11. Základní pojmy o grupách

In: Otakar Borůvka (author): Úvod do teorie grup. (Czech). Praha: Královská česká společnost nauk, 1944. pp. 51--58.

Persistent URL: http://dml.cz/dmlcz/401370

III. Grupy.

11. Základní pojmy o grupách.

Předmětem našich dalších úvah jsou grupy. Podle definice grupy, kterou jsme uvedli již v předcházejícím odst. 10., rozumíme grupou asociativní kvasigrupu. 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. 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.

Inversní prvky. Protože $\mathfrak{G}$ jest kvasigrupa 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 $ya = \underline{1}$; při tom symbol $\underline{1}$ označuje (i všude v dalším) jednotku grupy $\mathfrak{G}$. Snadno ukážeme, že důsledkem asociativního zákona jest 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 jest $y(ax) = (ya)x = \underline{1}x = x$ 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 jest 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 inversní. Všimněme si, že prvek inversní vzhledem k a může býti 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 jest sám k sobě inversní a jednak množiny skládající se vždy z páru vzájemně inversních prvků. Na př. v grupě $\mathfrak{Z}$ máme jednotku 0 a prvek inversní vzhledem k libovolnému prvku a jest $-a$; zmíněný význačný rozklad grupy $\mathfrak{Z}$ jest tento: $\{0\}, \{1, -1\}, \{2, -2\}, \ldots$ 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 jest patrno, 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 inversní vzhledem k součinu ab jest $b^{-1}a^{-1}$. Za tím účelem stačí zjistiti, že prvek $b^{-1}a^{-1}$ jest 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 inversní vzhledem k součinu* $a_1a_2 \dots a_n$ *libovolných* n ($\geqq 2$) *prvků* $a_1, a_2, \dots, a_n \in \mathfrak{G}$ *jest prvek* $a_n^{-1} \dots a_2^{-1}a_1^{-1}$.

K pojmu inversního prvku připojme ještě tuto poznámku: Jak jsme viděli, jest existence inversního 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 inversní a^{-1}, t. j. prvek splňující rovnosti $aa^{-1} = a^{-1}a = \underline{1}$, pak grupoid $\mathfrak{G}$ jest kvasigrupa 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 hoví rovnicím $ax = b$, $ya = b$ a sice $x = a^{-1}b$, $y = ba^{-1}$, a jak se snadno zjistí, jsou to jediné prvky mající tuto vlastnost. Můžeme tedy říci, že *vlastnost existence inversního prvku vzhledem ke každému prvku charakterisuje grupy mezi všemi asociativními grupoidy s jednotkou.*

Mocniny prvků. Nechť a značí libovolný prvek v $\mathfrak{G}$ a n libovolné přirozené číslo. Protože $\mathfrak{G}$ jest 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 nazýváme prvek $\underbrace{a^{-1}a^{-1} \dots a^{-1}}_{n}$ *-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. Jest účelné definovati také 0*-tou mocninu* a^0 prvku a a to tím, že jest 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* $\dots, -2, -1, 0, 1, 2, \dots$, při čemž ovšem některé z těchto prvků mohou býti identické.

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

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

a sice pro všechna celá čísla m, n.

Omezíme se na provedení důkazu prvního vzorce, abychom ušetřili místa, a přenecháváme čtenáři, aby si podobně ověřil i správnost vzorce druhého. Jestliže jedno anebo obě čísla m, n jsou 0, jest náš vzorec zřejmě správný. Jestliže obě čísla m, n jsou kladná, máme $a^m a^n = (\underbrace{a \dots a}_{m}) . (\underbrace{a \dots a}_{n}) = \underbrace{a \dots a}_{m+n} = a^{m+n}$ a tedy náš vzorec jest 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 uvažovati o případě, že jedno z obou čísel m, n jest kladné a druhé záporné. Jestliže číslo m jest kladné a n záporné, označíme $n' = -n$, takže m, n' značí kladná čísla a máme

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

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

Jestliže konečně číslo m jest 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 jest důkaz proveden.

