Def For a group $(G, *)$ a set $H \subseteq G$ is called a subgroup of G if the operation $*: G \times G \to G$ can be restricted to $H \times H \to H$ (that means: $a, b \in H \Rightarrow a * b \in H$), and $(H, *)$ is a group.

Proposition 13 For a finite group $(G, *)$ and an element $g \in G$ of order n, the set

$$\langle g \rangle := \{ g^0, g^1, \dots, g^{n-1} \}$$

is a subgroup of G.

Proof: the neutral element $e = g^0$ belongs to $\langle g \rangle$.

Every power g^i with $i \in \mathbb{N}_0$ belongs to $\langle g \rangle$, because

$$g^i = g^{i \bmod n} \in \langle g \rangle.$$ Apart from that

$$g^{-i} = (g^{-1})^i = (g^{n-1})^i = g^{(n-1) \cdot i} \in \langle g \rangle.$$ So,

we obtain $$\langle g \rangle = \{ g^i : i \in \mathbb{Z} \}$$

Once we know this, we know that:

$$(g^i, g^j) \longmapsto g^i * g^j = g^{i+j} \in \langle g \rangle, \text{ so that}$$

$$* : \langle g \rangle \times \langle g \rangle \longrightarrow \langle g \rangle \text{ is well defined.}$$

Associativity holds not only within $\langle g \rangle$, but also generally in the group G

We can also infer, remaining within $\langle g \rangle$:

$$(g^i)^{-1} = g^{-i} \in \langle g \rangle. \qquad \square$$

Def. For a finite group $(G, *)$ and $g \in G$ we call $\langle g \rangle$ the subgroup of G generated by g.

If $G = \langle g \rangle$ holds for some $g \in G$, then G is called cyclic and g is called a generator of G.

Theorem 14 For a prime number p, the group $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is a cyclic group.

We omit the proof of this interesting result.

Example

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$(\mathbb{Z}_4, +)$

$a = [0]_4$

$b = [1]_4$

$c = [2]_4$

$d = [3]_4$

$(\mathbb{Z}_5 \setminus \{0\}, \cdot)$

$a = [2]_5^0 = [1]_5$

$b = [2]_5$

$c = [2]_5^2 = [4]_5$

$d = [2]_5^3 = [3]_5$

Def For groups $(G, *)$ and $(H, \circ)$ a map $f: G \to H$ is called a group homomorphism if $f(a * b) = f(a) \circ f(b)$ for all $a, b \in G$.

If additionally, f is bijective, it is called a group isomorphism and the groups $(G, *)$ and $(H, \circ)$ are called isomorphic. Notation: $(G, *) \cong (H, \circ)$

Proposition 15 For a homomorphism $f: G \to H$ of groups $(G, *)$ and $(H, \circ)$ one has

$$f(e_G) = e_H$$

$$f(a^{-1}) = f(a)^{-1} \quad \text{for all } a \in G.$$

Proof: Exercise.

Example $(\mathbb{R}_{>0}, \cdot)$ the set of positive numbers with multiplication

$(\mathbb{R}, +)$ the set of real number with addition.

$(\mathbb{R}_{>0}, \cdot) \simeq (\mathbb{R}, +)$

$\log_2 : \mathbb{R}_{>0} \longrightarrow \mathbb{R}$ (logarithm) is an isomorphism

$\log_2(a \cdot b) = \log_2(a) + \log_2(b)$

$\log_2 1 = 0$

$\log_2 a^{-1} = -\log_2 a$

There is also the the inverse isomorphism

$\mathbb{R} \longrightarrow \mathbb{R}_{>0}$

$x \longmapsto 2^x$.

