Elementary group theory

GU4041, fall 2023

Columbia University

June 22, 2023

Outline

Definition of cyclic groups

So far we have seen the groups S_3, K_4, and $\mathbb{Z}_n$. The latter is an example of a *cyclic group*:

Definition

A group G is **cyclic** if it contains an element g, called a *generator*, such that every element is of the form

1. $e, g, g^2, \ldots, g^{n-1}$, if G is finite and $|G| = n$;
2. $e, g, g^{-1}, g^2, g^{-2}, \ldots$, if G is infinite.

The group $\mathbb{Z}$ is infinite cyclic under addition, with generator 1. The identity is 0 and the inverse of 1 is -1: $1 + (-1) = 0$.
One avoids writing $1^{-1} = -1$ because the exponent -1 is reserved for multiplication.

Definition of cyclic groups

So far we have seen the groups S_3, K_4, and $\mathbb{Z}_n$. The latter is an example of a *cyclic group*:

Definition

A group G is **cyclic** if it contains an element g, called a *generator*, such that every element is of the form

1. $e, g, g^2, \ldots, g^{n-1}$, if G is finite and $|G| = n$;
2. $e, g, g^{-1}, g^2, g^{-2}, \ldots$, if G is infinite.

The group $\mathbb{Z}$ is infinite cyclic under addition, with generator 1. The identity is 0 and the inverse of 1 is -1: $1 + (-1) = 0$.
One avoids writing $1^{-1} = -1$ because the exponent -1 is reserved for multiplication.

Definition of cyclic groups

So far we have seen the groups S_3, K_4, and $\mathbb{Z}_n$. The latter is an example of a *cyclic group*:

Definition

A group G is **cyclic** if it contains an element g, called a *generator*, such that every element is of the form

1. $e, g, g^2, \ldots, g^{n-1}$, if G is finite and $|G| = n$;
2. $e, g, g^{-1}, g^2, g^{-2}, \ldots$, if G is infinite.

The group $\mathbb{Z}$ is infinite cyclic under addition, with generator 1. The identity is 0 and the inverse of 1 is -1: $1 + (-1) = 0$.

One avoids writing $1^{-1} = -1$ because the exponent -1 is reserved for multiplication.

Definition of cyclic groups

So far we have seen the groups S_3, K_4, and $\mathbb{Z}_n$. The latter is an example of a *cyclic group*:

Definition

A group G is **cyclic** if it contains an element g, called a *generator*, such that every element is of the form

1. $e, g, g^2, \ldots, g^{n-1}$, if G is finite and $|G| = n$;
2. $e, g, g^{-1}, g^2, g^{-2}, \ldots$, if G is infinite.

The group $\mathbb{Z}$ is infinite cyclic under addition, with generator 1. The identity is 0 and the inverse of 1 is -1: $1 + (-1) = 0$.
One avoids writing $1^{-1} = -1$ because the exponent -1 is reserved for multiplication.

Another example of cyclic groups

The set $\mathbb{C}^\times$ of complex numbers $z \neq 0$ forms a group under multiplication.

It contains a cyclic subgroup C_n, with $|C_n| = n$, consisting of the numbers

$$1, g = e^{\frac{2\pi i}{n}}, g^2 = e^{\frac{4\pi i}{n}}, \ldots, g^k = e^{\frac{2k\pi i}{n}}, \ldots g^{n-1} = e^{\frac{2(n-1)\pi i}{n}}.$$

The nth power of g is

$$g^n = e^{\frac{2n\pi i}{n}} = e^{2\pi i} = 1.$$

Another example of cyclic groups

The set $\mathbb{C}^\times$ of complex numbers $z \neq 0$ forms a group under multiplication.
It contains a cyclic subgroup C_n, with $|C_n| = n$, consisting of the numbers

$$1, g = e^{\frac{2\pi i}{n}}, g^2 = e^{\frac{4\pi i}{n}}, \ldots, g^k = e^{\frac{2k\pi i}{n}}, \ldots g^{n-1} = e^{\frac{2(n-1)\pi i}{n}}.$$

The nth power of g is

$$g^n = e^{\frac{2n\pi i}{n}} = e^{2\pi i} = 1.$$

Another example of cyclic groups

The set $\mathbb{C}^\times$ of complex numbers $z \neq 0$ forms a group under multiplication.
It contains a cyclic subgroup C_n, with $|C_n| = n$, consisting of the numbers

$$1, g = e^{\frac{2\pi i}{n}}, g^2 = e^{\frac{4\pi i}{n}}, \ldots, g^k = e^{\frac{2k\pi i}{n}}, \ldots g^{n-1} = e^{\frac{2(n-1)\pi i}{n}}.$$

The nth power of g is

$$g^n = e^{\frac{2n\pi i}{n}} = e^{2\pi i} = 1.$$

Multiplication in cyclic groups

Suppose $g \in G$ is a generator. Then every element of G is of the form g^a, where a can be negative if $|G|$ is infinite and $g^0 = e$.

