Algr.

prednáška 19.3.2007

písomka

-homomorfizmus

Izomorfizmy grúp

Def: Nech G_1, G_2 sú grupy.
Homomorfizmus grúp $\varphi: G_1 \to G_2$ je **izomorfizmus** práve vtedy keď je φ bijekcia

Príklad: $G_1 = (\{0,1,2,3\}, \oplus)$

$G_2 = (\{1,-1,i,-i\}, \cdot)$ ... komplexné čísla

G_2	$\cdot$	1	(-1)	i	$(-i)$
	1	1	(-1)	i	$(-i)$
	(-1)	(-1)	1	$(-i)$	i
	i	i	$(-i)$	(-1)	1
	$(-i)$	$(-i)$	i	1	(-1)

G_1	$\oplus$	0	1	2	3
	0	0	1	2	3
	1	1	2	3	0
	2	2	3	0	1
	3	3	0	1	2

G_2 je podgrupa $(\mathbb{C}\setminus\{0\}, \cdot)$

$X \oplus Y = (X+Y)$ zvyšok po delení 4

G_1	$\cdot$	1	i	(-1)	$(-i)$
	1	1	i	(-1)	$(-i)$
	i	i	(-1)	$(-i)$	1
	(-1)	(-1)	$(-i)$	1	i
	$(-i)$	$(-i)$	1	i	(-1)

$\varphi: G_1 \to G_2$ izomorfná

$\varphi(0) = 1$

$\varphi(1) = i$

$\varphi(2) = -1$

$\varphi(3) = -i$

Príklad:

$G_1 = (\mathbb{R}, +)$

$G_2 = (\mathbb{R}^+, \cdot)$

$\varphi = G_1 \to G_2$

$\varphi(x) = e^x$

- bijektívne
- homomorfizmus

} izomorfizmus

Definícia: Grupy G_1, G_2 sú izomorfné (značíme $G_1 \cong G_2$), ak existuje izomorfizmus $\varphi: G_1 \to G_2$ □

Veta: Pre všetky grupy G_1, G_2, G_3

(R) a) $G_1 \cong G_1$ ($G_1 \xrightarrow{id} G$)

(S) b) $G_1 \cong G_2 \Rightarrow G_2 \cong G_1$ (lebo inverzné)

(T) c) $G_1 \cong G_2 \wedge G_2 \cong G_3 \Rightarrow G_1 \cong G_3$ (lebo zložené zobrazenie)

↳ ekvivalencia (jej trieda

Mocniny

Ak $(G,\cdot)$ je grupa, $a \in G$ potom definujeme pre $k \in \mathbb{Z}$

$a^k = \underbrace{a \cdot \ldots \cdot a}_{k\text{-krát}}$ (pre $k > 0$)

$a^0 = e$

$a^k = (a^{-1})^{-k}$ pre $k < 0$

Platí aditivita exponentov. $a^k \cdot a^l = a^{k+l}$ $\quad k, l \in \mathbb{Z}$

Rád prvku

Definícia: Nech G je grupa, nech $a \in G$. Rád prvku a je najmenšie $n \in \mathbb{N}^+$ také že $a^n = e$. Ak také n neexistuje, hovoríme, že a má rád ∞ □

Príklad: v S_3

$(123)^0 = ()$

$(123)^1 = (123)$

$(123)^2 = (123)(123) = (132)$

$(123)^3 = (123)^2(123) = (132)\cdot(123) = ()$

Rád (123) v S_3 je 3.

