MTH223A LECTURE NOTES CHAPTER 4

Yvette Fajardo-Lim

Mathematics and Statistics Department
De La Salle University - Manila

Outline

Outline

Cosets

Definition

For any $g \in G$, the subset $Hg = \{hg | h \in H\}$ of G is called a **right coset** *of H.*

Remark

1. $g \in Hg$, since $g = eg$ and $e \in H$.
2. If H is finite, say $H = \{h_1, \ldots h_n\}$, then $Hg = \{h_1 g, \ldots, h_n g\}$ and these elements $h_i g$ are all distinct by the Cancelation Laws.
3. H is one of its right cosets, since $H = He$.
4. Although each element $g \in G$ gives a right coset Hg, there is no claim that we obtain a different right coset for each element, in fact as we shall see this only happens if $H = \{e\}$.

Cosets

Definition

For any $g \in G$, the subset $Hg = \{hg | h \in H\}$ of G is called a **right coset** *of H.*

Remark

1. $g \in Hg$, since $g = eg$ and $e \in H$.
2. If H is finite, say $H = \{h_1, \ldots h_n\}$, then $Hg = \{h_1 g, \ldots, h_n g\}$ and these elements $h_i g$ are all distinct by the Cancelation Laws.
3. H is one of its right cosets, since $H = He$.
4. Although each element $g \in G$ gives a right coset Hg, there is no claim that we obtain a different right coset for each element, in fact as we shall see this only happens if $H = \{e\}$.

Cosets

Definition

For any $g \in G$, the subset $Hg = \{hg|h \in H\}$ of G is called a **right coset** *of H.*

Remark

1. *$g \in Hg$, since $g = eg$ and $e \in H$.*
2. *If H is finite, say $H = \{h_1, \ldots h_n\}$, then $Hg = \{h_1 g, \ldots, h_n g\}$ and these elements $h_i g$ are all distinct by the Cancelation Laws.*
3. *H is one of its right cosets, since $H = He$.*
4. *Although each element $g \in G$ gives a right coset Hg, there is no claim that we obtain a different right coset for each element, in fact as we shall see this only happens if $H = \{e\}$.*

Cosets

Definition

For any $g \in G$, the subset $Hg = \{hg | h \in H\}$ of G is called a **right coset** *of H.*

Remark

1. *$g \in Hg$, since $g = eg$ and $e \in H$.*
2. *If H is finite, say $H = \{h_1, \dots h_n\}$, then $Hg = \{h_1 g, \dots, h_n g\}$ and these elements $h_i g$ are all distinct by the Cancelation Laws.*
3. *H is one of its right cosets, since $H = He$.*
4. *Although each element $g \in G$ gives a right coset Hg, there is no claim that we obtain a different right coset for each element, in fact as we shall see this only happens if $H = \{e\}$.*

Cosets

Definition

For any $g \in G$, the subset $Hg = \{hg | h \in H\}$ of G is called a **right coset** *of H.*

Remark

1. *$g \in Hg$, since $g = eg$ and $e \in H$.*
2. *If H is finite, say $H = \{h_1, \dots h_n\}$, then $Hg = \{h_1 g, \dots, h_n g\}$ and these elements $h_i g$ are all distinct by the Cancelation Laws.*
3. *H is one of its right cosets, since $H = He$.*
4. *Although each element $g \in G$ gives a right coset Hg, there is no claim that we obtain a different right coset for each element, in fact as we shall see this only happens if $H = \{e\}$.*

Cosets

Example

Let $G = \mathbb{Z}$ and $H = 4\mathbb{Z}$. We have the following right cosets of H:

$$\begin{aligned}
4\mathbb{Z} + 0 &= \{4n | n \in \mathbb{Z}\} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}, \\
4\mathbb{Z} + 1 &= \{4n + 1 | n \in \mathbb{Z}\} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}, \\
4\mathbb{Z} + 2 &= \{4n + 2 | n \in \mathbb{Z}\} = \{\ldots, -6, -2, 2, 6, 10, \ldots\}, \\
4\mathbb{Z} + 3 &= \{4n + 3 | n \in \mathbb{Z}\} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}.
\end{aligned}$$

Cosets

Theorem

If $H \leq G$, the relation $\sim$ defined on G by $a \sim b \iff ab^{-1} \in H$ is an equivalence relation; the equivalence class containing a is the right coset Ha.

