19. Základní pojmy o grupách

In: Otakar Borůvka (author): Základy teorie grupoidů a grup. (Czech). Praha: Nakladatelství Československé akademie věd, 1962. pp. 147--155.

Persistent URL: http://dml.cz/dmlcz/401446

III. GRUPY

19. Základní pojmy o grupách

19.1. Axiomy grupy

Předmětem našich dalších úvah jsou grupy. Podle definice grupy, kterou jsme uvedli již v odst. **18.5.**1, rozumíme grupou pologrupu s dělením.

Podrobněji řečeno:

Libovolný grupoid $\mathfrak{G}$ se nazývá *grupa*, když jsou splněny tyto tzv. *axiomy grupy*:

1. *Pro libovolné prvky* $a, b, c \in \mathfrak{G}$ *platí rovnost* $a(bc) = (ab)c$.

2. *K libovolným prvkům* $a, b \in \mathfrak{G}$ *existuje prvek* $x \in \mathfrak{G}$ *splňující rovnici* $ax = b$ *a prvek* $y \in \mathfrak{G}$ *splňující rovnici* $ya = b$.

Těmto axiomům stručně říkáme *asociativní zákon* a *axiom o dělení*. V odst. **18.5.**1 jsme dále ukázali, že důsledkem těchto axiomů je jednak existence jednotky v $\mathfrak{G}$, tj. prvku $\underline{1} \in \mathfrak{G}$ vyznačujícího se tím, že pro $a \in \mathfrak{G}$ platí rovnosti $\underline{1}a = a\underline{1} = a$ a jednak jednoznačnost dělení v $\mathfrak{G}$. *Každá grupa je tedy quasigrupou s jednotkou* (*lupou*).

V dalším výkladu značí písmeno $\mathfrak{G}$ libovolnou grupu.

19.2. Inverzní prvky Inverze

Protože $\mathfrak{G}$ je quasigrupa s jednotkou, existuje ke každému prvku $a \in \mathfrak{G}$ jediný prvek $x \in \mathfrak{G}$ takový, že $ax = \underline{1}$ a jediný prvek $y \in \mathfrak{G}$ takový, že $ya = \underline{1}$; přitom symbol $\underline{1}$ označuje (i všude nadále) jednotku grupy $\mathfrak{G}$.

Snadno ukážeme, že důsledkem asociativního zákona je rovnost obou prvků

x, y. Utvoříme-li totiž součin prvku y s prvkem ax $(= \underline{1})$, obdržíme $y(ax) = y\underline{1} = y$. Podle asociativního zákona je $y(ax) = (ya)x = \underline{1}x = x$, a skutečně vychází $x = y$.

Ke každému prvku $a \in \mathfrak{G}$ existuje tedy jediný prvek, který se označuje a^{-1}, té vlastnosti, že $aa^{-1} = a^{-1}a = \underline{1}$. Tento prvek se nazývá *inverzní prvek vzhledem k a.*

Podle této definice je tedy inverzní prvek vzhledem k prvku a jediné řešení rovnice $ax = \underline{1}$ o neznámém prvku x a současně jediné řešení rovnice $ya = \underline{1}$ o neznámém prvku y. Protože rovnici $a^{-1}x = \underline{1}$ vyhovuje prvek a, je a prvek inverzní vzhledem k a^{-1}, tj. $(a^{-1})^{-1} = a$. Pravíme také, že prvky a, a^{-1} jsou inverzní. Všimněme si, že prvek inverzní vzhledem k a může být opět prvek a, neboť je např. $\underline{1}^{-1} = \underline{1}$.

Na grupě $\mathfrak{G}$ máme tedy význačný rozklad, jehož prvky jsou jednak množiny skládající se vždy z jednoho prvku, který je sám k sobě inverzní, jednak množiny skládající se vždy z dvojice vzájemně inverzních prvků.

Např. v grupě $\mathfrak{Z}$ máme jednotku 0 a prvek inverzní vzhledem k libovolnému prvku a je $-a$. Zmíněný význačný rozklad grupy $\mathfrak{Z}$ je tento: $\{0\}, \{1, -1\}, \{2, -2\}, \ldots$

Nechť a, b značí libovolné prvky v $\mathfrak{G}$. Z rovnosti $aa^{-1} = \underline{1}$ a podle asociativního zákona máme $a(a^{-1}b) = (aa^{-1})b = \underline{1}b = b$ a odtud je patrné, že prvek $a^{-1}b$ je (jediné) řešení rovnice $ax = b$. Podobně zjistíme, že prvek ba^{-1} je (jediné) řešení rovnice $ya = b$. Dále se snadno přesvědčíme, že prvek inverzní vzhledem k součinu ab je $b^{-1}a^{-1}$. Za tím účelem stačí zjistit, že prvek $b^{-1}a^{-1}$ je řešením rovnice $(ab)x = \underline{1}$; tato skutečnost vyplývá z rovností $(ab)(b^{-1}a^{-1}) = a(bb^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(\underline{1}a^{-1}) = aa^{-1} = \underline{1}$.

