Discrete Structures

B12. Groups – A Glimpse of Abstract Algebra

Malte Helmert, Gabriele Röger

University of Basel

October 28, 2026

Groups

Abstract Algebra

- Elementary algebra: "Arithmetics with variables"
  - e. g. $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ describes the solutions of $ax^2 + bx + c = 0$ where $a \neq 0$.
  - Variables for numbers and operations such as addition, subtraction, multiplication, division ...
  - "What you learn at school."

Abstract Algebra

- Elementary algebra: "Arithmetics with variables"
  - e. g. $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ describes the solutions of $ax^2 + bx + c = 0$ where $a \neq 0$.
  - Variables for numbers and operations such as addition, subtraction, multiplication, division ...
  - "What you learn at school."
- Abstract algebra: Generalization of elementary algebra
  - Arbitrary sets and operations on their elements
  - e. g. permutations of a given set S plus function composition
  - Abstract algebra studies arbitrary sets and operations based on certain properties (such as associativity).

Abstract Algebra

- Elementary algebra: "Arithmetics with variables"
  - e. g. $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ describes the solutions of $ax^2 + bx + c = 0$ where $a \neq 0$.
  - Variables for numbers and operations such as addition, subtraction, multiplication, division ...
  - "What you learn at school."
- Abstract algebra: Generalization of elementary algebra
  - Arbitrary sets and operations on their elements
  - e. g. permutations of a given set S plus function composition
  - Abstract algebra studies arbitrary sets and operations based on certain properties (such as associativity).

What if we ignore what the objects are and focus only on how their operations behave?

Binary operations

- A binary operation on a set S is a function $f : S \times S \to S$.

Binary operations

- A binary operation on a set S is a function $f : S \times S \to S$.
- e. g. $add : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ for addition of natural numbers.

Binary operations

- A binary operation on a set S is a function $f : S \times S \to S$.
- e. g. $add : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ for addition of natural numbers.
- In infix notation, we write the operator between the operands, e. g. $x + y$ instead of $add(x, y)$.

Quiz

Quiz

What do the following two sets together with the given operation have in common?

- The set of all integers $\mathbb{Z}$ together with addition $+$.
- The set of all permutations of the set $\{1, 2, 3, 4\}$ together with function composition.

Think of...

- What properties do the operations have in common?
- Is there an element that leaves every element unchanged with the given operation?
- Can every operation be undone again?

Groups

Definition (Group)

A group $G = \langle S, \cdot \rangle$ is given by a set S and
a binary operation $\cdot$ on S that satisfy the group axioms:

Groups

Definition (Group)

A group $G = \langle S, \cdot \rangle$ is given by a set S and
a binary operation $\cdot$ on S that satisfy the group axioms:

- Associativity: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in S$.

Groups

Definition (Group)

A group $G = \langle S, \cdot \rangle$ is given by a set S and
a binary operation $\cdot$ on S that satisfy the group axioms:

- Associativity: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in S$.
- Identity element: There exists an $e \in S$ such that
  for all $x \in S$ it holds that $x \cdot e = e \cdot x = x$.
  Element e is called identity or neutral element of the group.

Groups

Definition (Group)

A group $G = \langle S, \cdot \rangle$ is given by a set S and
a binary operation $\cdot$ on S that satisfy the group axioms:

- Associativity: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in S$.
- Identity element: There exists an $e \in S$ such that
  for all $x \in S$ it holds that $x \cdot e = e \cdot x = x$.
  Element e is called identity or neutral element of the group.
- Inverse element: For every $x \in S$ there is a $y \in S$ such that
  $x \cdot y = y \cdot x = e$, where e is the identity element.

