Matematika IV – 6. týden
Symetrie rovinných obrazců a elementární teorie grup

Jan Slovák

Masarykova univerzita
Fakulta informatiky

25. 3. - 29. 3. 2013

Obsah přednášky

1. Literatura
2. Grupy a grupoidy
3. Symetrie „logotypů“ a „dláždění“
4. Homomorfismy grup
5. Rozklady a faktorgrupy

Plán přednášky

1. Literatura
2. Grupy a grupoidy
3. Symetrie „logotypů“ a „dláždění“
4. Homomorfismy grup
5. Rozklady a faktorgrupy

Kde je dobré číst?

- Riley, K.F., Hobson, M.P., Bence, S.J. Mathematical Methods for Physics and Engineering, second edition, Cambridge University Press, Cambridge 2004, ISBN 0 521 89067 5, xxiii + 1232 pp.
- Kapitola 11 nové učebnice (bude průběžně doplňěna)

Plán přednášky

1 Literatura

2 Grupy a grupoidy

3 Symetrie „logotypů“ a „dláždění“

4 Homomorfismy grup

5 Rozklady a faktorgrupy

Chceme abstraktně pracovat s objekty a se situacemi, ve kterých je možné rovnice

$$a \cdot x = b$$

vždy jednoznačně řešit (tak jako u lineárních rovnic jsou objekty a a b jsou dány, zatímco x hledáme).
Jde o tzv. **teorii grup**. Všimněme si, že zatím nic nevíme o povaze objektů, ani co znamená ta „tečka“ v rovnici.

Chceme abstraktně pracovat s objekty a se situacemi, ve kterých je možné rovnice

$$a \cdot x = b$$

vždy jednoznačně řešit (tak jako u lineárních rovnic jsou objekty a a b jsou dány, zatímco x hledáme).
Jde o tzv. **teorii grup**. Všimněme si, že zatím nic nevíme o povaze objektů, ani co znamená ta „tečka“ v rovnici.
Nejprve projdeme příklady, ve kterých se s takovými objekty potkáváme, poté si zavedeme malý slovníček pojmů.

Example

1. Přirozená čísla $\mathbb{N} = \{0, 1, 2, \dots\}$, spolu s kteroukoliv z operací sčítání a násobení jsou asociativní a komutativní pologrupa s jednotkou, neexistují v ní ale inverzní prvky.

Example

1. Přirozená čísla $\mathbb{N} = \{0, 1, 2, \dots\}$, spolu s kteroukoliv z operací sčítání a násobení jsou asociativní a komutativní pologrupa s jednotkou, neexistují v ní ale inverzní prvky.
2. Celá čísla $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ jsou grupoid vůči kterékoliv z operací sčítání, odčítání, násobení. Jsou dokonce komutativní grupou vzhledem ke sčítání, jsou však jen komutativní pologrupou vůči násobení (neexistují inverze k prvkům $a \neq \pm 1$). Operace odčítání není ani asociativní (např. $(5 - 3) - 2 = 0 \neq 5 - (3 - 2) = 4$). Všimněte si také, že pro odečítání je nula pravý neutrální prvek, ne však levý. Dokonce v tomto případě levý neutrální prvek neexistuje.

Example

1. Přirozená čísla $\mathbb{N} = \{0, 1, 2, \dots\}$, spolu s kteroukoliv z operací sčítání a násobení jsou asociativní a komutativní pologrupa s jednotkou, neexistují v ní ale inverzní prvky.
2. Celá čísla $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ jsou grupoid vůči kterékoliv z operací sčítání, odčítání, násobení. Jsou dokonce komutativní grupou vzhledem ke sčítání, jsou však jen komutativní pologrupou vůči násobení (neexistují inverze k prvkům $a \neq \pm 1$). Operace odčítání není ani asociativní (např. $(5 - 3) - 2 = 0 \neq 5 - (3 - 2) = 4$). Všimněte si také, že pro odečítání je nula pravý neutrální prvek, ne však levý. Dokonce v tomto případě levý neutrální prvek neexistuje.
3. Racionální čísla $\mathbb{Q}$ jsou komutativní grupou vzhledem ke sčítání a nenulová racionální čísla jsou grupou vůči násobení. Celá čísla spolu se sčítáním jsou jejich podgrupou.

Example (pokračování)

1. Pro $k \in \mathbb{N}$, množina všech k-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$ je konečná grupa vůči násobení komplexních čísel. Např. pro $k = 2$ dostaneme grupu $\{-1, 1\}$ se dvěma prvky, které jsou oba samy sobě inverzí, zatímco pro $k = 4$ dostáváme grupu $G = \{1, i, -1, -i\}$.

Example (pokračování)

1. Pro $k \in \mathbb{N}$, množina všech k-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$ je konečná grupa vůči násobení komplexních čísel. Např. pro $k = 2$ dostaneme grupu $\{-1, 1\}$ se dvěma prvky, které jsou oba samy sobě inverzí, zatímco pro $k = 4$ dostáváme grupu $G = \{1, i, -1, -i\}$.
2. Množina Mat_n všech čtvercových matic je (nekomutativní) pologrupa vzhledem k násobení matic a komutativní grupa vzhledem ke sčítání matic.

Example (pokračování)

1. Pro $k \in \mathbb{N}$, množina všech k-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$ je konečná grupa vůči násobení komplexních čísel. Např. pro $k = 2$ dostaneme grupu $\{-1, 1\}$ se dvěma prvky, které jsou oba samy sobě inverzí, zatímco pro $k = 4$ dostáváme grupu $G = \{1, i, -1, -i\}$.
2. Množina Mat_n všech čtvercových matic je (nekomutativní) pologrupa vzhledem k násobení matic a komutativní grupa vzhledem ke sčítání matic.
3. Množina všech lineárních zobrazení $\mathrm{Hom}(V, V)$ na vektorovém prostoru je pologrupa vzhledem ke skládání zobrazení a komutativní grupa vzhledem ke sčítání zobrazení.

Example (pokračování)

1. Pro $k \in \mathbb{N}$, množina všech k-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$ je konečná grupa vůči násobení komplexních čísel. Např. pro $k = 2$ dostaneme grupu $\{-1, 1\}$ se dvěma prvky, které jsou oba samy sobě inverzí, zatímco pro $k = 4$ dostáváme grupu $G = \{1, i, -1, -i\}$.
2. Množina Mat_n všech čtvercových matic je (nekomutativní) pologrupa vzhledem k násobení matic a komutativní grupa vzhledem ke sčítání matic.
3. Množina všech lineárních zobrazení $\mathrm{Hom}(V, V)$ na vektorovém prostoru je pologrupa vzhledem ke skládání zobrazení a komutativní grupa vzhledem ke sčítání zobrazení.
4. V obou předchozích příkladech, podmnožina invertibilních objektů uvažované pologrupy tvoří grupu. V případě matic jde o tzv. grupu invertibilních matic, ve druhém o grupu lineárních transformací vektorového prostoru (tj. invertibilních lineárních zobrazení).

