Úvod do komutativní algebry: cvičení 2

26. října 2023

1. Buď R gaussovský obor a T jeho podílové těleso. Pro každý ireducibilní polynom $f \in T[x]$ existuje $u \in T\backslash\{0\}$ takové, že uf je ireducibilní prvek $R[x]$.

Řešení. Berme $u := \prod_p p^{-c_p(f)}$. Tento součin dává smysl, protože jen konečně mnoho prvočinitelů p může dát nenulový obsah polynomu, jelikož v každém jmenovateli každého koeficientu se účastní jen konečně mnoho prvočinitelů. Pak dostaneme $c_p(uf) = v_p(u)+c_p(f) = 0$ pro každé p, takže $uf \in R[x]$ je primitivní. Jelikož je zároveň ireducibilní v $T[x]$, je podle Gaussova lemmatu ireducibilní v $R[x]$.

2. Buď K těleso. Pak $K[x,y]$ i $K[x_1,x_2,\dots]$ (nekonečně mnoho proměnných) jsou gaussovské, ale $K[x,y]$ není obor hlavních ideálů (ale je noetherovský) a $K[x_1,x_2,\dots]$ není noetherovský ani obor hlavních ideálů.

Řešení. Z Gaussova lemmatu platí „R gaussovský $\implies$ $R[x]$ gaussovský“. Víme, že $K[x]$ je OHI, takže gaussovský, takže i $K[x,y] \simeq K[x][y]$ je gaussovský.

Podobně je gaussovský i každý $K[x_1,\dots,x_n]$. Toho využijeme pro $K[x_1,\dots]$, každý jeho prvek f používá jen konečně mnoho proměnných, takže sám leží v nějakém $K[x_1,\dots,x_n]$. To je gaussovské, takže tu máme jednoznačný rozklad. Navíc víme, že nemůže fungovat žádný rozklad, který by použil některou další proměnnou – měli bychom vůči ní už nutně kladný stupeň, kdežto f má vůči x_i, $i > n$ nulový stupeň. Jednoznačný rozklad f v $K[x_1,\dots,x_n]$ tak zůstává jednoznačný v $K[x_1,\dots]$.

$K[x,y]$ není OHI, protože (x,y), tj. ideál generovaný prvky x a y, nemůže být hlavní. Kdyby totiž $(x,y) = (f)$ pro nějaké $f \in K[x,y]$, muselo by být $f \mid x$, takže $\deg_y(f) \le \deg_y(x) = 0$, tedy f je konstantní vzhledem k y. Zcela analogicky je ale f konstantní vůči x. Je to tedy konstanta $f \in K$, což je spor, protože v (x,y) žádné konstanty neleží (každý člen obsahuje x nebo y v kladné mocnině). Tím spíše už ani $K[x_1,x_2,\dots]$ nemůže být OHI.

Noetherovskost: Hilbertova věta o bázi říká „R noetherovský $\implies$ $R[x]$ noetherovský“. Těleso K je triviálně noetherovské (má jen dva ideály), tedy $K[x]$ je noetherovský, tedy $K[x,y] \simeq K[x][y]$ je noetherovský. Naopak $K[x_1,x_2,\dots]$ není noetherovský, protože máme řetězec ideálů

$$(x_1) \subsetneq (x_1,x_2) \subsetneq (x_1,x_2,x_3) \subsetneq \cdots \subsetneq (x_1,\dots,x_n) \subsetneq \cdots$$

3. Popiš všechny ideály v okruhu $\mathbb{Z}/(150)$ a charakterizuj, které dvojice z nich jsou komaximální.

Řešení. Ideály v $\mathbb{Z}/(150)$ jsou tvaru $I/(150)$, kde I jsou ideály $(150) \subset I < \mathbb{Z}$. Protože $\mathbb{Z}$ je OHI, jsou tato I přesně tvaru (d) pro $d \mid 150 = 2\cdot 3\cdot 5^2$. Dva takové $I_1/(150)$, $I_2/(150)$ jsou komaximální, právě když jsou I_1, I_2 komaximální v $\mathbb{Z}$, což nastává tehdy, když jsou jejich generátory ($I_1 = (d_1)$, $I_2 = (d_2)$) nesoudělné – tedy např. $(2)/(150)$ a $(3)/(150)$ nebo $(6)/(150)$ a $(25)/(150)$.

