Grupa permutací, grupa zbytkových tříd

Petr Pupík

1.3.2010

Co nás dnes čeká

Opakování

1. Množina všech bijektivních zobrazení na konečné množině M tvoří spolu s operací skládání zobrazení grupu, které říkáme **grupa permutací**.
2. Je-li $|M| = n$, značíme grupu permutací symbolem Σ_n, nebo $\mathbb{S}_n$.
3. Platí, že $|\Sigma_n| = n!$.
4. Každou neidentickou permutaci můžeme napsat jako součin nezávislých cyklů.
5. Cyklus délky 2 nazýváme transpozice.
6. Každou permutaci můžeme napsat jako součin transpozic (cyklus délky k můžeme napsat jako součin $k - 1$ transpozic)

Opakování

Příklad

Uvažme permutace $\sigma, \rho \in \Sigma_7$. Rozložte permutace σ, ρ na součin nezávislých cyklů. Určete σ, ρ, $\rho \circ \sigma$. Rozložte permutaci σ na součin transpozic.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 1 & 5 & 7 & 2 & 6 \end{pmatrix}, \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 6 & 7 & 3 & 5 & 2 \end{pmatrix}.$$

Parita permutace

Definice

Řekneme, že cyklus délky k má paritu $(-1)^{k-1}$.

- Parita složení permutací je součinem parit jednotlivých permutací.
- Permutace parity 1 se nazývá sudá, permutace parity -1 se nazývá lichá
- Rozložíme-li permutaci na součin transpozic, z jejich počtu ihned můžeme určit paritu dané permutace.
- Permutace σ z předchozího příkladu je lichá.

Parita permutace

Paritu permutace můžeme stanovit i jiným způsobem.

Definice

Nechť je dána permutace $\pi \in \Sigma_n$. Nechť $i, j \in \{1, 2, \ldots, n\}$. Je-li pro $i < j$ v permutace $\pi(i) > \pi(j)$, řekneme, že dvojice $(\pi(i), \pi(j))$ tvoří v permutaci π inverzi.

Věta

Permutace $\pi \in \Sigma_n$ je sudá právě tehdy, když počet inverzí permutace π je sudé číslo.

- Zadáme-li si danou permutaci pomocí „grafu s šipkami“, dostáváme počet invrezí jako počet křížení šipek.
- Permutace σ z našeho příkladu má 5 inverzí.

Umocňování permutací, iverzní relace

Mocnina dané permutace a inverzní permutace k dané permutaci se snadno určí z rozkladu permutace na nezávislé cykly.

Věta

Umocníme-li cyklus délky k na k-tou (tj. složíme daný cyklus k-krát), dostaneme identitu.

- Určeme si osmou mocninu permutace σ z našeho příkladu.
- Inverzní relace se stanoví snadno přímo ze zadání nebo z rozkladu na nezávislé cykly. Ty totiž stačí „číst odzadu“.

Shodná zobrazení nechávající daný útvar na místě

Již na střední škole jste se jistě setkali se skládáním shodných zobrazení. Například zobrazíme-li libovolný útvar v osové souměrnosti podle osy *o* a výsledek opět zobrazíme v této osové souměrnosti, dostaneme původní útvar. Složením dvou osových souměrností s osami rovnoběžnými je posunutí a tak dále.

V mineralogii jste se jistě také setkali s krystalickými soustavami. Uvažovali jste zde jednotlivé soustavy a jejich symetrie.

Shodná zobrazení nechávající daný útvar na místě

Uvažujme nyní množinu zobrazení, která nechávají daný útvar sám na sobě. U čtverce tak dostáváme:

1. Identita
2. Dvě osové souměrnosti, jejichž osy procházejí středy protějších stran
3. Dvě osové souměrnosti takové, že úhlopříčky leží na osách těchto souměrností
4. Otočení (Rotace) o 90°, 180°, 270°.

Uvědomme si, že složením libovolných dvou z těchto zobrazení dostaneme opět zobrazení, které nechá čtverec sám na sobě. Očíslujeme-li si vrcholy čtverce čísly $1, 2, 3, 4$, dokážeme libovolné zobrazení zadat jako permutaci dané čtyřprvkové množiny. Dostáváme tak podmnožinu grupy Σ_4. Ta je zřejmě grupoidem, asociativita je zděděna z grupy Σ_4. Naše množina obsahuje neutrální prvek (identitu). Snadno se nahlédne, že také ke každému zobrazení existuje zobrazení inverzní, které také převádí čtverec sám na sebe. Dostali jsme tak uvnitř grupy Σ_4 další grupu (podgrupu grupy Σ_4).

Grupy symetrií

Zobecníme-li naše úvahy pro libovolný pravidelný n-úhelník, dostáváme grupu symetrií, která bude obsahovat n osových souměrností a n rotací. Tuto grupu nazýváme **dihedrální grupa** a značíme D_{2n} (v některých publikacích se značí D_n).

Příklad

Určete, jak vypadá grupa symetrií rovnostranného trojúhelníka.

K zamyšlení

Zkuste si sami určit, jak vypadá grupa symetrií pravidelného čtyřstěnu, grupa symetrií krychle.

Grupy symetrií

Nemusíme uvažovat pouze pravidelné n-úhelníky, ale prakticky libovolné útvary:

Kongruence

Dalším příkladem konečných (tentokrát komutativních) grup jsou grupy zbytkových tříd. Než si však řekneme, jak tyto grupy vypadají, musíme si říci něco o kongruencích.

Definice

Nechť $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Řekneme, že $a \equiv b \pmod{m}$, jestliže a, b dávají stejný zbytek po dělení číslem m.

