ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PEDAGOGICKÁ

KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

ŘEŠENÉ ÚLOHY Z OBECNÉ ALGEBRY

BAKALÁŘSKÁ PRÁCE

Lenka Šellerová

Vedoucí práce: Doc. RNDr. Jaroslav Hora, CSc.

Plzeň, 2014

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně s použitím uvedené literatury a zdrojů informací.

Plzeň, 9. dubna 2014

…….

Podpis

Touto cestou bych chtěla velmi poděkovat mému vedoucímu bakalářské práce **doc. RNDr. Jaroslavu Horovi, CSc.**, za odborné vedení, pomoc a cenné rady v průběhu jejího zpracování.

OBSAH

ÚVOD

Tématem této bakalářské práce jsou Řešené úlohy z obecné algebry. Toto téma je však velice obsáhlé, a proto jsem se zaměřila pouze na grupy. Mým cílem je seznámit čtenáře s teorií grup.

Tato práce je rozdělena do osmi kapitol. První kapitola s názvem Historie čtenáře informuje o tom, jak se teorie grup vyvíjela a kdy pojem grupa vznikl. Na tuto část již navazuje kapitola Základní pojmy, která se skládá ze tří podkapitol, jimiž jsou Binární algebraické operace, Algebraická struktura a Cvičení. První podkapitola se bude věnovat vlastnostem binárních algebraických operací, jako jsou komutativnost, asociativnost, existence neutrálního, inverzního a agresivního prvku a idempotentnost. Ve druhé podkapitole Algebraická struktura budeme definovat spolu s grupoidem, pologrupou a monoidem také grupu a podgrupu, které jsou hlavním cílem této bakalářské práce. Poslední podkapitolou je Cvičení. V němž se vyskytují řešené příklady, které mají za úkol shrnout celou předešlou látku. V třetí části se zabýváme homomorfizmem a izomorfizmem, jež jsou zvláštními případy zobrazení jedné algebraické struktury do jiné a zachovávají si určité vlastnosti. Na tuto látku již navazuje samotné členění grup. Tato bakalářská práce je zaměřena na grupy konečné, cyklické, normální, symetrické a alternující. Shrnutím těchto grup je poslední část práce s názvem Cvičení, ve kterém si čtenář může procvičit probranou látku.

V každé kapitole se nachází několik definic a vět. Pod většinou z nich je i příklad, který by měl čtenáři lépe vysvětlit a názorně ukázat, co daná definice nebo věta znamená.

1 HISTORIE

Matematická disciplína, která se zabývá grupami, se nazývá teorie grup. Je jednou z nejstarších a nejrozpracovanějších disciplín algebry. Její vznik je spjat s Galoisovým objevem kritéria řešitelnosti rovnic vyšších stupňů v radikálech. Z tohoto důvodu matematici nejprve studovali pouze konečné grupy permutací a později přišli na to, že při řešení různých problémů teorie grup mohou pracovat s libovolnou množinou objektů, na níž je definována určitá binární operace splňující jisté axiomy.

Tento objev dal vzniknout abstraktní teorii konečných grup. Velmi významnými osobnostmi, které jsou spojeny s teorií grup, jsou Frobenius, Hölder, Burnside a Schur. Teorie konečných grup se začala rozvíjet koncem 18. a začátkem 19. století. V této době byly objeveny klasické výsledky a základní metody. Matematici se však začali setkávat i s nekonečnými algebraickými strukturami, které splňovaly axiomy grupy.

Pojem konečná grupa se stal tedy speciálním případem pojmu grupa. Bouřlivý vývoj teorie grup byl zaznamenán až tehdy, kdy byla postavená na teoreticko-množinové základy a tím se tak stala abstraktní teorií. [5]

2 ZÁKLADNÍ POJMY

Grupa je jedním z nejdůležitějších a nejužitečnějších algebraických systémů. Lze ji definovat různými způsoby. Nejdříve je ale běžné uvést definice několika velmi důležitých pojmů jako například binární algebraická operace, grupoid, pologrupa.

2.1 BINÁRNÍ ALGEBRAICKÉ OPERACE

V širším slova smyslu můžeme binární operace brát jako zobrazení, které některým uspořádaným dvojicím prvků dané množiny M přiřazuje jeden nebo několik prvků množiny M .

Definice 1:

Binární operací $*$ definovanou na libovolné množině M rozumíme zobrazení kartézského součinu MxM do M . Symbolicky

$$* : MxM \to M$$

nebo též $$MxM \xrightarrow{*} M$$ [8]

Příklad 1:

Nechť $M \subset \mathbb{N}$: $[4; 4] \xrightarrow{+} 8$

tedy: $4+4=8$

Mezi nejznámější algebraické operace patří aritmetické operace sčítání a násobení, které mohou být prováděny na množinách čísel celých, přirozených, racionálních a komplexních. Operaci sčítání velmi často nazýváme aditivní operací a operaci násobení nazýváme multiplikativní operací.

Aritmetická operace odečítání nemůže být realizována na množině čísel přirozených, jelikož ke každé uspořádané dvojici (a, b) nemůže být přiřazeno číslo c ∈ N takové, aby platilo c = a – b. Z tohoto důvodu může být aritmetická operace odečítání prováděna pouze na množinách čísel celých, racionálních a komplexních. [9]

2.1.1 Vlastnosti binárních algebraických operací

2.1.1.1 Komutativní algebraická operace

Definice 2:

Operaci $*$ nazýváme *komutativní* na množině M právě tehdy, když platí

$$(\forall a,b \in M)\ a*b = b*a.$$

Tato rovnost se nazývá komutativní zákon.

Z definice je dobře vidět, že nezávisí na pořadí operandů. [8]

Příklad 2:

Nyní si uvedeme příklady komutativních operací s příslušnými obory, na kterých jsou tyto operace definovány. Je zřejmé, že ne každá operace je definována na všech číselných oborech.

Jako příklad komutativní algebraické operace můžeme uvést aritmetické operace sčítání a násobení, které jsou definovány na množinách $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ a $\mathbb{R}$. Další komutativní operací může být sjednocení, průnik a symetrický rozdíl množin.

Nechť M je množina a $P(M)$ značí systém všech jejích podmnožin, pak jsou operace sjednocení, průnik a symetrický rozdíl na $P(M)$ komutativní.

Logické operace konjunkce a disjunkce na množině logických výroků jsou komutativní.

Nechť V je vektorový prostor. Operace sčítání vektorů na V je komutativní.

Nechť M je množina všech čtvercových matic stupně n nad tělesem reálných čísel. Pak je operace sčítání matic na M komutativní.

Naopak číselné operace odečítání a dělení, násobení matic, skládání zobrazení, logická operace implikace obecně komutativní nejsou.

V předchozím odstavci hovoříme o tom, že operace odečítání a dělení, násobení matic, skládání zobrazení, logická operace implikace nejsou obecně komutativní. Neznamená to však, že neexistuje situace, kdy komutativita i u těchto operací nastane.

Jedná se však spíše o výjimky nebo modelové příklady, které mají cíleně vyjít jako komutativní.

2.1.1.2 Asociativní algebraická operace

Definice 3:

Operaci $*$ nazýváme *asociativní* na množině M právě tehdy, když platí

$$(\forall a,b,c \in M)\ (a*b)*c = a*(b*c).$$

Tato rovnost se nazývá asociativní zákon. [8]

Příklad 3:

Protože ne každá operace je ve všech číselných oborech definována, uvedeme si zde příklad operací, jež jsou asociativní s přehledem oborů, na kterých jsou definovány.

Jako příklad asociativní algebraické operace můžeme uvést aritmetické operace sčítání a násobení, které jsou definovány na množinách $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ a $\mathbb{R}$.

Nechť M je množina a $P(M)$ značí systém všech jejích podmnožin, pak jsou operace sjednocení, průnik symetrický rozdíl na $P(M)$ asociativní.

Logické operace konjunkce a disjunkce na množině logických výroků jsou asociativní.

Nechť V je vektorový prostor. Operace V je asociativní.

Nechť M je množina všech čtvercových matic stupně n nad tělesem reálných čísel. Pak je operace sčítání matic na M asociativní.

Mezi neasociativní operace patří číselné operace odečítání, dělení a množinová operace rozdíl.

Příklad 4:

Zjistěte, zda je binární operace $*$ definovaná na množině R předpisem $a*b = a+ab+b; a,b \in R$ asociativní.

Nejprve vypočteme levou a následně pravou stranu podmínky asociativnosti. Získané výsledky porovnáme, a pokud rovnost platí, můžeme konstatovat, že podmínka asociativnosti je splněna.

$$(a*b)*c=(a+ab+b)*c=(a+ab+b)+(a+ab+b)c+c=a+ab+b+ac+abc+bc+c=a+b+c+ab+ac+bc+abc$$

$$a*(b*c)=a*(b+bc+c)=a+a(b+bc+c)+(b+bc+c)=a+ab+abc+ac+b+bc+c=a+b+c+ab+ac+bc+abc$$

Binární operace je asociativní, jelikož jsme dokázali rovnost mezi $(a*b)*c=a*(b*c)$, platnou pro všechna $a, b, c \in R$.

2.1.1.3 Neutrální prvek

Definice 4:

Prvek e nazýváme *neutrálním* prvkem binární operace $*$ definované na množině M právě tehdy, když platí

$$(\forall a \in M)\ e*a=a*e=a.$$

Platí-li pouze

$$(\forall a \in M)\ e*a=a,$$

nazýváme prvek e *levým neutrálním* prvkem binární operace $*$.

Platí-li pouze

$$(\forall a \in M)\ a*e=a,$$

nazýváme prvek e *pravým neutrálním* prvkem binární operace $*$. [8]

Věta 1:

Nechť M je množina s binární operací $*$. Potom platí:

Existuje-li v množině M levý i pravý neutrální prvek, pak jsou si rovny a jde o oboustranný neutrální prvek.

V množině M existuje nejvýše jeden neutrální prvek. [2]

Příklad 5:

Určete neutrální prvek operace $*$ definované na množině $M \subset R$ předpisem:

$$a*b=2a+b; a,b \in M$$
$$a*e=e*a=a$$

$$e * a = a \qquad a * e = a$$
$$2e + a = a \qquad 2a + e = a$$
$$e = 0 \qquad e = -a$$

Výpočtem jsme zjistili, že existuje pouze levý neutrální prvek 0 právě tehdy, pokud 0 patří do množiny M.

Poznámka 1:

V případě standardních operací jako například sčítání, násobení, sčítání vektorů nebo násobení matic (a další) jsou neutrální prvky zřejmé.

Neutrální prvek pro sčítání:
$$a + 0 = a$$
$$e = 0$$

Neutrální prvek pro násobení:
$$a \cdot 1 = a$$
$$e = 1$$

Neutrální prvek pro sčítání vektorů:
$$\vec{v} + \vec{o} = \vec{v}$$
$$e = \vec{o}$$

Neutrální prvek pro násobení čtvercových matic:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mm} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mm} \end{pmatrix}$$

$$e = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

2.1.1.4 Inverzní prvek

Definice 5:

Prvek a^{-1} nazýváme *inverzním prvkem* k prvku a v binární operaci $*$ definované na množině M právě tehdy, když platí

$$a * a^{-1} = a^{-1} * a = e,$$

kde e je neutrální prvek operace $*$. [8]

Poznámka 2:

Nemá-li operace $*$ na zadané množině M neutrální prvek e, potom neexistuje ani prvek inverzní a nemá smysl ho vyšetřovat.

