

Abstraktní teorie dělitelnosti

5 Základní pojmy

5.1 Největší společný dělitel

1. Spočítejte $\text{NSD}(5 + 7i, 3 - i)$, $\text{NSD}(6 - 7i, 7 + i)$, $\text{NSD}(8 + 5i, 4 + i)$ v oboru $\mathbb{Z}[i]$. (Pomocí normy to bude jednodušší než pomocí Eukleidova algoritmu.) [1 + i, 2 + i, 1]
2. Spočítejte $\text{NSD}(6 - 3\sqrt{3}, 3 + \sqrt{3})$ v oboru $\mathbb{Z}[\sqrt{3}]$. [$\sqrt{3}$]

5.2 Ireducibilní prvky a rozklady

1. Najděte ireducibilní rozklad polynomů $x^3 - 2$ a $x^4 - x^2 - 2$ v oborech $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}_3[x]$ a $\mathbb{Z}_5[x]$. [ired., $(x - \sqrt[3]{2})(x^2 + x\sqrt[3]{2} + \sqrt[3]{4})$, $\prod_{k=0}^2 (x - e^{k2\pi i/3} \sqrt[3]{2})$, $(x+1)^3$, $(x+2)(x^2+3x+4)$; $(x^2+1)(x^2-2)$, $(x-\sqrt{2})(x+\sqrt{2})(x^2+1)$, $(x-\sqrt{2})(x+\sqrt{2})(x-i)(x+i)$, $(x^2+1)^2$, $(x+3)(x+2)(x^2-2)$]
2. Najděte ireducibilní rozklad polynomů $2x^2 + 2$ a $x^3 - 2$ v oborech $\mathbb{Z}[x]$, $\mathbb{Z}[i][x]$, $\mathbb{R}[x]$ a $\mathbb{C}[x]$. [$2 \cdot (x^2 + 1)$, $2(x-i)(x+1)$, ired., $(x-i)(2x+2i)$; ired., ired. neboť $a + bi = e^{k2\pi i/3} \sqrt[3]{2}$ nemá řešení pro $a, b, k \in \mathbb{Z}$, ... stejné jako v 5.2.1]
3. Najděte ireducibilní rozklad polynomu $2x^2 + 2x + 3$ v oborech $\mathbb{Q}(\sqrt{-5})[x]$ a $\mathbb{Z}[\sqrt{-5}][x]$. [$(x + \frac{1}{2} - \frac{1}{2}\sqrt{-5})(2x + 1 + \sqrt{-5})$, ired. neboť nemá kořen a všechny koeficienty jsou nesoudělné]
4. Dokažte, že všechny ireducibilní polynomy v $\mathbb{R}[x]$ mají stupeň ≤ 2 . [Pomocí základní věty algebry a seskupení sdružených kořenů.]
5. Rozhodněte, zda je polynom $x^4 + x^2 + 1$ ireducibilní v oboru $\mathbb{Z}_5[x]$. [Není, například lze vydělit obecným polynomem a získat soustavu rovnic pro koeficienty, získáme rozklad $(x^2 - x + 1)(x^2 + x + 1)$]
6. Najděte ireducibilní rozklad prvků 3, 5, 6, 7, $10 - 6i$, $9 + 3i$ a $11 + 2i$ v oboru $\mathbb{Z}[i]$. [ired., $(1 + 2i)(1 - 2i)$, $3(1 + i)(1 - i)$, ired., $(1 + i)^2(1 - i)(1 - 4i)$, $3(1 + i)(2 - i)$, $-(1 + 2i)^3$]
7. Najděte ireducibilní rozklad prvků 2, 3, 5 a $5 - 2\sqrt{-2}$ v oboru $\mathbb{Z}[\sqrt{-2}]$. [$-(i\sqrt{2})^2$, $(1 + i\sqrt{2})(1 - i\sqrt{2})$, ired., $(1 - i\sqrt{2})(3 + i\sqrt{2})$]