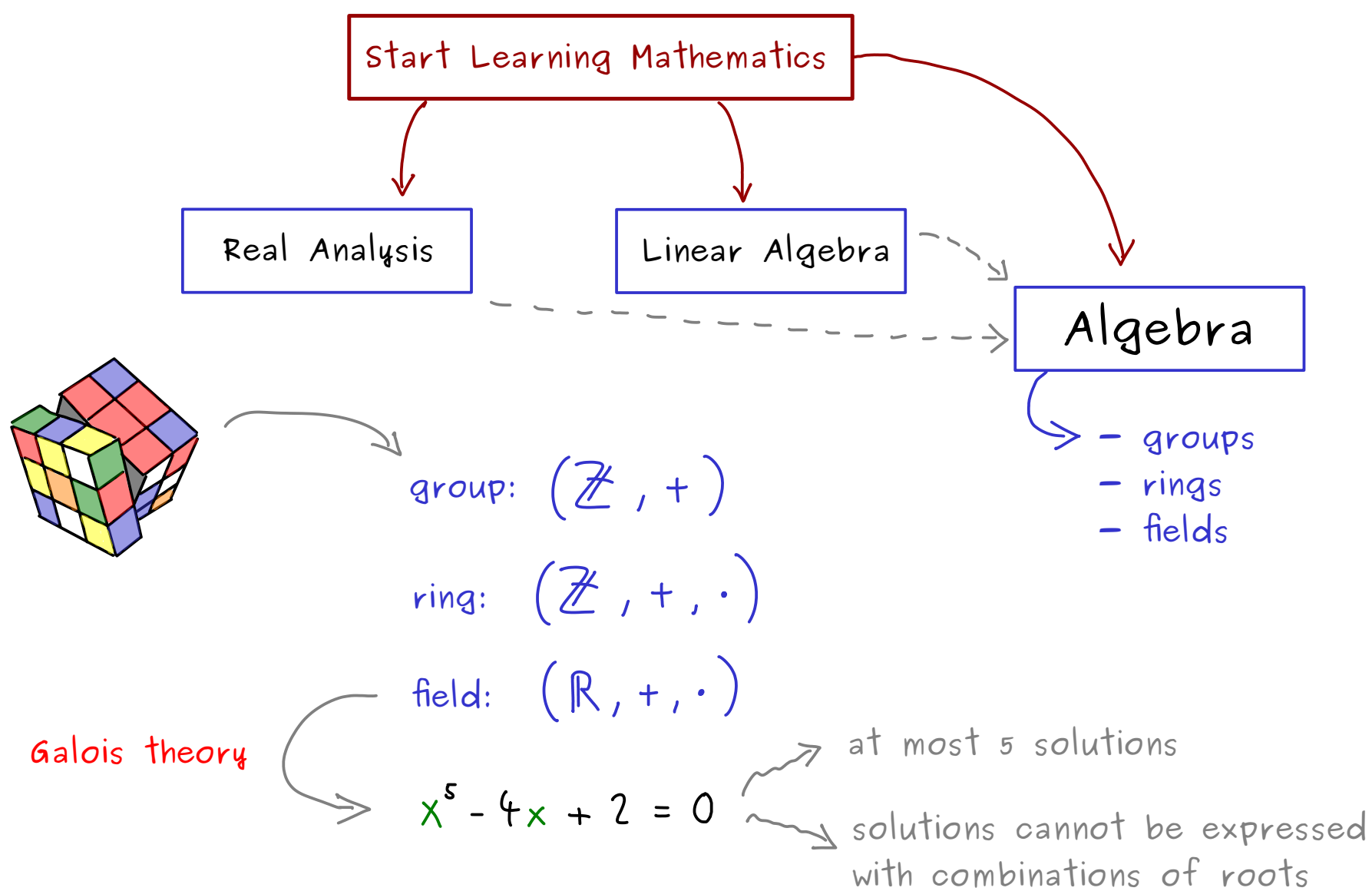


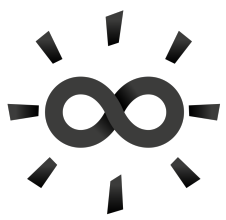
The Bright Side of Mathematics

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





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 $a + b \dots$
↑
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

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

$$\Leftrightarrow a \circ b \circ c$$

Example: set of functions $\mathcal{F}(\mathbb{R}) = \{ f \mid f: \mathbb{R} \rightarrow \mathbb{R} \text{ function} \}$

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

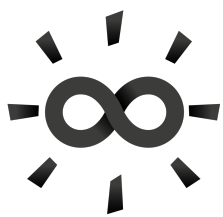
Take $f_1, f_2, f_3 \in \mathcal{F}(\mathbb{R})$ and define $g = f_1 \circ (f_2 \circ f_3) : \mathbb{R} \rightarrow \mathbb{R}$

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

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

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

$\Rightarrow (\mathcal{F}(\mathbb{R}), \circ)$ 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: $S = \left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \mid x, y \in \mathbb{R} \right\}$ 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.

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

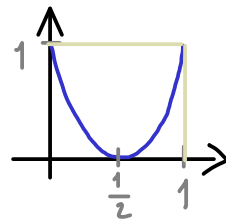
Definition: (S, \circ) semigroup with identity e (the neutral element), $a, b, c \in S$.