Příklad 6:

Určete inverzní prvek binární operace $*$, která je definovaná na množině R a je dána vztahem:

$$a * b = ab; a, b \in R$$

Vidíme, že operace $*$ je definovaná jako „obyčejný“ součin. Jak jsme již zjistili dříve, neutrální prvek u této operace je $e = 1$. Má tedy smysl hledat inverzní prvek.

$$a^{-1} * a = e$$
$$a^{-1} \cdot a = 1$$
$$a^{-1} = \frac{1}{a}$$

Protože se pohybujeme na množině reálných čísel, ke každému nenulovému reálnému číslu a vždy existuje inverzní prvek $\frac{1}{a} \in R$ a platí:

$$a * \left(\frac{1}{a}\right) = \left(\frac{1}{a}\right) * a = 1$$

V příkladu jsme zároveň zjistili, že pro „obyčejné“ násobení je inverzním prvkem k reálnému číslu a jeho převrácená hodnota $\frac{1}{a}$.

Příklad 7:

Ke každému racionálnímu číslu a existuje číslo opačné $-a$, které jej kompenzuje v operaci sčítání, tj. platí

$$a + (-a) = 0$$

Poznámka 3:

Je potřeba si říci, že v multiplikativním zápisu operace se místo neutrálního prvku často používá název jednotkový prvek a místo inverzního prvku prvek převrácený.

Podobně je tomu i v aditivním zápisu operace. V tomto případě totiž používáme název nulový prvek resp. opačný prvek.

2.1.1.5 Agresivní prvek

Definice 6:

Prvek g nazýváme *agresivním* prvkem binární operace $*$ definované na množině M právě tehdy, když platí

$$(\forall a \in M)\, g * a = a * g = g$$

Platí-li pouze

$$(\forall a \in M)\, g * a = g\,,$$

nazýváme prvek g *levým agresivním* prvkem binární operace $*$.

Platí-li pouze

$$(\forall a \in M)\, a * g = g\,,$$

nazýváme prvek g *pravým agresivním* prvkem binární operace $*$. [8]

2.1.1.6 Idempotentní prvek

Definice 7:

Operaci $*$ nazýváme *idempotentní* na množině M právě tehdy, když platí

$$(\forall a \in M)\, a * a = a.$$ [8]

2.2 ALGEBRAICKÁ STRUKTURA

Definice 8:

Pod algebraickou strukturou budeme rozumět množinu nějakých objektů (nemusí to být objekty matematické), na kterých je definována aspoň jedna binární operace. Tyto struktury budeme symbolicky označovat následovně: $(M,*),(K,\#,\circ)$. Obecně budeme hovořit o algebraické struktuře s jednou operací, se dvěma operacemi atd. [8]

2.2.1 Grupoid

Definice 9:

Grupoid je uspořádaná dvojice $(G;*)$, kde G je libovolná neprázdná množina a $*$ je binární operace na G. Množinu G nazýváme nosičem a operaci $*$ nazýváme operací grupoidu $(G;*)$.

Příklad 8:

$(N,+)$ operace sčítání na množině všech přirozených čísel;

$(N,\cdot)$ operace násobení na množině všech přirozených čísel;

$(Z,+)$ operace sčítání na množině všech celých čísel;

$(Z,\cdot)$ operace násobení na množině všech přirozených čísel.

2.2.2 Pologrupa a monoid

Definice 10:

Algebraickou strukturu $(P,*)$ nazýváme *pologrupou* právě tehdy, když operace $*$ splňuje následující axiom

$$(\forall a,b,c \in P)(a*b)*c = a*(b*c) \text{ (asociativnost).}$$

Jestliže je navíc splněn axiom

$$(\forall a,b \in P)\, a*b = b*a \text{ (komutativnost).}$$

nazýváme pologrupu *pologrupou komutativní* resp. a*belovskou pologrupou*.

Jestliže je navíc splněn axiom

$$(\exists e \in P)(\forall a \in P)\, e*a = a*e = a \text{ (existence neutrálního prvku),}$$

potom platí definice: [8]

Definice 11:

Grupoid G s asociativní operací $*$, ve kterém existuje neutrální prvek, se nazývá monoid, případně pologrupa s jednotkovým prvkem.

Jestliže navíc platí:

$$(\forall a,b \in G)\, a * b = b * a \text{ (komutativnost)},$$

nazýváme monoid monoidem *komutativním* resp. a*belovským monoidem*. [8]

Příklad 9:

Příkladem pologrup mohou být například:

$(N,+)$ Operace sčítání na množině všech přirozených čísel;

$(N,\cdot)$ Operace násobení na množině všech přirozených čísel;

$(Z,+)$ Operace sčítání na množině všech celých čísel;

$(Z,\cdot)$ Operace násobení na množině všech přirozených čísel.

Příklad 10:

Určete, zda je množina přirozených čísel N vzhledem k operaci násobení monoidem.

V příkladu 9 jsme již zjistili, že přirozená čísla jsou vzhledem k součinu pologrupou. Stačí tedy pouze vyšetřit existenci neutrálního prvku.

$$(\forall a \in N)\, e \cdot a = a \cdot e = a$$

$$e \cdot a = a \qquad\qquad a \cdot e = a$$
$$e = 1 \qquad\qquad e = 1$$

Levý i pravý neutrální prvek se rovnají a můžeme říct, že neutrální prvek existuje. Množina přirozených čísel N vzhledem k operaci násobení monoidem.

2.2.3 Grupa

Definice 12:

Algebraickou strukturu $(G,*)$ nazýváme *grupou* právě tehdy, když operace $*$ splňuje následující axiomy.

$$(\forall a,b,c \in G)\ (a * b) * c = a * (b * c) \text{ (asociativnost)},$$

$(\exists e \in G)(\forall a \in G)\ e * a = a * e = a$ (existence neutrálního prvku),

$(\forall a \in G)(\exists a^{-1} \in G)\ a * a^{-1} = a^{-1} * a = e$ (ke každému prvku existuje prvek inverzní).

Jestliže je navíc splněn axiom

$(\forall a, b \in G)\, a * b = b * a$ (komutativnost),

nazýváme grupu *grupou komutativní* resp. a*belovskou grupou*. [8]

Příklad 11:

Zjistěte, zda množina reálných čísel vzhledem k operaci sčítání tvoří (komutativní) grupu.

Aby operace sčítání na množině reálných čísel tvořila grupu, musí splňovat jisté podmínky.

Komutativnost:

$\forall a, b \in R : a + b = b + a$

$L = a + b$

$P = b + a$

$L = P$

Komutativní operace platí.

Asociativnost:

$\forall a, b, c \in R : (a + b) + c = a + (b + c)$

$L = (a + b) + c = a + b + c$

$P = a + (b + c) = a + b + c$

$L = P$

Asociativní zákon platí.

Existence neutrálního prvku:

$\exists e \in R\ \forall a \in R : a + e = a$

$a + e = a$

$e = 0$

Není třeba vyšetřovat i levý neutrální prvek, protože zde platí komutativnost. Neutrální prvek existuje a je roven 0.

Existence inverzního prvku:

$\forall a \in R\ \exists a^{-1} \in R : a + a^{-1} = a^{-1} + a = e$

$a + a^{-1} = a^{-1} + a = 0$

$a^{-1} = -a$

Inverzní prvek ke každému $a \in R$ také existuje.

Platí tedy, že množina reálných čísel s operací sčítání tvoří grupu.

Poznámka 4:

Množiny všech celých, racionálních, reálných čísel s operací sčítání tvoří grupu. Množina reálných čísel s operací násobení netvoří grupu. Neexistuje totiž inverzní prvek k číslu 0. Grupu však tvoří množina všech nenulových čísel s operací násobení. Množina všech celočíselných násobků pevného přirozeného čísla n s operací sčítání. Jako příklad zde můžeme ještě uvést nejmenší možnou grupu a to jednoprvkovou množinu $G = \{e\}$ s operací $e * e = e$.

2.2.4 Podgrupa

Definice 13:

Struktura $(H, \circ)$ je podgrupou grupy $(G, \cdot)$, právě když

1) $H \subseteq G$;
2) Operace „$\circ$“ je zúžením (restrikcí) operace „$\cdot$“ na množinu H, tj. $(\forall x, y \in H)(x \circ y = x \cdot y)$;
3) $(H, \circ)$ je grupa [4]

Věta 2:

Buď $(G,\cdot)$ grupa. Podmnožina H množina G je podgrupou v G, právě když

1) $H \neq \emptyset$,
2) $(\forall x, y \in H) x \cdot y^{-1} \in H$ [4]

Podgrupám se budeme věnovat později podrobněji (kapitola 6), pro tuto chvíli nám tato definice a věta stačí.

2.3 CVIČENÍ

V této části bychom si měli procvičit několik typů příkladů na binární operace, grupy, tj. látku, kterou jsme si v předešlé části definovali a ukázali pár příkladů.

Příklad 12:

Zjistěte, zda jsou sčítání a násobení binárními operacemi na množině reálných čísel.

sčítání: $(a,b) \in R \rightarrow (a+b) \in R$

násobení: $(a,b) \in R \rightarrow (a \cdot b) \in R$

Zjistili jsme, že operace sčítání a operace násobení jsou binárními operacemi v oboru reálných čísel. Na střední škole bychom použili tvrzení „množina R je uzavřená vzhledem k sčítání a násobení“.

Příklad 13:

Na množině $\mathbb{Z}$ je definována binární operace $*$ předpisem $\forall a,b \in \mathbb{Z} : a * b = 2(a+b)$. Zjistěte vlastnosti binární operace.

Komutativnost:

$\forall a,b \in \mathbb{Z} : a * b = b * a$

$L = 2(a+b)$

$P = 2(b+a)$

$L = P$

Komutativní zákon platí.

Asociativnost:

$\forall a,b,c \in \mathbb{Z} : (a*b)*c = a*(b*c)$

$L = 2(a+b)*c = 2\left[2(a+b)+c\right] = 4a+4b+2c$

$P = a*\left[2(b+c)\right] = 2\left[a+2(b+c)\right] = 2a+4b+4c$

$L \neq P$

Asociativní zákon neplatí.

Zákon krácení zleva:

$\forall a;b;c \in \mathbb{Z} : a*b = a*c \Rightarrow b = c$

Důkaz: $a*b = a*c$

$2(a+b) = 2(a+c)/:2$

$a+b = a+c$

$b = c$

Zákon krácení zleva platí. Zákon krácení zprava není třeba ověřovat, platí, což plyne z komutativnosti operace $*$.

Existence neutrálního prvku:

$a*b = 2(a+b)$

$\exists e \in \mathbb{Z}; \forall a \in \mathbb{Z} : a*e = a$

$2(a+e) = a$

$e = -\frac{a}{2}$

Pravý neutrální prvek není třeba vyšetřovat, protože operace $*$ je komutativní. Neutrální prvek $e \in Z$ by měl být pevný prvek, který nezávisí na a. Z tohoto důvodu neutrální prvek neexistuje.

Příklad 14:

Je dán grupoid $(R;*)$, kde $x*y=(x+2y)\cdot(2+xy)$. Zjistěte, zda operace $*$ je asociativní.

V případě, kdy máme podezření, že předložená operace asociativní není, bývá rychlejší metodou nalezení trojice prvků, pro niž neplatí asociativní zákon. To se v daném případě snadno podaří. Volme např. $x=1$, $y=-1$ a $z=2$.

Je $(x*y)*z=(1*-1)*2=(-1\cdot 1)*2=-1*2=3\cdot 0=0$,

$x*(y*z)=1*(-1*2)=1*(3\cdot 0)=1*0=1\cdot 2=2$.