Fact

The product of g^a and g^b is g^{a+b}.

The proof is the same as for addition of exponents in the multiplication of real numbers. If $a, b \geq 0$ then we just put them in order. If $a > 0 and -b < 0$ we write

$$g^a \cdot g^{-b} = [g \cdot g \cdot \dots \cdot g] \cdot [g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}]$$

(a copies of g, b copies of g^{-1}). Then we cancel the $g \cdot g^{-1}$ until there are only $a - b$ g's or $b - a$ g^{-1}'s left.

Multiplication in cyclic groups

Suppose $g \in G$ is a generator. Then every element of G is of the form g^a, where a can be negative if $|G|$ is infinite and $g^0 = e$.

Fact

The product of g^a and g^b is g^{a+b}.

The proof is the same as for addition of exponents in the multiplication of real numbers. If $a, b \geq 0$ then we just put them in order. If $a > 0 and - b < 0$ we write

$$g^a \cdot g^{-b} = [g \cdot g \cdot \dots \cdot g] \cdot [g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}]$$

(a copies of g, b copies of g^{-1}). Then we cancel the $g \cdot g^{-1}$ until there are only $a - b$ g's or $b - a$ g^{-1}'s left.

Multiplication in cyclic groups

Suppose $g \in G$ is a generator. Then every element of G is of the form g^a, where a can be negative if $|G|$ is infinite and $g^0 = e$.

Fact

The product of g^a and g^b is g^{a+b}.

The proof is the same as for addition of exponents in the multiplication of real numbers. If $a, b \geq 0$ then we just put them in order. If $a > 0 and - b < 0$ we write

$$g^a \cdot g^{-b} = [g \cdot g \cdot \dots \cdot g] \cdot [g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}]$$

(a copies of g, b copies of g^{-1}). Then we cancel the $g \cdot g^{-1}$ until there are only $a - b$ g's or $b - a$ g^{-1}'s left.

Multiplication in cyclic groups

Suppose $g \in G$ is a generator. Then every element of G is of the form g^a, where a can be negative if $|G|$ is infinite and $g^0 = e$.

Fact

The product of g^a and g^b is g^{a+b}.

The proof is the same as for addition of exponents in the multiplication of real numbers. If $a, b \geq 0$ then we just put them in order. If $a > 0 and - b < 0$ we write

$$g^a \cdot g^{-b} = [g \cdot g \cdot \cdots \cdot g] \cdot [g^{-1} \cdot g^{-1} \cdot \cdots \cdot g^{-1}]$$

(a copies of g, b copies of g^{-1}). Then we cancel the $g \cdot g^{-1}$ until there are only $a - b$ g's or $b - a$ g^{-1}'s left.

Generators in $\mathbb{Z}_n$

In $\mathbb{Z}_n$ we write $k \cdot [a]$ for the k-th "power" $[a]^k$ to avoid confusion. We know that $[1]$ is a generator in $\mathbb{Z}_n$, the elements are

$$[0], [1], [2] = [1] + [1], [3] = 3 \cdot [1], \ldots [n-1] = (n-1) \cdot [1].$$

What other elements can be generators? More precisely, which elements $[a]$ have the property that, for any $[b] \in \mathbb{Z}_n$, there is k such that $[b] = k \cdot [a]$? Think of this as solving an equation for k.
The answer: $[a]$ is a generator if and only if $gcd(a, n) = 1$.

Generators in $\mathbb{Z}_n$

In $\mathbb{Z}_n$ we write $k \cdot [a]$ for the k-th "power" $[a]^k$ to avoid confusion. We know that $[1]$ is a generator in $\mathbb{Z}_n$, the elements are

$$[0], [1], [2] = [1] + [1], [3] = 3 \cdot [1], \ldots [n-1] = (n-1) \cdot [1].$$

What other elements can be generators? More precisely, which elements $[a]$ have the property that, for any $[b] \in \mathbb{Z}_n$, there is k such that $[b] = k \cdot [a]$? Think of this as solving an equation for k.
The answer: $[a]$ is a generator if and only if $gcd(a, n) = 1$.