4. Buď R okruh. Pomocí Zornova lemmatu dokaž, že každý vlastní ideál je obsažený v nějakém maximálním ideálu.

Řešení. Buď dán ideál $I \subsetneq R$. Uvažme

$$\mathcal{A} := \{\text{ideál } J \mid I \subset J \subsetneq R\}$$

uspořádané inkluzí. Zjevně $I \in \mathcal{A}$, takže tato částečně uspořádaná množina je neprázdná. Kdykoliv je $\mathcal{B} \subset \mathcal{A}$ řetězec, položme $\tilde{J} := \bigcup \mathcal{B}$. To je ideál (viz první cvičení) a zjevně obsahuje I. Kdyby nebyl vlastní, pak by obsahoval 1, takže by 1 musela ležet už v nějakém $J \in \mathcal{B}$, což nelze. Tedy $J \in \mathcal{A}$. Tím jsou ověřeny podmínky Zornova lemmatu, tedy máme v $\mathcal{A}$ nějaké maximální M.

Tvrdíme, že je to maximální ideál. Kdyby nebyl, pak existuje nějaký ideál I', že $M \subsetneq I' \subsetneq R$. Jenže potom by I' byl vlastní a obsahoval I, takže $I' \in \mathcal{A}$, což je spor s maximalitou M. Takže M je skutečně maximální ideál obsahující I.

5. Použij důkaz Čínské zbytkové věty (zejména krok, kdy $1 = a_1 + a_2$) ke konstrukci explicitního izomorfismu $\mathbb{Z}/(n) \times \mathbb{Z}/(m) \simeq \mathbb{Z}/(mn)$ pro $n = 16, m = 35$. Jaké známé větě krok ze závorky odpovídá?

Řešení. Jeden směr izomorfismu $\mathbb{Z}/(mn) \to \mathbb{Z}/(n) \times \mathbb{Z}/(m)$ je triviální:

$$z + (mn) \mapsto (z + (n),\ z + (m)).$$

Abychom našli opačný izomorfismus $(a + (n), b + (m)) \mapsto ??? + (mn)$, potřebujeme $z_1 + (mn) \in \mathbb{Z}/(mn)$ takové, že $z_1 \mapsto (1, 0)$, a obdobně nějaké $z_2 \mapsto (0, 1)$. K tomu se hodí Bézoutova věta, protože když $xn + ym = 1$, pak stačí vzít $z_1 = ym$ a $z_2 = xn$.

Spustíme tedy rozšířený Eukleidův algoritmus na $n = 16$ a $m = 35$:

	35	1	0
	16	0	1
2	3	1	−2
5	1	−5	11

Tudíž $11 \cdot 16 + (-5) \cdot 35 = 1$. Vezmeme tedy $z_1 = (-5) \cdot 35 = -175$, $z_2 = 11 \cdot 16 = 176$, což dává explicitní izomorfismus

$$\begin{aligned} \mathbb{Z}/(n) \times \mathbb{Z}/(m) &\to \mathbb{Z}/(mn), \\ (a + (n), b + (n)) &\mapsto -175a + 176b + (mn). \end{aligned}$$

(Bézoutovy koeficienty vůbec nejsou jednoznačné, takže jako celá čísla bychom zde mohli zvolit i jiná čísla, nicméně jejich zbytkové třídy mod (mn) by měly být stále stejné.)

6. Uvědom si, že v uspořádané množině $\mathcal{A}$ může existovat i nespočetný řetězec $\mathcal{B}$, na jehož indexování nestačí přirozená čísla. Najdi pár příkladů takové situace. (Není v tom žádný chyták, jen by si člověk neměl utvořit představu, že v Zornovi stačí vyřešit řetězce indexované přirozenými čísly.)

Řešení. Třeba reálná čísla s jakýmkoliv uspořádáním, nebo potenční množina $\mathbb{R}$ uspořádaná inkluzí, nebo cokoliv jinačího. Gurmáni si též mohou představit svůj oblíbený obludně veliký kardinál či ordinál.

7. Nahlédni, že je-li $\varphi : R \to S$ homomorfismus okruhů, pak vztahy $\psi(r) := \varphi(r)$ pro $r \in R$ a $\psi(x) := x$ splňuje právě jeden homomorfismus $\psi : R[x] \to S[x]$. Navíc je ψ injektivní/surjektivní, právě když φ je injektivní/surjektivní.