Cosets

Example

Take $G = D_4$.

$*$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	ab^2
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

If $H = \{e, b\}$ *then*

$$\begin{aligned} He &= \{e, b\} = Hb \\ Ha &= \{a, ba\} = \{a, a^3b\} = Ha^3b \\ Ha^2 &= \{a^2, ba^2\} = \{a^2, a^2b\} = Ha^2b \\ Ha^3 &= \{a^3, ba^3\} = \{a^3, ab\} = Hab \end{aligned}$$

Cosets

In an exactly similar way we may define the left cosets of a subgroup H of G as the subsets of the form gH for $g \in G$. Their properties are analogous to those of right cosets; the left coset version of theorem 4.1 uses the element $a^{-1}b$ instead of ab^{-1}. Clearly, if G is abelian then left and right cosets are the same thing.

Cosets

In the previous example, the left cosets of H are

$$\begin{aligned} eH &= \{e, b\} = bH \\ aH &= \{a, ab\} = abH \\ a^2H &= \{a^2, a^2b\} = a^2bH \\ a^3H &= \{a^3, a^3b\} = a^3bH \end{aligned}$$

In general left and right cosets may be different.

Outline

Lagrange's Theorem

Theorem

(Lagrange's Theorem) If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$.

Example

1. D_4 has subgroups $\{e, a, a^2, a^3\}$ and $\{e, b\}$, and $4|8, 2|8$.
2. $(\mathbb{Z}_6, +)$ has subgroups $\{0, 2, 4\}$ and $\{0, 3\}$, and $3|6, 2|6$.

Lagrange's Theorem

Theorem

(Lagrange's Theorem) If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$.

Example

1. *D_4 has subgroups $\{e, a, a^2, a^3\}$ and $\{e, b\}$, and $4|8, 2|8$.*
2. *$(\mathbb{Z}_6, +)$ has subgroups $\{0, 2, 4\}$ and $\{0, 3\}$, and $3|6, 2|6$.*

Lagrange's Theorem

Theorem

(Lagrange's Theorem) If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$.

Example

1. D_4 *has subgroups* $\{e, a, a^2, a^3\}$ *and* $\{e, b\}$, *and* $4|8, 2|8$.
2. $(\mathbb{Z}_6, +)$ *has subgroups* $\{0, 2, 4\}$ *and* $\{0, 3\}$, *and* $3|6, 2|6$.

Lagrange's Theorem

Remark

Note that we have also shown that the number of right cosets of H in G is $|G|/|H|$; we call this number the **index of H in G***, and write it as $|G : H|$.*

Corollary

If $|G| = n$ and $g \in G$, then $o(g)|n$ and $g^n = e$.

Example

1. *The elements of D_4 have orders 1, 2 and 4, each of which divides 8.*
2. *The elements of $(Z_6, +)$ have orders 1, 2, 3 and 6, each of which divides 6.*

Lagrange's Theorem

Remark

Note that we have also shown that the number of right cosets of H in G is $|G|/|H|$; we call this number the **index of H in G**, *and write it as $|G : H|$.*

Corollary

If $|G| = n$ and $g \in G$, then $o(g)|n$ and $g^n = e$.

Example

1. *The elements of D_4 have orders 1, 2 and 4, each of which divides 8.*
2. *The elements of $(Z_6, +)$ have orders 1, 2, 3 and 6, each of which divides 6.*

Lagrange's Theorem

Remark

Note that we have also shown that the number of right cosets of H in G is $|G|/|H|$; we call this number the **index of H in G**, *and write it as $|G : H|$.*

Corollary

If $|G| = n$ and $g \in G$, then $o(g)|n$ and $g^n = e$.

Example

1. *The elements of D_4 have orders 1, 2 and 4, each of which divides 8.*
2. *The elements of $(Z_6, +)$ have orders 1, 2, 3 and 6, each of which divides 6.*

Lagrange's Theorem

Remark

Note that we have also shown that the number of right cosets of H in G is $|G|/|H|$; we call this number the **index of H in G**, *and write it as $|G : H|$.*

Corollary

If $|G| = n$ and $g \in G$, then $o(g)|n$ and $g^n = e$.

Example

1. *The elements of D_4 have orders 1, 2 and 4, each of which divides 8.*
2. *The elements of $(Z_6, +)$ have orders 1, 2, 3 and 6, each of which divides 6.*

Lagrange's Theorem

Corollary

A group of prime order is cyclic, and has no proper non-trivial subgroups; any non-identity element generates the group.

