Algebra 2 (NMAG 202)

poznámky k streamu

Jan Šťovíček

30. 3. 2020

Katedra algebry MFF UK

Působení grupy na množině

Definice

Působením grupy $(G, \cdot, ^{-1}, 1)$ na množině X rozumíme grupový homomorfismus $\varphi\colon G \to S(X)$.

$(S(X), \circ, ^{-1}, 1_X)$ je grupa permutací na množině X.

Pro $g \in G$ a $x \in X$ budeme místo $\varphi(g)(x)$ psát $g(x)$. Tj. máme

$$G \times X \to X,$$

$$(g, x) \mapsto g(x)$$

splňující

1. $(g \cdot h)(x) = g(h(x))$ $(\forall g, h \in G)(\forall x \in X)$,
2. $1(x) = x$ $(\forall x \in X)$.

Naopak každé $G \times X \to X$ splňující podmínky výše určuje působení G na X (definujeme $\varphi\colon G \to S(X)$ předpisem $\varphi(g) = g(-)$).

Relace tranzitivity a orbity

Definice
Mějme působení $\varphi\colon G \to S(X)$. Zavedeme na X relaci tranzitivity:
$x \sim y$ pokud $(\exists g \in G)(g(x) = y)$.

Lemma 5.1. Relace tranzitivity je ekvivalence na množině X.

Důkaz:

Reflexivita: $1(x) = x$.

Symetričnost: $g(x) = y \implies g^{-1}(y) = x$.

Tranzitivita: $g(x) = y$ a $h(y) = z \implies (h \cdot g)(x) = z$.

Definice
Bloky relace tranzitivity nazýváme orbity. Značení:

$$[x] = \{y \in X \mid x \sim y\} = \{g(x) \mid g \in G\} \qquad (x \in X).$$

Pevné body a stabilizátory

Definice
Mějme působení $\varphi\colon G \to S(X)$ a vezměme $g \in G$ a $x \in X$.

- x je pevným bodem g pokud $g(x) = x$. Množinu všech pevných bodů g značíme

$$X_g = \{x \in X \mid g(x) = x\}.$$

- Stabilizátorem prvku $x \in X$ nazveme množinu

$$G_x = \{g \in G \mid g(x) = x\}.$$

Lemma 5.2. G_x je podgrupa G.

Důkaz: $1(x) = x$ a
$g(x) = x = h(x) \implies (g \cdot h)(x) = g(h(x)) = x$ a $g^{-1}(x) = x$.

Mohutnost orbity = index stabilizátoru

Tvrzení 5.3. Mějme působení $\varphi\colon G \to S(X)$. Pak pro každé $x \in X$ platí

$$|[x]| = [G : G_x].$$

Je-li tedy G konečná, pak mohutnost orbity dělí řád grupy.

Důkaz: Ukážeme, že zobrazení

$$\psi\colon \{gG_x \mid g \in G\} \to [x],$$
$$gG_x \mapsto g(x)$$

je dobře definovaná bijekce. Dobrá definovanost a prostota:

$$gG_x = hG_x \iff h^{-1}g \in G_x \iff$$
$$h^{-1}(g(x)) = x \iff h(x) = g(x)$$

Surjektivita plyne přímo z definice orbity.

Cvičení: Jsou-li $x \sim y$, jak souvisí G_x a G_y?

Burnsideova věta

Věta 5.4 (Burnsideova věta). Nechť konečná grupa G působí na konečnou množinu X. Pak platí

$$|X/\sim| = \frac{1}{|G|} \cdot \sum_{g \in G} |X_g|.$$

Tj. počet orbit je roven průměrnému počtu pevných bodů.

Důkaz: Označme $M = \{(g, x) \mid g(x) = x\} \subseteq G \times X$. Pak

$$\sum_{x \in X} |G_x| = |M| = \sum_{g \in G} |X_g|.$$

$$\text{Tj. } \frac{1}{|G|} \cdot \sum_{g \in G} |X_g| = \frac{1}{|G|} \cdot \sum_{x \in X} |G_x| \overset{5.3}{=} \frac{1}{|G|} \cdot \sum_{x \in X} \frac{|G|}{|[x]|} = \sum_{x \in X} \frac{1}{|[x]|} =$$

$$\sum_{O \text{ orbita}} \sum_{x \in O} \frac{1}{|[x]|} = \sum_{O \text{ orbita}} 1 = |X/\sim|.$$

Cauchyova věta

Věta 5.5 (Cauchyova věta). Buď G konečná grupa p prvočíslo, které dělí řád G. Pak G obsahuje prvek řádu p.

Důkaz: Uvažujme množinu

$$X = \{(g_1, g_2, \ldots, g_p) \in G^p \mid g_1 g_2 \cdots g_p = 1\}$$

a akci grupy $\mathbb{Z}_p$ rotací o jednu pozici doprava.

Pak $|X| = |G|^{p-1}$ je dělitelné p a každá orbita má buď 1 nebo p prvků (Tvrzení 5.3).