- $x \in S$ 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 $z \circ c = e = c \circ z$ invertible

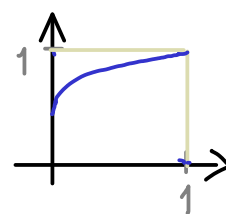
Example: Functions $f: [0,1] \rightarrow [0,1]$, $(\mathcal{F}([0,1]), \circ)$ semigroup

Neutral element: $\text{id}: [0,1] \rightarrow [0,1]$, $x \mapsto x$

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



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



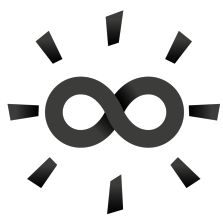
$$\hookrightarrow \tilde{f} \circ g = \text{id}$$

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

Remember:

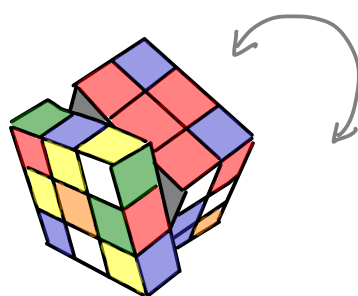
surjective \Leftrightarrow right invertible

injective \Leftrightarrow left invertible



Algebra - Part 4

(S, \circ) semigroup \rightsquigarrow $\begin{matrix} + \\ \text{neutral element} \\ \text{inverses} \end{matrix}$ \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: $\exists b \in G$: $b \circ a = e = a \circ b$

$\bar{a}^1 := b$ (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 $b \circ a = e$.
(*)

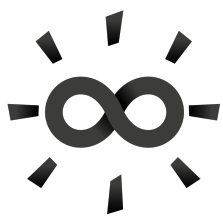
Choose $b \in G$

with $ba = e$. Then $ab \stackrel{(b)}{=} a(eb) \stackrel{(*)}{=} a(ba)b = (ab)(ab)$. (**)

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

$$\Rightarrow ab \stackrel{(b)}{=} e(ab) = c(ab)(ab) \stackrel{(**)}{=} c(ab) = e \Rightarrow (G3) \checkmark$$

$$\Rightarrow ae \stackrel{(*)}{=} a(ba) = (ab)a = ea = a \Rightarrow (G2) \checkmark$$



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: $\forall a \in G \exists b \in G$: $b \circ a = e = a \circ b$

$\overset{\curvearrowright}{a^{-1} := b} \quad \overset{\curvearrowright}{\text{(common notation)}}$

Uniqueness of inverses:

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

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

then $x = y$.

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

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

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

o	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 $\begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}$

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

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

$$S^* := \left\{ a \in S \mid \begin{array}{l} a \text{ is invertible} \\ \uparrow \\ a^{-1} \text{ exists} \end{array} \right\}$$

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

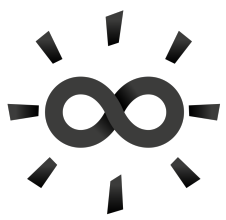
Proof: (1) $e \circ e = e \Rightarrow e \in S^*$ with $e^{-1} = e \Rightarrow$ (G2) ✓

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

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

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

□



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:

$$ax = ay \implies x = y \quad (\text{left cancellation property})$$

$$xb = yb \implies x = y \quad (\text{right cancellation property})$$

Proof: $x = x \underset{\substack{\uparrow \\ \text{neutral element}}}{e} = x(b b^{-1}) = (x b) b^{-1} = (y b) b^{-1} = y (b b^{-1}) = y$

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

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

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

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

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

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

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

(\impliedby) 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: $eb = e(a\tilde{x}) = (ea)\tilde{x} = a\tilde{x} = b \implies e$ left neutral

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

^{part 4}
 $\implies (S, \circ)$ is a group

□

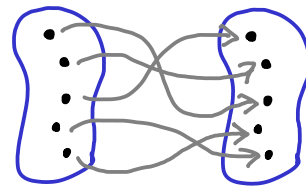
Proposition: Let (S, \circ) be a semigroup with $\text{ord}(S) < \infty$. Then:

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

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

Proof: For any map $f: S \rightarrow S$:

f is injective \iff f is surjective



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

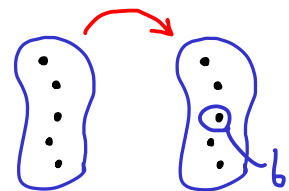
$$f_a(x) = ax, \quad g_a(x) = xa.$$

Then we have: both cancellation properties hold

$$\begin{aligned} \iff \forall a \in S: f_a(x) = f_a(y) &\implies x = y \\ g_a(x) = g_a(y) &\implies x = y \end{aligned}$$

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

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



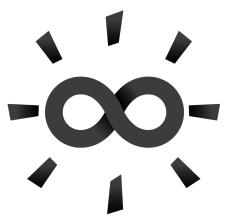
$$\iff \forall a \in S: \text{for every } b \in S \text{ there are}$$

$$x, y \in S: \begin{matrix} f_a(x) = b \\ \parallel \\ ax \end{matrix} \text{ and } \begin{matrix} g_a(y) = b \\ \parallel \\ ya \end{matrix}$$

