Př: Nechť $\mathbb{Q}(\sqrt{2}) = \{a+\sqrt{2}\,b \mid a,b \in \mathbb{Q}\}$. Potom $(\mathbb{Q}(\sqrt{2}),+)$ je grupa.

Nechť $\mathbb{Q}\times\mathbb{Q} = \{(a,b) \mid a,b \in \mathbb{Q}\}$ a sčítání na $\mathbb{Q}\times\mathbb{Q}$ definujeme předpisem

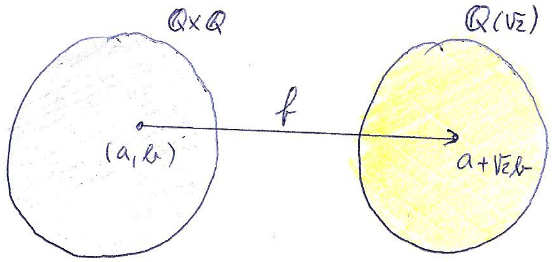
$$(a_1,b_1) + (a_2,b_2) = (a_1+a_2,\ b_1+b_2).$$

Potom $(\mathbb{Q}\times\mathbb{Q},+)$ je grupa. Dokažte, že $(\mathbb{Q}(\sqrt{2}),+) \approx (\mathbb{Q}\times\mathbb{Q},+)$.

Důkaz: Dokážeme, že $f: \mathbb{Q}\times\mathbb{Q} \to \mathbb{Q}(\sqrt{2})$ dané předpisem

$$f((a,b)) = a+\sqrt{2}\,b$$

je izomorfismus:



a) f je homomorfismus:

$$f((a_1,b_1)+(a_2,b_2)) = f((a_1+a_2,\ b_1+b_2)) = (a_1+a_2) + \sqrt{2}(b_1+b_2) = (a_1+\sqrt{2}b_1) + (a_2+\sqrt{2}b_2) = f((a_1,b_1)) + f((a_2,b_2))$$

2.) f je injektivní:

$$\underline{f((a_1,b_1)) = f((a_2,b_2))}$$
$$a_1+\sqrt{2}b_1 = a_2+\sqrt{2}b_2$$
$$a_1-a_2 = (b_2-b_1)\sqrt{2}$$

kdyby $b_1-b_2 \neq 0 \Rightarrow \underbrace{\frac{a_1-a_2}{b_2-b_1}}_{\in\mathbb{Q}} = \sqrt{2} \notin \mathbb{Q}$ spor! $\Rightarrow$

$\Rightarrow b_1-b_2=0$

$\Rightarrow a_1-a_2=0$

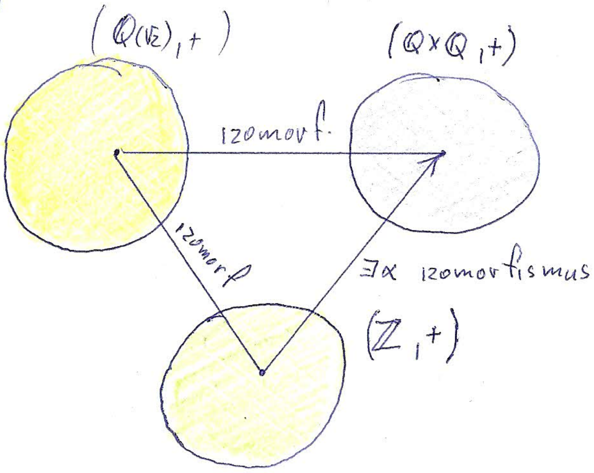
$\Rightarrow a_1=a_2 \wedge b_1=b_2 \quad \underline{\Rightarrow (a_1,b_1)=(a_2,b_2)}$

3.) f je surjektivní: $\forall\, a+\sqrt{2}b \in \mathbb{Q}(\sqrt{2})\ \exists\, (a,b)\in\mathbb{Q}\times\mathbb{Q} : f((a,b)) = a+\sqrt{2}b$

$\square$

Př: Dokažte, že grupa $(\mathbb{Q}(\sqrt{2}), +)$ není cyklická.

Důkaz: Dokázali jsme, že $(\mathbb{Q}(\sqrt{2}), +) \approx (\mathbb{Q}\times\mathbb{Q}, +)$. Předpokládejme (pro spor), že $(\mathbb{Q}(\sqrt{2}), +)$ je cyklická grupa. Protože $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$, je $(\mathbb{Q}(\sqrt{2}), +)$ nekonečná cyklická grupa a každá nekonečná cyklická grupa je izomorfní se $(\mathbb{Z}, +)$.