Jednoprvkové orbity jsou tvaru $\{(a, a, \ldots, a)\}$, kde $a^p = 1$ v G. Aspoň jedna taková existuje pro $a = 1$ a protože p dělí $|X|$, musí existovat aspoň jedna další.

Reprezentace grup

Definice

Reprezentací grupy $(G, \cdot, ^{-1}, 1)$ nad tělesem T rozumíme grupový homomorfismus $\varphi\colon G \to GL_n(T)$.

Reprezentace grup jsou také všudypřítomné, vyskytují se např. v důkazu Velké Fermatovy věty, ve standardním modelu částicové fyziky a na mnoha dalších místech. Odkazy:

1. Úvodní video: `https://www.youtube.com/watch?v=qpGDNKgfHHg`,
2. Proseminář: `http://www.karlin.mff.cuni.cz/~stanovsk/vyuka/proseminar.htm`.

Cyklické grupy – definice, příklady a věta

Definice
Grupa G je cyklická, pokud má jediný generátor, tj. existuje $a \in G$ takové, že

$$G = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}.$$

Příklady

- $\{e^{\frac{2\pi ik}{n}} \mid k \in \mathbb{Z}\} \leq \mathbb{C}^*$ je cyklická (samotná grupa $\mathbb{C}^*$ ale není!).
- $\mathbb{Z}_5^* = \langle 2 \rangle$, $\mathbb{Z}_7^* = \langle 3 \rangle$, $\mathbb{Z}_{11}^* = \langle 2 \rangle$, ...

Věta 4.6 Je-li T těleso a G konečná podgrupa T^*, pak je G cyklická.

Důkaz: příště.

Cyklické grupy až na isomorfismus

Věta 3.7 Každá cyklická grupa $(G, \cdot, ^{-1}, 1)$ je isomorfní buď

- grupě $(\mathbb{Z}, +, -, 0)$ nebo
- grupě $(\mathbb{Z}_n, +, -, 0)$ pro nějaké $n \geq 1$.

Důkaz: Podle předpokladu je $G = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$.

Případ č. 1: $\mathrm{ord}(a) = \infty$. $\varphi\colon \mathbb{Z} \to G, k \mapsto a^k$ je grupový homomorfismus (tvrzení 1.2) a je určitě na. Pokud $a^k = a^l$ pro $k > l$, pak $a^{k-l} = 0$, tedy $k - l = 0$ protože a má nekonečný řád. Tj. φ je isomorfismus.

Případ č. 2: $\mathrm{ord}(a) = n < \infty$. Nejdřív se ukáže, že $a^k = a^{k \bmod n}$ pro každé $k \in \mathbb{Z}$. Pak se podobně jako výše ukáže, že $\varphi\colon \mathbb{Z}_n \to G, k \mapsto a^k$ je isomorfismus.

Diskrétní logaritmus

Z věty 4.6 pro každé prvočíslo p existuje $a \in \mathbb{Z}_p^*$ (tzv. primitivní prvek $\mathbb{Z}_p$) a isomorfismus grup

$$\varphi \colon \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*,$$
$$k \mapsto a^k.$$

Výpočet zobrazení φ lze efektivně implementovat na počítači:

1. Napíšeme k ve dvojkové soustavě: $k = 2^{e_1} + 2^{e_2} + \cdots + 2^{e_r}$, $r \leq \log_2(k)$.
2. Spočítáme mocniny v $\mathbb{Z}_p$:
   $a_0 = a$, $a_1 = a^2$, $a_2 = (a^2)^2$, $\ldots$, $a_{i+1} = a_i^2$, $\ldots$,
3. Pak $a^k \equiv a_{e_1} \cdot a_{e_2} \cdots a_{e_r} \pmod{p}$.

Obecná efektivní implementace zobrazení $\varphi^{-1} \colon \mathbb{Z}_p \to Z_{p-1}$ není známa! Tj. pro dané $b \in \mathbb{Z}_p^*$ neumíme najít $k \in \mathbb{Z}_{p-1}$ takové, že $b \equiv a^k \pmod{p}$ (tzv. diskrétní logaritmus b při základu a).

Diffieho-Hellmanova výměna klíčů

Cíl: Alice a Bob se mají přes nezabezpečený kanál shodnou na společném tajném klíči.

Postup:

1. A a B se veřejně dohodnou na (velkém) prvočíslu p a generátoru a grupy $\mathbb{Z}_p^*$.
2. A si zvolí tajné číslo $n \in \mathbb{Z}_{p-1}$ a pošle B prvek $a^n \in \mathbb{Z}_p$.
3. B si zvolí tajné číslo $m \in \mathbb{Z}_{p-1}$ a pošle A prvek $a^m \in \mathbb{Z}_p$.
4. Pak A i B jsou ze zaslaných údajů schopni vypočítat prvek $a^{mn} = (a^m)^n = (a^n)^m \in \mathbb{Z}_p$. Tento prvek bude jejich tajný klíč.

Útočník odposlouchávající komunikaci se dozví p a trojici prvků (a, a^n, a^m) ze $\mathbb{Z}_p$. Není z těchto dat znám efektivní výpočet a^{mn} (tzv. Diffieho-Hellmanův problém).