Example

The group you filled up with $\{u, w, x, y, z\}$ is cyclic since its order is 5.

Lagrange's Theorem

Corollary

A group of prime order is cyclic, and has no proper non-trivial subgroups; any non-identity element generates the group.

Example

The group you filled up with $\{u, w, x, y, z\}$ is cyclic since its order is 5.

Lagrange's Theorem

Theorem

If $H, K \leq G$ and $(|H|, |K|) = 1$, then $H \cap K = \{e\}$.

Example

If $G = (\mathbb{Z}_6, +)$ we may take $H = \{0, 2, 4\}$ and $K = \{0, 3\}$, then $|H| = 3, |K| = 2$ and $(3, 2) = 1$, and $H \cap K = \{0\}$.

Lagrange's Theorem

Theorem

If $H, K \leq G$ *and* $(|H|, |K|) = 1$*, then* $H \cap K = \{e\}$ *.*

Example

If $G = (\mathbb{Z}_6, +)$ *we may take* $H = \{0, 2, 4\}$ *and* $K = \{0, 3\}$*, then* $|H| = 3, |K| = 2$ *and* $(3, 2) = 1$*, and* $H \cap K = \{0\}$*.*

Outline

Homomorphisms

Definition

Let G and H be groups. A map $\phi : G \to H$ is called a **homomorphism** *if*

$$\phi(ab) = \phi(a)\phi(b) \text{ for all } a, b \in G.$$

A homomorphism which is one-to-one is or injective called a **monomorphism**. *If it is onto or surjective, then it is called an* **epimorphism**. *A homomorphism which is both one-to-one and onto or bijective is called an* **isomorphism**. *If there is an isomorphism $G \to H$, we say that G and H are* **isomorphic**, *and write $G \cong H$.*

Homorphisms

Remark

Two finite groups G and H are isomorphic if their Cayley tables have the same structure, it is only the names of the elements which are different. Hence, we can "replace" the elements of G by those of H which is a bijection , and as the element in row a and column b is ab, we need the element in row $\phi(a)$ *and column* $\phi(b)$ *to be* $\phi(ab)$.

Homomorphisms

Example

The map $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ *defined by* $\phi(n) = 2n$ *for all* $n \in \mathbb{Z}$ *is a homomorphism, since*

$$\phi(m+n) = 2(m+n) = 2m+2n = \phi(m) + \phi(n)$$

for all $m, n \in \mathbb{Z}$.

If $m,\ n \in \mathbb{Z}$ *such that* $\phi(m) = 2m = 2n = \phi(n)$, *then* $m = n$ *and hence* ϕ *is one-to-one. However, all odd integers have no pre-images under* ϕ *and hence* ϕ *is not onto.*

Homomorphisms

Example

The map $\phi : (\mathbb{R}, +) \to (\mathbb{R}^+, \bullet)$ defined by $\phi(x) = e^x$ for all $x \in \mathbb{R}$ is a homomorphism, since

$$\phi(x + y) = e^{(x+y)} = e^x e^y = \phi(x)\phi(y)$$

for all $x, y \in \mathbb{R}$. If $x,\ y \in \mathbb{R}$ such that $\phi(x) = e^x = e^y = \phi(y)$,

then $x = y$. Also, if $y \in \mathbb{R}^+$ then we can find $x = \ln y$ such that $e^x = y$. This means that ϕ is both one-to-one and onto and hence, ϕ is an isomorphism.

Example

The map $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ *defined by* $\phi(r) = [r]$ *for all* $r \in \mathbb{Z}$ *is a homomorphism, since*

$$\phi(r+s) = [r+s] = [r] + [s] = \phi(r) + \phi(s)$$

for all $r, s \in \mathbb{R}^*$.

If $x,\ y \in \mathbb{Z},\ \ x \neq y$ *such that* $x = q_1 n + r,\ y = q_2 n + r$*, then* $\phi(x) = \phi(q_1 n + r) = r = \phi(y)$*, which shows that* ϕ *is not one-to-one. On the other hand, if* $r \in \mathbb{Z}_n$*, then for all integer values of* q*, we have* $x = qn + r \in \mathbb{Z}$ *and* $\phi(x) = \phi(qn + r) = r$*, which means that* ϕ *is onto and therefore an epimorphism.*

Homomorphisms

Theorem

Let $\phi : G \to H$ be a homomorphism, then:

1. $\phi(e_G) = e_H$;
2. $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$. ;
3. $\phi(g^n) = \phi(g)^n$ for all $g \in G, n \in \mathbb{Z}^+$.