Generators in $\mathbb{Z}_n$

In $\mathbb{Z}_n$ we write $k \cdot [a]$ for the k-th "power" $[a]^k$ to avoid confusion.
We know that $[1]$ is a generator in $\mathbb{Z}_n$, the elements are

$$[0], [1], [2] = [1] + [1], [3] = 3 \cdot [1], \ldots [n-1] = (n-1) \cdot [1].$$

What other elements can be generators? More precisely, which elements $[a]$ have the property that, for any $[b] \in \mathbb{Z}_n$, there is k such that $[b] = k \cdot [a]$? Think of this as solving an equation for k.
The answer: $[a]$ is a generator if and only if $gcd(a, n) = 1$.

Generators in $\mathbb{Z}_n$

We claim $[a]$ is a generator if and only if $gcd(a, n) = 1$.

Proof.

Suppose $gcd(a, n) = 1$. Then by Bezout there is c such that $ca \equiv 1 \pmod{n}$. Thus

$$c \cdot [a] = [ca] = [1].$$

Then for any b, we can take $k = bc$:

$$bc \cdot [a] = b \cdot [ca] = b \cdot [1] = [b].$$

Suppose $gcd(a, n) = d > 1$. Then for any k, $k \cdot [a] = [ka]$ and $gcd(ka, n) \geq d$. So ka can never be congruent to $1 \pmod{n}$. □

Thus a cyclic group of order n has $\phi(n)$ generators, where $\phi(n)$ is Euler's ϕ function.

Definition of subgroup

Definition

Let G be a group. The subset $H \subset G$ is a subgroup if

- $e \in H$,
- for all $h, h' \in H$, $hh' \in H$;
- for all $h \in H$, $h^{-1} \in H$.

Example: Any $g \in G$ *generates* a subgroup denoted $\langle g \rangle$:

$$\langle g \rangle = \{e, g^a, g^{-b}\}.$$

It is the *smallest subgroup* containing g, and it is cyclic, because g is a generator.

Definition of subgroup

Definition

Let G be a group. The subset $H \subset G$ is a subgroup if

- $e \in H$,
- for all $h, h' \in H$, $hh' \in H$;
- for all $h \in H$, $h^{-1} \in H$.

Example: Any $g \in G$ *generates* a subgroup denoted $\langle g \rangle$:

$$\langle g \rangle = \{e, g^a, g^{-b}\}.$$

It is the *smallest subgroup* containing g, and it is cyclic, because g is a generator.

Cyclic subgroups

Proposition

Suppose G is finite. Then for any g, the subset

$$H = \{e, g, g^2, \dots\}$$

(positive powers only) is a subgroup.

Proof.

Since G is finite, so is any subset. Thus at some point the powers repeat: there are $i < j$ such that $g^i = g^j$. Then

$$e = (g^i)^{-1} \cdot g^i = (g^i)^{-1} \cdot g^j = g^{j-i} = g \cdot g^{j-i-1}.$$

Thus $g^{j-i-1} = g^{-1}$ and so every element of H has its inverse in H. □

Cyclic subgroups

Proposition

Suppose G is finite. Then for any g, the subset

$$H = \{e, g, g^2, \dots\}$$

(positive powers only) is a subgroup.

Proof.

Since G is finite, so is any subset. Thus at some point the powers repeat: there are $i < j$ such that $g^i = g^j$. Then

$$e = (g^i)^{-1} \cdot g^i = (g^i)^{-1} \cdot g^j = g^{j-i} = g \cdot g^{j-i-1}.$$

Thus $g^{j-i-1} = g^{-1}$ and so every element of H has its inverse in H. □

Cyclic subgroups

Proposition

Suppose G is finite. Then for any g, the subset

$$H = \{e, g, g^2, \dots\}$$

(positive powers only) is a subgroup.

Proof.

Since G is finite, so is any subset. Thus at some point the powers repeat: there are $i < j$ such that $g^i = g^j$. Then

$$e = (g^i)^{-1} \cdot g^i = (g^i)^{-1} \cdot g^j = g^{j-i} = g \cdot g^{j-i-1}.$$

Thus $g^{j-i-1} = g^{-1}$ and so every element of H has its inverse in H. □

Order of an element

We see that in a finite group G, for every element $g \in G$ there is a positive integer a (it was $j - i$ in the proof) such that $g^a = e$.