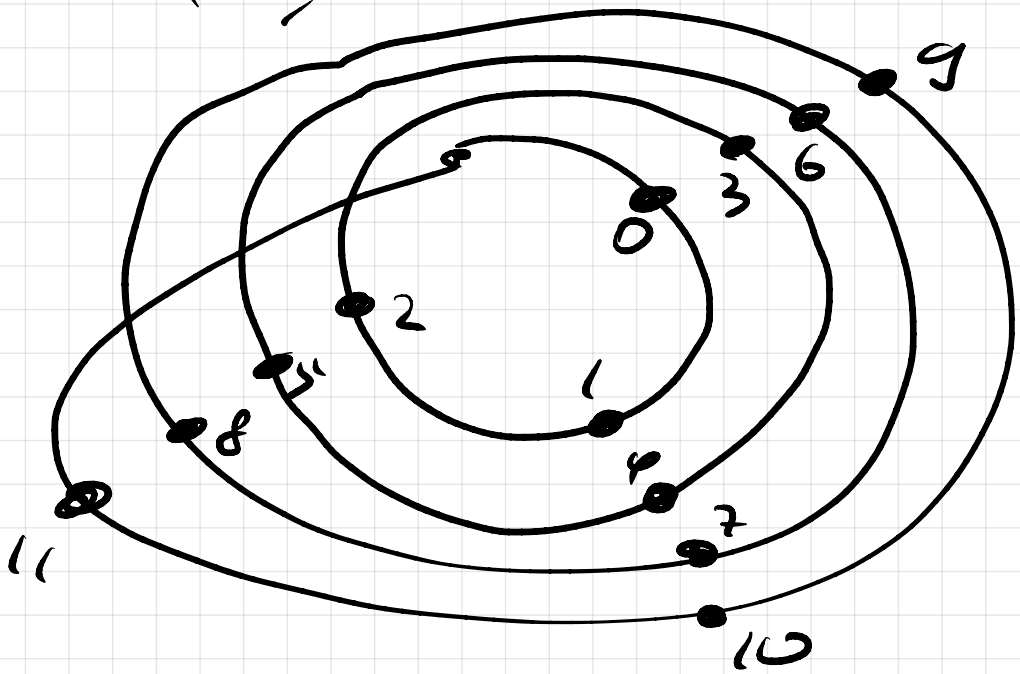
$\log_2 : \mathbb{R}_{>0} \to \mathbb{R}$

$\frac{1}{2} \cdot 32 = 16$

$2^{-1} \cdot 2^5 = 2^4$

$-1 + 5 = 4$

Example $f: \mathbb{Z}_{12} \longrightarrow \mathbb{Z}_3$ with $f([2]_{12}) = [2]_3$ is a group homomorphism of the groups $(\mathbb{Z}_{12}, +)$ and $(\mathbb{Z}_3, +)$.



$[0]_{12} \hookrightarrow [0]_3$
$[3]_{12} \hookrightarrow [0]_3$
$[6]_{12} \hookrightarrow [0]_3$
$[9]_{12} \hookrightarrow [0]_3$

Def. Let $(G_i, *_i)$ be groups $(i = 1, \dots, t)$

The direct product $(G_1 \times \dots \times G_t, *)$ of the groups $G_1, \dots, G_t$ is defined by

$$(g_1, g_2, \dots, g_t) * (h_1, h_2, \dots, h_t) := (g_1 *_1 h_1, g_2 *_2 h_2, \dots, g_t *_t h_t)$$

Informally: calculations in $G_1, \dots, G_t$ are done independently in parallel. If the groups are written additively $(G_i, +)$, then this is called a direct sum of groups and one uses the notation:

$$G_1 \oplus \dots \oplus G_t := G_1 \times \dots \times G_t \text{ and}$$

$$g_1 \oplus g_2 \oplus \dots \oplus g_t := (g_1, \dots, g_t).$$

Theorem 16 (Fundamental theorem of finite Abelian groups). Every finite Abelian group $(G, *)$ with more than one element is isomorphic to a direct sum of cyclic groups, whose sizes of powers of primes. This means, $(G, *)$ is isomorphic to $\mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_t}$ where

$q_i = p_i^{m_i}$, p_i is a prime number and $m_i \in \mathbb{N}$.

Furthermore, the numbers $q_1, \ldots, q_t$ are uniquely determined (up to ordering) by the group $(G, *)$.

Example

$$(\mathbb{Z}_{12}, +) \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_3$$

$4 = 2^2$

$3 = 3^1$

Example

$(\mathbb{Z}_{15}^{\times}, \cdot) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_4$, because:

$$\mathbb{Z}_{15}^{\times} = \{[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}\}$$

Chinese Remainder Theorem tells us that the ring $(\mathbb{Z}_{15}, +, \cdot)$ is isomorphic to $(\mathbb{Z}_3 \times \mathbb{Z}_5, +, \cdot)$ but

$$(\mathbb{Z}_3 \times \mathbb{Z}_5)^{\times} = \mathbb{Z}_3^{\times} \times \mathbb{Z}_5^{\times} = (\mathbb{Z}_3 \setminus \{0\}, \mathbb{Z}_5 \setminus \{0\})$$

