**The Bright Side of Mathematics**

The following pages cover the whole Algebra course of the Bright Side of Mathematics. Please note that the creator lives from generous supporters and would be very happy about a donation. See more here: https://tbsom.de/support

Have fun learning mathematics!

# Algebra – Part 1

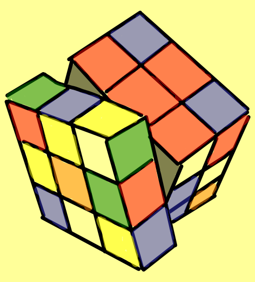
Start Learning Mathematics

Real Analysis

Linear Algebra

Algebra

- groups
- rings
- fields



group: $(\mathbb{Z}, +)$

ring: $(\mathbb{Z}, +, \cdot)$

field: $(\mathbb{R}, +, \cdot)$

Galois theory

$$x^5 - 4x + 2 = 0$$

at most 5 solutions

solutions cannot be expressed with combinations of roots

# Algebra – Part 2

**Definition:** Let $A$ be a set.

A map $F: A \times A \longrightarrow A$ is called a binary operation on $A$.

Instead of $F((a,b))$, we write $a \circ b$ or $a * b$ or $a F b$

or $a \cdot b$ or $ab$ or $a + b$ ...

juxtaposition

**Closure Law:** $a \circ b \in A$ for all $a, b \in A$

**Example:** $A = \{1,2,3\}$ , $\circ: A \times A \longrightarrow A$ binary operation defined by:

operation table:

| $\circ$ | 1 | 2 | 3 |
|---|---|---|---|
| 1 | 3 | 1 | 2 |
| 2 | 3 | 3 | 1 |
| 3 | 2 | 2 | 2 |

$1 \circ 2 = 1$
$2 \circ 1 = 3$ not equal!

$(1 \circ 2) \circ 3 = 1 \circ 3 = 2$
$1 \circ (2 \circ 3) = 1 \circ 1 = 3$ not equal!

**Definition:** A pair $(S, \circ)$ where $S$ is a set and $\circ$ is a binary operation on $S$ is called a semigroup if

$$a \circ (b \circ c) = (a \circ b) \circ c \quad \text{for all } a,b,c \in S \qquad \text{(associative)}$$

$$=: a \circ b \circ c$$

**Example:** Set of functions $\mathcal{F}(\mathbb{R}) = \{ f \mid f: \mathbb{R} \to \mathbb{R} \text{ function} \}$

together with composition $\circ: \mathcal{F}(\mathbb{R}) \times \mathcal{F}(\mathbb{R}) \longrightarrow \mathcal{F}(\mathbb{R})$ :

Take $f_1, f_2, f_3 \in \mathcal{F}(\mathbb{R})$ and define $g = f_1 \circ (f_2 \circ f_3) : \mathbb{R} \to \mathbb{R}$

$h = (f_1 \circ f_2) \circ f_3 : \mathbb{R} \to \mathbb{R}$

$$g(x) = f_1 \circ (f_2 \circ f_3)(x) = f_1((f_2 \circ f_3)(x)) = f_1(f_2(f_3(x)))$$

$$h(x) = ((f_1 \circ f_2) \circ f_3)(x) = (f_1 \circ f_2)(f_3(x)) = f_1(f_2(f_3(x)))$$

$\Longrightarrow$ $(\mathcal{F}(\mathbb{R}), \circ)$ semigroup

# Algebra – Part 3

$(S, \circ)$ semigroup $\rightsquigarrow$ $e \in S$ with $e \circ a = a = a \circ e$

**Definition:** An element $e \in S$ is called

- left neutral (=a left identity) $e \circ a = a$ for all $a \in S$
- right neutral (=a right identity) $a \circ e = a$ for all $a \in S$
- neutral (=an identity) $e \circ a = a = a \circ e$ for all $a \in S$

**Example:** $S = \left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \;\middle|\; x, y \in \mathbb{R} \right\}$ with $\circ$ given by the matrix multiplication

$\hookrightarrow$ $(S, \circ)$ semigroup

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ left neutral}$$

$$\begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ not right neutral}$$

**Fact:** Let $e \in S$ be left neutral and $\tilde{e} \in S$ be right neutral.

$$\left.\begin{array}{l} e \circ a = a \overset{\text{for } a = \tilde{e}}{\Longrightarrow} e \circ \tilde{e} = \tilde{e} \\ \qquad\qquad\qquad\qquad \parallel \\ b \circ \tilde{e} = b \overset{\text{for } b = e}{\Longrightarrow} e \circ \tilde{e} = e \end{array}\right\} \Rightarrow e = \tilde{e}$$

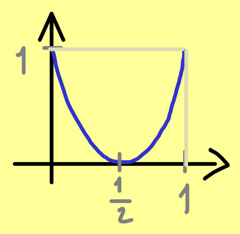
**Definition:** $(S, \circ)$ semigroup with identity $e$ (the neutral element), $a, b, c \in S$.

- $x \in S$ is called a left inverse of $a$ if $x \circ a = e$ (left invertible)
- $y \in S$ is called a right inverse of $b$ if $b \circ y = e$ (right invertible)
- $z \in S$ is called an inverse of $c$ $\quad z \circ c = e = c \circ z$ (invertible)

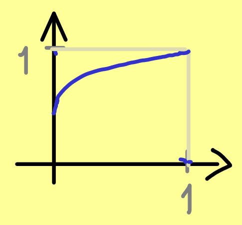
**Example:** Functions $f : [0,1] \to [0,1]$, $(\mathcal{F}([0,1]), \circ)$ semigroup

Neutral element: $\mathrm{id} : [0,1] \to [0,1]$, $x \mapsto x$

Right invertible: $\tilde{f} : [0,1] \to [0,1]$, $x \mapsto 4(x - \frac{1}{2})^2$




Right inverse of $\tilde{f}$: $g : [0,1] \to [0,1]$, $x \mapsto \frac{1}{2}\sqrt{x} + \frac{1}{2}$




$\hookrightarrow$ $\tilde{f} \circ g = \mathrm{id}$

$g \circ \tilde{f} \neq \mathrm{id}$

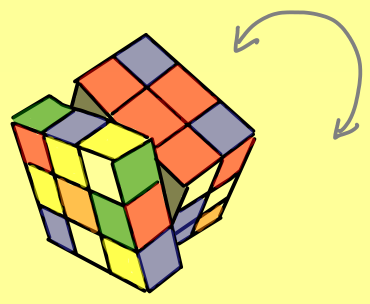
Remember:

surjective $\Leftrightarrow$ right invertible

injective $\Leftrightarrow$ left invertible

# Algebra – Part 4

$(S, \circ)$ semigroup $\rightsquigarrow$ + neutral element, inverses $\rightsquigarrow$ group



**Definition:** A pair $(G, \circ)$ is called a group if:

(a) $(G, \circ)$ semigroup.

(b) There is a left identity $e \in G$.