Groups

Definition (Group)

A group $G = \langle S, \cdot \rangle$ is given by a set S and
a binary operation $\cdot$ on S that satisfy the group axioms:

- Associativity: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in S$.
- Identity element: There exists an $e \in S$ such that
  for all $x \in S$ it holds that $x \cdot e = e \cdot x = x$.
  Element e is called identity or neutral element of the group.
- Inverse element: For every $x \in S$ there is a $y \in S$ such that
  $x \cdot y = y \cdot x = e$, where e is the identity element.

A group is called abelian if $\cdot$ is also commutative,
i. e. for all $x, y \in S$ it holds that $x \cdot y = y \cdot x$.

Niels Henrik Abel: Norwegian mathematician (1802–1829),
cf. Abel prize

Groups

Definition (Group)

A group $G = \langle S, \cdot \rangle$ is given by a set S and
a binary operation $\cdot$ on S that satisfy the group axioms:

- Associativity: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in S$.
- Identity element: There exists an $e \in S$ such that
  for all $x \in S$ it holds that $x \cdot e = e \cdot x = x$.
  Element e is called identity or neutral element of the group.
- Inverse element: For every $x \in S$ there is a $y \in S$ such that
  $x \cdot y = y \cdot x = e$, where e is the identity element.

A group is called abelian if $\cdot$ is also commutative,
i. e. for all $x, y \in S$ it holds that $x \cdot y = y \cdot x$.

Cardinality $|S|$ is called the order of the group.

Niels Henrik Abel: Norwegian mathematician (1802–1829),
cf. Abel prize

Example: $\langle \mathbb{Z}, + \rangle$

$\langle \mathbb{Z}, + \rangle$ is a group:

- $\mathbb{Z}$ is closed under addition, i. e. for $x, y \in \mathbb{Z}$ it holds that $x + y \in \mathbb{Z}$
- The $+$ operator is associative: for all $x, y, z \in \mathbb{Z}$ it holds that $(x + y) + z = x + (y + z)$.
- Integer 0 is the identity element: for all integers x it holds that $x + 0 = 0 + x = x$.
- Every integer x has an inverse element in the integers, namely $-x$, because $x + (-x) = (-x) + x = 0$.

Example: $\langle \mathbb{Z}, + \rangle$

$\langle \mathbb{Z}, + \rangle$ is a group:

- $\mathbb{Z}$ is closed under addition, i. e. for $x, y \in \mathbb{Z}$ it holds that $x + y \in \mathbb{Z}$
- The $+$ operator is associative: for all $x, y, z \in \mathbb{Z}$ it holds that $(x + y) + z = x + (y + z)$.
- Integer 0 is the identity element: for all integers x it holds that $x + 0 = 0 + x = x$.
- Every integer x has an inverse element in the integers, namely $-x$, because $x + (-x) = (-x) + x = 0$.

$\langle \mathbb{Z}, + \rangle$ also is an abelian group
because for all $x, y \in \mathbb{Z}$ it holds that $x + y = y + x$.

Example: Symmetric Group

Theorem (Symmetric Group)

Let M be a set. Then $\mathrm{Sym}(M) = \langle S, \cdot \rangle$, where

- *S is the set of all permutations of M, and*
- *$\cdot$ denotes function composition,*

is a group, called the symmetric group of M.

For finite set $M = \{1, \ldots, n\}$, we also use S_n to refer to the symmetric group of M.

Example: Symmetric Group

Theorem (Symmetric Group)

Let M be a set. Then $\mathrm{Sym}(M) = \langle S, \cdot \rangle$, where

- *S is the set of all permutations of M, and*
- *$\cdot$ denotes function composition,*

is a group, called the symmetric group of M.

For finite set $M = \{1, \ldots, n\}$, we also use S_n to refer to the symmetric group of M.

Is the symmetric group abelian?

Example: Symmetric Group

Theorem (Symmetric Group)

Let M be a set. Then $\mathrm{Sym}(M) = \langle S, \cdot \rangle$, where

- *S is the set of all permutations of M, and*
- *$\cdot$ denotes function composition,*

is a group, called the symmetric group of M.