Definition

Pro libovolnou množinu A:

- **binární operace** na A je zobrazení $A \times A \to A$, které budeme zpravidla značit $(a, b) \mapsto a \cdot b$, množina s binární operací je **grupoid**
- binární operace je **asociativní**, jestliže pro všechny prvky v A platí $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- binární operace je **komutativní**, jestliže pro všechny prvky v A platí $a \cdot b = b \cdot a$
- **levá jednotka** v A je takový prvek $e \in A$, že pro všechny prvky v A platí $e \cdot a = a$; obdobně pro **pravou jednotku** musí platit pro všechny prvky $a \cdot e = a$
- **jednotka** binární operace je prvek e, který je pravou i levou jednotkou zároveň
- **pologrupa** $(A, \cdot)$ je grupoid s binární operací, která je asociativní.

Definition (pokračování)

- prvek a^{-1} je **levou inverzí** k prvku a v pologrupě $(A, \cdot)$ s jednotkou e, jestliže platí $a^{-1} \cdot a = e$; obdobně je **pravou inverzí** a^{-1} takový prvek, pro který je $a \cdot a^{-1} = e$
- prvek a^{-1} je **inverzní** k a v pologrupě s jednotkou, jestliže je levou i pravou inverzí zároveň
- **grupa** $(G, \cdot)$ je pologrupa s jednotkou, ve které má každý prvek inverzi
- **komutativní grupa**, resp. **komutativní pologrupa**, je taková, kde je operace $\cdot$ komutativní.
- Je-li $(A, \cdot)$ grupa (případně pologrupa), pak její podmnožinu $B \subset A$, která je uzavřená vůči zúžení operace $\cdot$ a zároveň je spolu s touto operací grupou, nazýváme **podgrupa** v $(A, \cdot)$.

Zpravidla grupy a pologrupy potkáváme jako množiny zobrazení na pevně dané množině M, které jsou uzavřeny vůči skládání zobrazení. Často si ale tuto skutečnost přímo neuvědomujeme. Na každé konečné množině M, s $m = |M| \in \mathbb{N}$ prvky máme k dispozici m^m možných definic zobrazení (každý z m prvků můžeme zobrazit na kterýkoliv v M) a všechna taková zobrazení umíme skládat.

Zpravidla grupy a pologrupy potkáváme jako množiny zobrazení na pevně dané množině M, které jsou uzavřeny vůči skládání zobrazení. Často si ale tuto skutečnost přímo neuvědomujeme. Na každé konečné množině M, s $m = |M| \in \mathbb{N}$ prvky máme k dispozici m^m možných definic zobrazení (každý z m prvků můžeme zobrazit na kterýkoliv v M) a všechna taková zobrazení umíme skládat.

Pokud chceme, aby existovala k zobrazení $\alpha : M \to M$ jeho inverze α^{-1}, musí být α bijekcí. Složením dvou bijekcí vznikne opět bijekce a proto podmnožina Σ_m všech bijekcí na množině M o m prvcích je grupa. Říkáme jí **grupa permutací** na m prvcích.

Název **grupa permutací** přitom uvádí jinou souvislost, kdy místo bijekcí na konečné množině vnímáme permutace jako přerovnání rozlišitelných prvků. Potkávali jsme se s ní např. při studiu determinantů.

Název **grupa permutací** přitom uvádí jinou souvislost, kdy místo bijekcí na konečné množině vnímáme permutace jako přerovnání rozlišitelných prvků. Potkávali jsme se s ní např. při studiu determinantů.

V grupě permutací Σ_3 na číslech $\{1, 2, 3\}$ si třeba označíme jednotlivá pořadí

$$a = (1, 2, 3),\ b = (2, 3, 1),\ c = (3, 1, 2),$$
$$d = (1, 3, 2),\ e = (3, 2, 1),\ f = (2, 1, 3).$$

Skládání našich permutací je pak zadáno tabulkou

$\cdot$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	a	f	d	e
c	c	a	b	e	f	d
d	d	e	f	a	b	c
e	e	f	d	c	a	b
f	f	d	e	b	c	a

Všimněme si podstatného rozdílu mezi permutacemi a, b a c a dalšími třemi. Ty první tři tvoří tzv. **cyklus** generovaný prvkem b nebo prvkem c:

$$b^2 = c,\ b^3 = a,\ c^2 = b,\ c^3 = a$$

a samy o sobě jsou tyto tři prvky komutativní podgrupou. V ní a je jednotka, a b s c jsou vzájemně inverzní. Je tedy tato podgrupa stejná jako je grupa $\mathbb{Z}_3$ zbytkových tříd celých čísel modulo 3, resp. jako grupa třetích odmocnin z jedničky z jednoho z předchozích příkladů.

Všimněme si podstatného rozdílu mezi permutacemi a, b a c a dalšími třemi. Ty první tři tvoří tzv. **cyklus** generovaný prvkem b nebo prvkem c:

$$b^2 = c,\ b^3 = a,\ c^2 = b,\ c^3 = a$$

a samy o sobě jsou tyto tři prvky komutativní podgrupou. V ní a je jednotka, a b s c jsou vzájemně inverzní. Je tedy tato podgrupa stejná jako je grupa $\mathbb{Z}_3$ zbytkových tříd celých čísel modulo 3, resp. jako grupa třetích odmocnin z jedničky z jednoho z předchozích příkladů.
Další tři prvky jsou samy sobě inverzí a každý z nich je tedy společně s jednotkou a podgrupou stejnou jako je $\mathbb{Z}_2$. Říkáme, že b a c jsou **prvky řádu** 3, zatímco prvky d, e a f jsou řádu 2.

Obdobně se chovají všechny grupy permutací Σ_m.
Každá permutace σ rozkládá množinu M na disjunktní sjednocení maximálních invariantních podmnožin M_x, které dostaneme tak, že postupně vybíráme dosud nezpracované prvky $x \in M$ a do třídy rozkladu M_x přidáváme všechny akce iterací $\sigma^k(x)$, $k = 1, 2, \ldots,$ dokud není $\sigma^k(x) = x$.

Obdobně se chovají všechny grupy permutací Σ_m.
Každá permutace σ rozkládá množinu M na disjunktní sjednocení maximálních invariantních podmnožin M_x, které dostaneme tak, že postupně vybíráme dosud nezpracované prvky $x \in M$ a do třídy rozkladu M_x přidáváme všechny akce iterací $\sigma^k(x)$, $k = 1, 2, \ldots$, dokud není $\sigma^k(x) = x$.

