O grupách

4. kapitola. Pojem isomorfismu grup. Abstraktní pojetí grupy (typ isomorfismu)

In: Ladislav Rieger (author): O grupách. (Czech). Praha: Mladá fronta, 1974. pp. 43–[52].

Persistent URL: http://dml.cz/dmlcz/403815

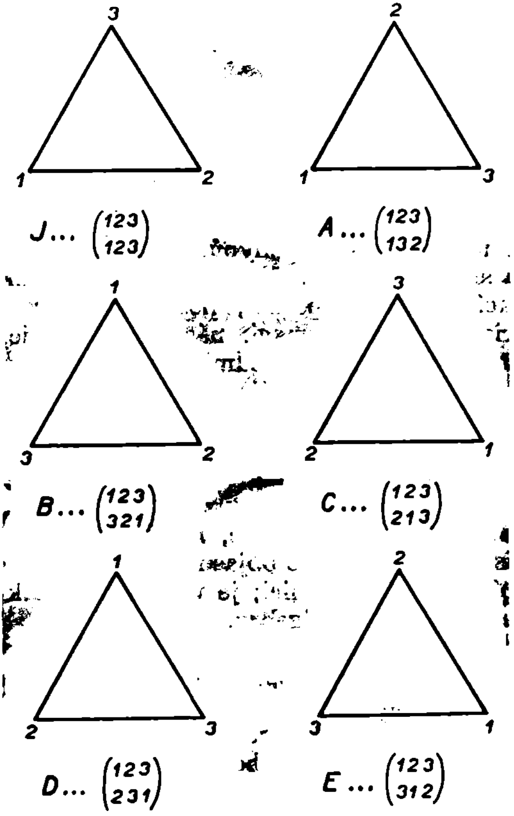
4. kapitola

POJEM ISOMORFISMU GRUP. ABSTRAKTNÍ POJETÍ GRUPY (TYP ISOMORFISMU)

Jak jsme v předchozím poznali, prvky grupy mohou být věci velmi rozmanitého druhu: např. zákrytové pohyby, čísla, permutace, geometrické transformace, matice, barvy, skupiny z daných předmětů. Násobení v grupě může být dáno velmi různými způsoby: např. skládáním zákrytových pohybů, násobením čísel v původním smyslu slova, sečítáním čísel, kombinováním permutací v daném pořadí, postupným prováděním geometrických transformací, násobením matic, mísením barev, shrnováním předmětů ze dvou skupin do jedné, pokud se nevyskytují v obou.

Stává se však, že dvě grupy, ačkoli se liší vzájemně buď ve svých prvcích (některých či ve všech), anebo ve způsobu, resp. výsledcích grupového násobení, anebo v obojím, přece jsou *téhož typu*, čili, jak se říká, jsou *isomorfní* (z řec. iso = stejně, morfos = tvar). Pojem isomorfismu grup si dříve objasníme na příkladech, než přistoupíme k jeho definici; je to jeden ze základních pojmů celé abstraktní algebry.

Vraťme se ke grupě zákrytových pohybů rovnostranného trojúhelníka z 2. kap. Označme si jeho vrcholy v základní poloze číslicemi 1, 2, 3 od levého dolního vrcholu počínaje proti směru ruček hodin (obr. 5). Pak s každým zákrytovým pohybem dojde k určité současné náhradě každého z čísel 1, 2, 3 opět jedním z čísel 1, 2, 3, čili k permutaci čísel 1, 2, 3, nebo chceme-li, k permutaci vrcholů. Obráceně, každá ze šesti permutací tří čísel 1, 2, 3 je takto dána právě jedním zákrytovým pohybem našeho trojúhelníka. Avšak co je důležitějšího: zastoupíme-li jednotlivé zákrytové pohyby našeho



Obr. 6

trojúhelníka odpovídajícími permutacemi, pak jsme tím již zastoupili i každý součin (výsledek složení) pohybů součinem permutací, odpovídajících po řadě daným pohybům. Tak např. permutace $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ odpovídá překlopení A kolem osy úhlu α, permutace $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ odpovídá otočení E roviny trojúhelníka o 240°.

