

Discrete Mathematics in Computer Science

Abstract Groups

Malte Helmert, Gabriele Röger

University of Basel

Abstract Algebra

- **Elementary algebra:** “Arithmetics with variables”

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 $a \neq 0$.

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 . . .

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

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

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

- **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).

Binary operations

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

Binary operations

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

Binary operations

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

Groups

Definition (Group)

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

Groups

Definition (Group)

A group $G = (S, \cdot)$ 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 $G = (S, \cdot)$ 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 $G = (S, \cdot)$ 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 $G = (S, \cdot)$ 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 $G = (S, \cdot)$ 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: $(\mathbb{Z}, +)$

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

$(\mathbb{Z}, +)$ 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 neutral 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 $x + (-x) = (-x) + x = 0$.

$(\mathbb{Z}, +)$ also is an **abelian group**

because for all $x, y \in \mathbb{Z}$ it holds that $x + y = y + x$.

Uniqueness of Identity and Inverses

Theorem

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

Uniqueness of Identity and Inverses

Theorem

Every group $G = (S, \cdot)$ 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 $e' = e$. \downarrow

inverse: homework assignment



Uniqueness of Identity and Inverses

Theorem

Every group $G = (S, \cdot)$ 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 $e' = e$. \downarrow

inverse: homework assignment □

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

Division – Right Quotient

Theorem

Let $G = (S, \cdot)$ be a group. Then for all $a, b \in S$ the equation $x \cdot b = a$ has exactly one solution x in S , namely $x = a \cdot b^{-1}$.

We call $a \cdot b^{-1}$ the right-quotient of a by b and also write it as a/b .

Division – Right Quotient

Theorem

Let $G = (S, \cdot)$ be a group. Then for all $a, b \in S$ the equation $x \cdot b = a$ has exactly one solution x in S , namely $x = a \cdot b^{-1}$.

We call $a \cdot b^{-1}$ the right-quotient of a by b and also write it as a/b .

Proof.

It is a solution: With $x = a \cdot b^{-1}$ it holds that
 $x \cdot b = (a \cdot b^{-1}) \cdot b = a \cdot (b^{-1} \cdot b) = a \cdot 1 = a$.



Division – Right Quotient

Theorem

Let $G = (S, \cdot)$ be a group. Then for all $a, b \in S$ the equation $x \cdot b = a$ has exactly one solution x in S , namely $x = a \cdot b^{-1}$.

We call $a \cdot b^{-1}$ the right-quotient of a by b and also write it as a/b .

Proof.

It is a solution: With $x = a \cdot b^{-1}$ it holds that $x \cdot b = (a \cdot b^{-1}) \cdot b = a \cdot (b^{-1} \cdot b) = a \cdot 1 = a$.

The solution is unique:

Assume x and x' are distinct solutions. Then $x \cdot b = a = x' \cdot b$. Multiplying both sides by b^{-1} , we get $(x \cdot b) \cdot b^{-1} = (x' \cdot b) \cdot b^{-1}$ and with associativity $x \cdot (b \cdot b^{-1}) = x' \cdot (b \cdot b^{-1})$.

With the axiom on inverse elements this leads to $x \cdot 1 = x' \cdot 1$ and with the axiom on the identity element ultimately to $x = x'$. ζ \square

Division – Left Quotient

Theorem

Let $G = (S, \cdot)$ be a group. Then for all $a, b \in S$ the equation $b \cdot x = a$ has exactly one solution x in S , namely $x = b^{-1} \cdot a$.

We call $b^{-1} \cdot a$ the left-quotient of a by b and also write it as $b \setminus a$.

Proof omitted

Quotients in Abelian Groups

Theorem

If $G = (S, \cdot)$ is an **abelian group** then it holds for all $x, y \in S$ that $x/y = y \setminus x$.

Proof.

Consider arbitrary $x, y \in S$. As \cdot is commutative, it holds that $x/y = x \cdot y^{-1} = y^{-1} \cdot x = y \setminus x$. □

Group Homomorphism

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

Definition (Group Isomorphism)

A **group homomorphism** that is **bijective** is called a **group isomorphism**. Groups G and H are called **isomorphic** if there is a group isomorphism from G to H .

