

Mathematics for Informatics

Algebra: Homomorphisms, permutations
(lecture 3 of 12)

Francesco DOLCE

dolcefra@cvut.cz

Czech Technical University in Prague

Winter 2026/2027

created: September 15, 2026, 14:13

The same groups and distinct elements (1/5)

$\mathbb{Z}_5^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The same groups and distinct elements (1/5)

$\mathbb{Z}_5^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

order: 4

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

order: 4

The same groups and distinct elements (1/5)

$\mathbb{Z}_5^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

order: 4

subgroups: $\{1\}$, $\{1, 4\}$, $\{1, 2, 3, 4\}$

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

order: 4

subgroups: $\{0\}$, $\{0, 2\}$, $\{0, 1, 2, 3\}$

The same groups and distinct elements (1/5)

$\mathbb{Z}_5^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

order: 4

subgroups: $\{1\}$, $\{1, 4\}$, $\{1, 2, 3, 4\}$

neutral element: 1

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

order: 4

subgroups: $\{0\}$, $\{0, 2\}$, $\{0, 1, 2, 3\}$

neutral element: 0

The same groups and distinct elements (1/5)

$\mathbb{Z}_5^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

order: 4

subgroups: $\{1\}$, $\{1, 4\}$, $\{1, 2, 3, 4\}$

neutral element: 1

inverse elements: $1^{-1} = 1$, $2^{-1} = 3$,
 $3^{-1} = 2$, $4^{-1} = 4$.

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

order: 4

subgroups: $\{0\}$, $\{0, 2\}$, $\{0, 1, 2, 3\}$

neutral element: 0

inverse elements: $-0 = 0$, $-1 = 3$,
 $-2 = 2$, $-3 = 1$.

The same groups and distinct elements (1/5)

$\mathbb{Z}_5^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

order: 4

subgroups: $\{1\}$, $\{1, 4\}$, $\{1, 2, 3, 4\}$

neutral element: 1

inverse elements: $1^{-1} = 1$, $2^{-1} = 3$,
 $3^{-1} = 2$, $4^{-1} = 4$.

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

order: 4

subgroups: $\{0\}$, $\{0, 2\}$, $\{0, 1, 2, 3\}$

neutral element: 0

inverse elements: $-0 = 0$, $-1 = 3$,
 $-2 = 2$, $-3 = 1$.

Aren't these two groups in fact the same group differing only in the "names" of their elements?

The same groups and distinct elements (2/5)

$\mathbb{Z}_5^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Let us try to rename the elements of the group $\mathbb{Z}_5^\times$ so to get $\mathbb{Z}_4^+$:

The same groups and distinct elements (2/5)

$\mathbb{Z}_5^\times$	0	2	3	4
0	0	2	3	4
2	2	4	0	3
3	3	0	4	2
4	4	3	2	0

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Let us try to rename the elements of the group $\mathbb{Z}_5^\times$ so to get $\mathbb{Z}_4^+$:

- The neutral element has very special and unique properties: we rename 1 to 0.

The same groups and distinct elements (2/5)

$\mathbb{Z}_5^\times$	0	2	3	2
0	0	2	3	2
2	2	2	0	3
3	3	0	2	2
2	2	3	2	0

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Let us try to rename the elements of the group $\mathbb{Z}_5^\times$ so to get $\mathbb{Z}_4^+$:

- The neutral element has very special and unique properties: we rename 1 to 0.
- If the complete structure should be preserved, then the only two-elements subgroup $\{1, 4\}$ (in $\mathbb{Z}_5^\times$) must correspond to the subgroup $\{0, 2\}$ (in $\mathbb{Z}_4^+$): we map $4 \leftrightarrow 2$.

The same groups and distinct elements (2/5)

$\mathbb{Z}_5^\times$	0	3	1	2
0	0	3	1	2
3	3	2	0	1
1	1	0	2	3
2	2	1	3	0

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Let us try to rename the elements of the group $\mathbb{Z}_5^\times$ so to get $\mathbb{Z}_4^+$:

- The neutral element has very special and unique properties: we rename 1 to 0.
- If the complete structure should be preserved, then the only two-elements subgroup $\{1, 4\}$ (in $\mathbb{Z}_5^\times$) must correspond to the subgroup $\{0, 2\}$ (in $\mathbb{Z}_4^+$): we map $4 \leftrightarrow 2$.
- Now, it remains to rename only 2 and 3; we can check that both remaining possibilities work; we choose, for instance, $3 \leftrightarrow 1$ and $2 \leftrightarrow 3$.

