

Úvod do theorie grup [2. rozšířené vydání]

11. Základní pojmy o grupách

In: Otakar Borůvka (author): Úvod do theorie grup [2. rozšířené vydání]. (Czech). Praha: Přírodovědecké vydavatelství, 1952. pp. 102--111.

Persistent URL: <http://dml.cz/dmlcz/401417>

Terms of use:

© Přírodovědecké vydavatelství

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://project.dml.cz>

III. GRUPY.

11. ZÁKLADNÍ POJMY O GRUPÁCH.

11.1. Axiomy grupy.

Předmětem našich dalších úvah jsou grupy. Podle definice grupy, kterou jsme uvedli již v odst. 10.5, rozumíme grupou asociativní quasigrupu. Podrobněji řečeno:

Libovolný grupoid \mathfrak{G} se nazývá grupa, když jsou splněny tyto t. zv. 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 jediný prvek $x \in \mathfrak{G}$ splňující rovnici $ax = b$ a jediný prvek $y \in \mathfrak{G}$ splňující rovnici $ya = b$.*

Tyto axiomy označujeme stručně jako *asociativní zákon* a *axiom o jednoznačném dělení*. V odst. 10.5 jsme dále ukázali, že důsledkem těchto axiomů jest existence jednotky v \mathfrak{G} , t. j. prvku $\underline{1} \in \mathfrak{G}$ vyznačujícího se tím, že pro $a \in \mathfrak{G}$ platí rovnosti $\underline{1}a = a\underline{1} = a$. *Každá grupa má tedy jednotku.*

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

11.2. Inversní prvky.

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 v dalším) 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 inversní prvek vzhledem k a . Podle této definice je tedy inversní prvek vzhledem k 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 , jest a prvek inversní vzhledem k a^{-1} ,

t. j. $(a^{-1})^{-1} = a$. Pravíme také, že prvky a, a^{-1} jsou inverzní. Všimněme si, že prvek inverzní vzhledem k a může být opět prvek a , neboť jest na př. $\underline{1}^{-1} = \underline{1}$.

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 páru vzájemně inverzních prvků.

Na př. 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: $\{0\}, \{1, -1\}, \{2, -2\}, \dots$

Nechť a, b značí libovolné prvky v \mathfrak{G} . Z rovnosti $aa^{-1} = \underline{1}$ a v důsledku asociativního zákona máme $a(a^{-1}b) = (aa^{-1})b = \underline{1}b = b$ a odtud je patrné, že prvek $a^{-1}b$ jest (jediné) řešení rovnice $ax = b$. Podobně zjistíme, že prvek ba^{-1} jest (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 zjistiti, 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 součinu $a_1a_2 \dots a_n$ libovolných n (≥ 2) prvků $a_1, a_2, \dots, a_n \in \mathfrak{G}$ je prvek $a_n^{-1} \dots a_2^{-1}a_1^{-1}$.*

K pojmu inverzního prvku připojme ještě tuto poznámku: Jak jsme viděli, jest 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} , t. j. prvek splňující rovnosti $aa^{-1} = a^{-1}a = \underline{1}$, pak grupoid \mathfrak{G} je quasigrupa, a tedy (protože jest 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 charakterisuje grupy mezi všemi asociativními grupoidy s jednotkou.*

11.3. Mocniny prvků.

Nechť a značí libovolný prvek v \mathfrak{G} a n libovolné přirozené číslo.

Protože \mathcal{G} je asociativní grupoid, jest jenom jeden prvek $\underbrace{aa \dots a}_n$.

Tento prvek se nazývá *n-tá mocnina* prvku a a označuje se symbolem a^n . 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 \mathcal{G} , takže $a^0 = \underline{1}$. Ke každému prvku $a \in \mathcal{G}$ jsme tím přiřadili nekonečně mnoho mocnin prvku a :

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

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

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

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

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 $a^m a^n = \underbrace{(a \dots a)}_m \cdot \underbrace{(a \dots a)}_n = \underbrace{a \dots a}_{m+n} = a^{m+n}$. 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. Jestliže číslo m je kladné a n záporné, označíme $n' = -n$, takže m, n' značí kladná čísla, a máme

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

Jestliže konečně číslo m je 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 na př. a libovolný prvek v grupě \mathfrak{G} , pak jednotlivé mocniny prvku a jsou: $\dots, -2a, -a, 0, a, 2a, \dots$; zejména pro $a = 1$ máme: $\dots, -2, -1, 0, 1, 2, \dots$ a vidíme, že množina všech mocnin prvku $1 \in \mathfrak{G}$ je celé pole grupy \mathfrak{G} .

