Úvod do komutativní algebry: cvičení 7

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

11. ledna 2024

Algebraická teorie čísel

Ukážeme si:

1. Najdi všechny jednotky v $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ pro $D = -2, -3, -7$.
* Pokud už jsi někdy viděl(a) Pellovu rovnici, zkus i $D = 2, 5$.

2. Ireducibilní prvky pro $K = \mathbb{Q}(\sqrt{-14})$:

a) Pokud má prvek $\alpha \in \mathcal{O}_K$ normu p, což je prvočíslo v $\mathbb{Z}$, pak je α ireducibilní v $\mathcal{O}_K$.
b) Najdi nějaký ireducibilní prvek v $\mathbb{Z}[\sqrt{-14}]$ s prvočíselnou normou.
c) Dokaž, že 3 a $1 + \sqrt{-14}$ jsou ireducibilní.
d) Dokaž, že $3 \cdot 3 \cdot 3 \cdot 3 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14})$ jsou dva různé ireducibilní rozklady.

3. Hlavní ideály pro $K = \mathbb{Q}(\sqrt{-14})$:

a) Dokaž, že $(17 + 2\sqrt{-14}, 20 + \sqrt{-14}) = (3 - \sqrt{-14})$ je hlavní ideál v $\mathbb{Z}[\sqrt{-14}]$.
b) $(2, \sqrt{-14})$ není hlavní ideál v $\mathbb{Z}[\sqrt{-14}]$.
c) Dokaž, že $(2 + \sqrt{-14}, 7 + 2\sqrt{-14}) = (3, 1 - \sqrt{-14})$ a že jde o vlastní ideál, který není hlavní.

4. Násobení ideálů pro $K = \mathbb{Q}(\sqrt{-14})$:

a) $(5 + \sqrt{-14}, 2 + \sqrt{-14})(4 + \sqrt{-14}, 2 - \sqrt{-14}) = (6, 3\sqrt{-14})$.
b) Buď $I = (3, 1 + \sqrt{-14})$. Pak $II' = (3)$, I není hlavní a $I \neq I'$.
c) Buď $J = (5, 1 + \sqrt{-14})$. Pak $(15) = IJI'J'$. Využij toho k nalezení dvou různých ireducibilních rozkladů 15.
d) * I, J jsou prvoideály.

5. Buď G podgrupa aditivní grupy $\mathbb{Z}^n$, kde $n \in \mathbb{N}$. Dokaž, že $G \simeq \mathbb{Z}^m$ pro nějaké m, $0 \leq m \leq n$. Jako důsledek nahlédni, že libovolný ideál v $\mathcal{O}_K$ lze zapsat nanejvýš dvěma generátory.

Další příklady (řeš klidně na přeskáčku): Úlohy s * jsou těžší.

6. Buď $K = \mathbb{Q}(\sqrt{D})$ a $\omega = \sqrt{D}$, resp. $\frac{1+\sqrt{D}}{2}$ pro $D \equiv 2, 3$, resp. $1 \pmod 4$. Pro $m \in \mathbb{Z}$ a $\alpha = a + b\omega \in \mathcal{O}_K$ dokaž, že $m \mid \alpha$ v $\mathcal{O}_K$, právě když $m \mid a, b$ v $\mathbb{Z}$. Nahlédni, že pro $D \equiv 1 \pmod 4$ nemusí totéž platit pro $m \mid a + b\sqrt{D}, a, b \in \mathbb{Z}$.

7. Vyřeš diofantické rovnice $x^2 + 1 = y^5$, $x^2 + 3 = y^3$ a $x^2 + 4 = y^3$.

8. Dokaž, že $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\sqrt{D}]$, resp. $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ pro $D \equiv 2, 3$, resp. $1 \pmod 4$.

9. Buď $K = \mathbb{Q}(\sqrt{D})$. Je-li $P < \mathcal{O}_K$ nenulový prvoideál a $\alpha \in \mathcal{O}_K$, potom $\alpha^{NP} \equiv \alpha \pmod P$.

10. Buď R gaussovský obor a T jeho podílové těleso. Je-li $u \in T$ celistvé nad R, pak $u \in R$.

11. * Je dáno prvočíslo $p > 5$ a přirozené k takové, že $p \mid k^2 + 5$. Dokaž, že existují přirozená m, n splňující $p^2 = m^2 + 5n^2$. Předpokládej, že víš, že třídová grupa $\mathbb{Z}[\sqrt{-5}]$ je dvouprvková.

12. ** Zkus si rozmyslet, že když $D \equiv 1 \pmod 4$, pak $\mathbb{Z}[\sqrt{D}]$ nikdy nemůže být gaussovský obor.

Hinty:

8. Dívej se, kdy má minimální polynom celočíselné koeficienty.

10. Věta o racionálním kořeni.

11. Najdi (prvo)ideál s normou p. Co potom třídová grupa říká o jeho druhé mocnině?

12. Cvičení **10.** poukazuje na něco, co $\mathbb{Z}[\sqrt{D}]$ nemá.