MATH 415

Modern Algebra I

Lecture 10: Homomorphisms of groups.

Homomorphism of groups

Definition. Let G and H be groups. A function $f : G \to H$ is called a **homomorphism** of groups if $f(g_1 g_2) = f(g_1) f(g_2)$ for all $g_1, g_2 \in G$.

Examples of homomorphisms:

- Residue modulo n of an integer.

For any $k \in \mathbb{Z}$ let $f(k)$ be the remainder of k after division by n. Then $f : \mathbb{Z} \to \mathbb{Z}_n$ is a homomorphism of the group $(\mathbb{Z}, +)$ onto the group $(\mathbb{Z}_n, +_n)$.

- Sign of a permutation.

The function $\operatorname{sgn} : S_n \to \{-1, 1\}$ is a homomorphism of the symmetric group S_n onto the multiplicative group $\{-1, 1\}$.

- Determinant of an invertible matrix.

The function $\det : GL(n, \mathbb{R}) \to \mathbb{R} \setminus \{0\}$ is a homomorphism of the general linear group $GL(n, \mathbb{R})$ onto the multiplicative group $\mathbb{R} \setminus \{0\}$.

- Linear transformation.

Any vector space is an abelian group with respect to vector addition. If $f : V_1 \to V_2$ is a linear transformation between vector spaces, then f is also a homomorphism of groups.

- Trivial homomorphism.

Given groups G and H, we define $f : G \to H$ by $f(g) = e_H$ for all $g \in G$, where e_H is the identity element of H.

- Natural projection onto a factor group.

Given a group G with a normal subgroup H, we define $f : G \to G/H$ by $f(g) = gH$ for all $g \in G$.

Properties of homomorphisms

Let $f : G \to H$ be a homomorphism of groups.

- The identity element e_G in G is mapped to the identity element e_H in H.

$f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$. Also, $f(e_G) = f(e_G)e_H$.
By cancellation in H, we get $f(e_G) = e_H$.

- $f(g^{-1}) = (f(g))^{-1}$ for all $g \in G$.

$f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$. Similarly,
$f(g^{-1})f(g) = e_H$. Thus $f(g^{-1}) = (f(g))^{-1}$.

- $f(g^n) = (f(g))^n$ for all $g \in G$ and $n \in \mathbb{Z}$.

- The order of $f(g)$ divides the order of g.

Indeed, $g^n = e_G \implies (f(g))^n = e_H$ for any $n \in \mathbb{N}$.

Properties of homomorphisms

Let $f : G \to H$ be a homomorphism of groups.

- If K is a subgroup of G, then $f(K)$ is a subgroup of H.

Follows since $e_G \in K$ and $f(e_G) = e_H$, $f(g_1)f(g_2) = f(g_1g_2)$ and $(f(g))^{-1} = f(g^{-1})$ for all $g, g_1, g_2 \in K$.

- If K is a subgroup of G and $\widetilde{K} = f(K)$, then $f(g) = h$ implies $f(gK) = h\widetilde{K}$ and $f(Kg) = \widetilde{K}h$ for all $g \in G$ and $h \in H$.

- If K is a normal subgroup of G and the homomorphism f is onto, then $f(K)$ is a normal subgroup of H.

Properties of homomorphisms

Let $f : G \to H$ be a homomorphism of groups.

- If L is a subgroup of H, then $f^{-1}(L)$ is a subgroup of G.
- If L is a subgroup of H and $\widehat{L} = f^{-1}(L)$, then $f(g) = h$ implies $f^{-1}(hL) = g\widehat{L}$ and $f^{-1}(Lh) = \widehat{L}g$ for all $g \in G$ and $h \in H$.
- If L is a normal subgroup of H, then $f^{-1}(L)$ is a normal subgroup of G.
- $f^{-1}(e_H)$ is a normal subgroup of G called the **kernel** of f and denoted $\mathrm{Ker}(f)$.

Indeed, the trivial subgroup $\{e_H\}$ is always normal.

Isomorphism of groups

Definition. Let G and H be groups. A function $f : G \to H$ is called an **isomorphism** of groups if it is bijective and $f(g_1 g_2) = f(g_1) f(g_2)$ for all $g_1, g_2 \in G$. In other words, an isomorphism is a bijective homomorphism.

The group G is said to be **isomorphic** to H if there exists an isomorphism $f : G \to H$. Notation: $G \cong H$.

Theorem Isomorphism is an equivalence relation on groups.

Sketch of the proof. The identity map on a group is an isomorphism. The inverse map of an isomorphism is also an isomorphism, and so is the composition of two isomorphisms.

Theorem The following features of groups are preserved under isomorphisms: **(i)** the number of elements, **(ii)** the number of elements of a particular order, **(iii)** being abelian, **(iv)** being cyclic, **(v)** having a subgroup of a particular order or particular index.

Examples of isomorphic groups

- $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$.

An isomorphism $f : \mathbb{R} \to \mathbb{R}^+$ is given by $f(x) = e^x$.

- $\big([0, t), +_t\big)$ and $\big([0, s), +_s\big)$, where $t, s > 0$.

An isomorphism $f : [0, t) \to [0, s)$ is given by $f(x) = s(x/t)$ for all $x \in [0, t)$.

- Any two cyclic groups $\langle g \rangle$ and $\langle h \rangle$ of the same order.

An isomorphism $f : \langle g \rangle \to \langle h \rangle$ is given by $f(g^n) = h^n$ for all $n \in \mathbb{Z}$.

- $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Both groups are cyclic groups of order 6.