The same groups and distinct elements (2/5)

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Let us try to rename the elements of the group $\mathbb{Z}_5^\times$ so to get $\mathbb{Z}_4^+$:

- The neutral element has very special and unique properties: we rename 1 to 0.
- If the complete structure should be preserved, then the only two-elements subgroup $\{1, 4\}$ (in $\mathbb{Z}_5^\times$) must correspond to the subgroup $\{0, 2\}$ (in $\mathbb{Z}_4^+$): we map $4 \leftrightarrow 2$.
- Now, it remains to rename only 2 and 3; we can check that both remaining possibilities work; we choose, for instance, $3 \leftrightarrow 1$ and $2 \leftrightarrow 3$.
- It suffices to reorder the rows. . . and we have the Cayley table of $\mathbb{Z}_4^+$.

The same groups and distinct elements (3/5)

We have found a way to rename the elements in one table to gain an exact copy of the other table (after rearranging rows and columns).

The same groups and distinct elements (3/5)

We have found a way to rename the elements in one table to gain an exact copy of the other table (after rearranging rows and columns).

This renaming is actually an **injective** mapping of the set $\{1, 2, 3, 4\}$ **onto** the set $\{0, 1, 2, 3\}$; let us denote it φ_1 :

$$\varphi_1(1) = 0, \quad \varphi_1(2) = 3, \quad \varphi_1(3) = 1, \quad \varphi_1(4) = 2.$$

The same groups and distinct elements (3/5)

We have found a way to rename the elements in one table to gain an exact copy of the other table (after rearranging rows and columns).

This renaming is actually an **injective** mapping of the set $\{1, 2, 3, 4\}$ **onto** the set $\{0, 1, 2, 3\}$; let us denote it φ_1 :

$$\varphi_1(1) = 0, \quad \varphi_1(2) = 3, \quad \varphi_1(3) = 1, \quad \varphi_1(4) = 2.$$

We have pointed out that the mapping φ_2 works as well:

$$\varphi_2(1) = 0, \quad \varphi_2(2) = 1, \quad \varphi_2(3) = 3, \quad \varphi_2(4) = 2.$$

The same groups and distinct elements (3/5)

We have found a way to rename the elements in one table to gain an exact copy of the other table (after rearranging rows and columns).

This renaming is actually an **injective** mapping of the set $\{1, 2, 3, 4\}$ **onto** the set $\{0, 1, 2, 3\}$; let us denote it φ_1 :

$$\varphi_1(1) = 0, \quad \varphi_1(2) = 3, \quad \varphi_1(3) = 1, \quad \varphi_1(4) = 2.$$

We have pointed out that the mapping φ_2 works as well:

$$\varphi_2(1) = 0, \quad \varphi_2(2) = 1, \quad \varphi_2(3) = 3, \quad \varphi_2(4) = 2.$$

Would all bijections do the same job? And if not, what makes these two so special?

The same groups and distinct elements (4/5)

Let us rename the elements of the group $\mathbb{Z}_5^\times$ according to the bijection φ_3 :

$$\varphi_3(1) = 0, \quad \varphi_3(2) = 3, \quad \varphi_3(3) = 2, \quad \varphi_3(4) = 1.$$

$\mathbb{Z}_5^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The same groups and distinct elements (4/5)

Let us rename the elements of the group $\mathbb{Z}_5^\times$ according to the bijection φ_3 :

$$\varphi_3(1) = 0, \quad \varphi_3(2) = 3, \quad \varphi_3(3) = 2, \quad \varphi_3(4) = 1.$$

$\varphi_3(\mathbb{Z}_5^\times)$	0	3	2	1
0	0	3	2	1
3	3	1	0	2
2	2	0	1	3
1	1	2	3	0

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The resulting table is not the Cayley table of the group $\mathbb{Z}_4^+$, because, e.g., $3 + 3 \pmod{4} \neq 1$.

The same groups and distinct elements (4/5)

Let us rename the elements of the group $\mathbb{Z}_5^\times$ according to the bijection φ_3 :

$$\varphi_3(1) = 0, \quad \varphi_3(2) = 3, \quad \varphi_3(3) = 2, \quad \varphi_3(4) = 1.$$

$\varphi_3(\mathbb{Z}_5^\times)$	0	3	2	1
0	0	3	2	1
3	3	1	0	2
2	2	0	1	3
1	1	2	3	0

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The resulting table is not the Cayley table of the group $\mathbb{Z}_4^+$, because, e.g., $3 + 3 \pmod{4} \neq 1$.