(c) Each $a \in G$ is left invertible, i.e. there exists $b \in G$ with $b \circ a = e$.

**This implies:** A set $G$ together with a binary operation $\circ$ is a group if:

(G1) $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in G$ (associative)

(G2) There is a unique identity $e \in G$: $e \circ a = a = a \circ e$ for all $a \in G$

(G3) Each $a \in G$ is invertible: $\exists\, b \in G$: $b \circ a = e = a \circ b$

$a^{-1} := b$ (common notation)

**Proof:** (a) $\Rightarrow$ (G1) ✓

Let $a \in G$.

> (b) There is a left identity $e \in G$.
>
> (c) Each $a \in G$ is left invertible, i.e. there exists $b \in G$ with $b \circ a = e$. (*)

Choose $b \in G$ with $ba = e$. Then $ab \overset{(b)}{=} a(eb) \overset{(*)}{=} a(ba)b = (ab)(ab)$. (**)

Choose $c \in G$ with $c(ab) = e$ (by (c))

$\Rightarrow$ $ab \overset{(b)}{=} e(ab) = c(ab)(ab) \overset{(**)}{=} c(ab) = e$ $\Rightarrow$ (G3) ✓

$\Rightarrow$ $ae \overset{(*)}{=} a(ba) = (ab)a = ea = a$ $\Rightarrow$ (G2) ✓

# Algebra - Part 5

**Group:** $G$ together with binary operation $\circ$ and:

(G1) associativity $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in G$

(G2) unique identity $e \in G$: $e \circ a = a = a \circ e$ for all $a \in G$

(G3) all inverses exist: $\forall a \in G \; \exists b \in G$: $b \circ a = e = a \circ b$

$a^{-1} := b$ (common notation)

**Uniqueness of inverses:**

$(S, \circ)$ semigroup with identity $e \in S$.

If $a \in S$ is a left invertible with $x$ $(x \circ a = e)$ and right invertible with $y$, $(a \circ y = e)$

then $x = y$.

**Proof:** $x = x \circ e = x \circ (a \circ y) = (x \circ a) \circ y = e \circ y = y$ $\square$

**Examples:** (a) $G = \{e\}$ with $e \circ e = e$ , $e^{-1} = e$

(b) $G = \{e, a\}$

| $\circ$ | $e$ | $a$ |
|---|---|---|
| $e$ | $e$ | $a$ |
| $a$ | $a$ | $e$ |

$a^{-1} = a$

(c) $(\mathbb{Z}, +)$ with identity $0$ and inverses $3 + (-3) = 0$

$(\mathbb{Q} \setminus \{0\}, \cdot)$ with identity $1$ and inverses $\frac{1}{4} \cdot \left(\frac{1}{4}\right)^{-1} = 1$

$(\mathbb{C}^{n \times n}, +)$ with identity $\begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$

$(\{A \in \mathbb{C}^{n \times n} \mid \det(A) \neq 0\}, \cdot)$ with identity $\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$

**General example:** Let $(S, \circ)$ be a semigroup with identity $e \in S$.

$$S^* := \{a \in S \mid a \text{ is invertible}\}$$

$a^{-1}$ exists

Then $(S^*, \circ)$ is a group.

**Proof:** (1) $e \circ e = e \Rightarrow e \in S^*$ with $e^{-1} = e \Rightarrow$ (G2) ✓

(2) $a \in S^* \Rightarrow$ $\begin{matrix} a^{-1} \circ a = e \\ a \circ a^{-1} = e \end{matrix}$ $\Rightarrow a^{-1} \in S^* \Rightarrow$ (G3) ✓

(3) $a, b \in S^* \Rightarrow (b^{-1} \circ a^{-1}) \circ (a \circ b) \overset{\text{associativity in } S}{=} b^{-1} \circ \underbrace{(a^{-1} \circ a)}_{e} \circ b = e$

$(a \circ b) \circ (b^{-1} \circ a^{-1}) \overset{\text{associativity in } S}{=} a \circ (b \circ b^{-1}) \circ a^{-1} = e$

$\Rightarrow (S^*, \circ)$ is a well-defined semigroup $\square$

BECOME A MEMBER

ON STEADY

The Bright Side of Mathematics

# Algebra - Part 6

$(S, \circ)$ semigroup. Let's write: $ab := a \circ b$

neutral element + all inverses

group

**Fact:** Let $(G, \circ)$ be a group and $a, b, x, y \in G$. Then:

$ax = ay \;\Rightarrow\; x = y$ (left cancellation property)

$xb = yb \;\Rightarrow\; x = y$ (right cancellation property)

**Proof:** $x = xe = x(bb^{-1}) = (xb)b^{-1} = (yb)b^{-1} = y(bb^{-1}) = y$

neutral element

**Definition:** $(S, \circ)$ semigroup (or group).

The order of $S$ is the number of elements in $S$:

$$\mathrm{ord}(S) := \begin{cases} |S| = \# S & \text{if } S \text{ is finite} \\ \infty & \text{if } S \text{ is not finite} \end{cases}$$

**Lemma:** Let $(S, \circ)$ be a semigroup. Then:

$(S, \circ)$ is group $\iff$ $\forall a, b \in S \;\exists x, y \in S : \; ax = b, \; ya = b$

**Proof:** $(\Rightarrow)$ Assume $(S, \circ)$ is a group. For given $a, b \in S$, set:

$x = a^{-1}b \quad , \quad y = ba^{-1}$

$(\Leftarrow)$ For given $a \in S$, there are $x, y \in S$ with $ax = a$, $ya = a$.

Let's call $e := y$ : $ea = a$

Let's take $b \in S$. Then there is $\tilde{x} \in S$ with $a\tilde{x} = b$.

We get: $eb = e(a\tilde{x}) = (ea)\tilde{x} = a\tilde{x} = b \;\Rightarrow\; e$ left neutral

For given $b \in S$ there is $\tilde{y} \in S$ such that: $\tilde{y}b = e \;\Rightarrow\; b$ left invertible

$\overset{\text{part 4}}{\Rightarrow}$ $(S, \circ)$ is a group $\square$

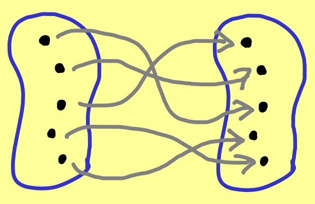
**Proposition:** Let $(S, \circ)$ be a semigroup with $\mathrm{ord}(S) < \infty$. Then:

$(S, \circ)$ is group $\iff$ both cancellation properties hold

$\begin{pmatrix} ax = ay \;\Rightarrow\; x = y \\ xb = yb \;\Rightarrow\; x = y \end{pmatrix}$

**Proof:** For any map $f : S \to S$:

$f$ is injective $\iff$ $f$ is surjective



For given $a \in S$, define $f_a : S \to S$ and $g_a : S \to S$ by

$f_a(x) = ax \quad , \quad g_a(x) = xa$.

