1-MAT-220 Algebra 1

12. februára 2012

Obsah

Kapitola 1

Grupy

1.1 Binárne operácie

{binop:JEDNNEUTR}

Tvrdenie 1.1.1. *Ak má binárna operácia $*$ na množine M neutrálny prvok, tak tento neutrálny prvok je jediný.*

1.2 Cayleyho veta

Ľahko vieme overiť že pre danú množinu M všetky bijekcie z M do M tvoria s operáciou skladania zobrazení grupu. (Dôkaz je presne rovnaký ako pre permutácie v prípade, že M bola konečná.) Túto grupu budeme označovať $(S(M), \circ)$ alebo stručnejšie $S(M)$.

Definícia 1.2.1. Pod *grupou transformácií množiny M* budeme rozumieť ľubovoľnú podgrupu grupy $(S(M), \circ)$.

Ekvivalentne by sme mohli grupu transformácií definovať tak, že je to množina bijekcií z M do M uzavretá na skladanie a inverzné zobrazenie. (V [KGGS] sa grupa transformácií definuje takto, pretože tento pojem je tu zavedený skôr než pojem grupy. Aj historické poradie, v akom matematici definovali tieto pojmy, je rovnaké.)

Definícia 1.2.2. Nech $(G, *)$ a $a \in G$.
Zobrazenie $f_a \colon G \to G$ dané predpisom $xf_a = a * x$ voláme *ľavá translácia.*
Zobrazenie $g_a \colon G \to G$ dané predpisom $xg_a = x * a$ voláme *pravá translácia.*

Lema 1.2.3. *Každá ľavá (pravá) translácia je bijekcia.*

Dôsledok 1.2.4. *Pre všetky $a \in G$ platí $f_a, g_a \in S(G)$.*

Lema 1.2.5. *Pre ľavé translácie platí*

$$g_b \circ g_a = g_{b*a}$$

Dôsledok 1.2.6. *Zobrazenie $a \mapsto g_a$ je homomorfizmus z G do $S(G)$.*

Dôsledok 1.2.7. *Pravé translácie tvoria podgrupu grupy $S(G)$.*

Dôkaz. DU □

Aby sme dokázali Cayleyho vetu, stačí už len ukázať, že práve uvedený homomorfizmus je v skutočnosti izomorfizmus na svoj obraz, t.j. že je injektívny.

{cayl:VTCAYL}

Veta 1.2.8 (Cayley)**.** *Každá grupa $(G, *)$ je izomorfná s nejakou grupou transformácií. Presnejšie, $(G, *)$ je izomorfná s podgrupou grupy $S(G)$ tvorenou všetkými pravými transláciami.*

Dôkaz. DU □

Dôsledok 1.2.9. *Ľubovoľná konečná grupa rádu n (t.j. taká, ktorá má n prvkov) je izomorfná s podgrupou grupy permutácií S_n.*

Príklad 1.2.10. Ilustrujme si Cayleyho vetu na príklade grupy $(\mathbb{Z}, +)$. (Keďže ide o komutatívnu grupu, v tomto prípade sú ľavé a pravé stranslácie totožné.)

V tomto prípade pre $a \in \mathbb{Z}$ máme zobrazenie $g_a \colon \mathbb{Z} \to \mathbb{Z}$

$$x g_a = x + a,$$

ktoré je očividne bijektívne, čiže $g_a \in S(\mathbb{Z})$. Takisto sa ľahko overí, že $g_{a+b} = g_a \circ g_b$, z čoho vidíme, že $a \mapsto g_a$ je homomorfizmus. Fakt, že tento homomorfizmus je injektívny, môžeme overiť podobne ako v dôkaze Cayleyho vety.

{cayl:PRSROT}

Príklad 1.2.11. Skúsme sa pozrieť na reprezentáciu grupy $(S, \cdot)$, kde $S = \{z \in \mathbb{C}; |z| = 1\}$ pomocou Cayleyho vety.

