

# Abelovy grupy

7. a 8. přednáška z kryptografie

# Obsah

- 1 Grupy a Abelovy grupy
- 2 Podgrupy
- 3 Grupové homomorfismy

# Grupy a Abelovy grupy

## Definice

- Množina  $G$  s binární operací  $*$  tvoří *grupu*, pokud je operace  $*$  asociativí, má neutrální prvek a má všechny inverzní prvky.
- Grupa, jejíž operace je navíc komutativní, se nazývá komutativní grupa nebo *Abelova grupa*.

## Příklady

- $(\mathbb{Z}_n, +)$  je Abelova grupa řádu  $n$  (aditivní grupa)
- $(\mathbb{Z}_n, \cdot)$  není grupa, neboť neexistuje inverzní prvek např. k 0
- $(\mathbb{Z}_n^*, \cdot)$  je Abelova grupa řádu  $\varphi(n)$  (multiplikativní grupa)

Poznámka: Počet prvků grupy se nazývá *řád grupy*.

# Grupy a Abelovy grupy

## Aditivní a multiplikatívni zápis

- Aditivní notace:  $(G, +, 0, -(\cdot))$   
operace  $+$ , nulový prvek  $0$ , opačný prvek k  $a$  je  $-a$ ;  
iterované sčítání je násobek  $\underbrace{a + a + \dots + a}_{k\text{-krát}} = ka$
- Multiplikatívni notace:  $(G, \cdot, 1, (\cdot)^{-1})$   
operace  $\cdot$ , jednotkový prvek  $1$ , inverzní prvek k  $a$  je  $a^{-1}$ ;  
iterované násobení je mocninu  $\underbrace{a \cdot a \cdot \dots \cdot a}_{k\text{-krát}} = a^k$

Poznámka: Většinou budeme používat multiplikatívni zápis.

# Grupy a Abelovy grupy

## Celočíselné mocniny

Nechť  $(G, \cdot)$  je grupa s neutrálním prvkem  $1$ ,  $a \in G$ ,  $k \in \mathbb{Z}$ .  
Celočíselnou mocninu prvku  $a$  definujeme takto:

- pro  $k > 0$  je  $a^k = \underbrace{a \cdot a \cdot \dots \cdot a}_{k\text{-krát}}$  (díky asociativitě)
- $a^0 = 1$  (díky neutrálnímu prvku)
- pro  $k < 0$  je  $a^k = (a^{-1})^{|k|}$  (díky inverznímu prvku)

## Tvrzení

Platí známé vzorce:  $a^{k+l} = a^k a^l$ ,  $(a^k)^l = a^{kl}$   
V Abelově grupě také:  $(ab)^k = a^k b^k$

# Grupy a Abelovy grupy

## Tvrzení

Nechť  $(G, \cdot)$  je grupa.

- Neutrální prvek je určen jednoznačně.  
Je-li  $e$  levý neutrální prvek,  $f$  pravý neutrální prvek,  
pak  $e = f$  je neutrální prvek.
- Inverzní prvek k prvku  $a$  je určen jednoznačně.  
Je-li  $b$  levý inverzní prvek k  $a$ ,  $c$  pravý inverzní prvek k  $a$ ,  
pak  $b = c$  je inverzní prvek k  $a$ .
- Socks and shoes lemma:  
V (nekomutativní) grupě je  $(ab)^{-1} = b^{-1}a^{-1}$ .

# Grupy a Abelovy grupy

## Tvrzení

Nechť  $(G, \cdot)$  je grupa.

- V grupě  $G$  lze krátit libovolným prvkem, tj. pro každé  $a \in G$  platí: je-li  $a \cdot x = a \cdot y$ , pak je  $x = y$ .

Tato vlastnost grupy necharakterizuje: v  $(\mathbb{Z}, \cdot)$  lze také krátit libovolným prvkem, přestože to není grupa.

- V grupě  $G$  mají všechny lineární rovnice  $a \cdot x = b$ ,  $y \cdot a = b$  řešení a to je jediné.

Tato vlastnost grupy charakterizuje: Každá pologrupa, v níž mají všechny lineární rovnice řešení, je už grupou.

- Levá translace libovolným prvkem  $a \in G$ ,  
 $I_a : G \rightarrow G : x \mapsto a \cdot x$ , je vzájemně jednoznačné zobrazení.

