, \mathrm{Id}_{\mathcal{P}(X)}, \emptyset, \cap, X)$ a generátor průniku hlavních ideálů generovaných prvky A a B. Kolik tyto ideály mají prvků?

V důsledku úvah z předchozího příkladu je ideál I generován právě sjednocením $A \cup B = \{1, 2, 3, 4, 7, 9\}$, tedy $I = \mathcal{P}(\{1, 2, 3, 4, 7, 9\})$. Konečně $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B) = \mathcal{P}(\{2, 4\})$.

Ideál J má zřejmě právě $2^6 = 64$ prvků a průnik ideálů $\mathcal{P}(A)$ a $\mathcal{P}(B)$, tedy ideál $\mathcal{P}(\{2, 4\})$ má právě $2^2 = 4$ prvky. □

Další úlohy

(1) Popište nejmenší normální podgrupu grupy $(\mathrm{GL}(2, \mathbf{C}), \cdot, ^{-1}, E)$ obsahující matici a) $\mathbf{G} = \begin{pmatrix} 2 & 3 \\ -3 & -4 \end{pmatrix}$, b) $\mathbf{G}^3$, c) $\mathbf{F} = \begin{pmatrix} 3 & 3 \\ 0 & 2 \end{pmatrix}$, d) $\mathbf{F}^3$,

(2) Popište nejmenší normální podgrupu grupy $(\mathrm{GL}(3, \mathbf{C}), \cdot, ^{-1}, E)$ obsahující matici a) $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, b) $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, c) $-\mathbf{E}$, d) $\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$,

(3) Rozhodněte, zda pro každé přirozené n nad každým tělesem existuje věrná reprezentace stupně n symetrické grupy $(S_n, \circ, ^{-1}, \mathrm{Id})$.

(4) Rozhodněte, zda pro každé přirozené n nad každým tělesem existuje věrná reprezentace stupně n alternující grupy $(A_n, \circ, ^{-1}, \mathrm{Id})$.

(5) Nechť existuje věrná reprezentace grupy $(G, \cdot, ^{-1}, 1)$ nad tělesem T stupně n. Dokažte pro každé $m > n$, že existuje věrná reprezentace grupy $(G, \cdot, ^{-1}, 1)$ nad T stupně m.

(6) Existuje věrná reprezentace cyklické grupy $(\mathbf{Z}_4, +, -, 0)$ stupně 1, 2, 3, 4 či 5 nad tělesem reálných čísel?

(7) Nechť $C_\infty(\mathbf{R})$ všechny hladké reálné fukce na $\mathbf{R}$. Dokažte, že je uspořádaná šestice $(C_\infty(\mathbf{R}), +, -, 0, \cdot, 1)$ $\mathbf{R}$-algebra. Rozhodněte, zda je derivace na $C_\infty(\mathbf{R})$ okruhový homomorfismus.

(8) Rozhodněte, pro které množiny C je ideál z 5.7 nulový.

(9) Dokažte, že jsou všechny ideály okruhu $(T^X, +, -, \mathbf{0}, \cdot, \mathbf{1})$ z z 5.8 hlavní právě tehdy, když je X konečná množina.