Faktorové grupy

10. marca 2022

Relácia ekvivalencie

Definícia

Relácia $R \subseteq A \times A$ je *relácia ekvivalencie,* ak je reflexívna, symetrická a tranzitívna; t.j. pre všetky $a, b, c \in A$ platí:

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

Triedy ekvivalencie:

$$[a]_R = [a] = \{b \in A; aRb\}$$

Rozklad

Definícia

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. $\bigcup\limits_{i \in I} A_i = A$.

Korešpondencia:

Relácie ekvivalencie na $A \leftrightarrow$ Rozklady množiny A

Ekvivalencie a rozklady

Lema

Nech R je relácia ekvivalencie. Potom

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

Veta

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

Ekvivalencie a rozklady

Veta

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

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

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

Súčin podmnožín

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

- Násobenie podmnožín je asociatívne, t.j. $A(BC) = (AB)C$ pre ľubovoľné podmnožiny $A, B, C \subseteq G$.
- Pre ľubovoľnú podmnožinu $A \subseteq G$ platí $eA = Ae = A$.
- Ak $B \subseteq C$, tak $AB \subseteq AC$ a $BA \subseteq CA$.
- Ak H je podgrupa grupy G a $h \in H$, tak $hH = H$.
- Ak H je podgrupa grupy G, tak $H^2 = H \cdot H = H$.

Súčin podmnožín

- Pre ľubovoľnú podmnožinu $A \subseteq G$ platí $(A^{-1})^{-1} = A$, kde používame označenie $A^{-1} = \{a^{-1}; a \in A\}$.
- Ak H je podgrupa grupy G, tak $H^{-1} = \{h^{-1}; h \in H\} = H$.
- Pre ľubovoľné podmnožiny $A, B \subseteq G$ platí $(AB)^{-1} = B^{-1} \cdot A^{-1}$.
- Ak K, H sú podgrupy grupy G, tak $(HK)^{-1} = K^{-1} \cdot H^{-1} = KH$.

Ľavé a pravé triedy

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

Príklad: $G = \mathbb{Z}$, $H = 3\mathbb{Z}$
Triedy: $\{3k; k \in \mathbb{Z}\}$, $\{3k + 1; k \in \mathbb{Z}\}$, $\{3k + 2; k \in \mathbb{Z}\}$

Ľavé a pravé triedy

Lema

Nech H je podgrupa G a $a, b \in G$. Potom $aH = bH$ práve vtedy, keď $b^{-1}a \in H$. (Ďalšou ekvivalentnou podmienkou je $a^{-1}b \in H$). Podobne platí $Ha = Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow ba^{-1} \in H$.

Tvrdenie

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.

Ľavé a pravé triedy

Definícia

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.*

Trieda neutrálneho prvku je podgrupa H:

$$eH = He = H$$

Ľavé a pravé triedy

Príklad

$G = (\mathbb{R}, +)$, $H = \{(x,x); x \in \mathbb{R}\}$

$$\{(x,y) \in \mathbb{R}^2; x - y = r\}$$

$$(r, 0) + H$$

Príklad

$G = \mathbb{Z}_8$, $H = 4\mathbb{Z}_8 = \{0, 4\}$
Triedy: $\{0,4\}$, $\{1,5\}$, $\{2,6\}$, $\{3,7\}$.

Lagrangeova veta

Lema

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

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.

Lagrangeova veta

Lema

Nech H je podgrupa grupy G. Potom zobrazenie

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

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

Definícia

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

Lagrangeova veta

Veta (Lagrangeova veta)

Ak G je konečná grupa a H je jej podgrupa, tak platí

$$|G| = |H|.[G : H].$$

Teda počet prvkov podgrupy H delí počet prvkov G.

Dôsledok

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

Lagrangeova veta

Dôsledok

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).

Dôsledok

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

Normálne podgrupy

Tvrdenie

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

$$aH = Hb \Rightarrow Ha = Hb$$

$$aH = Hb \Rightarrow aH = bH$$

Normálne podgrupy

Veta

Nech H je podgrupa G. Nasledujúce podmienky sú ekvivalentné:

i. $aH = Ha$ pre všetky $a \in G$,
ii. $aH \subseteq Ha$ pre všetky $a \in G$,
iii. $Ha \subseteq aH$ pre všetky $a \in G$,
iv. $aHa^{-1} \subseteq H$ pre všetky $a \in G$,
v. $H \subseteq aHa^{-1}$ pre všetky $a \in G$,
vi. $aHa^{-1} = H$ pre všetky $a \in G$,
vii. $\{aH; a \in G\} = \{Hb; b \in G\}$.

Normálne podgrupy

Podmienku $H \subseteq aHa^{-1}$ môžeme prepísať ako:

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

Definícia

Podgrupa H grupy G sa nazýva *normálna* (*invariantná*) *podgrupa*, ak spĺňa niektorú z ekvivalentných podmienok uvedených v predošlej vete. Označujeme $H \lhd G$.

Príklady

- $\{e\} \triangleleft G,\ G \triangleleft G$
- Každá podgrupa komutatívnej grupy je normálna

Príklady

	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)

- $A_3 = \{id, (123), (132)\} \lhd G$
- 2-prvkové podrupy nie sú normálne: $H_1 = \{id, (12)\}$, $H_2 = \{id, (13)\}$ a $H_3 = \{id, (23)\}$

Faktorové grupy

Veta

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.

Príklady

$G = \mathbb{Z},\ H = 3\mathbb{Z}$

	H	$1+H$	$2+H$
H	H	$1+H$	$2+H$
$1+H$	$1+H$	$2+H$	H
$2+H$	$2+H$	H	$1+H$

$$G/H \cong (\mathbb{Z}_3, \oplus)$$

Príklady

$G = (\mathbb{R} \times \mathbb{R}, +)$ a $H = \{(x, x); x \in \mathbb{R}\}$

$$(r, 0) + H \mapsto r$$

$G/H \cong (\mathbb{R}, +)$

Kanonický homomorfizmus

Veta (Kanonický homomorfizmus)

Ak G je grupa a H je normálna podgrupa G, tak zobrazenie $f : G \to G/H$ dané predpisom

$$f : a \mapsto aH$$

je surjektívny homomorfizmus. Tento homomorfizmus voláme kanonický homomorfizmus.
Navyše, jadro kanonického homomorfizmu je práve podgrupa H.

Veta o izomorfizme

Veta (Veta o izomorfizme)

Ak $f: G \to G'$ 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

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

Príklady

- $G/G \cong \{e\}$, $G/\{e\} \cong G$
- $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$
- $\mathbb{R} \times R/\{(x,x); x \in \mathbb{R}\} \cong \mathbb{R}$
- $\mathbb{Z}_8/4\mathbb{Z}_4 \cong Z_4$