Dostali jsme dva různé výsledky (0 a 2). Z tohoto důvodu grupoid $(R;*)$, kde $x*y=(x+2y)\cdot(2+xy)$, není pologrupou.

Příklad 15:

Zjistěte, zda grupoid $(Z,*)$ je grupou, je-li operace $*$ definována předpisem $\forall a,b\in Z\ \ a*b=|a\cdot b|$.

Aby se jednalo o grupu, musí být splněny tři podmínky. Grupoid musí být pologrupou, musí obsahovat neutrální prvek a inverzní prvek.

a) pologrupa

Nechť $a,b,c\in Z$ pak

$$(a*b)*c=|a\cdot b|*c=\big||a\cdot b|\cdot c\big|=|a\cdot b\cdot c|$$
$$a*(b*c)=a*|b\cdot c|=\big|a\cdot|b\cdot c|\big|=|a\cdot b\cdot c|$$

Grupoid $(Z,*)$ je pologrupou.

b) neutrální prvek

Musíme najít takový neutrální prvek $e\in G$, že pro libovolné $a\in G$ platí $e*a=a*e=a$.

Kdybychom si zvolili $a=-1$ a dosadili do předchozího řádku, vyjde $|e\cdot(-1)|=-1$, což nemůže platit.

Neutrální prvek neexistuje.

c) inverzní prvek

Inverzní prvky neexistují, protože neexistuje ani prvek neutrální.

Závěr: Grupoid $(G,*)$ není grupou, jelikož neobsahuje neutrální prvek.

Příklad 16:

Je dána množina M a operace $*$ na této množině. Rozhodněte, zda je $(M,*)$ grupoid. Pokud se bude jednat o grupoid, zjistěte, zda je daný grupoid dokonce pologrupou.

a) $M=\mathbb{N}$ **a pro libovolné** $x,y\in M$ **platí** $x*y=x-y$**,**

b) $M=\{-1,0,1\}$ **a pro libovolné** $x,y\in M$ **platí** $x*y=x\cdot y$**,**

c) $M=\{-1,0,1\}$ **a pro libovolné** $x,y\in M$ **platí** $x*y=x+y$**.**

a) Volme např. $x=3,y=5$. Pak ale $x*y=3*5=3-5\notin N$. Operace $*$ není na N neomezeně proveditelná a tudíž nejde o grupoid.

b) Volme např. $x=-1,y=0$. Pak $x*y=-1\cdot 0=0\in M$. Obdobně snadno zjistíme, že operace $*$ je na množině M proveditelná, tudíž se jedná o grupoid. Vyšetříme tedy ještě, zda je splněna podmínka asociativnosti.

$(x*y)*z=(x\cdot y)*z=x\cdot y\cdot z$

$x*(y*z)=x*(y\cdot z)=x\cdot y\cdot z$

Podmínka asociativnosti je splněna a tudíž můžeme říci, že se jedná o pologrupu.

c) O grupoid se nejedná. Lze to dokázat protipříkladem.

Volbou za $x=1$ a za $y=1$ dostáváme rovnost

$$x*y=x+y=1+1=2$$

Číslo 2 nepatří do množiny M, a z tohoto důvodu se o grupoid nejedná.

Příklad 17:

Na množině celých čísel Z vyšetřete binární operaci $*$ definovanou předpisem

$$a*b=(a+b)+1$$

Komutativnost:

$\forall a,b\in\mathbb{Z}: a*b=b*a$

$L=(a+b)+1$

$P=(b+a)+1$

$L=P$

Komutativní zákon platí.

Asociativnost:

$\forall a,b,c\in\mathbb{Z}: (a*b)*c=a*(b*c)$

$L=(a*b)*c=\left[(a+b)+1\right]*c=a+b+c+2$

$P=a*(b*c)=a*\left[(b+c)+1\right]=a+b+c+2$

$L=P$

Asociativní zákon platí.

Existence neutrálního prvku:

$a*b=(a+b)+1$

$\exists e\in\mathbb{Z};\forall a\in\mathbb{Z}: a*e=a$

$(a+e)+1=a$

$e=-1$

Neutrálním prvek je číslo -1.

Existence inverzního prvku:

$a*a^{-1}=e$

$a*a^{-1}=-1$

$a^{-1} = -1 - a$

Ke každému prvku existuje inverzní prvek a ten je dán rovností $a^{-1} = -1 - a$.

Poznámka 5:

V celé této práci budeme skládat zobrazení zleva.

Příklad 18:

Na množině $G = \{m, n, o, p\}$ je dána operace $*$ tabulkou. Rozhodněte, zda je grupoid $(G, *)$ komutativní, resp. asociativní, resp. jestli má neutrální prvek.

a)

$*$	***m***	***n***	***o***	***p***
m	*o*	*m*	*n*	*p*
n	*o*	*m*	*n*	*p*
o	*o*	*m*	*n*	*p*
p	*o*	*m*	*n*	*p*

b)

$*$	***m***	***n***	***o***	***p***
m	*o*	*m*	*n*	*m*
n	*m*	*m*	*p*	*n*
o	*n*	*p*	*n*	*o*
p	*m*	*n*	*o*	*p*

a) Ověřme, zda platí

$$(m * n) * p = m * (n * p)$$

$$(m * n) * p = m * p = p$$

$$m * (n * p) = m * p = p$$

$$p = p$$

Podmínka asociativnosti je v tomto případě splněna. Bylo by nutné ovařit ještě dalších 63 trojic. Snad se ale podaří najít nějaký protipříklad, pro který podmínka asociativnosti splněna není. Protipříkladem je například trojice *n*, *m*, *o*.

$$(n * m) * o = n * (m * o)$$

$$(n * m) * o = o * o = n$$

$$n * (m * o) = n * n = m$$

$$n \neq m$$

Nalezli jsme protipříklad a nyní můžeme říci, že grupoid není asociativní.

Tabulka není souměrná podle hlavní diagonály, proto není grupoid komutativní.

Prvky ve sloupcích i v řádcích se neopakují v záhlaví sloupců či řádků, a proto v tomto grupoidu neexistuje neutrální prvek.

b) Otestujeme, zda $(m*n)*o = m*(n*o)$.

Je $(m*n)*o = m*o = n$,

$m*(n*o) = m*p = m$,

$n \neq m$.

Grupoid není asociativní, jelikož nesplňuje podmínku asociativnosti.

Tabulka je souměrná podle hlavní diagonály a proto je grupoid komutativní.

Neutrálním prvkem je *p*, protože se prvky ve sloupci a v řádku opakují v záhlaví sloupce a řádku.

Příklad 19:

Je dána množina $M = \{x, y, z\}$ **a částečná tabulka operace** $*$ **na množině** M **.**

$*$	**x**	**y**	**z**
x	x	z	x
y	.	.	y
z	.	.	.

Doplňte tabulku tak, aby $(M, *)$

a) **byl grupoid s neutrálním prvkem;**
b) **byl grupoid, v němž má každý prvek inverzní prvek;**
c) **byla pologrupa.**

a)

∗	**x**	**y**	**z**
x	*x*	*z*	*x*
y	*z*	*x*	*y*
z	*x*	*y*	*z*

Neutrálním prvkem je **z**, protože se prvky ve sloupci/řádku shodují se záhlavím sloupce/řádku.

b)

∗	**x**	**y**	**z**
x	x	*z*	x
y	**z**	y	y
z	x	y	*z*

Inverzním prvkem k prvku *x* je *y*, k *y* je prvek *x* a prvek *z* je inverzní sám k sobě.

c)

Vypočtěme $(x*x)*y = x*y = z$ a $x*(x*y) = x*y = x$. Tím je jasné, že již v částečné tabulce je možné najít trojici prvků, pro něž neplatí asociativní zákon. Z dané částečné operační tabulky tedy nelze vytvořit operační tabulku pologrupy. Museli jsme ovšem danou trojici prvků objevit. Podobné hledání „vhodné“ trojice prvků může být dost náročné na čas a soustředěnost člověka.

Viděli jsme, že ověřování asociativity je v konečných algebraických strukturách často časově dost náročné. Mohly by tuto práci převzít programy počítačové algebry jako Maple či Mathematica? O nich je dobře známo, že zvládají mnohé výpočty z oblasti klasické i lineární algebry či matematické analýzy nebo pravděpodobnosti a statistiky. V poslední době se v nich objevují povely či balíčky, obsahující funkce, které se týkají algebraických struktur s konečnými nosiči, resp. teorie grup. Prozkoumejme alespoň některé funkce balíčku (package) Magna v programu Maple 17.

Již při zápisu konečné algebraické struktury Cayleyho tabulkou lze ušetřit trochu práce, dohodneme-li se, že její prvky očíslujeme přirozenými čísly 1, 2, …, *n*. V takovém

případě již nemusíme zadávat záhlaví řádků ani sloupců a pracujeme jakoby s maticemi. Po „zavolání“ balíčku Magma využijeme některé jeho povely, týkající se zkoumání asociativnosti operace. Program nám v okamžiku zjistí, že existuje 24 pologrup na množině G = $\{1, 2, 3\}$. Můžeme si je nechat vypsat do seznamu, což učiní další povel. Nakonec si ale povšimneme, že v prvním řádku matice kódující částečnou operační tabulku z příkladu 19 bude 1, 3, 1 a takovýto první řádek se v žádné ze 24 operačních tabulek vydaných počítačem nenachází. I odtud je vidět, že úkol daný v bodě c) příkladu 19 nelze splnit.

```
> with( Magma ) :
Enumerate( 3,'associative' );
```

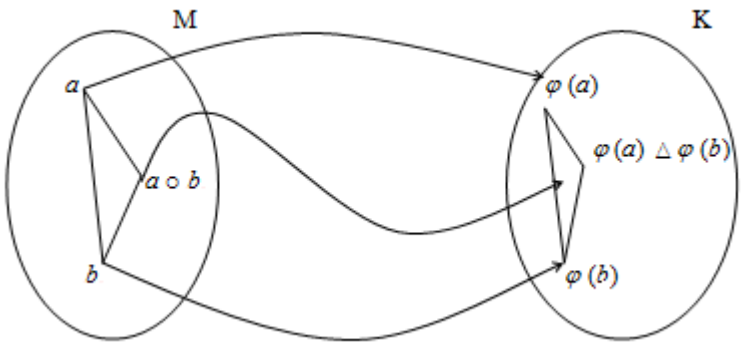
24

```
> Enumerate( 3, 'associative', 'output' = 'list' );
```

$$\left[\begin{bmatrix}1&1&1\\1&1&1\\1&1&1\end{bmatrix},\begin{bmatrix}1&1&1\\1&1&1\\1&1&2\end{bmatrix},\begin{bmatrix}1&1&1\\1&1&1\\1&1&3\end{bmatrix},\begin{bmatrix}1&1&1\\1&1&1\\1&2&3\end{bmatrix},\begin{bmatrix}1&1&1\\1&1&1\\3&3&3\end{bmatrix},\begin{bmatrix}1&1&1\\1&1&2\\1&1&3\end{bmatrix},\begin{bmatrix}1&1&1\\1&1&2\\1&2&3\end{bmatrix},\begin{bmatrix}1&1&1\\1&2&1\\1&1&3\end{bmatrix},\right.$$
$$\begin{bmatrix}1&1&1\\1&2&1\\3&3&3\end{bmatrix},\begin{bmatrix}1&1&1\\1&2&2\\1&2&2\end{bmatrix},\begin{bmatrix}1&1&1\\1&2&2\\1&2&3\end{bmatrix},\begin{bmatrix}1&1&1\\1&2&2\\1&3&3\end{bmatrix},\begin{bmatrix}1&1&1\\1&2&3\\1&2&3\end{bmatrix},\begin{bmatrix}1&1&1\\1&2&3\\1&3&2\end{bmatrix},\begin{bmatrix}1&1&1\\1&2&3\\3&3&3\end{bmatrix},\begin{bmatrix}1&1&1\\2&2&2\\3&3&3\end{bmatrix},$$
$$\left.\begin{bmatrix}1&1&3\\1&1&3\\1&1&3\end{bmatrix},\begin{bmatrix}1&1&3\\1&1&3\\3&3&1\end{bmatrix},\begin{bmatrix}1&1&3\\1&2&3\\1&1&3\end{bmatrix},\begin{bmatrix}1&1&3\\1&2&3\\1&3&3\end{bmatrix},\begin{bmatrix}1&1&3\\1&2&3\\3&3&1\end{bmatrix},\begin{bmatrix}1&2&2\\2&1&1\\2&1&1\end{bmatrix},\begin{bmatrix}1&2&3\\1&2&3\\1&2&3\end{bmatrix},\begin{bmatrix}1&2&3\\2&3&1\\3&1&2\end{bmatrix}\right]$$