For finite set $M = \{1, \ldots, n\}$, we also use S_n to refer to the symmetric group of M.

Is the symmetric group abelian?

What's the order of S_n?

Symmetric Group – Proof

Theorem

For set M, $\mathrm{Sym}(M) = (\{\sigma : M \to M \mid \sigma \text{ is bijective}\}, \cdot)$ is a group.

Proof.

- Closure: The product of two permutations of M is a permutation of M and hence in the set.
- Associativity: Function composition is always associative.
- Identity element: Function $\mathrm{id} : M \to M$ with $\mathrm{id}(x) = x$ is a permutation and for every permutation σ of M it holds that $\sigma\mathrm{id} = \mathrm{id}\sigma = \sigma$.
- Inverse element: For every permutation σ of M, also the inverse function σ^{-1} is a permutation of M and has the required properties.

Another Group: $\langle \mathbb{Z}_3, +_3 \rangle$

- $\mathbb{Z}_3 = \{0, 1, 2\}$
- $+_3$ is addition modulo 3:

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Another Group: $\langle \mathbb{Z}_3, +_3 \rangle$

- $\mathbb{Z}_3 = \{0, 1, 2\}$
- $+_3$ is addition modulo 3:

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\langle \mathbb{Z}_3, +_3 \rangle$ is a group:

- $\mathbb{Z}_3$ is closed under addition modulo 3: the remainder upon division by 3 is always in $\{0, 1, 2\}$.
- The $+_3$ operator is associative: for all $x, y, z \in Z_3$ we have $(((x + y) \bmod 3) + z) \bmod 3 = (x + ((y + z) \bmod 3)) \bmod 3$.
- Integer 0 is the identity element: for all $x \in \mathbb{Z}_3$ it holds that $(x + 0) \bmod 3 = (0 + x) \bmod 3 = x$.
- Every $x \in \mathbb{Z}_3$ has an inverse element in $\mathbb{Z}_3$: 1 is the inverse of 2 and vice versa. 0 is the inverse of 0.

Another Group: $\langle \mathbb{Z}_3, +_3 \rangle$

- $\mathbb{Z}_3 = \{0, 1, 2\}$
- $+_3$ is addition modulo 3:

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Is the group abelian?

$\langle \mathbb{Z}_3, +_3 \rangle$ is a group:

- $\mathbb{Z}_3$ is closed under addition modulo 3: the remainder upon division by 3 is always in $\{0, 1, 2\}$.
- The $+_3$ operator is associative: for all $x, y, z \in Z_3$ we have $(((x + y) \bmod 3) + z) \bmod 3 = (x + ((y + z) \bmod 3)) \bmod 3$.
- Integer 0 is the identity element: for all $x \in \mathbb{Z}_3$ it holds that $(x + 0) \bmod 3 = (0 + x) \bmod 3 = x$.
- Every $x \in \mathbb{Z}_3$ has an inverse element in $\mathbb{Z}_3$: 1 is the inverse of 2 and vice versa. 0 is the inverse of 0.

Generally: Cyclic Group of Order n

Theorem (Cyclic Group of Order n)

Let $n \in \mathbb{N}_1$. Then $\langle \mathbb{Z}_n, +_n \rangle$, where

- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$
- $+_n$ *is addition modulo n, defined as* $x +_n y = (x + y) \bmod n$,

is an abelian group, called cyclic group of order n.

(Without proof)

Uniqueness of Identity and Inverses

Instead of considering each group individually, we can prove statements for all groups at once.

Theorem

Every group $G = \langle S, \cdot \rangle$ has only one identity element and for each $x \in S$ the inverse of x is unique.

Uniqueness of Identity and Inverses

Instead of considering each group individually, we can prove statements for all groups at once.

Theorem

Every group $G = \langle S, \cdot \rangle$ has only one identity element and for each $x \in S$ the inverse of x is unique.