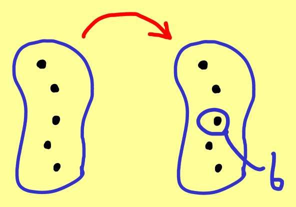
Then we have: both cancellation properties hold

$\iff \forall a \in S : \; f_a(x) = f_a(y) \;\Rightarrow\; x = y$

$\qquad\qquad\quad\; g_a(x) = g_a(y) \;\Rightarrow\; x = y$

$\iff \forall a \in S :$ $f_a$ and $g_a$ are injective

$\iff \forall a \in S :$ $f_a$ and $g_a$ are surjective



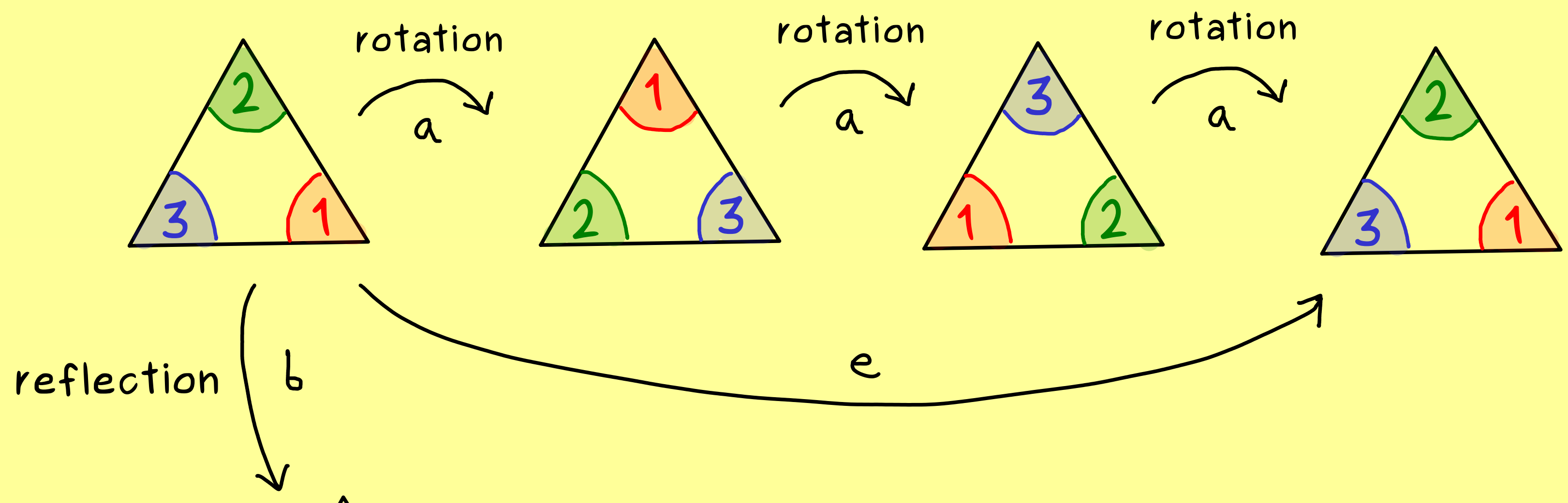
$\iff \forall a \in S :$ for every $b \in S$ there are

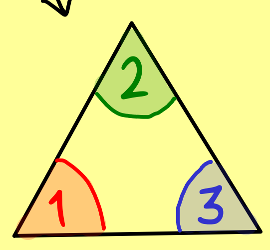
$x, y \in S : \; \underset{ax}{\underset{\parallel}{f_a(x)}} = b$ and $\underset{ya}{\underset{\parallel}{g_a(y)}} = b$

$\overset{\text{Lemma}}{\iff}$ $(S, \circ)$ is group $\square$

# Algebra - Part 7

Group:



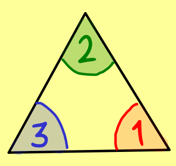



$\rightsquigarrow$ $b^2 = e \quad \Rightarrow \quad b^{-1} = b$

$a^3 = e \quad \Rightarrow \quad a^{-1} = a^2$

$ab \overset{?}{=} ba$

symmetry operations $\leftrightarrow$ permutations of $\{1,2,3\} =: X$



$S_3 := \{ f : X \to X \mid f \text{ bijective} \}$

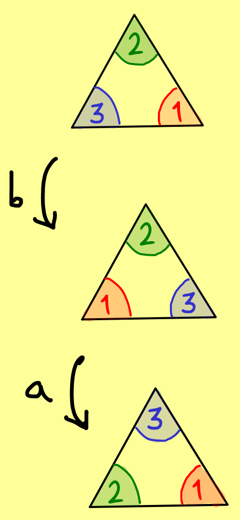
$\hookrightarrow$ symmetric group

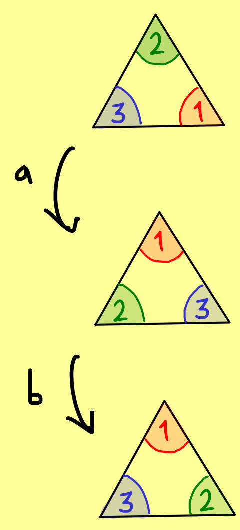
Example:

$f_b(1) = 3$, $f_b(2) = 2$, $f_b(3) = 1$

$f_a(1) = 2$, $f_a(2) = 3$, $f_a(3) = 1$

$\Rightarrow (S_3, \circ)$ composition of maps





We get: $(f_a \circ f_b)(1) = 1$ , $(f_b \circ f_a)(1) = 2$

$(f_a \circ f_b)(2) = 3$ , $(f_b \circ f_a)(2) = 1$

$(f_a \circ f_b)(3) = 2$ , $(f_b \circ f_a)(3) = 3$

$\Rightarrow$ not commutative!

Definition: A group $(G, \circ)$ (or semigroup) is called abelian or commutative if $a \circ b = b \circ a$ for all $a, b \in G$.

Examples: $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$ , $(\mathbb{R}, +)$ , $(\mathbb{C} \setminus \{0\}, \cdot)$ are abelian.