# Okruhy a tělesa

## Poznámka

- $(R, +, \cdot)$  se nazývá *okruh*, jestliže  $(R, +)$  je komutativní grupa,  $(R, \cdot)$  je pologrupa a platí oba distributivní zákony. Netriviální okruh s jednotkou se nazývá *obor*, pokud v něm lze krátit libovolným nenulovým prvkem. Netriviální okruh je *těleso*, pokud je  $(R - \{0\}, \cdot)$  grupa.
- Netriviální okruh je tělesem, právě když všechny lineární rovnice  $a \cdot x = b$ ,  $y \cdot a = b$ , kde  $a \neq 0$ , mají řešení.
- Každý konečný obor je tělesem, neboť prosté zobrazení  $l_a$  z konečné množiny do sebe už je vzájemně jednoznačné.



## Grupy a Abelovy grupy

### Definice

Jsou-li  $G_1, \dots, G_k$  grupy, pak množina  $G_1 \times \dots \times G_k$  všech  $k$ -tic spolu s operací, kterou provádíme "po souřadnicích" (v  $i$ -té souřadnici se počítá jako v  $G_i$ ) je také grupa. Nazývá se *direktní součin* grup  $G_1, \dots, G_k$ .

Jsou-li všechny grupy stejné,  $G_i = G$  pro  $1 \leq i \leq k$ , mluvíme o direktní mocnině a značíme  $G^{\times k}$ .

### Poznámka

S direktním součinem grup jsme se setkali u Čínské věty o zbytcích. Např.  $\mathbb{Z}_{15} \simeq \mathbb{Z}_3 \times \mathbb{Z}_5$ .

# Podgrupy

## Definice

Podmnožina  $H$  grupy  $(G, \cdot, 1, (-)^{-1})$  tvoří *podgrupu*, pokud pro každé  $a, b \in H$  platí:

- je-li  $a, b \in H$ , tak  $ab \in H$
- $1 \in H$
- je-li  $a \in H$ , pak  $a^{-1} \in H$

Aneb podgrupa je podmnožina uzavřená na binární operaci, neutrální prvek a inverzní prvky.

# Podgrupy

## Tvrzení

Nechť  $G$  je grupa a  $\emptyset \neq H \subseteq G$ . Následující tvrzení jsou ekvivalentní:

- $H$  je podgrupa v  $G$
- pro všechny  $a, b \in G$ : je-li  $a, b \in H$ , tak  $ab \in H$  a  $a^{-1} \in H$
- pro všechny  $a, b \in G$ : je-li  $a, b \in H$ , tak  $ab^{-1} \in H$

## Tvrzení

Nechť  $H_1, H_2$  jsou podgrupy v grupě  $G$ .

- $H_1 \cap H_2$  je podgrupa v  $G$ .
- Je-li  $G$  Abelova grupa, pak  $H_1 \cdot H_2 = \{h_1 h_2; h_1 \in H_1, h_2 \in H_2\}$  je podgrupa v  $G$ .

# Podgrupy

## Příklady

Nechť  $G$  je grupa.

- Zřejmě  $\{1\}$  a  $G$  jsou podgrupy v grupě  $G$ .
- Množina všech celých mocnin prvku  $a \in G$ ,  $M = \{a^k, k \in \mathbb{Z}\}$  tvoří podgrupu grupy  $G$ . Nazýváme ji *cyklická podgrupa* generovaná prvkem  $a$ , značíme ji  $\langle a \rangle$ .

Při aditivním značení grupy  $(G, +)$  by cyklická grupa  $\langle a \rangle$  byla podgrupou všech celých násobků prvku  $a$ .

## Podgrupy v $\mathbb{Z}$ a v $\mathbb{Z}_n$

### Tvrzení

Každá podgrupa v  $(\mathbb{Z}, +)$  je tvaru  $m\mathbb{Z}$  pro nějaké  $m \in \mathbb{Z}$ .  
Navíc:  $m_1\mathbb{Z} \subseteq m_2\mathbb{Z}$  právě, když  $m_2 \mid m_1$ .

### Tvrzení

Každá podgrupa v  $(\mathbb{Z}_n, +)$  je tvaru  $d\mathbb{Z}_n$  pro nějaké  $d \in \mathbb{Z}$ ,  
kde  $d \mid n$ .  
Navíc:  $d_1\mathbb{Z}_n \subseteq d_2\mathbb{Z}_n$  právě, když  $d_2 \mid d_1$ .

Tedy všechny podgrupy v  $(\mathbb{Z}_n, +)$  jsou cyklické a pro každého dělitele  $d$  čísla  $n$  je zde právě jedna podgrupa tvaru  $d\mathbb{Z}_n$ .  
Tato podgrupa má  $\frac{n}{d}$  prvků.