Podobným postupem se odvodí i výsledek obecnější, totiž že *prvek inverzní vzhledem k součinovému prvku $a_1a_2 \ldots a_n$ libovolné n $(\geqq 2)$-členné posloupnosti prvků $a_1, a_2, \ldots, a_n \in \mathfrak{G}$ je prvek $a_n^{-1} \ldots a_2^{-1}a_1^{-1}$.*

K pojmu inverzního prvku připojme ještě tuto poznámku: Jak jsme viděli, je existence inverzního prvku vzhledem k libovolnému prvku důsledkem charakteristických vlastností grupy. Jestliže naopak v nějakém asociativním grupoidu $\mathfrak{G}$ s jednotkou $\underline{1}$ existuje ke každému prvku $a \in \mathfrak{G}$ prvek inverzní a^{-1}, tj. prvek splňující rovnosti $aa^{-1} = a^{-1}a = \underline{1}$, pak grupoid $\mathfrak{G}$ je quasigrupa, a tedy (protože je asociativní) grupa. V tom případě totiž existují ke každým dvěma prvkům a, $b \in \mathfrak{G}$ prvky x, $y \in \mathfrak{G}$, které vyhovují rovnicím $ax = b$, $ya = b$, a to $x = a^{-1}b$, $y = ba^{-1}$, a jak se snadno zjistí, jsou to jediné prvky mající tuto vlastnost.

Můžeme tedy říci, že *vlastnost existence inverzního prvku vzhledem ke každému prvku charakterizuje grupy mezi všemi asociativními grupoidy s jednotkou.*

Existence inverzních prvků v grupě $\mathfrak{G}$ umožňuje definovat jisté prosté zobrazení grupy $\mathfrak{G}$ na sebe, jemuž později přisoudíme význačnou úlohu. Definujeme je tím, že ke každému prvku $a \in \mathfrak{G}$ přiřadíme inverzní prvek $a^{-1} \in \mathfrak{G}$. Tím obdržíme prosté zobrazení grupy $\mathfrak{G}$ na sebe, tedy permutaci na grupě $\mathfrak{G}$. Tato permutace je grupou $\mathfrak{G}$ jednoznačně určena. Nazýváme ji *inverze grupy* $\mathfrak{G}$; označení $\boldsymbol{n}$. Vidíme, že inverze $\boldsymbol{n}$ je zobrazení involutorní (**6.7**).

19.3. Mocniny prvků

Nechť a značí libovolný prvek v $\mathfrak{G}$ a n libovolné přirozené číslo. Protože $\mathfrak{G}$ je asociativní grupoid, je jenom jeden prvek $\underbrace{aa \dots a}_{n}$. Tento prvek se nazývá *n-tá mocnina* prvku a a označuje se symbolem a^n. Pro $n = 1$ máme $a^1 = a$. Podobně prvek $\underbrace{a^{-1}a^{-1} \dots a^{-1}}_{n}$ nazýváme *–n-tá mocnina* prvku a a označujeme jej symbolem a^{-n}. Podle těchto definic platí tedy vzorce $a^{-n} = (a^{-1})^n$, $a^{-n} = (a^n)^{-1}$. Tím máme definovány kladné a záporné mocniny prvku a. Je účelné definovat také *nultou mocninu* a^0 prvku a, a to tím, že je to jednotka grupy $\mathfrak{G}$, takže $a^0 = \underline{1}$. Ke každému prvku $a \in \mathfrak{G}$ jsme tím přiřadili nekonečně mnoho mocnin prvku a:

$$\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots,$$

s mocniteli $\dots, -2, -1, 0, 1, 2, \dots$, přičemž ovšem některé z těchto prvků mohou být identické.

Pro mocniny libovolného prvku $a \in \mathfrak{G}$ platí tyto vzorce:

$$(1) \qquad a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn},$$

a to pro všechna celá čísla m, n.