General example: $G = \{a, b, e\}$

group with three elements

| $\circ$ | a | b | e |
|---|---|---|---|
| a | $a^2$ | $\square$ | a |
| b | $\square$ | $b^2$ | b |
| e | a | b | e |

1st case: $a^{-1} = b$ , $b^{-1} = a$ $\Rightarrow$ $a \circ b = e$, $b \circ a = e$ $\rightsquigarrow$ abelian group

2nd case: $a^{-1} = a$ , $b^{-1} = b$ $\Rightarrow$ $(b \circ a) \circ (a \circ b) = b \circ \underbrace{a^2}_{=e} \circ b = e$

$\Rightarrow \underbrace{(a \circ b)^{-1}}_{= a \circ b} = (b \circ a)$ $\rightsquigarrow$ abelian group

Non-abelian group: Symmetric group $S_3$ : $|S_3| = 3! = 6$

Dihedral group $D_3$ (with $S_3 = D_3$) — order 6

# Algebra - Part 8

**modulus calculation:**

$$13 - \underset{\text{modulus } = m}{12} = 1$$

$$24 - 2 \cdot 12 = 0$$

$x \sim_m y \iff$ There is $q \in \mathbb{Z}$: $x - y = q \cdot m$

$x \equiv y \pmod{m}$

**Integers modulo m:** $\mathbb{Z}_m$ , $\mathbb{Z}/m\mathbb{Z}$ , $\mathbb{Z}/m$ , $\mathbb{Z}/\sim_m$

$$\mathbb{Z}_m := \{[0], [1], \ldots, [m-1]\}, \qquad m \in \mathbb{N}$$

for example with $m = 12$ : $[2] = \{2, 14, 26, 38, \ldots, -10, -22, \ldots\}$

**define addition:** $[k] + [\ell] := [k + \ell]$ well-defined

$[k] + [-k] = [0]$ identity

inverse

$\Rightarrow$ $(\mathbb{Z}_m, +)$ abelian group of order $m$

**Example:** $(\mathbb{Z}_2, +)$ : $[0] = \{0, 2, 4, \ldots, -2, -4, \ldots\}$

$[1] = \{1, 3, 5, 7, \ldots, -1, -3, \ldots\}$

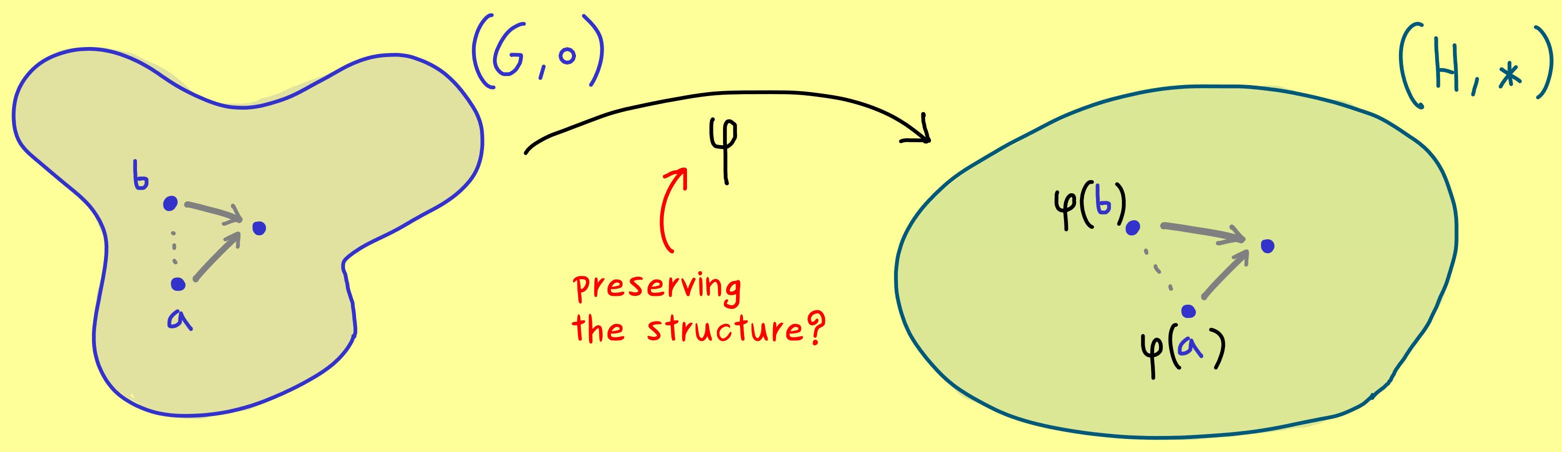
| + | [0] | [1] |
|---|---|---|
| [0] | [0] | [1] |
| [1] | [1] | [0] |

$(\mathbb{Z}_6, +)$ : $[0] = \{0, 6, 12, \ldots, -6, -12, \ldots\}$

$[1], [2], [3], [4], [5]$

| + | [0] | [1] | [2] | [3] | [4] | [5] |
|---|---|---|---|---|---|---|
| [0] | [0] | [1] | [2] | [3] | [4] | [5] |
| [1] | [1] | [2] | | | | |
| [2] | [2] | [3] | [4] | | | |
| [3] | [3] | [4] | [5] | [0] | | |
| [4] | [4] | [5] | [0] | [1] | [2] | |
| [5] | [5] | [0] | [1] | [2] | [3] | [4] |

# Algebra - Part 9




∘ binary operation
and identity and all inverses

∗ binary operation
and identity and all inverses

**Definition:** $(G,\circ), (H,*)$ groups. A map $\varphi: G \to H$ is called a group homomorphism if $\varphi(a \circ b) = \varphi(a) * \varphi(b)$ for all $a, b \in G$.

**Example:** $(G,\circ) = (\mathbb{R}, +)$, $(H, *) = (\mathbb{R}\setminus\{0\}, \cdot)$.

$$\varphi: G \to H, \quad x \mapsto e^x \quad \Longrightarrow \quad \begin{array}{l} \varphi(x+y) = e^{x+y} \\ \varphi(x)\cdot\varphi(y) = e^x \cdot e^y \end{array} \Big)\!\Big)$$

**Properties:** A group homomorphism satisfies:

(1) $\varphi(e_G) = e_H$ (identity is sent to identity)

(2) $\varphi(a^{-1}) = \varphi(a)^{-1}$ for all $a \in G$.

**Proof:** (1) $\varphi(e_G) = \varphi(e_G \circ e_G) = \varphi(e_G) * \varphi(e_G)$

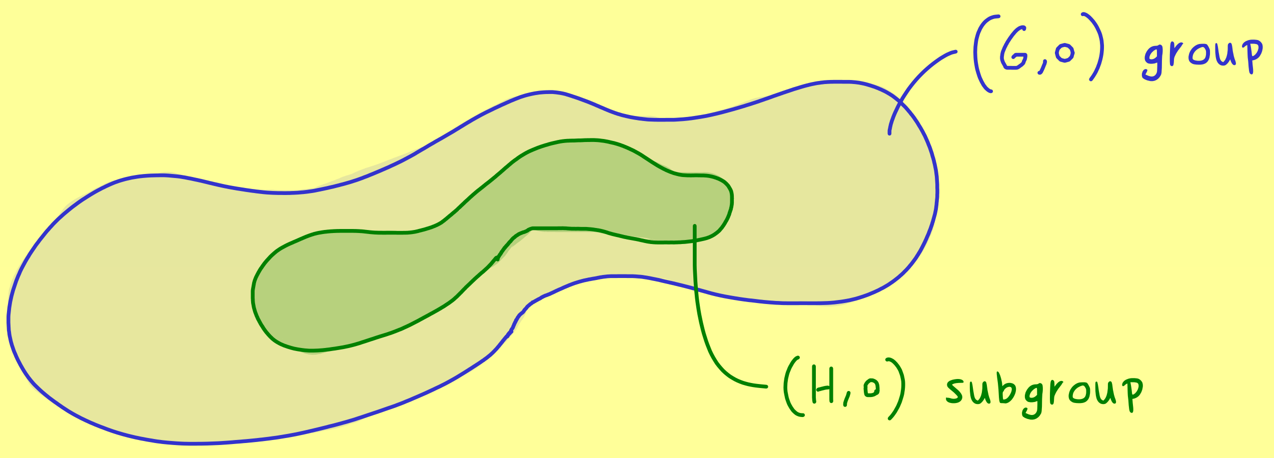
$$\Longrightarrow e_H = \varphi(e_G)^{-1} * \varphi(e_G) = \varphi(e_G)^{-1} * \big(\varphi(e_G) * \varphi(e_G)\big)$$