## Levé třídy podle podgrupy

### Definice

Nechť  $G$  je grupa,  $H$  je podgrupa v  $G$ ,  $a \in G$ .

**Levá třída podle podgrupy  $H$**  určená prvkem  $a$  je množina  $aH = \{ah, h \in H\}$ .

Analogicky se definuje pravá třída  $Ha$ .

### Poznámka

Je-li  $G$  Abelova grupa, pak  $aH = Ha$  pro každé  $a \in G$ .

Počet různých (levých) tříd se nazývá **index podgrupy  $H$**  v grupě  $G$ , značí se  $[G : H]$ .

## Levé třídy podle podgrupy

### Tvrzení

- Pro každé  $a \in G$  je  $|aH| = |H|$ .
- Všechny levé třídy tvoří rozklad na množině  $G$ , tj.  $G = \bigcup_{a \in G} aH$  a třídy  $aH$ ,  $bH$  jsou buď stejné, nebo disjunktní.

### Lagrangeova věta

Nechť  $G$  je konečná grupa a  $H$  je podgrupa grupy  $G$ .  
Pak řád podgrupy  $H$  dělí řád grupy  $G$ , přesněji  $|G| = [G : H] \cdot |H|$ .

### Poznámka

Pro podpologrupy konečné pologrupy podobná věta neplatí. Např. v pologrupě levých nul je každá podmnožina podpologrupou.

## Faktorová grupa podle podgrupy

### Tvrzení

Nechť  $G$  je Abelova grupa a  $H$  je podgrupa v  $G$ .

- Předpisem  $aH \cdot bH = abH$  je korektně definována operace na množině tříd. (Díky komutativitě výsledek nezávisí na volbě representantů tříd).
- Množina všech tříd grupy  $G$  podle podgrupy  $H$  spolu s touto operací tvoří opět grupu. Nazývá se *faktorová grupa* grupy  $G$  podle podgrupy  $H$  a značí se  $G/H$ .

### Poznámka

Nekomutativní grupu  $G$  lze faktorizovat jen podle *normální podgrupy*  $H$ , tj. jen když platí  $aH = Ha$  pro všechny  $a \in G$ .



## Kongruence podle podgrupy

### Příklad

$$(\mathbb{Z}/n\mathbb{Z}, +) = (\mathbb{Z}_n, +)$$

Přitom  $\mathbb{Z}_n$  jsme vytvořili faktorizací podle kongruence modulo  $n$ ,  $a \equiv b \pmod{n}$ , právě když  $n \mid a - b$ , právě když  $a - b \in n\mathbb{Z}$ .

### Definice

Nechť  $G$  je Abelova grupa,  $H$  je podgrupa v  $G$ ,  $a, b \in G$ .  
Řekneme, že  $a$  je *kongruentní s  $b$  podle podgrupy  $H$* ,  
 $a \equiv b \pmod{H}$ , pokud  $ab^{-1} \in H$ .

### Tvrzení

Následující tvrzení jsou ekvivalentní:

$$a \equiv b \pmod{H} \quad \text{iff} \quad Ha = Hb \quad \text{iff} \quad a = hb \text{ pro nějaké } h \in H.$$

# Kongruence podle podgrupy

## Tvrzení

- Kongruence podle podgrupy je relace ekvivalence na množině  $G$ , tedy rozloží  $G$  na třídy a to jsou přesně třídy  $aH$ , kde  $a \in G$ . (Toto platí pro všechny grupy.)
- Kongruence podle podgrupy je zachována při binární operaci (toto platí jen pro Abelovy grupy), tudíž lze definovat binární operaci na třídách přes representanty.
- Vznikne tak faktorová grupa grupy  $G$  podle kongruence modulo  $H$ , což je přesně grupa  $G/H$ .

Pro nekomutativní grupy lze zavést kongruenci jen modulo normální podgrupa.