Tzn. $(\mathbb{Q}\times\mathbb{Q} \approx \mathbb{Q}(\sqrt{2}) \wedge \mathbb{Q}(\sqrt{2}) \approx \mathbb{Z}) \Rightarrow \mathbb{Q}\times\mathbb{Q} \approx \mathbb{Z}$

$\Rightarrow$ Existuje izomorfismus $\alpha: \mathbb{Z} \to \mathbb{Q}\times\mathbb{Q}$

$\Rightarrow$ Předpokládejme, že $\alpha(1) = (a_0, b_0) \in \mathbb{Q}\times\mathbb{Q}$

$$\alpha(2) = \alpha(1+1) = \alpha(1)+\alpha(1) = (a_0, b_0)+(a_0, b_0) = (2a_0, 2b_0)$$

$$\alpha(3) = \alpha(2+1) = \alpha(2)+\alpha(1) = (2a_0, 2b_0)+(a_0, b_0) = (3a_0, 3b_0)$$

$$\vdots$$

$$\alpha(k) = (ka_0, kb_0) \Rightarrow \alpha(-k) = (-ka_0, -kb_0)$$

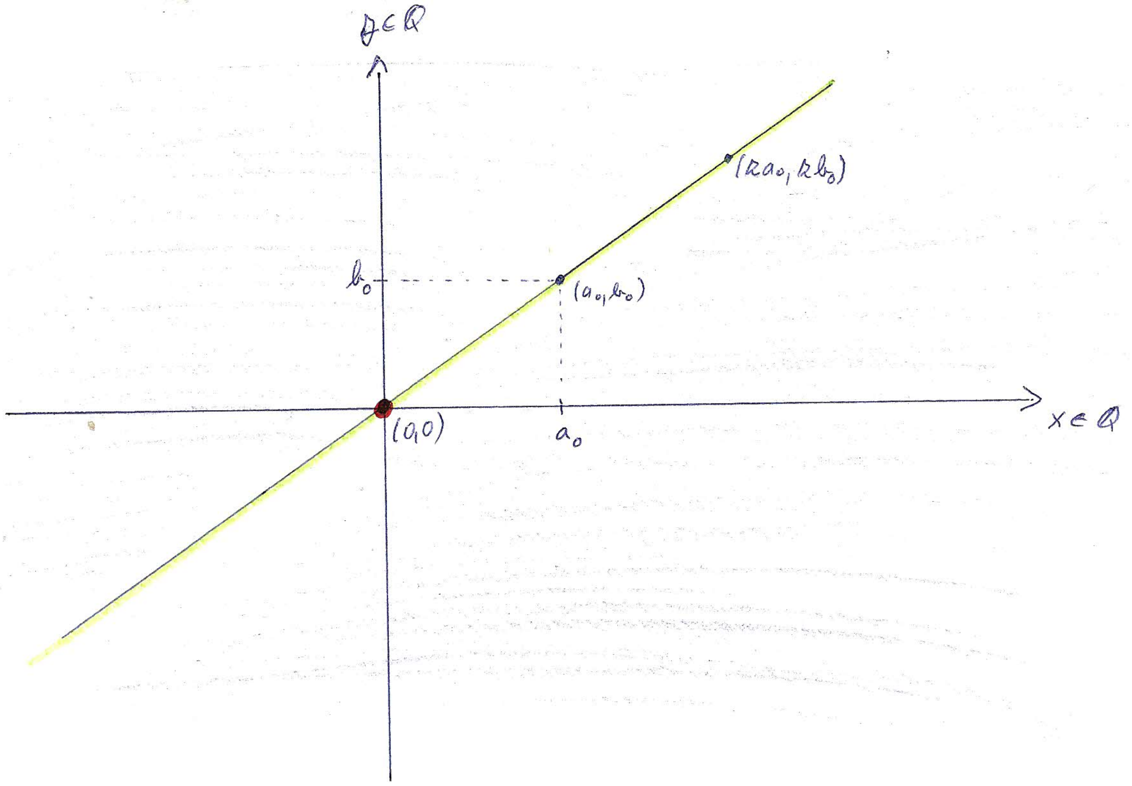
(inv. prvek se zobr. na inv. prvek)

$\Rightarrow \forall k \in \mathbb{Z}: \alpha(k) = (ka_0, kb_0)$

α je izomorfismus $\Rightarrow$ je surjektivní $\Rightarrow$

$$\mathbb{Q}\times\mathbb{Q} = \alpha(\mathbb{Z}) = \{(ka_0, kb_0) \mid k \in \mathbb{Z}\} = \{k(a_0, b_0) \mid k \in \mathbb{Z}\}$$

ale $\{k(a_0, b_0) \mid k \in \mathbb{Z}\} \neq \mathbb{Q}\times\mathbb{Q}$ spor!



