5. cvičení (27. března 2008)

Co jsme dělali?

Popsali jsme prvočísla v $\mathbb{Z}[i]$. Pak jsme pracovali okruhy $\mathbb{Z}[\alpha]$, kde α je kořen nějakého monického ireducibilního polynomu stupně 2 s celočíselnými koeficienty. Tento okruh často nemá jednoznačný rozklad na součin ireducibilních prvků - například $\mathbb{Z}[\sqrt{-5}]$ ani $\mathbb{Z}[\sqrt{-3}]$ nejsou euklidovské okruhy a nemají jednoznačné rozklady.

Označme $\omega = \frac{-1+\sqrt{-3}}{2}$. V $\mathbb{Z}[\omega]$ definujme $N(a+b\omega) = a^2 - ab + b^2$. Toto je o euklidovské zobrazení, a tedy v $\mathbb{Z}[\omega]$ má každý prvek jednoznačný rozklad na součin ireducibilních prvků.

Příklady

-1. V $\mathbb{Z}[\sqrt{-5}]$ platí $(7+\sqrt{-5})(7-\sqrt{-5}) = 2 \cdot 37$, všechny faktory jsou ireducibilní. $\mathbb{Z}[\sqrt{-5}]$ tedy nemá jednoznačný rozklad na součin ireducibilních prvků.

0. V $\mathbb{Z}[\sqrt{-3}]$ platí $7 \cdot \sqrt{-3} = (-2+\sqrt{-3})(-2\sqrt{-3}+3)$, všechny faktory jsou ireducibilní. $\mathbb{Z}[\sqrt{-5}]$ tedy nemá jednoznačný rozklad na součin ireducibilních prvků.

1. Popiš invertibilní prvky oboru $\mathbb{Z}[\omega]$.

2. Buď $R \subseteq \mathbb{C}$ obor uzavřený na konjugaci (existují obory, které nejsou uzavřené na konjugaci?). Pokud $\alpha|\beta$ v R, pak $\overline{\alpha}|\overline{\beta}$ v R.

3. Vyřeš rovnici $x^2 + 3 = y^3$ (příklad asi nejde dopočítat).

4. Vyřeš rovnici $x^3 + y^3 = z^3$ (tento příklad je poměrně obtížný).

5. Uvažujme $\mathbb{Z}[\alpha]$, kde α je kořen nějakého monického ireducibilního polynomu stupně 2 s celočíselnými koeficienty. Dokaž, že $\beta \mapsto \overline{\beta}$ je automorfismus tohoto okruhu.

6. Buď n bezčtvercové přirozené číslo (tedy takové, které není dělitelné druhou mocninou žádného prvočísla). Dokaž, že pokud $n \equiv 1 \pmod 4$, je $\mathbb{Z}[\frac{-1+\sqrt{n}}{2}]$ okruhem celistvých prvků tělesa $\mathbb{Q}[n]$, a že pokud $n \equiv -1 \pmod 4$, je $\mathbb{Z}[n]$ okruhem celistvých prvků tělesa $\mathbb{Q}[n]$. (Okruhem celistvých prvků rozumíme množinu všech těch prvků tělesa, které jsou kořenem nějakého monického polynomu.)