1 Rozklady podľa podgrupy, invariantné podgrupy

1.1 Relácie ekvivalencie a rozklady

Pripomenutie niektorých pojmov a tvrdení, z ktorých už veľa poznáte.

Definícia 1.1.1. *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 1.1.2. *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: {LMTRIEDY}

Lema 1.1.3. *Nech R je relácia ekvivalencie. Potom*

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

Veta 1.1.4. *Ak R je relácia ekvivalencie na A, tak množina všetkých tried ekvivalencie tvorí rozklad množiny A.*

Veta 1.1.5. *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 2 prvky sú v relácii R práve vtedy, keď ležia v tej istej 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 1.1.3 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 (DÚ – dá sa opäť použiť lema 1.1.3).

1.2 Triedy grupy podľa podgrupy

Najprv si zadefinujeme jeden pomocný pojem – násobenie komplexov.

Definícia 1.2.1. Nech G je grupa a $A, B \subseteq G$ sú jej ľubovoľné podmnožiny. Potom definujeme súčin AB ako

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

Niektoré užitočné vlastnosti násobenia komplexov zhrnieme v nasledujúcej leme: {LMKOMPL}

Lema 1.2.2. *Nech G je grupa.*

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

(ii) *Ak H je podgrupa grupy G, tak $H^2 = H.H = H$.* {lmitem5}

(iii) *Pre ľubovoľnú podmnožinu $A \subseteq G$ platí $(A^{-1})^{-1} = A$.*

(iv) *Ak H je podgrupa grupy G, tak $H^{-1} = \{h^{-1}; h \in H\} = H$.* {lmitem6}

(v) *Pre ľubovoľné podmnožiny $A, B \subseteq G$ platí $(AB)^{-1} = B^{-1}.A^{-1}$.* {lmitem4}

(vi) *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 monoide $(\mathcal{P}(G)\setminus\{\emptyset\})$ s násobením komplexov – H^{-1} jednoducho len označuje množinu inverzných prvkov ku prvkom z H.

Nebudeme dokazovať všetky časti tejto lemy nebudeme – prvé z nich sme robili na cvičeniach, ostatné zostávajú ako DÚ. Na ukážku si dokážme (iii).

Dôkaz. (iii): Pretože $(a^{-1})^{-1} = a$, každý prvok z A patrí aj do $(A^{-1})^{-1}$, čiže $A \subseteq (A^{-1})^{-1}$.

Obrátene, ak $b \in (A^{-1})^{-1}$, tak $b = (a^{-1})^{-1}$ pre nejaké $a \in A$, ale $(a^{-1})^{-1} = a$, teda $b = a \in A$. Ukázali sme aj inklúziu $(A^{-1})^{-1} \subseteq A$. □

Násobenie komplexov vo všeobecnosti nemusí byť komutatívne (ako kontrapríklad stačí zobrať v nekomutatívnej grupe 2 jednoprvkové množiny $\{a\}$ a $\{b\}$ pre prvky a a b, ktoré nekomutujú). Samozrejme, pre komutatívnu grupu je aj násobenie komplexov komutatívne.

Definícia 1.2.3. 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*.

Pomocou násobenia komplexov môžeme práve definované pojmy zapísať takto:

$$aH = \{a\}H,$$
$$Ha = H\{a\}.$$

Ako sme už spomenuli, násobenie komplexov vo všeobecnosti nemusí byť komutatívne, takisto ani nemusí vo všeobecnosti platiť $aH = Ha$. V ďalšej časti uvidíme, že podgrupy, ktoré majú túto vlastnosť sú z istého hľadiska zaujímavé. Je zrejmé, že táto rovnosť platí ak G je komutatívna.

Začali by sme však s tým, že ukážeme, že ľavé triedy G podľa H tvoria rozklad G (a podobne to platí pre pravé triedy).

