Homomorphisms

Sasha Patotski

Cornell University

ap744@cornell.edu

November 18, 2015
Last time

Definition

For $\sigma \in S_n$ define $\text{inv}(\sigma)$ to be the number of pairs $(ij)$ such that $i < j$ but $\sigma(i) > \sigma(j)$. This number $\text{inv}(\sigma)$ is called the number of inversions of $\sigma$.

Definition

Define the sign of $\sigma$ to be $\text{sgn}(\sigma) = (-1)^{\text{inv}(\sigma)}$.

For two permutations $\sigma, \tau$ we have $\text{sgn}(\sigma \circ \tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$.

Definition

Let $A_n \subset S_n$ be the subset consisting of even permutations. $A_n$ is called an alternating group (we have proved that this is indeed a group!).
Abstract group definition

Since most of you have seen this already, there is no reason to hide it.

Definition

A group $G$ is a set with a binary operation $* : G \times G \to G$ called multiplication such that

1. it’s associative, i.e. $(a * b) * c = a * (b * c)$;
2. there is an element $e \in G$, called unit, s.t. $a * e = e * a = a$ for all $a \in G$;
3. for any $a \in G$ there is an element $a^{-1}$, called $a$’s inverse, such that $a * a^{-1} = a^{-1} * a = e$

Definition

A subgroup of a group $G$ is a subset which is itself a group (with the multiplication induced from $G$).
If $G, H$ are groups, a map $\varphi : G \rightarrow H$ is called a **homomorphism** if

$$\varphi(a \ast b) = \varphi(a) \ast \varphi(b)$$
Homomorphism

**Definition**

If $G, H$ are groups, a map $\varphi : G \to H$ is called a **homomorphism** if

$$\varphi(a \ast b) = \varphi(a) \ast \varphi(b)$$

- Prove that for a homomorphism $\varphi$, necessarily $\varphi(e_G) = e_H$ and $\varphi(a^{-1}) = \varphi(a)^{-1}$. 

---

Sasha Patotski (Cornell University)
Homomorphism

Definition

If $G, H$ are groups, a map $\varphi: G \to H$ is called a **homomorphism** if

$$\varphi(a * b) = \varphi(a) * \varphi(b)$$

- Prove that for a homomorphism $\varphi$, necessarily $\varphi(e_G) = e_H$ and $\varphi(a^{-1}) = \varphi(a)^{-1}$.
- Let $\mathbb{Z}^\times$ denote the group $\{1, -1\}$ with the usual multiplication of integers. Prove that it is a group.
Homomorphism

**Definition**

If $G$, $H$ are groups, a map $\varphi : G \to H$ is called a **homomorphism** if

$$\varphi(a \ast b) = \varphi(a) \ast \varphi(b)$$

- Prove that for a homomorphism $\varphi$, necessarily $\varphi(e_G) = e_H$ and $\varphi(a^{-1}) = \varphi(a)^{-1}$.
- Let $\mathbb{Z}^\times$ denote the group $\{1, -1\}$ with the usual multiplication of integers. Prove that it is a group.

**Definition**

The **kernel** of a homomorphism $\varphi$ is $\ker \varphi = \{a \in G \mid \varphi(a) = e\}$

The **image** of a homomorphism $\varphi$ is $\operatorname{im} \varphi = \{\varphi(a) \in H \mid a \in G\}$
Homomorphism

**Definition**

If $G, H$ are groups, a map $\varphi : G \to H$ is called a **homomorphism** if

$$\varphi(a \ast b) = \varphi(a) \ast \varphi(b)$$

1. Prove that for a homomorphism $\varphi$, necessarily $\varphi(e_G) = e_H$ and $\varphi(a^{-1}) = \varphi(a)^{-1}$.
2. Let $\mathbb{Z}^\times$ denote the group $\{1, -1\}$ with the usual multiplication of integers. Prove that it is a group.