$$= \underbrace{\big(\varphi(e_G)^{-1} * \varphi(e_G)\big)}_{= e_H} * \varphi(e_G) = \varphi(e_G)$$

(2) $e_H = \varphi(e_G) = \varphi(a^{-1} \circ a) = \varphi(a^{-1}) * \varphi(a)$

$$\overset{\text{inverse unique}}{\Longrightarrow} \varphi(a)^{-1} = \varphi(a^{-1}) \qquad \square$$

# Algebra - Part 10

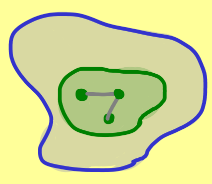



Example: $(\mathbb{R},+) \rightsquigarrow (\mathbb{Z},+)$ subgroup

Definition: Let $(G,\circ)$ be a group. A non-empty subset $H \subseteq G$ is called a subgroup of $G$ if $(H,\circ)$ forms a group.

We get a group homomorphism: $\varphi: H \longrightarrow G, \; x \longmapsto x$ , $\varphi(a \circ b) = \varphi(a) \circ \varphi(b)$

$$\Longrightarrow \underbrace{\varphi(e_H)}_{= e_H} = e_G$$



Proposition: Let $(G,\circ)$ be a group and $H \subseteq G$ be a non-empty subset.

Then: $H$ is a subgroup of $G$ $\Longleftrightarrow$ $\begin{cases} a \circ b \in H & \text{for all } a,b \in H \quad (*) \\ a^{-1} \in H & \text{for all } a \in H \quad (**) \end{cases}$

Proof: $(\Longrightarrow)$ Assume $(H,\circ)$ form a group.

$\Longrightarrow$ $\circ : H \times H \longrightarrow H$ is well-defined! $\Longrightarrow$ $(*)$ ✓

Neutral element in $H$ is the same as the neutral element in $G$:

$e = x^{-1} \circ x \overset{\text{inverses are unique}}{\Longrightarrow} x^{-1} \in H$ for all $x \in H$ $\Longrightarrow$ $(**)$ ✓

$(\Longleftarrow)$ Assume $(*), (**)$. Since $a \circ b \in H$ for all $a,b \in H$,

$\circ : H \times H \longrightarrow H$ is well-defined!

associative! ($G$ is a group)

Choose $a \in H \overset{(**)}{\Longrightarrow} a^{-1} \in H \overset{(*)}{\Longrightarrow} a \circ a^{-1} = e \in H$

$\Longrightarrow$ $(H,\circ)$ is a group $\square$

Example: (a) $(G,\circ)$ group. $\{e\}$ is subgroup of $G$; $G$ is subgroup of $G$ — trivial subgroups

(b) $(\mathbb{Z},+)$ group, $m \in \mathbb{N}$. $m\mathbb{Z} := \{ m \cdot k \mid k \in \mathbb{Z} \} \subseteq \mathbb{Z}$

$\Longrightarrow$ $(m\mathbb{Z},+)$ subgroup of $(\mathbb{Z},+)$

Recall: $\mathbb{Z}/m\mathbb{Z}$ is a group $\rightsquigarrow$ general construction $G/H$