Lemma

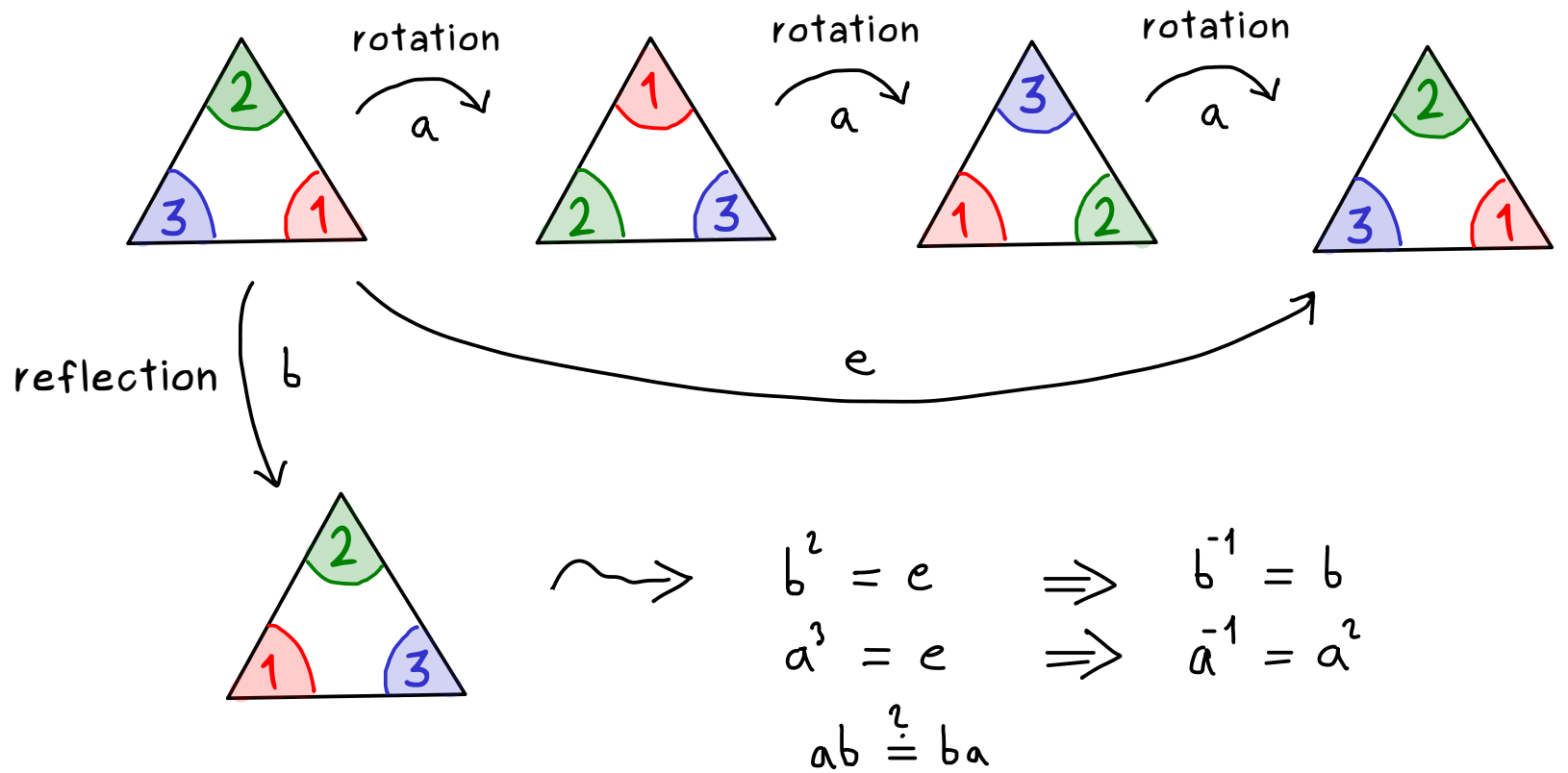
$$\iff (S, \circ) \text{ is group}$$

□



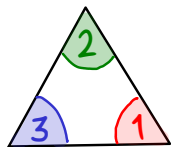
Algebra - Part 7

Group:



symmetry operations \iff

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



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

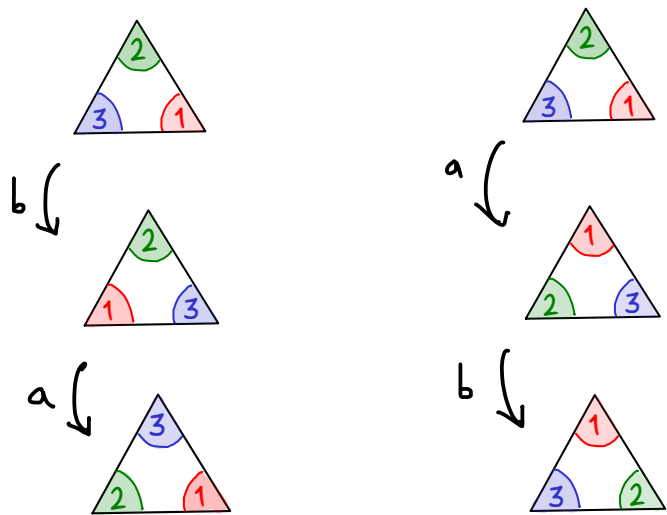
\hookrightarrow symmetric group

Example:

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

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

$\implies (S_3, \circ)$ 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

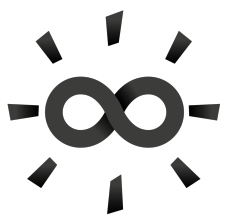
\circ	a	b	e
a	a^2	\square	a
b	\square	b^2	b
e	a	b	e

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

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

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

Non-abelian group: Symmetric group S_3 : $|S_3| = 3! = 6$ \searrow order 6
Dihedral group D_3 \swarrow



Algebra - Part 8

modulus calculation:

$$13 - 12 = 1$$

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

modulus = m

$$X \sim_m Y \Leftrightarrow \text{There is } q \in \mathbb{Z} \\ X - Y = q \cdot m$$

$$X \equiv Y \pmod{m}$$

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

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

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

define addition: $[k] + [l] := [k + l]$ well-defined

$$[k] + [-k] = [0] \quad \text{identity}$$

inverse

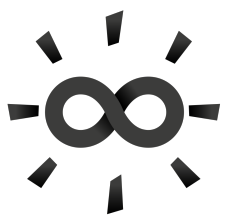
$$\Rightarrow (\mathbb{Z}_m, +) \text{ abelian group of order } m$$

Example: $(\mathbb{Z}_2, +)$: $[0] = \{ 0, 2, 4, \dots, -2, -4, \dots \}$
 $[1] = \{ 1, 3, 5, 7, \dots, -1, -3, \dots \}$

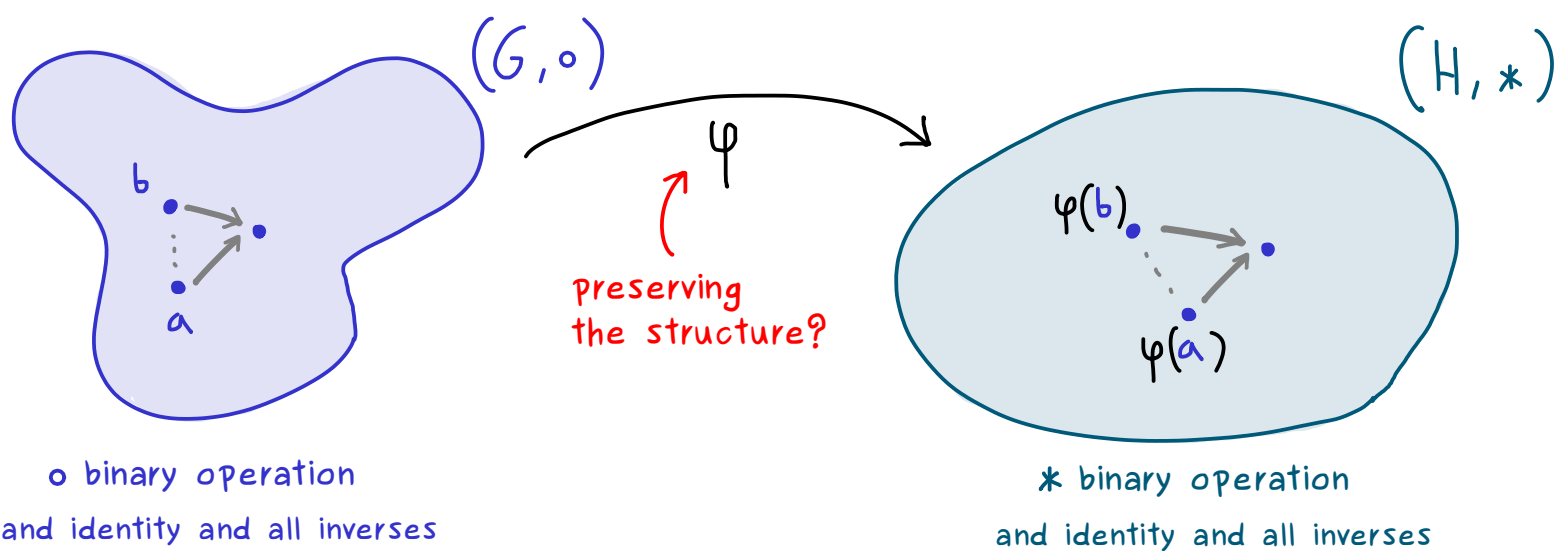
+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

$(\mathbb{Z}_6, +)$: $[0] = \{ 0, 6, 12, \dots, -6, -12, \dots \}$
 $[1], [2], [3], [4], [5]$

+	[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



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

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

$$\begin{aligned} \varphi: G &\rightarrow H \\ x &\mapsto e^x \end{aligned} \quad \Rightarrow \quad \begin{aligned} \varphi(x+y) &= e^{x+y} \\ \varphi(x) \cdot \varphi(y) &= e^x \cdot e^y \end{aligned} \quad \gg$$

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:

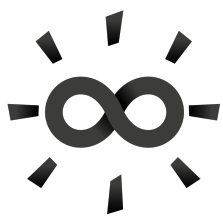
$$\begin{aligned} (1) \quad \varphi(e_G) &= \varphi(e_G \circ e_G) = \varphi(e_G) * \varphi(e_G) \\ \Rightarrow e_H &= \varphi(e_G)^{-1} * \varphi(e_G) = \varphi(e_G)^{-1} * (\varphi(e_G) * \varphi(e_G)) \\ &= \underbrace{(\varphi(e_G)^{-1} * \varphi(e_G))}_{= e_H} * \varphi(e_G) = \varphi(e_G) \end{aligned}$$

