1) grupa rotačních symetrií krychle má 24 prvků, jsou to:

a) rotace o 90°, 180°, 270° okolo přímek procházejících středy protějších stěn

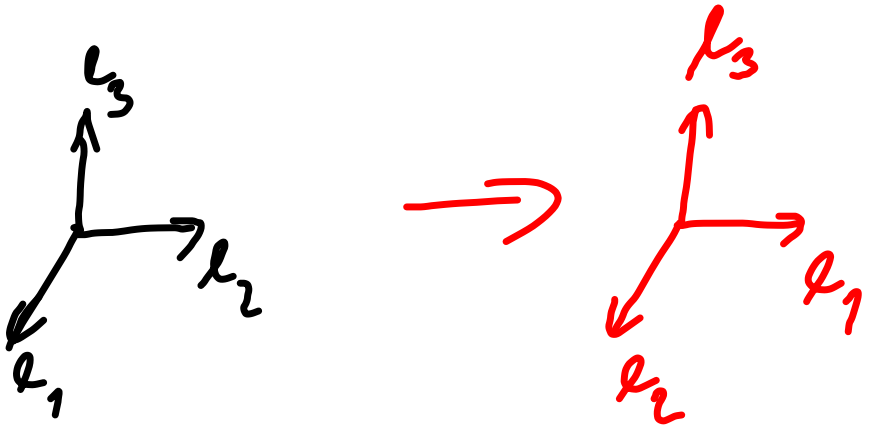
3×3

b) identita

c) rotace o 180° podle okolo přímek procházejících středy protějších hran.

6×1

d) rotace o 120° a 240° okolo tělesových úhlopříček (4×2)



Grupa všech symetrií krychle má 48 prvků.

$$\sigma = \overbrace{(195)}^{c_1}\overbrace{(26)}^{c_2}\overbrace{(3847)}^{c_3}$$

$c_1^3 = id$

$c_3^4 = id$

$c_2^2 = id$

$\sigma^{12} = id$

$2009 = 167 \cdot 12 + 5 \Rightarrow$

$$\sigma^{2009} = (\sigma^{12})^{167} \cdot \sigma^5 = id \cdot \sigma^5 = \sigma^5 =$$

$$\sigma^5 = (591)(26)(3847)$$

$$= c_1^5 \cdot c_2^5 \cdot c_3^5$$

$f : (M, \circ) \to (N, *)$

je homomorfismus grupoidů, jestliže

$$f(a \circ b) = f(a) * f(b)$$

$f : M \to N$ bijekce $\Rightarrow$ f izomorfismus

Musíme zadat obrazy všech (uspořádaných) dvojic ze trojprvkové množiny

~~3^2~~ 3^3

Tabulka operace na množině $\{a, b, c\}$.

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$x \circ y = x \circ z$
$\Downarrow$
$y = z$

Grupa je jediná.

(rozložních) symetrií

Symetrií rozložních tetraedru je 12

$\cong$ např. podgrupy v grupě A_4 (sudé permutace v S_4)

$A_4 = \{ id, (12)(34), (13)(24), (14)(23), (123), (213), (124), (214), (234), (324), (134), (314) \}$

Možný pořadí řádů podgrupy:

1, 2, 3, 4, 6, 12

$(12)(34)(12)(34) =$
$= (12)(12)(34)(34) = id$

1: $\{id\}$

2: musí být tvaru $\{id, a\}$, kde $a^2 = id$

jsou to $\{id, (12)(34)\}, \{id, (13)(24)\}, \{id, (14)(23)\}$

3: $\{id, (a\,b\,c)\}$, kde $\{a, b, c\} \subseteq \{1, 2, 3, 4\}$.

4: $\{id, (12)(34), (13)(24), (14)(23)\}$ ← jediná normální podgrupa v A_4.

6:

12: A_4

$H \subset G$

$g^{-1}Hg = H$

G/H

$g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$

$\varphi : \mathbb{N} \to \mathbb{N}$

$\varphi(1) = 1$

$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ pro m, n nesoudělná

$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$

$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \cdots \left(p_s^{\alpha_s} - p_s^{\alpha_s - 1}\right) =$

$= n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right)$

$(\mathbb{Z}_m, \cdot)$

---

u, v Bezoutovy koeficienty

$\gcd(a,b) = 1$:

$$au + bv = 1 \quad \Rightarrow$$

$$au \equiv 1 \pmod{b}$$

$\Leftrightarrow$ u je inverze k a v multiplikativní pologrupě $(\mathbb{Z}_b, \cdot)$

$(\mathbb{Z}_m^*, \cdot)$ ... grupa invertibilních prvků (vzhledem k násobení)

Bezoutovy koef. nalezneme pomocí Eukl. algoritmu:

$$(*) \quad 35 = 2\cdot 16 + 3$$

$$16 = 5\cdot 3 + 1 \quad \Rightarrow \quad 1 = 16 - 5\cdot 3 \overset{(*)}{=}$$

$$3 = 3\cdot 1 + 0 \qquad\qquad = 16 - 5\cdot(35 - 2\cdot 16) =$$

$$= 11\cdot 16 - 5\cdot 35$$

$$\Rightarrow 11 = 16^{-1} \text{ v } \mathbb{Z}_{35}$$

V $\mathbb{Z}_{11}$ to znamená, že

$$4^{10} \equiv 1 \pmod{11}$$

Uvažme uživatele $A, B, C, \ldots$

Každý uživatel zvolí dvě velká prvočísla p_A, q_A a spočítá $N_A = p_A \cdot q_A$, $\varphi(N_A) = (p_A - 1)(q_A - 1)$.

Zvolí e_A nesoudělné s $\varphi(N_A)$, dopočítá z něhož f_A tak, že $e_A \cdot f_A \equiv 1 \pmod{\varphi(N_A)}$.

Uživatel A zveřejní N_A a e_A.

Jestliže chce B něco poslat uživateli A, převede zprávu Z, $0 < Z < N_A$, spočítá

$$X \equiv Z^{e_A} \bmod N_A, \quad 0 < X < N_A$$

X je šifrovaná zpráva.

A dešifruje:

$$X^{f_A} \equiv \left(Z^{e_A}\right)^{f_A} = Z^{2\cdot\varphi(N_A)+1} \equiv Z \pmod{N_A}$$

$$\uparrow$$

$$\text{pro } (Z, N_A) = 1$$

Pokud by B chtěl podepsat zprávu z:

$$X \equiv \left(Z^{e_A}\right) \quad (N_A)$$

$$X^{f_B} \equiv Y \quad (N_B)$$

dešifrování

$$\left(X^{f_B}\right)^{e_B} = X \quad (N_B) \qquad X^{f_A} \equiv Z \; (N_A)$$

$$13243^{1751143} \pmod{5755893}$$

$$x^{11} \qquad 11 = 1011$$

$$x^{11} = \left((x^2)^2 \cdot x\right)^2 \cdot x$$