V tomto prípade máme $x g_z = xz$. Z Moivrovej vety vieme, že vynásobenie komplexných číslom z s jednotkovou veľkosťou presne zodpovedá otočeniu bodu v komplexnej rovine okolo počiatku o uhol φ taký, že $z = \cos\varphi + i \sin\varphi$. Čiže v tomto prípade tvoria grupu transformácií z Cayleyho vety všetky otočenia kružnice okolo nuly.

Kapitola 2

Faktorizácia

2.1 Relácie ekvivalencie a rozklady

Definícia 2.1.1. *Relácia ekvivalencie* je relácia R na množine A, ktorá je reflexívna, symetrická a tranzitívna; t.j. pre všetky $a, b, c \in A$ platí:

$$aRa$$
$$aRb \Rightarrow bRa$$
$$aRb \wedge bRc \Rightarrow aRc$$

Množina $\{b \in A; aRb\}$ sa nazýva *triedou ekvivalencie s reprezentantom* a a označuje sa $[a]_R$, prípadne len $[a]$.

Definícia 2.1.2. *Rozklad množiny* A je taká množina $\mathcal{A} = \{A_i; i \in I\}$ neprázdnych podmnožín množiny A, že platí:

(i) Pre všetky $i, j \in I$ platí buď $A_i = A_j$ alebo $A_i \cap A_j = \emptyset$.

(ii) $\bigcup_{i \in I} A_i = A$.

Pred hlavnými výsledkami týkajúcimi sa rozkladov a ekvivalencií uvedieme si ešte jednu lemu:

{ekv:LMTRIEDY}

Lema 2.1.3. *Nech R je relácia ekvivalencie. Potom*

$$aRb \Leftrightarrow [a]_R = [b]_R.$$

Veta 2.1.4. *Ak R je relácia ekvivalencie na A, tak množina všetkých tried ekvivalencie tvorí rozklad množiny A.*

Veta 2.1.5. *Ak $\mathcal{A} = \{A_i; i \in I\}$ je rozklad množiny A, tak relácia R definovaná tak, že*

$$aRb \qquad \Leftrightarrow \qquad (\exists i \in I) a \in A_i \wedge b \in A_i$$

je relácia ekvivalencie. (*Definícia relácie R vlastne hovorí, že dva prvky sú v relácii R práve vtedy, keď ležia v tej istej množine rozkladu $\mathcal{A}$.*)

Videli sme, že relácii ekvivalencie na množina A môžeme priradiť rozklad množiny A a opačne. Chceli by sme ukázať, že táto korešpondencia medzi reláciami ekvivalencie a rozkladmi je jednojednoznačná; čiže relácie ekvivalencie a rozklady sú vlastne len 2 rôzne pohľady na tú istú vec.

Označme rozklad prislúchajúci relácii ekvivalencie R ako $\mathcal{A}_R$ a reláciu ekvivalencie danú rozkladom $\mathcal{A}$ ako $R_{\mathcal{A}}$. My vlastne chceme ukázať, že tieto 2 priradenia sú navzájom inverzné, čiže $R_{\mathcal{A}_R} = R$ a $\mathcal{A}_{R_{\mathcal{A}}} = \mathcal{A}$.

(Tu je tiež dôležité si uvedomiť, čo znamená že 2 relácie resp. 2 rozklady sú rovnaké. Relácie chápeme ako podmnožiny $A \times A$, 2 relácie sa R a R' sa rovnajú práve vtedy, keď platí $aRb \Leftrightarrow aR'b$ pre všetky $a, b \in A$. Rovnosť pre rozklady takisto chápeme ako rovnosť množín – to znamená, že rovnaké rozklady pozostávajú z tých istých podmnožín.)

