$(\mathbb{Z}_5^\times, \cdot) = \langle [2] \rangle$

$=$

$\langle 2, 4, 3, 1 \rangle$

$(\mathbb{Z}_7^\times, \cdot) \neq \langle [2] \rangle$

$= \langle [3] \rangle$

$\langle 3, 3^2 = 2, 6, 4, 5, 1 \rangle$

$\mathbb{Z}[x]$

pokyvy $f = x$

$g = 2$

$\gcd(x, 2) = \pm 1$

$f(x) = x^2 - 2 \in \mathbb{Z}[x]$

je ireducibilní nad $\mathbb{Z}$ $\Leftarrow$

nemá kořeny v $\mathbb{Z}$

$\Rightarrow$ ireducibilní nad $\mathbb{Q}$

$\Rightarrow$ $x^2 - 2$ nemá kořeny v $\mathbb{Q}$

obdobně $x^2 - a$, kde $a \in \mathbb{Z}$

$a \neq \square$

$$a_n x^n + \dots + a_1 x + a_0 = 0$$

$\frac{r}{s} \in \mathbb{Q}$, $(r,s) = 1$

$$a_n \cdot \left(\frac{r}{s}\right)^n + \dots + a_1 \cdot \left(\frac{r}{s}\right) + a_0 = 0 \quad \Big| \; s^n$$

$$a_n \cdot r^n + a_{n-1} r^{n-1} \cdot s + \dots + a_1 r s^{n-1} + a_0 s^n = 0$$

$s \nmid$

$r \mid \nearrow \Rightarrow r \mid a_0 s^n \wedge (r,s) = 1$

$\Rightarrow r \mid a_0$

anal. $s \mid a_n$

POZOR!

nemá kořeny $\not\Rightarrow$ f je ireducibilní

$f = (x^2+1)^2$ nad $\mathbb{R}$

[kořeny v $\mathbb{C}$: $\pm i$ dvojnásobné

nad $\mathbb{C}$: $f = (x+i)(x-i)(x+i)(x-i)$

$= (x+i)^2(x-i)^2$

$$f = g \cdot h$$

$$= (b_m x^m + \dots + b_0) \cdot (c_k x^k + \dots + c_0)$$

$b_i, c_j \in \mathbb{Z}$

$$a_0 = b_0 \cdot c_0$$

$$a_1 = b_1 \cdot c_0 + b_0 \cdot c_1$$

$$a_2 = b_2 \cdot c_0 + b_1 \cdot c_1 + b_0 \cdot c_2$$

$$\vdots$$

$$a_{m+k} = b_m \cdot c_k$$

$p \mid a_0 = b_0 \cdot c_0 \overset{\text{Euklid}}{\Rightarrow} p \mid b_0 \wedge p \mid c_0$

$p \mid a_1 \wedge p \mid b_0 \Rightarrow p \mid b_1 \cdot c_0 \Rightarrow p \mid b_1$

$\vdots$

$p \mid b_m \Rightarrow p \mid a_{m+k}$ ↯

α kořen f násobnosti $k > 1 \iff$

$(x-\alpha)^2 \mid f \iff \exists g : (x-\alpha) \nmid g$

$f = g(x-\alpha)^k$

$f' = g' \cdot (x-\alpha)^k + g \cdot (x-\alpha)^{k-1} \cdot k$

$\Rightarrow (x-\alpha)^{k-1} \mid f' \wedge (x-\alpha)^k \nmid f'$

$\Rightarrow \alpha$ je kořen f' násobnosti $k-1$.

Př: sym. polynom

$f = x_1^2 + x_2^2$

$s_1 = x_1 + x_2$

$s_2 = x_1 \cdot x_2$

$f = s_1^2 - 2s_2$

$g = x_1^2 x_2 + x_1 x_2^2 + x_1^3 + x_2^3$

$g = x_1^2(x_1 + x_2) + x_2^2(x_1 + x_2) =$

$= (x_1^2 + x_2^2)(x_1 + x_2) = (s_1^2 - 2s_2)s_1 =$

$= \underline{s_1^3 - 2s_1 s_2}$

Viètovy (Newtonovy) vztahy

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$$

$$f(x) = (x - x_1)\cdot(x - x_2)\cdots(x - x_n)$$

$$a_{n-1} = -(x_1 + \dots + x_n) = -S_1$$

$$a_{n-2} = x_1x_2 + \dots + x_{n-1}x_n = S_2$$

$$\vdots$$

$$a_0 = (-1)^n \cdot x_1 \cdots x_n = (-1)^n \cdot S_n$$

Př: Určete f s kořeny x_1^2, x_2^2, kde x_1, x_2 jsou kořeny $x^2 + \underbrace{13}_{=S_1}x + \underbrace{7}_{S_2}$

$(e, \varphi(n)) = 1$

Bezout: $\exists k, l \in \mathbb{Z}$:

$k \cdot e + l \cdot \varphi(n) = 1 \quad / \bmod \varphi(n)$

$k \cdot e \equiv 1 \pmod{\varphi(n)}$

$k \cdot e = d$

$e \cdot d \equiv 1 \ (\varphi(n))$ $\quad (e, \varphi(n)) = 1$

$e \cdot d = 1 + k \cdot \varphi(n)$

$$(M^e)^d = M^{1+k\cdot\varphi(n)} = M \cdot \left(M^{\varphi(n)}\right)^k \equiv M \ (n)$$

$M^{\varphi(n)} \equiv 1 \ (n)$

$(M, n) = 1$

Eulerova věta