Úvod do komutativní algebry: cvičení 1

10. října 2022

1. Dokaž, že sjednocení řetězce (libovolně mnoha) ideálů $I_1 \subset I_2 \subset I_3 \subset \cdots$ je ideál.

Řešení. Buď okruh R a zkoumané sjednocení I. Pro $a, b \in I$, $r \in R$ máme dokázat $a + b \in I$, $ra \in I$. Z definice sjednocení musí být pro nějaké indexy být $a \in I_k$, $b \in I_\ell$. Pro $m = \max\{k, \ell\}$ pak už $a, b \in I_m$, takže definicí ideálu $a + b$ i ra leží v $I_m \subset I$.

2. Pro ideály I, J definujme $I + J := \{a + b \mid a \in I, b \in J\}$. Dokaž, že $I + J$ je nejmenší ideál v R, který obsahuje I a J.

Řešení. $I + J$ je ideál: součet generických prvků z $I + J$ je

$$(a_1 + b_1) + (a_2 + b_2) = \underbrace{(a_1 + a_2)}_{\in I} + \underbrace{(b_1 + b_2)}_{\in J}.$$

Obdobně $r(a+b) = ra+rb \in I+J$. Dále $I+J$ triviálně obsahuje I i J. Naopak když nějaký ideál K obsahuje I i J, musí uzavřeností na sčítání obsahovat všechna $a + b$, tedy obsahovat $I + J$.

3. Buď R okruh a M ideál v R. Dokaž:

a) M je maximální, právě když pro všechna $a \in R \setminus M$ platí $R = M + aR$.
b) Pokud M je maximální a $a \in R \setminus M$, pak existují $m \in M$ a $r \in R$ taková, že $1 = m + ar$.

Řešení. a) $M + aR$ je ideál ostře větší než M (má navíc prvek a), z maximality už to tedy musí být celé R. Opačným směrem, když $M \subsetneq I \subset R$, volbou $a \in M \setminus I$ dostaneme $R = M + aR \subset I$, takže $I = R$, což dá maximalitu M.

b) Ideál na levé straně $R = M + aR$ obsahuje jedničku, takže i napravo ji lze tvarem $m + ar$ vyjádřit.

4. Urči: $\mathbb{Q}[x]/(x + 2)$, $\mathbb{Q}[x]/(x^2 - 2)$, $\mathbb{Q}[x]/(x^2 - 1)$, $\mathbb{R}[x]/(x^2 - 2)$, $\mathbb{Z}[x]/(x^2 - 2)$.

Řešení. Vyjde po řadě $\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q} \times \mathbb{Q}$, $\mathbb{R} \times \mathbb{R}$ a $\mathbb{Z}[\sqrt{2}]$. Strategie: modulení ireducibilním polynomem = přidání kořene; součin různých ireducibilních polynomů rozlámeme Čínskou zbytkovou větou. Např. pro $\mathbb{Q}[x]/(x^2 - 2)$ pošleme homomorfismus

$$\begin{aligned} \mathbb{Q}[x] &\to \mathbb{Q}[\sqrt{2}], \\ f &\mapsto f(\sqrt{2}). \end{aligned}$$

Obraz je celé $\mathbb{Q}[\sqrt{2}]$, jádro je $(x^2 - 2)$ (minimální polynom $\sqrt{2}$). 1. věta o izomorfismu dá výsledek. Pro $\mathbb{Q}[x]/(x^2 - 1)$ musíme nejdřív rozložit na $\mathbb{Q}[x]/(x - 1) \times \mathbb{Q}[x]/(x + 1)$, oba činitelé jsou pak izomorfní $\mathbb{Q}$.

5. Mějme ideály I, J, K okruhu R. Dokaž, že $IJ \subset I \cap J$ a $I(J + K) = IJ + IK$. Najdi příklad, kdy $IJ \neq I \cap J$.

Řešení. Ideály jsou uzavřené na násobení, takže pro $a \in I$, $b \in J$ je speciálně $ab \in I$. Ideál IJ je tvořen součty takových součinů, takže $IJ \subset I$. Úplně analogicky $IJ \subset J$, takže $IJ \subset I \cap J$.