Omezíme se na provedení důkazu prvního vzorce, abychom ušetřili místo, a přenecháváme čtenáři, aby si podobně ověřil i správnost vzorce druhého. Jestliže jedno nebo obě čísla m, n jsou 0, je náš vzorec zřejmě správný. Jestliže obě čísla m, n jsou kladná, máme $a^m a^n = \underbrace{(a \dots a)}_{m}\underbrace{(a \dots a)}_{n} = \underbrace{a \dots a}_{m+n} = a^{m+n}$. Náš vzorec je tedy opět správný. Jsou-li obě čísla m, n záporná, označíme $m' = -m$, $n' = -n$, takže m', n' značí kladná čísla a máme $a^m a^n = a^{-m'}a^{-n'} = \underbrace{(a^{-1} \dots a^{-1})}_{m'}\underbrace{(a^{-1} \dots a^{-1})}_{n'} =$ $= \underbrace{a^{-1} \dots a^{-1}}_{m'+n'} = a^{-(m'+n')} = a^{-m'-n'} = a^{m+n}$. Zbývá tedy ještě uvažovat o případě, že jedno z obou čísel m, n je kladné a druhé záporné. Je-li číslo m kladné a n záporné, označíme $n' = -n$, takže m, n' značí kladná čísla, a máme

$$a^m a^n = a^m a^{-n'} = \underbrace{(a \dots a)}_{m}\underbrace{(a^{-1} \dots a^{-1})}_{n'} =$$

$$= \begin{cases} \overbrace{a \dots a}^{m-n'} = a^{m-n'} = a^{m+n}, \text{ když } m > n'; \\ \underline{1} = a^0 = a^{m-n'} = a^{m+n}, \text{ když } m = n'; \\ \underbrace{a^{-1} \dots a^{-1}}_{n'-m} = a^{-(n'-m)} = a^{m+n}, \text{ když } m < n'. \end{cases}$$

Je-li konečné číslo m záporné a n kladné, označíme $m' = -m$, takže m', n značí kladná čísla, a vidíme, že platí tyto rovnosti: $a^m a^n = a^{-m'}a^n = (a^{-1})^{m'}[(a^{-1})^{-1}]^n =$

$= (a^{-1})^{m'}(a^{-1})^{-n} = (a^{-1})^{m'-n} = a^{-(m'-n)} = a^{-m'+n} = a^{m+n}$, a tím je důkaz proveden.

Značí-li např. a libovolný prvek v grupě $\mathfrak{Z}$, pak jednotlivé mocniny prvku a jsou: $\ldots, -2a, -a, 0, a, 2a, \ldots$; zejména pro $a = 1$ máme: $\ldots, -2, -1, 0, 1, 2, \ldots$ a vidíme, že množina všech mocnin prvku $1 \in \mathfrak{Z}$ je celé pole grupy $\mathfrak{Z}$.

19.4. Podgrupa a nadgrupa

1. Definice. Nechť $\mathfrak{A}$ značí libovolný podgrupoid v $\mathfrak{G}$. Podle **12.9.**8 je $\mathfrak{A}$ grupoid asociativní. Když $\mathfrak{A}$ je grupa, tj. když je nadto quasigrupou, pak pravíme, že $\mathfrak{A}$ je *podgrupa* v $\mathfrak{G}$ nebo že $\mathfrak{G}$ je *nadgrupa na* $\mathfrak{A}$, a píšeme jako obvykle: $\mathfrak{A} \subset \mathfrak{G}$ nebo $\mathfrak{G} \supset \mathfrak{A}$.

Podgrupu $\mathfrak{A}$ v $\mathfrak{G}$ nazýváme *vlastní*, je-li vlastním podgrupoidem v $\mathfrak{G}$, je-li tedy pole A podgrupy $\mathfrak{A}$ vlastní podmnožinou v $\mathfrak{G}$. V tom případě pravíme, že $\mathfrak{G}$ je vlastní nadgrupa na $\mathfrak{A}$. V grupě $\mathfrak{G}$ existují alespoň dvě podgrupy, a to tzv. *největší podgrupa*, která je totožná s grupou $\mathfrak{G}$, a tzv. *nejmenší podgrupa* $\mathfrak{E}$, jejíž pole se skládá z jediného prvku $\underline{1}$. Jsou to tzv. *krajní* neboli *extrémní podgrupy v* $\mathfrak{G}$.