The bijection φ_3 does not give rise to the same structure of the group $\mathbb{Z}_4^+$; only φ_1 and φ_2 have this property.

The same groups and distinct elements (5/5)

The desired property, which only the bijections φ_1 and φ_2 have, is the following:

for all $n, m \in \{1, 2, 3, 4\}$, we have $\varphi(n \times_5 m) = \varphi(n) +_4 \varphi(m)$,

where $\times_5$ denotes the operation in the group $\mathbb{Z}_5^\times$, and $+_4$ the one in the group $\mathbb{Z}_4^+$.

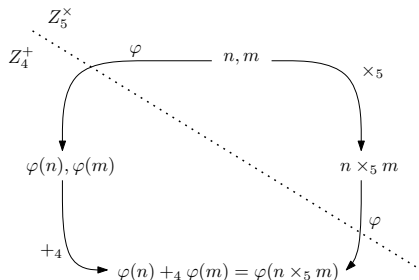
The same groups and distinct elements (5/5)

The desired property, which only the bijections φ_1 and φ_2 have, is the following:

for all $n, m \in \{1, 2, 3, 4\}$, we have $\varphi(n \times_5 m) = \varphi(n) +_4 \varphi(m)$,

where $\times_5$ denotes the operation in the group $\mathbb{Z}_5^\times$, and $+_4$ the one in the group $\mathbb{Z}_4^+$.

*In words: If we apply the operation $\times_5$ to two arbitrary elements of the group $\mathbb{Z}_5^\times$ and then we send the result to $\mathbb{Z}_4^+$ by φ , we obtain the same result as when we first transform by φ the elements to $\mathbb{Z}_4^+$ and **then** apply the operation $+_4$.*



Homomorphism and isomorphism

Definition

Let $G = (M, \circ_G)$ and $H = (N, \circ_H)$ be two groupoids. The mapping $\varphi : M \rightarrow N$ is a **homomorphism** from G to H if

$$\text{for all } x, y \in M, \text{ we have } \varphi(x \circ_G y) = \varphi(x) \circ_H \varphi(y).$$

If, moreover, φ is injective (resp. surjective, resp. bijective) we say that φ is a **monomorphism** (resp. **epimorphism**, resp. **isomorphism**).

Homomorphism and isomorphism

Definition

Let $G = (M, \circ_G)$ and $H = (N, \circ_H)$ be two groupoids. The mapping $\varphi : M \rightarrow N$ is a **homomorphism** from G to H if

$$\text{for all } x, y \in M, \text{ we have } \varphi(x \circ_G y) = \varphi(x) \circ_H \varphi(y).$$

If, moreover, φ is injective (resp. surjective, resp. bijective) we say that φ is a **monomorphism** (resp. **epimorphism**, resp. **isomorphism**).

A homomorphism preserves the structure given by the binary operation: the result is the same if we first apply the operation and then the homomorphism or if we proceed inversely.

The only thing needed to define a homomorphism is that the set is closed under the binary operation; this is why we have defined homomorphism for the most general structures, i.e., groupoids.

Isomorphic groups

Definition

*If there exists an isomorphism between two groups, these groups are **isomorphic**.*

Isomorphic groups

Definition

*If there exists an isomorphism between two groups, these groups are **isomorphic**.*

Example

The two groups $\mathbb{Z}_5^\times$ and $\mathbb{Z}_4^+$ are isomorphic. We have even found two distinct isomorphisms: φ_1 and φ_2 .

Isomorphic groups

Definition

*If there exists an isomorphism between two groups, these groups are **isomorphic**.*

Example

The two groups $\mathbb{Z}_5^\times$ and $\mathbb{Z}_4^+$ are isomorphic. We have even found two distinct isomorphisms: φ_1 and φ_2 .

Isomorphic groups have the same order.

Fundamental properties of homomorphisms (1/2)

Theorem

Let φ be a homomorphism from a group $G = (M, \circ_G)$ to a group $H = (N, \circ_H)$.
The group $\varphi(G) = (\varphi(M), \circ_H)$ is a subgroup of H .

Fundamental properties of homomorphisms (1/2)

Theorem

Let φ be a homomorphism from a group $G = (M, \circ_G)$ to a group $H = (N, \circ_H)$.
The group $\varphi(G) = (\varphi(M), \circ_H)$ is a subgroup of H .

Proof.