Proof.

identity: Assume that there are two identity elements $e, e' \in S$ with $e \neq e'$. Then for all $x \in S$ it holds that $x \cdot e = e \cdot x = x$ and that $x \cdot e' = e' \cdot x = x$. Using $x = e'$, we get $e' \cdot e = e'$ and using $x = e$ we get $e' \cdot e = e$, so overall $e' = e$. $\lightning$

inverse: homework assignment $\square$

We often denote the identity element with $\mathbf{1}$ and the inverse of x with x^{-1}.

Homomorphisms and Isomorphisms

Group Homomorphism

A group homomorphism is a mapping from one group to another that preserves group structure:

Definition (Group homomorphism)

Let $G = (S, \cdot)$ and $G' = (S', \circ)$ be groups.

A homomorphism from G to G' is a function $f : S \to S'$ such that for all $x, y \in S$ it holds that $f(x \cdot y) = f(x) \circ f(y)$.

Group Homomorphism

A group homomorphism is a mapping from one group to another that preserves group structure:

Definition (Group homomorphism)

Let $G = (S, \cdot)$ and $G' = (S', \circ)$ be groups.

A homomorphism from G to G' is a function $f : S \to S'$ such that for all $x, y \in S$ it holds that $f(x \cdot y) = f(x) \circ f(y)$.

Combining elements and then mapping gives the same result as mapping first and then combining:

$$\begin{array}{ccc} G \times G & \xrightarrow{\cdot} & G \\ \downarrow \langle f,f \rangle & & \downarrow f \\ G' \times G' & \xrightarrow{\circ} & G' \end{array}$$

Group Homomorphisms Preserve Identity

Theorem

Every group homomorphism f from $G = (S, \cdot)$ to $G' = (S', \circ)$ maps the identity element e of G to the identity element e' of G'.

Proof.

Since e is an identity element, it holds that $e = e \cdot e$ and thus $f(e) = f(e \cdot e)$.

Group Homomorphisms Preserve Identity

Theorem

Every group homomorphism f from $G = (S, \cdot)$ to $G' = (S', \circ)$ maps the identity element e of G to the identity element e' of G'.

Proof.

Since e is an identity element, it holds that $e = e \cdot e$ and thus $f(e) = f(e \cdot e)$.

With the homomorphism property, we get $f(e) = f(e) \circ f(e)$.

Group Homomorphisms Preserve Identity

Theorem

Every group homomorphism f from $G = (S, \cdot)$ to $G' = (S', \circ)$ maps the identity element e of G to the identity element e' of G'.

Proof.

Since e is an identity element, it holds that $e = e \cdot e$ and thus $f(e) = f(e \cdot e)$.

With the homomorphism property, we get $f(e) = f(e) \circ f(e)$.

Multiplying with $\circ$ by $f(e)^{-1}$ and using the associativity of $\circ$ gives $f(e) \circ f(e)^{-1} = (f(e) \circ f(e)) \circ f(e)^{-1} = f(e) \circ (f(e) \circ f(e)^{-1}) = f(e)$.

Group Homomorphisms Preserve Identity

Theorem

Every group homomorphism f from $G = (S, \cdot)$ to $G' = (S', \circ)$ maps the identity element e of G to the identity element e' of G'.

Proof.

Since e is an identity element, it holds that $e = e \cdot e$ and thus $f(e) = f(e \cdot e)$.

With the homomorphism property, we get $f(e) = f(e) \circ f(e)$.

Multiplying with $\circ$ by $f(e)^{-1}$ and using the associativity of $\circ$ gives $f(e) \circ f(e)^{-1} = (f(e) \circ f(e)) \circ f(e)^{-1} = f(e) \circ (f(e) \circ f(e)^{-1}) = f(e)$.

