Faktorokruhy a kořenová/rozkladová nadtělesa

1. Ověřte, že je $\mathbb{Z}_3[\alpha]/(\alpha^2+1)$ těleso a spočítejte
   (a) $(\alpha)^5 = \alpha$
   (b) α^{-1}
   (c) $(\alpha+1)^{-1}$
   (d) $2\alpha \cdot (2\alpha+1)$
   (e) $\alpha^{-1} \cdot (\alpha+2)$

$\underline{a\alpha + b}$, $a, b \in \mathbb{Z}_3$

$\to 9$ prvků

a) $\alpha^5 : (\alpha^2+1) = \alpha^3 + 2\alpha \; (\alpha)$

$2\alpha^3$

b) NSD $(\alpha, \alpha^2+1) = \boxed{1 = f \cdot \alpha} + \cancel{g \cdot (\alpha^2+1)}$ mod α^2+1

α^2+1	1	0
α	0	1
1	1	$-\alpha = 2\alpha$

g $-\alpha$

$\alpha^2+1 : \alpha = \alpha$

$\alpha^{-1} = 2\alpha$

d) $2\alpha \cdot (2\alpha+1) = 4\alpha^2 + 2\alpha = \alpha^2 + 2\alpha$

$(\alpha^2 + 2\alpha) : \underline{(\alpha^2+1)} = f \; (g)$

$\cancel{\alpha^2} + 2\alpha - (\alpha^2 + 1) = 2\alpha - 1 = 2\alpha + 2$

-1

$\mathbb{Z}_3[\alpha]/(\alpha^2+1)$

f

$f = 0$

$\alpha^2 + 1 = 0$

$\boxed{\alpha^2 = -1}$

a) $\alpha^5 = \alpha^2 \cdot \alpha^2 \cdot \alpha = (-1)(-1) \cdot \alpha =$
$= \alpha$

3. Buď T těleso a $a \in T$. Dokažte, že je těleso $T[\alpha]/(\alpha - a)$ izomorfní tělesu T.
4. Dokažte, že je těleso $\mathbb{Q}[\alpha]/(\alpha^3 - 2)$ izomorfní tělesu $\mathbb{Q}(\sqrt[3]{2})$.

$T[\alpha]/(\alpha - a) \simeq T$

polynomy st. nejv. 0, tedy skaláry

$a, b \quad a \cdot b$

3. Buď T těleso a $a \in T$. Dokažte, že je těleso $T[\alpha]/(\alpha - a)$ izomorfní tělesu T.

4. Dokažte, že je těleso $\mathbb{Q}[\alpha]/(\alpha^3 - 2)$ izomorfní tělesu $\mathbb{Q}(\sqrt[3]{2})$.

$\alpha^3 - 2 = 0$
$\alpha^3 = 2$

$$\boxed{a\alpha^2 + b\alpha + c} \xmapsto{\varphi} a\sqrt[3]{4} + b\sqrt[3]{2} + c \quad \boxed{x\sqrt[3]{4} + y\sqrt[3]{2} + z}$$

(a, b, c) $\qquad$ (x, y, z)

$a, b, c, x, y, z \in \mathbb{Q}$

násobení: $\underset{\alpha^2}{(1,0,0)} \cdot \underset{\alpha^2}{(1,0,0)} = \alpha^4 = \alpha \cdot \alpha^3 = 2\alpha = (0,2,0)$