$(\mathbb{Z}_3 \setminus \{0\}, \cdot) \simeq (\mathbb{Z}_2, +)$

$(\mathbb{Z}_5 \setminus \{0\}, \cdot) \simeq (\mathbb{Z}_4, +)$

By the Chinese Remainder Theorem we have the isomorphy of the rings $(\mathbb{Z}_{15}, +, \cdot)$ and $(\mathbb{Z}_3 \times \mathbb{Z}_5, +, -)$ via $[z]_{15} \longleftrightarrow ([z]_3, [z]_5)$

mod 3 \ mod 5	0	1	2	3	4
0	0	6	12	3	9
1	10	1	7	13	4
2	5	11	2	8	14

$[12]_{15} \longleftrightarrow ([0]_3, [2]_5)$ not invertible

$[7]_{15} \longleftrightarrow ([1]_3, [2]_5)$

$([1]_3, [2]_5)^{-1} =$

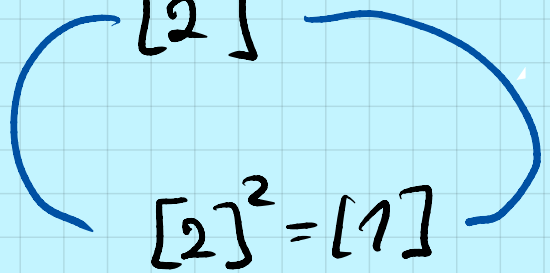
$([1]_3^{-1}, [2]_5^{-1}) =$

$[7]_{15}^{-1} = [13]_{15} \longleftrightarrow ([1]_3, [3]_5)$ invertible

$\mathbb{Z}_{15}^{\times}$ corresponds to those pairs of cosets $(x_1, x_2) \in \mathbb{Z}_3 \times \mathbb{Z}_5$ for which $x_1 \neq 0$ and $x_2 \neq 0$.

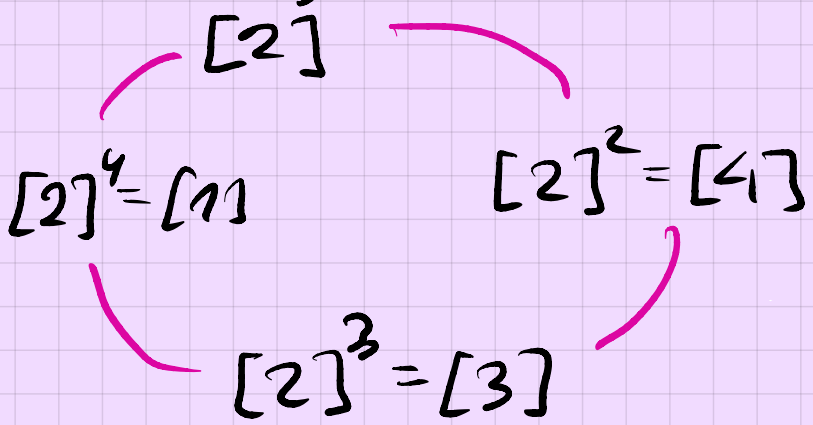
So, the group $(\mathbb{Z}_{15}^{\times}, \cdot)$ is isomorphic to the group $(\mathbb{Z}_3\setminus\{0\} \times \mathbb{Z}_5\setminus\{0\}, \cdot)$

In $\mathbb{Z}_3\setminus\{0\}$:



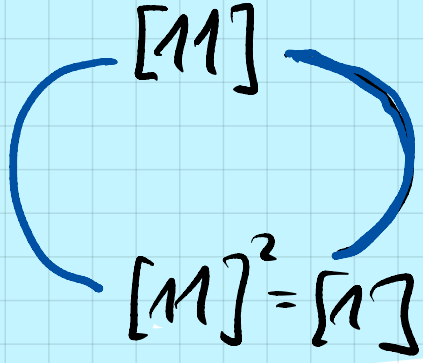
Cyclic of order 2.

In $\mathbb{Z}_5\setminus\{0\}$:



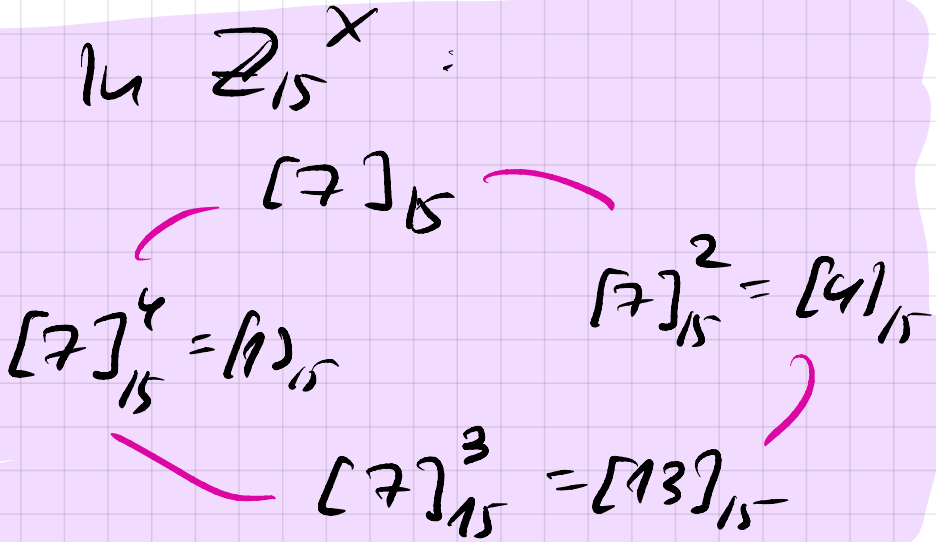
Cyclic of order 4

In $\mathbb{Z}_{15}^{\times}$:



Cyclic subgroup of order 2

In $\mathbb{Z}_{15}^{\times}$:



$[2]_5^1 = [2]_5$ $\quad$ $([1]_3, [2]_5)^1 = ([1]_3, [2]_5) \leftrightarrow [7]_{15}$

$[2]_5^2 = [4]_5$ $\quad$ $([1]_3, [2]_5)^2 = ([1]_3, [4]_5) \leftrightarrow [4]_{15}$

$[2]_5^3 = [3]_5$ $\quad$ $([1]_3, [2]_5)^3 = ([1]_3, [3]_5) \leftrightarrow [13]_{15}$

$[2]_5^4 = [1]$ $\quad$ $([1]_3, [2]_5)^4 = ([1]_3, [1]_5) \leftrightarrow [1]_{15}$

Let's have a conceptual description of our group

$(\mathbb{Z}_{15}^\times, \cdot)$ $\quad$ $g := [11]_{15}$ $\quad$ $h := [7]_{15}$

$$g^2 = 1$$
$$h^4 = 1$$
$$gh = hg$$

← That's the rules of the "game"

$g^3 = g^2 \cdot g = 1 \cdot g = g$

$[2]_{15} = gh$

1	h	h^3	h^2
g	gh	gh^3	gh^2

$$[2]_{15} \longleftrightarrow ([2]_3, [2]_5) = \underbrace{([2]_3, [1]_5)}_{\updownarrow} \cdot \underbrace{([1]_3, [2]_5)}_{\updownarrow}$$

$$\updownarrow \qquad\qquad \updownarrow$$

$$[11]_{15} \qquad [7]_{15}$$

$$[2]_{15}^{101} = (gh)^{101} = g^{101} \cdot h^{101} = g \cdot h$$

More generally: $g^i h^j = g^{i \bmod 2} \; h^{j \bmod 4}$

This means that

$$g^i h^j \longleftrightarrow ([i]_2, [j]_4)$$

$$\Rightarrow (\mathbb{Z}_{15}^{\times}, \cdot) \simeq (\mathbb{Z}_2 \oplus \mathbb{Z}_4, +)$$

$$g^3 h^2 \cdot g^8 \cdot h^3 = g^{3+8} \; h^{2+3} = g^1 \cdot h^1$$

$3+8 \equiv 1 \pmod 2$

$2+3 \equiv 1 \pmod 4$

Example

$$(\mathbb{Z}_{30}, +) \simeq (\mathbb{Z}_6 \oplus \mathbb{Z}_5, +) \text{ by Chinese Rem. Theorem}$$

$$(\mathbb{Z}_6, +) \simeq (\mathbb{Z}_2 \oplus \mathbb{Z}_3, +) \text{ by}$$

$$\Rightarrow (\mathbb{Z}_{30}, +) = (\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5, +)$$

Example

$$(\mathbb{Z}_{30}^{\times}, \cdot) \overset{?}{\simeq} (\mathbb{Z}_2 \oplus \mathbb{Z}_4, +)$$

Why?

ElGamal encryption system

Alice chooses an element g of a very-big-prime order n in a group $(G, \cdot)$. She chooses a random number $k \in \{2, \ldots, n-2\}$ as a private key and publishes the triple

(n, g, g^k) as a public key.

To send a message $x \in G$ to Alice,

Bob generates a random number

$t \in \{2, \ldots, n-2\}$ and sends the pair

$y = (y_1, y_2)$ with $y_1 = g^t$ and

$y_2 = x \cdot (g^k)^t = x \cdot g^{kt}$ as

a cipher text to Alice.

To decipher y to the plain text

x, Alice calculates

$$y_2 \cdot y_1^{-k} = x \cdot g^{kt} \cdot (g^t)^{-k} = x.$$

In order to Break the cryptosystem, Eve needs to get k from (q, g, g^k) This is known as the discrete logarithm problem (DLP); if this is hard to solve in $(G, \cdot)$, the cryptosystem is safe.

In order to Break the ciphertext Eve needs to solve the system

$$\begin{cases} g^t = y_1 \\ x \cdot g^{kt} = y_2 \end{cases}$$

in the unknowns x and t

If one get t from $g^t = y_1$, then one

can calculate $y_2 \cdot (g^k)^{-t}$

$= x \cdot g^{kt} \cdot (g^k)^{-t} = x$

But for solving $g^t = y_1$ in t, one needs to solve the DLP.