Značí-li na př. a libovolný prvek v grupě $\mathfrak{Z}$, 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 $1 \in \mathfrak{Z}$ jest celé pole grupy $\mathfrak{Z}$.

Podgrupa a nadgrupa. Nechť $\mathfrak{A}$ značí libovolný podgrupoid v $\mathfrak{G}$. Podle cvič. 7. v odst. 6. jest $\mathfrak{A}$ grupoid asociativní. Když $\mathfrak{A}$ jest grupa, t. j. když jest kvasigrupa, pak pravíme, že $\mathfrak{A}$ jest *podgrupa* v $\mathfrak{G}$ anebo, že $\mathfrak{G}$ jest *nadgrupa* na $\mathfrak{A}$ a píšeme jako obvykle: $\mathfrak{A} \subset \mathfrak{G}$ anebo $\mathfrak{G} \supset \mathfrak{A}$. 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 $\mathfrak{G}$ jest vlastní nadgrupa na $\mathfrak{A}$. V grupě $\mathfrak{G}$ existují alespoň dvě podgrupy: T. zv. *největší* podgrupa, která jest totožná s grupou $\mathfrak{G}$ a t. zv. *nejmenší* podgrupa $\mathfrak{E}$, jejíž pole se skládá z jediného prvku $\underline{1}$.

Uvažujme o libovolné podgrupě $\mathfrak{A}$ v $\mathfrak{G}$. Označme písmenem j jednotku podgrupy $\mathfrak{A}$. Jest 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} inversním 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 $\mathfrak{G}$ jest současně jednotkou podgrupy $\mathfrak{A}$. Odtud plyne dále, že inversní prvek v podgrupě $\mathfrak{A}$ vzhledem k libovolnému prvku $a \in \mathfrak{A}$ jest prvek a^{-1}, t. j. inversní prvek vzhledem k a v grupě $\mathfrak{G}$. Když tedy libovolný podgrupoid v $\mathfrak{G}$ jest 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 jest 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 inversní 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 jest 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}, jest grupoidní a tedy jest polem podgrupy v $\mathfrak{G}$. Podobnou úvahu jako o prvku ab^{-1} můžeme provésti i o prvku $a^{-1}b$.

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 inversní prvek $-b$, skládá se $\mathfrak{A}$ buď jenom z prvku 0, anebo 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 jest prvkem podgrupy $\mathfrak{A}$. Podgrupa $\mathfrak{A}$ ovšem obsahuje všechny mocniny prvku a, t. j. celé násobky čísla a:

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

Nechť b značí libovolný prvek v $\mathfrak{A}$. Jak víme (v. pozn. pod čarou na str. 25.), existují 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, 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 ale jest zřejmé, že množina všech celých násobků libovolného nezáporného čísla spolu s příslušným násobením jest 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 existovati podgrupoidy aniž by byly podgrupami. Další poznámka připínající se k hořejším úvahám jest tato: Třebaže se nám podařilo určiti všechny podgrupy v grupě $\mathfrak{Z}$, bylo by neskromné očekávati podobný úspěch u jiných grup, jejichž násobení jest složitější; nalézti pravidlo, podle něhož by bylo možno určiti všechny podgrupy v každé grupě, jest úloha posud nerozřešená.

Průnik a součin 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 $\mathfrak{G}$. Jest zřejmé, že $\mathfrak{A} \cap \mathfrak{B}$ jest asociativní podgrupoid v $\mathfrak{G}$ s jednotkou $\underline{1}$ a tedy stačí zjistiti, že obsahuje s každým svým prvkem a současně inversní 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 jest důkaz proveden. Můžeme tedy říci, že *každé dvě podgrupy v* $\mathfrak{G}$ *mají průnik a tento průnik jest podgrupou v* $\mathfrak{G}$. Tento výsledek se dá snadno rozšířiti na libovolný počet podgrup v $\mathfrak{G}$.

