Algebra — cvičení 4, řešení

1. Máme najít $0 < B < 55$, pro něž je $B^{27} \mod 55 = 47$. Jelikož víme, že $55 = 5 \cdot 11$, víme také, že $\varphi(55) = 40$. Potřebujeme najít inverzní prvek k 27 v $\mathbb{Z}_{40}$ (ten existuje, neboť 27 a 40 jsou nesoudělná). Buď použijeme rozšířený Eukleidův algoritmus, nebo přímo uhodneme, že $27 \cdot 3 = 81 \equiv 1 \pmod{40}$. Dostáváme $B = 47^3 \mod 55 = (-8)^3 \mod 55 = 38$.

2. (b) Rozkládáme polynom $x^4 - x^2 - 2$. Po případné substituci $y = x^2$ snadno spočteme jeho kořeny. Hledané rozklady pak jsou následující:

- nad $\mathbb{C}$: $(x - i)(x + i)(x - \sqrt{2})(x + \sqrt{2})$;
- nad $\mathbb{R}$: $(x^2 + 1)(x - \sqrt{2})(x + \sqrt{2})$;
- nad $\mathbb{Q}$: $(x^2 + 1)(x^2 - 2)$
- nad $\mathbb{Z}_3$: zde máme $x^4 - x^2 - 2 = x^4 + 2x^2 + 1 = (x^2 + 1)^2$;
- nad $\mathbb{Z}_5$: najdeme kořen(y) v $\mathbb{Z}_5$, čímž obdržíme rozklad $(x - 2)(x - 3)(x^2 - 2)$.

4. Hledáme ireducibilní rozklady v $\mathbb{Z}[i]$: $3, 7$ jsou ireducibilní prvky, jelikož se jedná o prvočísla $\equiv 3 \pmod{4}$; $5 = (2 + i)(2 - i)$; $10 - 6i = (1 + i)(1 - i)^2(4 + i)$, kde $(4 + i)$ je ireducibilní, neboť má (prvočíselnou) normu 17.

5. Hledáme ireducibilní rozklady v $\mathbb{Z}[i\sqrt{2}]$: $2 = (i\sqrt{2})(-i\sqrt{2})$; $3 - i\sqrt{2}$ je ireducibilní, neboť má (prvočíselnou) normu 11; $5 - i\sqrt{2} = (1 + i\sqrt{2})^2(-1 - i\sqrt{2})$, zde jsme po zjištění, že $\nu(5 - i\sqrt{2}) = 27$, využili toho, že prvek normy 3 je (až na asociovanost, tj. v případě oboru $\mathbb{Z}[i\sqrt{2}]$ až na znaménko) jediný, a sice $1 + i\sqrt{2}$.

6. Ukazujeme, že prvočísla $\equiv 3 \pmod{4}$ jsou ireducibilními prvky v $\mathbb{Z}[i]$. Mějme proto nějaké takové prvočíslo p. Pak v $\mathbb{Z}[i]$ máme $\nu(p) = p^2$. Pokud by p nebylo ireducibilní, musel by v $\mathbb{Z}[i]$ existovat prvek normy p. To ale není možné, jelikož pro $a, b \in \mathbb{Z}$ je $\nu(a + bi) = a^2 + b^2 \not\equiv 3 \pmod{4}$. (Pro sudé a, b je jeho druhá mocnina 0 modulo 4, pro liché a, b je naopak rovna 1.)

8. Ukažte, že v oboru $\mathbb{Z}[\sqrt{2}]$ neexistuje prvek s normou 23. Opět nám v zadání trochu zaúřadoval šotek. Zjevně $\nu(5 + \sqrt{2}) = 23$. V zadání mělo být 27 místo 23. Pak jde o to, že číslo tvaru $a^2 - 2b^2$ nemůže dávat zbytky 3 či 5 po dělení 8, takže ani jeho absolutní hodnota nemůže dávat zbytek 3.

