3 Okruhy

V této kapitole se seznámíme se základy teorie okruhů. Po obecné části se budeme věnovat okruhům polynomů v jedné proměnné. Jedná se o součást tzv. komutativní algebry, která je podstatná pro pozdější vybudování teorie těles.

Definice. Množina R spolu se dvěma binárními operacemi $+$ a $\cdot$ se nazývá *okruh*, pokud jsou splněny následující podmínky:

1) $R(+)$ je komutativní grupa,
2) $R(\cdot)$ je pologrupa s neutrálním prvkem,
3) platí *distributivní zákony*, tedy pro každou trojici prvků $a, b, c \in R$ platí

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{a} \qquad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Neutrální prvek ve sčítání okruhu budeme vždy značit 0, opačný prvek ve sčítání k prvku a budeme značit $-a$ (aditivní zápis). Neutrální prvek v násobení budeme nazývat jednotka okruhu a značit 1. Je-li násobení v okruhu R komutativní, pak mluvíme o *komutativním okruhu*. Opět budeme při zápisu často vynechávat operaci násobení a místo $a \cdot b$ psát ab, pokud bude jasné, ve kterém okruhu počítáme.

Úkol. Odvoďte z definice okruhu, že $0 \cdot a = 0 = a \cdot 0$ pro všechna $a \in R$. Dále odvoďte, že platí $(-1) \cdot a = -a$.

Příklady okruhů. 1) Základním příkladem komutativního okruhu je okruh celých čísel $\mathbb{Z}$. Dále konečné okruhy $\mathbb{Z}_n$, $n \in \mathbb{N}$, se sčítáním a násobením modulo n.

2) Je-li R komutativní okruh, pak můžeme definovat *okruh polynomů v jedné proměnné* nad R, který značíme $R[x]$. Později se budeme těmto komutativním okruhům podrobně věnovat. Stejným postupem můžeme definovat okruhy polynomů ve více (navzájem komutujících) proměnných, například ve dvou proměnných $R[x, y] = (R[x])[y]$.

3) Porovnáním definic okamžitě zjistíme, že každé těleso je zároveň také okruhem. V definici tělesa je navíc požadavek na existenci inverzních prvků v násobení ke všem nenulovým prvkům (a obvykle se požaduje komutativita násobení).

4) V předchozí kapitole jsme mluvili o pologrupě $\mathrm{M}_n(T)$ všech matic řádu n nad tělesem T. Měli jsme na mysli operaci násobení matic. Přidáme-li bežné sčítání matic po složkách, získáme nekomutativní (pro $n > 1$) *maticový okruh* $\mathrm{M}_n(T)$. Neutrálním prvkem v násobení je jednotková matice, ve sčítání je to nulová matice.

Úkol. Je-li R okruh, pak z předchozí kapitoly víme, že lze operace $+$ a $\cdot$ přenést na potenci $\mathrm{P}(R)$. Víme také, že sčítání a násobení podmnožin po prvcích jsou opět asociativní operace. Bude $\mathrm{P}(R)$ s těmito operacemi opět okruh? Přesněji: které vlastnosti z definice okruhu zůstanou zachovány a které se poruší?

3.A Obecná teorie

Podobně, jako v případě grup, budeme nejdříve studovat homomorfismy, kongruence a faktorizace okruhů. Teorii, kterou v této podkapitole vybudujeme, budeme aplikovat v dalším výkladu především na okruhy polynomů.

Definice. Zobrazení $f : R \to S$ okruhu R do okruhu S se nazývá *homomorfismus* (přesněji okruhový homomorfismus), pokud pro každé $a, b \in R$ platí:

$$f(a+b) = f(a) + f(b), \quad f(a \cdot b) = f(a) \cdot f(b) \quad \text{a} \quad f(1) = 1.$$

Operace v obou okruzích z definice značíme stejně, i když by například přesněji mělo být $f(1_R) = 1_S$. Toto zjednodušení by však nemělo vést k omylům.

Zobrazení $f : R \to S$ je tedy homomorfismus okruhů právě když je to homomorfismus vzhledem k aditivním i multiplikativním pologrupám a zachovává jednotku. Z toho plyne, že speciálně je $f : R(+) \to S(+)$ homomorfismus grup a tedy *zachovává i nulu a opačné prvky.*

Monomorfismus, epimorfismus a izomorfismus bude v tomto pořadí opět znamenat prostý, na a bijektivní homomorfismus.