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

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 $f : \mathbb{Z} \rightarrow \{1, -1\}$ 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 $f : \mathbb{Z} \rightarrow \{1, -1\}$ 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

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

Outlook

- A **subgroup** of $G = (S, \cdot)$ is a group $H = (S', \circ)$ 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
 - group homomorphisms preserve many properties of subgroups

Outlook

- A **subgroup** of $G = (S, \cdot)$ is a group $H = (S', \circ)$ 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
 - group homomorphisms preserve many properties of subgroups
- 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

Discrete Mathematics in Computer Science

Symmetric Group and Permutation Groups

Malte Helmert, Gabriele Röger

University of Basel

Reminder: Permutations



Definition (Permutation)

Let S be a set. A **bijection** $\pi : S \rightarrow S$ is called a **permutation of S** .

Symmetric Group

Theorem (Symmetric Group)

Let M be a set. Then $\text{Sym}(M) = (S, \cdot)$, 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 $M = \{1, \dots, n\}$, we also use S_n to refer to the symmetric group of M .

Symmetric Group

Theorem (Symmetric Group)

Let M be a set. Then $\text{Sym}(M) = (S, \cdot)$, 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 $M = \{1, \dots, n\}$, we also use S_n to refer to the symmetric group of M .

Is the symmetric group abelian?

Symmetric Group

Theorem (Symmetric Group)

Let M be a set. Then $\text{Sym}(M) = (S, \cdot)$, 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 $M = \{1, \dots, n\}$, 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 I

Theorem

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

Definition (Group)

A group $G = (S, \cdot)$ 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.

To show: closure, associativity, identity, inverse element

Symmetric Group – Proof II

Theorem

For set M , $\text{Sym}(M) = (\{\sigma : M \rightarrow M \mid \sigma \text{ is bijective}\}, \cdot)$ 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 $\text{id} : M \rightarrow M$ with $\text{id}(x) = x$ is a permutation and for every permutation σ of M it holds that $\sigma \text{id} = \text{id}\sigma = \sigma$.
- **Inverse element:** For every permutation σ of M , also the inverse function σ^{-1} is a permutation of M and has the required properties.



Generating Sets

Definition

A **generating set** of a group $G = (S, \circ)$ is a set $S' \subseteq S$ such that every $e \in S$ can be expressed as a combination (under \circ) of finitely many elements of S' and their inverses.

Empty product is identity by definition, so no need to have it in S' .

Generating Sets

Definition

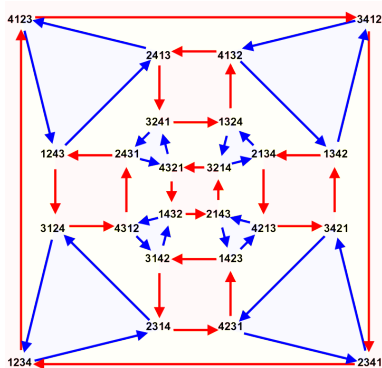
A **generating set** of a group $G = (S, \circ)$ is a set $S' \subseteq S$ such that every $e \in S$ can be expressed as a combination (under \circ) of finitely many elements of S' and their inverses.

Empty product is identity by definition, so no need to have it in S' .

- For $n \geq 2$, S_n is generated by $\{(i \ i+1) \mid i \in \{1, \dots, n-1\}\}$.
- For $n > 2$, S_n is generated by $\{(1 \ 2), (1 \ \dots \ n)\}$.

Generating Sets – Example

$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \right\}$ is a generating set of S_4 .



Permutation Group

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

Permutation Group

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

Definition (Permutation Group)

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

Permutation Group

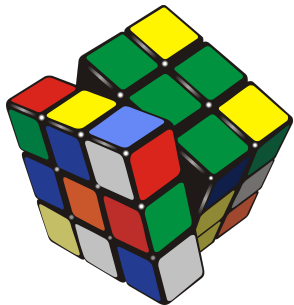
Sometimes, we do not want to consider **all** possible permutations.

Definition (Permutation Group)

A **permutation group** is a group $G = (S, \cdot)$, 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



			1	2	3						
			4	5	6						
			6	7	8						
9	10	11	17	18	19	25	26	27	33	34	35
12	13	14	20	21	22	28	29	30	36	37	38
14	15	16	22	23	24	30	31	32	38	39	40
			41	42	43						
			44	45	46						
			46	47	48						

- 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 $48! \approx 1.24 \cdot 10^{61}$