So there is a smallest positive integer n such that $g^n = e$. This element is the *order* of g, and the subgroup $\langle g \rangle \subset G$ is then a cyclic group of order n.

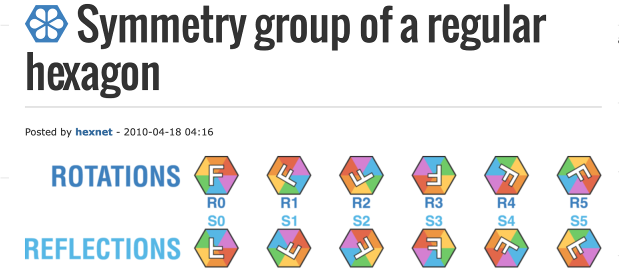
Order of an element

We see that in a finite group G, for every element $g \in G$ there is a positive integer a (it was $j - i$ in the proof) such that $g^a = e$.

So there is a smallest positive integer n such that $g^n = e$. This element is the *order* of g, and the subgroup $\langle g \rangle \subset G$ is then a cyclic group of order n.

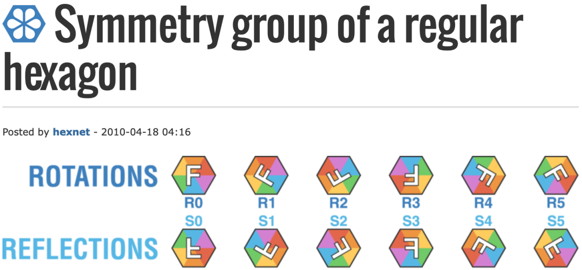
The dihedral group

Let $n \geq 3$ be an integer. The *dihedral group* D_{2n} (often written D_n, but not in this class) is the group of symmetries of the regular n-gon.



The dihedral group

Let $n \geq 3$ be an integer. The *dihedral group* D_{2n} (often written D_n, but not in this class) is the group of symmetries of the regular n-gon.



Properties of the dihedral group

The group D_{2n} contains a cyclic subgroup of rotations of order n. If we think of the n-gon inscribed in the unit circle around 0, then the rotations are by elements of C_n, the n-th roots of unity; or equivalently, by multiples of $\frac{2\pi}{n}$.

Let $s \in D_{2n}$ be rotation (counterclockwise) by $\frac{2\pi}{n}$, f (for flip) reflection in the y-axis.

Then $s^n = f^2 = e$. But

$$fsf = s^{-1}; \ \ fs = s^{-1}f = s^{n-1}f.$$

Properties of the dihedral group

The group D_{2n} contains a cyclic subgroup of rotations of order n. If we think of the n-gon inscribed in the unit circle around 0, then the rotations are by elements of C_n, the n-th roots of unity; or equivalently, by multiples of $\frac{2\pi}{n}$.
Let $s \in D_{2n}$ be rotation (counterclockwise) by $\frac{2\pi}{n}$, f (for flip) reflection in the y-axis.
Then $s^n = f^2 = e$. But

$$fsf = s^{-1};\ fs = s^{-1}f = s^{n-1}f.$$

Picture of the formula $fsf = s^{-1}$

Multliplication in D_{2n}

So the elements of D_{2n} are all of the form $e, s, s^2, \ldots, s^{n-1}$ and $f, fs, fs^2, \ldots, fs^{n-1}$.

Thus there are $2n$ elements. Any two elements can be multiplied using the relations we know:

$$s^a \cdot f = s^{a-1} \cdot f \cdot s^{-1} = s^{a-2} \cdot f \cdot s^{-2} \cdots = f \cdot s^{-a};$$

$$s^a \cdot fs^b = f \cdot s^{b-a}.$$

Multliplication in D_{2n}

So the elements of D_{2n} are all of the form $e, s, s^2, \ldots, s^{n-1}$ and $f, fs, fs^2, \ldots, fs^{n-1}$.
Thus there are $2n$ elements. Any two elements can be multiplied using the relations we know:

$$s^a \cdot f = s^{a-1} \cdot f \cdot s^{-1} = s^{a-2} \cdot f \cdot s^{-2} \cdots = f \cdot s^{-a};$$

$$s^a \cdot fs^b = f \cdot s^{b-a}.$$

Multliplication in D_{2n}

So the elements of D_{2n} are all of the form $e, s, s^2, \ldots, s^{n-1}$ and $f, fs, fs^2, \ldots, fs^{n-1}$.
Thus there are $2n$ elements. Any two elements can be multiplied using the relations we know:

$$s^a \cdot f = s^{a-1} \cdot f \cdot s^{-1} = s^{a-2} \cdot f \cdot s^{-2} \cdots = f \cdot s^{-a};$$

$$s^a \cdot fs^b = f \cdot s^{b-a}.$$

Multliplication in D_{2n}

Lemma

For any G and $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$.