Řešení. Pro obecné $f = \sum_{i=0}^{d} r_i x^i \in R[x]$ položme prostě

$$\psi(f) = \sum_{i=0}^{d} \varphi(r_i) x^i.$$

Že ψ respektuje sčítání je přímočaré, násobení je o něco méně přímočaré, ale stále snadné (koeficienty součiny polynomů jsou nějaké výrazy obnášející násobení a sčítání, což homomorfismus φ obojí zachovává). Jelikož jen aplikujeme φ „po koeficientech“, zachování injektivity/surjektivity je taky jasné.

8. Ať je R okruh a $I_1, \ldots, I_n$ po dvou komaximální ideály v R. Uvědom si, že z ČZV máme speciálně izomorfismus multiplikativních grup $(R/(I_1 \cdots I_n))^\times \simeq (R/I_1)^\times \times \cdots \times (R/I_n)^\times$. Jako aplikaci tohoto faktu si rozmysli, že pro lichá prvočísla $p \neq q$ nemůže být grupa $(\mathbb{Z}/(pq))^\times$ cyklická.

Řešení. Okruhová struktura už v sobě obsahuje strukturu multiplikativní grupy, takže jejich izomorfismus je jen zeslabením plné ČZV. Následně řád $(a, b) \in \mathbb{Z}_p^\times \times \mathbb{Z}_q^\times$ je nejmenším společným násobkem řádů a a b. Kvůli $\gcd(p - 1, q - 1) \geq 2$ pak řád nemůže dosáhnout $(p - 1)(q - 1)$.

9. Dokaž Zornovým lemmatem: ve vektorovém prostoru lze libovolnou lineárně nezávislou množinu rozšířit na bázi.

Řešení. Uvažuj lineárně nezávislé nadmnožiny dané množiny uspořádané inkluzí a použij Zornovo lemma. Maximální mezi nimi musí být i generující, jinak by nebyla maximální.

10. Buď $(M, \leq)$ částečně uspořádaná množina. Dokaž pomocí Zornova lemmatu, že uspořádání $\leq$ jde rozšířit na lineární uspořádání, čili že existuje uspořádání $\preceq$ na M, které je lineární a splňuje: $x \leq y \Rightarrow x \preceq y$ pro všechna $x, y \in M$.

Řešení. Částečné uspořádání je relace, tj. nějaká podmnožina $M \times M$, takže je samotné můžeme uspořádávat inkluzí. Mějme tedy

$$\mathcal{A} := \{\preceq \supset \leq \mid \preceq \text{ je částečné uspořádání množiny } M\}.$$

Podobně jako v předchozích ukázkách ověříme podmínky Zornova lemmatu; horní závorou řetězce je vždy jeho sjednocení. Pak máme v $\mathcal{A}$ nějaké maximální $\trianglelefteq$. Pro spor nechť není lineární, tedy nechť je v něm nějaká neporovnatelná dvojice x, y, tedy ani (x, y), ani (y, x) není prvek $\trianglelefteq$. Pak si můžeme vybrat, aby y bylo větší než x, a přidat tento vztah spolu se všemi okamžitými důsledky z tranzitivity. Formálně řečeno, vezmeme

$$\widetilde{\trianglelefteq} := \trianglelefteq \cup \{(a, b) \mid a, b \in M,\ a \trianglelefteq x,\ y \trianglelefteq b\}$$

a tvrdíme, že to je opět částečné uspořádání, což bude spor s maximalitou $\trianglelefteq$.

- Reflexivita: jasná, všechny dvojice (m, m) už v $\trianglelefteq$ byly.
- Antisymetrie: aby neplatila, muselo by už dříve v $\trianglelefteq$ ležet nějaké (b, a). Pak aby ale díky $y \trianglelefteq b \trianglelefteq a \trianglelefteq x$ musely být y a x porovnatelné, což je spor.
- Tranzitivita: aby neplatila, musíme mít nějaká $k, \ell, m \in M$ tak, že $k \mathrel{\widetilde{\trianglelefteq}} \ell$, $\ell \mathrel{\widetilde{\trianglelefteq}} m$, ale nikoliv $k \mathrel{\widetilde{\trianglelefteq}} m$. Pokud budeme používat jen porovnání, která už byla v $\trianglelefteq$, nic se nezměnilo, takže BÚNO uvažujme, že $(k, \ell) \in \widetilde{\trianglelefteq}$ je jedna z dvojic tvaru (a, b), co jsme přidali, tedy $k \trianglelefteq x$ a $y \trianglelefteq \ell$. Odkud pochází dvojice $(\ell, m) \in \widetilde{\trianglelefteq}$? Pokud už bylo $\ell \trianglelefteq m$, pak máme jednoduše $y \trianglelefteq \ell \trianglelefteq m$, takže $y \trianglelefteq m$, takže i (k, m) bude jedna z dvojic, které jsme přidali do $\widetilde{\trianglelefteq}$. Naopak pokud by měla (ℓ, m) být jedna z dvojic, co jsme přidali, znamená to $\ell \trianglelefteq x$ a $y \trianglelefteq m$. Ale už jsme měli i $y \trianglelefteq \ell$, takže dohromady $y \trianglelefteq \ell \trianglelefteq x$, což znamená, že x, y byly porovnatelné.

