i) v grupě existuje prvek x řádu 4 $\Rightarrow$ grupa, je cyklická, je to grupa $\{x^4 = x^0 = e, x, x^2, x^3\}$ (a naopak)

Pro libovolnou jinou čtyřprvkovou grupu s generátorem y platí zobrazení: $e \mapsto e$, $x \mapsto y$, $x^2 \mapsto y^2$, $x^3 \mapsto y^3$

nadále izomorfismus grup.

ii) v grupě existují pouze prvky řádu 2 (kromě neutrálního prvku e). Označme je a, b, c. Potom musí

$ab = ba = c$ (kdyby $ab = e \Rightarrow a = b^{-1}$ ↯
$ab = a \Rightarrow b = e$ ↯
$ab = b \Rightarrow a = e$ ↯

Pro libovolnou jinou dvojprvkovou grupu s prvky a', b', c' nebo dva je přiřazení

$$f: \begin{array}{l} a' \mapsto a \\ b' \mapsto b \\ c' \mapsto c \\ e \mapsto e \end{array}$$

$$f(a' \cdot b') = f(c') = c$$
$$f(a') \cdot f(b') = a \cdot b = c$$

izomorfismem grup.

---

3) Zjistěme zbytek $23^{25^{25}}$ po dělení číslem 100.

Jsou je jednoznačně určen zbytky daného čísla po dělení čísly 4 a 25

$$23^{25^{25}} \equiv x \pmod{25} \qquad x \in \langle 0, 24 \rangle$$

$23^{20} \equiv 1 \pmod{25}$ $\left(\varphi(25) = 5^2 - 5 = 20\right.$

$\left. 23^{\varphi(25)} \equiv 1 \pmod{25}\right)$

Zjistěme nyní zbytek čísla 24^{25} po dělení číslem 20:

$$\left.\begin{aligned} 24^{25} &\equiv 0 \pmod 4 \\ 24^{25} &\equiv (-1)^{25} \equiv -1 \pmod 5 \end{aligned}\right\} \Rightarrow 24^{25} \equiv 4 \pmod{20}$$

$$23^{24^{25}} = 23^{20 \cdot k + 4} \equiv \left(23^{20}\right)^k \cdot 23^4 \equiv 1 \cdot 23^4 \equiv \quad k \in \mathbb{N}$$

$$\equiv 1 \cdot (-2)^4 = 16 \pmod{25}$$

Jestliže zjistíme zbytek čísla $23^{23^{25}}$ po dělení 4:

$$23^{23^{25}} \equiv (-1)^{24^{25}} = 1 \pmod 4$$

$23^{24^{25}} \equiv 41 \pmod{100}$,

Poslední dvě cifry čísla $23^{21^{25}}$ jsou 41.

G je podgrupa permutací na množině X.

Orbity akce G na X.

(Př. permutace $\langle (123)(45) \rangle$ na mn. $\{1,2,3,4,5\}$
má orbity $\{1,2,3\}$ a $\{4,5\}$)

Označme-li N počet orbit a pro lib. $g \in G$ označme S_g množinu všech prvků z X, které nechává g na místě ($g(x)=x$), pak platí

$$|N| = \frac{1}{|G|} \sum_{g \in G} |S_g|$$ (Burnsidovo lemma)

X ... množina všech obarvení krychle
barvami $(|X| = 3^6)$

G ... rotační symetrie krychle

$|G| = 24$

Určete mocnin $|S_g|$ pro jednotlivé typy rotací

i) identita $|S_g| = 3^6$

ii) rotace podle osy procházející středy protějších stěn

α) o $90°$ (resp. $-90°$) $|S_g| = 3^3$ (3.2)