Remark

Note that if G and H are both additive groups, then (3) is written $\phi(ng) = n\phi(g)$.

Homomorphisms

Theorem

Let $\phi : G \to H$ be a homomorphism, then:

1. $\phi(e_G) = e_H$;
2. $\phi(g^{-1}) = \phi(g)^{-1}$ *for all* $g \in G$. ;
3. $\phi(g^n) = \phi(g)^n$ *for all* $g \in G, n \in \mathbb{Z}^+$.

Remark

Note that if G and H are both additive groups, then (3) is written $\phi(ng) = n\phi(g)$.

Homomorphisms

Theorem

Let $\phi : G \to H$ be a homomorphism, then:

1. $\phi(e_G) = e_H$;
2. $\phi(g^{-1}) = \phi(g)^{-1}$ *for all* $g \in G$. ;
3. $\phi(g^n) = \phi(g)^n$ *for all* $g \in G, n \in \mathbb{Z}^+$.

Remark

Note that if G and H are both additive groups, then (3) is written $\phi(ng) = n\phi(g)$.

Homomorphisms

Theorem

Let $\phi : G \to H$ be a homomorphism, then:

1. $\phi(e_G) = e_H$;
2. $\phi(g^{-1}) = \phi(g)^{-1}$ *for all* $g \in G$. ;
3. $\phi(g^n) = \phi(g)^n$ *for all* $g \in G, n \in \mathbb{Z}^+$.

Remark

Note that if G and H are both additive groups, then (3) is written $\phi(ng) = n\phi(g)$.

Homomorphisms

Example

1. *Take* $G = (\mathbb{R}^*, \bullet)$ *and* $H = (\mathbb{R}^*, \bullet)$ *with the map* $\phi : G \to H$ *defined by* $\phi(x) = x^2$ *for all* $x \in \mathbb{R}^*$*: we have* $e_G = 1$*, and* $\phi(1) = 1^2 = 1 = e_H$*; the inverse of* $x \in G$ *is* $\frac{1}{x}$*, and* $\phi\left(\frac{1}{x}\right) = \left(\frac{1}{x}\right)^2 = \frac{1}{x^2}$ *which is the inverse of* $x^2 = \phi(x)$*; the nth power of* x *is* x^n*, and* $\phi(x^n) = (x^n)^2 = x^2 n = (x^2)^n$*, which is the nth power of* $x^2 = \phi(x)$*.*
2. *Take* $G = (\mathbb{R}, +)$ *and* $H = (\mathbb{R}^+, \bullet)$*, with the map* $\phi : G \to H$ *defined by* $\phi(x) = e^x$ *for all* $x\mathbb{R}$*: we have* $e_G = 0$*, and* $\phi(0) = e^0 = 1 = e_H$*; the inverse of* $x \in G$ *is* $-x$*, and* $\phi(-x) = e^{-x}$*, which is the inverse of* $e^x = \phi(x)$*; the nth power of* x *is* nx*, and* $\phi(nx) = e^{(nx)} = (e^x)^n$*, which is the nth power of* $e^x = \phi(x)$*.*

Homomorphisms

Example

1. *Take $G = (\mathbb{R}^*, \bullet)$ and $H = (\mathbb{R}^*, \bullet)$ with the map $\phi : G \to H$ defined by $\phi(x) = x^2$ for all $x \in \mathbb{R}^*$: we have $e_G = 1$, and $\phi(1) = 1^2 = 1 = e_H$; the inverse of $x \in G$ is $\frac{1}{x}$, and $\phi\left(\frac{1}{x}\right) = \left(\frac{1}{x}\right)^2 = \frac{1}{x^2}$ which is the inverse of $x^2 = \phi(x)$; the nth power of x is x^n, and $\phi(x^n) = (x^n)^2 = x^2 n = (x^2)^n$, which is the nth power of $x^2 = \phi(x)$.*
2. *Take $G = (\mathbb{R}, +)$ and $H = (\mathbb{R}^+, \bullet)$, with the map $\phi : G \to H$ defined by $\phi(x) = e^x$ for all $x\mathbb{R}$: we have $e_G = 0$, and $\phi(0) = e^0 = 1 = e_H$; the inverse of $x \in G$ is $-x$, and $\phi(-x) = e^{-x}$, which is the inverse of $e^x = \phi(x)$; the nth power of x is nx, and $\phi(nx) = e^{(nx)} = (e^x)^n$, which is the nth power of $e^x = \phi(x)$.*

