Group Theory

Involutions

by Lukas Wrana

Table of contents

Chapter 01

Fundamentals

Definition

A **Group** is an ordered pair $(G, *)$ of a set G and a binary operator

$$* : \begin{cases} G \times G \to G \\ (a, b) \mapsto a * b \\ \end{cases}$$

that satisfies the group axioms:

- **Associativity**

  $$\forall a, b, c \in G : \quad (a * b) * c = a * (b * c)$$

- **Identity element**

  $\exists e \in G$ such that $\forall a \in G : \quad a * e = e * a = a$

- **Inverse element**

  $$\forall g \in G \; \exists a^{-1} \in G : \quad a * a^{-1} = a^{-1} * a = e$$

Definition

Given two groups, $(G, *)$ and $(H, \cdot)$, a **group homomorphism** from $(G, *)$ to $(H, \cdot)$ is a function

$$f: G \to H$$

such that $\forall u, v \in G$ it holds that

$$f(u * v) = f(u) \cdot f(v)$$

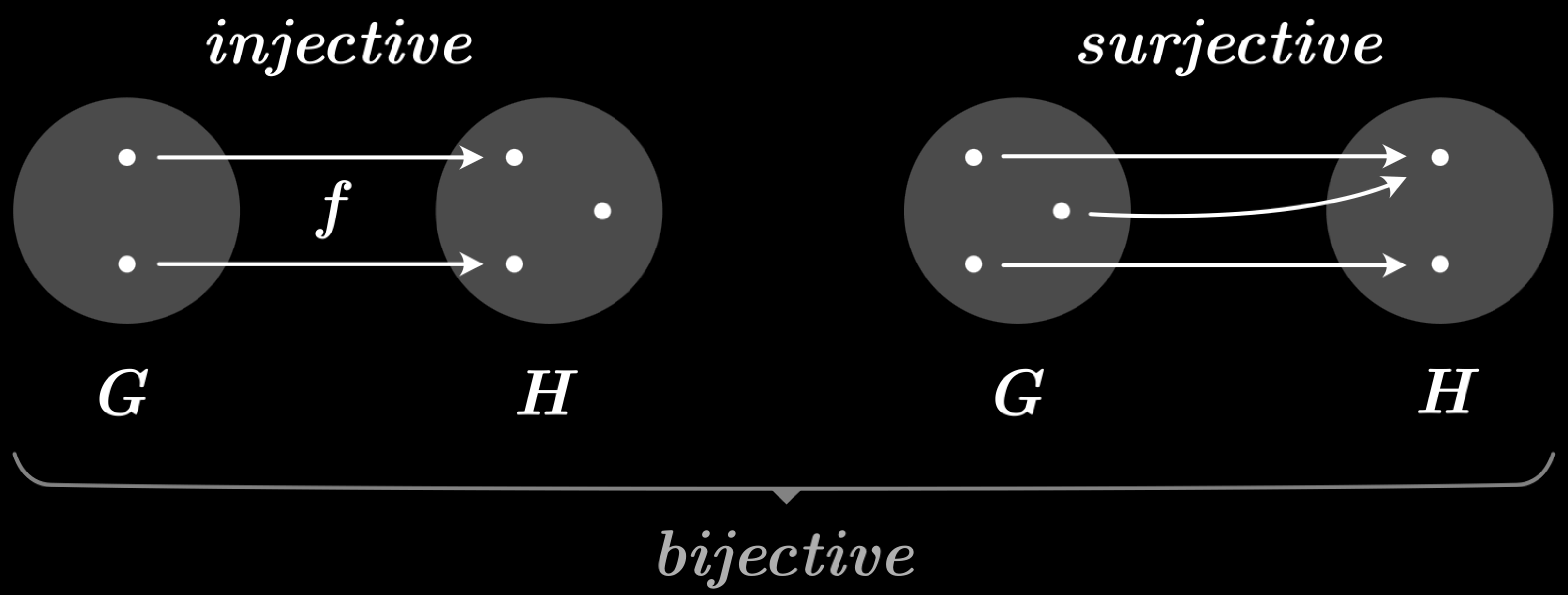
Further remarks

From this property, we can also deduce that

- $f(e_G) = e_H$
- $f(u^{-1}) = h(u)^{-1}$

Definition

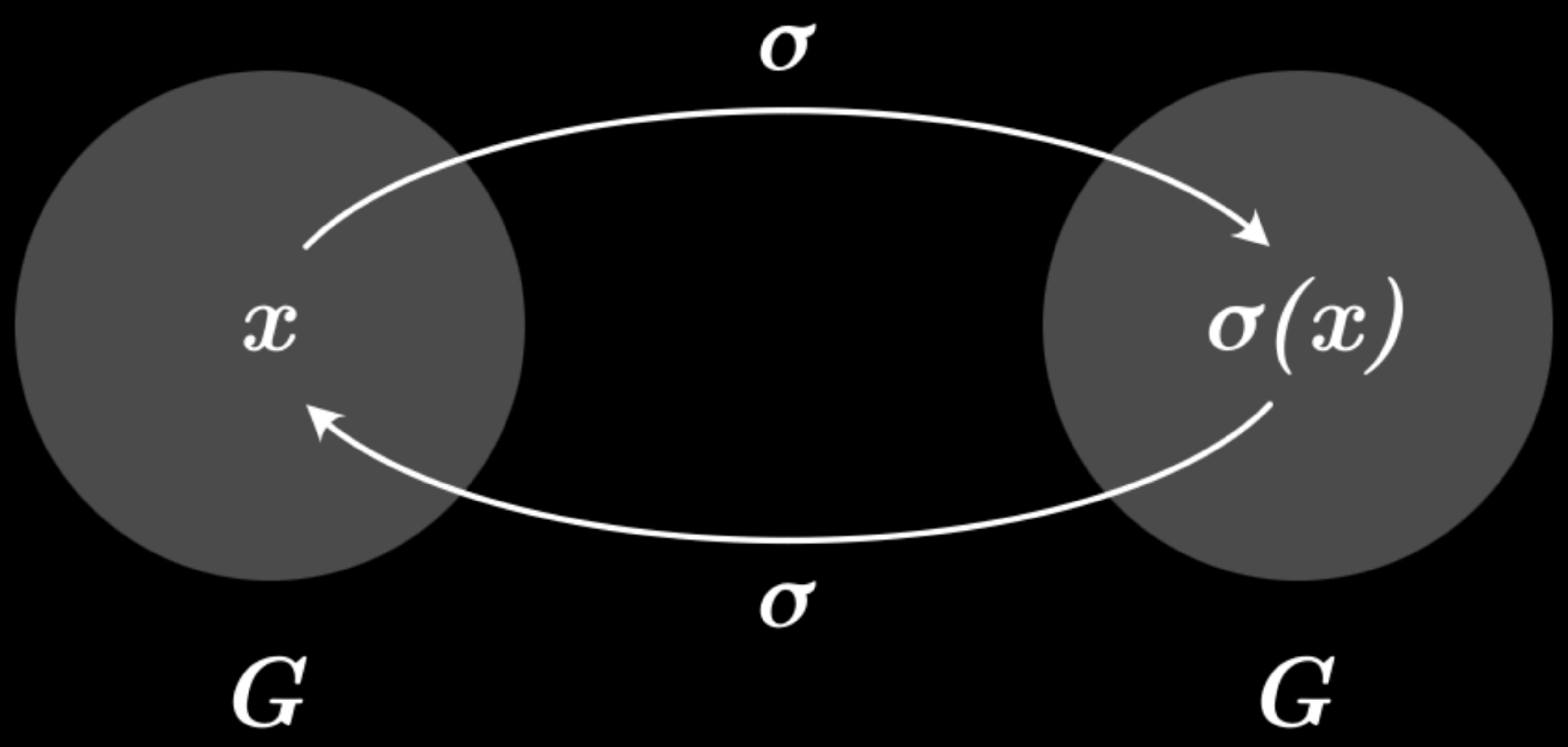
An **automorphism** is a bijective homomorphism of an object into itself.



Definiton

Given a group $(G, *)$, a group automorphism σ is an **involution**, if

$$\sigma(\sigma(x)) = x \qquad \forall x \in G$$



Definiton

An involution σ on a group $(G, *)$ has **<u>no non-trivial-fixpoints</u>** if the identity element $e \in G$ is the only fixpoint of σ:

$$\forall g \in G : \quad (\ \sigma(g) = g \Rightarrow g = e\ )$$

We call $e \in G$ a trivial fixpoint of σ.