3 HOMOMORFIZMUS A IZOMORFIZMUS

Tyto dva pojmy známe již z geometrie. Představují totiž zobrazení, která zachovávají určité vlastnosti. Podobně je tomu i v algebře. Zobrazení homomorfizmus a izomorfizmus si můžeme představit jako dva podobné a shodné trojúhelníky. Homomorfizmus (podobnost) zachovává pouze některé vlastnosti binárních operací. Izomorfizmus (shodnost) zachovává všechny vlastnosti binárních operací.



Obrázek 1: Homomorfizmus

Definice 14:

Zobrazení $\varphi: M \to K$ nazveme homomorfním zobrazením algebraické struktury (M, o) do algebraické struktury $(K, \triangle)$ právě tehdy, když platí

$$(\forall a, b \in M)\ \varphi(a \circ b) = \varphi(a) \triangle \varphi(b)\,.$$

Jestliže zobrazení φ je surjektivní, nazýváme algebraickou strukturu $(K, \triangle)$ homomorfním obrazem algebraické struktury (M, o) a budeme značit

$$(M, o) \sim (K, \triangle)\,.$$

Jestliže zobrazení φ je bijektivní, potom algebraické struktury (M, o), $(K, \triangle)$ nazýváme izomorfními a budeme značit

$$(M, o) \cong (K, \triangle)\,.\ [8]$$

Věta 3:

Nechť $(M,o)\sim(K,\triangle)$, tj. algebraická struktura $(K,\triangle)$ je homomorfním obrazem algebraické struktury (M,o), potom platí:

1) Jestliže operace o je komutativní, je i operace $\triangle$ komutativní.
2) Jestliže operace o je asociativní, je i operace $\triangle$ asociativní.
3) Jestliže operace o má neutrální prvek, má i operace $\triangle$ neutrální prvek.
4) Jestliže operace o má agresivní prvek, má i operace $\triangle$ agresivní prvek.
5) Pro obraz inverzního prvku platí $\varphi\left(a^{-1}\right)=\left[\varphi(a)\right]^{-1}$. (Zachování inverzního prvku.)
6) Jestliže operace o je idempotentní, je i operace $\triangle$ idempotentní. [8]

Definice 15:

Nechť $\varphi: G\to H$ je nějaký homomorfizmus grup. Jeho obraz je množina

$$\mathrm{Im}(\varphi)=\varphi * G=\{\varphi(g); g\in G\}$$

Tato podmnožina grupy H je uzavřená vzhledem na součin, inverzní prvky a jednotku a je to teda podgrupa grupy H. Na druhé straně množina

$$Ker(\varphi)=\{g; g\in G, \varphi(g)=1\in H\}^{*}$$

Je podgrupou grupy G a nazýváme ji jádrem homomorfizmu φ. Přitom platí:

1) $\varphi: G\to H$ je epimorfizmus $\leftrightarrow$ $\mathrm{Im}(\varphi)=H$
2) $\varphi: G\to H$ je monomorfizmus $\leftrightarrow$ $Ker(\varphi)=1$
3) $\varphi: G\to H$ je izomorfizmus $\leftrightarrow$ $Ker(\varphi)=1$ a $\mathrm{Im}(\varphi)=H$ [3]

Příklad 20:

Uvažujeme zobrazení φ definované předpisem:

1) $\varphi:(\mathbb{R}^{+},\cdot)\to(\mathbb{R},+)$

$(\forall x\in\mathbb{R}^{+})\ \varphi(x)=\log x$

2) $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$

$(\forall x \in \mathbb{Z})\ \varphi(x) = x - 1$

3) $\varphi : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$

$(\forall x \in \mathbb{R})\varphi(x) = e^x$

1)

- φ je bijekce
- $(\forall x, y \in \mathbb{R}^+)\ \varphi(x \cdot y) = \log(x \cdot y) = \log x + \log y = \varphi(x) + \varphi(y)$

φ je tedy izomorfizmus.

2)

- $(\forall x, y \in \mathbb{Z})\varphi(x + y) = x + y - 1$

$$\varphi(x) + \varphi(y) = x - 1 + y - 1 = x + y - 2$$

Tedy $\varphi(x + y) \neq \varphi(x) + \varphi(y)$, tj. φ není homomorfizmus.

3)

- $(\forall x, y \in \mathbb{R})\ \varphi(x \cdot y) = e^x \cdot e^y = e^{(x+y)} = \varphi(x) \cdot \varphi(y)$

φ tedy je izomorfizmus.

4 KONEČNÉ GRUPY

Definice 16:

Grupa $(G,\cdot)$ se nazývá nekonečná, je-li její nosič, tj. množina G, nekonečná. V opačném případě říkáme, že $(G,\cdot)$ je konečná grupa a řádem této grupy rozumíme počet prvků množiny G. [2]

Jako příklad bychom mohli uvést grupu shodností reprodukující rovnostranný trojúhelník. Tato grupa je konečná řádu 6.

Příklad 21:

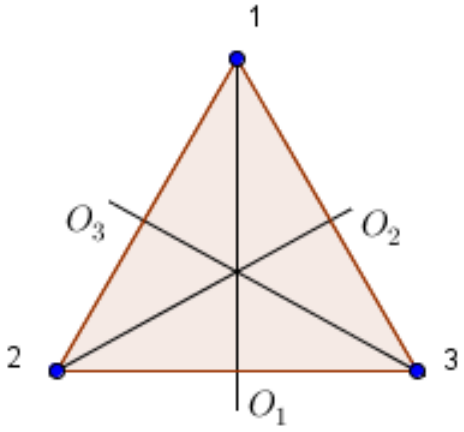
Určete všechny shodnosti v rovině reprodukující rovnostranný trojúhelník. Sestavte Cayleyovu tabulku zachycující operaci skládání těchto shodností.

Shodnosti reprodukující rovnostranný trojúhelník v rovině jsou identita (I), rotace (R) a osová souměrnost (O). Otočením trojúhelníka o 120^0, resp. 240^0, resp. 360^0 po směru hodinových ručiček dostáváme 3 ze symetrií (identitu a 2 rotace). Značíme (I,R,R^2). Překlopením trojúhelníka T okolo výšky procházející vrcholem 1,2,3 dostáváme další 3 symetrie O_1,O_2,O_3. Dostáváme tak množinu G šesti symetrií trojúhelníka T:

Přijmeme označení pro:

$$G=\{1,R,R^2,O_1,O_2,O_3\},$$

a situaci můžeme nakreslit následovně.



Obrázek 2: Shodná zobrazení rovnostranného trojúhelníka v rovině

Sestavíme Cayleyovu tabulku, která zachycuje binární operaci skládání shodností reprodukující rovnostranný trojúhelník. Shodnosti budeme skládat následovně (poznámka 5). Vezmeme-li si například $R \circ O_1 = O_3$, začínáme zleva R a k němu přidáváme O_1.

Tabulka 1: Cayleyho tabulka reprodukující rovnostranný trojúhelník

*	I	R	R^2	O_1	O_2	O_3
I	I	R	R^2	O_1	O_2	O_3
R	R	R^2	I	O_3	O_1	O_2
R^2	R^2	I	R	O_2	O_3	O_1
O_1	O_1	O_2	O_3	I	R	R^2
O_2	O_2	O_3	O_1	R^2	I	R
O_3	O_3	O_1	O_2	R	R^2	I

Věta 4:

Nechť $(G,\cdot)$ je grupa, $\emptyset \neq H \leq G$. $(H,\cdot)$ je podgrupou grupy $(G,\cdot)$ právě tehdy, když pro všechna $a,b \in H$ je $a \cdot b^{-1} \in H$. [2]

Poznámka 6:

Každá grupa je podgrupou sama sebe a podgrupou kterékoli grupy $(G,\cdot)$ je vždy jednotková podgrupa, tj. podgrupa obsahující pouze neutrální prvek. Tyto dvě podgrupy se nazývají nevlastní a všechny ostatní podgrupy se nazývají vlastní.

Příklad 22:

Nalezněte všechny podgrupy grupy shodností v rovině, reprodukujících rovnostranný trojúhelník. Kromě nevlastních podgrup nalezneme zřejmě tyto vlastní podgrupy: $H_1 = (\{R, R^2, I\}, \circ)$ - podgrupa rotací; $H_2 = (\{I, O_1\}, \circ)$, $H_3 = (\{I, O_2\}, \circ)$, $H_4 = (\{I, O_3\}, \circ)$. Všimněme si, že řád kterékoli podgrupy H_i, $i = 1,2,3,4$ dělí řád grupy G, tj. číslo 6.

Věta 5:

Průnik libovolného neprázdného systému podgrup grupy G je opět podgrupa grupy G. [2]

Definice 17:

Nechť $(G,\cdot)$ je grupa a g její libovolný prvek. Existuje-li nejmenší kladné celé číslo n tak, že $g^n = 1$, pak říkáme, že n je řád prvku g, resp. že prvek g je řádu n v grupě $(G,\cdot)$.

Píšeme: $n = o(g)$, resp. $n = |g|$.

Jestliže takové číslo n neexistuje, pak říkáme, že prvek g je nekonečného řádu. [7]

Příklad 23:

Pokuste se popsat grupy řádu 6.

Tento příklad si rozdělíme na dvě části.

1. V první části uvedeme tabulku cyklické grupy řádu 6. Jejím generátorem je prvek a, přičemž platí $a^6 = 1$.

Tabulka 2: Cayleyova tabulka cyklické grupy řádu 6

*	I	a	a^2	a^3	a^4	a^5
I	I	**a**	$\mathbf{a^2}$	$\mathbf{a^3}$	$\mathbf{a^4}$	$\mathbf{a^5}$
a	**a**	$\mathbf{a^2}$	$\mathbf{a^3}$	$\mathbf{a^4}$	$\mathbf{a^5}$	I
$\mathbf{a^2}$	$\mathbf{a^2}$	$\mathbf{a^3}$	$\mathbf{a^4}$	$\mathbf{a^5}$	I	a
$\mathbf{a^3}$	$\mathbf{a^3}$	$\mathbf{a^4}$	$\mathbf{a^5}$	I	a	$\mathbf{a^2}$
$\mathbf{a^4}$	$\mathbf{a^4}$	$\mathbf{a^5}$	I	a	$\mathbf{a^2}$	$\mathbf{a^3}$
$\mathbf{a^5}$	$\mathbf{a^5}$	I	a	$\mathbf{a^2}$	$\mathbf{a^3}$	$\mathbf{a^4}$

2. Ve druhé části se budeme zabývat necyklickou grupou řádu 6, jejíž nejednotkové prvky jsou řádu 2 nebo 3. Jiný řád mít nemohou, což plyne z důsledku Lagrangeovy věty. Nejdříve ukážeme, že v grupě musí existovat prvek řádu 3. Nejednotkové prvky řádu 2 by v grupě G existovaly v opačném případě, např. $a \neq b$. To by ovšem znamenalo, že grupa G by obsahovala Kleinovu čtyřgrupu H, což není možné v důsledku Langrangeovy věty.