O libovolných grupách $\mathfrak{A}, \mathfrak{B}, \mathfrak{G}$ platí zřejmě tyto výroky:

a) *Když* $\mathfrak{B}$ *je podgrupou v* $\mathfrak{A}$ *a* $\mathfrak{A}$ *podgrupou v* $\mathfrak{G}$, *pak* $\mathfrak{B}$ *je podgrupou v* $\mathfrak{G}$.

b) *Když* $\mathfrak{A}, \mathfrak{B}$ *jsou podgrupy v* $\mathfrak{G}$ *a jejich pole* A, B *jsou ve vztahu* $B \subset A$, *je* $\mathfrak{B}$ *pogrupou v* $\mathfrak{A}$.

2. *Charakteristická vlastnost podgrup.* Uvažujme o libovolné podgrupě $\mathfrak{A}$ v $\mathfrak{G}$. Označme písmenem j jednotku podgrupy $\mathfrak{A}$. Je nějaký vztah mezi jednotkou $\underline{1}$ grupy $\mathfrak{G}$ a jednotkou j podgrupy $\mathfrak{A}$? Podle definice jednotky j podgrupy $\mathfrak{A}$ platí pro libovolný prvek $a \in \mathfrak{A}$ rovnost $a = ja$ a současně ovšem platí $a = \underline{1}a$. Z toho vzhledem k **19.1.**2 vychází rovnost: $j = \underline{1}$. Vidíme, že *jednotka grupy* $\mathfrak{G}$ *je současně jednotkou podgrupy* $\mathfrak{A}$. Odtud plyne dále, že inverzní prvek v podgrupě $\mathfrak{A}$ vzhledem k libovolnému prvku $a \in \mathfrak{A}$ je prvek a^{-1}, tj. inverzní prvek vzhledem k a v grupě $\mathfrak{G}$.

Když tedy libovolný podgrupoid v $\mathfrak{G}$ *je podgrupou v* $\mathfrak{G}$, *pak obsahuje jednotku grupy* $\mathfrak{G}$ *a s každým svým prvkem a současně prvek* a^{-1}, *a naopak, když nějaký podgrupoid v* $\mathfrak{G}$ *tyto vlastnosti má, pak je podgrupou v* $\mathfrak{G}$.

Pomocí tohoto výsledku snadno odvodíme jistou vlastnost podgrup, která je charakterizuje mezi podgrupoidy. Podgrupa $\mathfrak{A}$ obsahuje, jak víme, s každým svým prvkem současně prvek vzhledem k němu inverzní, a tedy, když obsahuje nějaké prvky a, b, pak obsahuje i prvek ab^{-1}. Když naopak o nějakém podgrupoidu v $\mathfrak{G}$ platí, že současně s každými dvěma prvky a, b obsahuje i prvek ab^{-1}, pak zejména (pro $b = a$) obsahuje jednotku $\underline{1}$ grupy $\mathfrak{G}$ a (pro $a = \underline{1}$) rovněž prvek b^{-1}, a je tedy podgrupou v $\mathfrak{G}$, jak vyplývá z hořejšího výsledku.

Podgrupy v $\mathfrak{G}$ *jsou* tedy *mezi všemi podgrupoidy v* $\mathfrak{G}$ *charakterizovány vlastností, že s každými svými dvěma prvky a, b obsahují i prvek* ab^{-1}.

Ostatně si všimněme, že libovolná neprázdná podmnožina $A \subset \mathfrak{G}$, která s každými svými dvěma prvky a, b obsahuje i prvek ab^{-1}, je grupoidní, a tedy je polem podgrupy v $\mathfrak{G}$. Podobnou úvahu jako o prvku ab^{-1} můžeme provést i o prvku $a^{-1}b$.

3. Příklad. Uvažujme opět o grupě $\mathfrak{Z}$. Nechť $\mathfrak{A}$ značí libovolnou podgrupu v $\mathfrak{Z}$. Protože $\mathfrak{A}$ obsahuje s každým svým prvkem b současně inverzní prvek $-b$, skládá se $\mathfrak{A}$ buď jenom z prvku 0 nebo obsahuje kromě záporných také kladná čísla. V prvním případě je $\mathfrak{A}$ nejmenší podgrupa v $\mathfrak{Z}$. V druhém případě označme písmenem a nejmenší kladné číslo, které je prvkem podgrupy $\mathfrak{A}$. Podgrupa $\mathfrak{A}$ ovšem obsahuje všechny mocniny prvku a, tj. celé násobky čísla a:

$$\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots$$

Nechť b značí libovolný prvek v $\mathfrak{A}$. Jak víme, existují pak celá čísla q, r taková, že $b = qa + r$, $0 \leqq r \leqq a - 1$. Protože podgrupa $\mathfrak{A}$ obsahuje čísla b, qa, obsahuje i číslo $b - qa = r$, a protože neobsahuje kladných čísel menších než a, je $r = 0$. Vychází tedy $b = qa$ a vidíme, že podgrupa $\mathfrak{A}$ nemá jiných prvků než všechny celé násobky čísla a. Můžeme tedy říci, že v obou případech se podgrupa $\mathfrak{A}$ skládá ze všech celých násobků jistého nezáporného čísla. Naopak je však zřejmé, že množina všech celých násobků libovolného nezáporného čísla spolu s příslušným násobením je podgrupou v $\mathfrak{Z}$.

Máme tedy výsledek, že se *všechny podgrupy v* $\mathfrak{Z}$ *skládají ze všech celých násobků jednotlivých nezáporných čísel.* Všimněme si, že všechny *kladné* násobky libovolného *kladného* čísla tvoří podgrupoid, avšak nikoli podgrupu v $\mathfrak{Z}$. V grupách mohou tedy existovat podgrupoidy, aniž jsou podgrupami.

4. Poznámka. Třebaže se nám podařilo určit všechny podgrupy v grupě $\mathfrak{Z}$, bylo by neskromné očekávat podobný úspěch u jiných grup, jejichž násobení je složitější. Nalézt pravidlo, podle něhož by bylo možno určit všechny podgrupy v každé grupě, je úloha posud nerozřešená.

19.5. Průnik a součin podgrup

1. *Průnik podgrup.* Uvažujme nyní o dvou libovolných podgrupách $\mathfrak{A}, \mathfrak{B} \subset \mathfrak{G}$. Protože obě podgrupy obsahují prvek $\underline{1} \in \mathfrak{G}$, existuje, jak víme z úvah o grupoidech, jejich průnik $\mathfrak{A} \cap \mathfrak{B}$ a snadno ukážeme, že tento průnik je opět podgrupou v $\mathfrak{G}$. Je zřejmé, že $\mathfrak{A} \cap \mathfrak{B}$ je asociativní podgrupoid v $\mathfrak{G}$ s jednotkou $\underline{1}$, a stačí tedy zjistit, že obsahuje s každým svým prvkem a současně inverzní prvek a^{-1}. Když $a \in \mathfrak{A} \cap \mathfrak{B}$, pak platí současně $a \in \mathfrak{A}$, $a \in \mathfrak{B}$, a protože $\mathfrak{A}, \mathfrak{B}$ jsou podgrupy, plyne odtud $a^{-1} \in \mathfrak{A}$, $a^{-1} \in \mathfrak{B}$, takže máme $a^{-1} \in \mathfrak{A} \cap \mathfrak{B}$, a tím je důkaz proveden. Můžeme tedy říci, že *každé dvě podgrupy v* $\mathfrak{G}$ *mají průnik a tento průnik je podgrupou v* $\mathfrak{G}$. Současně

vidíme, že je podgrupou v každé z těchto podgrup. Tento výsledek se dá snadno rozšířit na libovolný počet podgrup v $\mathfrak{G}$.

2. *Součin podgrup.* Předpokládejme nyní, že *podgrupy* $\mathfrak{A}, \mathfrak{B}$ *jsou vzájemně zaměnitelné*, tj. že platí rovnost $AB = BA$, kde A (B) značí pole podgrupy $\mathfrak{A}$ ($\mathfrak{B}$). Za tohoto předpokladu existuje součin $\mathfrak{AB}$ podgrup $\mathfrak{A}, \mathfrak{B}$ (**12.9.9**) a opět snadno zjistíme, že je podgrupou v $\mathfrak{G}$. Skutečně, je asociativní a jak plyne ze vztahů $\underline{1} \in \mathfrak{A}$, $\underline{1} \in \mathfrak{B}$, $\underline{1} = \underline{1}\,\underline{1} \in \mathfrak{AB}$, obsahuje jednotku $\underline{1}$ grupy $\mathfrak{G}$. Dále je každý prvek v $\mathfrak{AB}$ součin ab jistého prvku $a \in \mathfrak{A}$ s jistým prvkem $b \in \mathfrak{B}$; prvek inverzní vzhledem k ab je $b^{-1}a^{-1}$ a z rovnosti $BA = AB$ vyplývá, že je v podgrupoidu $\mathfrak{AB}$, a tím je ukázáno, že $\mathfrak{AB}$ *je podgrupa* v $\mathfrak{G}$. Všimněme si, že platí také **19.7.6**. Dále je $\mathfrak{AB} \supset \mathfrak{A}$, $\mathfrak{AB} \supset \mathfrak{B}$ a zejména $\mathfrak{A}^2$, tj. součin $\mathfrak{AA}$, je podgrupa $\mathfrak{A}$ v $\mathfrak{G}$. Rovněž je důležité, abychom si uvědomili, že *v každé abelovské grupě* (jsou každé dvě podgrupy vzájemně zaměnitelné a tedy) *existuje součin každých dvou podgrup a je opět podgrupou.*