Z lemy 2.1.3 vidíme, že ak priradíme relácii ekvivalencie rozklad, tak v rovnakých podmnožinách budú práve tie prvky, ktoré sú v relácii R, a teda skutočne platí $R_{\mathcal{A}_R} = R$. Platnosť rovnosti $\mathcal{A}_{R_{\mathcal{A}}} = \mathcal{A}$ pre ľubovoľný rozklad sa tiež ukáže pomerne jednoducho. DU

Cvičenia

{ekvcvic:ULOEKVZOBR}

Úloha 2.1.1. a) Nech $f\colon A \to B$ je surjektívne zobrazenie. Dokážte, že relácia R na množine A určená predpisom $aRa' \Leftrightarrow f(a) = f(a')$ je relácia ekvivalencie a triedy rozkladu sú množiny $f^{-1}(\{b\}) = f^{-1}(b)$ pre $b \in B$.
b) Nech R je relácia ekvivalencie na množine A a nech B je množina všetkých tried ekvivalencie. Dokážte, že zobrazenie $f\colon A \to B$, ktoré každému prvku priradí jeho triedu ekvivalencie (teda $f\colon a \mapsto [a]$) je surjektívne.
c) V predchádzajúcej časti sme každému surjektívnemu zobrazeniu priradili reláciu ekvivalencie a obrátene. Dokážte, že tieto dve priradenia sú navzájom inverzné.

2.2 Rozklad grupy podľa podgrupy

Definícia 2.2.1. Nech G je grupa a $A, B \subseteq G$ sú jej ľubovoľné podmnožiny. Potom definujeme *súčin AB podmnožín A, B* ako

$$AB = \{ab; a \in A, b \in B\}.$$

V prípade, že jedna z množín je jednoprvková, budeme používať stručnejší zápis aB namiesto $\{a\}B$ a Ab namiesto $A\{b\}$.

Niektoré užitočné vlastnosti násobenia podmnožín zhrnieme v nasledujúcej leme:

{rozkl:LMKOMPL}

Lema 2.2.2. *Nech G je grupa.*

(i) *Násobenie podmnožín je asociatívne, t.j. $A(BC) = (AB)C$ pre ľubovoľné podmnožiny $A, B, C \subseteq G$.*

(ii) *Pre ľubovoľnú podmnožinu $A \subset G$ platí $eA = Ae = A$.*

(iii) *Ak H je podgrupa grupy G a $h \in H$, tak $hH = H$.*

{rozkl:lmitem5}

(iv) *Ak H je podgrupa grupy G, tak $H^2 = H.H = H$.*

(v) *Pre ľubovoľnú podmnožinu $A \subseteq G$ platí $(A^{-1})^{-1} = A$, kde používame označenie $A^{-1} = \{a^{-1}; a \in A\}$.*

{ozkl:lmitem6}

(vi) *Ak H je podgrupa grupy G, tak $H^{-1} = \{h^{-1}; h \in H\} = H$.*

{ozkl:lmitem4}

(vii) *Pre ľubovoľné podmnožiny $A, B \subseteq G$ platí $(AB)^{-1} = B^{-1}.A^{-1}$.*

(viii) *Ak K, H sú podgrupy grupy G, tak $(HK)^{-1} = K^{-1}.H^{-1} = KH$.*

Označenie H^{-1} v predchádzajúcej leme neznamená, že by táto množina bola inverzným prvkom ku H v $\mathcal{P}(G) \setminus \{\emptyset\}$ s operáciou násobenia podmnožín – H^{-1} jednoducho len označuje množinu inverzných prvkov ku prvkom z H.

Definícia 2.2.3. Ak H je podgrupa grupy G, tak označíme pre $a \in G$

$$aH = \{ah; h \in H\},$$
$$Ha = \{ha; h \in H\}.$$

Množiny aH nazývame *ľavé triedy grupy G podľa H* (alebo ľavé triedy grupy G modulo H), množiny Ha sú *pravé triedy grupy G podľa H*.