The proof is: $h^{-1}g^{-1} \cdot (gh) = h^{-1} \cdot h = e$.

Now we compute

$$(fs^i)^{-1} = (s^i)^{-1}f^{-1} = s^{-i}f = fs^i.$$

Thus for any i,

$$(fs^i)^2 = e.$$

Indeed, each fs^i is a reflection around some axis. (Check geometrically.)

Multliplication in D_{2n}

Lemma

For any G and $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$.

The proof is: $h^{-1}g^{-1} \cdot (gh) = h^{-1} \cdot h = e$.
Now we compute

$$(fs^i)^{-1} = (s^i)^{-1}f^{-1} = s^{-i}f = fs^i.$$

Thus for any i,

$$(fs^i)^2 = e.$$

Indeed, each fs^i is a reflection around some axis. (Check geometrically.)

Multliplication in D_{2n}

Lemma

For any G and $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$.

The proof is: $h^{-1}g^{-1} \cdot (gh) = h^{-1} \cdot h = e$.
Now we compute

$$(fs^i)^{-1} = (s^i)^{-1}f^{-1} = s^{-i}f = fs^i.$$

Thus for any i,

$$(fs^i)^2 = e.$$

Indeed, each fs^i is a reflection around some axis. (Check geometrically.)

Every subgroup of a cyclic group is cyclic

The following theorem will be used constantly.

Theorem

Let G be a cyclic group, $H \subset G$ a subgroup. Then H is cyclic.

Proof: Let $g \in G$ be a generator. Let a be the smallest integer > 0 such that $\gamma = g^a \in H$. If there is no such integer then $H = \{e\}$.
Otherwise, let $h \in H$. Then $h = g^c$ for some c. We may assume $c > 0$; if not, replace h by h^{-1}.
Thus g^a and $g^c \in H$. So for any $r, s \in \mathbb{Z}$,

$$(g^a)^r \cdot (g^c)^s = g^{ra+sc} \in H.$$

By Bezout's theorem, if $d = gcd(a, c)$, then $d = ra + sc$ for some r, s, so $g^d \in H$. Moreover $d \mid a$ and so $d \leq a$.

Every subgroup of a cyclic group is cyclic

The following theorem will be used constantly.

Theorem

Let G be a cyclic group, $H \subset G$ a subgroup. Then H is cyclic.

Proof: Let $g \in G$ be a generator. Let a be the smallest integer > 0 such that $\gamma = g^a \in H$. If there is no such integer then $H = \{e\}$. Otherwise, let $h \in H$. Then $h = g^c$ for some c. We may assume $c > 0$; if not, replace h by h^{-1}.

Thus g^a and $g^c \in H$. So for any $r, s \in \mathbb{Z}$,

$$(g^a)^r \cdot (g^c)^s = g^{ra+sc} \in H.$$

By Bezout's theorem, if $d = gcd(a, c)$, then $d = ra + sc$ for some r, s, so $g^d \in H$. Moreover $d \mid a$ and so $d \leq a$.

Every subgroup of a cyclic group is cyclic

The following theorem will be used constantly.

Theorem

Let G be a cyclic group, $H \subset G$ a subgroup. Then H is cyclic.

Proof: Let $g \in G$ be a generator. Let a be the smallest integer > 0 such that $\gamma = g^a \in H$. If there is no such integer then $H = \{e\}$. Otherwise, let $h \in H$. Then $h = g^c$ for some c. We may assume $c > 0$; if not, replace h by h^{-1}.
Thus g^a and $g^c \in H$. So for any $r, s \in \mathbb{Z}$,

$$(g^a)^r \cdot (g^c)^s = g^{ra+sc} \in H.$$

By Bezout's theorem, if $d = gcd(a, c)$, then $d = ra + sc$ for some r, s, so $g^d \in H$. Moreover $d \mid a$ and so $d \leq a$.

Every subgroup of a cyclic group is cyclic

The following theorem will be used constantly.

Theorem

Let G be a cyclic group, $H \subset G$ a subgroup. Then H is cyclic.