3. Příklad. V grupě $\mathfrak{Z}$ mají každé dvě podgrupy průnik i součin. Určeme např. průnik a součin podgrup $\mathfrak{A}, \mathfrak{B}$, jejichž pole jsou

$$\{\ldots, -8, -4, 0, 4, 8, \ldots\},$$
$$\{\ldots, -14, -7, 0, 7, 14, \ldots\}.$$

Každé číslo v průniku $\mathfrak{A} \cap \mathfrak{B}$ je současně celým násobkem čísla 4 i čísla 7 a tedy je celým násobkem nejmenšího společného násobku čísel 4, 7, tj. čísla 28. Průnik $\mathfrak{A} \cap \mathfrak{B}$ se tedy skládá z čísel

$$\ldots, -56, -28, 0, 28, 56, \ldots$$

Pokud jde o součin $\mathfrak{AB}$, obsahuje zřejmě číslo $4 + 7 = 11$. Dále $\mathfrak{AB}$, jakožto podgrupa v $\mathfrak{Z}$, se skládá ze všech celých násobků jistého celého nezáporného čísla a (**19.4.3**). Tedy 11 je celý násobek čísla a a tedy $a = 1$ nebo $a = 11$, neboť 11 je prvočíslo. Protože $\mathfrak{AB}$ zřejmě obsahuje také např. číslo 4, je $a = 1$, protože 4 není celým násobkem čísla 11. Vychází tedy, že se podgrupa $\mathfrak{AB}$ skládá ze všech celých násobků čísla 1, takže je totožná s grupou $\mathfrak{Z}$.

19.6. Poznámky o multiplikačních tabulkách konečných grup

1. *Charakteristické vlastnosti tabulek.* Nechť $\mathfrak{G}$ značí libovolnou *konečnou* grupu a uvažujme o příslušné multiplikační tabulce. Protože v grupě $\mathfrak{G}$ platí pravidla o krácení (**18.3.1**), vyskytnou se v multiplikační tabulce v každém řádku a v každém sloupci napravo od svislého a pod vodorovným záhlavím symboly všech prvků grupy $\mathfrak{G}$. Vyskytne se tam tedy zejména $\underline{1}$ a se symbolem každého prvku současně symbol prvku inverzního. Zřejmě jsou tyto vlastnosti pro multiplikační tabulku ko-

nečné grupy charakteristické, jestliže současně platí asociativní zákon. Např. multiplikační tabulky pro grupy řádu 1, 2, 3, jejichž prvky označíme $\underline{1}$, a, b, jsou tyto:

	$\underline{1}$
$\underline{1}$	$\underline{1}$

	$\underline{1}$	a
$\underline{1}$	$\underline{1}$	a
a	a	$\underline{1}$

	$\underline{1}$	a	b
$\underline{1}$	$\underline{1}$	a	b
a	a	b	$\underline{1}$
b	b	$\underline{1}$	a

Pro grupy řádu 4, jejichž prvky jsme označili $\underline{1}$, a, b, c jsou možné dvě různé multiplikační tabulky, a to:

	$\underline{1}$	a	b	c
$\underline{1}$	$\underline{1}$	a	b	c
a	a	$\underline{1}$	c	b
b	b	c	a	$\underline{1}$
c	c	b	$\underline{1}$	a

	$\underline{1}$	a	b	c
$\underline{1}$	$\underline{1}$	a	b	c
a	a	$\underline{1}$	c	b
b	b	c	$\underline{1}$	a
c	c	b	a	$\underline{1}$

Tyto multiplikační tabulky se najdou tím způsobem, že se o součinu každého prvku s každým stejným nebo různým prvkem uváží (a to se zřetelem k okolnosti, že se v multiplikační tabulce vyskytnou v každém řádku a v každém sloupci napravo od svislého a pod vodorovným záhlavím symboly všech prvků grupy a každý jenom jednou), který prvek to může být, a na konec se verifikuje, že je splněn asociativní zákon. Avšak tento postup je bez dalších znalostí o grupách zdlouhavý. Třebaže jsou známa pravidla, pomocí kterých lze určit multiplikační tabulky všech grup jistých řádů, zůstává hlavním dosud neřešeným problémem výčet všech konečných grup libovolného řádu.