V G tedy existuje prvek $a \neq 1$, kdy $a^3 = 1$. Kromě prvků 1, a, $a^2 = b$ musí grupa G obsahovat ještě jeden prvek c. Lehce zjistíme, že i prvky $ac = d$ a $ac^2 = e$. Tímto

způsobem jsme zjistili šest prvků grupy G, které budeme potřebovat ke konstrukci cyklické grupy řádu 6.

Dalším krokem bude ukázat, že $c^2 = 1$. V grupě G platí zákon krácení zleva i zprava, a proto vyloučíme možnosti $c^2 = c$, $c^2 = ac$ a $c^2 = a^2c$. Důvodem je, že prvek c je různý od prvků 1, a, a^2. Kdyby platilo $c^2 \neq 1$, potom by prvek c měl řád 3, a tedy $c^3 = 1$. Tímto dostáváme však spor, pokud by $c^2 = a$, platilo by $1 = c^3 = ac = d$ a nebo také pokud $c^2 = a^2$, potom $1 = c^3 = a^2c = e$. Je splněna možnost $c^2 = 1$.

Obdobně ukážeme, že $\mathrm{d}^2 = 1$, resp. $\mathrm{e}^2 = 1$. Prvek d, resp. e je různý od prvků 1, a, a^2. Zde platí také zákon krácení zleva i zprava a proto můžeme možnosti $d^2 = d$, $d^2 = ad$, $d^2 = a^2d$, resp. $e^2 = e$, $e^2 = ae$, $e^2 = a^2e$ vyloučit, protože by také vedly ke sporu. Kdyby neplatilo $d^2 = 1$, resp. $e^2 = 1$, potom by prvek d, resp. e měl řád 3, a tedy $d^3 = 1$, resp. $e^3 = 1$.

Pokud $d^2 = a$, resp. $e^2 = a$, platilo by $1 = d^3 = ad = e$, resp. $1 = e^3 = ae = c$, čímž se dostáváme opět do sporu. Další možnost, která vede ke sporu je $d^2 = a^2$, resp. $e^2 = a^2$. Muselo by totiž platit $1 = d^2 = a^2d = c$, resp. $1 = e^2 = a^2e = d$. To pro nás znamená $d^2 = e^2 = 1$.

Sestojíme tedy Cayleyovu tabulku na množině $M = \{1, a, b, c, d, e\}$

Tabulka 3: Cayleyova tabulka necyklické grupy řádu 6

*	**1**	**a**	**b**	**c**	**d**	**e**
1	1	a	b	c	d	e
a	a	b	1	d	e	c
b	b	1	a	e	c	d
c	c	e	d	1	b	a
d	d	c	e	a	1	b
e	e	d	c	b	a	1

Každá cyklická grupa je grupou komutativní. Z tabulky lze vyčíst, že tato grupa není komutativní. To je další důvod, proč nemůže jít o cyklickou grupu.

5 CYKLICKÉ GRUPY

Definice 18:

Buď M podmnožina grupy G. Průnik všech podgrup grupy G obsahujících množinu M nazýváme podgrupou generovanou množinou M a značíme $\{M\}$. Jestliže $\{M\}=G$, pak M nazýváme množinou generátorů grupy G. Grupa G generovaná jednoprvkovou množinou $\{g\}$ se nazývá cyklická. Píšeme $G=\langle g\rangle$. [2]

Věta 6:

Buď M podmnožina grupy G. Je-li $M=\emptyset$, pak $\{M\}=\{e\}$ (tj. neprázdná množina generuje triviální podgrupu). Je-li $M\neq\emptyset$, pak $\{M\}=\left\{m_1^{e_1}\cdot m_2^{e_2}\cdot\ldots\cdot m_n^{e_n};m_i\notin M,e_i\in Z,i=1,2,\ldots,n\in N\right\}$. (Neprázdná množina generátorů M nageneruje tudíž množinu „slov“ konečné délky tvořených celočíselnými mocninami prvků množiny M). [2]

Věta 7:

Buď $<a>$ cyklická grupa. Pak buď všechny celočíselné mocniny prvku a jsou navzájem různé a cyklická grupa $<a>$ je nekonečná, nebo existuje přirozené číslo n tak, že $<a>=\left\{a,a^2,\ldots,a^n=e\right\}$. Přitom $a^m=e$ právě když n|m. [2]

Věta 8:

Buď $<a>$ konečná cyklická grupa řádu n. Pak $<a^k>=<a>$ právě tehdy, když $(k,n)=1$. (Připomeňme, že symbolem (k,n) značíme největší společný dělitel čísel k, n). [2]

Tvrzení:

1) Každá podgrupa cyklické grupy je opět cyklická.
2) Je-li $<a>$ konečná cyklická grupa řádu n a d přirozené číslo dělící n, $n=d\cdot m$, pak $<a>$ obsahuje jedinou podgrupu řádu d, totiž $<a^m>$. [2]

Z toho tvrzení vyplývá, že konečná cyklická grupa $<a>$ řádu n má právě tolik různých podgrup, kolik přirozených dělitelů má číslo n.

Definice 19:

Buď H podgrupa grupy G, $a \in G$. Pak množinu $aH = \{ah, h \in H\}$/resp. $Ha = \{ha, h \in H\}$/ nazýváme levou/resp. pravou/třídou grupy G podle podgrupy H určenou prvkem a. [2]

Příklad 24:

Je dána grupa G shodností v rovině reprodukujících rovnostranný trojúhelník ABC (viz příklad 17) tj. $G = (\{I, O_1, O_2, O_3, R, R^2\}, \circ)$. Podgrupu H označme podgrupou rotací, $H = (\{I, R, R^2\}, \circ)$. Utvořme všechny levé třídy grupy G podle podgrupy H.

Máme

$$IH = \{I, R, R^2\} \qquad O_1H = \{O_1, O_2, O_3\}$$

$$RH = \{R, R^2, I\} \qquad O_2H = \{O_2, O_1, O_3\}$$

$$R^2H = \{R^2, R, I\} \qquad O_3H = \{O_3, O_2, O_1\}.$$

Ukazuje se, že každé dvě levé/pravé/ třídy se buďto rovnají, nebo jsou disjunktní. Vznikl tedy rozklad množiny $\{I, O_1, O_2, O_3, R, R^2\}$ na třídy. To platí obecně.

Věta 9:

Každé dvě levé třídy grupy G podle podgrupy H se buďto rovnají nebo jsou disjunktní. [2]

5.1 Lagrangeova věta:

Lagrangeova věta jasně vymezuje řády podgrup, které jsou možné.

Věta 10:

Buď H podgrupa konečné grupy G. Potom $|G| = H.[G:H]$. Přitom $|G|, |H|$ značí řád grup G, H. [2]

Důkaz:

Levé třídy grupy G podle podgrupy H tvoří rozklad množiny G na třídy. Těchto tříd je $[G:H]$ a každé dvě mají stejný počet prvků jako podgrupa H, tj. $|H|$. Celkem tedy $|G| = |H|.[G:H]$. [2]

Důsledek:

1) Řád podgrupy i index podgrupy dané konečné grupy G dělí vždy řád grupy G.
2) V konečné grupě G dělí číslo $o(g)$ číslo $|G|$, tj. řád prvku g /tj. řád jím generované cyklické grupy/ dělí číslo G.
3) Konečné grupy prvočíselného řádu mají pouze nevlastní podgrupy. [2]

5.2 Eulerova funkce

Definice 20:

Funkce φ definovaná předpisem: pro každé $n \in N$ značí $\varphi(n)$ počet všech čísel $k \in N_0$ takových, že $k \leq n$ a že $D(k,n) = 1$, se nazývá Eulerova funkce. [4]

Věta 11:

Pro Eulerovu funkci φ platí $(\forall a,b \in N_0) D(a,b) = 1 \Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$.

Toto tvrzení zachycuje takzvanou multiplikativnost, jež je velmi důležitou vlastností Eulerovy funkce. [4]. Přímým výpočtem se snadno ověří, že pro prvočíslo *p* a *n* $\in$ N platí $\varphi(p) = p - 1$, $\varphi(p^n) = p^n\left(1 - \frac{1}{p}\right)$.

Příklad 25:

Udejte všechny možné generátory cyklické grupy Z_8.

Abychom nalezli prvek n ze Z_8, jež by generoval tuto grupu, je nutné a stačí, aby n nebyl soudělný s 8. Proto dostáváme pouze čísla 1, 3, 5 a 7.

Příklad 26:

Dokažte, že pro grupu Z_{14} je možné nalézt šest různých generátorů.

Tento důkaz lze provést dvěma způsoby. První způsob je elementární, ale vhodný jen pro grupy s malým počtem prvků. Grupa Z_{14} nemá mnoho prvků a z toho důvodu dokážeme generátory vypsat. Musíme vypsat čísla, jež jsou nesoudělná s číslem 14 v Z. Generátory této grupy jsou 1, 3, 5, 9, 11 a 13.

Druhý způsob je v tomto příkladu sice zdlouhavější, ale jeho postup je výhodnější pro jiné příklady. Nemůžeme se být jisti, že vždy dostaneme grupu, ve které dokážeme vypsat všechny generátory.

Pro tuto variantu použijeme Eulerovu funkci, kterou jsme si zde před chvílí definovali. Určíme tedy hodnotu Eulerovy funkce. Nejprve nalezneme prvočíselný rozklad čísla $14 = 2 \cdot 7$. Počet generátorů cyklické grupy Z_{14} podle rovnice $\varphi(14) = (2-1) \cdot (7-1) = 6$ je šest.

Příklad 27:

Určete počet generátorů cyklické grupy G řádu 550.

Zde vidíme, že vypisováním generátorů by bylo velmi zdlouhavé, a proto musíme využít Eulerovy funkce. Prvním krokem bude výpis prvočíselného rozkladu čísla $550 = 2 \cdot 5^2 \cdot 11$.

Vypočteme $\varphi(550) = \varphi(2) \cdot \varphi\left(5^2\right) \cdot \varphi(11)$,

$$\varphi(550) = (2-1) \cdot 5^2 \cdot \left(1 - \frac{1}{5}\right) \cdot (11-1) = 200 .$$

Počet generátorů cyklické grupy G je tedy 200.

