$$\boxed{x^3 + px + q = 0}$$

$$\begin{aligned} x_1 + x_2 + x_3 &= 0 \\ x_1x_2 + x_1x_3 + x_2x_3 &= p \\ x_1x_2x_3 &= -q \end{aligned}$$

$\sqrt[3]{1}:\quad 1 \qquad \varepsilon = \cos\frac{2\pi}{3} + \mathrm{i}\sin\frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}\,\mathrm{i} \qquad \varepsilon^2 = \cos\frac{4\pi}{3} + \mathrm{i}\sin\frac{4\pi}{3} = -\frac{1}{2} - \frac{\sqrt{3}}{2}\,\mathrm{i}$

$$t_1 = x_1 + \varepsilon\, x_2 + \varepsilon^2\, x_3 \qquad t_2 = x_1 + \varepsilon\, x_3 + \varepsilon^2\, x_2$$

t_1 tedy nezmění hodnotu při aplikaci permutací $(1,2,3)$ a $(1,2,3)^2$
t_1 nezmění hodnotu při aplikaci permutací z $\mathbb{A}_3 = [(1,2,3)]$
násobení t_1 číslem ε odpovídá aplikaci permutací z $\mathbb{A}_3$
zbylé permutace v $\mathbb{S}_3$ jsou $(2,3)\mathbb{A}_3$ aplikací permutace $(2,3)$ na t_1 vznikne t_2

$t_1 + t_2 + 0 = 3x_1$:	$\varepsilon^2\, t_1 + \varepsilon\, t_2 + 0 = 3x_2$:	$\varepsilon\, t_1 + \varepsilon^2\, t_2 + 0 = 3x_3$:
$t_1 = x_1 + \varepsilon\, x_2 + \varepsilon^2\, x_3$	$\varepsilon^2\, t_1 = \varepsilon^2\, x_1 + x_2 + \varepsilon\, x_3$	$\varepsilon\, t_1 = \varepsilon\, x_1 + \varepsilon^2\, x_2 + x_3$
$t_2 = x_1 + \varepsilon\, x_3 + \varepsilon^2\, x_2$	$\varepsilon\, t_2 = \varepsilon\, x_1 + \varepsilon^2\, x_3 + x_2$	$\varepsilon^2\, t_2 = \varepsilon^2\, x_1 + x_3 + \varepsilon\, x_2$
$0 = x_1 + x_2 + x_3$	$0 = x_1 + x_2 + x_3$	$0 = x_1 + x_2 + x_3$

$$t_1^3 + t_2^3 = \left(x_1 + \varepsilon\, x_2 + \varepsilon^2\, x_3\right)^3 + \left(x_1 + \varepsilon\, x_3 + \varepsilon^2\, x_2\right)^3$$

$$= 2\, x_3^3 - 3\, x_2\, x_3^2 - 3\, x_1\, x_3^2 - 3\, x_2^2\, x_3 + 12\, x_1\, x_2\, x_3 - 3\, x_1^2\, x_3 + 2\, x_2^3 - 3\, x_1\, x_2^2 - 3\, x_1^2\, x_2 + 2\, x_1^3$$

uvážíme-li, že

$$(x_1 + x_2 + x_3)^3 = x_3^3 + 3\, x_2\, x_3^2 + 3\, x_1\, x_3^2 + 3\, x_2^2\, x_3 + 6\, x_1\, x_2\, x_3 + 3\, x_1^2\, x_3 + x_2^3 + 3\, x_1\, x_2^2 + 3\, x_1^2\, x_2 + x_1^3$$

dostaneme: $\quad t_1^3 + t_2^3 = 2\,(x_1 + x_2 + x_3)^3 \; - \; 9\ \left(x_1x_2^2 + x_1^2x_2 \; + \; x_1x_3^2 + x_1^2x_3 \; + \; x_3x_2^2 + x_3^2x_2\right)$

$$= 2{\cdot}0^3 - 9\ \left(x_1x_2\,(x_1 + x_2 + x_3) - x_1x_2x_3 + x_1x_3\,(x_1 + x_2 + x_3) - x_1x_2x_3 + x_2x_3\,(x_1 + x_2 + x_3) - x_1x_2x_3\right)$$

$$= -\,9\ (-3\, x_1x_2x_3) = 27x_1x_2x_3 = -27q$$

$$\boxed{t_1^3 + t_2^3 = -27q}$$

$$(t_1^3 - t_2^3)^2 = \left(\left(x_1 + \varepsilon\, x_2 + \varepsilon^2\, x_3\right)^3 - \left(x_1 + \varepsilon\, x_3 + \varepsilon^2\, x_2\right)^3\right)^2$$

$$-27\, x_2^2\, x_3^4 + 54\, x_1\, x_2\, x_3^4 - 27\, x_1^2\, x_3^4 + 54\, x_2^3\, x_3^3 - 54\, x_1\, x_2^2\, x_3^3 - 54\, x_1^2\, x_2\, x_3^3 + 54\, x_1^3\, x_3^3 - 27\, x_2^4\, x_3^2 - 54\, x_1\, x_2^3\, x_3^2 + 162\, x_1^2\, x_2^2\, x_3^2$$
$$-54\, x_1^3\, x_2\, x_3^2 - 27\, x_1^4\, x_3^2 + 54\, x_1\, x_2^4\, x_3 - 54\, x_1^2\, x_2^3\, x_3 - 54\, x_1^3\, x_2^2\, x_3 + 54\, x_1^4\, x_2\, x_3 - 27\, x_1^2\, x_2^4 + 54\, x_1^3\, x_2^3 - 27\, x_1^4\, x_2^2$$

$$\boxed{(t_1^3 - t_2^3)^2 = (2 \cdot 27)^2 \cdot \left(\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3\right)}$$

$$(t_1^3 + t_2^3) \pm \sqrt{(t_1^3 - t_2^3)^2} = 2\, t_{1,2}^3 = -27q \pm 2 \cdot 27 \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$$

$$x_1 = \frac{t_1}{3} + \frac{t_2}{3} = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

Grupa

algebraická struktura s jednou binární operací, která je asociativní, existuje neutrální prvek a ke každému prvku také existuje prvek inverzní

Příklady:
$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$
všechny permutace tří prvků: $(\mathbb{S}_3, \cdot)$, podgrupou je $(\mathbb{A}_3, \cdot)$

Cyklická grupa řádu n

$$G = \{a^k,\ k = 0, 1, 2, \ldots, n\}$$

Příklad cyklické grupy řádu 4: $\{\mathrm{i}^n, n \in \mathbb{N}\} = \{\mathrm{i}, -1, -\mathrm{i}, 1\}$

Faktorizace grup

faktorizovat – rozložit (vlastně „něco ignorovat“) Například: $\mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5$
$5\mathbb{Z}$ — násobky 5, $\mathbb{Z}_5$ — zbytky po dělení 5