Součin obou permutací $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} . \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ je permutace odpovídající překlopení kolem osy úhlu β, $B = A . E$ (viz tab. v 2. kap. a obr. 6).

Vidíme tedy, že symetrickou grupu permutací S_3 můžeme od grupy zákrytových pohybů rovnostranného trojúhelníka odlišit jen konkrétní povahou prvků (jednou pohyby roviny trojúhelníka, podruhé permutace) a různým způsobem, jakým se provádí násobení. Pomocí vhodného vzájemně jednoznačného přiřazení prvků jedné grupy k prvkům druhé lze však přenést násobení z jedné grupy do druhé a obráceně.

Abychom náš příklad doplnili, sestrojme si ještě i grupu skládající se ze šesti dvojřádkových matic, která bude rovněž typu naší grupy všech permutací tří předmětů, čili typu grupy všech zákrytových pohybů rovnostranného trojúhelníka, a to pomocí příkladů 2 a 3 ze 3. kap.

Euklidovské otočení D roviny rovnostranného trojúhelníka o úhel 120° (čili o $\frac{2}{3}\pi$) je dáno lineární homogenní transformací

$$x = -\tfrac{1}{2}x' - \tfrac{1}{2}\sqrt{3}y'$$
$$y = \tfrac{1}{2}\sqrt{3}x' - \tfrac{1}{2}y'$$

protože

$$a_{11} = \cos\frac{2\pi}{3} = -\tfrac{1}{2},\ a_{12} = -\sin\frac{2\pi}{3} = -\tfrac{1}{2}\sqrt{3},$$

$$a_{21} = \sin\frac{2\pi}{3} = \tfrac{1}{2}\sqrt{3},\ a_{22} = \cos\frac{2\pi}{3} = -\tfrac{1}{2}$$

Podobně otočení $D^2 = E$ o $240°$ $\left(\text{čili o } \frac{4\pi}{3}\right)$ je dáno transformací

$$\begin{aligned} x &= -\tfrac{1}{2}x' + \tfrac{1}{2}\sqrt{3}y' \\ y &= -\tfrac{1}{2}\sqrt{3}x' - \tfrac{1}{2}y' \end{aligned}$$

Konečně překlopení C kolem osy úhlu γ je dáno transformací

$$\begin{aligned} x &= -x' \\ y &= y' \end{aligned}$$

Z obou otočení D a E a z překlopení C dovedeme složit všechny ostatní zákrytové pohyby rovnostranného trojúhelníka (viz tab. z 2. kap.), neboť nalézáme $A = CD$, $B = CE$. Nahraďme tedy zákrytové pohyby příslušnými, analyticky je vyjadřujícími lineárními homogenními transformacemi, skládání pohybů nahraďme postupným prováděním transformací a konečně transformace a jejich postupné provádění nahraďme příslušnými maticemi a jejich násobením podle předchozího odstavce. Dostaneme celkem toto vzájemně jednoznačné přiřazení zákrytových pohybů k permutacím a permutací k maticím 2. stupně (s reálnými koeficienty), které vzájemně přenáší skládání pohybů v násobení permutací a v násobení matic (srov. tab. I a obr. 6):