Příklady. 1) Zobrazení modulo $n : \mathbb{Z} \to \mathbb{Z}_n$ je pro $n \in \mathbb{N}$ epimorfismus okruhů.

2) Je-li $f : \mathbb{Z} \to \mathbb{Z}$ okruhový homomorfismus, pak pro $n \in \mathbb{N}$ musí být $f(n) = f(n \cdot 1) = f(1 + 1 + ... + 1) = f(1) + f(1) + ... + f(1) = n \cdot f(1) = n \cdot 1 = n$. Dále f zachovává nulu a opačné prvky, tedy pro $n \in \mathbb{N} \cup \{0\}$ je $f(-n) = -f(n) = -n$. Vidíme, že v tomto případě je f vždy pouze identita. Naopak násobení pevným číslem $a \in \mathbb{Z}$, tedy pro $b \in \mathbb{Z}$ definujeme $f(b) = a \cdot b$, je homomorfismus grup $\mathbb{Z}(+) \to \mathbb{Z}(+)$.

3) Komplexní sdružení $- : \mathbb{C} \to \mathbb{C}$ je okruhový izomorfismus.

Úkol. 1) Dokažte, že jediný okruhový homomorfismus $\mathbb{Q} \to \mathbb{Q}$ je identita.

2) Dokažte, že jediný okruhový izomorfismus $\mathbb{R} \to \mathbb{R}$ je identita. (Hint: použijte vlastnosti kvadrátů.)

3) Ať je $f : \mathbb{C} \to \mathbb{C}$ okruhový homomorfismus, který je identický na $\mathbb{R}$. Dokažte, že potom je f buď identita, nebo komplexní sdružení.

Jak již víme, základním prostředkem ke zkoumání algebraických struktur jsou kongruence.

Definice. Ekvivalence $\sim$ na okruhu R se nazývá *kongruence*, pokud pro každé a_1, a_2, $b_1, b_2 \in R$ takové, že $a_1 \sim a_2$ a $b_1 \sim b_2$, platí $a_1 + b_1 \sim a_2 + b_2$ a zároveň $a_1 \cdot b_1 \sim a_2 \cdot b_2$.

Tedy kongruence na okruhu jsou takové ekvivalence, které jsou kongruencemi vzhledem k oběma binárním operacím. Kongruence $\sim$ na okruhu R je speciálně kongruencí komutativní grupy $R(+)$. Můžeme proto i v tomto případě používat vlastnosti grupových kongruencí. Například víme, že kongruence na grupě jednoznačně odpovídají normálním podgrupám. Pro naši grupu $R(+)$ to znamená, že lze kongruenci ekvivalentně zadat

nějakou podgrupou I (normalita je zde díky komutativitě triviálně splněná), a třídy kongruence jsou pak právě rozkladové třídy podle I. Pro okruhy budeme potřebovat silnější pojem *ideálu*, pro který dokážeme vzájemně jednoznačný vztah:

kongruence na okruhu $\leftrightarrow$ *ideály okruhu.*

Definice. Ať je R okruh. Podgrupa I aditivní grupy $R(+)$ se nazývá *ideál*, pokud pro každé $a \in R$ a každé $b \in I$ platí $a \cdot b \in I$ a také $b \cdot a \in I$.

V řeči násobení podmnožin v pologrupě $\mathrm{P}(R(\cdot))$ lze ideály definovat vlastností $a \cdot I \subseteq I$ a $I \cdot a \subseteq I$ pro všechna $a \in R$. Pak samozřejmě také platí $A \cdot I \cdot B \subseteq I$ pro každou dvojici množin $A, B \in \mathrm{P}(R(\cdot))$.

Kongruence a ideály okruhů. Ať je R okruh a $\sim$ ať je kongruence na R. Z toho, že $\sim$ je kongruence grupy $R(+)$ plyne, že $\sim$ je jednoznačně určená třídou nuly $[0]_\sim$. Označme $I = [0]_\sim$. Víme, že I je podgrupa $R(+)$ a že rozkladové třídy podle I jsou přesně třídy kongruence $\sim$. Pro $a \in R$ a $b \in I$ platí $ab \sim a \cdot 0 = 0 = 0 \cdot a \sim b \cdot a$, neboť $b \sim 0$. Dokázali jsme, že I je ideál okruhu R. Rozkladovým třídám $a+I = \{a+b\ ;\ b \in I\} = [a]_\sim$ budeme říkat *rozkladové třídy podle ideálu* I.

