**Základní algebraické objekty**

# 4 Číselné obory

## 4.1 Okruhová a tělesová rozšíření

**1.** Popište prvky uvedených oborů a porovnejte je pomocí inkluze:

(a) $\mathbb{Z}[\sqrt{6}]$, $\mathbb{Z}[\sqrt{24}]$, $\mathbb{Z}[\sqrt{2},\sqrt{3}]$. $[\mathbb{Z}[\sqrt{24}] \subsetneq \mathbb{Z}[\sqrt{6}] \subsetneq \mathbb{Z}[\sqrt{2},\sqrt{3}]]$

(b) $\mathbb{Q}[\sqrt{6}]$, $\mathbb{Q}[\sqrt{24}]$, $\mathbb{Q}[\sqrt{2},\sqrt{3}]$. $[\mathbb{Q}[\sqrt{24}] = \mathbb{Q}[\sqrt{6}] \subsetneq \mathbb{Q}[\sqrt{2},\sqrt{3}]]$

**2.** Jsou obory $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ a $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$ totožné? Jaká by byla odpověď pro $\mathbb{Z}[\sqrt{2},\sqrt{3}]$ a $\mathbb{Z}[\sqrt{2}+\sqrt{3}]$? [ano; ne, koukněte na vztah parity koeficientů u $\sqrt{2}$ a $\sqrt{3}$]

**3.** Popište prvky oborů $\mathbb{Q}[\sqrt[3]{s}]$ a $\mathbb{Q}(\sqrt[3]{s})$. Jsou totožné? [Ano, prozkoumejte násobení prvkem $\sqrt[3]{s}$ jako lineární zobrazení nad $\mathbb{Q}$ z $\mathbb{Q}[\sqrt[3]{s}]$ do $\mathbb{Q}[\sqrt[3]{s}]$, je prosté?]

**4.** 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. [Právě pro $s = \pm t$]

## 4.2 Kvadratická rozšíření celých čísel

**1.** Najděte v oboru $\mathbb{Z}[\sqrt{3}]$ nekonečně mnoho invertibilních prvků. [např. $\{(2+\sqrt{3})^k; k \in \mathbb{Z}\}$]

**2.** Dělte se zbytkem v oboru $\mathbb{Z}[i]$ dvojice $(5+7i) : (3-i)$, $(3+2i) : (1-2i)$, $(3+2i) : (1+i)$. $[1+3i;\ 2i;\ 3-i]$

**3.** Pokud umíme dělit se zbytkem, můžeme provádět Eukleidův algoritmus (jednoznačnost dělení nebyla nikde potřeba). Spočtěte pomocí Eukleidova algoritmu $\mathrm{NSD}(5+3i, 13+18i)$ v oboru $\mathbb{Z}[i]$. $[-1-4i]$

**4.** Dělte se zbytkem v oboru $\mathbb{Z}[\sqrt{-2}]$ dvojici $(1+4\sqrt{2}i) : (3+\sqrt{2}i)$. $[1+\sqrt{2}i]$

**5.** Dokažte, že v oborech $\mathbb{Z}[\sqrt{2}]$ a $\mathbb{Z}[\sqrt{3}]$ lze dělit se zbytkem. (*Návod:* Sice schází geometrická představa, nicméně funguje podobný algoritmus dělení založený na zaokrouhlování koeficientů podílu. Důkaz odhadu normy zbytku je o něco komplikovanější.)

## 4.3 Dělení polynomů se zbytkem

**1.** Dělte se zbytkem polynomy $x^4+3x^3+4x^2+x+3$ a $x^2+2$ v oborech $\mathbb{Z}[x]$ a $\mathbb{Z}_5[x]$. [$x^2+3x+2$ zbytek $-5x-1$; $x^2+3x+2$ zbytek $4$]

**2.** Dělte se zbytkem polynomy $x^4+x^2+x$ a $x^2+x+1$ v oborech $\mathbb{Z}[x]$ a $\mathbb{Z}_2[x]$. [$x^2-x+1$ zbytek $x-1$; $x^2+x+1$ zbytek $x+1$]

## 4.4 Kořeny a dělitelnost

**1.** Najděte polynom $f \in \mathbb{Z}_{15}[x]$ stupně 3, který má aspoň 9 různých kořenů v okruhu $\mathbb{Z}_{15}$. $[5x^3-5x]$