Konečné grupy

Věta. *Nechť p je prvočíslo a G je p-grupa řádu $|G| = p^2$. Pak je G komutativní.* Důkaz.

Důsledek. *Nechť p je prvočíslo. Pak existují, až na izomorfismus, právě dvě grupy řádu p^2, a sice $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Poznámka. Pro libovolnou konečnou grupu G nám Lagrangeova věta říká, že řád každé podgrupy grupy G dělí řád grupy G. Naopak se můžeme ptát, jestli pro každého dělitele d řádu grupy G existuje podgrupa H grupy G mající řád d. Takto obecně to pravda není, například grupa $\mathcal{A}_4$ řádu 12 nemá žádnou podgrupu řádu 6. Je to však pravda, je-li d mocnina prvočísla.

Věta (Cauchy). *Nechť G je konečná grupa a p prvočíslo dělící řád grupy G. Pak G obsahuje alespoň jednu podgrupu řádu p.* Důkaz.

Věta (Sylow). *Nechť G je konečná grupa, p prvočíslo a $k \in \mathbb{N}$ takové, že p^k je dělitelem řádu grupy G. Pak G obsahuje alespoň jednu podgrupu řádu p^k.*

p-Sylowské podgrupy

Definice. Nechť G je konečná grupa, p prvočíslo a $k \in \mathbb{N}$ takové, že p^k je největší mocnina p dělící řád grupy G, tj. $|G| = p^k \cdot m$, přičemž $p \nmid m$. Pak libovolná podgrupa grupy G mající řád p^k se nazývá **p-Sylowská podgrupa** grupy G (někdy též Sylowova p-podgrupa).

Příklad. Grupa $(\mathcal{S}_3, \circ)$ řádu 6 obsahuje tři 2-Sylowské podgrupy, totiž $\{\mathrm{id}, (1,2)\}$, $\{\mathrm{id}, (1,3)\}$, $\{\mathrm{id}, (2,3)\}$. Obsahuje také jedinou 3-Sylowskou podgrupu, totiž $\{\mathrm{id}, (1,2,3), (1,3,2)\}$.

Věta (Sylow). Nechť G je konečná grupa, p prvočíslo a $k \in \mathbb{N}$ takové, že $|G| = p^k \cdot m$ a $p \nmid m$. Označme r počet p-Sylowských podgrup grupy G. Pak platí

- $r \equiv 1 \pmod{p}$, $\quad r \mid m$;
- *libovolná podgrupa grupy G, jejíž řád je mocnina p, je podgrupou některé p-Sylowské podgrupy grupy G;*
- *jestliže H, K jsou p-Sylowské podgrupy grupy G, pak existuje $g \in G$ tak, že předpis $h \mapsto g \cdot h \cdot g^{-1}$ určuje izomorfismus $H \to K$.*

Struktura konečných komutativních grup

Věta. Nechť $(G, \cdot)$ je konečná komutativní grupa, $|G| > 1$. Pak existují (ne nutně různá) prvočísla $p_1, \ldots, p_s$ a $k_1, \ldots, k_s \in \mathbb{N}$ tak, že

$$(G, \cdot) \cong (\mathbb{Z}_{p_1^{k_1}}, +) \times \cdots \times (\mathbb{Z}_{p_s^{k_s}}, +).$$

Tento rozklad grupy G na součin cyklických p-grup je určen jednoznačně až na pořadí činitelů. Zřejmě platí $|G| = p_1^{k_1} \cdots p_s^{k_s}$.

Příklad. Užijme větu k tomu, abychom zjistili, jak mohou vypadat komutativní grupy řádu 8. Podle předchozí věty jde o to, jakými způsoby je možné napsat 8 jako součin mocnin prvočísel: $8 = 2^3 = 2^2 \cdot 2 = 2 \cdot 2 \cdot 2$, proto každá komutativní grupa řádu 8 je izomorfní s právě jednou z grup $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Zdůrazněme, že tento výčet se týká jen komutativních grup, existují i nekomutativní grupy řádu 8, například grupa symetrií čtverce $\mathbb{D}_4$.

Okruhy

Definice. Množina R spolu se dvěma operacemi $+$ a $\cdot$ se nazývá **okruh**, jestliže platí:

- $(R, +)$ je komutativní grupa,
- $(R, \cdot)$ je pologrupa s neutrálním prvkem,
- platí distributivní zákony, tj. pro libovolné prvky $a, b, c \in R$ je $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a$ (užíváme obvyklou konvenci o tom, že násobení má přednost před sčítáním).

Příklady. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ jsou okruhy.
Pro libovolné $m \in \mathbb{N}$ je $(\mathbb{Z}_m, +, \cdot)$ okruh. Důkaz distributivního zákona.
Množina všech čtvercových matic $M_{n,n}(R)$, kde R značí $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$ a $n \in \mathbb{N}$, tvoří okruh $(M_{n,n}(R), +, \cdot)$.
Množina všech polynomů $R[x]$, kde R značí $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$, tvoří okruh $(R[x], +, \cdot)$.

Příklad. $(\mathbb{N}, +, \cdot)$ okruhem není.