Since $f(e) \circ f(e)^{-1}$ is the identity element e' of G', it follows that $f(e) = e'$. □

Group Homomorphisms Map Inverses to Inverses

Theorem

Every group homomorphism f from $G = (S, \cdot)$ to $G' = (S', \circ)$ maps for every $x \in S$ its inverse x^{-1} to the inverse of $f(x)$.

Proof.

Consider an arbitrary $x \in S$.

Since $x \cdot x^{-1} = e$, where e is the identity element of G, we have $f(x) \circ f(x^{-1}) = f(x \cdot x^{-1}) = f(e)$.

Since homomorphisms preserve identity, $f(e)$ is the identity element e' of G'.

Thus, $f(x) \circ f(x^{-1}) = e'$ and $f(x^{-1})$ is the inverse of $f(x)$. □

Group Homomorphism – Example

- Consider $G = (\mathbb{Z}, +)$ and $H = (\{1, -1\}, \cdot)$ with

Group Homomorphism – Example

- Consider $G = (\mathbb{Z}, +)$ and $H = (\{1, -1\}, \cdot)$ with
  - $1 \cdot 1 = -1 \cdot -1 = 1$

Group Homomorphism – Example

- Consider $G = (\mathbb{Z}, +)$ and $H = (\{1, -1\}, \cdot)$ with
  - $1 \cdot 1 = -1 \cdot -1 = 1$
  - $1 \cdot -1 = -1 \cdot 1 = -1$

Group Homomorphism – Example

- Consider $G = (\mathbb{Z}, +)$ and $H = (\{1, -1\}, \cdot)$ with
  - $1 \cdot 1 = -1 \cdot -1 = 1$
  - $1 \cdot -1 = -1 \cdot 1 = -1$
- Let $f : \mathbb{Z} \to \{1, -1\}$ with $f(x) = \begin{cases} 1 & \text{if } x \text{ is even} \\ -1 & \text{if } x \text{ is odd} \end{cases}$

Group Homomorphism – Example

- Consider $G = (\mathbb{Z}, +)$ and $H = (\{1, -1\}, \cdot)$ with
  - $1 \cdot 1 = -1 \cdot -1 = 1$
  - $1 \cdot -1 = -1 \cdot 1 = -1$
- Let $f : \mathbb{Z} \to \{1, -1\}$ with $f(x) = \begin{cases} 1 & \text{if } x \text{ is even} \\ -1 & \text{if } x \text{ is odd} \end{cases}$
- f is a homomorphism from G to H:
  for all $x, y \in \mathbb{Z}$ it holds that

$$
\begin{aligned}
f(x+y) &= \begin{cases} 1 & \text{if } x+y \text{ is even} \\ -1 & \text{if } x+y \text{ is odd} \end{cases} \\
&= \begin{cases} 1 & \text{if } x \text{ and } y \text{ have the same parity} \\ -1 & \text{if } x \text{ and } y \text{ have different parity} \end{cases} \\
&= \begin{cases} 1 & \text{if } f(x) = f(y) \\ -1 & \text{if } f(x) \neq f(y) \end{cases} \\
&= f(x) \cdot f(y)
\end{aligned}
$$

Isomorphic Groups

Definition (Group Isomorphism)

A group homomorphism that is bijective is called a group isomorophism.

Groups G and H are called isomorphic (written $G \cong H$) if there is a group isomorphism from G to H.

From a practical perspective, isomorphic groups are identical up to renaming.

Group Isomorphism – Example

Consider the groups $G = \langle \mathbb{Z}, + \rangle$ and $H = \langle 2\mathbb{Z}, + \rangle$,
where $2\mathbb{Z}$ is the set of all even integers, and $+$ is addition.

Define $f : \mathbb{Z} \to 2\mathbb{Z}$ as $f(x) = 2x$.