6 NORMÁLNÍ PODGRUPY

Definice 21:

Řekneme, že podgrupa H grupy G je normální podgrupou grupy G (značíme $H \triangleleft G$), jestliže pro každé $g \in G$ je $gH = Hg$. Jednotková grupa a grupa G jsou normálními podgrupami grupy G (tzv. nevlastní normální podgrupy). Všechny ostatní normální podgrupy grupy G se nazývají vlastní. [2]

Definice 22:

Indexem podgrupy H v grupě G budeme rozumět počet tříd v levém resp. pravém rozkladu grupy G podle podgrupy H. Užíváme značení $[G:H]$. [2]

Věta 12:

Nechť H je podgrupa grupy G. Jestliže $[G:H]=2$, pak $H \triangleleft G$. [7]

Důkaz:

Je-li $[G:H]=2$, pak v G existují právě dvě různé levé třídy, a to $H = 1H$, druhá je aH pro některé $a \notin H$. Nechť $h \in H, g \in G$. Předpokládejme, že $g^{-1}hg \notin H$.

1. Jestliže $g \in H$, pak $g^{-1} \in H$ neboť H je podgrupa a tedy $g^{-1}hg \in H$, což je spor.
2. Jestliže $g \notin H$, pak $g^{-1} \notin H$ tedy pak $g^{-1}H \neq H$. Jelikož $[G:H]=2$, je $aH = g^{-1}H$, a tedy $g^{-1}hg \notin H$, takže $g^{-1}hg \in g^{-1}H$. Odtud dostáváme $g^{-1}hg = g^{-1}h_0$ pro některé $h_0 \in H$, tedy $hg = h_0$, tj. $g = h^{-1}h_0 \in H$, což je opět spor. Musí tedy platit $g^{-1}hg \in H$, tj. $H \triangleleft G$. [7]

Věta 13:

Průnik libovolné množiny normálních podgrup grupy G je normální podgrupou grupy G. [6]

Věta 14:

Podgrupa vnořená libovolnou množinou normálních podgrup grupy G je také normální podgrupou grupy G. [6]

Poznámka 7:

Můžeme konstatovat, že všechny podgrupy Abelovy grupy jsou zároveň normálními podgrupami. Normálními podgrupami grupy G jsou sama grupa G a jednotková podgrupa E. Grupa G se nazývá jednoduchá, pokud neobsahuje jiné normální podgrupy než G a E. [6]

Věta 15:

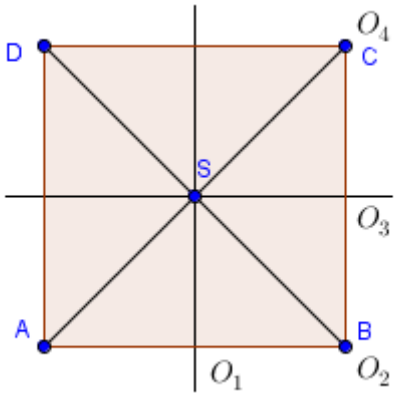
Jednoduchou Abelovou grupou je každá konečná cyklická grupa prvočíselného řádu a jiné jednoduché Abelovy grupy neexistují. [6]

Příklad 28:

Nechť je dána grupa shodností v rovině G reprodukující čtverec $ABCD$ s binární operací * skládání shodných zobrazení a podgrupa rotací $H = \{I, R, R^2, R^3\}$. Zjistěte, zda se jedná o normální podgrupu.

Shodných zobrazení v rovině, která zobrazují čtverec $ABCD$ na sebe, je 8. Těmito zobrazeními jsou identita (I), rotace (R, R^2, R^3) se středem S o 90° resp. 180°, resp. 270° (pro tento příklad budeme uvažovat rotaci po směru hodinových ručiček) a čtyři osové souměrnosti (O_1, O_2, O_3, O_4) pomocí os O_1, O_2, O_3 *a* O_4.

Abychom mohli pokračovat dál, sestrojíme čtverec s osami souměrnosti a napíšeme si operační tabulku.



Obrázek 3: Shodná zobrazení čtverce ABCD

Tabulka 4: Operační tabulka shodných zobrazení čtverce ABCD

*	**I**	**R**	**R^2**	**R^3**	**O_1**	**O_2**	**O_3**	**O_4**
I	I	R	R^2	R^3	O_1	O_2	O_3	O_4
R	R	R^2	R^3	I	O_2	O_3	O_4	O_1
R^2	R^2	R^3	I	R	O_3	O_4	O_1	O_2
R^3	R^3	I	R	R^2	O_4	O_1	O_2	O_3
O_1	O_1	O_4	O_3	O_2	I	R^3	R^2	R
O_2	O_2	O_1	O_4	O_3	R	I	R^3	R^2
O_3	O_3	O_2	O_1	O_4	R^2	R	I	R^3
O_4	O_4	O_3	O_2	O_1	R^3	R^2	R	I

Nejprve sestrojíme všechny levé třídy grupy G podle podgrupy H:

$$I\ H = \{I, R, R^2, R^3\} \qquad O_1\ H = \{O_1, O_4, O_3, O_2\}$$

$$R\ H = \{R, R^2, R^3, I\} \qquad O_2\ H = \{O_2, O_1, O_4, O_3\}$$

$$R^2\ H = \{R^2, R^3, I, R\} \qquad O_3\ H = \{O_3, O_2, O_1, O_4\}$$

$$R^3\ H = \{R^3, I, R, R^2\} \qquad O_4\ H = \{O_4, O_3, O_2, O_1\}$$

Nyní vytvoříme všechny pravé třídy grupy G podle podgrupy H:

$$H\ I = \{I, R, R^2, R^3\} \qquad H\ O_1 = \{O_1, O_4, O_3, O_2\}$$

$$H\ R = \{R, R^2, R^3, I\} \qquad H\ O_2 = \{O_2, O_1, O_4, O_3\}$$

$$H\ R^2 = \{R^2, R^3, I, R\} \qquad H\ O_3 = \{O_3, O_2, O_1, O_4\}$$

$$H\ R^3 = \{R^3, I, R, R^2\} \qquad H\ O_4 = \{O_4, O_3, O_2, O_1\}$$

Následně zjistíme, zda se nám levé a pravé třídy rovnají, platí-li tedy předpis z definice 23, že $gH = Hg$:

$$I\ H = \{I, R, R^2, R^3\} = H\ I \qquad O_1\ H = \{O_1, O_4, O_3, O_2\} = H\ O_1$$

$$R\ H = \{R, R^2, R^3, I\} = H\ R \qquad O_2\ H = \{O_2, O_1, O_4, O_3\} = H\ O_2$$

$$R^2\ H = \{R^2, R^3, I, R\} = H\ R^2 \qquad O_3\ H = \{O_3, O_2, O_1, O_4\} = H\ O_3$$

$$R^3\ H = \{R^3, I, R, R^2\} = R^3\ H \qquad O_4\ H = \{O_4, O_3, O_2, O_1\} = H\ O_4$$

Zjišťujeme tedy, že podgrupa H je normální podgrupou grupy G, tj. platí $H \lhd G$.

Tento příklad lze řešit ještě jiným efektivnějším postupem s využitím definice 22 a věty 12. Grupa G má osm prvků. Její podgrupa H má pouze čtyři prvky. Je $[G:H] = 2$. Existují tedy právě dvě levé a právě dvě pravé třídy grupy G podle podgrupy H. Pokud je $g \in H$, je $gH = H = Hg$. Jestliže $g \notin H$, je $gH = G - H = Hg$. Je tedy $H \lhd G$.

Zároveň jsme na tomto příkladu dokázali tvrzení věty 12 a potvrdili i její důkaz.

Výsledek toho příkladu byl předem jasný. Mohli bychom zkusit vzít jinou podgrupu $H = \{I, O_1\}$ a zjistit, zda je normální podgrupou grupy G.

Sestrojením levých tříd a následně pravých tříd grupy G podle podgrupy H zjistíme, že levé a pravé třídy se nerovnají. Tato podgrupa H tedy není normální podgrupou grupy G.

7 SYMETRICKÉ A ALTERNUJÍCÍ GRUPY

Shodné zobrazení v rovině resp. v prostoru, které zobrazuje daný objekt sám na sebe, nazýváme symetrií útvaru v rovině resp. v prostoru. Množinou všech symetrií tohoto útvaru spolu s operací skládání zobrazení je grupa symetrií.

V kapitole 2.2.3 jsme si definovali grupu. Víme tedy, že grupa splňuje asociativitu, obsahuje neutrální i inverzní prvek. V grupě symetrií je tomu stejně. Pokud složíme dvě symetrie, dostáváme opět symetrii. Již tedy vidíme, že podmínka asociativnosti je splněna, jelikož skládání zobrazení je asociativní. Do množiny symetrií patří identické zobrazení, které nechává daný útvar na místě. Z toho vyplývá, že neutrální prvek také existuje. Zbývá už jen dokázat existenci inverzního prvku, kterou dokážeme následujícím tvrzením. Symetrie jsou bijektivními zobrazeními, a proto je zřejmé, že ke každé symetrii nutně existuje symetrie inverzní.

Definice 23:

Množina všech permutací na $M=\{1,2,...,n\}$ je vzhledem k operaci násobení permutací grupou, nazýváme ji symetrická grupa stupně n a značíme S_n. [7]

Definice 24:

Nechť $M=\{1,2,...,n\}$ je množina, s_1, s_2, …, s_k její prvky a π permutace na množině M taková, že $\pi(s_1)=s_2$, $\pi(s_2)=s_3$, …, $\pi(s_{k-1})=s_k$, $\pi(s_k)=s_1$ a každý $s\in M=\{s_1,\ s_2\ ,\ ...,s_k\}$ je samodružným bodem permutace π. Permutaci π pak nazýváme cyklem a zapisujeme $\pi=(s_1,\ s_2,\ ...,\ s_k)$. Číslo k se nazývá délka cyklu. Cykl délky dva se nazývá transpozice. Dva cykly $(s_1,\ s_2,\ ...,\ s_k)$ a $(t_1,\ t_2,\ ...,\ t_m)$ se nazývají nezávislé, jestliže $\{s_1,\ s_2,\ ...,\ s_k\}\cap\{t_1,\ t_2,\ ...,\ t_m\}=\varnothing$. Konečná množina cyklů se nazývá nezávislá, jsou-li každé dva cykly z této množiny nezávislé. V opačném případě říkáme, že cykly jsou závislé. [2]

Definice 25:

Řekneme, že permutace π je sudá a její znaménko značíme $\pi = 1$, jestliže ji lze rozložit v součin sudého počtu transpozic. V opačném případě říkáme, že permutace π je lichá a její znaménko značíme $\pi = -1$. [2]

Významné postavení mezi grupami symetrií zaujímají dihedrální grupy D_n, jež jsou grupami symetrií pravidelných n-úhelníků pro $n \geq 3$ spolu s operací skládání. Těmito symetriemi jsou rotace a osová souměrnost. Počet symetrií pravidelného n-úhelníku určuje

- n-rotací

  pravidelný n-úhelník lze otočit okolo svého středu o úhel $\frac{2k\pi}{n}$, kde $k = 0,...,n-1$, aby se zobrazil opět sám na sebe (pokud $k = 0$ jedná se o identickou symetrii)
- n-osových souměrností, jak pro liché tak i pro sudé n:

  liché n: osy procházející každým vrcholem a středem protilehlé strany (celkem n)

  sudé n: osa pro každou dvojici protilehlých vrcholů (celkem $\frac{n}{2}$)

  osa pro každou dvojici protilehlých středů stran (celkem $\frac{n}{2}$) [7]

Grupa D_n obsahuje právě $2n$ symetrií (n rotací a n osových souměrností)

Označíme vrcholy n-úhelníku postupně čísly 1, 2, …, n. Potom je každá symetrie určena tím, jak zobrazuje vrcholy 1, 2,…, n tohoto n-úhelníku. Směr označuje orientaci zachovávání úhlů. (Může být po směru či proti směru hodinových ručiček). [7]

Dihedrální grupa D_n je podgrupou symetrické grupy S_n, neboť se skládá právě z těch permutací množiny $\{1,2,...,n\}$, které vzniknou, když čísly 1, 2, …, n očíslujeme vrcholy pravidelného n-úhelníku a poté uvažujeme všechny jeho symetrie. [7]

Rotace zachovávají pořadí vrcholů i jejich směr.

