Příklad (3.1)
Nalezněte ireducibilní rozklad polynomu $x^4 + 1$ nad tělesy $\mathbb{C}$, $\mathbb{R}$ a $\mathbb{Z}_5$.

Řešení
Ze střední školy víme, že rovnice $x^4 + 1 = 0$ má 4 řešení tvaru $e^{k\frac{2\pi}{4}+\frac{\pi}{4}}$ (jelikož $-1 = e^{\pi}$), tedy rozklad v $\mathbb{C}$ bude

$$x^4 + 1 = \left(x - e^{\pi/4}\right) \cdot \left(x - e^{3\pi/4}\right) \cdot \left(x - e^{5\pi/4}\right) \cdot \left(x - e^{7\pi/4}\right) =$$

$$\left(x - \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right) \cdot \left(x + \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right) \cdot \left(x + \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) \cdot \left(x - \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right),$$

jelikož polynomy stupně 1 jsou v tělese ireducibilní.

Pro rozklad v reálných číslech si můžeme všimnout, že prostřední dva činitelé a krajní dva jsou rozklady rozdílu čtverců:

$$x^4+1 = \left(x + \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right) \cdot \left(x + \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) \cdot \left(x - \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) \cdot \left(x - \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right) =$$

$$= \left(x^2 + x\sqrt{2} + 1\right) \cdot \left(x^2 - x\sqrt{2} + 1\right).$$

To už je ireducibilní rozklad, protože dělitelé polynomu mají menší stupeň. A polynom stupně 0 je invertibilní, a pokud by existoval polynom stupně jedna dělící $x^4 + 1$, pak by existoval i kořen v reálných číslech, ale my víme, že všechny 4 kořeny jsou komplexní ($\mathbb{C} \setminus \mathbb{R}$).

V $\mathbb{Z}_5$ polynom $x^4 + 1$ nemá kořeny, jelikož pro $x \equiv 0$ je to 1 a pro $x \not\equiv 0$ je $x^4 \equiv 1$ (z Eulerovy věty), tedy $x^4 + 1 \equiv 2$. Tudíž hledáme rozklad na polynomy stupně dva. Když jsme nepochodili s kořeny $x^4 + 1$, můžeme zkusit najít kořeny $y^2 + 1$. Jednoduchým otestováním se dostaneme ke kořenům 2 a 3. Tedy:

$$x^4 + 1 \equiv \left(x^2 - 3\right) \cdot \left(x^2 - 2\right) \equiv \left(x^2 + 2\right) \cdot \left(x^2 + 3\right).$$

Příklad (3.2)
Nalezněte (nějaký) ireducibilní rozklad prvku $16 + i\sqrt{5}$ v oboru $\mathbb{Z}[i\sqrt{5}]$.

Řešení
Víme, že norma na $\mathbb{Z}[i\sqrt{5}]$ je dána $\nu(a+b\cdot i\sqrt{5}) = |a^2+5b^2|$, tedy $\nu(16+i\sqrt{5}) = |256+5| = 261 = 3^2 \cdot 29$. Víme, že pokud $a|b$, pak $\nu(a)|\nu(b)$, tedy zkusíme rozklad na prvky norem 9 a 29, jelikož 3 je moc malá, protože pro $|b| > 0$ je $\ni (a+bi\sqrt{5}) \geq 5$, tedy jediným prvkem $\mathbb{Z}[i\sqrt{5}]$ s normou 3 je 3 a ta už na první pohled $16+i\sqrt{5}$ nedělí.

Prvky s normou $9 = 2^2 + 5 \cdot 1^2$ a $29 = 3^3 + 5 \cdot 2^2$ jsou například $2 + i\sqrt{5}$ a $3 + 2i\sqrt{5}$, ale ty vynásobené mezi sebou nedají $16 + i\sqrt{5}$. Tak zkusíme změnit znaménko a:

$$16 + i\sqrt{5} = (2 - i\sqrt{5})(3 + 2i\sqrt{5}),$$

kde norma prvního je 9, tedy všichni nevlastní dělitelé musí mít normu 3 a to už víme, že nejde, a norma druhého je 29, což je prvočíslo, tedy jsme opravdu našli ireducibilní rozklad.

Příklad (3.3)
Nalezněte největšího společného dělitele čísel $4+6i$ a $3-7i$ v oboru $\mathbb{Z}[i]$.

Řešení
Víme, že $\mathbb{Z}[i]$ je eulerovský, tedy použijeme eukleidův algoritmus:

$$3-7i, 4+6i : \frac{3-7i}{4+6i} = \frac{(3-7i)(4-6i}{52} = \frac{-30-46i}{52} = \frac{-52-52i}{52} + \frac{22+6i}{52} \doteq -1-i.$$

Zaokrouhlujeme tak, aby norma zbytku byla nejmenší. Zbytek můžeme dopočítat z předchozího výpočtu, nebo: $3-7i-(4+6i)\cdot(-1-i) = 3-7i-2+10i = 1+3i$.

$$4+6i, 1+3i : \frac{4+6i}{1+3i} = \frac{(4+6i)(1-3i)}{10} = \frac{22-6i}{10} = \frac{20-10i}{10} + \frac{2+4}{10} \doteq 2-i.$$

$$4+6i-(2-i)\cdot(1+3i) = 4+6i-5-5i = -1+i.$$

$$1+3i, -1+i : \frac{1+3i}{-1+i} = \frac{(1+3i)(-1-i)}{2} = 1-2i.$$

Tudíž zbytek nula a $\mathrm{NSD}(4+6i, 3-7i) = -1+i$ (a všechna sdružená čísla).

Příklad (3.4)
Zvolme pevné $z \in \mathbb{C}$. Ukažte, že množina $\{f \in \mathbb{Q}[x] | f(z) = 0\}$ tvoří ideál okruhu $\mathbb{Q}[x]$.

Důkaz
Stačí ukázat uzavřenost na sčítání, opačný prvek a násobení libovolným prvkem $\mathbb{Q}[x]$:

$$f, g \in \mathbb{Q}[x] \wedge f(z) = g(z) = 0 \implies (f+g)(z) = 0+0 = 0,$$

$$f \in \mathbb{Q}[x] \wedge f(z) = 0 \implies (-f)(z) = -0 = 0,$$

$$f, g \in \mathbb{Q}[x] \wedge f(z) = 0 \implies (f \cdot g)(z) = f(z) \cdot g(z) = 0 \cdot g(z) = 0.$$

□