2. *Normální tabulky.* Každou multiplikační tabulku grupy libovolného řádu můžeme především zjednodušit tím, že vynecháme obě záhlaví. Do prvního řádku napíšeme pak onen řádek multiplikační tabulky, který má na prvním místě symbol $\underline{1}$; do druhého onen řádek, který má symbol $\underline{1}$ na druhém místě, atd., a do posledního řádku napíšeme onen, v němž symbol $\underline{1}$ je na místě posledním. Multiplikační tabulka takto upravená se nazývá *normální.* Např. normální multiplikační tabulky grup řádů 1, 2, 3, 4, jejichž prvky jsme označili $\underline{1}$, a, b, c, jsou tyto:

$\underline{1}$

$\underline{1}$	a
a	$\underline{1}$

$\underline{1}$	a	b
b	$\underline{1}$	a
a	b	$\underline{1}$

$\underline{1}$	a	b	c
a	$\underline{1}$	c	b
c	b	$\underline{1}$	a
b	c	a	$\underline{1}$

$\underline{1}$	a	b	c
a	$\underline{1}$	c	b
b	c	$\underline{1}$	a
c	b	a	$\underline{1}$

3. *Obdélníkové pravidlo.* V každé normální multiplikační tabulce je na každém místě v hlavní úhlopříčně symbol jednotky. Uvažujme o normální multiplikační

tabulce nějaké konečné grupy. Symbol součinu libovolného prvku a s libovolným prvkem b je ovšem na průsečíku řádku začínajícího písmenem a a sloupce začínajícího písmenem b. Jsou-li a, b souměrně položeny vzhledem k hlavní úhlopříčně, máme $ab = \underline{1}$, a odtud vychází, že prvky a, b jsou inverzní. Vidíme tedy, že v prvním řádku naší tabulky jsou zleva doprava napsány symboly inverzních prvků vzhledem k prvkům v prvním sloupci, tak jak jdou po sobě shora dolů.

Uvažujme o libovolných třech prvcích x, y, z, jejichž symboly spolu s $\underline{1}$ tvoří v naší tabulce vrcholy obdélníka, a to tak, že např. x je v témž sloupci a y v témž řádku jako $\underline{1}$, a tedy z je v témž řádku jako x a v témž sloupci jako y. Nechť a, b jsou písmena, jimiž začínají řádky obsahující $\underline{1}$, x, a podobně nechť c, d jsou písmena, jimiž začínají sloupce obsahující $\underline{1}$, y. Pak tedy např. x je na průsečíku řádku začínajícího písmenem b a sloupce začínajícího písmenem c, takže $x = bc$, a podobně odvodíme i další rovnosti: $y = ad$, $z = bd$, $\underline{1} = ac$. Z poslední rovnosti vidíme, že prvky a, c jsou inverzní, takže současně platí vztah $ca = \underline{1}$. Máme tedy: $xy = (bc)(ad) = b(ca)d = b\underline{1}d = bd = z$, takže $xy = z$ a tato rovnost vyjadřuje tzv. *obdélníkové pravidlo*:

Když v normální multiplikační tabulce symboly některých čtyř prvků, z nichž jeden je $\underline{1}$, *tvoří vrcholy obdélníka, pak prvek ležící na vrcholu protějším k prvku* $\underline{1}$ *je součinem prvku, nacházejícího se na vrcholu v témž sloupci jako* $\underline{1}$ *s prvkem položeným na vrcholu zbývajícím.*

Např. v normální multiplikační tabulce grupy řádu 4, která je v odst. **19.6.**2 napsána poslední, tvoří prvky $\underline{1}$, c v druhém řádku spolu s prvky b, a ve čtvrtém řádku vrcholy obdélníka. Podle obdélníkového pravidla je tedy $bc = a$ a skutečně na průsečíku řádku začínajícího písmenem b a sloupce začínajícího písmenem c je prvek a.