Príklad 1.2.4. Triedy $\mathbb{Z}$ podľa $3\mathbb{Z}$ sú $\{3k; k \in \mathbb{Z}\}$, $\{3k+1; k \in \mathbb{Z}\}$ a $\{3k+2; k \in \mathbb{Z}\}$. Je zrejmé, že tvoria rozklad množiny $\mathbb{Z}$ – každé celé číslo je buď tvaru $3k$, $3k+1$ alebo $3k+2$. {LMAINVB}

Lema 1.2.5. *Nech H je podgrupa G a $a, b \in G$. Potom $aH = bH$ práve vtedy, keď $b^{-1}a \in H$.*
Podobne platí $Ha = Hb \Leftrightarrow ab^{-1} \in H$.

Dôkaz. $\boxed{\Rightarrow}$ Ak $aH = bH$, tak $a \in bH$, čiže $a = bh$ pre nejaké $h \in H$. Z toho $b^{-1}a = h \in H$.
$\boxed{\Leftarrow}$ Ak $b^{-1}a \in H$, tak $b^{-1}aH = H$, a teda $bH = b(b^{-1}aH) = (bb^{-1})aH = eaH = aH$.
Dôkaz druhej časti tejto lemy je analogický. □

Tvrdenie 1.2.6. *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.

Dôkaz. Každá trieda aH obsahuje prvok a, je teda neprázdna. Overme teda ešte ostatné dve podmienky z definície rozkladu.
Platí $\bigcup_{a\in G} aH \supseteq \bigcup_{a\in G}\{a\} = G$, teda zjednotenie všetkých ľavých tried je celé G.
Nech $a, b \in G$. Stačí ukázať, že ak $aH \cap bH \neq \emptyset$, tak $aH = bH$. Nech teda $x \in aH \cap bH$. To znamená, že $x = ah = bh'$ pre nejaké $h, h' \in H$. Z rovnosti $ah = bh'$ ľahko dostaneme $b^{-1}a = h'h^{-1}$, a teda $b^{-1}a \in H$. Podľa lemy 1.2.5 potom platí $aH = bH$
Dôkaz pre pravé triedy je skoro identický. □

Teraz ukážeme nejaké tvrdenia hovoriace o počtoch (mohutnostiach) tried rozkladu G podľa H.

Lema 1.2.7. *Nech H je podgrupa grupy G a $a \in G$. Potom zobrazenie $\varphi\colon H \to aH$ definované ako*

$$\varphi\colon a \mapsto ah$$

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

Dôkaz. Zobrazenie φ je injekcia: $a\varphi = b\varphi \Rightarrow ah = bh \Rightarrow a = b$ (podľa zákonov o krátení).
Priamo z definície množiny aH vyplýva, že φ je aj surjekcia.
Dôkaz pre zobrazenie ψ by bol analogický. □

Z predchádzajúcej lemy okamžite dostávame, že:

Veta 1.2.8. *Nech H je konečná podgrupa G. Potom počet prvkov každej ľavej triedy aH je rovnaký. Takisto sa rovná počtu prvkov ľubovoľnej pravej triedy Hb.*

Lema 1.2.9. *Nech H je podgrupa grupy G. Potom zobrazenie*

$$\varphi\colon aH \mapsto Ha^{-1}$$

je bijekcia medzi množinami tried $\{aH; a \in G\}$ a $\{Ha; a \in G\}$.

Dôkaz. Platí $(aH)^{-1} = H^{-1}a^{-1} = Ha^{-1}$. Preto $Ha^{-1} = Hb^{-1} \Leftrightarrow (aH)^{-1} = (bH)^{-1} \Leftrightarrow aH = bH$. (Využili sme lemu 1.2.2(iii,v).) □

Na základe predchádzajúcej vety má zmysel nasledujúca definícia.

Definícia 1.2.10. 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*.

{VTLAG}

Veta 1.2.11 (Lagrangeova veta). *Ak G je konečná grupa a H je jej podgrupa, tak platí*

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

Teda počet prvkov grupy H delí počet prvkov G.

Dôkaz. Máme rozklad množiny G na $[G\colon H]$ tried rovnakej veľkosti $|H|$. Potom $|G| = [G\colon H]|H|$.