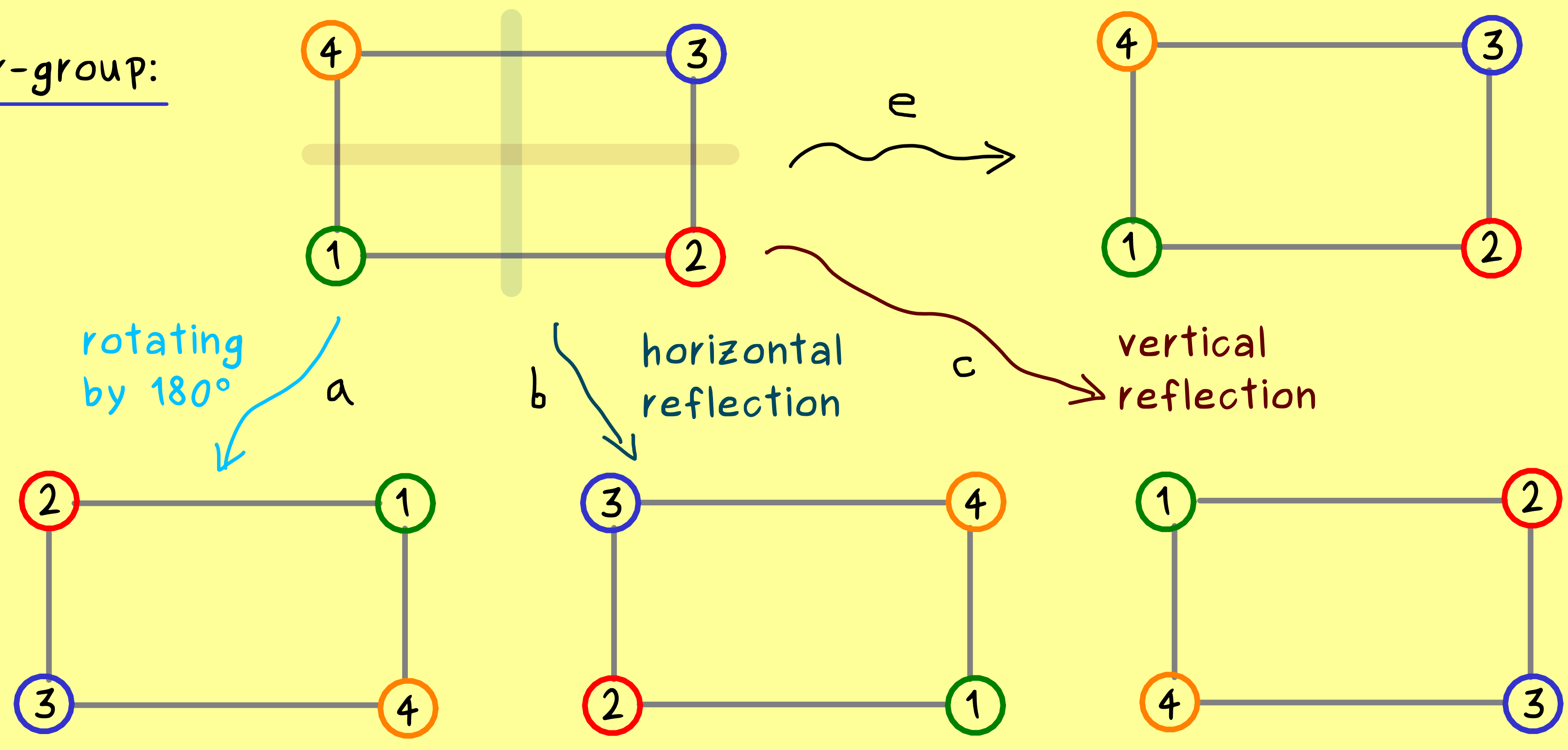
# Algebra - Part 11

**Recall subgroups:** $(G,\circ) \rightsquigarrow H \subseteq G$, $(H,\circ)$ group $\rightsquigarrow H$ subgroup of $G$ $\rightsquigarrow H \leq G$

**Proposition:** $(G,\circ)$ group, $H \subseteq G$ non-empty subset.

$$H \leq G \iff \begin{cases} a \circ b \in H & \text{for all } a,b \in H \\ a^{-1} \in H & \text{for all } a \in H \end{cases}$$

**Klein four-group:**




| $\circ$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

$\rightsquigarrow$ associativity ✓

$(G,\circ)$ with $G = \{e,a,b,c\}$ and $\circ$ satisfying the table above defines the so-called Klein four group, called $K_4$.

**Proposition:** Let $(G,\circ)$ be a group with $\mathrm{ord}(G) < \infty$, $H \subseteq G$ be a non-empty subset.

Then: $H \leq G \iff a \circ b \in H$ for all $a,b \in H$

**Proof:** $(\Rightarrow)$ ✓ $(\Leftarrow)$ $(H,\circ)$ semigroup of finite order and both cancellation properties hold

$$\begin{pmatrix} a \circ x = a \circ y \Rightarrow x = y \\ x \circ b = y \circ b \Rightarrow x = y \end{pmatrix}$$

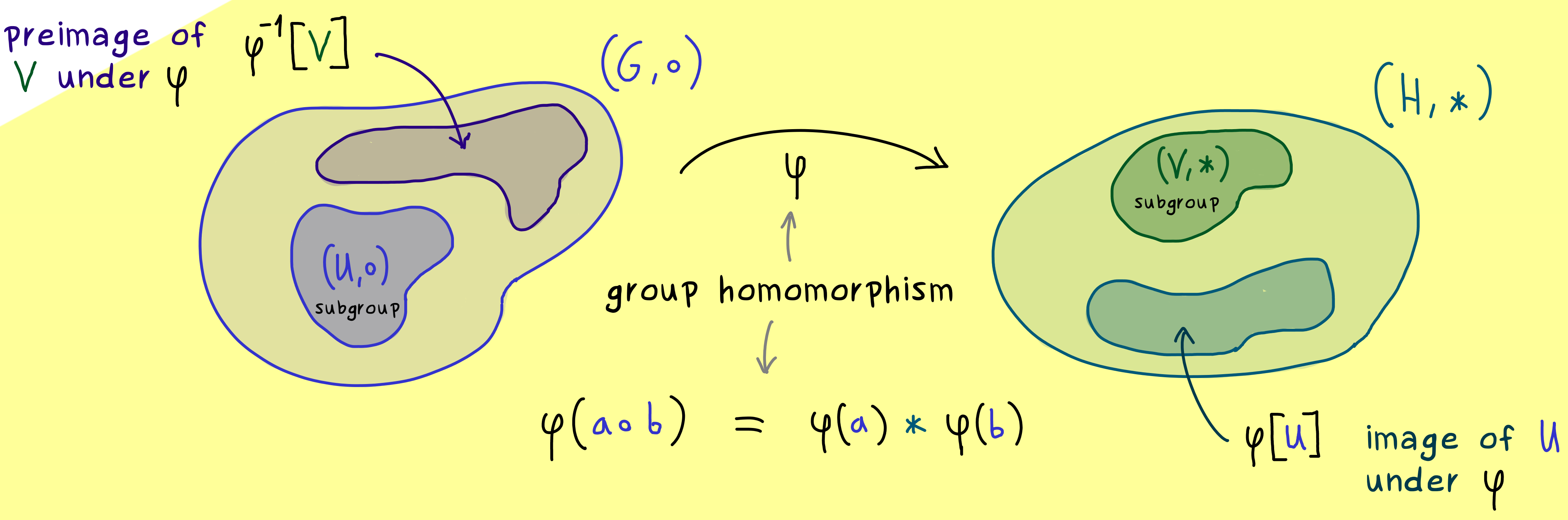
$\overset{\text{part 6}}{\Longrightarrow}$ $(H,\circ)$ is a group $\square$

**Example:** $G = \{e,a,b,c\}$ Klein four-group.

subgroups: $H_1 = \{e\}$, $H_2 = \{e,a\}$, $H_3 = \{e,b\}$, $H_4 = \{e,c\}$, $H_5 = G$

$\rightsquigarrow$ we have 5 subgroups

# Algebra - Part 12




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

**Proposition:** $(G,\circ),(H,*)$ groups, $\varphi: G \longrightarrow H$ group homomorphism.

If $U \subseteq G$ is a subgroup of $G$ and $V \subseteq H$ is a subgroup of $H$,

then: (a) $\varphi[U] \subseteq H$ is a subgroup of $H$

(b) $\varphi^{-1}[V] \subseteq G$ is a subgroup of $G$

**Proof:** (a) Take $a,b \in \varphi[U] \subseteq H$. We find $x,y \in U$ with $\varphi(x) = a$, $\varphi(y) = b$.

Then: $a * b = \varphi(x) * \varphi(y) = \varphi(\underbrace{x\circ y}_{\in U \text{ (subgroup!)}}) \in \varphi[U]$

$a^{-1} = \varphi(x)^{-1} = \varphi(\underbrace{x^{-1}}_{\in U \text{ (subgroup!)}}) \in \varphi[U]$

$\overset{\text{part 10}}{\Longrightarrow} (\varphi[U], *)$ subgroup

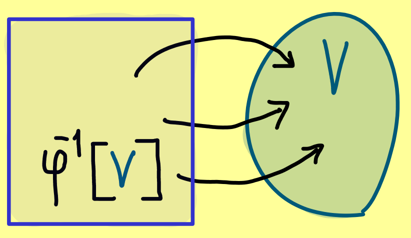
(b) Take $x,y \in \varphi^{-1}[V]$. We find $a,b \in V$ with $\varphi(x) = a$, $\varphi(y) = b$.