Pro $I(J + K) = IJ + IK$ dokažme obě inkluze, uvažujeme $a \in I$, $b \in J$, $c \in K$. Nalevo je součet součinů tvaru $a(b + c)$, napravo nějaký součet součinů ab plus součet součinů ac. Součiny tvaru $a(b + c)$ umíme roznásobit a interpretovat jako prvky ideálu napravo – to je inkluze „$\subset$“. Pro opačnou inkluzi můžeme každé ab přepsat na $a(b+0)$ a každé ac na $a(0+c)$, čímž vyrábíme tvary z levé strany – to je inkluze „$\supset$“.

6. Dokaž, že operace na faktorokruhu jsou definované korektně a že jde o okruh (a dokaž ostatní věci z přednášky, které jsme nechali jako cvičení).

Řešení. R okruh, I ideál, $a, b \in R$. Chceme ověřit, že pro $x \in a + I$, $y \in b + I$ bude fungovat $x + y \in (a + b) + I$ a obdobně $xy \in ab + I$. K tomu vyjádříme $x = a + i_1$, $y = b + i_2$ a s pomocí uzavřenosti ideálu na sčítání a na násobení prvkem okruhu máme

$$x + y = a + i_1 + b + i_2 = (a + b) + \underbrace{(i_1 + i_2)}_{\in I},$$
$$xy = (a + i_1)(b + i_2) = ab + \underbrace{(ai_2 + bi_1 + i_1 i_2)}_{\in I}.$$

7. Dokaž 3. větu o izomorfismu: Je-li R okruh, $I < R$ ideál a $S \subset R$ podokruh, pak je $S+I$ podokruh v R a platí $(S + I)/I \simeq S/(S \cap I)$.

Řešení. Že $S + I$ je podokruh, se rutinně ověří (má jedničku, je uzavřený na sčítání i násobení). Dále směřujme k použití 1. věty o izomorfismu. Projekce $\pi\colon R \twoheadrightarrow R/I$, $r \mapsto r + I$ je surjektivní homomorfismus. Zužme ho na podokruh S a pojmenujme φ. Aby $\varphi(s) = s + I$ bylo 0, musí $s \in I$, takže $\operatorname{Ker} \varphi = S \cap I$. V obrazu se objeví přesně zbytkové třídy tvaru $s + I$, takže $\operatorname{Im} \varphi = (S + I)/I$ (jedna inkluze je zřejmá, pro tu druhou si uvědom, že cokoliv tvaru $s + i + I$ je jednoduše totéž jako $s + I$). 1. věta o izomorfismu pak dává výsledek.

8. Uvažujme okruh $\mathbb{Z}$ a uvažujme v něm ideály $I = (168)$ a $J = (288)$.

a) Jak vypadají všechny maximální ideály a prvoideály v $\mathbb{Z}$?
b) Urči $I + J$, IJ, $I \cap J$, $I^2 + J$.
c) Najdi všechny prvoideály, které obsahují ideál I, J, IJ, $I \cap J$, resp. J^2.

Řešení. a) Hlavní ideály generované prvočísly.

b) Viz část a) v následujícím cvičení, vyjde $I + J = (24)$, $IJ = (48\,384)$, $I \cap J = (2016)$, $I^2 + J = (288)$.

c) Prvoideály obsahující (x) odpovídají prvočíslům dělícím x. Stačí tedy použít $168 = 2^3 \cdot 3 \cdot 7$, $288 = 2^5 \cdot 3^2$ a vždy vzít prvočísla z rozkladu.

9. Buď R obor hlavních ideálů a $a, b \in R$.

a) Urči $(a)(b)$, $(a) + (b)$, $(a) \cap (b)$.
b) Jak vypadají všechny maximální ideály a prvoideály v R?
c) Dokaž, že faktor R podle nenulového prvoideálu je těleso.