{rozkl:LMAINVB}

Lema 2.2.4. *Nech H je podgrupa G a $a, b \in G$. Potom $aH = bH$ práve vtedy, keď $b^{-1}a \in H$.*
Podobne platí $Ha = Hb \Leftrightarrow ab^{-1} \in H$.

Tvrdenie 2.2.5. *Ľavé triedy grupy G podľa jej podgrupy H tvoria rozklad G. (Inak: $\{aH; a \in G\}$ je rozklad množiny G.)*
Pravé triedy grupy G podľa jej podgrupy H tvoria rozklad G.

Definícia 2.2.6. Nech G je grupa a H je podgrupa. Rozklad $\{aH; a \in G\}$ sa nazýva *ľavý rozklad G podľa H* a rozklad $\{Ha; a \in G\}$ sa nazýva *pravý rozklad G podľa H*.

Všimnime si, že $eH = He = H$, teda ako jedna z ľavých (pravých) tried sa vždy vyskytne podgrupa H.

Lema 2.2.7. *Nech H je podgrupa grupy G a $a \in G$. Potom zobrazenie $\varphi\colon H \to aH$ definované ako*

$$\varphi\colon h \mapsto ah$$

je bijekcia.
Podobne zobrazenie $\psi\colon H \to Ha$, $\psi\colon h \mapsto ha$ je bijekcia.

Veta 2.2.8. *Nech H je konečná podgrupa G. Potom počet prvkov každej ľavej triedy aH je rovnaký (a rovná sa počtu prvkov podgrupy H). Takisto sa rovná počtu prvkov ľubovoľnej pravej triedy Hb.*

Na základe predchádzajúcej vety, ktorá hovorí, že počet ľavých a pravých tried je rovnaký, má zmysel nasledujúca definícia.

Definícia 2.2.9. Nech H je podgrupa konečnej grupy. Potom $[G\colon H]$ je počet všetkých ľavých (pravých) tried rozkladu G podľa H. Toto číslo nazývame *indexom grupy G podľa H*.

{rozkl:VTLAG}

Veta 2.2.10 (Lagrangeova veta)**.** *Ak G je konečná grupa a H je jej podgrupa, tak platí*

$$|G| = |H|.[G\colon H].$$

Teda počet prvkov podgrupy H delí počet prvkov G.

Nasledujúci výsledok by snáď mohol vysvetlovať, prečo namiesto počtu prvkov konečnej grupy niekedy používame aj termín *rád grupy*.

{rozkl:DOS1}

Dôsledok 2.2.11. *Ak G je konečná grupa, tak rád každého prvku delí rád grupy G (počet prvkov grupy G).*

Dôkaz. Stačí si uvedomiť, že rád prvku a je počet prvkov podgrupy $[a]$. □

{rozkl:DOSPRV}

Dôsledok 2.2.12. *Ak G je p-prvková grupa a p je prvočíslo, tak každý jej prvok okrem neutrálneho prvku je generátorom G (a teda G je cyklická).*

Dôkaz. Rád prvku $a \neq e$ nie je 1 a keďže je deliteľ prvočísla p, musí byť rovný p. Teda $[a]$ obsahuje p rôznych prvkov $e, a^1, a^2, \ldots, a^{p-1}$, čiže $[a] = G$. □

Dôsledok 2.2.13. *Každá 4-prvková grupa je izomorfná buď so $\mathbb{Z}_4$ alebo so $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

Dôkaz. Nech G je 4-prvková grupa. Podľa dôsledku 2.2.11 rády jej prvkov môžu byť jedine 1, 2 alebo 4. Ak G obsahuje prvok rádu 4, tak tento prvok je jej generátor. V tomto prípade dostávame, že G je cyklická a $G \cong \mathbb{Z}_4$.

Druhá možnosť je, že všetky prvky s výnimkou neutrálneho majú rád 2, čiže pre každý prvok platí $a^2 = e$, kde e je neutrálny prvok G. Inak povedané, pre všetky $a \in G$ platí $a = a^{-1}$. Z toho dostávame aj to, že G je komutatívna: $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.