Z toho je zrejmé aj to, že $|H| \mid |G|$ (počet prvkov H delí počet prvkov G). □

Na tomto mieste treba spomenúť, že neplatí obrátenie Lagrangovej vety v tom zmysle, že pre každý deliteľ k čísla $|G|$ (počtu prvkov grupy G) by musela existovať k-prvková podgrupa. (Pre cyklické grupy však toto tvrdenie platí, tam dokonca existuje jediná k-prvková podgrupa. Takéto tvrdenie – že by počtom prvkov bola podgrupa jednoznačne určená – takisto vo všeobecnosti neplatí.)

{DOS1}

Dôsledok 1.2.12. *Ak G je konečná grupa, tak rád každého prvku delí počet prvkov grupy G.*

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

Dôsledok 1.2.13. *Ak G je p-prvková grupa a p je prvočíslo, tak každý jej prvok okrem neutrálneho prvku je generátorom G.*

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 1.2.14. *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 1.2.12 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 jenodznačne 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 $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. □

1.3 Invariantné podgrupy

Dostali sme teda rozklad G podľa ľavých tried a rozklad G podľa pravých tried. Tieto 2 rozklady môžu byť vo všeobecnosti rôzne – my sa budeme snažiť nájsť podmienky, kedy sú rovnaké.

{TVRAHHB}

Tvrdenie 1.3.1. *Nech H je podgrupa grupy G. Ak $aH = Hb$, tak $Ha = Hb$.* (*Takisto za týchto predpokladov platí $aH = bH$.*)

Dôkaz. Ak $aH = Hb$, tak $a \in Hb$, čiže $a = hb$ pre nejaké $h \in H$. Potom $h = ab^{-1} \in H$ a podľa lemy 1.2.5 máme $Ha = Hb$.

Dôkaz druhej časti tvrdenia je analogický. □

{VTINV}

Veta 1.3.2. *Nech H je podgrupa G. Nasledujúce podmienky sú ekvivalentné:*

{item:IT1}

(i) $aH = Ha$ *pre všetky* $a \in G$,

{item:IT2}

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

{item:IT3}

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

{item:DEFINV}

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

{item:IT4}

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

{item:AHHB}

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

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

Dôkaz. Zrejmé: (i) ⇒ (ii), (i) ⇒ (iii)

(ii) ⇒ (iv): Ak platí $aH \subseteq Ha$, tak platí aj $aHa^{-1} \subseteq (Ha)a^{-1} = H(aa^{-1}) = He = H$.

Podobne sa ukáže (iii) ⇒ (iv): Máme $Ha^{-1} \subseteq a^{-1}H$, preto $aHa^{-1} \subseteq aa^{-1}H = H$.

Očividne $H \subseteq aHa^{-1}$, preto (iv) ⇒ (v).

(v) ⇒ (i): Ak $H = aHa^{-1}$, tak $Ha = (aHa^{-1})a = aH(a^{-1}a) = a(He) = aH$.

Takisto implikácia (i) ⇒ (vi) je zrejmá. Opačná implikácia (vi) ⇒ (i) vyplýva z tvrdenia 1.3.1. Z rovnosti $\{aH; a \in G\} = \{Hb; b \in G\}$ totiž vyplýva, že každé aH sa musí rovnať nejakému Hb, ale potom podľa tvrdenia 1.3.1 platí aj $aH = Ha$.

Dokázali sme:
(i) ⇒ (ii) ⇒ (iv) ⇒ (v) ⇒ (i),
(i) ⇒ (iii) ⇒ (iv) ⇒ (v) ⇒ (i),
(i) ⇔ (vi),
z čoho vyplýva, že všetky uvedené podmienky sú ekvivalentné. □

Definícia 1.3.3. Podgrupa H grupy G sa nazýva *normálna* (*invariantná*) *podgrupa,* ak spĺňa niektorú z ekvivalentných podmienok uvedených vo vete 1.3.2.

Ak G je komutatívna grupa, tak každá jej podgrupa je invariantná.
Z vety 1.3.2 vidíme, že pre invariantnú podgrupu ľavé a pravé triedy rozkladu sú totožné.

1.4 Faktorové grupy

Veta 1.4.1. *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 definovné násobenie je to isté ako násobenie komplexov. 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 $(aH)(a^{-1}H) = (aa^{-1})H = eH = H$. □

Príklad 1.4.2. $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$