obor integrity? $\mathbb{Z}_2 = \{0, 1\}$ ✓

$\mathbb{Z}_3 = \{0, 1, 2\}$ $1 \cdot 1 = 1$, $1 \cdot 2 = 2$ ✓

$2 \cdot 2 = 1$

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$ $2 \cdot 2 = 0$ NE

obecně

$\mathbb{Z}_k$ je obor integrity právě pro k prvočíselné matice:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$\mathbb{Z}_5$

$$1^{-1} = 1$$
$$2^{-1} = 3$$
$$3^{-1} = 2$$
$$4^{-1} = 4$$

$\mathbb{R}$

$\downarrow$

$\mathbb{C} = \mathbb{R} + i\mathbb{R} \qquad i^2 = -1$

$\mathbb{H} = \mathbb{C} + j\mathbb{C} \qquad j^2 = -1$

$$\mathbb{H} = \mathbb{R} + i\mathbb{R} + j\mathbb{R} + \underbrace{ij}_{\substack{\| \\ k}}\mathbb{R}$$

$$\boxed{ij = -ji}$$

$c \cdot 0$:

$$\underbrace{c \cdot a} = c \cdot (a + 0)$$

$$= \underbrace{c \cdot a} + \boxed{\begin{matrix} c \cdot 0 \\ \| \\ 0 \end{matrix}}$$

polynom $\quad a_0 + a_1 x + a_2 x^2 + \ldots$

$\mathbb{K}[x] \qquad f : \mathbb{K} \to \mathbb{K}$

$$f(x) = \sum_{i=0}^{k} a_i x^i \mapsto (x \mapsto f(x))$$

$$\mathbb{Z}_2 \qquad \underset{\substack{\neq \\ 0}}{x^2 + x} = f(x) \mapsto \left\{ \begin{array}{l} 0 \mapsto 0 \\ 1 \mapsto 0 \end{array} \right\}$$

$$|\mathbb{K}| < \infty, \quad \mathbb{K} = \{a_0, a_1, \dots, a_k\}$$

$$f(x) = (x - a_0) \cdot (x - a_1) \cdot \ldots \cdot (x - a_k)$$

$$= x^{k+1} + \dots$$

$$f \cdot g = a_k \cdot b_\ell \, x^{k+\ell} + \dots$$

$\deg k$ $\qquad \deg \ell$ $\qquad a_k \neq 0$, $b_\ell \neq 0$

$$\Downarrow \quad a_k \cdot b_\ell \neq 0$$

$$a \in \mathbb{K} \qquad e \in \mathbb{K} \qquad e \cdot e' = 1$$

$$a = e \cdot (e' \cdot a)$$

$$12 = 2 \cdot 2 \cdot 3 = (-2) \cdot 2 \cdot (-3)$$

$$x = \underbrace{\sqrt{x}}_{\parallel} \cdot \sqrt{x}$$

$$x^{1/2} \cdot x^{1/2}$$

1

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

$$\begin{array}{l}
x^3 + x^2 \\
\hline
0 \quad -x^2 + x + 1 \\
\quad -x^2 - x \\
\hline
\quad 0 \quad 2x + 1 \\
\quad\quad 2x + 2 \\
\hline
\quad\quad -1
\end{array}$$

$$\Rightarrow \underbrace{x^3 + x + 1}_{f} = \underbrace{(x^2 - x + 2)}_{q}\underbrace{(x + 1)}_{g} \underbrace{- 1}_{r}$$

$f(x)$ má kořen b $\quad \deg f > 0$

$$f(x) = q \cdot \underbrace{(x-b)}_{\deg = 1} + \underbrace{r}_{\deg = 0 \text{ nebo } r = 0}$$

$$f(b) = q \cdot 0 + \underbrace{r(\cancel{b}) = 0}$$ ✓

$\Rightarrow q(x)$ má $\deg q = \deg f - 1$

$f, g \in \mathbb{K}[x]$

$$f = q_1 g + r_1$$

$$g = q_2 r_1 + r_2$$

$$\vdots$$

$$r_{p-1} = q_{p+1} r_p + 0 \qquad r_p = h$$

dělení se zbytkem

$$h = r_p = r_{p-1} - q_{p+1} r_p$$

$$= r_{p-2} - q_p \left(r_{p-3} - q_{p-1} r_{p-2} \right)$$

$$\vdots$$

$$= A \cdot f + B g$$

$f(x) = x^4 + x^3 + x + 2$ nad $\mathbb{Z}_3$

$0, 1, 2 \longmapsto \neq 0$

nerozložitelné polynomy stupně 2 nad $\mathbb{Z}_3$:

$x^2 + 2x + 2$, $x^2 + x + 2$, $x^2 + 1$

$f(x) = (x^2 + x + 2) \cdot (x^2 + 1)$

$$\mathbb{N} = \{0, 1, 2, \ldots\}$$

$$\mathbb{Z} = \{(a-b),\ a, b \in \mathbb{N}\}/\sim$$

$$\mathbb{Q} = \left\{\frac{a}{b},\ a \in \mathbb{Z},\ b \in \mathbb{Z} - \{0\}\right\}/\sim$$

$$\frac{a}{b} = \frac{a'}{b'} \iff \underbrace{ab' = ba'}$$

podílové těleso pro obor integrit.

$$\left(\frac{a}{b}\right)^{-1} = \left(\frac{b}{a}\right)$$