Oproti tomu osová souměrnost vždy mění směr. Dvojí změnou pořadí dostaneme původní pořadí. Složením libovolných dvou zrcadlení (osová souměrnost podle osy procházející vrcholem) dostaneme rotaci. [7]

Tabulka 5: Cayleyho tabulka pro grupu Dn

Cayleyho tabulka pro grupu D_n:

$\circ$	I	R	R^2	...	R^{n-1}	O	$O\circ R$	$O\circ R^2$	...	$O\circ R^{n-1}$
I	I	R	R^2	...	R^{n-1}	O	$O\circ R$	$O\circ R^2$	...	$O\circ R^{n-1}$
R	R	R^2	$R^{3 \bmod n}$	...	I	$O\circ R^{n-1}$	O	$O\circ R$	...	$O\circ R^{n-2}$
R^2	R^2	$R^{3 \bmod n}$	$R^{4 \bmod n}$	...	R	$O\circ R^{n-2}$	$O\circ R^{n-1}$	O	...	$O\circ R^{n-3}$
⋮	⋮	⋮	⋮	...	⋮	⋮	⋮	⋮	...	⋮
R^{n-1}	R^{n-1}	I	R	...	R^{n-2}	$O\circ R$	$O\circ R^2$	$O\circ R^{3 \bmod n}$	...	O
O	O	$O\circ R$	$O\circ R^2$	...	$O\circ R^{n-1}$	I	R	R^2	...	R^{n-1}
$O\circ R$	$O\circ R$	$O\circ R^2$	$O\circ R^{3 \bmod n}$	...	O	R^{n-1}	I	R	...	R^{n-2}
$O\circ R^2$	$O\circ R^2$	$O\circ R^{3 \bmod n}$	$O\circ R^{4 \bmod n}$	...	$O\circ R$	R^{n-2}	R^{n-1}	I	...	R^{n-3}
⋮	⋮	⋮	⋮	...	⋮	⋮	⋮	⋮	...	⋮
$O\circ R^{n-1}$	$O\circ R^{n-1}$	O	$O\circ R$	...	$O\circ R^{n-2}$	R	R^2	$R^{3 \bmod n}$	...	I

Definice 26:

Každá podgrupa dihedrální grupy D_n je generována maximálně dvěma prvky. Dostáváme jen tři druhy podgrup grupy symetrií D_n pravidelného n-úhelníku:

- $\left\{I, R^j, R^{2j}, ..., R^{n-j}\right\}$ pro každé $j \mid n$,
- $\left\{I, O\circ R^i\right\}$ pro všechna $0 \le i < n$,
- $\left\{I, R^k, R^{2k}, ..., R^{n-k}, O\circ R^h, O\circ R^{2k+h}, O\circ R^{n-k+h}\right\}$ pro každé $k \mid n$ a každé $0 \le h < n$ [7]

7.1 Cayleyho věta:

Věta 16:

Každá konečná grupa $(G,*)$ řádu n je izomorfní s jistou podgrupou symetrické grupy S_n (neboli grupu $(G,*)$ lze izomorfně vnořit do grupy S_n). [7]

Pokud bychom permutací rozuměli prosté zobrazení jakékoliv množiny (i nekonečné) na sebe, mohli bychom vyslovit tuto větu i v obecnějším tvaru.

Věta 17:

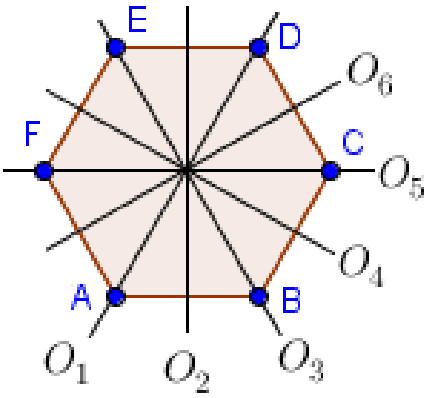
Libovolná množina $(G,*)$ je izomorfní s jistou podgrupou grupy všech permutací množiny G. [7]

Jako příklad dihedrální grupy D_n si nyní uvedeme grupu shodností v rovině reprodukujících pravidelný šestiúhelník.

Příklad 29:

Nechť je dána grupa shodností v rovině G reprodukující pravidelný šestiúhelník $ABCDEF$ s binární operací * skládání shodných zobrazení. Sestavte Cayleyovu tabulku zachycující operaci skládání těchto shodností a popište alespoň jednu netriviální podgrupu této grupy.

Nejdříve je dobré představit si, jak jsou symetrie v šestiúhelníku zobrazeny, a proto si sestrojíme obrázek 5.



Obrázek 4: Shodná zobrazení šestiúhelníku ABCDEF v rovině

Shodných zobrazení v rovině, která zobrazují pravidelný šestiúhelník $ABCDEF$ na sebe je 12. Jsou jimi identita (Id), zobrazení samo na sebe. Dále pak pět rotací, které otočí pravidelný šestiúhelník okolo svého středu po směru hodinových ručiček o úhel n $n\cdot 60^{\circ}$, kde $n=1,2,\ldots,5$. Jak již víme z předchozí části, osové souměrnosti můžeme dělit na sudé a

liché. Dále je zde šest osových symetrií, z nichž jsou 3 sudé a 3 liché. Tabulku můžeme doplnit využitím permutací nebo doplněním do tabulky pro dihedrální grupy D_n. Rychlejší způsob je doplnění dihedrální tabulky D_n.

Tabulka 5: Operační tabulka shodných zobrazení šestiúhelníku ABCDEF

*	Id	R	R^2	R^3	R^4	R^5	O_1	O_2	O_3	O_4	O_5	O_6
Id	Id	R	R^2	R^3	R^4	R^5	O_1	O_2	O_3	O_4	O_5	O_6
R	R	R^2	R^3	R^4	R^5	Id	O_2	O_3	O_4	O_5	O_6	O_1
R^2	R^2	R^3	R^4	R^5	Id	R	O_3	O_4	O_5	O_6	O_1	O_2
R^3	R^3	R^4	R^5	Id	R	R^2	O_4	O_5	O_6	O_1	O_2	O_3
R^4	R^4	R^5	Id	R	R^2	R^3	O_5	O_6	O_1	O_2	O_3	O_4
R^5	R^5	Id	R	R^2	R^3	R^4	O_6	O_1	O_2	O_3	O_4	O_5
O_1	O_1	O_6	O_5	O_4	O_3	O_2	Id	R^5	R^4	R^3	R^2	R
O_2	O_2	O_1	O_6	O_5	O_4	O_3	R	Id	R^5	R^4	R^3	R^2
O_3	O_3	O_2	O_1	O_6	O_5	O_4	R^2	R	Id	R^5	R^4	R^3
O_4	O_4	O_3	O_2	O_1	O_6	O_5	R^3	R^2	R	Id	R^5	R^4
O_5	O_5	O_4	O_3	O_2	O_1	O_6	R^4	R^3	R^2	R	Id	R^5
O_6	O_6	O_5	O_4	O_3	O_2	O_1	R^5	R^4	R^3	R^2	R	Id

Podgrupou grupy symetrií pravidelného šestiúhelníku je například grupa, již jsme rozebírali již v příkladu 21, a to grupa symetrií rovnostranného trojúhelníku.

Příklad 30:

Popište 30 různých podgrup grupy S_6 izomorfních s S_3.

Nejprve se pokusíme nalézt podgrupy, které nechávají na místě tři prvky z uvažovaných šesti. Ty ovšem musí být izomorfní s S_3. Podgrup, které splňují tuto podmínku je $\binom{6}{3} = 20$. Generují je dvojice typu $\{(1\ 2\ 3), (1\ 2)\}$. Odkážeme-li se na

geometrii, pomůže nám například grupa rovnostranného trojúhelníka, která je podgrupou grupy pravidelného šestiúhelníku. Dostáváme například podgrupu generovanou permutacemi $(1\ \ 2\ \ 3)\,(4\ \ 5\ \ 6)$, $(1\ \ 2)\,(4\ \ 5)$. Tímto způsobem lze popsat 30 různých podgrup, avšak jich existuje mnohem více.

Vezmeme-li si ze symetrické grupy S_n n-tého stupně pouze podmnožinu sudých permutací A_n, dostáváme následující tvrzení:

Permutace z n prvků je sudá a počet faktorů v každém rozkladu této permutace na součin transpozic je sudý. Z toho vyplývá, že součin sudých permutací z n prvků je opět sudou permutací. Protože platí, že inverzní permutace k sudé permutaci je sudá, je A_n podgrupou grupy S_n. [6]

Definice 27:

Pro každé $n>1$ je množina A_n všech sudých permutací množiny n podgrupou grupy S_n a má $\frac{(n!)}{2}$ prvků. Tato grupa se nazývá alternující grupa stupně n. [6]

Věta 18:

Množina A_n všech sudých permutací množiny $M=\{1,2,...,n\}$, $n\geq 2$, tvoří podgrupu symetrické grupy S_n indexu 2. Je tedy normální podgrupou. [7]

Věta 19:

Je-li $n\geq 2$, pak množina transpozic $\{(1,p);p=2,...,n\}$ je množinou generátorů symetrické grupy S_n. Je-li $n\geq 3$, pak množina cyklů délky 3 $\{(1,2,p);p=3,...,n\}$ je množina generátorů alternující grupy A_n. [7]

8 CVIČENÍ

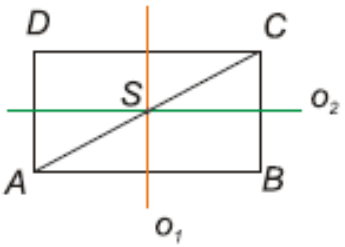
Příklad 31:

Určete všechny shodnosti v rovině reprodukující obdélník. Sestavte Cayleyovu tabulku zachycující operaci skládání těchto shodností a dokažte, že vytvářejí grupu.

Identita: $I = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}$

Osová souměrnost:

$$O_1(o_1) = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$$



Obrázek 5: Shodná zobrazení obdélníka ABCD v rovině

$$O_2(o_2) = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$$

Rotace:

$$R_1(S, +180^0) = S(S) = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$$

Tabulka 6: Cayleyho tabulka reprodukující obdélník

*	I	R	O_1	O_2
I	I	R	O_1	O_2
R	R	I	O_2	O_1
O_1	O_1	O_2	I	R
O_2	O_2	O_1	R	I

Příklad 32:

Vyjádřete každou z následujících permutací ve tvaru součinu disjunktních cyklů:

$\begin{pmatrix}1&2&3&4&5&6\\2&6&4&5&3&1\end{pmatrix}, \begin{pmatrix}1&2&3&4&5&6\\5&3&1&6&2&4\end{pmatrix}, \begin{pmatrix}1&2&3&4&5&6&7\\7&4&2&3&6&5&1\end{pmatrix}.$

První permutaci lze psát ve tvaru $(1\ \ 2\ \ 6)\,(3\ \ 4\ \ 5)$, je řádu tři a inverzní permutací je $(1\ \ 6\ \ 2)\,(3\ \ 5\ \ 4)$.