Lemma

Every group $(G, *)$ has a trivial involution, namely the identity id.

proof:

Let $(G, *)$ be an arbitrary Group. For every $x \in G$:

$$x = \mathrm{id}(x) = \mathrm{id}(\mathrm{id}(x))$$

$\Rightarrow$ id is an involution.

$\square$

Example

Real negation

$$-:\begin{cases}\mathbb{R}\to\mathbb{R},\\ x\mapsto -x\end{cases}$$

is an involution on $(\mathbb{R},+)$.

proof:

For $x,y\in\mathbb{R}$:

$$-(x+y)=-x+(-y)$$

and

$$x=-(-x)=-(-(x))$$

... $\Rightarrow$ real negation is an involution on $(\mathbb{R},+)$.

Chapter 02

Main theorem

Theorem

Let $(G, *)$ be a finite group. If an involution with no non-trivial fixpoints on $(G, *)$ exists, then $(G, *)$ is commutative.

proof: Later ...

Lemma

Let $(G, *)$ be a finite group and σ be an involution on G. If σ has no non-trivial fixpoints, then:

$$\forall g \in G\ \exists x \in G : \quad g = x^{-1} * \sigma(x)$$

proof:

In essence, we want to show surjectivity of a function:

$$x \mapsto x^{-1} * \sigma(x)$$

Because G is finite, we can conclude surjectivity by injectivity.

So, lets prove injectivity...

Suppose $x, y \in G$ with $x^{-1} * \sigma(x) = y^{-1} * \sigma(y)$.

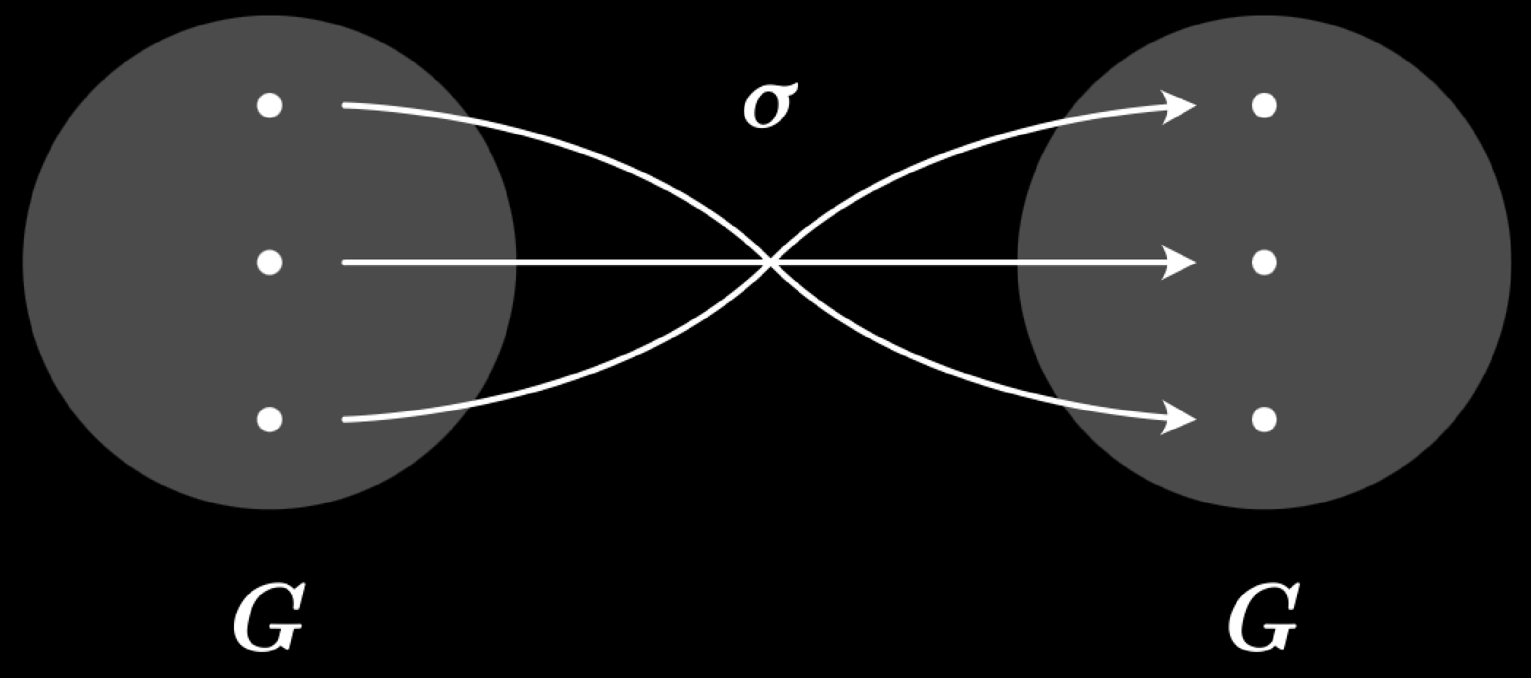
$$\begin{align}
x &= \sigma(\sigma(x)) \tag{1}\\
&= \sigma(x * x^{-1} * \sigma(x)) \tag{2}\\
&= \sigma(x * y^{-1} * \sigma(y)) \tag{3}\\
&= \sigma(x) * \sigma(y^{-1}) * \sigma(\sigma(y)) \tag{4}\\
&= \sigma(x) * \sigma(y^{-1}) * y \tag{5}
\end{align}$$