Zákrytový pohyb (rovnostr. trojúh.)	Permutace (3 vrcholů)	Matice (2. stupně)
Překlopení A (kolem osy úhlu α)	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	$\begin{pmatrix} \frac{1}{2} & \frac{1}{2}\sqrt{3} \\ \frac{1}{2}\sqrt{3} & -\frac{1}{2} \end{pmatrix}$
Překlopení B (kolem osy úhlu β)	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	$\begin{pmatrix} \frac{1}{2} & -\frac{1}{2}\sqrt{3} \\ -\frac{1}{2}\sqrt{3} & -\frac{1}{2} \end{pmatrix}$
Překlopení C (kolem osy úhlu γ)	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$
Otočení D o $+120°$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$\begin{pmatrix} -\frac{1}{2} & -\frac{1}{2}\sqrt{3} \\ \frac{1}{2}\sqrt{3} & -\frac{1}{2} \end{pmatrix}$
Otočení E o $+240°$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	$\begin{pmatrix} -\frac{1}{2} & \frac{1}{2}\sqrt{3} \\ -\frac{1}{2}\sqrt{3} & -\frac{1}{2} \end{pmatrix}$
Identický pohyb J	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Takovému vzájemně jednoznačnému přiřazení prvků jedné grupy k prvkům jiné grupy, jaké je tu vyznačeno, tedy takovému, které vystihuje násobení v jedné grupě násobením v jiné (které převádí násobení v jedné grupě v násobení v druhé), říkáme *isomorfní zobrazení* jedné grupy na druhou grupu; obě grupy pak platí za (vzájemně) isomorfní. Uveďme si ještě jeden každému dobře známý příklad takového isomorfního zobrazení jedné grupy na druhou. První grupa budiž *multiplikativní* grupa všech *kladných* reálných čísel, druhá grupa budiž *aditivní* grupa *všech* reálných čísel *vůbec*. Pak za isomorfní zobrazení první grupy na druhou můžeme považovat logaritmování (řekněme při základu 10). Ke každému kladnému číslu je dána jediná reálná hodnota jeho logaritmu při základu 10, každé reálné číslo (kladné, záporné i nula) je desítkovým logaritmem právě jednoho kladného reálného čísla, a co hlavního, logaritmus součinu se rovná součtu logaritmů, čili násobení kladných reálných čísel se vystihuje (početně jednodušším) sečítáním čísel reálných (vůbec), totiž příslušných logaritmů. Z tohoto příkladu též vidíme, že takové isomorfní zobrazení jedné grupy (např. multiplikativní grupy kladných reálných čísel) na jinou grupu (např. aditivní grupu všech reálných čísel) nemusí být jen jedno, neboť právě takový isomorfismus dává i logaritmování při jiném, třeba při tzv. přirozeném základu.

Přistupme nyní k obšírné a přesné definici důležitého pojmu isomorfního zobrazení a isomorfismu grup.

Definice

Buďtež G a H dvě grupy. Nechť ke každému prvku x z grupy G je přiřazením f dán přesně jeden prvek $y = f(x)$ z grupy H, tzv. obraz prvku x z G při zobrazení f, tak, že jsou splněny tyto dvě podmínky:

(i) ke každému prvku y z grupy H existuje právě jeden prvek x z grupy G tak, že $y = f(x)$,

(ii) pro každé dva prvky x_1 a x_2 z grupy G je splněna rovnost

$$f(x_1x_2) = f(x_1) \,.\, f(x_2)$$

(jestliže součin v G vyznačujeme prostým psaním činitelů vedle sebe a součin v H kvůli rozlišení vyznačujeme tečkou mezi činiteli). Pak zobrazení f se nazývá isomorfní zobrazení grupy G na grupu H.

Říkáme, že grupa G_1 je isomorfní s grupou G_2 jestliže existuje aspoň jedno takové isomorfní zobrazení G_1 na G_2, a vyznačujeme to symbolem

$$G_1 \cong G_2$$

V předchozím příkladě H byla multiplikativní grupa kladných reálných čísel, G byla aditivní grupa všech reálných čísel čili „." jest třeba nahradit „+" (při čemž nic nevadí, že zde náhodou všechny prvky první grupy jsou obsaženy mezi prvky druhé grupy, což je ovšem možné jen při nekonečných grupách) isomorfní zobrazení f byl desítkový logaritmus, $f(x) = \log_{10} x$.

Jaký smysl má pojem isomorfismu grup?