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

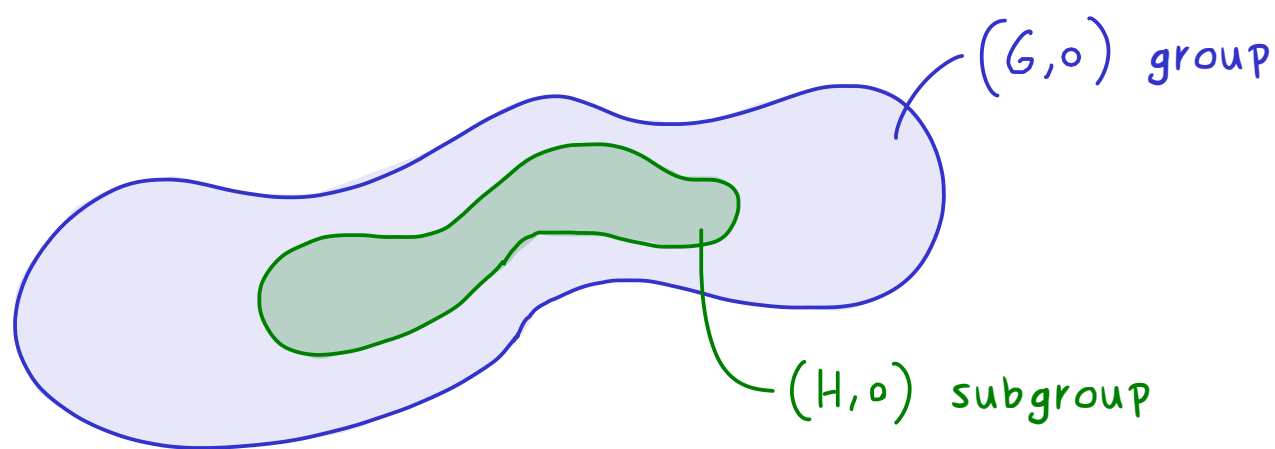
inverse unique

$$\Rightarrow \varphi(a)^{-1} = \varphi(a^{-1})$$

□



Algebra - Part 10

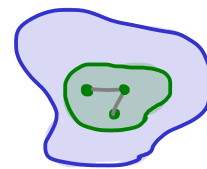


Example: $(\mathbb{R}, +)$ ← $(\mathbb{Z}, +)$
subgroup

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: $\psi: H \rightarrow G$, $\psi(a \circ b) = \psi(a) \circ \psi(b)$
 $x \mapsto x$
 $\Rightarrow \psi(e_H) = e_G$
 \parallel
 e_H

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



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

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

$\implies \circ: H \times H \rightarrow H$ is well-defined! $\implies (*) \checkmark$

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

$e = \bar{x}^{-1} \circ x \xrightarrow{\text{inverses are unique}} \bar{x}^{-1} \in H$ for all $x \in H \implies (**)$ \checkmark

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

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

associative! (G is a group)

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

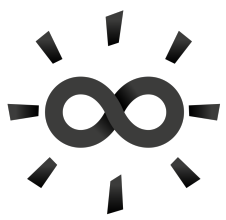
$\implies (H, \circ)$ is a group □

Example: (a) (G, \circ) group. $\left. \begin{array}{l} \{e\} \text{ is subgroup of } G \\ G \text{ is subgroup of } G \end{array} \right\} \text{ trivial subgroups}$