9. Nalezněte nějaký prvek nějakého oboru, který bude mít alespoň *tři* různé rozklady na ireducibilní prvky. Uvažujme kupříkladu obor $\mathbb{Z}[i\sqrt{5}]$. Zde máme $36 = 2 \cdot 2 \cdot 3 \cdot 3 = (1 + i\sqrt{5})^2(1 - i\sqrt{5})^2 = 2 \cdot 3 \cdot (1 + i\sqrt{5})(1 - i\sqrt{5})$. Využíváme toho, že v $\mathbb{Z}[i\sqrt{5}]$ zjevně neexistují prvky normy 2, ani prvky normy 3.

10. Nejprve ukážeme, že $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Uvědomme si, že inkluze $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \supseteq \mathbb{Q}[\sqrt{2} + \sqrt{3}]$ je triviální. Pro inkluzi opačnou stačí, když najdeme v $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$ prvek $\sqrt{2}$. Je užitečné spočíst si malé mocniny prvku $\sqrt{2} + \sqrt{3}$:

- $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$;
- $(\sqrt{2} + \sqrt{3})^3 = 2\sqrt{2} + 6\sqrt{3} + 9\sqrt{2} + 3\sqrt{3} = 11\sqrt{2} + 9\sqrt{3}$;
- $(\sqrt{2} + \sqrt{3})^4 = 13 + 8\sqrt{6} + 36 + 12\sqrt{6} = 49 + 20\sqrt{6}$.

Vidíme, že $2\sqrt{2} = (\sqrt{2}+\sqrt{3})^3 - 9(\sqrt{2}+\sqrt{3})$, takže $\sqrt{2} = \frac{1}{2}2\sqrt{2} \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$.

V případě rozšíření $\mathbb{Z}$ opět triviálně vidíme, že $\mathbb{Z}[\sqrt{2},\sqrt{3}] \supseteq \mathbb{Z}[\sqrt{2}+\sqrt{3}]$. Z postupu výše ale opačná inkluze neplyne, jelikož jsme potřebovali $\frac{1}{2} \in \mathbb{Q}$. Dostaneme pouze $2\sqrt{2} \in \mathbb{Z}[\sqrt{2}+\sqrt{3}]$. K tomu, abychom si uvědomili, že $\sqrt{2} \notin \mathbb{Z}[\sqrt{2}+\sqrt{3}]$, využijeme něco málo lineární algebry.

Těleso $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ má, jakožto vektorový prostor nad $\mathbb{Q}$, bázi $(1,\sqrt{2},\sqrt{3},\sqrt{6})$. Abychom si uvědomili, že tomu tak skutečně je, stačí vědět, že $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$, a tedy že báze prostoru $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ nad tělesem $\mathbb{Q}[\sqrt{2}]$ je $(1,\sqrt{3})$. Už ale víme, že $\mathbb{Q}[\sqrt{2},\sqrt{3}] = \mathbb{Q}[\sqrt{2}+\sqrt{3}]$, a z výpočtů mocnin výše vidíme, že bází vektorového prostoru $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ nad $\mathbb{Q}$ je také $(1,\sqrt{2}+\sqrt{3},(\sqrt{2}+\sqrt{3})^2,(\sqrt{2}+\sqrt{3})^3)$. V této bázi má prvek $\sqrt{2}$ jediné vyjádření, a sice $\sqrt{2} = \frac{(\sqrt{2}+\sqrt{3})^3}{2} - \frac{9(\sqrt{2}+\sqrt{3})}{2}$.

Pokud by prvek $\sqrt{2}$ náležel do $\mathbb{Z}[\sqrt{2}+\sqrt{3}]$, musel by existovat polynom $f \in \mathbb{Z}[x]$ takový, že $f(\sqrt{2}+\sqrt{3}) = \sqrt{2}$. Vzhledem k tomu, že $(\sqrt{2}+\sqrt{3})^4 = 10(\sqrt{2}+\sqrt{3})^2 - 1$, šlo by f bez újmy na obecnosti volit stupně menšího než 4. Tím bychom ale dostali odlišné vyjádření $\sqrt{2}$ pomocí bázových prvků než to jediné uvedené na konci předchozího odstavce, což by byl spor.