Označme prvky tejto grupy e, a, b, c. Zatiaľ o nich vieme toto:

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

Podľa zákonov o krátení sa každý prvok vyskytne v ľubovoľnom riadku a v ľubovoľnom stĺpci tabuľky grupovej operácie práve raz. Tento fakt nám umožní jednoznačne doplniť prázdne miesta v tabuľke. Všimnime si napríklad, že prvok ab nemôže byť a, e ani b (inak by sme mali v niektorom riadku alebo stĺpci tento prvok dvakrát). Podobnú úvahu môžeme urobiť pre prvok ba. Dostávame:

	e	a	b	c
e	e	a	b	c
a	a	e	c	
b	b	c	e	
c	c			e

Teraz už v každom riadku a stĺpci máme jediné voľné miesto, teda zostávajúci prvok je jednoznačne určený

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Pretože aj $\mathbb{Z}_2 \times \mathbb{Z}_2$ má tú vlastnosť, že všetky prvky okrem neutrálneho majú rád 2, a práve sme ukázali, že touto podmienkou je grupa jednoznačne určená (až na označenie prvkov – čiže až na izomorfizmus), máme $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. □

2.3 Normálne podgrupy

{normal:TVRAHHB}

Tvrdenie 2.3.1. *Nech H je podgrupa grupy G. Ak $aH = Hb$, tak $Ha = Hb$. (Takisto za týchto predpokladov platí $aH = bH$.)*

{normal:VTINV}

Veta 2.3.2. *Nech H je podgrupa G. Nasledujúce podmienky sú ekvivalentné:*

{normal:IT1}

(i) $aH = Ha$ *pre všetky* $a \in G$,

{normal:IT2}

(ii) $aH \subseteq Ha$ *pre všetky* $a \in G$,

{normal:IT3}

(iii) $Ha \subseteq aH$ *pre všetky* $a \in G$,

{normal:DEFINV}

(iv) $aHa^{-1} \subseteq H$ *pre všetky* $a \in G$,

{normal:IT5}

(v) $H \subseteq aHa^{-1}$ *pre všetky* $a \in G$,

{normal:IT4}

(vi) $aHa^{-1} = H$ *pre všetky* $a \in G$,

{normal:AHHB}

(vii) $\{aH; a \in G\} = \{Hb; b \in G\}$.

Všimnime si, že podmienku (v) môžeme zapísať aj tak, že platí $aha^{-1} \in H$ pre všetky $h \in H$ a $a \in G$, čiže

$$h \in H \qquad \Rightarrow \qquad aha^{-1} \in H. \tag{2.1}$$

{normal:EQDEFINV}

Definícia 2.3.3. Podgrupa H grupy G sa nazýva *normálna* (*invariantná*) *podgrupa,* ak spĺňa niektorú z ekvivalentných podmienok uvedených vo vete 2.3.2. Označujeme $H \triangleleft G$.

Ak G je komutatívna grupa, tak každá jej podgrupa je invariantná.

Z vety 2.3.2 vidíme, že pre invariantnú podgrupu ľavé a pravé triedy rozkladu sú totožné.

Príklad 2.3.4. Pre každú grupu G sú jej podgrupy G a $\{e\}$ normálnymi podgrupami.

Pretože v komutatívnej grupe je každá podgrupa normálna, úloha zistiť, či nejaká podgrupa je normálna, je zaujímavá len v nekomutatívnom prípade.