Proof: Let $g \in G$ be a generator. Let a be the smallest integer > 0 such that $\gamma = g^a \in H$. If there is no such integer then $H = \{e\}$. Otherwise, let $h \in H$. Then $h = g^c$ for some c. We may assume $c > 0$; if not, replace h by h^{-1}.
Thus g^a and $g^c \in H$. So for any $r, s \in \mathbb{Z}$,

$$(g^a)^r \cdot (g^c)^s = g^{ra+sc} \in H.$$

By Bezout's theorem, if $d = gcd(a, c)$, then $d = ra + sc$ for some r, s, so $g^d \in H$. Moreover $d \mid a$ and so $d \leq a$.

Subgroups of cyclic groups

By Bezout's theorem, if $d = gcd(a, c)$, then $d = ra + sc$ for some r, s, so $g^d \in H$. Moreover $d \mid a$ and so $d \leq a$.
Since a is chosen to be minimum, $d = a$. But since we also know $d \mid c$, $b = c/d$ means $h = \gamma^b$. Thus γ is a generator of H. This completes the proof.

Theorem

Let G be a finite cyclic group, $|G| = n$. Then for every divisor d of n, there is exactly one subgroup $H \subset G$ with $|H| = d$.

Subgroups of cyclic groups

By Bezout's theorem, if $d = gcd(a, c)$, then $d = ra + sc$ for some r, s, so $g^d \in H$. Moreover $d \mid a$ and so $d \leq a$.
Since a is chosen to be minimum, $d = a$. But since we also know $d \mid c$, $b = c/d$ means $h = \gamma^b$. Thus γ is a generator of H. This completes the proof.

Theorem

Let G be a finite cyclic group, $|G| = n$. Then for every divisor d of n, there is exactly one subgroup $H \subset G$ with $|H| = d$.

Subgroups of cyclic groups

By Bezout's theorem, if $d = gcd(a, c)$, then $d = ra + sc$ for some r, s, so $g^d \in H$. Moreover $d \mid a$ and so $d \leq a$.
Since a is chosen to be minimum, $d = a$. But since we also know $d \mid c$, $b = c/d$ means $h = \gamma^b$. Thus γ is a generator of H. This completes the proof.

Theorem

Let G be a finite cyclic group, $|G| = n$. Then for every divisor d of n, there is exactly one subgroup $H \subset G$ with $|H| = d$.

Subgroups of cyclic groups

By Bezout's theorem, if $d = gcd(a, c)$, then $d = ra + sc$ for some r, s, so $g^d \in H$. Moreover $d \mid a$ and so $d \leq a$.
Since a is chosen to be minimum, $d = a$. But since we also know $d \mid c$, $b = c/d$ means $h = \gamma^b$. Thus γ is a generator of H. This completes the proof.

Theorem

Let G be a finite cyclic group, $|G| = n$. Then for every divisor d of n, there is exactly one subgroup $H \subset G$ with $|H| = d$.

Proof of the theorem on subgroups of cyclic groups

Proof of existence Let $d \mid n$, so $n = md$ for some m. Let g be a generator of G. Consider the subset $\{e, g^m, g^{2m}, \ldots, g^{(d-1)m}\} \subset G$. It has d elements and it's easy to see it's a subgroup.

Proof of uniqueness Suppose $H \subset G$ is a subgroup, $|H| = d$. We know H is cyclic. Let h be a generator of H, so $h^d = e$. But $h = g^a$ for some minimal $a > 0$. (Unless $|H| = 1$, in which case $H = \{e\}$.) Then

$$g^{ad} = h^d = e$$

so ad is a multiple of $n = md$. Thus a is a multiple of m. Since a is minimal, $a = m$, and we are done.

Proof of the theorem on subgroups of cyclic groups

Proof of existence Let $d \mid n$, so $n = md$ for some m. Let g be a generator of G. Consider the subset $\{e, g^m, g^{2m}, \ldots, g^{(d-1)m}\} \subset G$. It has d elements and it's easy to see it's a subgroup.

Proof of uniqueness Suppose $H \subset G$ is a subgroup, $|H| = d$. We know H is cyclic. Let h be a generator of H, so $h^d = e$. But $h = g^a$ for some minimal $a > 0$. (Unless $|H| = 1$, in which case $H = \{e\}$.) Then

$$g^{ad} = h^d = e$$

so ad is a multiple of $n = md$. Thus a is a multiple of m. Since a is minimal, $a = m$, and we are done.