Príklad

$(\mathbb{Z}, +)$

$1^0 = 0$

$1^1 = 1$

$1^2 = 1+1 = 2$

$1^3 = 1+1+1 = 3$

$\vdots$

Veta: Ak G je grupa, $a \in G$ potom $[a] = \{a^k : k \in \mathbb{Z}\}$ je abelovská podgrupa G

Dôkaz: (SUB1) $\forall x, y \in [a] : x \cdot y \in [a]$

Ak $x, y \in [a]$, potom existujú $k_1, k_2 \in \mathbb{Z}$ $x = a^{k_1}$, $y = a^{k_2}$

potom $x \cdot y = a^{k_1} \cdot a^{k_2} = a^{k_1+k_2} \in [a]$, lebo $k_1 + k_2 \in \mathbb{Z}$

(SUB2) $\forall x \in [a] : x^{-1} \in [a]$. Existuje $k \in \mathbb{Z}$ také že $x = a^k$

$x^{-1} = (a^k) = \underbrace{(a \ldots a)^{-1}}_{k\text{-krát}} =$ (ak $k > 0$)

↓ minulá prednáška

$= a^{-1} \ldots a^{-1} = (a^{-1})^k = a^{-k}$

Podobne pre $k<0$
$k=0$

Abelovskosť: $x, y \in [a]$

$x = a^{k_1}$

$y = a^{k_2}$

? $x \cdot y \overset{?}{=} y \cdot x$

$a^{k_1} \cdot a^{k_2} = a^{k_2} \cdot a^{k_1}$

$a^{k_1} \cdot a^{k_2} = a^{k_1+k_2}$

$a^{k_2} \cdot a^{k_1} = a^{k_2+k_1}$

$k_1+k_2 = k_2+k_1$

Veta: Ak G je konečná grupa, potom každý prvok má (konečný) rád.

Dôkaz: Uvažujme postupnosť

$a^1, a^2, a^3, \dots \rightarrow$ prvky G

G je konečná, teda iste sa to zopakuje

Existujú $k, l \in N^+$, $k < l$, $a^k = a^l$

$a^k = a^l \quad k < l$

vynásobme rovnosť a^{-k}

$a^k \cdot a^{-k} = a^l \cdot a^{-k}$

$a^k \cdot a^{-k} = a^{k+(-k)} = a^0 = e$

Teda $a^{l-k} = e$; $l-k > 0$
$l-k \in N^+$

Našli sme $m \in \mathbb{N}^+$ $(m = l-k)$ s vlastnosťou $a^m = e$, zrejme existuje aj najmenšie možné také m. □

Pravé a ľavé kosety (triedy) danej podgrupy

Príklad:

Uvažujme $G = S_3$

Vezmime podgrupu $H = \{(), (12)\}$

Uvažujme množinu množín

$\{H \cdot x : x \in S_3\}$

pričom

$H.x$ je definované takto

$H.x = \{y.x : y \in H\}$

Ráčtajme $H.X$ pre rôzne x

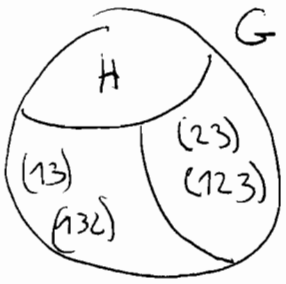
$H.() = \{().(), (12).()\} = \{(), (12)\}$

$H.(12) = \{().(12), (12).(12)\} = \{(12), ()\}$

$H(23) = \{().(23), (12).(23)\} = \{(23), (123)\} = H.(123)$

$H(13) = \{().(13), (12).(13)\} = \{(13), (132)\} = H.(132)$

AHA



→ rozklad G podľa H na pravé kosety

Definícia: Nech G je grupa nech H je podgrupa G.

Pravý koset prvku $x \in G$ podľa H je množina $H.x = \{y.x : y \in H\}$

Ľavý je $x.H = \{x.y : y \in H\}$

Veta: Nech G je grupa. Systém množín $\{Hx : x \in G\}$ tvorí rozklad G. Navyše ak G je konečná, všetky triedy tohto rozkladu majú rovnako veľa prvkov ako H

Dôkaz: (R0): Každé Hx je neprázdne. Zrejme áno, lebo $H \neq \emptyset$

(R1): Zjednotenie všetkých Hx je rovné G

$$\bigcup_{x \in G} Hx = G$$

($\subseteq$): Keďže každé $Hx \subseteq G$,

$$\bigcup_{x \in G} Hx \subseteq G$$

($\supseteq$) $\bigcup_{x \in G} Hx \supseteq G$ Nech $a \in G$, $H.a = \{y.a : y \in H\}$

H je podgrupa G, teda $e \in H$

Teda $e \cdot a \in H \cdot a$, ale $e \cdot a = a$.