11.4. Podgrupa a nadgrupa.

11.4.1. Definice. Necht \mathfrak{A} značí libovolný podgrupoid v \mathfrak{G} . Podle cvič. 6.9.7 jest \mathfrak{A} grupoid asociativní. Když \mathfrak{A} je grupa, t. j. když je quasigrupa, 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 t. zv. *největší podgrupa*, která je totožná s grupou \mathfrak{G} , a t. zv. *nejmenší podgrupa* \mathfrak{E} , jejíž pole se skládá z jediného prvku $\underline{1}$.

11.4.2. 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 $a = ja$. Utvoříme-li součin prvku a s prvkem a^{-1} , inverzním vzhledem k a v grupě \mathfrak{G} , obdržíme $\underline{1} = aa^{-1} = (ja)a^{-1} = j(aa^{-1}) = j\underline{1} = j$ a vidíme, že vychází rovnost $\underline{1} = j$, takže *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} , t. j. 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 charakterisuje 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} charakterisovány 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 $a^{-1}b$.

11.4.3. 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 jest \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 , t. j. celé násobky čísla a :

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

Nechť b značí libovolný prvek v \mathfrak{A} . Jak víme (viz pozn. pod čarou na str. 42), existují celá čísla q, r taková, že $b = qa + r$, $0 \leq r < a$. Protože podgrupa \mathfrak{A} obsahuje čísla b, qa , obsahuje i číslo $b - qa = r$, a protože neobsahuje kladných čísel menších než a , jest $r = 0$. 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 všechny podgrupy v \mathfrak{Z} se 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.

Další poznámka připínající se k hořejším úvahám je tato: Třebaže se

nám podařilo určití 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, jest úloha posud nerozřešená.*

11.5. Průnik a součin podgrup.

11.5.1. 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 jest 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}* . Tento výsledek se dá snadno rozšířit na libovolný počet podgrup v \mathfrak{G} .

11.5.2. Součin podgrup. Předpokládejme nyní, že podgrupy $\mathfrak{A}, \mathfrak{B}$ jsou zaměnitelné, t. j. že platí rovnost $AB = BA$, kde $A (B)$ značí pole podgrupy $\mathfrak{A} (\mathfrak{B})$. Za tohoto předpokladu existuje součin $\mathfrak{A}\mathfrak{B}$ podgrup $\mathfrak{A}, \mathfrak{B}$ (viz 6.9.8) a opět snadno zjistíme, že je podgrupou v \mathfrak{G} . Skutečně, je asociativní a jak plyne ze vztahů $\underline{1} \in \mathfrak{A}$, $\underline{1} \in \mathfrak{B}$, $\underline{1} = \underline{1}\underline{1} \in \mathfrak{A}\mathfrak{B}$, obsahuje jednotku $\underline{1}$ grupy \mathfrak{G} . Dále je každý prvek v $\mathfrak{A}\mathfrak{B}$ 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 $\mathfrak{A}\mathfrak{B}$, a tím jest ukázáno, že $\mathfrak{A}\mathfrak{B}$ je podgrupa v \mathfrak{G} . Všimněme si, že platí také 11.7.6. Dále je $\mathfrak{A}\mathfrak{B} \supset \mathfrak{A}$, $\mathfrak{A}\mathfrak{B} \supset \mathfrak{B}$ a zejména \mathfrak{A}^2 , t. j. součin $\mathfrak{A}\mathfrak{A}$, je podgrupa 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.*

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

$$\begin{aligned} &\{\dots, -8, -4, 0, 4, 8, \dots\}, \\ &\{\dots, -14, -7, 0, 7, 14, \dots\}. \end{aligned}$$

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, t. j. čísla 28. Průnik $\mathfrak{A} \cap \mathfrak{B}$ se tedy skládá z čísel

$$\dots, -56, -28, 0, 28, 56, \dots$$

Pokud jde o součin $\mathfrak{A}\mathfrak{B}$, obsahuje zřejmě číslo $4 + 7 = 11$ a $\mathfrak{A}\mathfrak{B}$, jakožto podgrupa v \mathfrak{Z} , se skládá ze všech celých násobků jistého celého nezáporného čísla a . Tedy 11 jest celý násobek čísla a a tedy $a = 1$ nebo $a = 11$, neboť 11 jest prvočíslo. Protože $\mathfrak{A}\mathfrak{B}$ zřejmě obsahuje také na př. číslo 4, jest $a = 1$, protože 4 není celým násobkem čísla 11. Vyčází tedy, že podgrupa $\mathfrak{A}\mathfrak{B}$ se skládá ze všech celých násobků čísla 1, takže je totožná s grupou \mathfrak{Z} .