## Faktorový okruh podle ideálu

### Poznámka

- Nechť  $(R, +, \cdot)$  je komutativní okruh. Podmnožina  $I \subset R$  se nazývá *ideál* okruhu  $R$ , jestliže
  - $(I, +)$  je podgrupa grupy  $(R, +)$ ,
  - pro všechny  $r \in R$  a všechny  $i \in I$  je  $r \cdot i \in I$ .
- Chceme-li vytvořit *faktorový komutativní okruh*, musíme použít ideál, pak lze přes reprezentanty korektně definovat sčítání i násobení na třídách.
- Každý ideál v  $\mathbb{Z}$  je tvaru  $m\mathbb{Z}$  pro nějaké  $m \in \mathbb{Z}$ . Faktorový okruh je  $(\mathbb{Z}/m\mathbb{Z}, +, \cdot) = (\mathbb{Z}_m, +, \cdot)$  okruh zbytkových tříd modulo  $m$ .

# Grupové homomorfismy

## Definice

Nechť  $(G_1, \cdot)$ ,  $(G_2, \circ)$  jsou grupy.

Zobrazení  $f : G_1 \rightarrow G_2$  se nazývá *grupový homomorfismus*, pokud pro všechna  $a, b \in G_1$  platí:

- $f(a \cdot b) = f(a) \circ f(b)$
- $f(1) = 1$
- $f(a^{-1}) = f(a)^{-1}$

## Tvrzení

Nechť  $(G_1, \cdot)$ ,  $(G_2, \circ)$  jsou grupy.

Zobrazení  $f : G_1 \rightarrow G_2$  je grupový homomorfismus, právě když pro všechna  $a, b \in G_1$  je  $f(a \cdot b) = f(a) \circ f(b)$ .

# Grupové homomorfismy

## Příklady

- Pro libovolné grupy  $G_1, G_2$  je zobrazení  $f : G_1 \rightarrow G_2 : a \mapsto 1$  grupový homomorfismus.
- Necht'  $H$  je podgrupa grupy  $G$ . Vnoření  $i : H \rightarrow G$  a přirozená projekce  $\pi : G \rightarrow G/H : a \mapsto aH$  jsou grupové homomorfismy.
- Pro libovolnou grupu  $G$  pro libovolné  $a \in G$  je  $f : (Z, +) \rightarrow G : z \mapsto a^z$  grupový homomorfismus.
- Pro libovolnou Abelovu grupu  $G$  je  $m$ -tá mocnina  $\rho : G \rightarrow G : a \mapsto a^m$  grupový homomorfismus.

# Grupové isomorfismy

## Definice

Nechť  $(G_1, \cdot)$ ,  $(G_2, \circ)$  jsou grupy.

Grupový homomorfismus  $f : G_1 \rightarrow G_2$ , který je navíc vzájemně jednoznačným zobrazením, se nazývá *grupový isomorfismus*.

## Tvrzení

Nechť  $n = \prod_{i=1}^k p_i^{e_i}$ , kde prvočísla  $p_i$  jsou navzájem různá.

Zobrazení  $\theta : \mathbb{Z}_n \rightarrow \mathbb{Z}_{p_1^{e_1}} \times \dots \times \mathbb{Z}_{p_k^{e_k}} : a \mapsto (a_1, \dots, a_k)$ ,

kde  $0 \leq a_i < p_i^{e_i}$  splňují  $a \equiv a_i \pmod{p_i^{e_i}}$ ,

je grupový izomorfismus aditivních grup:  $\mathbb{Z}_n \cong \prod_{i=1}^k \mathbb{Z}_{p_i^{e_i}}$

Restrikce zobrazení  $\theta$  na množinu  $\mathbb{Z}_n^*$  je grupový isomorfismus

multiplikativních grup:  $\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \dots \times \mathbb{Z}_{p_k^{e_k}}^*$

# Okruhové homomorfismy

## Poznámka

- Necht'  $(R_1, +, \cdot)$ ,  $(R_2, +, \cdot)$  jsou komutativní okruhy s jednotkou. Zobrazení  $f : R_1 \rightarrow R_2$  se nazývá *okruhový homomorfismus*, pokud je to grupový homomorfismus aditivních grup a respektuje násobení a jednotkový prvek.
- $f$  je okruhový homomorfismus, pokud pro všechna  $a, b \in R_1$  platí:  $f(a + b) = f(a) + f(b)$ ,  $f(a \cdot b) = f(a) \cdot f(b)$ ,  $f(1) = 1$ .
- Čínské zbytkové zobrazení  $\theta$  je okruhový isomorfismus.

# Grupové isomorfismy

## Tvrzení

Nechť  $G$  je Abelova grupa,  $H_1, H_2$  jsou její podgrupy.  
Pokud  $H_1 \cap H_2 = \{1\}$ , pak  $H_1 \times H_2 \cong H_1 \cdot H_2$ ,  
zobrazení  $f : H_1 \times H_2 \rightarrow H_1 \cdot H_2 : (h_1, h_2) \mapsto h_1 h_2$  je grupový isomorfismus.