Především ten, že stačí dokázat poučku o jedné určité grupě, abychom tím měli zároveň dáno neomezené množství odpovídajících pouček pro každou grupu, která se ukáže být s danou grupou isomorfní. Je to požadavek obecnosti výsledků teorie grup, který nutí k jasnému zavedení a využití pojmu isomorfismu.

Abstraktní teorie grup se tedy nezabývá určitou konkrétní grupou (jako např. je grupa permutací daného počtu předmětů nebo grupa matic s reálnými koeficienty daného stupně), nýbrž formuluje svoje poučky tak, aby platily pro všechny konkrétní, vzájemně isomorfní grupy současně, a to nejen pro ty, které již známe, nýbrž i pro všechny, s nimiž bychom se kdy mohli setkat. Čili abstraktní teorie grup má za své vlastní předměty celé typy vzájemně isomorfních grup (typy isomorfie, nebo jak se méně vhodně, ale stručněji říká, a b s t r a k t n í g r u p y), nikoli jednotlivé grupy samotné. Abstrahuje se tu tedy jak od (početních) způsobů, jakými je v té které grupě vytváření součinu z jeho činitelů zavedeno (ať již si vzpomeneme např. na násobení permutací nebo násobení matic), tak i od samotného druhu prvků grupy (od toho, zda jsou to permutace nebo pohyby nebo i čísla.) Takováto abstrakce je právě nutná k tomu, abychom, přenášejíce vlastnosti a zákonitosti z jedné grupy na druhou (s touto isomorfní), nepřenesli případně omylem nějakou specifickou vlastnost, založenou v povaze prvků nebo ve způsobu provádění násobení jedné konkrétní grupy, tedy vlastnost či vztah, které do vlastní teorie grup nepatří.

Pro typ isomorfismu grup je tedy podstatný 1. počet jejich prvků (v příslušném zobecnění i na tzv. nekonečný počet čili mohutnost množství prvků grupy), 2. okolnost, že ke každým dvěma prvkům grupy v daném pořadí je (nějak) stanoven jednoznačně jejich součin podrobený axiomům (1) až (4), lhostejno, jakým způsobem se násobení uskuteční.

Smysl popsané abstrakce v teorii grup je dále v tom, že abstraktní teorie grup, nepřestávajíc na abstraktním zevšeobecňování vlastností známých konkrétních grup systematicky hledá všechny typy grup, které jenom (popř. ještě za dodatečných předpokladů) jsou vůbec logicky možné, i když předem příklady takových grup známy nejsou; naopak, klade si, mimo jiné, za úkol takové příklady uměle hledat, sestrojovat je. Užitečnost takového počínání pro seznání grupové zákonitosti je právě taková, jako v přírodních vědách pokusné sestrojování přírodních dějů za umělých podmínek, které sice (popřípadě zatím) v přírodě nebyly nalezeny, ale mají pro poznání dané přírodní zákonitosti důležitý význam teoretický (jehož praktický dosah se musí dříve či později objevit).

Cvičení

1. Dokažte, že multiplikativní grupa všech komplexních čísel $\neq 0$ (tvaru $x + iy$) je isomorfní multiplikativní grupou matic tvaru

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \quad (x,\ y \text{ reálná čísla, } xy \neq 0)$$

2. Ukažte, že grupa zákrytových pohybů nekonečného pásu na obr. 3 je isomorfní s aditivní grupou celých čísel. (Udejte přesně isomorfní zobrazení.)

3. Ukažte, že grupa zákrytových otočení pravidelného n-úhelníka a multiplikativní grupa všech n-tých odmocnin z 1 jsou isomorfní grupy (cyklické grupy řádu n). (Udejte přesně isomorfní zobrazení.)

4. *Ukažte, že Booleova grupa ze 3. kap. a grupa ze cvič. 8* (za touž kap.) jsou isomorfní grupy (při stejném počtu daných předmětů). (Isomorfní zobrazení přiřazuje podmnožině předmětů jakožto prvku jedné grupy skupinu všech zbývajících předmětů (její doplněk) jakožto prvek druhé grupy.)