Proof of the theorem on subgroups of cyclic groups

Proof of existence Let $d \mid n$, so $n = md$ for some m. Let g be a generator of G. Consider the subset $\{e, g^m, g^{2m}, \dots, g^{(d-1)m}\} \subset G$. It has d elements and it's easy to see it's a subgroup.

Proof of uniqueness Suppose $H \subset G$ is a subgroup, $|H| = d$. We know H is cyclic. Let h be a generator of H, so $h^d = e$. But $h = g^a$ for some minimal $a > 0$. (Unless $|H| = 1$, in which case $H = \{e\}$.) Then

$$g^{ad} = h^d = e$$

so ad is a multiple of $n = md$. Thus a is a multiple of m. Since a is minimal, $a = m$, and we are done.

Proof of the theorem on subgroups of cyclic groups

Proof of existence Let $d \mid n$, so $n = md$ for some m. Let g be a generator of G. Consider the subset $\{e, g^m, g^{2m}, \ldots, g^{(d-1)m}\} \subset G$. It has d elements and it's easy to see it's a subgroup.

Proof of uniqueness Suppose $H \subset G$ is a subgroup, $|H| = d$. We know H is cyclic. Let h be a generator of H, so $h^d = e$. But $h = g^a$ for some minimal $a > 0$. (Unless $|H| = 1$, in which case $H = \{e\}$.) Then

$$g^{ad} = h^d = e$$

so ad is a multiple of $n = md$. Thus a is a multiple of m. Since a is minimal, $a = m$, and we are done.

Homomorphisms

Let G and H be groups, with identity elements e_G and e_H. A *homomorphism* from G to H is a function $f : G \to H$ such that, for all $g, g' \in G$,

$$f(gg') = f(g)f(g').$$

This already implies that

$$f(e_G) = f(e_H).$$

Indeed, let $f(e_G) = h$. Now $e_G \cdot e_G = e_G$ by definition, so

$$f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G) \Rightarrow h = h \cdot h.$$

Now multiply both sides by h^{-1}:

$$e_H = h^{-1}h = h^{-1}h \cdot h = h.$$

In the same way, we prove that, for all g, $f(g^{-1}) = f(g)^{-1}$.

Homomorphisms

Let G and H be groups, with identity elements e_G and e_H. A *homomorphism* from G to H is a function $f : G \to H$ such that, for all $g, g' \in G$,

$$f(gg') = f(g)f(g').$$

This already implies that

$$f(e_G) = f(e_H).$$

Indeed, let $f(e_G) = h$. Now $e_G \cdot e_G = e_G$ by definition, so

$$f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G) \Rightarrow h = h \cdot h.$$

Now multiply both sides by h^{-1}:

$$e_H = h^{-1}h = h^{-1}h \cdot h = h.$$

In the same way, we prove that, for all g, $f(g^{-1}) = f(g)^{-1}$.

Homomorphisms

Let G and H be groups, with identity elements e_G and e_H. A *homomorphism* from G to H is a function $f : G \to H$ such that, for all $g, g' \in G$,

$$f(gg') = f(g)f(g').$$

This already implies that

$$f(e_G) = f(e_H).$$

Indeed, let $f(e_G) = h$. Now $e_G \cdot e_G = e_G$ by definition, so

$$f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G) \Rightarrow h = h \cdot h.$$

Now multiply both sides by h^{-1}:

$$e_H = h^{-1}h = h^{-1}h \cdot h = h.$$

In the same way, we prove that, for all g, $f(g^{-1}) = f(g)^{-1}$.

Homomorphisms

Let G and H be groups, with identity elements e_G and e_H. A *homomorphism* from G to H is a function $f : G \to H$ such that, for all $g, g' \in G$,

$$f(gg') = f(g)f(g').$$

This already implies that

$$f(e_G) = f(e_H).$$

Indeed, let $f(e_G) = h$. Now $e_G \cdot e_G = e_G$ by definition, so

$$f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G) \Rightarrow h = h \cdot h.$$

Now multiply both sides by h^{-1}:

$$e_H = h^{-1}h = h^{-1}h \cdot h = h.$$

In the same way, we prove that, for all g, $f(g^{-1}) = f(g)^{-1}$.