Homomorphisms

Corollary

If G has finite order n and $\phi : G \to H$ is a homomorphism, then the order of $\phi(g)$ divides n; if ϕ is one-to-one, then the order of $\phi(g)$ equals n.

Example

Consider the multiplicative groups $\mathbb{R}^*$ and $\mathbb{R}^+$; the element -1 of $\mathbb{R}^*$ has order 2, whereas $\mathbb{R}^+$ has no such element, so they cannot be isomorphic.

Homomorphisms

Corollary

If G has finite order n and $\phi : G \to H$ is a homomorphism, then the order of $\phi(g)$ divides n; if ϕ is one-to-one, then the order of $\phi(g)$ equals n.

Example

Consider the multiplicative groups $\mathbb{R}^*$ and $\mathbb{R}^+$; the element -1 of $\mathbb{R}^*$ has order 2, whereas $\mathbb{R}^+$ has no such element, so they cannot be isomorphic.

Homorphisms

Theorem

If $\phi : G \to H$ and $\theta : H \to K$ are both homomorphisms, so is $\phi \circ \theta : G \to K$.

Theorem

If $\phi : G \to H$ is an isomorphism, so is $\phi^{-1} : H \to G$.

Homomorphisms

Theorem

If $\phi : G \to H$ and $\theta : H \to K$ are both homomorphisms, so is $\phi \circ \theta : G \to K$.

Theorem

If $\phi : G \to H$ is an isomorphism, so is $\phi^{-1} : H \to G$.

Homorphisms

Definition

An isomorphism $\phi : G \to G$ is called an **automorphism** *of G.*

Remark

The previous two theorems show that the set of automorphisms of G actually form a group.

Theorem

Any two cyclic groups of the same order are isomorphic.

Homorphisms

Definition

An isomorphism $\phi : G \to G$ is called an **automorphism** *of G.*

Remark

The previous two theorems show that the set of automorphisms of G actually form a group.

Theorem

Any two cyclic groups of the same order are isomorphic.

Homomorphisms

Definition

An isomorphism $\phi : G \to G$ is called an **automorphism** *of G.*

Remark

The previous two theorems show that the set of automorphisms of G actually form a group.

Theorem

Any two cyclic groups of the same order are isomorphic.

Outline

Kernel of a Homomorphism

Definition

Given a homomorphism $\phi : G \to H$, the **kernel** *of ϕ is the subset $Ker\phi = \{g \in G | \phi(G) = e_H\}$ of G, while the image of ϕ is the subset $\phi(G) = \{\phi(g) | g \in G\}$ of H.*

Example

1. *If $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ is defined by $\phi(n) = 2n$ for all $n \in \mathbb{Z}$, then $Ker\phi = \{0\}$ and $\phi(G) = 2\mathbb{Z}$.*
2. *If $\phi : (\mathbb{R}^*, \bullet) \to (\mathbb{R}^*, \bullet)$ defined by $\phi(x) = x^2$ for all $x \in \mathbb{R}^*$, then $Ker\phi = \{-1, 1\}$ and $\phi(G) = \mathbb{R}^+$.*
3. *If $\phi : (\mathbb{R}, +) \to (\mathbb{R}^+, \bullet)$ defined by $\phi(x) = e^x$ for all $x \in \mathbb{R}$, then $Ker\phi = \{0\}$ and $\phi(G) = \mathbb{R}^+$.*
4. *If $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ defined by $\phi(r) = [r]$ for all $r \in \mathbb{Z}$, then $Ker\phi = \{n\mathbb{Z}\}$ and $\phi(G) = \mathbb{Z}_n$.*

Kernel of a Homomorphism

Definition

Given a homomorphism $\phi : G \to H$, the **kernel** *of ϕ is the subset $Ker\phi = \{g \in G | \phi(G) = e_H\}$ of G, while the image of ϕ is the subset $\phi(G) = \{\phi(g) | g \in G\}$ of H.*