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

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

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



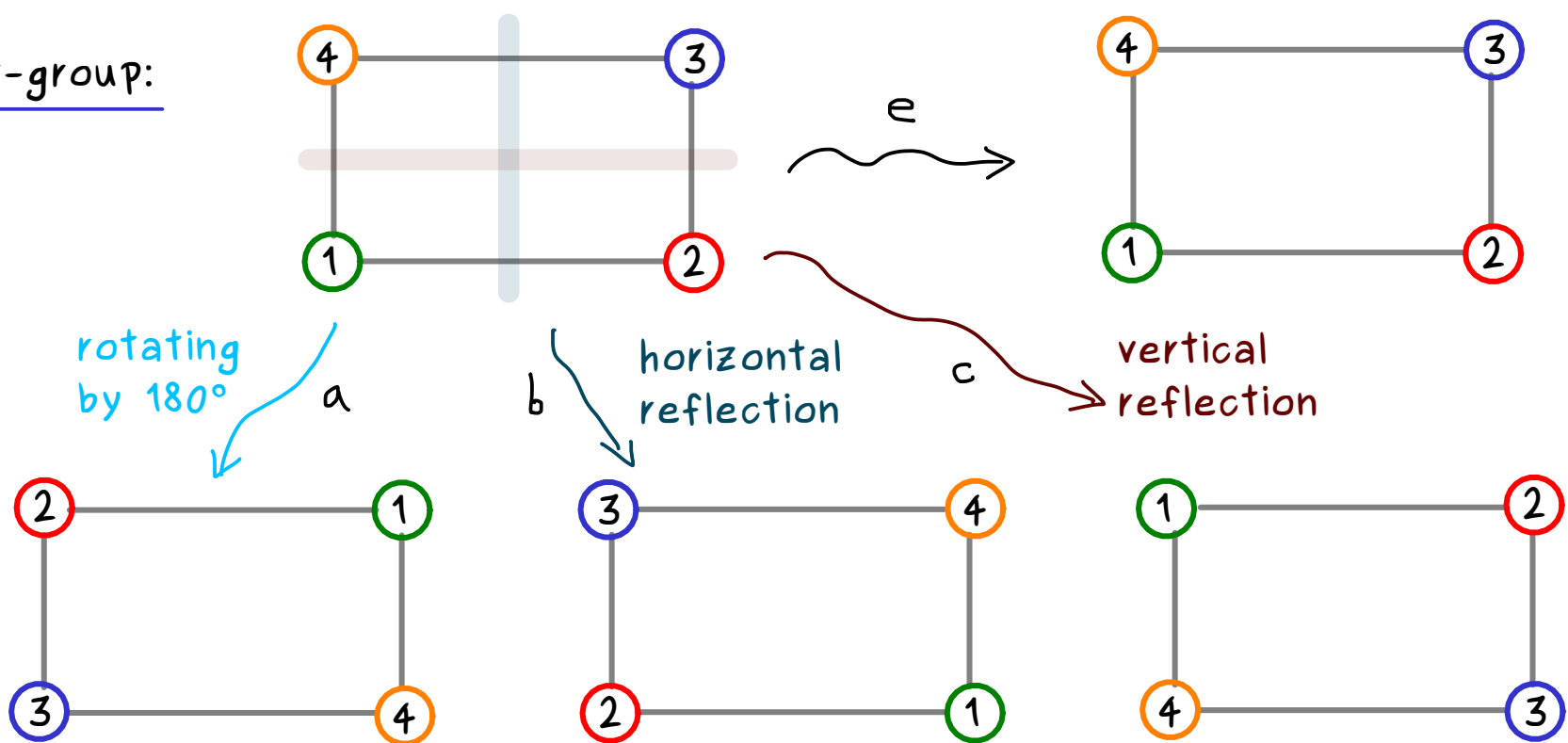
Algebra - Part 11

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

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 $\text{ord}(G) < \infty$, $H \subseteq G$ be a non-empty subset.

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

Proof: (\implies) ✓ (\impliedby) (H, \circ) semigroup of finite order and both cancellation properties hold

$$\left(\begin{array}{l} a \circ x = a \circ y \implies x = y \\ x \circ b = y \circ b \implies x = y \end{array} \right)$$

part 6

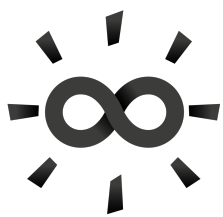
$\implies (H, \circ)$ is a group

□

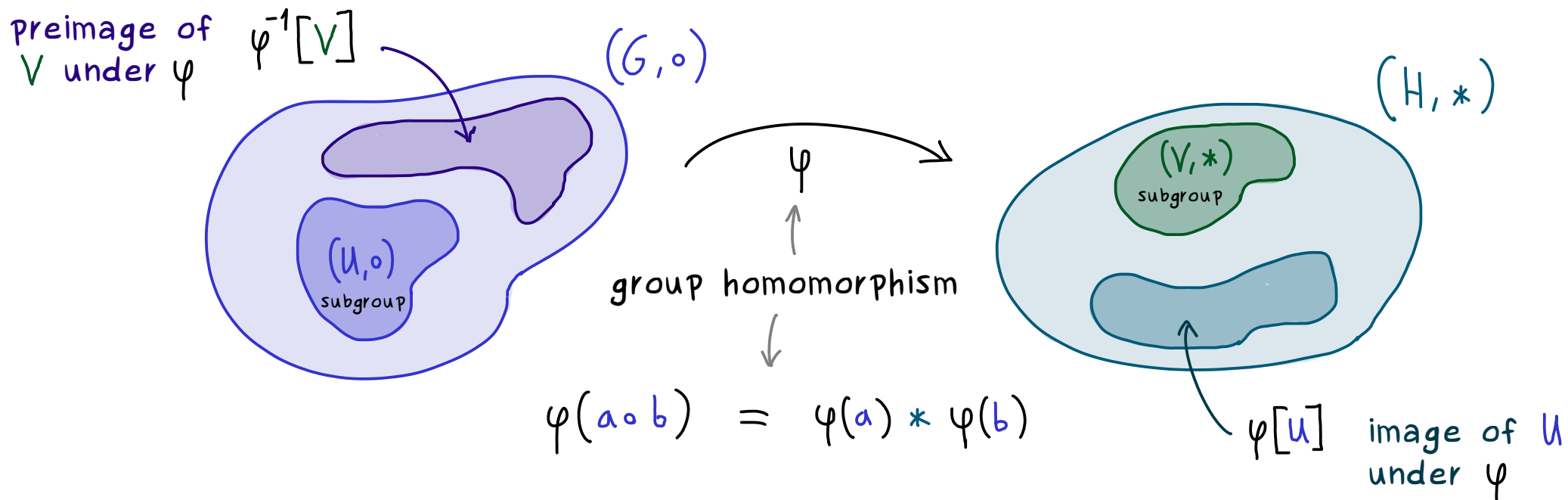
Example: $G = \{e, a, b, c\}$ Klein four-group.