Isomorphisms of direct products of groups

- If $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$.

If $f_1 : G_1 \to H_1$ and $f_2 : G_2 \to H_2$ are isomorphisms, then a map $f : G_1 \times G_2 \to H_1 \times H_2$ given by $f(g_1, g_2) = (f_1(g_1), f_2(g_2))$ for all $g_1 \in G_1$ and $g_2 \in G_2$ is also an isomorphism.

- $G \times H \cong H \times G$.

An isomorphism $f : G \times H \to H \times G$ is given by $f(g, h) = (h, g)$ for all $g \in G$ and $h \in H$.

- $(G \times H) \times K \cong G \times H \times K \cong G \times (H \times K)$.

Isomorphisms $f_1 : G \times H \times K \to (G \times H) \times K$ and $f_2 : G \times H \times K \to G \times (H \times K)$ are given by $f_1(g, h, k) = ((g, h), k)$ and $f_2(g, h, k) = (g, (h, k))$.

- $\{e\} \times G \cong G \times \{e\} \cong G$.

Isomorphisms $f_1 : G \to \{e\} \times G$ and $f_2 : G \to G \times \{e\}$ are given by $f_1(g) = (e, g)$ and $f_2(g) = (g, e)$ for all $g \in G$.

Fundamental Theorem on Homomorphisms Given a homomorphism $f : G \to H$, the factor group $G/\operatorname{Ker}(f)$ is isomorphic to $f(G)$.

Proof. Let K denote the kernel $\operatorname{Ker}(f)$ of the homomorphism f. We define a map $\phi : G/K \to f(G)$ by $\phi(gK) = f(g)$ for all $g \in G$. To verify that $\phi(gK)$ is determined uniquely, we need to show that $g'K = gK \implies f(g') = f(g)$. Indeed, if the cosets $g'K$ and gK are the same then $g' = gk$ for some $k \in K$. Hence $f(g') = f(gk) = f(g)f(k) = f(g)e_H = f(g)$.

The fact that ϕ is a homomorphism of groups will follow from the definition of the factor group. For any cosets g_1K and g_2K of the subgroup K, we have $\phi\big((g_1K)(g_2K)\big) = \phi(g_1g_2K) = f(g_1g_2) = f(g_1)f(g_2) = \phi(g_1K)\phi(g_2K)$.

By construction, ϕ is surjective. To prove injectivity, we need to show that $f(g') = f(g) \implies g'K = gK$. Let $a = g^{-1}g'$. If $f(g') = f(g)$ then $f(a) = f(g^{-1})f(g') = (f(g))^{-1}f(g') = (f(g))^{-1}f(g) = e_H$. Hence $a \in K$. Consequently, $g' = ga \in gK$ so that $g'K = gK$. Thus ϕ is bijective.

Examples

- $f : \mathbb{Z} \to \mathbb{Z}_n$, given by $f(k) = k \bmod n$.

The kernel of the homomorphism f is the subgroup $n\mathbb{Z}$; the image is the entire group $\mathbb{Z}_n$. Hence $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

- $f : \mathbb{R} \to \mathbb{C} \setminus \{0\}$, given by $f(x) = e^{2\pi i x}$.

The kernel of the homomorphism f is $\mathbb{Z}$; the image is the multiplicative group of all complex numbers of absolute value 1. Hence the latter is isomorphic to the factor group $\mathbb{R}/\mathbb{Z}$.

- $f : GL(n, \mathbb{R}) \to \mathbb{R} \setminus \{0\}$, given by $f(M) = \det M$.

The kernel of the homomorphism f is the special linear group $SL(n, \mathbb{R})$; the image is the entire multiplicative group $\mathbb{R} \setminus \{0\}$. Hence $SL(n, \mathbb{R})$ is a normal subgroup of $GL(n, \mathbb{R})$ and $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \cong \mathbb{R} \setminus \{0\}$.

Examples of non-isomorphic groups

- S_3 and $\mathbb{Z}_7$.

S_3 has order 6 while $\mathbb{Z}_7$ has order 7.

- S_3 and $\mathbb{Z}_6$.

$\mathbb{Z}_6$ is abelian while S_3 is not.

- $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$.

$\mathbb{Z}$ is cyclic while $\mathbb{Z} \times \mathbb{Z}$ is not.

- $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Q}$.

$\mathbb{Z} \times \mathbb{Z}$ is generated by two elements $(1, 0)$ and $(0, 1)$ while $\mathbb{Q}$ cannot be generated by a finite set.

- $(\mathbb{R}, +)$ and $(\mathbb{R} \setminus \{0\}, \cdot)$.

$(\mathbb{R} \setminus \{0\}, \cdot)$ has an element of order 2, namely, -1. In $(\mathbb{R}, +)$, every element different from 0 has infinite order.

- $\mathbb{Z} \times \mathbb{Z}_3$ and $\mathbb{Z} \times \mathbb{Z}$.

$\mathbb{Z} \times \mathbb{Z}_3$ has an element of finite order different from the identity element, e.g., $(0, 1)$, while $\mathbb{Z} \times \mathbb{Z}$ does not.

- $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Orders of elements in $\mathbb{Z}_8$: 1, 2, 4 and 8; in $\mathbb{Z}_4 \times \mathbb{Z}_2$: 1, 2 and 4; in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$: only 1 and 2.

- $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Both groups have elements of order 1, 2 and 4. However $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$ has $2^3 - 1 = 7$ elements of order 2 while $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has $2^4 - 1 = 15$.