## Definice

Nechť  $G$  je Abelova grupa,  $H_1, H_2$  jsou její podgrupy.  
Pokud  $G = H_1 \cdot H_2$  a  $H_1 \cap H_2 = \{1\}$ , pak je grupa  $G$  *vnitřním direktním součinem* podgrup  $H_1$  a  $H_2$ . Značíme  $G = H_1 \dot{\times} H_2$ .

Podle tvrzení výše se pak dá každý prvek  $g \in G$  jednoznačně zapsat ve tvaru  $g = h_1 h_2$  pro nějaká  $h_1 \in H_1, h_2 \in H_2$ .



# Grupové homomorfismy

## Definice

Nechť  $f : G_1 \rightarrow G_2$  je grupový homomorfismus.

- *Obraz* homomorfismu je množina  $Im f = \{b \in G_2; b = f(a) \text{ pro nějaké } a \in G_1\}$ .
- *Jádro* homomorfismu je množina  $Ker f = \{a \in G_1; f(a) = 1\}$ .

## Tvrzení

Nechť  $f : G_1 \rightarrow G_2$  je grupový homomorfismus.

- $Ker f$  je podgrupa grupy  $G_1$  (dokonce normální podgrupa).
- $Im f$  je podgrupa grupy  $G_2$ .
- Obraz podgrupy je podgrupa a vzor podgrupy je podgrupa.
- $f$  je prostý homomorfismus, právě když  $Ker f = \{1\}$ .

# Grupové homomorfismy

## 1.věta o isomorfismu

Nechť  $f : G \rightarrow G'$  je grupový homomorfismus.

Pak  $G/\text{Ker } f \cong \text{Im } f$ .

Speciálně zobrazení  $\varphi : G/\text{Ker } f \rightarrow G' : a \text{Ker } f \mapsto f(a)$  je prostý grupový homomorfismus, jehož obrazem je  $\text{Im } f$ .

Aneb platí  $\varphi \circ \pi = f$ , kde  $\pi$  je přirozená projekce a operace  $\circ$  je skládání zobrazení.

## Poznámka

Nechť  $f : R \rightarrow R'$  je okruhový homomorfismus, pak  $R/\text{Ker } f \cong \text{Im } f$ .

Faktorový okruh  $R/\text{Ker } f$  lze vytvořit, protože  $\text{Ker } f$  je ideál.

# Grupové homomorfismy

## Důsledek

Nechť  $f : G \rightarrow G'$  je grupový (okruhový) homomorfismus.  
Pak každý prvek  $b \in \text{Im } f$  má stejně vzorů.

Je-li prvek  $a$  jedním řešením rovnice  $f(x) = b$ , pak rovnici řeší právě všechny prvky z třídy  $a \text{ Ker } f$ .

Každé řešení má tvar  $x = ac$ , kde  $c$  je řešení rovnice  $f(x) = 1$ .

Tento fakt (v aditivním tvaru) známe z řešení soustav lineárních rovnic.

# Grupové homomorfismy

## $m$ –té mocniny a odmocniny

Nechť  $G$  je Abelova grupa, pak  $\rho : G \rightarrow G : a \mapsto a^m$  je grupový homomorfismus.

- $\text{Ker } \rho = \{a \in G, a^m = 1\} = \sqrt[m]{1}$  (množina všech  $m$ -tých odmocnin z 1) tvoří podgrupu grupy  $G$ .
- $\text{Im } \rho = \{a^m, a \in G\} = G^m$  (množina všech  $m$ -tých mocnin prvků z  $G$ ) tvoří podgrupu grupy  $G$ .
- $G/\text{Ker } \rho \simeq \text{Im } \rho$  a příslušný isomorfismus je  $\varphi : a\text{Ker } \rho \mapsto a^m$ .

Tedy každý prvek  $b \in G^m$  má stejně moc  $m$ –tých odmocnin. Najdeme-li jedno řešení rovnice  $x^m = b$ , označme je  $a$ , pak každé řešení má tvar  $x = ac$ , kde  $c$  je nějaké řešení rovnice  $x^m = 1$ .

# Abelovy grupy

## Literatura

- Shoup: A Computational Introduction to Number Theory and Algebra. Kapitola 6.1-4.  
<http://shoup.net/ntb/>
- Více o okruzích najdete tamtéž v kapitole 7.