Each element in $\varphi(G)$ can be written as $\varphi(x)$ for some $x \in M$.

Fundamental properties of homomorphisms (1/2)

Theorem

Let φ be a homomorphism from a group $G = (M, \circ_G)$ to a group $H = (N, \circ_H)$.
The group $\varphi(G) = (\varphi(M), \circ_H)$ is a subgroup of H .

Proof.

Each element in $\varphi(G)$ can be written as $\varphi(x)$ for some $x \in M$.

- For all $x, y, z \in M$ we have that

$$\begin{aligned}(\varphi(x) \circ_H \varphi(y)) \circ_H \varphi(z) &= \varphi(x \circ_G y) \circ_H \varphi(z) = \varphi((x \circ_G y) \circ_G z) = \\ &= \varphi(x \circ_G (y \circ_G z)) = \varphi(x) \circ_H \varphi(y \circ_G z) = \varphi(x) \circ_H (\varphi(y) \circ_H \varphi(z))\end{aligned}$$

Fundamental properties of homomorphisms (1/2)

Theorem

Let φ be a homomorphism from a group $G = (M, \circ_G)$ to a group $H = (N, \circ_H)$. The group $\varphi(G) = (\varphi(M), \circ_H)$ is a subgroup of H .

Proof.

Each element in $\varphi(G)$ can be written as $\varphi(x)$ for some $x \in M$.

- For all $x, y, z \in M$ we have that

$$\begin{aligned}(\varphi(x) \circ_H \varphi(y)) \circ_H \varphi(z) &= \varphi(x \circ_G y) \circ_H \varphi(z) = \varphi((x \circ_G y) \circ_G z) = \\ &= \varphi(x \circ_G (y \circ_G z)) = \varphi(x) \circ_H \varphi(y \circ_G z) = \varphi(x) \circ_H (\varphi(y) \circ_H \varphi(z))\end{aligned}$$

- Denote by e_G the neutral element in G . Then $\varphi(e_G)$ is the neutral element in $\varphi(G)$ because, for all $x \in M$, we have $\varphi(e_G) \circ_H \varphi(x) = \varphi(e_G \circ_G x) = \varphi(x)$.

Fundamental properties of homomorphisms (1/2)

Theorem

Let φ be a homomorphism from a group $G = (M, \circ_G)$ to a group $H = (N, \circ_H)$. The group $\varphi(G) = (\varphi(M), \circ_H)$ is a subgroup of H .

Proof.

Each element in $\varphi(G)$ can be written as $\varphi(x)$ for some $x \in M$.

- For all $x, y, z \in M$ we have that

$$\begin{aligned}(\varphi(x) \circ_H \varphi(y)) \circ_H \varphi(z) &= \varphi(x \circ_G y) \circ_H \varphi(z) = \varphi((x \circ_G y) \circ_G z) = \\ &= \varphi(x \circ_G (y \circ_G z)) = \varphi(x) \circ_H \varphi(y \circ_G z) = \varphi(x) \circ_H (\varphi(y) \circ_H \varphi(z))\end{aligned}$$

- Denote by e_G the neutral element in G . Then $\varphi(e_G)$ is the neutral element in $\varphi(G)$ because, for all $x \in M$, we have $\varphi(e_G) \circ_H \varphi(x) = \varphi(e_G \circ_G x) = \varphi(x)$.
- It can be shown similarly that the inverse of $\varphi(x)$ is $\varphi(x^{-1})$. □

Fundamental properties of homomorphisms (2/2)

Consequences of the previous theorem and its proof:

- A homomorphism always maps the neutral element of one group to the neutral element of the other group.

Fundamental properties of homomorphisms (2/2)

Consequences of the previous theorem and its proof:

- A homomorphism always maps the neutral element of one group to the neutral element of the other group.
- Inverse elements are preserved as well: $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Fundamental properties of homomorphisms (2/2)

Consequences of the previous theorem and its proof:

- A homomorphism always maps the neutral element of one group to the neutral element of the other group.
- Inverse elements are preserved as well: $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Example

$$\begin{aligned}\varphi : \mathbb{Z}_4^+ &\rightarrow \mathbb{Z}_8^+ \\ n &\mapsto 2n\end{aligned}$$

is a homomorphism and $\varphi(\mathbb{Z}_4^+)$ is the subgroup $\{0, 2, 4, 6\} \leq \mathbb{Z}_8^+$.