Kongruence

Věta

Nechť $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. *Následující podmínky jsou ekvivalentní:*

1. $a \equiv b \pmod{m}$
2. $m|(a-b)$
3. $\exists k \in \mathbb{Z} : a = b + mk$

Věta

Nechť $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{N}$, $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$. *Potom platí, že*

1. $a + c \equiv b + d \pmod{m}$
2. $a \cdot c \equiv b \cdot d \pmod{m}$

Kongruence

Věta (Bezoutova)

Nechť $a, b \in \mathbb{Z}$. Potom existují celá čísla x, y taková, že $ax + by = (a, b)$.

Důkaz plyne z Euklidova algoritmu.

Věta (Malá Fermatova)

Nechť $a, m \in \mathbb{N}$, $(a, p) = 1$. Potom platí, že

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p).$$

Několik způsobů důkazů.

Zbytkové třídy

Relace kongruence je na množině celých čísel relací ekvivalence. Můžeme tedy uvážit rozklad příslušný této ekvivalenci. Dostáváme tak množinu tříd, kterým říkáme zbytkové třídy modulo m. Nyní budeme chtít na množině zbytkových tříd definovat nové operace sčítání a násobení. Položme

$$[a]_m + [b]_m = [a + b]_m$$

$$[a]_m \cdot [b]_m = [a \cdot b]_m$$

Uvědomme si, že tato definice je korektní.

- Označme množinu všech zbytkových tříd modulo m symbolem $\mathbb{Z}_m$. V anglické literatuře můžete najít označení $\mathbb{Z}/m\mathbb{Z}$. Toto označení si vysvětlíme později.

Grupa zbytkových tříd

Věta

$(\mathbb{Z}_m, +)$ *tvoří komutativní grupu.*

Věta

$(\mathbb{Z}_m, \cdot)$ *tvoří komutativní pologrupu s neutrálním prvkem.*

Grupa invertibilních prvků

Nechť G je pologrupa s neutrálním prvkem. Označme $G^\times$ množinu všech prvků, které mají v G inverzi.

Věta

$G^\times$ je grupa.

Eulerova funkce

Pokusme se nyní určit, ke kterým prvkům existuje v pologrupě $(\mathbb{Z}_m, \cdot)$ inverzní prvek a kolik prvků bude mít výsledná grupa.

Definice

Funkce φ, která přiřadí přirozenému číslu m počet přirozených čísel, která jsou menší nebo rovna m a jsou s m nesoudělná, se nazývá eulerova funkce.

- $\varphi(1) = 1$
- $\varphi(p) = p - 1$
- $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$
- Pro libovolná $m, n \in \mathbb{N}$, $(m, n) = 1$, platí, že $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.
- $\varphi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = (p_1 - 1)p_1^{\alpha_1 - 1} \cdots (p_k - 1)p_k^{\alpha_k - 1}$

Grupa zbytkových tříd

Věta

Nechť a, b jsou celá čísla, m přirozené. Potom existuje celé číslo x takové, že $ax \equiv b \pmod{m}$ právě tehdy, když $(a, m)|b$.

Důsledek

Grupa $(\mathbb{Z}_m^\times, \cdot)$ má $\varphi(m)$ prvků.

- Určete, kolik prvků má grupa $(\mathbb{Z}_p^\times, \cdot)$, $(\mathbb{Z}_{24}^\times, \cdot)$.
- Určete inverzi k prvku $[5]_{17}$ v grupě $(\mathbb{Z}_{17}^\times, \cdot)$.

Podgrupy

Definice

Nechť $(G, \star)$ je grupa, $\emptyset \neq H \subseteq G$. Je-li $(H, \star)$ grupa, říkáme, že H je podgrupa grupy G.

Věta

Nechť $(G, \star)$ je grupa, $\emptyset \neq H \subseteq G$. Potom H je podgrupa grupy G právě tehdy, když

1. $\forall a, b \in H : a \cdot b \in H$
2. $\forall a \in H : a^{-1} \in H$

Podgrupy

1. $\mathbb{Z}$ je podgrupa grup $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
2. Každá podgrupa $\mathbb{Z}$ je tvaru $m\mathbb{Z} = \{ma \mid a \in \mathbb{Z}\}$.
3. $\mathbb{R}^+$ je podgrupa grupy $\mathbb{R}^*$.
4. $\mathcal{SL}_n(\mathbb{R})$ je podgrupa grupy $\mathcal{GL}_n(\mathbb{R})$.
5. D_{2n} je podgrupa grupy Σ_n.
6. Množina A_n všech sudých permutací tvoří podgrupu Σ_n.

Podgrupy

Věta

Nechť G je grupa, K, L její podgrupy. Potom $K \cap L$ je podgrupa grupy K.

Definice

Nechť $M \subseteq G$, potom množinu

$$\langle M \rangle = \bigcap_{\text{podgrupy } H, M \subseteq H} H$$

nazýváme podgrupa generovaná množinou M.

Cyklické grupy

Věta

Nechť G je grupa, K, L její podgrupy, $a \in G$. Potom

1. $\langle K \cup L \rangle = \{k \cdot l \mid k \in K, l \in L\}$
2. $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Definice

Řekneme, že grupa G je cyklická, jestliže je generovaná nějakým svým prvkem.

Cyklické grupy

1. $\mathbb{Z} = \langle 1 \rangle$
2. $\mathbb{Z}_m = \langle [1]_m \rangle$.
3. $D_8 = \langle r_{90^\circ}, o \rangle$
4. $\mathbb{Z}_7^* = \langle [3]_7 \rangle$