Každou permutaci tak dostáváme jako složení jednodušších permutací, tzv. cyklů, které se chovají jako identická permutace vně M_x a tak jako σ na M_x.

Obdobně se chovají všechny grupy permutací Σ_m.
Každá permutace σ rozkládá množinu M na disjunktní sjednocení maximálních invariantních podmnožin M_x, které dostaneme tak, že postupně vybíráme dosud nezpracované prvky $x \in M$ a do třídy rozkladu M_x přidáváme všechny akce iterací $\sigma^k(x)$, $k = 1, 2, \ldots,$ dokud není $\sigma^k(x) = x$.

Každou permutaci tak dostáváme jako složení jednodušších permutací, tzv. cyklů, které se chovají jako identická permutace vně M_x a tak jako σ na M_x.

Pokud přitom očíslujeme prvky v M_x jako pořadí $(1, 2, \ldots, |M_x|)$ tak aby i odpovídalo $\sigma^i(x)$, pak je naše permutace prostým posunutím o jednu pozici v cyklu (tj. poslední prvek je zobrazen zpátky na první). Odtud název **cyklus**. Zjevně přitom tyto cykly komutují, takže je jedno, v jakém pořadí z nich permutaci σ složíme.

Nejjednodušší cykly jsou jednoprvkové pevné body permutace σ.
Dvouprvkové $(x, \sigma(x))$, kde $\sigma(\sigma(x)) = x$ se nazývají **transpozice**.

Nejjednodušší cykly jsou jednoprvkové pevné body permutace σ. Dvouprvkové $(x, \sigma(x))$, kde $\sigma(\sigma(x)) = x$ se nazývají **transpozice**.

Každý cyklus zjevně můžeme poskládat z permutací sousedních prvků (necháme „probublat“ první prvek nakonec) $\Rightarrow$ každou permutaci napsat jako složení transpozic sousedních prvků. Skutečnost, jestli potřebujeme sudý nebo lichý počet permutací je na našich volbách nezávislá.

Nejjednodušší cykly jsou jednoprvkové pevné body permutace σ. Dvouprvkové $(x, \sigma(x))$, kde $\sigma(\sigma(x)) = x$ se nazývají **transpozice**.

Každý cyklus zjevně můžeme poskládat z permutací sousedních prvků (necháme „probublat“ první prvek nakonec) $\Rightarrow$ každou permutaci napsat jako složení transpozic sousedních prvků. Skutečnost, jestli potřebujeme sudý nebo lichý počet permutací je na našich volbách nezávislá.

Máme proto definováno dobře zobrazení $\mathrm{sgn} : \Sigma_m \to \mathbb{Z}_2 = \{\pm 1\}$, tzv. **paritu** permutace. Dokázali jsme si znovu tvrzení, která jsme již využívali při studiu determinantů:

Theorem

Každá permutace konečné množiny je složením cyklů. Cyklus délky ℓ lze vyjádřit jako složení $\ell - 1$ transpozic. Parita cyklu délky ℓ je $(-1)^{\ell-1}$. Parita složení permutací je součinem parit jednotlivých z nich, tzn. že zobrazení sgn *převádí složení permutací $\sigma \circ \tau$ na součin* $\operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau$ *v komutativní grupě $\mathbb{Z}_2$.*

Plán přednášky

1 Literatura

2 Grupy a grupoidy

3 Symetrie „logotypů“ a „dláždění“

4 Homomorfismy grup

5 Rozklady a faktorgrupy

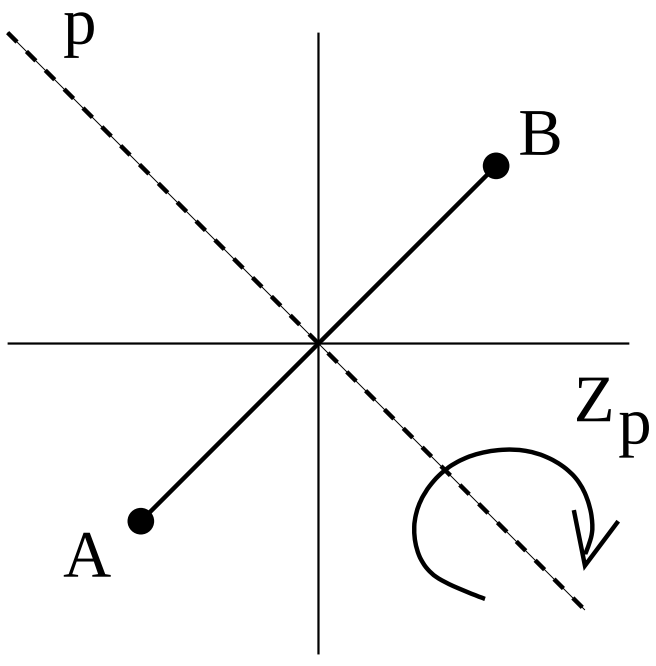
Každé zobrazení roviny do sebe, které zachovává vzdálenosti bodů je affinní, tj. je složením lineárního a vhodné translace (hezké cvičení na diferenciální počet – ale teď zjevně offtopic ;-).
Lineární část takového zobrazení přitom musí navíc být ortogonální.
Všechna taková zobrazení tedy tvoří grupu všech ortogonálních transformací (nebo také euklidovských transformací) v rovině (viz 4. přednáška 1. semestr).

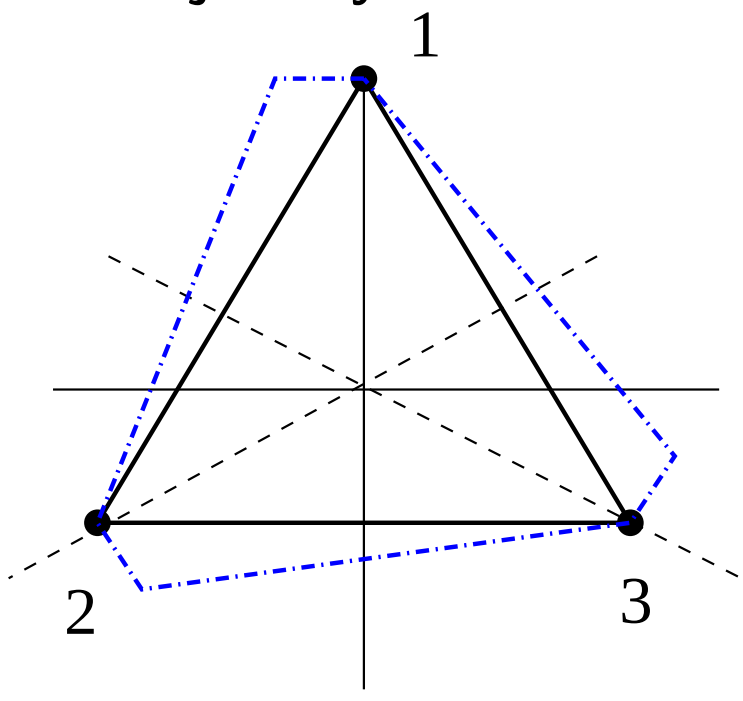
Každé zobrazení roviny do sebe, které zachovává vzdálenosti bodů je affinní, tj. je složením lineárního a vhodné translace (hezké cvičení na diferenciální počet – ale teď zjevně offtopic ;-).
Lineární část takového zobrazení přitom musí navíc být ortogonální.
Všechna taková zobrazení tedy tvoří grupu všech ortogonálních transformací (nebo také euklidovských transformací) v rovině (viz 4. přednáška 1. semestr).