β) o $180°$ $|S_g| = 3^4$ (3.1)

iii) rotace o $180°$ podle středů protějších hran

$|S_g| = 3^3$ (6 rotací)

iv) Rotace o 120° (resp. -120°) podle tělesové úhlopříčky

$|S_g| = 3^2$ (4×2 rotací)

$$|N| = \frac{1}{|G|} \sum_{g \in G} |S_g| = \frac{1}{24}\left(3^6 + 6\cdot 3^3 + 3\cdot 3^4 + 6\cdot 3^2 + 8\cdot 3\right)$$

i) ii)4 ii)3 iii) iv)

$$= 57$$

$\mathbb{R}[x]$ ... polynomy o jedné neznámé s reálnými koeficienty

obor integrity ... $c \cdot d = 0 \Rightarrow c = 0 \vee d = 0$

($\mathbb{Z}_6$ není obor integrity)

okruh $(R, +, \cdot)$

dělitelé nenulového prvku vzhledem k násobení se nazývají jednotky (= invertibilní prvky v okruhu)

Polynom má kořen $\alpha \Rightarrow$ není ireducibilní
(je dělitelný polynomem $x-\alpha$)

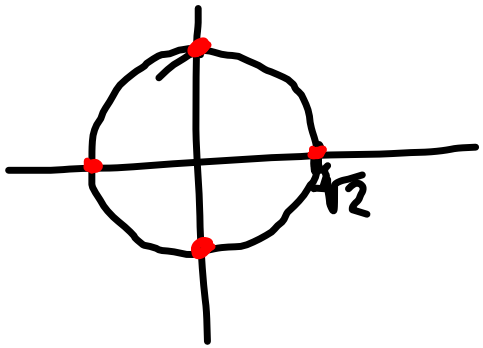
Polynom nemá kořeny $\Rightarrow$ může, ale nemusí být ireducibilní

V $\mathbb{C}[x]$ je libovolný polynom součinem lineárních polynomů.

V $\mathbb{R}[x]$ ... jsou ireducibilní polynomy jsou právě všechny lineární polynomy a kvadratické s nápornou diskriminací

1) jde o lo, nalož vždy kořeny daného polynomu

$x^4 = 2 \Rightarrow$



$\Rightarrow x_1 = \sqrt[4]{2}$

$x_2 = \sqrt[4]{2}\, i$

$x_3 = -\sqrt[4]{2}$

$x_4 = -\sqrt[4]{2}\, i$

$$(x^4 - 2) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}\, i)(x + \sqrt[4]{2}\, i)$$

2) $$(x^4 - 2) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + \sqrt{2})$$

3) Má kořeny? Nemá kořeny.

Tj.: buď je ired. nebo je součinem 2 polynomů stupně 2.

Nechť:

$x^5 - 2 = (x^2 + ax + b)(x^2 + cx + d)$ $\quad a, b, c, d \in \mathbb{Z}_5$

$x^0: \; bd = -2 \Rightarrow b^2 = -2 = 3$ ($\nexists$ (bez nuly) $b \in \mathbb{Z}_5$)

$x^1: \; ad + bc = 0 \Rightarrow ad - ab = 0 \Rightarrow a(d-b) = 0$

$\Rightarrow d = b$

$x^2: \; b + d + ac = 0$

$x^3: \; c + a = 0 \Rightarrow a = -c$

Polynom... je tedy nad $\mathbb{Z}_5$ ireducibilní.

1) ostatní kořeny

	1	0	-1	-4	-3	-2
2	1	2	3	2	1	0

$P(x)$ $x^5 - x^3 - 4x^2 - 3x - 2 = (x-2)(x^4 + 2x^3 + 3x^2 + 2x + 1)$

Hledáme dále kořeny polynomu

$x^4 + 2x^3 + 3x^2 + 2x + 1 = 0 \quad / \cdot \frac{1}{x^2}$

$x^2 + 2x + 3 + \frac{2}{x} + \frac{1}{x^2} = 0$ substituce $x + \frac{1}{x} = u$

$x^2 + \frac{1}{x^2} + 2 = u^2$

$u^2 - 2 + 2u + 3 = 0$

$u^2 + 2u + 1 = 0$

$(u+1)^2 = 0 \Rightarrow$

$u_{1,2} = -1$

$x + \frac{1}{x} = -1$

$x^2 + x + 1 = 0$

$x_{3,4} = \frac{-1 \pm \sqrt{3}\,i}{2}$

$$P(x) = (x-2)(x^2+x+1)^2$$