Řešení. a) $(a)(b) = (ab)$, $(a) + (b) = (\mathrm{NSD}(a, b))$, $(a) \cap (b) = (\mathrm{nsn}(a, b))$.

b) Jsou to přesně hlavní ideály generované ireducibilními prvky/prvočiniteli (v OHI je ireducibilní = prvočinitel). V důsledku c) jsou prvoideály automaticky maximální.

c) Buď (p) prvoideál, pak je (p) ireducibilní. Chceme, aby libovolný nenulový prvek v $R/(p)$ měl inverz. Pro $a \notin (p)$ je ale $(a) + (p) = (\mathrm{NSD}(a, p)) = (1)$, takže $xa + yp = 1$ pro nějaká x, y. Pak ale $xy \equiv 1 \pmod{p}$.

10. Pro podmnožiny A, B okruhu R definujme $A \odot B := \{ab \mid a \in A, b \in B\}$ (pozor, toto neodpovídá násobení ideálů). Buď I ideál v R. Dokaž, že $(a + I) \odot (b + I) \subset ab + I$. Platí opačná inkluze?

Řešení. Dokazovaná inkluze je prostě to, že násobení prvků ve faktorokruhu modulo I funguje. Opačná inkluze neplatí: např. $2 \cdot 2 + 3\mathbb{Z}$ obsahuje jedničku, ale $(2 + 3\mathbb{Z}) \odot (2 + 3\mathbb{Z})$ nikoliv.

11. Uvažujme obor hlavních ideálů $\mathbb{Q}[x]$ a ideály $I = (x^3 + x^2 + 2x + 2)$ a $J = (x^3 - 2x^2 + 2x - 4)$.

a) Urči $I + J$, IJ, $I \cap J$, $I^2 + J^3$.
b) Které faktory modulo hlavní ideál z bodu a) jsou obory?
c) Najdi všechny prvoideály, které obsahují ideál I, J, IJ, $I \cap J$, resp. J^2.

Řešení. Faktorizujme polynomy:

$$x^3 + x^2 + 2x + 2 = (x + 1)(x^2 + 2), \qquad x^3 - 2x^2 + 2x - 4 = (x - 2)(x^2 + 2).$$

Snadno tedy v a) určíme potřebná NSD a nsn:

$$I + J = (x^2 + 2), \qquad IJ = \Big((x^3 + x^2 + 2x + 2) \cdot (x^3 - 2x^2 + 2x - 4)\Big),$$
$$I \cap J = \Big((x + 1)(x - 2)(x^2 + 2)\Big), \quad I^2 + J^3 = \Big((x^2 + 2)^2\Big).$$

b) Faktor je obor, pokud modulíme prvoideálem, což zde odpovídá ireducibilnímu polynomu. Tedy pouze $I + J$, ostatní máme zapsány jako součiny více polynomů.

c) Opět vezmeme všechny hlavní ideály generované ireducibilními polynomy z rozkladu.

12. Buď R noetherovský okruh a $I < R$ ideál. Dokaž, že R/I je také noetherovský.

Řešení. Pro spor nebuď R/I noetherovský. Ideály v R/I jsou přesně tvaru J/I pro $J < I$, takže pro nenoetherovskost R/I musíme mít nekonečný rostoucí řetězec

$$J_1/I \subsetneq J_2/I \subsetneq J_3/I \subsetneq \cdots$$

Pak je ale i $J_1 \subsetneq J_2 \subsetneq J_3 \subsetneq \cdots$ nekonečný rostoucí řetězec ideálů v R – spor.

13. Mějme v okruhu R prvek e splňující $e^2 = e$. Dokaž, že $R \simeq (e) \times (1 - e)$, když ideály vpravo uvažujeme jako podokruhy – co jsou v nich „jedničky“?

Řešení. Díky $e^2 = e$ můžeme $(e) = eR$ brát jako okruh s „jedničkou“ e. (Zadání trochu lže, technicky to není podokruh R, protože má jinou jedničku.) Analogicky platí $(1 - e)^2 = 1 - e$, takže máme $(1-e)$ jako okruh s „jedničkou“ $1-e$. Pak přímočaře najdeme a ověříme izomorfismus

$$\begin{aligned} R &\leftrightarrow (e) \times (1 - e), \\ r &\mapsto (er, (1 - e)r), \\ ea + (1 - e)b &\mapsfrom (ea, (1 - e)b). \end{aligned}$$