Všechna taková jsou složením

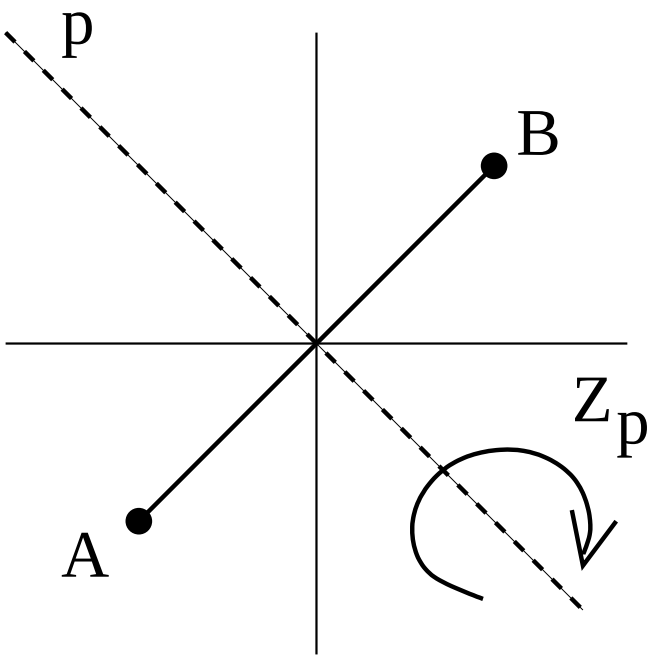
- translací T_a o vektor a
- rotací R_φ o jakýkoliv úhel φ kolem počátku
- zrcadlení Z_ℓ vůči jakékoliv přímce ℓ procházející počátkem.

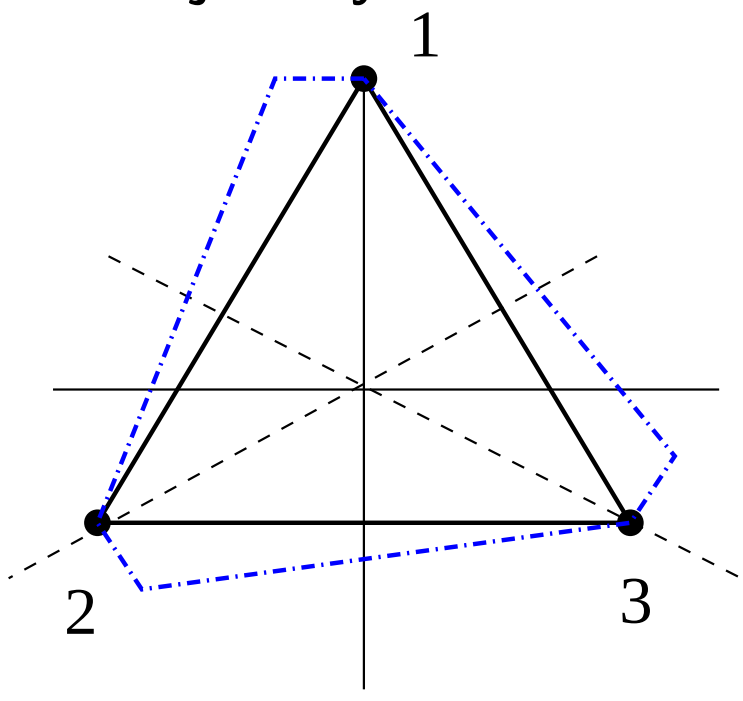
Uvažme ohraničený rovinný obrazec, pro začátek úsečku a rovnostranný trojúhelník. Ptáme se, **jak moc jsou symetrické?**





Uvažme ohraničený rovinný obrazec, pro začátek úsečku a rovnostranný trojúhelník. Ptáme se, **jak moc jsou symetrické?**





Tzn. vůči kterým trasformacím (zachovávajícím velikost) jsou invariantní? Všechny symetrie pevně zvoleného útvaru budou vždy tvořit grupu (většinou pouze s jediným prvkem, identickým zobrazením).

symetrie úsečky

U úsečky je situace obzvlášť jednoduchá – na první pohled je zřejmé, že jedinými jejími netriviálními symetriemi jsou rotace o π, zrcadlení vůči ose této úsečky a zrcadlení vůči úsečce samotné a všechny tyto symetrie jsou samy sobě inverzí. Celá grupa symetrií úsečky má tedy čtyři prvky. Její tabulka násobení vypadá takto:

$\cdot$	R_0	R_π	Z_H	Z_V
R_0	R_0	R_π	Z_H	Z_V
R_π	R_π	R_0	Z_V	Z_H
Z_H	Z_H	Z_V	R_0	R_π
Z_V	Z_V	Z_H	R_π	R_0

a je tedy celá tato grupa komutativní.

symetrie rovnostranného trojúhelníku

Symetrií nacházíme více: můžeme rotovat o $\pi/3$ nebo můžeme zrcadlit vůči osám stran.

symetrie rovnostranného trojúhelníku

Symetrií nacházíme více: můžeme rotovat o $\pi/3$ nebo můžeme zrcadlit vůči osám stran.

Abychom dostali grupu celou, musíme přidat všechna složení takovýchto transformací.
Víme, že složení dvou zrcadlení je vždy otočením (4. přednáška 1. semestru). Složení takových zrcadlení v opačném pořadí dá otočení o stejný úhel, ale s opačnou orientací. V našem případě tedy zrcadlení kolem dvou různých os vygenerují postupnou opakovanou aplikací všechny symetrie, který bude dohromady šest.

Jestliže si umístíme trojúhelník v souřadnicích jako na obrázku, bude našich šest transformací zadáno maticemi

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; b = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \; c = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

$$d = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \; e = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \; f = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

Sestavením tabulky pro násobení, tak jak jsme ji udělali pro grupu permutací Σ_3 obdržíme právě stejný výsledek.