Druhou permutaci můžeme zapsat ve tvaru $(1\ \ 5\ \ 2\ \ 3)\,(4\ \ 6)$, je řádu čtyři a inverzní permutací k ní je $(1\ \ 3\ \ 2\ \ 5)\,(4\ \ 6)$.

Třetí permutaci lze vyjádřit jako součin $(1\ \ 7)\,(2\ \ 4\ \ 3)\,(5\ \ 6)$. Je řádu šest a má inverzní permutaci $(1\ \ 7)\,(2\ \ 3\ \ 4)\,(5\ \ 6)$.

Příklad 33:

Určete, jaký nejvyšší řád mohou mít permutace z grupy S_{10} a S_{16}.

V prvním kroku rozložíme permutace v součin nezávislých cyklů tak, aby nejmenší společný násobek jejich délek byl co největší.

S_{10} : *nsn* (4,6) = 24

S_{16} : *nsn* (2,6,8) = 92

Permutace v grupě S_{10} mohou být až řádu 24 a v grupě S_{16} až řádu 92.

Příklad 34:

Řešte v S_6 rovnici: $A\cdot B\cdot X = C$, je-li $A=\begin{pmatrix}1&2&3&4&5&6\\2&5&6&4&1&3\end{pmatrix}, B=(1\ \ 4\ \ 6\ \ 3)(2\ \ 5)$,

$C=\begin{pmatrix}1&2&3&4&5&6\\4&3&2&6&5&1\end{pmatrix}$.

Při řešení rovnice budeme postupovat v několika krocích. V prvním kroku si rovnici zapíšeme a nahradíme příslušnými permutacemi. Permutaci X zapíšeme ve tvaru

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \end{pmatrix}$. Při výpočtu postupujeme zprava doleva. Skládáním permutací na levé straně rovnice potřebujeme docílit, aby se levá strana rovnala pravé.

$$A \cdot B \cdot X = C$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 4 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 6 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 6 & 5 & 1 \end{pmatrix}$$

V druhém kroku provedeme složení permutací A a B. Získáme permutaci D.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 6 & 5 & 1 \end{pmatrix}$$

Po složení permutací D a X na levé straně rovnice by měla vyjít permutace shodná s permutací C. Nyní jsme už tedy schopni vypozorovat výsledek. Začneme prvkem 1 v permutaci X, tak X_1 musí mít takovou hodnotu, abychom po složení s permutací D získali hodnotu 4. Z toho vyplývá, že prvek X_1 musí být roven 1. Analogicky budeme postupovat až do X_6

1. $x_1 \rightarrow 4$ $\quad\quad$ $x_1 = 1$

2. $x_2 \rightarrow 3$ $\quad\quad$ $x_2 = 4$

3. $x_3 \rightarrow 2$ $\quad\quad$ $x_3 = 3$

4. $x_4 \rightarrow 6$ $\quad\quad$ $x_4 = 6$

5. $x_5 \rightarrow 5$ $\quad\quad$ $x_5 = 5$

6. $x_6 \rightarrow 1$ $\quad\quad$ $x_6 = 2$

Řešením rovnice $A \cdot B \cdot X = C$ v S_6 vyšlo $X = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 5 & 2 \end{pmatrix}$.

Příklad 35:

V množině komplexních čísel C řešte rovnici $x^4 = 1$. Ukažte, že množina všech kořenů této rovnice spolu s operací násobení komplexních čísel tvoří cyklickou grupu.

Nejprve musíme zjistit kořeny rovnice. V množině komplexních čísel C má rovnice $x^4 = 1$ právě čtyři kořeny 1, i, -1 a $-i$. Dostali jsme tedy čtyř prvkovou grupu. Sestavíme operační tabulku.

Tabulka 7: Cayleyova tabulka cyklické grupy řádu 4

*	**1**	**i**	**-1**	**-i**
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

Zjišťujeme, že se jedná o cyklickou grupu. Generátory jsou prvky i, resp. $-i$. Vezmeme-li si například $(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$ a $(-i)^4 = 1$. Z tabulky 6 vidíme, že cyklická grupa obsahuje kromě nevlastních podgrup i podgrupu cyklickou řádu 2, která je generována prvkem -1.

ZÁVĚR

Cílem této práce bylo seznámit čtenáře s teorií grup. V každé kapitole bylo použito několik důležitých definic a vět, z nichž některé byly lépe vysvětleny na příkladech. Dále zde bylo obsaženo několik řešených příkladů, které měly čtenáři poskytnout lepší návod na řešení daných problémů.

RESUMÉ

This bachelor thesis deals with Solving problems in the general algebra. Since this theme is very comprehensive I focus on the groups only. Therefore, the aim of this thesis is to introduce the theory of groups.

The thesis is divided into eight chapters. Each chapter covers couple definitions and sentences. Most of these definitions and sentences are also provided with an example which further illustrates what a specific definition or sentence means. Furthermore, the work includes two chapters which contain couple solved examples which should provide a reader with the instructions to solve the further matters.

SEZNAM LITERATURY

[1] WEIL, J., J. HOCQUEMILLEROVÁ, D. ALLOUCH, A. MÉZARD, J. - C. VAILLANT, Ch. DELORME, Ch. LAVITOVÁ a J. - C. RAOULT. Rozpracovaná řešení úloh z vyšší algebry. 1. vyd. Praha: Academia, 1987. ISBN 21/111/87.

[2] HORA, Jaroslav. ALGEBRA I. 1. vyd. Plzeň: Pedagogická fakulta v Plzni, 1991. ISBN 80-7043-030-3.

[3] LANE, S.Mac a G. BIRKHOFF. Algebra. 1. vyd. Bratislava: ALFA, 1973. ISBN 63-556-72.

[4] BLAŽEK, Jaroslav, KOMAN, Milan, VOJTÁŠKOVÁ, Blanka. Algebra a teoretická aritmetika: II. díl. 1. vyd. Praha: Státní pedagogické nakladatelství, 1985. ISBN 14-470-85.

[5] LEGÉŇ, Anton. Grupy, okruhy a zväzy. 1. vyd. Bratislava: ALFA, 1980. ISBN 63-184-80.

[6] KUROŠ, A. G. Kapitoly z obecné algebry. 2. vyd. Praha: Academia, 1977. ISBN 104-21-852.

[7] HOLUBOVÁ, Růžena. Grupy [online]. 2010 [cit. 2014-04-03]. Dostupné z: http://files.mfgio.webnode.cz/200000003-b558eb6530/Grupy.pdf

[8] DRÁBEK, Jaroslav. Binární operace. Jejich vlastnosti. Algebraické struktury a jejich zobrazení [online]. [cit. 2014-04-03]Dostupné z: http://www.kmt.zcu.cz/subjects/ela.html

[9] Burian, K., Libicher, J.: Algebra 1. 2. vyd. Ostrava: Pedagogická fakulta v Ostravě, 1976

[10] MAREŠ, Jan. Grupy [online]. 2013 [cit. 2014-04-09]. Dostupné z: http://people.fjfi.cvut.cz/maresjan/data/grupy_publ.pdf

[11] Symetrické grupy. Symetrické grupy [online]. 2014 [cit. 2014-04-09]. Dostupné z: katmatprf.ujepurkyne.com/materialy/KMA_kuril_LINALGkapitola06.pdf

[12] HAŠEK, Roman. Lineární algebra: Permutace. Definice determinantu. Vlastnosti determinantu. Lineární algebra [online]. 2014 [cit. 2014-04-09]. Dostupné z: http://home.pf.jcu.cz/~hasek/lalgebra/Pr6/LA_Permutace_2011.pdf

[13] HORČÍK, Rostislav. Permutační grupy. Cykly a transpozice. Aplikace [online]. 2010 [cit. 2014-04-09]. Dostupné z: http://www2.cs.cas.cz/~horcik/Teaching/handout13.pdf

[14] VALD, Denis. Permutace [online]. 2010 [cit. 2014-04-09]. Dostupné z: http://www.karlin.mff.cuni.cz/~vald/Cviceni_8.pdf

[15] TIRPÁKOVÁ, Anna a Dagmar MARKECHOVÁ. Základy elementárnej aritmetiky: Vybrané kapitoly [online]. 1. vyd. Nitra: Fakulta prírodných vied UKF, 2011 [cit. 2014-04-09]. ISBN 978-80-. Dostupné z: http://www.km.fpv.ukf.sk/upload_publikacie/20120125_140546__1.pdf

[16] NÝVLTOVÁ, Eva. Některé poznatky z teorie grup a jejich praktické aplikace [online]. 2005 [cit. 2014-04-09]. Dostupné z: http://pdf.truni.sk/download?zbornik/smolenice/nyvltova.pdf

[17] STANOVSKÝ, David. Příklady z algebry. Sbírka úloh [online]. 2014 [cit. 2014-04-09]. Dostupné z: http://www.karlin.mff.cuni.cz/~stanovsk/vyuka/sbirka.pdf

[18] Grupy. Algebra 1 [online]. 2011 [cit. 2014-04-09]. Dostupné z: http://www.primat.cz/cuni-mff/predmety/algebra-i/grupy/71584

[19] BEČVÁŘ, Jindřich. Lineární algebra [online]. Praha: Matematicko-fyzikální fakulta Univerzity Karlovy, 2010 [cit. 2014-04-09]. ISBN 978-80-7378-135-4. Dostupné z: http://www.mff.cuni.cz/fakulta/mfp/download/books/becvar_-_linearni_algebra.pdf

[20] MARVAN, Michal. Homomorfismy. Matematický ústav Slezské univerzity [online]. 2000 [cit. 2014-04-09]. Dostupné z: http://www.slu.cz/math/cz/knihovna/docs/algebra1/2.-homomorfismy

[21] DRÁPAL, Aleš. Teorie grup-základní aspekty. Matematicko-fyzikální fakulta Univerzity Karlovy [online]. 2009 [cit. 2014-04-09]. Dostupné z: http://artax.karlin.mff.cuni.cz/~korbm0am/grupy.pdf

[22] MUSIL, Vít. Grupy - sbírka příkladů. Bakalářská práce [online]. 2005 [cit. 2014-04-09]. Dostupné z: http://www.math.muni.cz/~klima/Algebra/grupy_sbirka.pdf

[23] OLŠÁK, Petr. Lineární algebra. Lineární algebra [online]. 2007 [cit. 2014-04-09]. Dostupné z: ftp://math.feld.cvut.cz/olsak/linal/linal.pdf

[24] ČECHOVÁ, Ivana. Konečné grupy malých řádů. Bakalářská práce [online]. 2012 [cit. 2014-04-09]. Dostupné z:

https://otik.uk.zcu.cz/xmlui/bitstream/handle/11025/5433/Konecne_grupy_malych_radu_Cechova_Ivana_2012.pdf?sequence=1

[25] Sbírka úloh z Lineární Algebry. Přírodovědecká fakulta MU [online]. 2014 [cit. 2014-04-09]. Dostupné z: http://www.math.muni.cz/~cadek/LA/sbirka.pdf

[26] BICAN, Ladislav. Lineární algebra a geometrie [online]. Praha: Academia, 2000 [cit. 2014-04-09]. ISBN 80-200-0843-8. Dostupné z: http://www.ulozto.cz/xvnWH1P/bican-ladislav-linearni-algebra-a-geometrie-pdf

[27] Syntetická geometrie. Trial [online]. 2012 [cit. 2014-04-09]. Dostupné z: http://trial.zcu.cz/predmety/SG/SG12.pdf

SEZNAM TABULEK

SEZNAM OBRÁZKŮ