**Definition**

The **kernel** of a homomorphism $\varphi$ is $\ker \varphi = \{ a \in G \mid \varphi(a) = e \}$

The **image** of a homomorphism $\varphi$ is $\text{im } \varphi = \{ \varphi(a) \in H \mid a \in G \}$

1. Prove that $\ker \varphi$ and $\text{im } \varphi$ are subgroups of $G$ and $H$, respectively.
Thus, $sgn$ gives a homomorphism

$$sgn: S_n \to \mathbb{Z}^\times$$
Thus, $sgn$ gives a **homomorphism**

$$sgn: S_n \rightarrow \mathbb{Z}^\times$$

- Alternating group $A_n$ is just the kernel $A_n = \ker(sgn)$. 
Thus, $sgn$ gives a \textbf{homomorphism}

$$sgn: S_n \rightarrow \mathbb{Z}^\times$$

Alternating group $A_n$ is just the kernel $A_n = \ker(sgn)$.

**Definition**

A homomorphism $\varphi: G \rightarrow H$ is called an \textbf{isomorphism} if $\varphi$ is a bijection. Two groups $G, H$ are called \textbf{isomorphic} if there exists an isomorphism $\varphi: G \rightarrow H$. 
Thus, $sgn$ gives a **homomorphism**

$$sgn: S_n \rightarrow \mathbb{Z}^\times$$

Alternating group $A_n$ is just the kernel $A_n = \ker(sgn)$.

**Definition**

A homomorphism $\varphi: G \rightarrow H$ is called an **isomorphism** if $\varphi$ is a bijection. Two groups $G, H$ are called **isomorphic** if there exists an isomorphism $\varphi: G \rightarrow H$.

Isomorphic groups are considered “the same” in group theory.
For all the homomorphisms below, what are their kernels and images?

- Between any groups $G, H$ there is a trivial homomorphism $\varphi : G \rightarrow H$, given by $\varphi(g) = e_H$, for all $g \in G$. 

The map $n \mapsto n \pmod{m}$ defines a homomorphism $\mathbb{Z} \rightarrow \mathbb{Z}/m$. 

Let $\text{GL}_n(\mathbb{R})$ denote the group of invertible $n \times n$ matrices. Then taking determinant $\det$ defines a homomorphism $\det : \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R} \times$. 

There are no nontrivial homomorphisms $\mathbb{Z}/m \rightarrow \mathbb{Z}$, but there are non-trivial homomorphism in the opposite direction (see above).

For a fixed $m \in \mathbb{Z}$, the map $\varphi_m : \mathbb{Z} \rightarrow \mathbb{Z}$ given by $\varphi_m(n) = nm$ defines a homomorphism. 

For any abelian group $G$, the map $\varphi_m : G \rightarrow G$ given by $g \mapsto g^m$ is a homomorphism. 

The same map for non-abelian group is not necessarily a homomorphism (can you give an example?).
Examples

For all the homomorphisms below, what are their kernels and images?

- Between any groups $G, H$ there is a trivial homomorphism $\varphi: G \to H$, given by $\varphi(g) = e_H$, for all $g \in G$.
- The map $n \mapsto n \pmod m$ defines a homomorphism $\mathbb{Z} \to \mathbb{Z}/m$. 
Examples

For all the homomorphisms below, what are their kernels and images?

- Between any groups $G, H$ there is a trivial homomorphism $\varphi : G \rightarrow H$, given by $\varphi(g) = e_H$, for all $g \in G$.
- The map $n \mapsto n \mod m$ defines a homomorphism $\mathbb{Z} \rightarrow \mathbb{Z}/m$.
- Let $GL_n(\mathbb{R})$ denote the group of invertible $n \times n$ matrices. Then taking determinant $\det$ defines a homomorphism $\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$. 

There are no nontrivial homomorphisms $\mathbb{Z}/m \rightarrow \mathbb{Z}$, but there are non-trivial homomorphisms in the opposite direction (see above).

For any abelian group $G$, the map $\varphi_m : G \rightarrow G$ given by $g \mapsto g^m$ defines a homomorphism. The same map for non-abelian group is not necessarily a homomorphism (can you give an example?).
Examples

For all the homomorphisms below, what are their kernels and images?