Naopak začneme s ideálem I okruhu R. Označme $\sim_I$ kongruenci grupy $R(+)$, jejíž třídy jsou rozkladové třídy podle podgrupy I. Ukážeme, že $\sim_I$ je kongruence okruhu R. Pro $a_1, a_2, b_1, b_2 \in R$ takové, že $a_1 \sim_I a_2$ a $b_1 \sim_I b_2$, platí $a_1 + I = a_2 + I$ a $b_1 + I = b_2 + I$. Tedy existují prvky $c, d \in I$ tak, že $a_1 = a_1 + 0 = a_2 + c$ a $b_1 = b_1 + 0 = b_2 + d$. Zbývá vypočítat:

$$a_1 b_1 = (a_2 + c) \cdot (b_2 + d) = a_2 b_2 + a_2 d + c(b_2 + d) \sim_I a_2 b_2 + 0 = a_2 b_2,$$

neboť z vlastností ideálu plyne, že $a_2 d,\ c(b_2 + d) \in I$ a tedy $a_2 d + c(b_2 + d) \in I$.

Ideály v $\mathbb{Z}$. Každá kongruence grupy $\mathbb{Z}(+)$ je zároveň kongruencí okruhu $\mathbb{Z}$. Pro $k \in \mathbb{Z}$ a $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ totiž platí, že je-li $a_1 \equiv_k a_2$ a $b_1 \equiv_k b_2$, pak je $a_1 b_1 \equiv_k a_2 b_2$. To podle popisu kongruencí na $\mathbb{Z}(+)$ znamená, že množiny tvaru $k \cdot \mathbb{Z}$, $k \in \mathbb{Z}$, jsou právě všechny ideály okruhu $\mathbb{Z}$.

Faktorizace okruhů. Faktorizovat lze podle kongruence, tedy v případě okruhu podle ideálu. Ať je I ideál okruhu R. Již umíme zkonstruovat faktorovou grupu $R/I = R(+)/I = \{a + I\ ;\ a \in R\}$ s operací $(a + I) + (a' + I) = (a + a') + I$. Pro I ideál můžeme na množině R/I definovat také násobení $(a + I) \cdot (a' + I) = (a \cdot a') + I$. Podstatné pro správnost této definice je to, že nezávisí na volbě prvků $a \in a + I$, $a' \in a' + I$. Pro $c, d \in I$ a prvky $b = a + c \in a + I$ a $b' = a' + d \in a' + I$ totiž platí $bb' + I = (a+c) \cdot (a'+d) + I = (aa' + ad + c(a'+d)) + I = aa' + (ad + c(a'+d) + I) = aa' + I$, neboť z vlastností ideálu je $ad + c(a' + d) \in I$. Snadno se ověří, že množina R/I spolu s již definovanými operacemi $+$ a $\cdot$ je opět okruh. Nulový prvek R/I je třída $0 + I = I$, jednotkový prvek je třída $1 + I$. Tento okruh budeme nazývat *faktorový okruh* R *podle ideálu* I.

Zobrazení $p : R \to R/I$ definované pro $a \in R$ předpisem $p(a) = a + I$ budeme opět nazývat *přirozená projekce*. Víme, že p je homomorfismus aditivních grup. Dále máme $p(1) = 1 + I = 1_{R/I}$ a pro $a, b \in R$ je $p(ab) = ab + I = (a + I)(b + I) = p(a)p(b)$. Tedy p je okruhový homomorfismus a platí $I = p^{-1}(0_{R/I})$.