{normal:PRS3}

Príklad 2.3.5. Preskúmajme, ktoré podgrupy S_3 sú normálne. Zostavme najprv tabuľku grupovej operácie. (Do riadku φ a stĺpca τ zapisujeme $\varphi \circ \tau$.)

	id	(12)	(13)	(23)	(123)	(132)
id	id	(12)	(13)	(23)	(123)	(132)
(12)	(12)	id	(132)	(123)	(23)	(13)
(13)	(13)	(123)	id	(132)	(12)	(23)
(23)	(23)	(132)	(123)	id	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	id
(132)	(132)	(23)	(12)	(13)	id	(123)

Teraz skúsme nájsť všetky podgrupy grupy S_3. Z Lagrangeovej vety 2.2.10 vieme, že (okrem podgrúp $\{e\}$ a S_3) stačí hladať podgrupy rádu 2 a 3. Podľa dôsledku 2.2.12 ide o cyklické grupy, teda nám stačí nájsť všetky prvky rádu 2 resp. 3.

Prvky rádu 2 sú práve cykly dĺžky 2. Tie vygenerujú podgrupy $H_1 = \{id, (12)\}$, $H_2 = \{id, (13)\}$ a $H_3 = \{id, (23)\}$.

Napríklad pre podgrupu $H_1 = \{id, (12)\}$ máme $(13)H_1 = \{(13), (123)\}$ a $H_1(13) = \{(13), (132)\}$. Keďže sme dostali pre ten istý prvok inú ľavú a pravú triedu, podgrupa H_1 nespĺňa podmienku (i) z vety 2.3.2, a teda nie je normálna.

Podobným spôsobom môžeme overiť, že ani ostatné 2-prvkové podgrupy nie sú normálne.

Prvky rádu 3 sú trojcykly (123) a (132). Obe generujú tú istú 3-prvkovú podgrupu $A_3 = \{id, (123), (132)\}$ pozostávajúcu z párnych permutácií množiny $\{1, 2, 3\}$. Vidíme, že pravý i ľavý rozklad je rovnaký, jeho triedy sú množina A_3 (párne permutácie) a jej doplnok $S_3 \setminus A_3$ (nepárne permutácie). Teda A_3 spĺňa podmienku (vii) z vety 2.3.2, čiže je normálna. (Na zdôvodnenie toho, že H_4 je normálna sme mohli použiť aj všeobecnejší fakt, že každá podgrupa indexu 2 je normálna – úloha 2.3.1.)

Cvičenia

{normalcvic:INDEX2}

Úloha 2.3.1. Ak H je podgrupa G a $[G : H] = 2$, tak H je normálna podgrupa. Navyše, pre každý prvok $x \in G$ platí $x^2 \in H$.

{permcvic:A4LAGR}

Úloha 2.3.2*. Dokážte, že grupa A_4 párnych permutácií 4-prvkovej množiny nemá žiadnu 6-prvkovú podgrupu.

2.4 Faktorové grupy

Veta 2.4.1. *Ak G je grupa a H je jej invariantná podgrupa, tak na množine všetkých tried G podľa H môžeme definovať operáciu $\cdot$ ako*

$$(aH) \cdot (bH) = (ab)H.$$

Táto operácia je dobre definovaná (nezávisí od výberu reprezentanta triedy) a množina všetkých tried G podľa H s touto operáciou tvorí grupu. Túto grupu označujeme G/H a nazývame faktorová grupa *grupy G podľa H.*

Je dôležité si uvedomiť, že faktorovú grupu môžeme definovať iba pre invariantnú podgrupu.

Dôkaz. Všetky tvrdenia vety vlastne vyplývajú z toho, že takto definované násobenie je to isté ako násobenie podmnožín grupy G. Platí totiž

$$(aH)(bH) = (aH)(Hb) = a(HH)b = aHb = a(Hb) = a(bH) = (ab)H.$$

Z toho vyplýva, že operácia, ktorú sme definovali je dobre definovaná a takisto, že je asociatívna.

Pretože $eH = H$ a $HH = H$, trieda eH je neutrálny prvok.