- Homomorphism:

$$f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$$

- Bijective: every even integer $2x$ is the image of exactly one integer x.

$$\boxed{\langle \mathbb{Z}, + \rangle \cong \langle 2\mathbb{Z}, + \rangle}$$

Subgroups

Subgroup

Definition

A subgroup of a group $G = \langle S, \cdot \rangle$ is a group $H = \langle S', \circ \rangle$ with $S' \subseteq S$ and $\circ$ the restriction of $\cdot$ to $S' \times S'$.

- S' always contains the identity element and is closed under group operation and inverse.
- The image of a subgroup under a group homomorphism is a subgroup of the target group (without proof).

Subgroup – Example

Reminder: For every set M, the symmetric group $\mathrm{Sym}(M)$ is $\langle S, \cdot \rangle$, where

- S is the set of all permutations of M, and
- $\cdot$ denotes function composition,

Sometimes, we do not want to consider all possible permutations.

Subgroup – Example

Reminder: For every set M, the symmetric group $\mathrm{Sym}(M)$ is $\langle S, \cdot \rangle$, where

- S is the set of all permutations of M, and
- $\cdot$ denotes function composition,

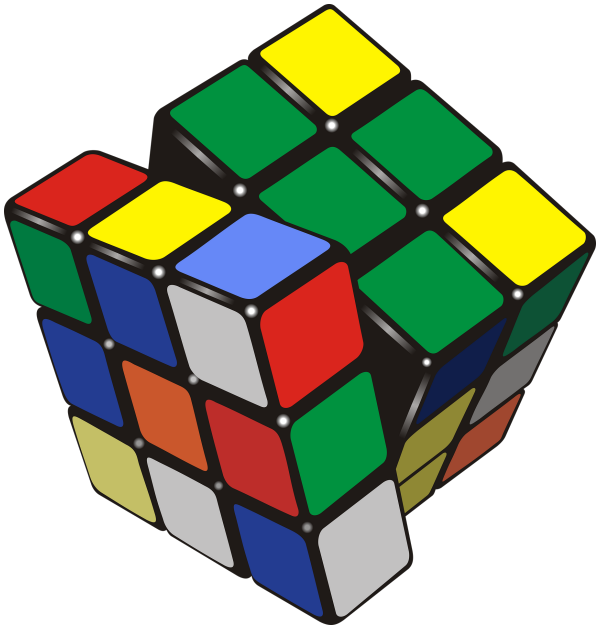
Sometimes, we do not want to consider all possible permutations.

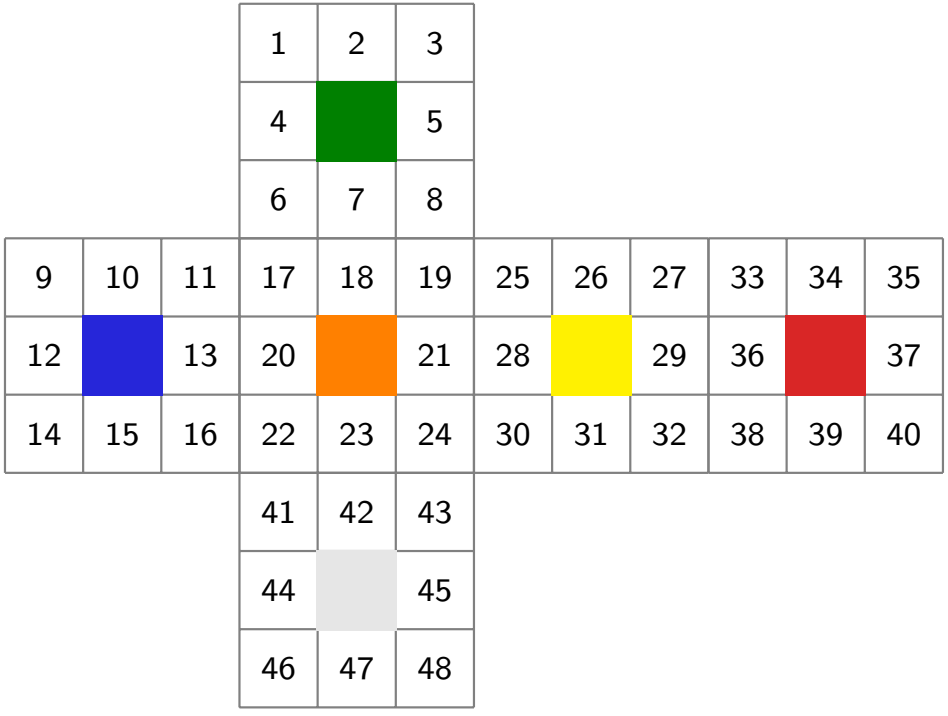
Definition (Permutation Group)