11.6. Poznámky o multiplikačních tabulkách konečných grup.

11.6.1. Význačné vlastnosti tabulek. Necht \mathfrak{G} značí libovolnou konečnou grupu a uvažujme o příslušné multiplikační tabulce. Protože \mathfrak{G} je quasigrupa, 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} a tedy se tam vyskytne zejména $\underline{1}$ a se symbolem každého prvku současně symbol prvku inverzního. Na př. multiplikační tabulky pro grupy řádů 1, 2, 3, jejichž prvky označíme $\underline{1}, a, b$, jsou tyto:

$$\begin{array}{c|c} & \underline{1} \\ \hline \underline{1} & \underline{1} \end{array} \qquad \begin{array}{c|c} & \underline{1} a \\ \hline \underline{1} & \underline{1} a \\ a & a \underline{1} \end{array} \qquad \begin{array}{c|ccc} & \underline{1} & a & b \\ \hline \underline{1} & \underline{1} a & b \\ a & a b & \underline{1} \\ b & b \underline{1} & a \end{array}$$

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

$$\begin{array}{c|cccc} & \underline{1} & a & b & c \\ \hline \underline{1} & \underline{1} a & b & c \\ a & a \underline{1} & c & b \\ b & b c & a \underline{1} \\ c & c b & \underline{1} a \end{array} \qquad \begin{array}{c|cccc} & \underline{1} & a & b & c \\ \hline \underline{1} & \underline{1} a & b & c \\ a & a \underline{1} & c & b \\ b & b c & \underline{1} a \\ c & c b & a \underline{1} \end{array}$$

Tyto multiplikační tabulky se najdou tím způsobem, že se o součinu každého prvku s každým 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 zdoluhavý. 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.

11.6.2. 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*. Na př. normální multiplikační tabulky grup řádů 1, 2, 3, 4, jejichž prvky jsme označili 1, a , b , c , jsou tyto:

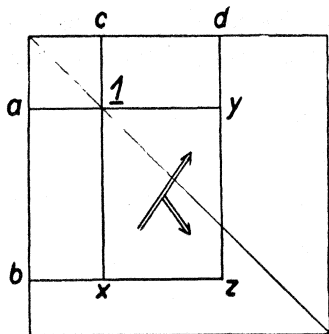
$$\begin{array}{ccc}
 \underline{1} & \underline{1} a & \underline{1} a b \\
 & a \underline{1} & b \underline{1} a \\
 & & a b \underline{1} \\
 \\
 \underline{1} a b c & & \underline{1} a b c \\
 a \underline{1} c b & & a \underline{1} c b \\
 c b \underline{1} a & & b c \underline{1} a \\
 b c a \underline{1} & & c b a \underline{1}
 \end{array}$$

11.6.3. 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 jest ovšem na průsečiku řádku začínajícího písmenem a a sloupce začínajícího písmenem b . Když a , b jsou 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 na-

psány 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 na př. x je v témže sloupci a y v témže řádku jako $\underline{1}$, a tedy z je v témže řádku jako x a v témže sloupci jako y . Necht a, b jsou písmena, jimiž začínají řádky obsahující $\underline{1}, x$, a podobně necht c, d jsou písmena, jimiž začínají sloupce obsahující $\underline{1}, y$. Pak tedy na př. 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 t. zv. *obdélníkové pravidlo*:

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



Obr. 12.

Na př. v normální multiplikační tabulce grupy řádu 4, která je v odst. 11.6.2 napsána jako 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 . Obdélníkové pravidlo je v pří-

padě, že $\underline{1}$ je na levém horním vrcholu obdélníka, znázorněno na obr. 12. Součin prvku x s prvkem y je prvek z .

11.7. Cvičení.

11.7.1. Grupoid, jehož pole je množina všech euklidovských pohybů na přímce $f[a]$, $g[a]$ nebo v rovině $f[\alpha; a, b]$, $g[\alpha; a, b]$ a násobení je definováno skládáním pohybů (viz cvič. 5.5.1), je grupa, t. zv. *úplná*

grupa euklidovských pohybů na přímce nebo v rovině. V úplné grupě euklidovských pohybů na přímce nebo v rovině tvoří všechny euklidovské pohyby $f[a]$ nebo $f[\alpha; a, b]$ podgrupu. Uveďte některé další podgrupy v těchto grupách! — *Poznámka.* Na př. euklidovská geometrie v rovině popisuje, jak víme z gymnasia, 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.

11.7.2. Grupoid, jehož pole je množina $2n$ permutací vrcholů pravidelného n -úhelníka v rovině ($n \geq 3$), které jsme popsali ve cvič. 4.6.4, a násobení je definováno skládáním permutací (viz cvič. 5.5.2), je grupa, t. zv. *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.

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

11.7.4. Když ke každému prvku a libovolné grupy \mathcal{G} přiřadíme inverzní prvek a^{-1} , obdržíme prosté zobrazení grupy \mathcal{G} na sebe; když grupa \mathcal{G} jest abelovská, pak toto zobrazení jest automorfismus.

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

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

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

11.7.8. Každá grupa má centrum.