... up to isomorphism (1/2)

Isomorphic groups are in fact identical, they differ only in the names of their elements (as we have seen in the case of groups $\mathbb{Z}_4^+$ and $\mathbb{Z}_5^\times$).

If we say that there exists one group with a certain property **up to isomorphism**, it means that all groups with this property are isomorphic to each other.

We prove three well-known statements of this kind.

... up to isomorphism (1/2)

Isomorphic groups are in fact identical, they differ only in the names of their elements (as we have seen in the case of groups $\mathbb{Z}_4^+$ and $\mathbb{Z}_5^\times$).

If we say that there exists one group with a certain property **up to isomorphism**, it means that all groups with this property are isomorphic to each other.

We prove three well-known statements of this kind.

Theorem

- *Any two infinite cyclic groups are isomorphic.*
- *For each $n \in \mathbb{N}$, any two cyclic groups of order n are isomorphic.*

... up to isomorphism (1/2)

Isomorphic groups are in fact identical, they differ only in the names of their elements (as we have seen in the case of groups $\mathbb{Z}_4^+$ and $\mathbb{Z}_5^\times$).

If we say that there exists one group with a certain property **up to isomorphism**, it means that all groups with this property are isomorphic to each other.

We prove three well-known statements of this kind.

Theorem

- *Any two infinite cyclic groups are isomorphic.*
- *For each $n \in \mathbb{N}$, any two cyclic groups of order n are isomorphic.*

Proof: hint.

Let $G = \langle a \rangle$ be a cyclic group with generator a .

We show that an arbitrary infinite cyclic group is isomorphic to the group $(\mathbb{Z}, +)$, and that an arbitrary cyclic group of order n is isomorphic to $\mathbb{Z}_n^+$.

The rest follows from the transitivity of the relation “to be isomorphic”. □

... up to isomorphism (1/2)

Isomorphic groups are in fact identical, they differ only in the names of their elements (as we have seen in the case of groups $\mathbb{Z}_4^+$ and $\mathbb{Z}_5^\times$).

If we say that there exists one group with a certain property **up to isomorphism**, it means that all groups with this property are isomorphic to each other.

We prove three well-known statements of this kind.

Theorem

- Any two infinite cyclic groups are isomorphic.
- For each $n \in \mathbb{N}$, any two cyclic groups of order n are isomorphic.

Proof: hint.

Let $G = \langle a \rangle$ be a cyclic group with generator a .

We show that an arbitrary infinite cyclic group is isomorphic to the group $(\mathbb{Z}, +)$, and that an arbitrary cyclic group of order n is isomorphic to $\mathbb{Z}_n^+$.

The rest follows from the transitivity of the relation “to be isomorphic”. □

$(\mathbb{Z}, +)$ and $\mathbb{Z}_n^+$ are the only cyclic groups up to isomorphism.

... up to isomorphism (2/2)

The **Klein group** is the group $(\mathbb{Z}_2 \times \mathbb{Z}_2, \circ)$, where

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$$

and $\circ$ is the component-wise addition modulo 2: e.g., $(1, 0) \circ (1, 1) = (0, 1)$.

... up to isomorphism (2/2)

The **Klein group** is the group $(\mathbb{Z}_2 \times \mathbb{Z}_2, \circ)$, where

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$$

and $\circ$ is the component-wise addition modulo 2: e.g., $(1, 0) \circ (1, 1) = (0, 1)$.

The Klein group is not cyclic and thus cannot be isomorphic to $\mathbb{Z}_4^+$!

It is possible to show this (try it, it is easy):

Theorem

There exists only two groups of order 4 which are not isomorphic.

$\mathbb{Z}_4^+$ and the Klein group are the only two groups of order 4 up to isomorphism.

Permutations (1/2)

The **symmetric group** S_n of the set of all permutations over $\{1, 2, 3, \dots, n\}$ with the operation of composition.

Permutations (1/2)

The **symmetric group** $\mathcal{S}_n$ of the set of all permutations over $\{1, 2, 3, \dots, n\}$ with the operation of composition.

- A (**n -**)**permutation** is a bijection of the set $\{1, 2, 3, \dots, n\}$ to itself, so $\mathcal{S}_n$ is the set of bijections on $\{1, 2, 3, \dots, n\}$.

Permutations (1/2)

The **symmetric group** $\mathcal{S}_n$ of the set of all permutations over $\{1, 2, 3, \dots, n\}$ with the operation of composition.