19.7. Cvičení

1. Grupoid, jehož pole je množina všech euklidovských pohybů na přímce $\boldsymbol{f}[a]$, $\boldsymbol{g}[a]$ nebo v rovině $\boldsymbol{f}[\alpha; a, b]$, $\boldsymbol{g}[\alpha; a, b]$ a násobení je definováno skládáním pohybů (**11.5.**1), je grupa, tzv. *úplná grupa euklidovských pohybů na přímce* nebo *v rovině*. V úplné grupě euklidovských pohybů na přímce nebo v rovině tvoří všechny euklidovské pohyby $\boldsymbol{f}[a]$ nebo $\boldsymbol{f}[\alpha; a, b]$ podgrupu. Uveďte některé další podgrupy v těchto grupách.

Poznámka. Např. euklidovská geometrie v rovině popisuje, jak víme, vlastnosti útvarů složených z bodů a přímek, jako jsou různé konfigurace bodů a přímek, trojúhelníky, kuželosečky atp. Tato geometrie je podložena úplnou grupou euklidovských pohybů v rovině v tom smyslu, že se dva útvary považují za shodné, když se dají na sebe zobrazit některým euklidovským pohybem.

2. Grupoid, jehož pole je množina $2n$ permutací vrcholů pravidelného n-úhelníka v rovině ($n \geqq 3$), které jsme popsali ve cvič. **8.8.**4, a násobení je definováno skládáním permutací, je grupa zvaná *diedrická permutační grupa řádu* $2n$. Tato grupa obsahuje kromě nejmenší podgrupy další vlastní podgrupy: podgrupu řádu n skládající se ze všech prvků odpovídajících otočením vrcholů pravidelného n-úhelníka okolo jeho středu; n podgrup řádu 2 skládajících se vždy z identické

permutace a z permutace odpovídající přiřazení k vrcholům pravidelného n-úhelníka vrcholů souměrně položených vzhledem k některé ose souměrnosti.

3. Počet prvků, které jsou samy k sobě inverzní, je v každé konečné grupě sudého (lichého) řádu suchý (lichý).

4. V každé konečné grupě je každý podgrupoid podgrupou (srv. **18.7.**7).

5. Inverze každé abelovské grupy představuje automorfizmus této grupy.

6. V každé abelovské grupě tvoří všechny prvky, které jsou samy k sobě inverzní, podgrupu.

7. V každé abelovské grupě $\mathfrak{G}$ platí pro každé dva prvky $a, b \in \mathfrak{G}$ a libovolné celé číslo n vzorec: $(ab)^n = a^n b^n$. Uveďte příklad, že v neabelovských grupách tento vzorec vždycky neplatí.

8. Když $\mathfrak{A}$, $\mathfrak{B}$ jsou podgrupy v grupě $\mathfrak{G}$ a součin jejich polí AB je polem podgrupy v $\mathfrak{G}$, pak $\mathfrak{A}$, $\mathfrak{B}$ jsou vzájemně zaměnitelné.

9. Když $\mathfrak{A} \subset \mathfrak{B}$ jsou podgrupy v grupě $\mathfrak{G}$ pak $\mathfrak{A}\mathfrak{B} = \mathfrak{B}\mathfrak{A} = \mathfrak{B}$, $\mathfrak{A} \cap \mathfrak{B} = \mathfrak{A}$. Když také $\mathfrak{E}$ je podgrupa v $\mathfrak{G}$ a je zaměnitelná s $\mathfrak{A}$, pak i podgrupa $\mathfrak{E} \cap \mathfrak{B}$ je zaměnitelná s $\mathfrak{A}$.

10. Každá grupa má centrum.

11. Budiž $p \in \mathfrak{G}$ libovolný prvek v grupě $\mathfrak{G}$. Definujeme v $\mathfrak{G}$ nové násobení, v němž součiny vyjádříme znaménkem $\circ$, tímto pravidlem: Pro libovolné prvky $x, y \in \mathfrak{G}$ je součin $x \circ y$ dán vzorcem $x \circ y = xp^{-1}y$. Pak platí: a) grupoid $\mathring{\mathfrak{G}}$, jehož polem je pole G grupy $\mathfrak{G}$ a násobení je definováno uvedeným způsobem, představuje grupu; b) jednotkou grupy $\mathring{\mathfrak{G}}$ je prvek p, prvek inverzní k libovolnému bodu $x \in \mathring{\mathfrak{G}}$ je $px^{-1}p$. — Poznámka. Grupu $\mathring{\mathfrak{G}}$ budeme v dalším výkladu nazývat: *(p)-grupa přidružená ke grupě* $\mathfrak{G}$.