- Between any groups $G, H$ there is a trivial homomorphism $\varphi: G \to H$, given by $\varphi(g) = e_H$, for all $g \in G$.
- The map $n \mapsto n(\mod m)$ defines a homomorphism $\mathbb{Z} \to \mathbb{Z}/m$.
- Let $GL_n(\mathbb{R})$ denote the group of invertible $n \times n$ matrices. Then taking determinant $\det$ defines a homomorphism $\det: GL_n(\mathbb{R}) \to \mathbb{R}^\times$.
- There are no nontrivial homomorphisms $\mathbb{Z}/m \to \mathbb{Z}$, but there are non-trivial homomorphism in the opposite direction (see above).
Examples

For all the homomorphisms below, what are their kernels and images?

- Between any groups $G, H$ there is a trivial homomorphism $\varphi: G \to H$, given by $\varphi(g) = e_H$, for all $g \in G$.
- The map $n \mapsto n \pmod{m}$ defines a homomorphism $\mathbb{Z} \to \mathbb{Z}/m$.
- Let $GL_n(\mathbb{R})$ denote the group of invertible $n \times n$ matrices. Then taking determinant $\det$ defines a homomorphism $\det: GL_n(\mathbb{R}) \to \mathbb{R}^\times$.
- There are no nontrivial homomorphisms $\mathbb{Z}/m \to \mathbb{Z}$, but there are non-trivial homomorphism in the opposite direction (see above).
- For a fixed $m \in \mathbb{Z}$, the map $\varphi_m: \mathbb{Z} \to \mathbb{Z}$ given by $\varphi_m(n) = nm$ defines a homomorphism.
Examples

For all the homomorphisms below, what are their kernels and images?

- Between any groups $G, H$ there is a \textbf{trivial} homomorphism $\varphi: G \to H$, given by $\varphi(g) = e_H$, for all $g \in G$.
- The map $n \mapsto n \pmod{m}$ defines a homomorphism $\mathbb{Z} \to \mathbb{Z}/m$.
- Let $GL_n(\mathbb{R})$ denote the group of invertible $n \times n$ matrices. Then taking determinant $\det$ defines a homomorphism $\det: GL_n(\mathbb{R}) \to \mathbb{R}^\times$.
- There are no \textbf{nontrivial} homomorphisms $\mathbb{Z}/m \to \mathbb{Z}$, but there are non-trivial homomorphism in the opposite direction (see above).
- For a fixed $m \in \mathbb{Z}$, the map $\varphi_m: \mathbb{Z} \to \mathbb{Z}$ given by $\varphi_m(n) = nm$ defines a homomorphism.
- For any \textbf{abelian} group $G$, the map $\varphi_m: G \to G$ given by $g \mapsto g^m$ is a homomorphism.
For all the homomorphisms below, what are their kernels and images?

- Between any groups $G, H$ there is a trivial homomorphism $\varphi: G \to H$, given by $\varphi(g) = e_H$, for all $g \in G$.
- The map $n \mapsto n \mod m$ defines a homomorphism $\mathbb{Z} \to \mathbb{Z}/m$.
- Let $GL_n(\mathbb{R})$ denote the group of invertible $n \times n$ matrices. Then taking determinant $\det$ defines a homomorphism $\det: GL_n(\mathbb{R}) \to \mathbb{R}^\times$.
- There are no nontrivial homomorphisms $\mathbb{Z}/m \to \mathbb{Z}$, but there are non-trivial homomorphism in the opposite direction (see above).
- For a fixed $m \in \mathbb{Z}$, the map $\varphi_m: \mathbb{Z} \to \mathbb{Z}$ given by $\varphi_m(n) = nm$ defines a homomorphism.
- For any abelian group $G$, the map $\varphi_m: G \to G$ given by $g \mapsto g^m$ is a homomorphism.
- The same map for non-abelian group is not necessarily a homomorphism (can you give an example?).