množinu těchto permutací M_n. Dokažte, že množina M_n má tyto vlastnosti: 1. Když $p \in M_n$, $q \in M_n$, pak také $qp \in M_n$; 2. $e \in M_n$; 3. když $p \in M_n$, pak také $p^{-1} \in M_n$.

4.6.5. **Každé dvě cyklické permutace každé množiny o n (≥ 1) prvcích, jejichž cykly nemají společných prvků, jsou zaměnitelné.**

II. GRUPOIDY.

5. O NÁSOBENÍ V MNOŽINĚ.

5.1. Pojem násobení v množině.

Násobením v množině G rozumíme nějaké pravidlo, jímž je ke každé uspořádané dvojici prvků $a, b \in G$ jednoznačně přiřazen opět některý prvek $c \in G$. Tento prvek c se nazývá *součin prvku a s prvkem b* a značí se symbolem $a.b$ nebo kratčeji ab. Z těchto definic je zřejmé, že slovo násobení jest jenom název pro nějaké pravidlo, podrobněji popsané v naší definici, a že v konkretních případech nemusí míti nic společného s pojmem aritmetického násobení, které známe z obecné školy; podobná poznámka platí ovšem o součinu a o symbolech $a.b$, ab. V jakém smyslu zobecňuje pojem násobení v množině G pojem zobrazení množiny G do sebe, na to odpověď plyne snadno z porovnání obou definic: Každé zobrazení množiny G do sebe přiřazuje jednoznačně ke každému prvku v G opět nějaký prvek v G; každé násobení v množině G přiřazuje jednoznačně ke každé uspořádané dvojici prvků v G opět nějaký prvek v G. Jestliže je dáno násobení v množině G, pak je zejména jednoznačně určen součin každého prvku $a \in G$ opět s prvkem a; místo aa píšeme někdy stručněji a^2.

5.2. Násobení abelovské.

Násobení v množině G může míti zvláštní vlastnosti. Tak na příklad není naší definicí vyloučeno, že násobení přiřazuje k některým dvěma opačně uspořádaným dvojicím prvků v G dva různé prvky, takže se může státi, že součin některého prvku a s některým prvkem b je různý od součinu prvku b s prvkem a, t. j. $ab \neq ba$.

Jestliže pro některé dva prvky $a, b \in G$ platí rovnost $ab = ba$, pak se prvky a, b nazývají vzájemně zaměnitelné neboli *vzájemně komutativní; jestliže každé dva prvky v G jsou vzájemně zaměnitelné, pak se násobení nazývá abelovské* neboli *komutativní.*

Násobení v množině může míti ovšem i jiné význačné vlastnosti a o některých, které jsou pro náš účel důležité, pojednáme později. V následujícím odstavci uvedeme příklady násobení, na něž v dalším výkladu častěji poukážeme.

5.3. Příklady násobení v množině.

5.3.1. G je množina všech celých čísel a násobení je definováno takto: Součin libovolného prvku $a \in G$ s libovolným prvkem $b \in G$ je číslo $a + b$. V tomto případě je tedy násobením sečítání v obvyklém smyslu. Z rovnosti $a + b = b + a$, která platí pro každé dva prvky $a, b \in G$, plyne, že toto násobení jest abelovské.

5.3.2. Nechť n je libovolné přirozené číslo a G nějaká množina skládající se z přirozených čísel, která obsahuje všechna čísla $0, \ldots, n - 1$. Násobení v množině G definujeme takto: Součin ab libovolného prvku $a \in G$ s libovolným prvkem $b \in G$ je zbytek dělení čísla $a + b$ číslem n. Součin ab je tedy vždy jedno z čísel $0, \ldots, n - 1$. Toto násobení nazýváme *sečítání vzhledem k modulu n*; je zřejmé, že je také abelovské.

5.3.3. G je množina všech permutací nějaké konečné množiny řádu n (≥ 1) a násobení je definováno takto: Součin $\boldsymbol{p}.\boldsymbol{q}$ libovolného prvku $\boldsymbol{p} \in G$ s libovolným prvkem $\boldsymbol{q} \in G$ je složená permutace $\boldsymbol{qp}$. V tomto případě je tedy násobení skládání permutací. Z dřívějšího výkladu víme, že nemusí být abelovské.

