4 Přes kvadratická rozšíření vzhůru k ideálům!

Zadání
Verze ze dne 13. března 2024

Cíle cvičení: Dnes se pustíme do dělení a rozkladů v kvadratických rozšířeních celých čísel. U některých z nich budeme umět s využitím normy dokonce dělit se zbytkem a počítat největší společné dělitele. Cvičení zakončíme výhledem do světa ideálů a kupodivu se nám v něm dělení bude docela hodit.

Úlohy, které bychom určitě měli umět řešit:

Úloha 4.1. Vydělte se zbytkem číslo α číslem β

(a) v oboru $\mathbb{Z}[i]$, jestliže $\alpha = 5 + 7i$, $\beta = 3 - i$,

(b) v oboru $\mathbb{Z}[i]$, jestliže $\alpha = 3 + 2i$, $\beta = 1 + i$,

(c) v oboru $\mathbb{Z}[\sqrt{2}i]$, jestliže $\alpha = 4$, $\beta = 1 - \sqrt{2}i$,

(d) v oboru $\mathbb{Z}[\sqrt{2}i]$, jestliže $\alpha = 1 + 4\sqrt{2}i$, $\beta = 3 + \sqrt{2}i$

Všimněme si, že máme-li v obecném oboru posloupnosti nenulových prvků $\{a\}_{i=0}^{n}$ a $\{q\}_{i=1}^{n}$, pro niž platí $a_{i+1} = a_{i-1} - q_i a_i$ pro $i = 1, \ldots, n$ a $a_n \mid a_{n-1}$, pak

$$a_n = \mathrm{NSD}(a_n, a_{n-1}) = \cdots = \mathrm{NSD}(a_i, a_{i-1}) = \cdots = \mathrm{NSD}(a_n, a_{n-1}),$$

což znamená, že pokud pomocí obdoby dělení se zbytkem z tvrzení 4.4 využívajícího normu na oboru $\mathbb{Z}[\sqrt{s}]$ úspěšně proběhne Eukleidův algoritmus (tj, poslední zbytek je 0), dostaneme na výstupu největší společný dělitel.

Úloha 4.2. Najděte největší společné dělitele

(a) $\mathrm{NSD}(3 + i, 4 + 2i)$ v oboru $\mathbb{Z}[i]$,

(b) $\mathrm{NSD}(3 + 4i, 7 + 2i)$ v oboru $\mathbb{Z}[i]$,

(c) $\mathrm{NSD}(6 - 3\sqrt{3}, 3 + \sqrt{3})$ v oboru $\mathbb{Z}[\sqrt{3}]$.

Úloha 4.3. Spočítejte ireducibilní rozklady prvků

(a) 3, 5, 6, $10 - 6i$ v $\mathbb{Z}[i]$,

(b) 2, 3 v $\mathbb{Z}[\sqrt{2}i]$.

Úloha 4.4. Najděte $a \in \mathbb{N}$ tak, aby byl hlavní ideál $a\mathbb{Z}$ oboru celých čísel roven ideálu

(a) $2\mathbb{Z} \cap 3\mathbb{Z}$,

(b) $2\mathbb{Z} + 3\mathbb{Z}$,

(c) $28\mathbb{Z} + 63\mathbb{Z}$,

(d) $15\mathbb{Z} + 18\mathbb{Z} + 40\mathbb{Z}$,

(e) $(-28)\mathbb{Z} \cap (-63)\mathbb{Z}$.

Úloha 4.5. Ať R je obor hlavních ideálů (například eukleidovský obor). Dokažte, že pro zadaná $a, b \in R$ je $aR \cap bR = cR$ a $aR + bR = dR$, kde $c = \mathrm{nsn}(a, b)$ a $d = \mathrm{NSD}(a, b)$.

Úloha 4.6. Nechť $R = \mathbb{Z}[i]$. Najděte $a, b \in R$ taková, že

$$aR = (3+i)R + (4+2i)R \quad \text{a} \quad bR = (3+i)R \cap (4+2i)R.$$

A teď něco na konec cvičení a následnou afterparty:

Úloha 4.7. Vysvětlete následující „rozpor“:

- V oboru $\mathbb{Z}[i\sqrt{3}]$ platí $(-2)2 = (i\sqrt{3}+1)(i\sqrt{3}-1)$, a proto se nejedná o obor s jednoznačným rozkladem (tj. Gaussův obor).
- V oboru $\mathbb{Z}[\sqrt{2}]$ platí $\sqrt{2}\sqrt{2} = (-4+3\sqrt{2})(4+3\sqrt{2})$, a přesto se jedná o obor s jednoznačným rozkladem.

Úloha 4.8. Vysvětlete, proč například pro prvky $\sqrt{5}+1$ a 2 v oboru $\mathbb{Z}[\sqrt{5}]$ Eukleidův algoritmus selže. Jak dopadne Eukleidův algoritmus v témže oboru pro prvky $1 - 2\sqrt{5}$ a 2?

Úloha 4.9. Spočítejte

(a) ireducibilní rozklady prvků 7, $9 + 3i$ v oboru $\mathbb{Z}[i]$,

(b) $\mathrm{NSD}(3 + 6i, 12 - 3i)$, $\mathrm{NSD}(5 + 3i, 13 + 18i)$ v oboru $\mathbb{Z}[i]$,

(c) ireducibilní rozklady prvků $3 - i\sqrt{2}$ a $5 - i\sqrt{2}$ v oboru $\mathbb{Z}[i\sqrt{2}]$,

(d) ireducibilní rozklady prvku $3 + \sqrt{2}$ a $3 - 8\sqrt{2}$ v oboru $\mathbb{Z}[\sqrt{2}]$.

Úloha 4.10. Najděte v oboru $\mathbb{Z}[\sqrt{3}]$ nekonečně mnoho invertibilních prvků.

Úloha 4.11. Najděte generátory hlavních ideálů $aR + bR$ a $aR \cap bR$, pokud

(a) $R = \mathbb{Z}[i]$, $a = 3 + 4i$, $b = 7 + 2i$,

(b) $R = \mathbb{Z}[\sqrt{3}]$, $a = 6 - 3\sqrt{3}$, $3 + \sqrt{3}$, zde můžete bez důkazu použít fakt, že je $\mathbb{Z}[\sqrt{3}]$ eukleidovský obor.

Úloha 4.12. Nechť $S = \mathbb{Z}[x]$ a uvažujme ideály $I = 2S + xS$ a $J = 3S + xS$. Ukažte, že:

1. I, J nejsou hlavní ideály.
2. množina $\{ab \mid a \in I, b \in J\}$ netvoří ideál v okruhu S.

Úloha 4.13. Najděte v okruhu polynomů $R = \mathbb{Z}_5[x, y]$ ideál, který není hlavní.

Úloha 4.14. Buď $\mathcal{R}$ komutativní okruh a $a \in R$ splňující $a^n = 0$. Dokažte, že je prvek $1 - a$ invertibilní v $\mathcal{R}$. Platí toto tvrzení i v okruzích s nekomutativním násobením?

Úloha 4.15.* Rozhodněte, pro která $s, t \in \mathbb{Z}$ platí $\sqrt{s} \in \mathbb{Z}[\sqrt{t}]$. Uvažujte s, t taková, že nejsou dělitelná čtvercem prvočísla.