11. Buď R gaussovský obor a T jeho podílové těleso. Mějme nekonstantní primitivní polynom $f \in R[x]$. Pak f je ireducibilní v $T[x]$, právě když je ireducibilní v $R[x]$.

Řešení. Viz Tvrzení 1.16b ve skriptech.

12. * Buď F konečné těleso. Nahlédni, že libovolné zobrazení $f : F \to F$ lze zapsat polynomem.

Řešení. Polynomy $x - a$ pro $a \in F$ jsou vzájemně nesoudělné. Můžeme tedy použít Čínskou zbytkovou větu: když položíme kongruence $f \equiv F(a) \pmod{x-a}$, bude existovat polynom, který je všechny splňuje. Jenže $f \equiv f(a) \pmod{x-a}$, takže takový polynom se bude ve všech bodech shodovat s F.

13. * (Eisensteinovo kritérium) Mějme primitivní polynom $f = a_n x^n + \cdots + a_1 x + a_0$ s celočíselnými koeficienty a prvočíslo p. Dokaž, že pokud $p \nmid a_n$, $p \mid a_i$ pro $i = 0, 1, \ldots, n-1$ a $p^2 \nmid a_0$, pak je f ireducibilní nad $\mathbb{Z}$. Zkus se zamyslet nad zobecněním pro obecný obor integrity R namísto $\mathbb{Z}$.

Řešení. Pro spor je f reducibilní, tedy $f = gh$. Pak musí g i h být primitivní, takže pro reducibilitu musí být nekonstantní. Vše zmodulíme p, obrazy našich polynomů (v $\mathbb{Z}_p[x]$) budeme značit vlnkou. Pak $\tilde{f} = \tilde{g}\tilde{h}$. Jenže ze zadání je $\tilde{f} = a_n x^n$. Víme, že $\mathbb{Z}_p[x]$ je eukleidovský, tedy i OHI, tedy i gaussovský, takže z jednoznačných rozkladů musí být $\tilde{g} = b_k x^k$, $\tilde{h} = c_\ell x^\ell$, kde $k + \ell = n$. Z nekonstantnosti dále $k, \ell \geq 1$. Pak ale p dělilo oba absolutní členy v g i h, takže a_0 musí být násobek p^2 – to je spor.

14. * Pomocí Zornova lemmatu dokaž, že pokud v okruhu R existuje vlastní ideál, který není konečně generovaný, pak v něm také existuje prvoideál, který není konečně generovaný.

Řešení. Standardně pomocí Zornova lemmatu zkonstruujeme ideál, který je maximální *mezi těmi ideály, jež nejsou konečně generované*, nazvěme ho P. Poté zbývá dokázat, že tento ideál je prvoideál. K tomu je potřeba postupovat sporem a využít toho, že každý větší ideál už musí být konečně generovaný. Zde je osnova důkazu postupující podle této (`https://math.stackexchange.com/a/146899`) odpovědi na stackexchangi – dorozmyšlení, jednotlivých kroků je ponecháno čtenáři:

1) Když pro spor P nebude prvoideál, vezmi $x, y \in R$ takové, že $xy \in P$, ale $x, y \notin P$.
2) $P + (y)$ je nad P, takže už je konečně generovaný: $P + (y) = (p_1 + r_1 y, \ldots, p_n + r_n y)$.
3) $P_y := \{s \in R \mid sy \in P\}$ je ideál a leží nad P, takže opět $P_y = (s_1, \ldots, s_m)$.
4) Vezmi libovolné $p \in P$, vyjádři ho jako prvek $P + (y)$ pomocí generátorů.
5) Příslušnou lineární kombinaci $r_1, \ldots, r_n$ vyjádři jako prvek P_y pomocí generátorů.
6) $P = (p_1, \ldots, p_n, s_1, \ldots, s_m)$, spor.