5.3.4. G je množina všech rozkladů nějaké množiny a násobení je definováno takto: Součin $\bar{A} \,.\, \bar{B}$ libovolného prvku $\bar{A} \in G$ s libovolným prvkem $\bar{B} \in G$ je rozklad $[\bar{A}, \bar{B}]$, příp. $(\bar{A}, \bar{B})$. Obě násobení jsou abelovská, jak plyne z **2.6.2.2a** a **2.7.2.2a.**

5.4. Multiplikační tabulka.

5.4.1. *Popis multiplikační tabulky.* Když množina G je konečná a její prvky jsme označili na př. písmeny $a, b, \ldots, m$, pak libovolné násobení v G můžeme popsati v t. zv. *multiplikační tabulce*, kterou sestavíme takto:

Do prvního řádku a do prvního sloupce, které obvykle od ostatních oddělujeme vodorovnou a svislou čarou, napíšeme všechna písmena $a, b, \ldots, m$, a to zpravidla v témže pořadí, v prvním řádku odleva doprava a v prvním sloupci od shora dolů. Napravo od každého písmene x v prvním sloupci, a to pod jednotlivá písmena $a, b, \ldots, m$ stojící v prvním řádku, napíšeme písmena označující jednotlivé součiny $xa, xb, \ldots, xm$.

První řádek a první sloupec, oddělené od ostatních čarami, nazýváme *záhlaví tabulky*. Každá multiplikační tabulka má tedy kromě vodorovného a svislého záhlaví ještě právě tolik řádků a sloupců, kolik má množina G prvků. Když písmena $a, b, \ldots, m$ jsou v obou záhlavích napsána v témže pořádku, pak se násobení abelovské projeví v tabulce patrně tím, že tabulka je souměrná vzhledem k hlavní úhlopříčně, t. j. v jejím libovolném j-tém řádku a v libovolném k-tém sloupci za oběma záhlavími je týž prvek jako v k-tém řádku a j-tém sloupci.

5.4.2. *Příklady multiplikačních tabulek.* Jako příklad uvedeme multiplikační tabulky pro násobení v množině G všech permutací nějaké množiny H, která se skládá z $n = 1, 2, 3$ prvků, při čemž násobení je skládání permutací, jak jsme je popsali v hořejším příkladě **5.3.3.** Protože všech permutací množiny H, a tedy prvků množiny G, je $n! = 1, 2, 6$, mají tyto multiplikační tabulky, kromě obou záhlaví, $n! = 1, 2, 6$ řádků a týž počet sloupců.

Pro $n = 1$. Množina G se skládá z identické permutace $\mathbf{e}$. Označíme-li onen prvek, z něhož se množina H skládá, písmenem a, je symbol této permutace $\begin{pmatrix} a \\ a \end{pmatrix}$ a multiplikační tabulka je tato:

	e
e	**e**

Pro $n = 2$. Množina G se skládá ze dvou permutací. Označíme-li prvky množiny H písmeny a, b, jsou symboly těchto permutací $\begin{pmatrix} a & b \\ a & b \end{pmatrix}$, $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$. První z nich jest identická permutace $\mathbf{e}$, druhou označíme na př. a. Permutace složené jsou: $\mathsf{ee} = \mathsf{e}$, $\mathsf{ae} = \mathsf{a}$, $\mathsf{ea} = \mathsf{a}$, $\mathsf{aa} = \mathsf{e}$, a odtud vychází tato multiplikační tabulka:

	e	a
e	e	a
a	a	e

Pro $n = 3$. Množina G se skládá ze šesti permutací. Označíme-li prvky množiny H písmeny a, b, c, jsou symboly těchto permutací

$$\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}, \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}.$$