Inverzný prvok k aH je $a^{-1}H$, pretože $(aH)(a^{-1}H) = (aa^{-1})H = eH = H$. □

2.5 Vety o izomorfizme

V úlohe 2.1.1 sme videli jednojednoznačný vzťah medzi surjektívnymi zobrazeniami a reláciami ekvivalencie. V prípade, že na danej množine máme navyše grupovú štruktúru, surjektívne homomorfizmy budú podobným spôsobom zodpovedať normálnym podgrupám (a navyše, ako uvidíme v cvičeniach za touto časťou, istým špeciálnym reláciam ekvivalencie, ktoré voláme kongruencie).

{izom:VTKANON}

Veta 2.5.1 (Kanonický homomorfizmus)**.** *Ak G je grupa a H je normálna podgrupa G, tak zobrazenie $f\colon G \to G/H$ dané predpisom*

$$f\colon a \mapsto aH$$

je surjektívny homomorfizmus. Tento homomorfizmus voláme kanonický homomorfizmus.

Navyše, jadro kanonického homomorfizmu je práve podgrupa H.

Vidíme teda, že pre každú faktorovú grupu máme surjektívny homomorfizmus. Obrátené tvrdenie dáva nasledujúca veta:

{izom:VTIZOM}

Veta 2.5.2 (Veta o izomorfizme)**.** *Ak $f\colon G \to G'$ je homomorfizmus grúp, tak* $\operatorname{Ker} f$ *je normálna podgrupa grupy G a faktorová grupa $G/\operatorname{Ker} f$ je izomorfná s podgrupou* $\operatorname{Im} f$ *grupy G'.*

Dôsledok 2.5.3. *Ak $f\colon G \to H$ je surjektívny homomorfizmus grúp, tak grupa H je izomorfná s faktorovou grupou $G/\operatorname{Ker} f$.*

Vety 2.5.1 a 2.5.2 nám hovoria, že normálne podgrupy sú práve jadrá homomorfizmov. (Jadro každého homomorfizmu je normálna podgrupa a obrátene, pre každú normálnu podgrupu máme epimorfizmus na faktorovú grupu, ktorého jadrom je práve táto podgrupa.)

Dôkaz nasledujúceho tvrdenia je veľmi podobný tej časti dôkazu vety 2.5.2, v ktorej sme dokazovali, že ide o homomorfizmus.

{izom:LMKERHOM}

Lema 2.5.4. *Nech $f\colon G \to G'$ je grupový homomorfizmus. Nech H je normálna podgrupa G taká, že $H \subseteq \operatorname{Ker} f$. Potom zobrazenie $\varphi\colon G/H \to G'$ dané predpisom*

$$\varphi(aH) = af$$

je dobre definované a je to grupový homomorfizmus.

Navyše, ak f je epimorfizmus, tak aj φ je epimorfizmus.

Ak túto lemu použijeme na kanonický homomorfizmus $\varphi\colon G \to G/K$, dostaneme:

{izom:DOSKERHOM}

Dôsledok 2.5.5. *Ak H, K sú normálne podgrupy grupy G a $H \subseteq K$, tak zobrazenie $f\colon G/H \to G/K$*

$$f\colon aH \mapsto aK$$

je surjektívny homomorfizmus.

Pomocou predchádzajúcej vety môžeme odvodiť výsledok, ktorý pripomína „krátenie“ pre faktorové grupy. Dôležité je uvedomiť si, že ak H, K sú normálne podgrupy G a $H \subseteq K$, tak H je normálna podgrupa K. Navyše K/H je podmnožina G/H tvorená triedami aH pre ktoré $a \in K$.

{izom:VTIZOM2}

Veta 2.5.6 (Tretia veta o izomorfizme)**.** *Ak H, K sú normálne podgrupy G, pričom $H \subseteq K \subseteq G$, tak K/H je normálna podgrupa G/H a platí*

$$G/K \cong (G/H)/(K/H).$$

Ukážeme si ešte jeden výsledok o faktorových grupách.