Nyní budeme formulovat analogie vět o homomorfismech grup pro okruhy. Důkazy budou opět využívat naše znalosti o grupových homomorfismech. Nejdříve rozšíříme pojem jádra a obrazu homomorfismu na homomorfismy okruhů. Ať je $f : R \to S$ okruhový homomorfismus. Jádro a obraz f definujeme jako jádro a obraz homomorfismu aditivních grup $f : R(+) \to S(+)$, tedy *jádro* $\mathrm{Ker}(f) = f^{-1}(0) = \{a \in R \ ; \ f(a) = 0\}$ a *obraz* $\mathrm{Im}(f) = f(R) = \{b \in S \ ; \ b = f(a)$ pro nějaké $a \in R\}$. Opět u operací i neutrálních prvků vynecháváme index příslušného okruhu.

K formulaci věty o jádru a obrazu potřebujeme pojem podokruhu.

Definice. Buď S podmnožina okruhu R. Řekneme, že S je *podokruh*, je-li S podgrupa $R(+)$ a zároveň podpologrupa $R(\cdot)$ a je-li $1 \in S$.

Jinými slovy je podokruh podmnožina uzavřená na sčítání, opačné prvky a nulu a také na násobení a jednotku. Samozřejmě je podokruh vzhledem k daným operacím sám opět okruhem.

Úkol. Víme, že existují podpologrupy i podgrupy generované podmnožinami. Pro podokruhy platí totéž. Dokažte si obdobné tvrzení o podokruhu generovaném podmnožinou X okruhu R. Jaký je obecný tvar prvků podokruhu generovaného X? (Hint: Pro konstrukci podokruhu využijte již dokázaná tvrzení o generování podpologrupy $R(\cdot)$ a podgrupy $R(+)$.)

Úkol. Lze si představit těleso $\mathbb{C}$ jako podokruh maticového okruhu $\mathrm{M}_2(\mathbb{R})$?

Věta 3.1 (jádro a obraz okruhového homomorfismu) *Ať je $f : R \to S$ homomorfismus okruhů. Pak je $\mathrm{Im}(f)$ podokruh S a $\mathrm{Ker}(f)$ je ideál okruhu R. Okruhy $R/\mathrm{Ker}(f)$ a $\mathrm{Im}(f)$ jsou izomorfní.*

Důkaz. Homomorfismus f zachovává obě binární operace i jednotku, tudíž je $\mathrm{Im}(f)$ podokruh S. Dále víme, že $\mathrm{Ker}(f)$ je podgrupa $R(+)$. Zvolme $a \in R$ a $b \in \mathrm{Ker}(f)$. Platí $f(ab) = f(a)f(b) = f(a) \cdot 0 = 0$, tedy $ab \in \mathrm{Ker}(f)$. Podobně $ba \in \mathrm{Ker}(f)$ a proto je $\mathrm{Ker}(f)$ ideál R.

Víme, že zobrazení $\varphi : R/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ definované předpisem $\varphi(a + \mathrm{Ker}(f)) = f(a)$ je izomorfismus aditivních grup. Zbývá ukázat, že zachovává jednotku a násobení. Máme $\varphi(1 + \mathrm{Ker}(f)) = f(1) = 1$ a dále $\varphi((a + \mathrm{Ker}(f)) \cdot (b + \mathrm{Ker}(f))) = \varphi(ab + \mathrm{Ker}(f)) = f(ab) = f(a)f(b) = \varphi(a + \mathrm{Ker}(f)) \cdot \varphi(b + \mathrm{Ker}(f))$. □

Z předchozího plyne, že

kongruence na okruhu odpovídají přesně ideálům a také jádrům okruhových

homomorfismů.

Věta 3.2 *Ať je $f : R \to S$ epimorfismus okruhů. Pak je přiřazení $\overline{I} \mapsto f^{-1}(\overline{I})$ bijekce z množiny ideálů okruhu S na množinu ideálů okruhu R obsahujících* $\mathrm{Ker}(f)$.

Důkaz. Víme, že přiřazení $\overline{I} \mapsto f^{-1}(\overline{I})$ je bijekce z množiny všech podgrup grupy $S(+)$ (všechny podgrupy jsou zde normální) na množinu podgrup grupy $R(+)$ obsahujících $\mathrm{Ker}(f)$. K dokončení důkazu potřebujeme ukázat, že podgrupa $\overline{I}$ je ideál S právě když je podgrupa $I = f^{-1}(\overline{I})$ ideál R.