Example

1. *If $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ is defined by $\phi(n) = 2n$ for all $n \in \mathbb{Z}$, then $Ker\phi = \{0\}$ and $\phi(G) = 2\mathbb{Z}$.*
2. *If $\phi : (\mathbb{R}^*, \bullet) \to (\mathbb{R}^*, \bullet)$ defined by $\phi(x) = x^2$ for all $x \in \mathbb{R}^*$, then $Ker\phi = \{-1, 1\}$ and $\phi(G) = \mathbb{R}^+$.*
3. *If $\phi : (\mathbb{R}, +) \to (\mathbb{R}^+, \bullet)$ defined by $\phi(x) = e^x$ for all $x \in \mathbb{R}$, then $Ker\phi = \{0\}$ and $\phi(G) = \mathbb{R}^+$.*
4. *If $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ defined by $\phi(r) = [r]$ for all $r \in \mathbb{Z}$, then $Ker\phi = \{n\mathbb{Z}\}$ and $\phi(G) = \mathbb{Z}_n$.*

Kernel of a Homomorphism

Definition

Given a homomorphism $\phi : G \to H$, the **kernel** *of ϕ is the subset $Ker\phi = \{g \in G | \phi(G) = e_H\}$ of G, while the image of ϕ is the subset $\phi(G) = \{\phi(g) | g \in G\}$ of H.*

Example

1. *If $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ is defined by $\phi(n) = 2n$ for all $n \in \mathbb{Z}$, then $Ker\phi = \{0\}$ and $\phi(G) = 2\mathbb{Z}$.*
2. *If $\phi : (\mathbb{R}^*, \bullet) \to (\mathbb{R}^*, \bullet)$ defined by $\phi(x) = x^2$ for all $x \in \mathbb{R}^*$, then $Ker\phi = \{-1, 1\}$ and $\phi(G) = \mathbb{R}^+$.*
3. *If $\phi : (\mathbb{R}, +) \to (\mathbb{R}^+, \bullet)$ defined by $\phi(x) = e^x$ for all $x \in \mathbb{R}$, then $Ker\phi = \{0\}$ and $\phi(G) = \mathbb{R}^+$.*
4. *If $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ defined by $\phi(r) = [r]$ for all $r \in \mathbb{Z}$, then $Ker\phi = \{n\mathbb{Z}\}$ and $\phi(G) = \mathbb{Z}_n$.*

Kernel of a Homomorphism

Definition

Given a homomorphism $\phi : G \to H$, the **kernel** *of ϕ is the subset $Ker\phi = \{g \in G | \phi(G) = e_H\}$ of G, while the image of ϕ is the subset $\phi(G) = \{\phi(g) | g \in G\}$ of H.*

Example

1. *If $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ is defined by $\phi(n) = 2n$ for all $n \in \mathbb{Z}$, then $Ker\phi = \{0\}$ and $\phi(G) = 2\mathbb{Z}$.*
2. *If $\phi : (\mathbb{R}^*, \bullet) \to (\mathbb{R}^*, \bullet)$ defined by $\phi(x) = x^2$ for all $x \in \mathbb{R}^*$, then $Ker\phi = \{-1, 1\}$ and $\phi(G) = \mathbb{R}^+$.*
3. *If $\phi : (\mathbb{R}, +) \to (\mathbb{R}^+, \bullet)$ defined by $\phi(x) = e^x$ for all $x \in \mathbb{R}$, then $Ker\phi = \{0\}$ and $\phi(G) = \mathbb{R}^+$.*
4. *If $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ defined by $\phi(r) = [r]$ for all $r \in \mathbb{Z}$, then $Ker\phi = \{n\mathbb{Z}\}$ and $\phi(G) = \mathbb{Z}_n$.*

Kernel of a Homomorphism

Definition

Given a homomorphism $\phi : G \to H$, the **kernel** *of ϕ is the subset $Ker\phi = \{g \in G | \phi(G) = e_H\}$ of G, while the image of ϕ is the subset $\phi(G) = \{\phi(g) | g \in G\}$ of H.*