První z nich jest identická permutace e, ostatní označíme po pořádku $\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}, \mathsf{f}$. Permutace složené jsou:

$$\begin{array}{llllll}
\mathsf{ee} = \mathsf{e}, & \mathsf{ae} = \mathsf{a}, & \mathsf{be} = \mathsf{b}, & \mathsf{ce} = \mathsf{c}, & \mathsf{de} = \mathsf{d}, & \mathsf{fe} = \mathsf{f}, \\
\mathsf{ea} = \mathsf{a}, & \mathsf{aa} = \mathsf{b}, & \mathsf{ba} = \mathsf{e}, & \mathsf{ca} = \mathsf{d}, & \mathsf{da} = \mathsf{f}, & \mathsf{fa} = \mathsf{c}, \\
\mathsf{eb} = \mathsf{b}, & \mathsf{ab} = \mathsf{e}, & \mathsf{bb} = \mathsf{a}, & \mathsf{cb} = \mathsf{f}, & \mathsf{db} = \mathsf{c}, & \mathsf{fb} = \mathsf{d}, \\
\mathsf{ec} = \mathsf{c}, & \mathsf{ac} = \mathsf{f}, & \mathsf{bc} = \mathsf{d}, & \mathsf{cc} = \mathsf{e}, & \mathsf{dc} = \mathsf{b}, & \mathsf{fc} = \mathsf{a}, \\
\mathsf{ed} = \mathsf{d}, & \mathsf{ad} = \mathsf{c}, & \mathsf{bd} = \mathsf{f}, & \mathsf{cd} = \mathsf{a}, & \mathsf{dd} = \mathsf{e}, & \mathsf{fd} = \mathsf{b}, \\
\mathsf{ef} = \mathsf{f}, & \mathsf{af} = \mathsf{d}, & \mathsf{bf} = \mathsf{c}, & \mathsf{cf} = \mathsf{b}, & \mathsf{df} = \mathsf{a}, & \mathsf{ff} = \mathsf{e},
\end{array}$$

a vychází tato multiplikační tabulka:

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d	f	c
b	b	e	a	f	c	d
c	c	f	d	e	b	a
d	d	c	f	a	e	b
f	f	d	c	b	a	e

Ve všech těchto multiplikačních tabulkách jsme napsali v obou záhlavích symboly $\mathsf{e}, \mathsf{a}, \ldots, \mathsf{f}$ jednotlivých prvků množiny G v témže pořadí a vidíme, že v případech $n = 1, 2$ jsou hořejší tabulky souměrné vzhledem k hlavní úhlopříčně, kdežto v případě $n = 3$ je multiplikační tabulka nesouměrná. Odtud plyne, že naše násobení v množině G je v případech $n = 1, 2$ abelovské, ale v případě $n = 3$ abelovské není.

Příkladů násobení v množinách se dá uvésti nepřehledné množství. Stačí vzíti libovolnou abstraktní neprázdnou množinu G a ke každé uspořádané dvojici prvků $a, b \in G$ jednoznačně přiřaditi některý prvek v G. Když množina G je konečná, pak můžeme přiřazení definovat v tabulce, v níž na jednotlivých místech, pod vodorovným záhlavím a napravo od svislého, napíšeme symboly některých prvků množiny G, které zvolíme podle libosti. Každá volba těchto prvků určuje pak jisté násobení, pro které naše tabulka je multiplikační.

5.5. Cvičení.

5.5.1. V množině všech euklidovských pohybů na přímce $\mathfrak{f}[a]$ a rovněž v množině skládající se ze všech euklidovských pohybů na přímce $\mathfrak{f}[a]$, $\mathfrak{g}[a]$ (viz **3.10.5**) můžeme definovat násobení skládáním pohybů, podobně jako v příkladě **5.3.3.** Podobný výsledek platí o množině všech euklidovských pohybů v rovině $\mathfrak{f}[\alpha; a, b]$ a o množině všech euklidovských pohybů v rovině $\mathfrak{f}[\alpha; a, b]$, $\mathfrak{g}[\alpha; a, b]$ (viz **3.10.6**).