Takže $a \in H \cdot a \subseteq \bigcup_{x \in G} Hx \quad (a = x)$

(R2) Treba dokázať, že množiny v $\{Hx : x \in G\}$ sú „po dvoch disjunktné"

Zj.

$$Hx_1 \neq Hx_2 \Rightarrow Hx_1 \cap Hx_2 = \emptyset$$

to je to isté ako

$$Hx_1 \cap Hx_2 \neq \emptyset \Rightarrow Hx_1 = Hx_2$$

Nech $Hx_1 \cap Hx_2 \neq \emptyset$. Potom existuje $z \in Hx_1 \cap Hx_2$

Teda $z \in Hx_1$, $z \in Hx_2$

$z \in Hx_1$ znamená $z = y_1 \cdot x_1$ pre nejaké $y_1 \in H$

$z \in Hx_2$ znamená $z = y_2 \cdot x_2$ pre nejaké $y_2 \in H$

Podme dokázať $Hx_1 \subseteq Hx_2$ (opačná implikácia sa dokáže podobne)

$Hx_1 \overset{?}{\subseteq} Hx_2$

Každé $w \in Hx_1$ patrí do Hx_2 ?

Nech $w \in Hx_1$. Potom $w = y \cdot x$ pre nejaké $y \in H$

Máme 3 rovnosti

$z = y_1 \cdot x_1$

$z = y_2 \cdot x_2$

$w = y \cdot x_1$

$z = y_1 \cdot x_1$ / zľava $(y_1)^{-1}$

$y_1^{-1} z = \underbrace{y_1^{-1} \cdot y_1}_{e} \cdot x_1$

$y_1^{-1} \cdot z = x_1 e$ – dosadíme do $w = y \cdot x$

$w = y \cdot y_1^{-1} \cdot z$ → použijeme $z = y_2 \cdot x_2$

$w = y \cdot y_1^{-1} \cdot y_2 \cdot x_2 \Rightarrow w \in H \cdot x_2$

$\in H$

- Každé Hx má rovnako veľa prvkov ako H, ak G je konečná.

Uvažujme pre dané $x \in G$ zobrazenie

$\tilde{\gamma}_x : H \Rightarrow Hx$

$\tilde{\gamma}_x(\gamma) = \gamma \cdot x$

Zrejme je $\tilde{\gamma}_x$ surjekcia (vid' def. Hx)

Injektivita $\tilde{\gamma}_x$

Nech $\tilde{\gamma}_x(\gamma_1) = \tilde{\gamma}_x(\gamma_2)$

$x \cdot \gamma_1 = x \cdot \gamma_2$

$\Downarrow$ krátenie

$\gamma_1 = \gamma_2$

Existuje teda bijekcia

$\tilde{\gamma}_x : H \Rightarrow Hx$ i H, Hx majú rovnako veľa prvkov □

Veta: (Lagrangeova)

Počet prvkov podgrupy H konečnej grupy G je deliteľom počtu prvkov G ($|H| \mid |G|$)

Dôkaz

$\{Hx : x \in G\}$ je rozklad G.

Každé Hx má rovnako veľa prvkov ako H

Teda Hx majú rovnako veľa prvkov, a to $|H|$.

→ všetky rovnaký počet ⇒ rovný H

$|G| = k|H|$, kde, k je počet tried v $\{Hx : x \in G\}$ □

Dôsledok: Ak G je grupa, ktorá má prvočíselne veľa prvkov, potom G je abelovská

Dôkaz: Vezmi $a \in G$. $[a]$ je abelovská podgrupa

$a \neq e$

$|[a]| \mid |G|$, $|G|$ prvočíslo, $|[a]| > 1$ ⇒ $|[a]| = |G|$

$\Downarrow$

$[a] = G$