Dihedrální grupy

Obdobně umíme nacházet grupy symetrií s k různými rotacemi a k zrcadleními. Stačí si k tomu vzít pravidelný k-úhelník. Takové grupy symetrií se často označují jako grupy D_k a říká se jim **dihedrální grupy** řádu k.

Dihedrální grupy

Obdobně umíme nacházet grupy symetrií s k různými rotacemi a k zrcadleními. Stačí si k tomu vzít pravidelný k-úhelník. Takové grupy symetrií se často označují jako grupy D_k a říká se jim **dihedrální grupy** řádu k.

Tyto grupy jsou nekomutativní pro všechny $k \geq 3$, zatímco D_2 je komutativní. Název patrně je odvozen od skutečnosti, že D_2 je grupa symetrií molekuly vodíku.

cyklické grupy

Stejně tak lze snadno najít obrazce, které mají pouze rotační symetrie a jde tedy o komutativní grupy, které se v chemii značí jako C_k. Říkáme jim **cyklické grupy** řádu k. K tomu postačí např. uvažovat pravidelný mnohoúhelník, u kterého nesymetricky ale pořád stejně pozměníme chování hran, viz. čerchované rozšíření trojúhelníku na předchozím obrázku.
Všimněme si, že grupu C_2 lze realizovat dvěma způsoby – buď jedinou netriviální rotací o π nebo jediným zrcadlením.

Klasifikace symetrií

Theorem

Nechť je M ohraničená množina v rovině $\mathbb{R}^2$. Pokud má diskrétní grupu symetrií, pak je buď triviální nebo jedna z grup C_k, D_k, s $k \geq 1$.

Složitější chování lze vypozorovat u rovinných obrazců v pásech nebo v celé rovině (něco jako možnosti symetrií pro různé dlažby).

Složitější chování lze vypozorovat u rovinných obrazců v pásech nebo v celé rovině (něco jako možnosti symetrií pro různé dlažby).

Uvažme množinu M, která je celá obsažena v pásu uzavřeném mezi dvěma rovnoběžkami. Pro symetrie takové množiny nepřicházejí v úvahu žádné netriviální rotace, kromě R_π, a jediná možná zrcadlení jsou buď podle osy pásu nebo nějaké na pás kolmé přímky.
K dispozici jsou ještě translace podle vektoru rovnoběžného s osou pásu. Všimněme si, že každá netriviální translace svými iteracemi zapřičiní, že celá grupa symetrií M bude již nutně nekonečná a dvě zrcadlení podle různých rovnoběžných přímek budou translací.

Docela jednoduchý je popis všech **diskrétních grup** symetrií pro dláždění rovinných pásů. (Obraz libovolného bodu při působení všemi prvky grupy je diskrétní podmnožinou v rovině.)
Každá taková grupa je generována některými z následujících symetrií: translace T, posunuté (vertikální) zrcadlení G, vertikální zrcadlení V, horizontální zrcadlení H a rotace R o úhel π.

Docela jednoduchý je popis všech **diskrétních grup** symetrií pro dláždění rovinných pásů. (Obraz libovolného bodu při působení všemi prvky grupy je diskrétní podmnožinou v rovině.)
Každá taková grupa je generována některými z následujících symetrií: translace T, posunuté (vertikální) zrcadlení G, vertikální zrcadlení V, horizontální zrcadlení H a rotace R o úhel π.

Theorem

Těchto grup je sedm typů. Jsou generovány

1. *jedinou translací T*
2. *jediným posunutým zrcadlením G*
3. *jednou translací T a jedním vertikálním zrcadlením V*
4. *jednou translací T a jednou rotací R*
5. *jedním posunutým zrcadlením G a jednou rotací R*
6. *jednou translací T a horizontálním zrcadlením H*
7. *jednou translací T, horizontálním zrcadlením H a jedním vertikálním zrcadlením V*

Složitější je to se symetriemi obrazců, které vyplní celou rovinu.

Všech takových grup symetrií v rovině je pouze sedmnáct. Říká se jim dvourozměrné krystalografické grupy.

Plán přednášky

1 Literatura

2 Grupy a grupoidy

3 Symetrie „logotypů“ a „dláždění“

4 Homomorfismy grup

5 Rozklady a faktorgrupy

připomenutí:

- **pologrupa** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **grupa** $(G, \cdot)$ je pologrupa s jednotkou, ve které má každý prvek inverzi
- **komutativní grupa**, resp. **komutativní pologrupa**, je taková, kde je operace $\cdot$ komutativní.
- Je-li $(A, \cdot)$ grupa (případně pologrupa), pak její podmnožinu $B \subset A$, která je uzavřená vůči zúžení operace $\cdot$ a zároveň je spolu s touto operací grupou, nazýváme **podgrupa** v $(A, \cdot)$.

Definition

Zobrazení $f : G \to H$ mezi dvěmi grupami G a H se nazývá **homomorfismus grup**, jestliže respektuje násobení, tj. pro všechny prvky $a, b \in G$ platí

$$f(a \cdot b) = f(a) \cdot f(b).$$

Povšimněme si, že násobení vlevo je uvnitř grupy G předtím, než zobrazujeme, zatímco vpravo jde o násobení v H poté, co zobrazujeme.

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Theorem

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e \in G$ je jednotka v H*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Theorem

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e \in G$ je jednotka v H*
2. *obraz podgrupy $K \subset G$ je podgrupa $f(K) \subset H$.*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Theorem

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e \in G$ je jednotka v H*
2. *obraz podgrupy $K \subset G$ je podgrupa $f(K) \subset H$.*
3. *vzorem $f^{-1}(K) \subset G$ podgrupy $K \subset H$ je podgrupa.*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Theorem

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e \in G$ je jednotka v H*
2. *obraz podgrupy $K \subset G$ je podgrupa $f(K) \subset H$.*
3. *vzorem $f^{-1}(K) \subset G$ podgrupy $K \subset H$ je podgrupa.*
4. *obraz inverze k prvku je inverzí obrazu. tj. $f(a^{-1}) = f(a)^{-1}$.*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Theorem

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e \in G$ je jednotka v H*
2. *obraz podgrupy $K \subset G$ je podgrupa $f(K) \subset H$.*
3. *vzorem $f^{-1}(K) \subset G$ podgrupy $K \subset H$ je podgrupa.*
4. *obraz inverze k prvku je inverzí obrazu. tj. $f(a^{-1}) = f(a)^{-1}$.*
5. *je-li f zároveň bijekcí, pak i inverzní zobrazení f^{-1} je homomorfismus.*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Theorem

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e \in G$ je jednotka v H*
2. *obraz podgrupy $K \subset G$ je podgrupa $f(K) \subset H$.*
3. *vzorem $f^{-1}(K) \subset G$ podgrupy $K \subset H$ je podgrupa.*
4. *obraz inverze k prvku je inverzí obrazu. tj. $f(a^{-1}) = f(a)^{-1}$.*
5. *je-li f zároveň bijekcí, pak i inverzní zobrazení f^{-1} je homomorfismus.*
6. *f je injektivní zobrazení právě, když $f^{-1}(e) = \{e\}$.*

Definition

Podgrupa $f^{-1}(e)$ jednotkového prvku $e \in H$ se nazývá **jádro** homomorfismu f a značíme ji $\ker f$. Bijektivní homomorfismus grup nazýváme **izomorfismus**.