Okruhy

Definice. $(R, +, \cdot)$ je **okruh**, jestliže:

- $(R, +)$ je komutativní grupa,
- $(R, \cdot)$ je pologrupa s neutrálním prvkem,
- platí distributivní zákony, tj. pro libovolné prvky $a, b, c \in R$ je $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$

Označení. Neutrální prvek grupy $(R, +)$ značíme 0 a nazýváme **nula okruhu** R, zatímco neutrální prvek pologrupy $(R, \cdot)$ značíme 1 a nazýváme **jednička okruhu** R.
Inverzní prvek k prvku $a \in R$ v grupě $(R, +)$ se nazývá **opačný prvek**, značíme $-a$.
Symbolem $a - b$ rozumíme $a + (-b)$.
Mocninu prvku $a \in R$ nazýváme **násobek prvku** a značíme na pro libovolné $n \in \mathbb{Z}$.
Součet $a_1 + \cdots + a_n$ prvků okruhu R lze stručně zapsat $\sum_{i=1}^{n} a_i$.

Základní vlastnosti okruhů

Definice. Okruh $(R, +, \cdot)$ se nazývá **triviální**, má-li R jediný prvek.

Věta. *Nechť R je okruh. Pak platí*

- $\forall a \in R: \ a \cdot 0 = 0 \cdot a = 0,$ *Důkaz.*
- $\forall a, b \in R: \ (-a) \cdot b = a \cdot (-b) = -(a \cdot b),$
- $\forall a, b, c \in R:$
  $a \cdot (b - c) = a \cdot b - a \cdot c, \quad (b - c) \cdot a = b \cdot a - c \cdot a,$
- $\forall n, m \in \mathbb{N} \ \forall a_1, \ldots, a_n, b_1, \ldots, b_m \in R:$
  $(a_1 + \cdots + a_n) \cdot (b_1 + \cdots + b_m) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i \cdot b_j,$
- $\forall n, m \in \mathbb{Z} \ \forall a, b \in R: \ (na) \cdot (mb) = (n \cdot m)(a \cdot b).$ *Důkaz.*

Věta. *Okruh R je triviální, právě když v něm platí $1 = 0$.*

Definice. Okruh R se nazývá **komutativní**, je-li pologrupa $(R, \cdot)$ komutativní.

Definice. Prvky a, b okruhu R se nazývají **dělitelé nuly**, jestliže $a \neq 0$, $b \neq 0$, avšak $a \cdot b = 0$.

Obory integrity

Definice. Netriviální komutativní okruh R se nazývá **obor integrity**, pokud nemá dělitele nuly.

Označení. Množinu všech nenulových prvků okruhu R značíme R^*. Netriviální komutativní okruh R je tedy obor integrity, právě když $(R^*, \cdot)$ je pologrupa.

Věta. Netriviální komutativní okruh R je obor integrity, právě když v něm platí **zákon o krácení**, *tj. pro každé $a, b, c \in R$ platí*

$$a \neq 0, \ a \cdot b = a \cdot c \quad \Longrightarrow \quad b = c.$$

Důkaz.

Definice. Nechť R je okruh. Invertibilní prvek pologrupy $(R, \cdot)$ se nazývá **jednotka** okruhu R. Množinu všech jednotek okruhu R značíme $R^\times$.

Poznámka. Nezaměňujte pojmy jednička a jednotka okruhu. Okruh má jedinou jedničku, kdežto jednotek může mít více. Vždy je jednička jednotkou. Okruhy s jedinou jednotkou jsou výjimečné (například okruh $\mathbb{Z}_2$). Nezaměňujte R^* a $R^\times$. Uvědomte si, že nové označení je v souladu s užívaným $\mathbb{Z}_m^\times$.

Tělesa

$R^* = R - \{0\}$ ... množina nenulových prvků okruhu R,
$R^\times = \{a \in R;\ \exists b \in R :\ a \cdot b = b \cdot a = 1\}$ ... množina invertibilních prvků okruhu R.

Věta. Nechť R je okruh. Pak $(R^\times, \cdot)$ je grupa.

Definice. Netriviální komutativní okruh R se nazývá **těleso**, pokud je každý jeho nenulový prvek jednotkou.

Věta. *Netriviální komutativní okruh R je těleso, právě když $R^* = R^\times$, tedy právě když $(R^*, \cdot)$ je grupa.*

Důsledek. *Každé těleso je oborem integrity.*

Příklad. Okruh celých čísel $\mathbb{Z}$ je oborem integrity, který není tělesem.

Věta. *Každý konečný obor integrity je tělesem.* Důkaz.

Věta. *Okruh zbytkových tříd $\mathbb{Z}_m$ je oborem integrity, právě když je tělesem, což nastane právě když m je prvočíslo.* Důkaz.

Charakteristika okruhu

Definice. Nechť R je okruh. Nejmenší přirozené číslo n takové, že $n1 = 0$, se nazývá **charakteristika** okruhu R. Pokud takové n neexistuje (tedy pro všechna $k \in \mathbb{N}$ platí $k1 \neq 0$), řekneme, že charakteristika okruhu R je nula.

Označení. Charakteristiku okruhu R značíme $\operatorname{char} R$.

Příklady. $\operatorname{char} \mathbb{Z} = \operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$, $\operatorname{char} \mathbb{Z}_m = m$.

Věta. *Nechť R je okruh, $m = \operatorname{char} R$. Pak pro každé $a \in R$ platí $ma = 0$.* Důkaz.

Věta. *Nechť R je obor integrity, pak $\operatorname{char} R$ je buď 0, nebo prvočíslo.*