Komutativní okruhy: Cvičení 7

v roce 2019/2020 se nekonalo

1. Najdi všechny jednotky v $\mathbb{Q}(\sqrt{D})$ pro $D = -2, -3, -7$, *2, *5.

2. 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 $m|\alpha$ v $\mathcal{O}_K$, právě když $m|a, b$ v $\mathbb{Z}$. Dokaž, že to nemusí platit pro $m|a + b\sqrt{D}, a, b \in \mathbb{Z}$.

3. Ireducibilní prvky:

   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.

4. Hlavní ideály:

   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) Pomocí faktorokruhů modulo daný ideál dokaž, že $(2 + \sqrt{-14}, 7 + 2\sqrt{-14}) = (3, 1 - \sqrt{-14})$ a že jde o vlastní ideál (protože norma všech prvků je dělitelná 3).

5. Násobení ideálů:

   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.

Další příklady:

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

7. Dokonči důkaz důsledku 4.2 z přednášky, že každý prvek K jde vyjádřit jako α/n pro $\alpha \in \mathcal{O}_K$ a $n \in \mathbb{N}$.

8. Buď G podgrupa aditivní grupy $\mathbb{Z}^n$, kde $n \in \mathbb{N}$. Dokaž, že $G \simeq \mathbb{Z}^m$ pro nějaké m, $0 \leq m \leq n$.

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

Úlohy s * jsou trochu těžší.