Example

1. *If $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ is defined by $\phi(n) = 2n$ for all $n \in \mathbb{Z}$, then $Ker\phi = \{0\}$ and $\phi(G) = 2\mathbb{Z}$.*
2. *If $\phi : (\mathbb{R}^*, \bullet) \to (\mathbb{R}^*, \bullet)$ defined by $\phi(x) = x^2$ for all $x \in \mathbb{R}^*$, then $Ker\phi = \{-1, 1\}$ and $\phi(G) = \mathbb{R}^+$.*
3. *If $\phi : (\mathbb{R}, +) \to (\mathbb{R}^+, \bullet)$ defined by $\phi(x) = e^x$ for all $x \in \mathbb{R}$, then $Ker\phi = \{0\}$ and $\phi(G) = \mathbb{R}^+$.*
4. *If $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ defined by $\phi(r) = [r]$ for all $r \in \mathbb{Z}$, then $Ker\phi = \{n\mathbb{Z}\}$ and $\phi(G) = \mathbb{Z}_n$.*

Kernel and Image of a Homomorphism

Theorem

If $\phi : G \to H$ is a homomorphism, then Ker$\phi \leq G$ and $\phi(G) \leq G$.

Theorem

If G is cyclic and $\phi : G \to H$ is a homomorphism, then $\phi(G)$ is also cyclic.

Theorem

$\phi : G \to H$ is one-to-one if and only if Ker$\phi = \{e_G\}$.

Kernel and Image of a Homomorphism

Theorem

If $\phi : G \to H$ is a homomorphism, then Ker$\phi \leq G$ and $\phi(G) \leq G$.

Theorem

If G is cyclic and $\phi : G \to H$ is a homomorphism, then $\phi(G)$ is also cyclic.

Theorem

$\phi : G \to H$ is one-to-one if and only if Ker$\phi = \{e_G\}$.

Kernel and Image of a Homomorphism

Theorem

If $\phi : G \to H$ is a homomorphism, then Ker$\phi \leq G$ and $\phi(G) \leq G$.

Theorem

If G is cyclic and $\phi : G \to H$ is a homomorphism, then $\phi(G)$ is also cyclic.

Theorem

$\phi : G \to H$ is one-to-one if and only if Ker$\phi = \{e_G\}$.

Kernel and Image of a Homomorphism

Theorem

Let $\phi : G \to H$ be a homomorphism with $Ker\phi = K$, and take $g \in G$ and $h \in \phi(G)$; then the set $\{x \in G | \phi(x) = h\}$ equals the right coset Kg.

Example

Take the homomorphism $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}_5, +)$ defined by $\phi(r) = [r]$ for all $r \in \mathbb{Z}$; then $Ker\phi = 5\mathbb{Z}$. If we take $g = 7$ then $h = \phi(g) = [7] = [2]$; the set of elements $x \in \mathbb{Z}$ with $\phi(x) = [2]$ is the right coset $5\mathbb{Z} + 2 = 5\mathbb{Z} + 7$.

Kernel and Image of a Homomorphism

Theorem

Let $\phi : G \to H$ be a homomorphism with Ker$\phi = K$, and take $g \in G$ and $h \in \phi(G)$; then the set $\{x \in G | \phi(x) = h\}$ equals the right coset Kg.

Example

Take the homomorphism $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}_5, +)$ defined by $\phi(r) = [r]$ for all $r \in \mathbb{Z}$; then Ker$\phi = 5\mathbb{Z}$. If we take $g = 7$ then $h = \phi(g) = [7] = [2]$; the set of elements $x \in \mathbb{Z}$ with $\phi(x) = [2]$ is the right coset $5\mathbb{Z} + 2 = 5\mathbb{Z} + 7$.

Kernel and Image of a Homomorphism

Corollary

Let $\phi : G \to H$ be a homomorphism, and suppose $|G| = n, |Ker\phi| = m, \phi(G) = r$; then $n = mr$.

Example

If $|G| = 16$ and $|H| = 9$, the only homomorphism $\phi : G \to H$ is the trivial map sending all elements of G to e_H since $|\phi(G)|$ must divide both 16 and 9, it must be 1, so $\phi(G) = e_H$.

Kernel and Image of a Homomorphism

Corollary

Let $\phi : G \to H$ be a homomorphism, and suppose $|G| = n, |Ker\phi| = m, \phi(G) = r$; then $n = mr$.

Example

If $|G| = 16$ and $|H| = 9$, the only homomorphism $\phi : G \to H$ is the trivial map sending all elements of G to e_H since $|\phi(G)|$ must divide both 16 and 9, it must be 1, so $\phi(G) = e_H$.