Then: $\varphi(x\circ y) = \varphi(x) * \varphi(y) = a * b \in V$

$\Longrightarrow x\circ y \in \varphi^{-1}[V]$

$\varphi(x^{-1}) = \varphi(x)^{-1} = a^{-1} \in V$

$\Longrightarrow x^{-1} \in \varphi^{-1}[V] \overset{\text{part 10}}{\Longrightarrow} (\varphi^{-1}[V], \circ)$ subgroup $\square$

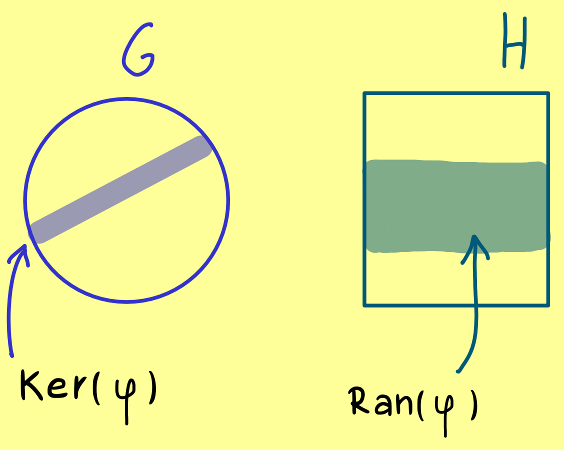



**Special cases:** $\varphi: G \longrightarrow H$ group homomorphism.

$\varphi^{-1}[\{e\}] =: \mathrm{Ker}(\varphi)$ kernel of $\varphi$

$\varphi[G] =: \mathrm{Ran}(\varphi)$ range of $\varphi$

$(\mathrm{im}(\varphi)$ image of $\varphi)$

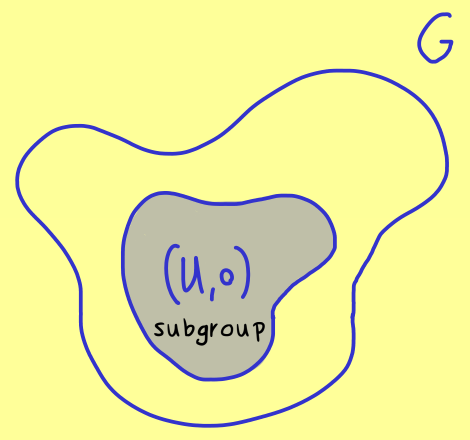



**Example:** $\varphi: \mathbb{Z} \longrightarrow \{e, a\}$

$k \longmapsto \begin{cases} e, & k \text{ even} \\ a, & k \text{ odd} \end{cases}$ $\rightsquigarrow$ group homomorphism! $\varphi(k+m) = \varphi(k)\circ\varphi(m)$

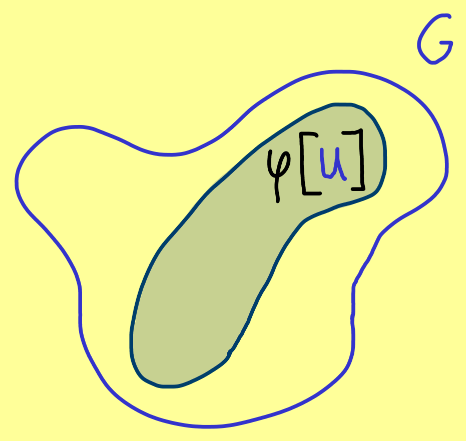
$\mathrm{Ker}(\varphi) = \{\text{even numbers}\} = 2\cdot\mathbb{Z}$ subgroup!

# Algebra - Part 13




$\varphi: G \to G$

group homomorphism
$=$
group endomorphism




**Important case:** $\underbrace{\text{inner}}$ $\underbrace{\text{automorphisms}}$ : $\varphi: G \to G$ group homomorphism that can be written as $\varphi(x) = g\, x\, g^{-1}$

inner: $\varphi$ is represented by an inner element

automorphisms: endomorphism + isomorphism

isomorphism = (bijective and homomorphism in both directions)

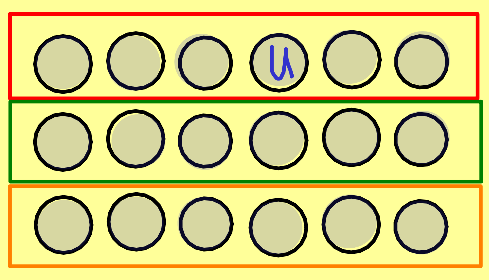
**We already know:** $U \subseteq G$ subgroup $\Rightarrow$ $\varphi[U]$, $\varphi^{-1}[U]$ subgroups

**Definition:** Two subgroups $U, V \subseteq G$ are called conjugate subgroups if there is an element $g \in G$: $V = g U g^{-1} := \{ g u g^{-1} \mid u \in U \}$

$= \varphi[U]$ for $\varphi: G \to G$, $\varphi(x) = g\, x\, g^{-1}$

**Remember:** This defines an equivalence relation on the set of subgroups of $G$.

Hence:



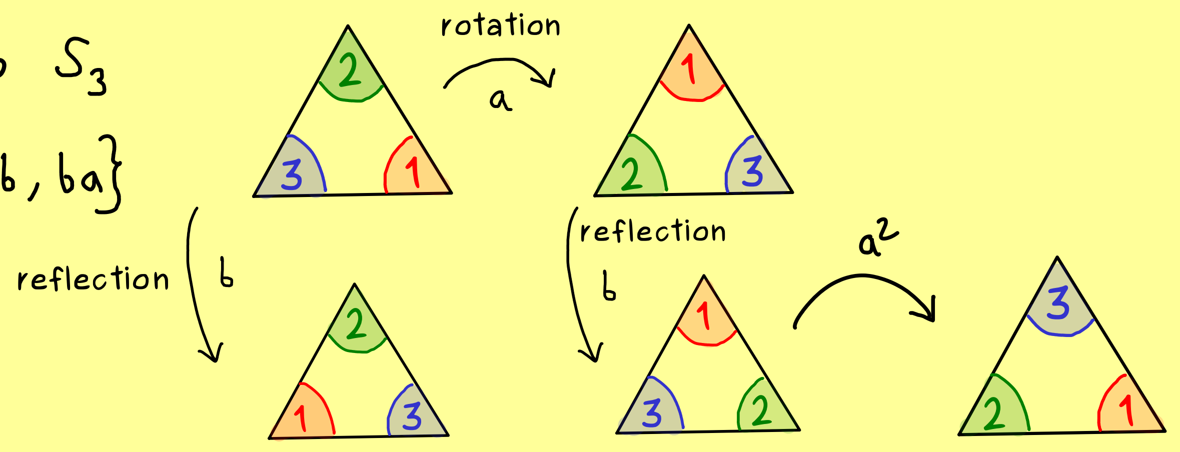

$[U] := \{ g U g^{-1} \mid g \in G \}$

equivalence class

Trivial for abelian groups: $g U g^{-1} = \{ u g g^{-1} \mid u \in U \} = U$

**Example:** Symmetric group $S_3$

$S_3 = \{ e, a, b, a^2, ab, ba \}$




$U = \{ e, b \}$ $\xrightarrow{\text{conjugate subgroups}}$

$a U a^{-1} = \{ e, \underbrace{aba^2}_{ba} \} = \{ e, ba \}$

$a^2 U (a^2)^{-1} = \{ e, \underbrace{a^2 b a}_{ab} \} = \{ e, ab \}$

$ab\, U (ab)^{-1} = \{ e, a\underbrace{bb}_{=e}(ab) \} = \{ e, ba \}$

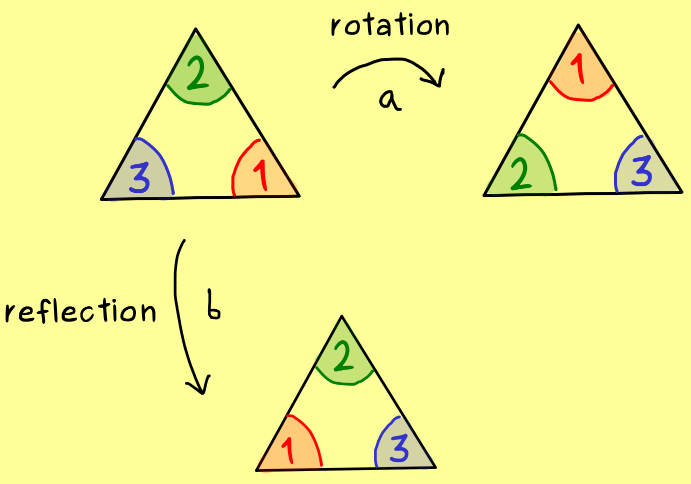
$ba\, U (ba)^{-1} = \{ e, ba\underbrace{b(ba)}_{e} \} = \{ e, ab \}$

$b U b^{-1} = e U e^{-1} = U$

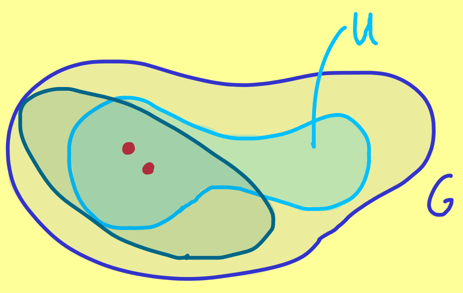
# Algebra - Part 14

Recall: Symmetric group $S_3$

is generated by the two elements $a, b$




Definition: Let $G$ be a group and $S \subseteq G$ be a subset.




$$\langle S \rangle := \bigcap_{\substack{U \subseteq G \text{ subgroup} \\ \text{with } S \subseteq U}} U$$

We say: $S$ generates the subgroup $\langle S \rangle$.

Proposition: Intersection of subgroups is also a subgroup.

Proof: Assume: $G$ group, $U_j \subseteq G$ subgroups for all $j \in J$, $\tilde{U} := \bigcap_{j \in J} U_j$.

Obvious: $e \in \tilde{U}$ ✓

Take $a, b \in \tilde{U} \implies a, b \in U_j$ for all $j \in J$

$\overset{U_j \text{ subgroup}}{\implies}$ $ab \in U_j$ and $a^{-1} \in U_j$ for all $j \in J$

$\implies ab \in \tilde{U}$ and $a^{-1} \in \tilde{U}$ $\square$

Fact: If $S \neq \emptyset$ and $S^{-1} := \{ s^{-1} \mid s \in S \}$, then:

$$\langle S \rangle = \{ a_1 a_2 \cdots a_n \in G \mid n \in \mathbb{N},\ a_1, \dots, a_n \in S \cup S^{-1} \}$$

Example: Symmetric group $S_3$: $S = \{a, b\}$, $S^{-1} = \{a^2, b\}$

$\rightsquigarrow ab, ba, bb = e, \dots$ just six elements

$$S_3 = \langle a, b \rangle$$

Definition: A group $G$ is called cyclic if there is element $g \in G$ such that $\langle g \rangle = G$.

In other words: $G = \{ g^k \mid k \in \mathbb{Z} \}$ with $g^0 :=$ identity element in $G$

# Algebra - Part 15

Cyclic group: $G = \langle g \rangle$ for a particular $g \in G$

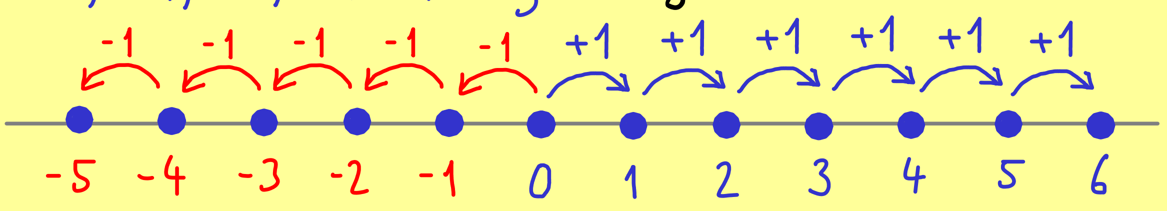
$= \{ g^k \mid k \in \mathbb{Z} \}$ with $g^0 :=$ identity element in $G$

always abelian: $g^k g^m = g \cdot g \cdots g \cdot g \cdot g \cdots g = g^{k+m} = g^m g^k$

Examples: (a) $G = \{e\}$ , $G = \langle e \rangle$ $\quad ( G = \langle \emptyset \rangle )$

(b) $\mathbb{Z} = \{ \ldots, -2, -1, 0, 1, 2, \ldots \}$ together with addition $+$

We know:



$\mathbb{Z} = \langle 1 \rangle = \{ \underbrace{1 + 1 + \cdots + 1}_{k \text{ times}} \mid k \in \mathbb{Z} \} = \{ k \cdot 1 \mid k \in \mathbb{Z} \}$

cyclic group! $\mathbb{Z} = \langle -1 \rangle$

(c) subgroups of $(\mathbb{Z}, +)$ : $m \in \mathbb{N}$

$m\mathbb{Z} := \{ m \cdot k \mid k \in \mathbb{Z} \} \subseteq \mathbb{Z}$ , $3\mathbb{Z} = \{ \ldots, -6, -3, 0, 3, 6, \ldots \}$

also cyclic: $m\mathbb{Z} = \langle m \rangle$

(d) $\mathbb{Z}/_{m\mathbb{Z}}$ is a finite abelian group! $\mathbb{Z}/_{3\mathbb{Z}} = \{ [0], [1], [2] \}$

addition $[k] + [1] = [k+1]$

$\mathbb{Z}/_{m\mathbb{Z}} = \langle [1] \rangle$ cyclic!

Important Result: For each natural number $m \in \mathbb{N}$ or $m = \infty$ , there is a cyclic group of order $m$.