Předpokládejme, že $\overline{I}$ je ideál S. Zvolme $a \in R$ a $b \in I$. Platí $f(ab) = f(a)f(b) \in \overline{I}$, neboť $f(b) \in \overline{I}$. Tedy $ab \in f^{-1}(\overline{I}) = I$. Podobně lze ukázat $ba \in I$ a tudíž je I ideál R.

Ať je I ideál R. Zvolme $\overline{a} \in S$ a $\overline{b} \in \overline{I}$. Jistě existují prvky $a \in R$, $b \in I$ tak, že $f(a) = \overline{a}$ a $f(b) = \overline{b}$, neboť f je epimorfismus. Máme $\overline{a}\overline{b} = f(a)f(b) = f(ab) \in f(I) = \overline{I}$, protože $ab \in I$. Podobně $\overline{b}\overline{a} \in \overline{I}$ a $\overline{I}$ je ideál S. □

Věta 3.3 (věta o izomorfismu pro okruhy) *Je-li $f : R \to S$ epimorfismus okruhů a $\overline{I}$ je ideál S, pak jsou okruhy $S/\overline{I}$ a $R/f^{-1}(\overline{I})$ izomorfní.*

Důkaz. Podle Věty 3.2 je $I = f^{-1}(\overline{I})$ ideál R a tedy můžeme uvažovat faktor R/I. Položme $\tilde{f} = p \circ f : R \to S/\overline{I}$, kde $p : S \to S/\overline{I}$ je přirozená projekce. Podle důkazu Věty o izomorfismu pro grupy víme, že $\tilde{f}$ je epimorfismus a $\mathrm{Ker}(\tilde{f}) = I$. Ovšem $\tilde{f}$ je složení dvou okruhových homomorfismů, tedy je to opět okruhový homomorfismus a podle Věty 3.1 máme $R/I \cong S/\overline{I}$. □

Definice. Okruh R se nazývá *jednoduchý*, pokud jeho jediné ideály jsou 0 a R.

Používáme značení 0 pro nejmenší (triviální) ideál místo přesnějšího $\{0\}$. Pojem jednoduchosti pro grupy a okruhy se dá shrnout do společné formulace: daná grupa nebo okruh *nemá vlastní kongruence.*

Příklad. Ať je T (komutativní) těleso, například $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$. Maticový okruh $\mathrm{M}_n(T)$, $n \geq 1$, je jednoduchý. Pro $n = 1$ tvrdíme, že těleso T je jednoduchý okruh. To je ale snadné si uvědomit. Nenulový ideál I tělesa T obsahuje nějaké $0 \neq b \in I$. Pro b^{-1} inverzi k b v násobení platí $1 = b^{-1}b \in I$. Ovšem pokud $1 \in I$, pak $a = a \cdot 1 \in I$ pro každé $a \in R$. Tedy $I = R$.

Pro $n > 1$ musíme počítat jen o trochu více. Nenulový ideál I okruhu $\mathrm{M}_n(T)$ obsahuje nějakou nenulovou matici B. Uvědomme si, že násobením maticemi zleva můžeme provádět na B řádkové úpravy, násobením zprava sloupcové úpravy. Matice B obsahuje na nějakém místě i, j nenulový prvek tělesa T. Můžeme násobením zleva vynulovat všechny řádky kromě i-tého a násobením zprava vynulovat všechny sloupce kromě j-tého. Vznikne matice, která je nenulová pouze v místě i, j. Vhodným vynásobením i-tého řádku (tedy násobením vhodnou maticí zleva) získáme matici, která má v místě i, j prvek 1. Tento prvek můžeme opět řádkovými a sloupcovými úpravami přesunout na místo $1, 1$. Získali jsme matici $B_1 \in I$, která má na místě $1, 1$ prvek 1 a jinde je nulová. Podobně dostaneme matice $B_i \in I$, $i = 1, ..., n$, které jsou na místě i, i rovny 1 a jinde

jsou nulové. Máme proto $E = B_1 + B_2 + ... + B_n \in I$, kde E je jednotková matice. Pak pro každou matici $A \in \mathrm{M}_n(T)$ je $A = A \cdot E \in I$ a tudíž $I = \mathrm{M}_n(T)$.