Definition

Podgrupa $f^{-1}(e)$ jednotkového prvku $e \in H$ se nazývá **jádro** homomorfismu f a značíme ji $\ker f$. Bijektivní homomorfismus grup nazýváme **izomorfismus**.

Z předchozích tvrzení okamžitě vyplývá, že homomorfismus $f : G \to H$ s triviálním jádrem je izomorfismem na obraz $f(G)$.

Example

(1) Pro každou grupu permutací $G = \Sigma_n$ jsme definovali zobrazení $\mathrm{sgn} : \Sigma_n \to \mathbb{Z}_2$ přiřazující permutaci její paritu. Jde o homomorfismus grup. Jádrem tohoto homomorfismu jsou permutace se sudou paritou.

Example

(1) Pro každou grupu permutací $G = \Sigma_n$ jsme definovali zobrazení $\mathrm{sgn} : \Sigma_n \to \mathbb{Z}_2$ přiřazující permutaci její paritu. Jde o homomorfismus grup. Jádrem tohoto homomorfismu jsou permutace se sudou paritou.
(2) Grupa symetrií rovnostranného trojúhelníka je izomorfní s grupou permutací Σ_3. Zvolíme-li realizaci Σ_3 tak, že za množinu tří prvků pro permutace vezmeme vrcholy trojúhelníka a jednotlivým symetriím přiřadíme permutace těchto vrcholů, které vyvolají.

Example

(1) Pro každou grupu permutací $G = \Sigma_n$ jsme definovali zobrazení $\mathrm{sgn} : \Sigma_n \to \mathbb{Z}_2$ přiřazující permutaci její paritu. Jde o homomorfismus grup. Jádrem tohoto homomorfismu jsou permutace se sudou paritou.
(2) Grupa symetrií rovnostranného trojúhelníka je izomorfní s grupou permutací Σ_3. Zvolíme-li realizaci Σ_3 tak, že za množinu tří prvků pro permutace vezmeme vrcholy trojúhelníka a jednotlivým symetriím přiřadíme permutace těchto vrcholů, které vyvolají.
(3) Zobrazení $\exp : \mathbb{R} \to \mathbb{R}_+$ (nebo $\mathbb{C} \to \mathbb{C} \setminus 0$), je homomorfismus aditivní grupy reálných nebo komplexních čísel na multiplikativní grupu kladných reálných čísel, resp. na multiplikativní grupu všech nenulových komplexních čísel. V případě reálných čísel jde o izomorfismus. Pro komplexní čísla dostáváme netriviální jádro $2k\pi i$, $k \in \mathbb{Z}$.

Example

(4) Determinant matice je zobrazením, které každé matici skalárů z $\mathbb{K}$ přiřazuje nějaký skalár v $\mathbb{K}$ (pracovali jsme s $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$). Cauchyova věta o determinantu součinu čtvercových matic $\det(A \cdot B) = (\det A) \cdot (\det B)$ je tvrzením, že pro grupu $G = GL(n, \mathbb{K})$ invertibilních matic je $\det : G \to \mathbb{K} \setminus 0$ homomorfismem grup.

Example

(4) Determinant matice je zobrazením, které každé matici skalárů z $\mathbb{K}$ přiřazuje nějaký skalár v $\mathbb{K}$ (pracovali jsme s $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$). Cauchyova věta o determinantu součinu čtvercových matic $\det(A \cdot B) = (\det A) \cdot (\det B)$ je tvrzením, že pro grupu $G = GL(n, \mathbb{K})$ invertibilních matic je $\det : G \to \mathbb{K} \setminus 0$ homomorfismem grup.

(5) Pro každé dvě grupy G, H definujeme **součin grup** $G \times H$ takto: Jako množina je $G \times H$ skutečně součin a násobení definujeme po složkách. tj. $(a, x) \cdot (b, y) = (a \cdot b, x \cdot y)$. Zobrazení

$$p_G : G \times H \ni (a, x) \mapsto a \in G, \quad p_H : G \times H \ni (a, x) \mapsto x$$

jsou surjektivní homomorfismy s jádry

$$\ker p_G = \{(e_G, x);\ x \in H\} \qquad \ker p_H = \{(a, e_H); a \in G\}.$$

Example

(6) Grupy zbytkových tříd $\mathbb{Z}_k$ jsou izomorfní grupám komplexních k–tých odmocnin z jedničky, což jsou zároveň izomorfní obrazy konečných grup otočení v rovině o celé násobky úhlu $\frac{2\pi}{k}$.

Example

(6) Grupy zbytkových tříd $\mathbb{Z}_k$ jsou izomorfní grupám komplexních k–tých odmocnin z jedničky, což jsou zároveň izomorfní obrazy konečných grup otočení v rovině o celé násobky úhlu $\frac{2\pi}{k}$.
(7) Grupa $\mathbb{Z}_6$ je izomorfní součinu $\mathbb{Z}_2 \times \mathbb{Z}_3$. Skutečně, $\mathbb{Z}_6 \subset \mathbb{C}^*$ je tvořeno body na jednotkové kružnici v komplexní rovině ve vrcholech pravidleného šestiúhelníku, $\mathbb{Z}_2$ pak odpovídá ± 1, $\mathbb{Z}_3$ pravidelnému trojúhelníku s jedním vrcholem v jedničce. Jestliže budeme ztotožňovat příslušné body s otočeními v rovině, které jedničku převede právě do nich, pak skládání dvou takových otočení bude vždy komutativní a kombinacemi jednoho otočení ze $\mathbb{Z}_2$ a jednoho ze $\mathbb{Z}_3$ dostaneme právě všechna otočení ze $\mathbb{Z}_6$.