5.5.2. V množině $2n$ permutací vrcholů pravidelného n-úhelníka v rovině ($n \geqq 3$), které jsme popsali ve cvič. **4.6.4**, můžeme definovat násobení skládáním permutací podobně jako v příkladě **5.3.3.** Sestavte pro toto násobení v případech $n = 4, 5, 6$ multiplikační tabulky!

5.5.3. V příkladě **5.3.2** se může množina G skládati právě jenom z čísel $0, \ldots, n - 1$. Sestavte pro tento případ, a to pro $n = 1, 2, 3, 4, 5$, multiplikační tabulky!

5.5.4. Když přirozená čísla a, b jsou menší nebo rovna nějakému přirozenému číslu $n \geqq 5$, pak počet prvočísel, která dělí číslo $10a + b$, je $\leqq n$. Odtud plyne, že v množině G, která se skládá z čísel $1, 2, \ldots, n$, můžeme definovat násobení takto: Součin $a.b$ libovolného prvku $a \in G$ s libovolným prvkem $b \in G$ je počet prvočísel, která dělí číslo $10a + b$. Přesvědčte se, že pro $n = 6$ je příslušná multiplikační tabulka tato:

	1	2	3	4	5	6
1	1	3	1	2	2	4
2	2	2	1	4	2	2
3	1	5	2	2	2	4
4	1	3	1	3	3	2
5	2	3	1	4	2	4
6	1	2	3	6	2	3

5.5.5. V systému všech podmnožin libovolné neprázdné množiny můžeme definovat násobení tím, že ke každé uspořádané dvojici podmnožin přiřadíme jejich součet. Můžeme násobení podobně definovat pomocí průniku?

5.5.6. Vymyslete sami příklady násobení v množinách!

6. ZÁKLADNÍ POJMY O GRUPOIDECH

6.1. Definice.

Libovolná neprázdná množina G spolu s nějakým násobením $\mathbf{M}$ v G se nazývá grupoid. G se nazývá pole a $\mathbf{M}$ násobení grupoidu. Grupoidy budeme označovati velkými německými písmeny, a to zpravidla stejnými jako jejich pole. Na př. označujeme grupoid, jehož pole jsme označili G, písmenem $\mathfrak{G}$, a když jsme nějaký grupoid označili $\mathfrak{G}$, pak písmeno G značí zpravidla jeho pole.

6.2. Grupoid abstraktní, abelovský, permutační; grupoidy $\mathfrak{Z}$, $\mathfrak{Z}_n$, $\mathfrak{S}_n$.

Na grupoidy přenášíme pojmy a symboly, které jsme definovali pro jejich pole. Tak na př. mluvíme *o prvcích grupoidu* místo o prvcích pole grupoidu a píšeme $a \in \mathfrak{G}$ místo $a \in G$, podobně mluvíme *o podmnožinách v grupoidu* a píšeme na př. $A \subset \mathfrak{G}$ nebo $\mathfrak{G} \supset A$, mluvíme *o rozkladech v grupoidu a na grupoidu, o řádu grupoidu, o zobrazení grupoidu do nějaké množiny, do nějakého drupoidu nebo na grupoid,* atd. *Když G je abstraktní množina, nazývá se grupoid $\mathfrak{G}$ abstraktní.*

Rovněž pojmy a symboly, které jsme definovali pro násobení, přenášíme na grupoidy. Tedy zejména má každá uspořádaná dvojice prvků $a, b \in \mathfrak{G}$ jistý součin $a.b$, stručněji ab, a *když pro každé $a, b \in \mathfrak{G}$ platí rovnost $ab = ba$, nazývá se grupoid $\mathfrak{G}$ abelovský neboli komutativní.* Také můžeme ke každému konečnému grupoidu $\mathfrak{G}$ přiřadit multiplikační tabulku, v níž je popsáno násobení v $\mathfrak{G}$. V odstavci **5.4.2** jsme uvedli několik příkladů násobení a každý z nich je současně příkladem grupoidu.

V dalším výkladu častěji poukážeme zejména na tyto tři grupoidy,