Věta 3.4 *Jednoduchý komutativní okruh je těleso.*

Důkaz. Zvolme $a \in R$, $a \neq 0$, R jednoduchý komutativní okruh. Uvažme množinu $I = aR = \{ab \ ; \ b \in R\}$. Snadno zjistíme, že je I ideál (dokažte si!). Dále $I \neq 0$, neboť $a \in I$, a tedy musí být $I = R$. To znamená, že $ab = 1$ pro nějaké $b \in R$ (samozřejmě je pak i $ba = 1$). Našli jsme inverzi k libovolně zvolenému nenulovému prvku a. □

Další příklady jednoduchých okruhů se dají získat jako faktory daného okruhu podle takzvaných maximálních ideálů.

Definice. Ideál I okruhu R se nazývá *maximální*, pokud $I \neq R$ a pokud pro každý ideál J platí, že je-li $I \leq J \neq R$, pak $I = J$.

Jedná se tedy o ideály maximální vzhledem k inkluzi. Důležitou vlastností okruhů s jednotkou je existence maximálních ideálů.

Lemma 3.5 *Je-li I ideál okruhu R, $I \neq R$, pak existuje J maximální ideál R, který obsahuje I.*

Důkaz. Tvrzení dokážeme pomocí Zornova lemmatu. Můžeme předpokládat, že $R \neq 0$, jinak tvrzení triviálně platí. Označme $\mathbf{I} = \{I \leq R \ ; \ I \text{ ideál } R, \ I \neq R\}$ množinu všech ideálů různých od celého okruhu. Máme $0 \in \mathbf{I}$, tedy $\mathbf{I}$ je neprázdná množina. Ať je L nějaká lineárně uspořádaná množina a I_u, $u \in L$, systém nějakých ideálů z $\mathbf{I}$ takový, že pro všechna $u, v \in L$, $u \leq v$, platí $I_u \leq I_v$. Takový systém ideálů se nazývá *řetězec*. Označme $I = \bigcup_{u \in L} I_u$. Platí, že I je opět ideál. Ukažme například uzavřenost I na sčítání. Zvolme $a, b \in I$. Z vlastností sjednocení existují indexy $u, v \in L$ tak, že $a \in I_u$ a $b \in I_v$. Označme $w = \max(u, v)$. Máme $a, b \in I_w$, tedy $a + b \in I_w$ a proto je $a + b \in I$. Zbylé vlastnosti ideálu lze ověřit zcela analogicky.

Pro ideál J okruhu R platí, že $J \neq R$ právě když $1 \notin J$. Totiž pokud $1 \in J$, pak je $a = a \cdot 1 \in J$ pro každé $a \in R$ a $J = R$. Máme tedy $1 \notin I_u$ pro všechna $u \in L$ a proto $1 \notin \bigcup_{u \in L} I_u = I$. Dokázali jsme, že $I \in \mathbf{I}$.

Víme, že je množina $\mathbf{I}$ neprázdná a uzavřená na sjednocení řetězců. To podle Zornova lemmatu zaručuje nad každým prvkem $\mathbf{I}$ existenci v inkluzi maximálního prvku. Tyto maximální prvky jsou právě maximální ideály, čímž je dokončen důkaz tvrzení. □

Věta 3.6 *Ať je I maximální ideál okruhu R. Pak je R/I jednoduchý okruh. Je-li R navíc komutativní, pak je R/I těleso.*

Důkaz. První část tvrzení plyne přímo z Věty 3.2. Je-li R komutativní, pak je R/I jednoduchý komutativní okruh a můžeme použít Větu 3.4. □

Příklad. Již jsme řekli, že všechny ideály $\mathbb{Z}$ jsou tvaru $k\mathbb{Z}$, $k \in \mathbb{Z}$. Přitom platí, že $k\mathbb{Z} \leq m\mathbb{Z}$ právě když $m|k$. Tedy uspořádání ideálů inkluzí je obrácené uspořádání dělitelnosti na $\mathbb{Z}$. Maximální ideály proto odpovídají minimálním prvkům v dělitelnosti, tedy maximální ideály jsou ideály tvaru $p\mathbb{Z}$, p prvočíslo. Z předchozího tvrzení opět plyne známý fakt, že $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ je těleso pro p prvočíslo.

Úkol. Můžeme vyjádřit každý ideál $\mathbb{Z}$ jako průnik (některých) maximálních ideálů? Které ideály lze takto vyjádřit?