Veta 2.5.7 (Tretia veta o izomorfizme)**.** *Nech G je grupa, N je normálna podgrupa G a S je podgrupa G. Potom množina SN tvorí podgrupu grupy G, N je normálna podgrupa SN, $S \cap N$ je normálna podgrupa S a platí*

$$S/(S \cap N) \cong SN/N.$$

Videli sme, že normálne podgrupy zodpovedajú homomorfizmom – zobrazeniam, ktoré rešpektujú grupovú operáciu. V úlohách 2.5.1 a 2.5.2 môžeme vidieť, ako súvisia s reláciami, ktoré rešpektujú grupovú operáciu. Takéto relácie nazývame kongruenciami.

{izom:DEFKONG}

Definícia 2.5.8. Nech $(G, *)$ je grupa. Relácia ekvivalencie R na množine G sa nazýva *kongruencia,* ak platí

$$(a_1, b_1) \in R, (a_2, b_2) \in R \quad \Rightarrow \quad (a_1 * b_1, a_2 * b_2) \in R.$$

Cvičenia

{izomcvic:KONG

Úloha 2.5.1. Nech G je grupa.
a) Pre normálnu podgrupu H definujme reláciu R ako $aRb \Leftrightarrow a^{-1}b \in H$. Dokážte, že táto relácia je kongruencia (definícia 2.5.8). Dokážte, že rozklad zodpovedajúci relácii R je práve rozklad G podľa podgrupy H.
b) Dokážte, že ak R je kongruencia na G, tak $[e]_R$ je normálna podgrupa G. Navyše, rozklad určený reláciou ekvivalencie R je práve rozklad G podľa tejto podgrupy.
c) Overte, že priradenia medzi normálnymi podgrupami G a kongruenciami na G z predchádzajúcich častí úlohy sú navzájom inverzné.

{izomcvic:KONGHOM}

Úloha 2.5.2. Nech $(G, *)$ je grupa.
a) Ak $f\colon G \to H$ je homomorfizmus, tak relácia R na množine G daná predpisom $xRy \Leftrightarrow f(x) = f(y)$ je kongruencia (pozri úlohu 2.1.1).
b) Ak R je kongruencia na G, tak na množine G/R tried ekvivalencie predpis $[a] * [b] = [a * b]$ dobre definuje binárnu operáciu a G/R s touto binárnou operáciou tvorí grupu. Navyše, zobrazenie $a \mapsto [a]$ je surjektívny homomorfizmus z G do G/R a jeho jadro je $[e]$.

Úloha 2.5.3*. Dokážte, že v grupe $(\mathbb{Q}, +)$ neexistuje maximálna (vzhľadom na inklúziu) vlastná podgrupa. T.j. neexistuje podgrupa S grupy $(\mathbb{Q}, +)$ také, že ak $S \subseteq T$ a T je podgrupa, tak $T = S$ alebo $T = \mathbb{Q}$. (Inak povedané: Jediné podgrupy obsahujúce S by boli S a $\mathbb{Q}$.)

Kapitola 3

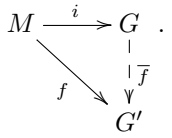
Grupy II

3.1 Akcie grúp

3.2 Vloženie pologrupy do grupy

{polog:TVRPOLOGRUPA}

Tvrdenie 3.2.1. *Ak $(M, *)$ je komutatívna pologrupa s krátením, tak existuje grupa $(G, \circ)$ a injektívny homomorfizmus $i\colon M \to G$ taký, že pre každý homomorfizmus $f\colon M \to G'$ z M do grupy G' existuje práve jeden homomorfizmus $\overline{f}\colon G \to G'$ taký, že $f = \overline{f} \circ i$.*



Inak povedané, každú komutatívnu pologrupu s krátením možno vnoriť do grupy a táto grupa i príslušné vnorenie sú určené jednoznačne až na izomorfizmus.

Literatúra

[KGGS] Tibor Katriňák, Martin Gavalec, Eva Gedeonová, and Jaroslav Smítal. *Algebra a teoretická aritmetika 1.* UK, Bratislava, 2002.

Register

Zoznam symbolov