A permutation group is a group $G = \langle S, \cdot \rangle$,
where S is a set of permutations of some set M and
$\cdot$ is the composition of permutations in S.

Every permutation group is a subgroup of a symmetric group and every such subgroup is a permutation group.

Permutation Group – Example





- Consider all permutations achievable with valid moves.
- Subgroup of S_{48} with order
  $43\,252\,003\,274\,489\,856\,000 \approx 4.3 \cdot 10^{19}$ (43 quintillion)
- S_{48} has order $48! \approx 1.24 \cdot 10^{61}$

Generating Sets

Generating Sets

Definition

Let $G = \langle S, \circ \rangle$ be a group and $X \subseteq S$.

The subgroup generated by X, denoted by $\langle X \rangle$, is the smallest subgroup $G' = \langle S', \circ \rangle$ of G with $X \subseteq S'$.

If $\langle X \rangle = G$, then X is called a generating set of G.

A group is cyclic if there is a generating set consisting of only one element.

- Starting with the elements of X, we can obtain every element of S' by finitely often applying the group operation $\circ$ and taking inverses.
- The empty product is identity by definition, so the identity element is always in S'.

Example

Consider group $\langle \mathbb{Z}_6, +_6 \rangle$.
The inverses are $0 \leftrightarrow 0, 1 \leftrightarrow 5, 2 \leftrightarrow 4, 3 \leftrightarrow 3$.

What subgroup does $\{2\}$ generate?

Example

Consider group $\langle \mathbb{Z}_6, +_6 \rangle$.
The inverses are $0 \leftrightarrow 0, 1 \leftrightarrow 5, 2 \leftrightarrow 4, 3 \leftrightarrow 3$.

What subgroup does $\{2\}$ generate?
Group $\langle \{0, 2, 4\}, +_6 \rangle$

What subgroup does $\{1\}$ generate?

Example

Consider group $\langle \mathbb{Z}_6, +_6 \rangle$.
The inverses are $0 \leftrightarrow 0, 1 \leftrightarrow 5, 2 \leftrightarrow 4, 3 \leftrightarrow 3$.

What subgroup does $\{2\}$ generate?
Group $\langle \{0, 2, 4\}, +_6 \rangle$

What subgroup does $\{1\}$ generate?
Group $\langle \{0, 1, \ldots, 5\}, +_6 \rangle = \langle \mathbb{Z}_6, +_6 \rangle$
$\rightarrow \langle \mathbb{Z}_6, +_6 \rangle$ is cyclic.

Summary and Outlook

Summary

- A group is a set with an associative operation, an identity element, and inverses.
- A group homomorphism maps the elements of one group to elements of another group, preserving the group structure.
- A bijective homomorphism is an isomorphism.
- Isomorphic groups have the same structure (identical up to renaming).
- A subgroup of G is itself a group, formed from a subset of the elements of G.
- A set of elements generates a group if every element can be built from them and their inverses with the group operation.
- A group generated by one element is called cyclic.

Outlook

There are many other algebraic structures, e. g.

- Semi-group: requires only associativity
- Monoid: requires associativity and identity element
- Ringoids: algebraic structures with two binary operations
  - multiplication and addition
  - multiplication distributes over addition
  - e. g. ring and field