Úvod do komutativní algebry: cvičení 2

web cvičení: `gimli.ms.mff.cuni.cz/~matej/komalg23`

26. října 2023

Gaussovo lemma, Čínská zbytková věta, využití Zornova lemmatu

Ukážeme si:

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

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.

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

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

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?

Další příklady (řeš klidně na přeskáčku):

Úlohy s * jsou těžší.

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.)

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

8. Ať je R okruh a $I_1, \dots, I_n$ 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.

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

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 $x, y \in M$.

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 $R[x]$.

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

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 $i = 0, 1, \dots, n-1$ a $p^2 \nmid a_0$, pak je f ireducibilní nad $\mathbb{Z}$. Zkus se zamyslet nad zobecněním pro obecný obor integrity R namísto $\mathbb{Z}$.

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.

Hinty:

12. Čínská zbytková věta v $F[x]$. Lineární polynomy dávají maximální ideály. (Alternativně Lagrangeova interpolace.)

13. Předpokládej pro spor $f = gh$, zobraz celou situaci projekcí $\mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}_p[x]$ a využij jednoznačných rozkladů.