$\boxed{(a_0, b_0) \neq (0,0)} \Rightarrow$

Body o souřadnicích (ka_0, kb_0) leží na přímce, nevyplňují celou rovinu $Q \times Q$.

$\boxed{(a_0, b_0) = (0,0)} \Rightarrow$

$(k \cdot a_0, kb_0) = (0,0) \Rightarrow$ Body o souřadnicích (ka_0, kb_0) splývají s počátkem $\Rightarrow$ nevyplňují celou rovinu $Q \times Q$.

Věta: Nechť a_1 je generátorem cyklické grupy $(G_1, \cdot)$ a a_2 je generátorem cyklické grupy $(G_2, \cdot)$ a $|G_1| = |G_2| = n \in \mathbb{N}$. Zobrazení $f : G_1 \to G_2$ definované předpisem

$$\forall k \in \mathbb{N} : f(a_1^k) = a_2^k$$

je izomorfismem grup $(G_1, \cdot)$ a $(G_2, \cdot)$.

Důkaz: a) f je izomorfismus:

$\forall a, b \in G \ \exists k_1, k_2 \in \{1, \dots, n\} : \quad a = a_1^{k_1} \quad$ a $\quad b = a_1^{k_2}$

Proto $f(a \cdot b) = f(a_1^{k_1} \cdot a_2^{k_2}) = f(a_1^{k_1+k_2}) = a_2^{k_1+k_2} = a_2^{k_1} \cdot a_2^{k_2} = f(a) \cdot f(b)$.

b) f je injektivní

Předpokládejme, že $a = a_1^{k_1}$ a $b = a_1^{k_2}$ (to můžeme, protože $G_1 = \langle a_1 \rangle$), kde $k_1, k_2 \in \{1, \dots, n\}$.

Dále předpokládejme, že
$$f(a) = f(b)$$
$$f(a_1^{k_1}) = f(a_2^{k_2})$$
$$a_2^{k_1} = a_2^{k_2}$$

Protože $k_1, k_2 \in \{1, \dots, n\}$ a $|a_2| = n$ je zřejmé, že $k_1 = k_2$.

Proto $a = b$.

c) f je surjektivní

$\forall \ b = a_2^k \in G_2 \quad \exists \ a = a_1^k \in G_1 : \quad f(a) = f(a_1^k) = a_2^k = b$.

$f: (\mathbb{Z}_{11} - \{0\}, \cdot) \rightarrow (\mathbb{Z}_{10}, +)$ izomorfismy.

$f_1(2) = 3$	$f_2(2) = 7$	$f_3(2) = 9$	$f_4(2) = 1$
$2 \rightarrow 3$	$2 \rightarrow 7$	$2 \rightarrow 9$	$2 \rightarrow 1$
$2^2 = 4 \rightarrow 6 = 2 \cdot 3$	$4 \rightarrow 4$	$4 \rightarrow 8$	$4 \rightarrow 2$
$2^3 = 8 \rightarrow 9 = 3 \cdot 3$	$8 \rightarrow 1$	$8 \rightarrow 7$	$8 \rightarrow 3$
$\vdots$ $5 \rightarrow 2$ $\vdots$	$5 \rightarrow 8$	$5 \rightarrow 6$	$5 \rightarrow 4$
$10 \rightarrow 5$	$10 \rightarrow 5$	$10 \rightarrow 5$	$10 \rightarrow 5$
$9 \rightarrow 8$	$9 \rightarrow 2$	$9 \rightarrow 4$	$9 \rightarrow 6$
$7 \rightarrow 1$	$7 \rightarrow 9$	$7 \rightarrow 3$	$7 \rightarrow 7$
$3 \rightarrow 4$	$3 \rightarrow 6$	$3 \rightarrow 2$	$3 \rightarrow 8$
$6 \rightarrow 7$	$6 \rightarrow 3$	$6 \rightarrow 1$	$6 \rightarrow 9$
$1 \rightarrow 0$	$1 \rightarrow 0$	$1 \rightarrow 0$	$1 \rightarrow 0$

f_1

mod 11

$\cdot$	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

mod 10

+	0	3	4	6	2	7	1	9	8	5
0	0	3	4	6	2	7	1	9	8	5
3	3	6	7	9	5	0	4	2	1	8
4	4	7	8	0	6	1	5	3	2	9
6	6	9	0	2	8	3	7	5	4	1
2	2	5	6	8	4	9	3	1	0	7
7	7	0	1	3	9	4	8	6	5	2
1	1	4	5	7	3	8	2	0	9	6
9	9	2	3	5	1	6	0	8	7	4
8	8	1	2	4	0	5	9	7	6	3
5	5	8	9	1	7	2	6	4	3	0