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



Proposition: $(G, \circ), (H, *)$ groups, $\varphi: G \rightarrow H$ 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: $a * b = \varphi(x) * \varphi(y) = \varphi(\underbrace{x \circ y}_{\in U \text{ (subgroup!)}}) \in \varphi[U]$
 $a^{-1} = \varphi(x)^{-1} = \varphi(\underbrace{x^{-1}}_{\in U \text{ (subgroup!)}}) \in \varphi[U]$ part 10 $\Rightarrow (\varphi[U], *)$ subgroup

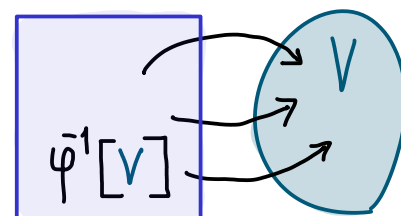
(b) Take $x, y \in \varphi^{-1}[V]$. We find $a, b \in V$ with $\varphi(x) = a, \varphi(y) = b$.

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

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

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

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

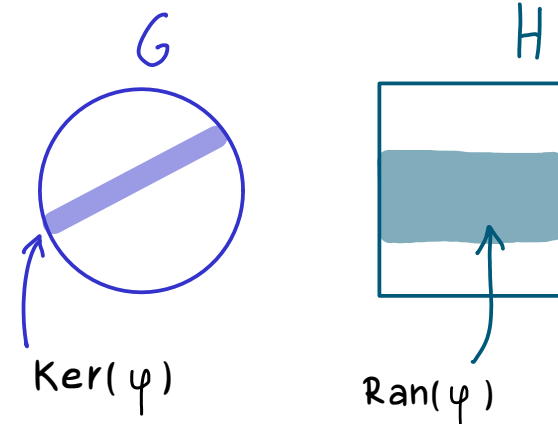


Special cases: $\varphi: G \rightarrow H$ group homomorphism.

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

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

$$(\text{im}(\varphi) \quad \text{image of } \varphi)$$



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

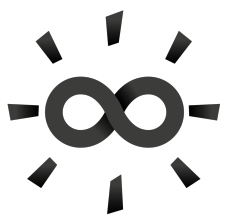
$$k \mapsto \begin{cases} e, & k \text{ even} \\ a, & k \text{ odd} \end{cases}$$



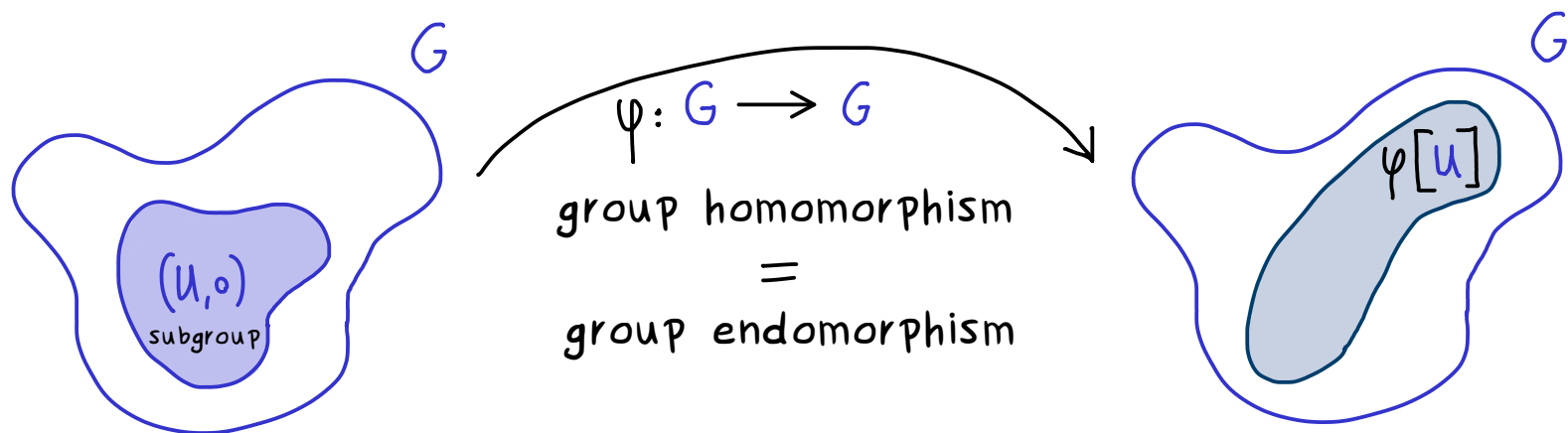
group homomorphism!

$$\varphi(k+m) = \varphi(k) \circ \varphi(m)$$

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



Algebra - Part 13



Important case: inner automorphisms: $\psi: G \rightarrow G$ group homomorphism that can be written as $\psi(x) = g x g^{-1}$

ψ is represented by an inner element

endomorphism + isomorphism \equiv (bijective and homomorphism in both directions)

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

Definition: Two subgroups $U, V \subseteq G$ are called conjugate subgroups

if there is an element $g \in G$: $V = g U g^{-1} := \{g u g^{-1} \mid u \in U\}$
 $\equiv \psi[U]$ for $\psi: G \rightarrow G$
 $\psi(x) = g x g^{-1}$