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 $\mathfrak{AB}$ podgrup $\mathfrak{A}$, $\mathfrak{B}$ (v. cvič. 8. v odst. 6.) a opět snadno zjistíme, že jest podgrupou v $\mathfrak{G}$. Skutečně jest 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 jest každý prvek v $\mathfrak{AB}$ součin ab jistého prvku $a \in \mathfrak{A}$ s jistým prvkem $b \in \mathfrak{B}$; prvek inversní vzhledem k ab jest $b^{-1}a^{-1}$ a z rovnosti $BA = AB$ vyplývá, že jest v podgrupoidu $\mathfrak{AB}$ a tím jest ukázáno, že $\mathfrak{AB}$ *jest podgrupa v* $\mathfrak{G}$. Všimněme si, že platí vztahy $\mathfrak{AB} \supset \mathfrak{A}, \mathfrak{B}$ a že zejména $\mathfrak{A}^2$, t. j. součin $\mathfrak{AA}$, jest podgrupa v $\mathfrak{G}$. Rovněž jest důležité, abychom si uvědomili, že *v každé abelovské grupě* (jsou každé dvě podgrupy zaměnitelné a tedy) *existuje součin každých dvou podgrup a jest opět podgrupou.*

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

$$\ldots, \quad -8, \quad -4, \quad 0, \quad 4, \quad 8, \quad \ldots,$$
$$\ldots, \quad -14, \quad -7, \quad 0, \quad 7, \quad 14, \quad \ldots$$

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

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

Pokud jde o součin $\mathfrak{AB}$, tento obsahuje zřejmě číslo $4 + 7 = 11$ a $\mathfrak{AB}$, 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 $a = 1$ anebo $a = 11$, neboť 11 jest prvočíslo. Protože $\mathfrak{AB}$ zřejmě obsahuje také na př. číslo 4, jest $a = 1$, protože 4 není celým násobkem čísla 11. Vychází tedy, že podgrupa $\mathfrak{AB}$ se skládá ze všech celých násobků čísla 1, takže jest totožná s grupou $\mathfrak{Z}$.

Poznámky o multiplikačních tabulkách konečných grup. Nechť $\mathfrak{G}$ značí libovolnou konečnou grupu a uvažujme o příslušné multiplikační tabulce! Protože $\mathfrak{G}$ jest kvasigrupa, vyskytnou se v multiplikační tabulce v každém řádku a v každém sloupci napravo od svislého a pod vodorov-

ným záhlavím symboly všech prvků grupy $\mathfrak{G}$ a tedy se tam vyskytne zejména $\underline{1}$ a se symbolem každého prvku současně symbol prvku inversního. Na př. multiplikační tabulky pro grupy řádů 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 možny 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 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 býti a na konec se verifikuje, že jest splněn asociativní zákon. Avšak tento postup jest bez dalších znalostí o grupách zdlouhavý. Třebaže jsou známa pravidla, pomocí kterých lze určiti multiplikační tabulky všech grup jistých řádů, zůstává hlavním dosud neřešeným problémem výčet všech konečných grup libovolného řádu.

Každou multiplikační tabulku grupy libovolného řádu můžeme především zjednodušiti 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 $\underline{1}$ jest 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 $\underline{1}, a, b, c$, jsou tyto:

$\underline{1}$

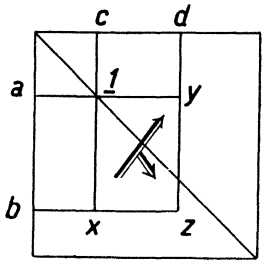
$\underline{1}\ a$
$a\ \underline{1}$

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

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

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

V každé normální multiplikační tabulce jest tedy 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 průsečíku 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 inversní. Vidíme tedy, že v prvním řádku naší tabulky jsou od leva do prava napsány symboly inversních prvků vzhledem k prvkům v prvním sloupci, tak jak jdou po sobě od 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 jest v témže sloupci a y v témže řádku jako $\underline{1}$ a tedy z jest v témže řádku jako x a v témže 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 na př. x jest 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 inversní, 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 $\underline{1}$ jest součinem prvku na vrcholu v témže sloupci jako $\underline{1}$ s prvkem na vrcholu zbývajícím. Na př. v normální multiplikační tabulce grupy řádu 4., která jest na str. 56. napsána jako poslední, tvoří prvky $\underline{1}, c$ v druhém řádku spolu s prvky b, a ve čtvrtém řádku vrcholy obdélníka; podle obdélníkového pravidla jest tedy $bc = a$ a skutečně na průsečíku řádku začínajícího písmenem b a sloupce začínajícího písmenem c jest prvek a. Obdélníkové pravidlo jest v případě, že $\underline{1}$ jest na levém horním vrcholu obdélníka, znázorněno na obr. 10: Součin prvku x s prvkem y jest prvek z.