$$\begin{align}
\Rightarrow x * y^{-1} &= \sigma(x) * \sigma(y^{-1}) \tag{6}\\
&= \sigma(x * y^{-1}) \tag{7}
\end{align}$$

We have no non-trivial fixpoints, so $x * y^{-1}$ has to be the trivial fixpoint:

$$\begin{aligned}
\Rightarrow \quad x * y^{-1} &= e \\
\Leftrightarrow \quad x &= y
\end{aligned}$$

$\Rightarrow x \mapsto x^{-1} * \sigma(x)$ is injective.



Since G is finite, we can conclude that $x \mapsto x^{-1} * \sigma(x)$ is also surjective on G.

$$\Rightarrow \forall g \in G\ \exists x \in G : \quad g = x^{-1} * \sigma(x)$$

$\square$

Lemma

Let $(G, *)$ be a finite group and σ be an involution on G. If σ has no non-trivial fixpoints, then:

$$\forall g \in G : \quad \sigma(g) = g$$

proof:

In the previous Lemma, we showed that

$$\forall g \in G \; \exists x \in G : \quad g = x^{-1} * \sigma(x)$$

We can expand on that result:

$$\begin{aligned} \Rightarrow \sigma(g) &= \sigma(x^{-1} * \sigma(x)) && (8) \\ &= \sigma(x^{-1}) * \sigma(\sigma(x)) && (9) \\ &= \sigma(x^{-1}) * x && (10) \\ &= (\sigma(x))^{-1} * x && (11) \\ &= (x^{-1} * \sigma(x))^{-1} && (12) \\ &= g^{-1} && (13) \end{aligned}$$

□

Theorem

Let $(G, *)$ be a finite group. If an involution with no non-trivial fixpoints on $(G, *)$ exists, then $(G, *)$ is commutative.

proof:

Let $a, b \in G$.

$$\begin{aligned} a * b &= (a^{-1})^{-1} * (b^{-1})^{-1} && (14) \\ &= (b^{-1} * a^{-1})^{-1} && (15) \\ &= \sigma(b^{-1} * a^{-1}) && (16) \\ &= \sigma(b^{-1}) * \sigma(a^{-1}) && (17) \\ &= b * a && (18) \end{aligned}$$

$\Rightarrow (G, *)$ is commutative

$\square$

Chapter 03

Counter example

Definiton

A **free group** $(Fs, *)$ over a given set S consists of all words that can be build by elements of S or their inverse.

Elements of S are called **generators**. Two constructed words are considered different unless their equality follows from the group axioms.

Universal property

Given any function f from S to a group $(G, *)$, there exists a unique homomorphism

$$\phi : \quad F_S \mapsto G$$

$$\begin{tikzcd}
 & F_S \arrow[dr, dashed, "\Phi"] & \\
S \arrow[ur] \arrow[rr, "f"'] & & G
\end{tikzcd}$$

Counter-Example

We will look at a free group $(F_2, *)$ on two generators $\{a, b\}$:

$$e, \quad ab, \quad a^{-1}bb, \quad a^{-1}bbaab^{-1}a, \quad \ldots$$

We can define an automorphism s that swaps the generators over a free group $(F_2, *)$.

$$s(x) := \begin{cases} a, & \text{if } x = b \\ b, & \text{if } x = a \end{cases}$$

This function is just defined on the generators, but by the universal property of free groups, it also constructs a unique automorphism on the whole group.