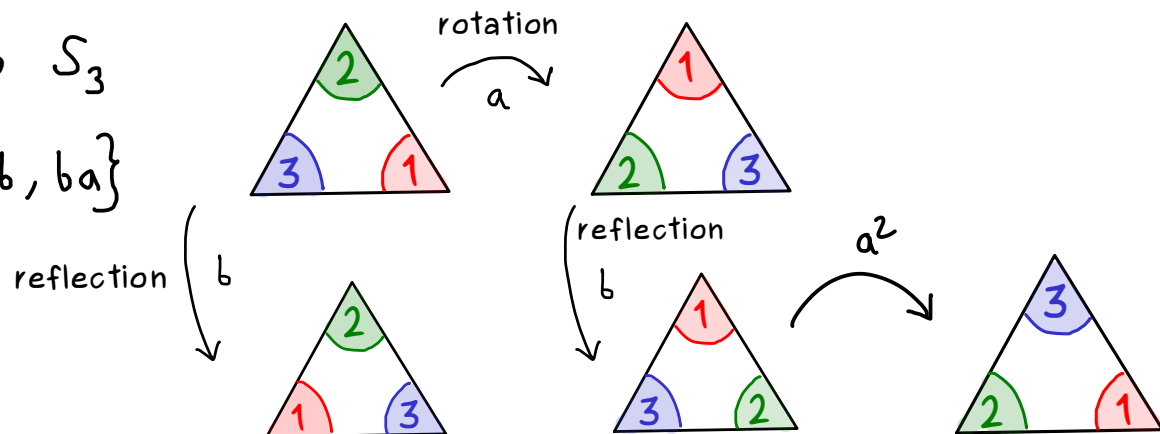
Remember: This defines an equivalence relation on the set of subgroups of G .

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

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



$U = \{e, b\}$ conjugate subgroups \rightsquigarrow

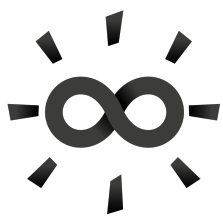
$$a U a^{-1} = \{e, \underbrace{aba^2}_{ba}\} = \{e, ba\}$$

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

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

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

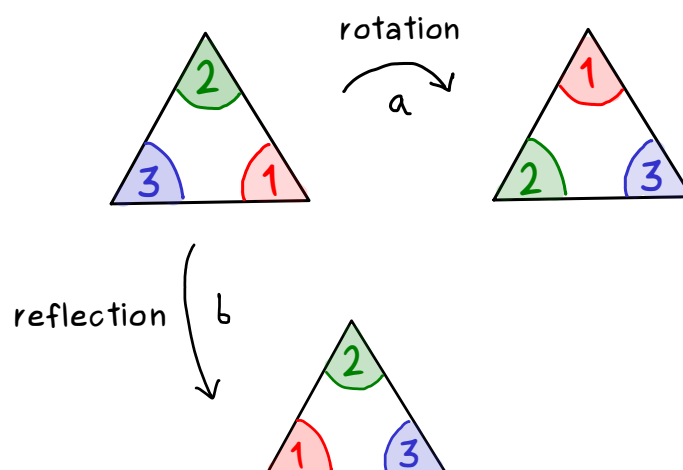
$$b U b^{-1} = e U e^{-1} = U$$



Algebra - Part 14

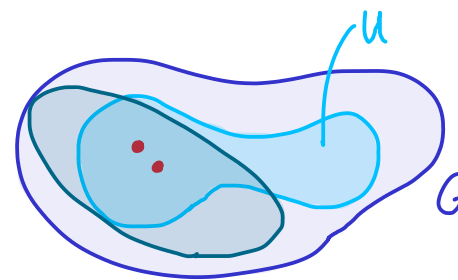
Recall: Symmetric group S_3

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 $j \in J$

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

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

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

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

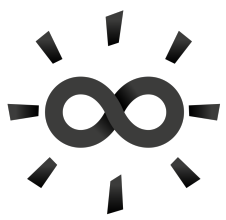
Example: Symmetric group S_3 : $S = \{a, b\}$, $S^{-1} = \{a^2, b\}$

$\leadsto ab, ba, bb = e, \dots$ 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

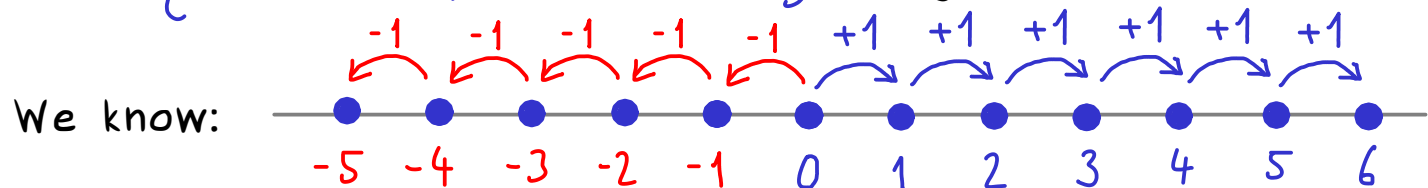
Cyclic group: $G = \langle g \rangle$ for a particular $g \in G$

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

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) $G = \{e\}$, $G = \langle e \rangle$ ($G = \langle \emptyset \rangle$)

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



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

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

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

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

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

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

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