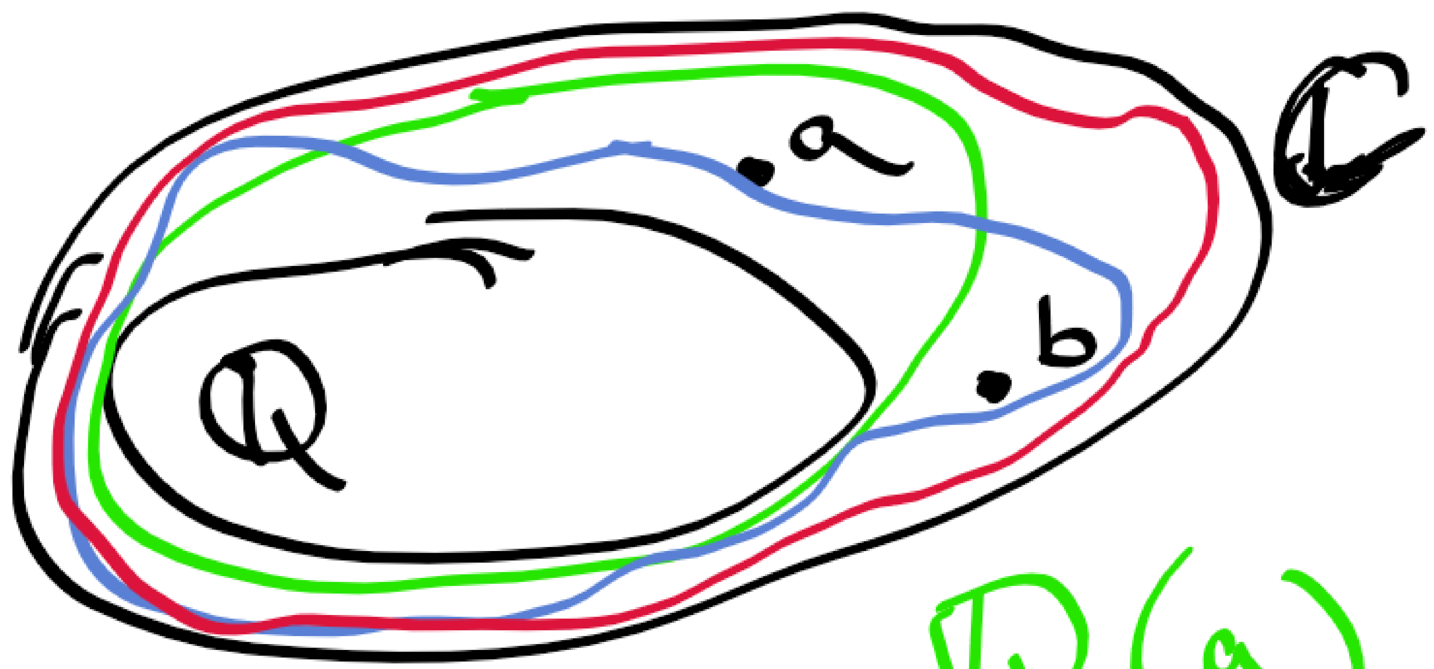
$\underset{\sqrt[3]{4}}{(1,0,0)} \cdot \underset{\sqrt[3]{4}}{(1,0,0)} = \sqrt[3]{4} \cdot \sqrt[3]{4} = \sqrt[3]{16} = \sqrt[3]{8} \cdot \sqrt[3]{2} = 2 \cdot \sqrt[3]{2} = (0,2,0)$

$\alpha^3 \cdot \alpha^2$ $\quad \mathbb{Q}[\alpha]/(\alpha^3 - 2) \not\cong \mathbb{Q}[\alpha]$

5. Napište všechna kořenová a rozkladová nadtělesa polynomů

(a) $x^2 - 2$
(b) $x^3 - 2x^2 - 2x - 3$
(c) $*\ x^n - 1$

nad tělesem $\mathbb{Q}$ obsažená v $\mathbb{C}$.



$\mathbb{Q}(a)$

$\mathbb{Q}(b)$

$\mathbb{Q}(a, b)$

a) $\sqrt{2}, -\sqrt{2}$

$$\mathbb{Q}(\sqrt{2}) \qquad \mathbb{Q}(-\sqrt{2})$$

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$$

5. Napište všechna kořenová a rozkladová nadtělesa polynomů

(a) $x^2 - 2$

(b) $x^3 - 2x^2 - 2x - 3$

(c) * $x^n - 1$

nad tělesem $\mathbb{Q}$ obsažená v $\mathbb{C}$.

b) $\frac{M}{S}$ .... 3 je kořen $\longrightarrow$ $\mathbb{Q}(3) = \mathbb{Q}$

$$(x^3 - 2x^2 - 2x - 3) : (x - 3) = \underline{x^2 + x + 1}$$

$x^2 - 2x - 3$

$x - 3$

$$D = b^2 - 4ac = -3$$

$$\Rightarrow \frac{-b \pm \sqrt{D}}{2a} = \begin{cases} \frac{-1 + i\sqrt{3}}{2} \rightarrow \mathbb{Q}\left(\frac{-1+i\sqrt{3}}{2}\right) \\ \qquad\qquad\qquad\qquad \| \\ \frac{-1 - i\sqrt{3}}{2} \rightarrow \mathbb{Q}\left(\frac{-1-i\sqrt{3}}{2}\right) \\ \qquad\qquad\qquad\qquad \| \end{cases}$$

$$\mathbb{Q}\left(3, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\right) = \mathbb{Q}\left(\frac{-1+i\sqrt{3}}{2}\right)$$

6. Popište rozkladové nadtěleso polynomu $x^2 + x + 1$ nad $\mathbb{Z}_2$ a rozložte v něm daný polynom na lineární členy.

$\mathbb{Z}_2 \leq \mathbb{Z}_2[\alpha] / (\alpha^2 + \alpha + 1)$ ... má kořen α

$\hookrightarrow \{\alpha, \alpha+1, 1, 0\}$

$(x^2 + x + 1) = (x - \alpha)(\cancel{\alpha} - ?) =$

$= \boxed{(x - \alpha)(x - (\alpha + 1))}$

$x^2 + x + 1 \longrightarrow \alpha^2 + \alpha + 1 = 0 \quad (\text{mod } \alpha^2 + \alpha + 1)$

$\hookrightarrow$ kořen α a $\alpha + 1$ v $\mathbb{Z}_2[\alpha]/(\alpha^2 + \alpha + 1)$

$(x^2 + x + 1) : (x - \alpha) = x + (\alpha + 1)$

$\alpha x + x + 1$

$(\alpha + 1) \cdot x + 1$

$\alpha(\alpha + 1) + 1 =$

$= \alpha^2 + \alpha + 1 = 0$