Obr. 10.

Cvičení. 1. Grupoid, jehož pole jest množina všech euklidovských pohybů na přímce $\boldsymbol{f}[a]$, $\boldsymbol{g}[a]$ anebo v rovině $\boldsymbol{f}[\alpha; a, b]$, $\boldsymbol{g}[\alpha; a, b]$ a násobení jest definováno skládáním pohybů (v. cvič. 1. v odst. 5.) jest grupa, t. zv. *úplná grupa euklidovských pohybů na přímce* anebo *v rovině*. V úplné grupě euklidovských pohybů na přímce anebo v rovině tvoří všechny euklidovské pohyby $\boldsymbol{f}[a]$ anebo $\boldsymbol{f}[\alpha; a, b]$ podgrupu. Uveďte některé další podgrupy v těchto grupách! — Poznámka. Na př. euklidovská geometrie v rovině popisuje, jak víme ze střední školy, vlastnosti útvarů slože-

ných z bodů a přímek, jako jsou různé konfigurace bodů a přímek, trojúhelníky, kuželosečky, atp. Tato geometrie jest podložena úplnou grupou euklidovských pohybů v rovině v tom smyslu, že se dva útvary považují za shodné, když se dají na sebe zobraziti některým euklidovským pohybem.

2. Grupoid, jehož pole jest množina $2n$ permutací vrcholů pravidelného n-úhelníka v rovině ($n \geqq 3$), které jsme popsali ve cvič. 4. v odst. 4., a násobení jest definováno skládáním permutací (v. cvič. 2. v odst. 5.) jest grupa, která se nazývá *diedrická 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 inversní, jest v každé konečné grupě sudého (lichého) řádu sudý (lichý).

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

5. V každé abelovské grupě tvoří všechny prvky, které jsou samy k sobě inversní, podgrupu.

6. 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 $\mathfrak{C}$ jest podgrupa v $\mathfrak{G}$ a jest zaměnitelná s $\mathfrak{A}$, pak i podgrupa $\mathfrak{C} \cap \mathfrak{B}$ jest zaměnitelná s $\mathfrak{A}$.

7. Každá grupa má centrum.

12. O rozkladech grup vytvořených podgrupami.

Velmi důležitá vlastnost grup záleží v tom, že každá podgrupa v libovolné grupě určuje na ní jisté rozklady. Uvažujme opět o libovolné grupě $\mathfrak{G}$ a o nějaké podgrupě $\mathfrak{A} \subset \mathfrak{G}$! Nechť a značí libovolný prvek v $\mathfrak{G}$. Podmnožina $a\mathfrak{A}$ v $\mathfrak{G}$, t. j. tedy množina součinů prvku a s každým prvkem v $\mathfrak{A}$, nazývá se *levá třída prvku a vzhledem k podgrupě* $\mathfrak{A}$, anebo stručněji, víme-li, že jde o podgrupu $\mathfrak{A}$, *levá třída prvku a* a podobně nazývá se podmnožina $\mathfrak{A}a$, t. j. množina součinů každého prvku v $\mathfrak{A}$ s prvkem a *pravá třída prvku a vzhledem k podgrupě* $\mathfrak{A}$, stručněji: *pravá třída prvku a*. Všimněme si, že pole A podgrupy $\mathfrak{A}$ jest současně levá i pravá třída prvku $\underline{1}$ vzhledem k $\mathfrak{A}$. V několika jednoduchých větách popíšeme nejprve vlastnosti levých tříd; vlastnosti pravých tříd jsou analogické, a třebaže je kvůli úspoře místa výslovně neuvádíme, doporučujeme čtenáři, aby si je rovněž promyslil.