Examples of homomorphisms

Example

Suppose $m \mid n$ are positive integers. Then reduction modulo n can be followed by reduction modulo m:

$$f : \mathbb{Z}_n \to \mathbb{Z}_m ; f([a]_n) = [a]_m.$$

Example

If $G = GL(n, \mathbb{R})$, $H = \mathbb{R}^\times$, $\det : G \to H$ is a homomorphism. This is the familiar fact:

$$\det(AB) = \det(A) \cdot \det(B)$$

if A and B are invertible $n \times n$ matrices.

Example

Let $G = \mathbb{R}^n$, $H = \mathbb{R}^m$. Then a linear transformation $T : \mathbb{R}^n \to \mathbb{R}^m$ is a

Examples of homomorphisms

Example

Suppose $m \mid n$ are positive integers. Then reduction modulo n can be followed by reduction modulo m:

$$f : \mathbb{Z}_n \to \mathbb{Z}_m ; f([a]_n) = [a]_m.$$

Example

If $G = GL(n, \mathbb{R})$, $H = \mathbb{R}^\times$, $\det : G \to H$ is a homomorphism. This is the familiar fact:

$$\det(AB) = \det(A) \cdot \det(B)$$

if A and B are invertible $n \times n$ matrices.

Example

Let $G = \mathbb{R}^n$, $H = \mathbb{R}^m$. Then a linear transformation $T : \mathbb{R}^n \to \mathbb{R}^m$ is a

Examples of homomorphisms

Example

Suppose $m \mid n$ are positive integers. Then reduction modulo n can be followed by reduction modulo m:

$$f : \mathbb{Z}_n \to \mathbb{Z}_m; f([a]_n) = [a]_m.$$

Example

If $G = GL(n, \mathbb{R})$, $H = \mathbb{R}^\times$, $\det : G \to H$ is a homomorphism. This is the familiar fact:

$$\det(AB) = \det(A) \cdot \det(B)$$

if A and B are invertible $n \times n$ matrices.

Example

Let $G = \mathbb{R}^n$, $H = \mathbb{R}^m$. Then a linear transformation $T : \mathbb{R}^n \to \mathbb{R}^m$ is a

Properties of homomorphisms

A bijective homomorphism $f : G \to H$. is called an *isomorphism*. If $G = H$ it is called an *automorphism*.

Proposition

Let $f : G \to H$ be a bijective homomorphism. Let $f^{-1} : H \to G$ be the inverse function. Then f^{-1} is also a homomorphism (thus an isomorphism).

Proof: Let $h_1, h_2 \in H$. By assumption, there are unique $g_1, g_2 \in G$ such that $f(g_1) = h_1, f(g_2) = h_2$. Thus

$$f(g_1 g_2) = f(g_1) f(g_2) = h_1 \cdot h_2.$$

Hence

$$f^{-1}(h_1 \cdot h_2) = g_1 g_2 = f^{-1}(h_1) \cdot f^{-1}(h_2).$$

Properties of homomorphisms

A bijective homomorphism $f : G \to H$. is called an *isomorphism*. If $G = H$ it is called an *automorphism*.

Proposition

Let $f : G \to H$ be a bijective homomorphism. Let $f^{-1} : H \to G$ be the inverse function. Then f^{-1} is also a homomorphism (thus an isomorphism).

Proof: Let $h_1, h_2 \in H$. By assumption, there are unique $g_1, g_2 \in G$ such that $f(g_1) = h_1, f(g_2) = h_2$. Thus

$$f(g_1 g_2) = f(g_1) f(g_2) = h_1 \cdot h_2.$$

Hence

$$f^{-1}(h_1 \cdot h_2) = g_1 g_2 = f^{-1}(h_1) \cdot f^{-1}(h_2).$$

Examples of homomorphisms

Example

Let $G = D_{2n}$, with generators s, f; $H = \mathbb{Z}_2$. Define $\phi : G \to H$ by the formula

$$\phi(s^a) = [0]; \phi(fs^b) = [1].$$

Then for example

$$\phi(fs^b \cdot fs^c) = \phi(f^2 s^{c-b}) = \phi(s^{c-b}) = [0] = [1] + [1] = \phi(fs^b) + \phi(fs^c).$$

Examples of homomorphisms

Example

Let $G = D_{2n}$, with generators s, f; $H = \mathbb{Z}_2$. Define $\phi : G \to H$ by the formula

$$\phi(s^a) = [0]; \phi(fs^b) = [1].$$

Then for example

$$\phi(fs^b \cdot fs^c) = \phi(f^2 s^{c-b}) = \phi(s^{c-b}) = [0] = [1] + [1] = \phi(fs^b) + \phi(fs^c).$$

More on equivalence relations