- A (**n -**)**permutation** is a bijection of the set $\{1, 2, 3, \dots, n\}$ to itself, so $\mathcal{S}_n$ is the set of bijections on $\{1, 2, 3, \dots, n\}$.
- Each permutation $\pi \in \mathcal{S}_n$ can be defined by listing its values:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \pi(1) & \pi(2) & \pi(3) & \cdots & \pi(n) \end{pmatrix}.$$

The first row could be deleted, and so, e.g., $(1 \ 2 \ 4 \ 3 \ 5) \in \mathcal{S}_5$ is the permutation swapping elements **3** and **4**.

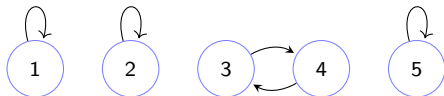
Permutations (1/2)

The **symmetric group** $\mathcal{S}_n$ of the set of all permutations over $\{1, 2, 3, \dots, n\}$ with the operation of composition.

- A (**n -permutation**) is a bijection of the set $\{1, 2, 3, \dots, n\}$ to itself, so $\mathcal{S}_n$ is the set of bijections on $\{1, 2, 3, \dots, n\}$.
- Each permutation $\pi \in \mathcal{S}_n$ can be defined by listing its values:

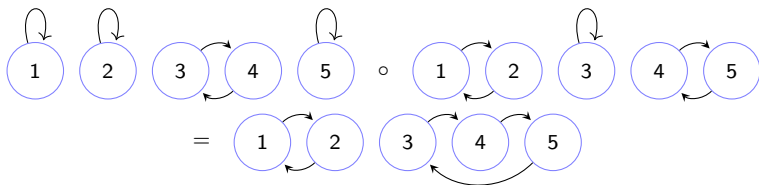
$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \pi(1) & \pi(2) & \pi(3) & \cdots & \pi(n) \end{pmatrix}.$$

The first row could be deleted, and so, e.g., $(1 \ 2 \ 4 \ 3 \ 5) \in \mathcal{S}_5$ is the permutation swapping elements **3** and **4**.



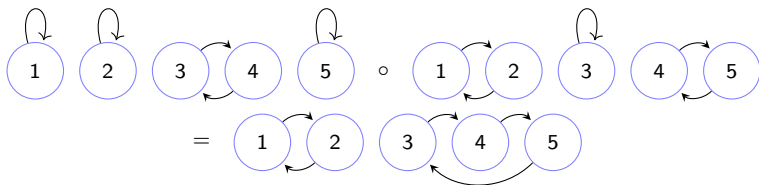
Permutations (2/2)

- Composition of permutations: $(1\ 2\ 4\ 3\ 5) \circ (2\ 1\ 3\ 5\ 4) = (2\ 1\ 4\ 5\ 3)$.



Permutations (2/2)

- Composition of permutations: $(1\ 2\ 4\ 3\ 5) \circ (2\ 1\ 3\ 5\ 4) = (2\ 1\ 4\ 5\ 3)$.



- The composition of permutations is associative, the permutation $(1\ 2\ 3\ \dots\ n)$ is the neutral element, and the inverse element is the inverse permutation. Hence, $\mathcal{S}_n$ is a group of order $n! = n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1$.

Group of permutations

Subgroups of the symmetric group $\mathcal{S}_n$ are called **groups of permutations**.

Example

The permutation $(1\ 2\ 4\ 3\ 5) \in \mathcal{S}_5$ swapping the elements 3 and 4 generates a subgroup of $\mathcal{S}_5$ containing two elements: $(1\ 2\ 4\ 3\ 5)$ and $(1\ 2\ 3\ 4\ 5)$.

Group of permutations

Subgroups of the symmetric group $\mathcal{S}_n$ are called **groups of permutations**.

Example

The permutation $(1\ 2\ 4\ 3\ 5) \in \mathcal{S}_5$ swapping the elements 3 and 4 generates a subgroup of $\mathcal{S}_5$ containing two elements: $(1\ 2\ 4\ 3\ 5)$ and $(1\ 2\ 3\ 4\ 5)$.

The structure of the subgroups of $\mathcal{S}_n$ is very (in some sense maximally) rich:

Theorem (Cayley)

Each finite group is isomorphic to some group of permutations.

Proof: hint only for interested.

Let a be an element of a group G of order n with a binary operation $\circ$. Put $\pi_a(x) = a \circ x$. Since in any group we can divide uniquely, π_a is a bijection and thus a permutation. The desired monomorphism is the mapping defined for each element a in this way: $\varphi(a) = \pi_a$. □