Example

(6) Grupy zbytkových tříd $\mathbb{Z}_k$ jsou izomorfní grupám komplexních k–tých odmocnin z jedničky, což jsou zároveň izomorfní obrazy konečných grup otočení v rovině o celé násobky úhlu $\frac{2\pi}{k}$.
(7) Grupa $\mathbb{Z}_6$ je izomorfní součinu $\mathbb{Z}_2 \times \mathbb{Z}_3$. Skutečně, $\mathbb{Z}_6 \subset \mathbb{C}^*$ je tvořeno body na jednotkové kružnici v komplexní rovině ve vrcholech pravidleného šestiúhelníku, $\mathbb{Z}_2$ pak odpovídá ± 1, $\mathbb{Z}_3$ pravidelnému trojúhelníku s jedním vrcholem v jedničce. Jestliže budeme ztotožňovat příslušné body s otočeními v rovině, které jedničku převede právě do nich, pak skládání dvou takových otočení bude vždy komutativní a kombinacemi jednoho otočení ze $\mathbb{Z}_2$ a jednoho ze $\mathbb{Z}_3$ dostaneme právě všechna otočení ze $\mathbb{Z}_6$.
V aditivní notaci vypadá izomorfismus takto:

$$[0]_6 \mapsto ([0]_2, [0]_3),\ [1]_6 \mapsto ([1]_2, [2]_3)$$
$$[2]_6 \mapsto ([0]_2, [1]_3),\ [3]_6 \mapsto ([1]_2, [0]_3)$$
$$[4]_6 \mapsto ([0]_2, [2]_3),\ [5]_6 \mapsto ([1]_2, [1]_3)$$

Libovolný prvek a v grupě G je obsažen v minimální podgrupě $\{a, a^2, a^3, \dots\}$, která jej obsahuje.
Je zjevné, že je tato podgrupa komutativní, a pokud je celá grupa G konečná, nutně musí jednou nastat případ $a^k = e$.

Libovolný prvek a v grupě G je obsažen v minimální podgrupě $\{a, a^2, a^3, \dots\}$, která jej obsahuje.
Je zjevné, že je tato podgrupa komutativní, a pokud je celá grupa G konečná, nutně musí jednou nastat případ $a^k = e$.
Nejmenší k s touto vlastností nazýváme **řád prvku** a v G. Grupa G je **cyklická grupa** je-li celé G generované nějakým svým prvkem a výše uvedeným způsobem.

Libovolný prvek a v grupě G je obsažen v minimální podgrupě $\{a, a^2, a^3, \dots\}$, která jej obsahuje.
Je zjevné, že je tato podgrupa komutativní, a pokud je celá grupa G konečná, nutně musí jednou nastat případ $a^k = e$.
Nejmenší k s touto vlastností nazýváme **řád prvku** a v G. Grupa G je **cyklická grupa** je-li celé G generované nějakým svým prvkem a výše uvedeným způsobem.
Z definice přímo vyplývá, že každá cyklická grupa je izomorfní buď grupě celých čísel $\mathbb{Z}$ (pokud je nekonečná) nebo některé grupě zbytkových tříd $\mathbb{Z}_k$ (když je konečná).

Plán přednášky

1 Literatura

2 Grupy a grupoidy

3 Symetrie „logotypů“ a „dláždění“

4 Homomorfismy grup

5 Rozklady a faktorgrupy

Uvažme grupu G a její podgrupu H. Na množině prvků grupy G definujeme relaci $a \sim_H b$ jestliže $b^{-1} \cdot a \in H$.
Je to relace ekvivalence:

Uvažme grupu G a její podgrupu H. Na množině prvků grupy G definujeme relaci $a \sim_H b$ jestliže $b^{-1} \cdot a \in H$.
Je to relace ekvivalence:

- $a^{-1} \cdot a = e \in H$,

Uvažme grupu G a její podgrupu H. Na množině prvků grupy G definujeme relaci $a \sim_H b$ jestliže $b^{-1} \cdot a \in H$.
Je to relace ekvivalence:

- $a^{-1} \cdot a = e \in H$,
- je-li $b^{-1} \cdot a = h \in H$, potom $a^{-1} \cdot b = (b^{-1} \cdot a)^{-1} = h^{-1} \in H$,

Uvažme grupu G a její podgrupu H. Na množině prvků grupy G definujeme relaci $a \sim_H b$ jestliže $b^{-1} \cdot a \in H$.
Je to relace ekvivalence:

- $a^{-1} \cdot a = e \in H$,
- je-li $b^{-1} \cdot a = h \in H$, potom $a^{-1} \cdot b = (b^{-1} \cdot a)^{-1} = h^{-1} \in H$,
- je-li $c^{-1} \cdot b \in H$ a zároveň je $b^{-1} \cdot a \in H$, potom $c^{-1} \cdot a = c^{-1} \cdot b \cdot b^{-1} \cdot a \in H$.

Celá grupa G se tedy rozpadá na tzv. **levé třídy rozkladu** podle podgrupy H vzájemně ekvivalentních prvků.

Celá grupa G se tedy rozpadá na tzv. **levé třídy rozkladu** podle podgrupy H vzájemně ekvivalentních prvků.
Třídu příslušející prvku a značíme $a \cdot H$ a skutečně platí, že

$$a \cdot H = \{a \cdot h;\ h \in H\},$$

neboť prvek b je ve stejné třídě s a, právě když jde takovýmto způsobem vyjádřit.

Celá grupa G se tedy rozpadá na tzv. **levé třídy rozkladu** podle podgrupy H vzájemně ekvivalentních prvků.
Třídu příslušející prvku a značíme $a \cdot H$ a skutečně platí, že

$$a \cdot H = \{a \cdot h;\ h \in H\},$$

neboť prvek b je ve stejné třídě s a, právě když jde takovýmto způsobem vyjádřit.
Množinu všech levých tříd rozkladu podle podgrupy H označujeme G/H.

Celá grupa G se tedy rozpadá na tzv. **levé třídy rozkladu** podle podgrupy H vzájemně ekvivalentních prvků.
Třídu příslušející prvku a značíme $a \cdot H$ a skutečně platí, že

$$a \cdot H = \{a \cdot h;\ h \in H\},$$

neboť prvek b je ve stejné třídě s a, právě když jde takovýmto způsobem vyjádřit.
Množinu všech levých tříd rozkladu podle podgrupy H označujeme G/H.
Obdobně definujeme pravé třídy rozkladu $H \cdot a$. Příslušná ekvivalence je: $a \sim b$, jestliže $a \cdot b^{-1} \in H$. Proto

$$H \setminus G = \{H \cdot a;\ a \in G\}.$$

Theorem

Pro třídy rozkladu grupy platí:

Theorem

Pro třídy rozkladu grupy platí:

1. *Levé a pravé třídy rozkladu podle podgrupy $H \subset G$ splývají právě, když pro každé $a \in G$, $h \in H$ platí $a \cdot h \cdot a^{-1} \in H$.*

Theorem

Pro třídy rozkladu grupy platí:

1. *Levé a pravé třídy rozkladu podle podgrupy $H \subset G$ splývají právě, když pro každé $a \in G$, $h \in H$ platí $a \cdot h \cdot a^{-1} \in H$.*
2. *Všechny třídy (levé i pravé) mají shodnou mohutnost s podgrupou H.*

Corollary

Nechť G je konečná grupa s n prvky, H její podgrupa. Potom

Corollary

Nechť G je konečná grupa s n prvky, H její podgrupa. Potom

1. *Mohutnost $n = |G|$ je součinem mohutnosti H a mohutnosti G/H, tj.*

$$|G| = |G/H| \cdot |H|$$

Corollary

Nechť G je konečná grupa s n prvky, H její podgrupa. Potom

1. *Mohutnost $n = |G|$ je součinem mohutnosti H a mohutnosti G/H, tj.*
$$|G| = |G/H| \cdot |H|$$
2. *Přirozené číslo $|H|$ je dělitelem čísla n.*

Corollary

Nechť G je konečná grupa s n prvky, H její podgrupa. Potom

1. *Mohutnost $n = |G|$ je součinem mohutnosti H a mohutnosti G/H, tj.*
$$|G| = |G/H| \cdot |H|$$
2. *Přirozené číslo $|H|$ je dělitelem čísla n.*
3. *Je-li $a \in G$ prvek řádu k, pak k dělí n.*

Corollary

Nechť G je konečná grupa s n prvky, H její podgrupa. Potom

1. *Mohutnost $n = |G|$ je součinem mohutnosti H a mohutnosti G/H, tj.*
$$|G| = |G/H| \cdot |H|$$
2. *Přirozené číslo $|H|$ je dělitelem čísla n.*
3. *Je-li $a \in G$ prvek řádu k, pak k dělí n.*
4. *pro každé $a \in G$ je $a^n = e$.*

Corollary

Nechť G je konečná grupa s n prvky, H její podgrupa. Potom

1. *Mohutnost $n = |G|$ je součinem mohutnosti H a mohutnosti G/H, tj.*
$$|G| = |G/H| \cdot |H|$$
2. *Přirozené číslo $|H|$ je dělitelem čísla n.*
3. *Je-li $a \in G$ prvek řádu k, pak k dělí n.*
4. *pro každé $a \in G$ je $a^n = e$.*
5. *je-li mohutnost grupy G prvočíslo, pak je G izomorfní cyklické grupě $\mathbb{Z}_n$.*

Corollary

Nechť G je konečná grupa s n prvky, H její podgrupa. Potom

1. *Mohutnost $n = |G|$ je součinem mohutnosti H a mohutnosti G/H, tj.*
$$|G| = |G/H| \cdot |H|$$
2. *Přirozené číslo $|H|$ je dělitelem čísla n.*
3. *Je-li $a \in G$ prvek řádu k, pak k dělí n.*
4. *pro každé $a \in G$ je $a^n = e$.*
5. *je-li mohutnost grupy G prvočíslo, pak je G izomorfní cyklické grupě $\mathbb{Z}_n$.*

Druhému tvrzení se říkává Lagrangeova věta, předposlednímu malá Fermatova věta.

Podgrupy H, pro které platí, že $a \cdot h \cdot a^{-1} \in H$ pro všechny $a \in G$, $h \in H$, se nazývají **normální podgrupy**.

Podgrupy H, pro které platí, že $a \cdot h \cdot a^{-1} \in H$ pro všechny $a \in G$, $h \in H$, se nazývají **normální podgrupy**.
Pro normální podgrupy je dobře definováno násobení na G/H vztahem

$$(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H.$$

Skutečně, volbou jiných reprezentantů $a \cdot h$, $b \cdot h'$ dostaneme opět stejný výsledek

$$(a \cdot h \cdot b \cdot h') \cdot H = ((a \cdot b) \cdot (b^{-1} \cdot h \cdot b) \cdot h') \cdot H.$$

Podgrupy H, pro které platí, že $a \cdot h \cdot a^{-1} \in H$ pro všechny $a \in G$, $h \in H$, se nazývají **normální podgrupy**.
Pro normální podgrupy je dobře definováno násobení na G/H vztahem

$$(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H.$$

Skutečně, volbou jiných reprezentantů $a \cdot h$, $b \cdot h'$ dostaneme opět stejný výsledek

$$(a \cdot h \cdot b \cdot h') \cdot H = ((a \cdot b) \cdot (b^{-1} \cdot h \cdot b) \cdot h') \cdot H.$$

Násobení na G/H má všechny vlastnosti grupy.

V komutativních grupách jsou všechny podgrupy normální.
Podmnožina

$$n\mathbb{Z} = \{na;\ a \in \mathbb{Z}\} \subset \mathbb{Z}$$

zadává v celých číslech podgrupu a její faktorgrupou je právě (aditivní) grupa zbytkových tříd $\mathbb{Z}_n$.

V komutativních grupách jsou všechny podgrupy normální.
Podmnožina

$$n\mathbb{Z} = \{na;\ a \in \mathbb{Z}\} \subset \mathbb{Z}$$

zadává v celých číslech podgrupu a její faktorgrupou je právě (aditivní) grupa zbytkových tříd $\mathbb{Z}_n$.
Všechna jádra homomorfismů jsou normální podgrupy. Naopak, jestliže je podgrupa $H \subset G$ normální, pak zobrazení

$$p : G \to G/H, \quad a \mapsto a \cdot H$$

je surjektivní homomorfismus grup s jádrem H. Skutečně, p je dobře definované, přímo z definice násobení na G/H je vidět, že to musí být homomorfismus a je zjevně na. Je tedy vidět, že normální podgrupy jsou právě všechna jádra homomorfismů.

Pro libovolný homomorfismus grup $f : G \to K$ je dobře definován také homomorfismus

$$\tilde{f} : G/\ker f \to K,\ \tilde{f}(a \cdot H) = f(a),$$

který je injektivní.

Pro libovolný homomorfismus grup $f : G \to K$ je dobře definován také homomorfismus

$$\tilde{f} : G/\ker f \to K,\ \tilde{f}(a \cdot H) = f(a),$$

který je injektivní.
Zdánlivě paradoxní je příklad homomorfismu $\mathbb{C}^* \to \mathbb{C}^*$ definovaný na nenulových komplexních číslech vztahem $z \mapsto z^k$ s přirozeným k. Zjevně jde o surjektivní homomorfismus a jeho jádro je množina k–tých odmocnin z jedničky, tj. cyklická podgrupa $\mathbb{Z}_k$. Předchozí úvaha tedy dává pro všechna přirozená k izomorfismus

$$\tilde{f} : \mathbb{C}^*/\mathbb{Z}_k \to \mathbb{C}^*.$$

Tento příklad ukazuje, že u nekonečných grup nejsou počty s mohutnostmi tak přehledný jako u konečných grup