Group Theory

Topic No. 1

Group Theory

Properties of Real Numbers

Properties of Real Numbers

Number Systems

$\mathbb{N}$ ={ 1, 2, 3, … }

$\mathbb{Z}$={…, -2, -1, 0, 1, 2, … }

$\mathbb{Q}$={p/q | p, q ∈ $\mathbb{Z}$ and q≠0}

$\mathbb{Q}'$= Set of Irrational Numbers

$\mathbb{R}$=$\mathbb{Q}$ ∪ $\mathbb{Q}'$

Properties of Real Numbers

0.131313…=0.13+ 0.0013+0.000013+…

=13/100+13/10000+

13/1000000+…

=(13/100)(1+1/100+

1/10000+…)

=(13/100)(100/99)

=13/99

Properties of Real Numbers

- e=2.718281828459045… ∈ $\mathbb{Q}'$
- √2=1.414213562373095… ∈ $\mathbb{Q}'$
- √5=2.23606797749978… ∈ $\mathbb{Q}'$
- ∀ *a*, b ∈ $\mathbb{R}$, *a*.b ∈ $\mathbb{R}$
- ∀ *a*, b ∈ $\mathbb{R}$, *a*+b ∈ $\mathbb{R}$
- ∀ *a*, b, c ∈ $\mathbb{R}$, (*a*+b)+c=*a*+(b+c)
- For example, (1/4+3)+ √7=(13+4 √7)/4=1/4+(3+ √7)

Properties of Real Numbers

- ∀ *a*, b, c ∈ $\mathbb{R}$, (*a*b)c=*a*(bc)
- For instance, ((-2/3)4)√2=(-8/3) √2 =(-2/3)(4 √2)
- For every *a* ∈ $\mathbb{R}$ and 0 ∈ $\mathbb{R}$, *a*+0=*a*=0+*a*
- For every *a* ∈ $\mathbb{R}$ and 1 ∈ $\mathbb{R}$, *a*.1=*a*=1.*a*
- For every *a* ∈ $\mathbb{R}$ there exists -*a* ∈ $\mathbb{R}$ such that *a*+(-*a*)=*0*=(-*a*)+*a*
- For every *a* ∈ $\mathbb{R}$\{0} there exists 1/*a* ∈ $\mathbb{R}$\{0} such that *a*(1/*a*)=*1*=(1/*a*)*a*
- ∀ *a*, b ∈ $\mathbb{R}$, *a*+b=b+*a*
- ∀ *a*, b ∈ $\mathbb{R}$, *a*.b=b.*a*

Group Theory

Topic No. 2

Group Theory

Properties of Complex Numbers

Properties of Complex Numbers

- $\mathbb{C}=\{a+bi \mid a, b \in \mathbb{R}\}$
- $\forall\ a+bi, c+di \in \mathbb{C}$, $(a+bi)+(c+di)=(a+c)+(b+d)i \in \mathbb{C}$
- $\forall\ a+bi, c+di \in \mathbb{C}$, $(a+bi).(c+di)=(ac-bd)+(ad+bc)i \in \mathbb{C}$
- $\forall\ a+bi, c+di, e+fi \in \mathbb{C}$, $[(a+bi)+(c+di)]+(e+fi)=$ $[(a+c)+(b+d)i]+(e+fi)=[(a+c)+e]+[(b+d)+f]i$ $=[a+(c+e)]+[b+(d+f)]i=(a+bi)+[(c+e)+(d+f)i]=$ $(a+bi)+[(c+di)+(e+fi)]$

Properties of Complex Numbers

- $\forall\ a+bi, c+di, e+fi \in \mathbb{C}$, $[(a+bi).(c+di)].(e+fi)$
  $=[(ac-bd)+(bc+ad)i].(e+fi)$
  $=[(ac-bd)e-(bc+ad)f]+[(bc+ad)e+(ac-bd)f]i$
  $=[a(ce-df)-b(de+cf)]+[a(de+cf)]+b(ce-df)]i$
  $=(a+bi).[(ce-df)+(de+cf)i]=(a+bi).[(c+di).(e+fi)]$
- For every $a+bi \in \mathbb{C}$ and $0=0+0i \in \mathbb{C}$, $(a+bi)+0=$ $(a+bi)+(0+0i)=(a+0)+(b+0)i=a+bi=0+(a+bi)$
- For every $a+bi \in \mathbb{C}$ and $1=1+0i \in \mathbb{C}$, $(a+bi).1=$ $(a+bi).(1+0i)=(a.1-0b)+(b.1+0.a)i=a+bi=1.(a+bi)$

Properties of Complex Numbers

- For every $a+bi \in \mathbb{C}$ there exists $-a-bi \in \mathbb{C}$ such that $(a+bi)+(-a-bi)=(a+(-a))+(b+(-b))i=0+0i=0=(-a-bi)+(a+bi)$
- For every $a+bi \in \mathbb{C}\backslash\{0\}$ there exists
  $1/(a+bi)=a/(a^2+b^2)-(b/(a^2+b^2))i \in \mathbb{C}\backslash\{0\}$
  such that $(a+bi).(a/(a^2+b^2)-(b/(a^2+b^2))i\ )$
  $= (a^2+b^2)/(a^2+b^2)+((ab-ab)/(a^2+b^2))i=1+0i=1$
  $=(a/(a^2+b^2)-(b/(a^2+b^2))i\ )(a+bi)$

Properties of Complex Numbers

- $\forall\ a+bi, c+di \in \mathbb{C}$,
  $(a+bi)+(c+di)=(a+c)+(b+d)i$
  $=(c+a)+(d+b)i=(c+di)+(a+bi)$
- $\forall\ a+bi, c+di \in \mathbb{C}$,
  $(a+bi).(c+di)$
  $=(ac-bd)+ (ad+bc)i$
  $=(ca-db)+(cb+da)i$
  $=(c+di).(a+bi)$

Group Theory

Topic No. 3

Group Theory

Binary Operations

Binary Operations

Definition

A binary operation $*$ on a set S is a function mapping S x S into S.

For each $(a, b) \in S \times S$, we will denote the element $*((a, b))$ of S by $a*b$.

Binary Operations

- Usual addition '+' is a binary operation on the sets $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{R}^+$, $\mathbb{Q}^+$, $\mathbb{Z}^+$
- Usual multiplication '.' is a binary operation on the sets $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{R}^+$, $\mathbb{Q}^+$, $\mathbb{Z}^+$
- Usual multiplication '.' is a binary operation on the sets $\mathbb{R}\backslash\{0\}$, $\mathbb{C}\backslash\{0\}$, $\mathbb{Q}\backslash\{0\}$, $\mathbb{Z}\backslash\{0\}$

Binary Operations

Let $M(\mathbb{R})$ be the set of all matrices with real entries.

The usual matrix addition is not a binary operation on this set since A+B is not defined for an ordered pair (A, B) of matrices having different numbers of rows or of columns.

Binary Operations

Usual addition '+' is not a binary operation on the sets $\mathbb{R}\backslash\{0\}$, $\mathbb{C}\backslash\{0\}$, $\mathbb{Q}\backslash\{0\}$, $\mathbb{Z}\backslash\{0\}$ since

$2+(-2)=0 \notin \mathbb{Z}\backslash\{0\}\subset\mathbb{Q}\backslash\{0\}$
$\subset \mathbb{R}\backslash\{0\} \subset \mathbb{C}\backslash\{0\}$.

Binary Operations

Definition

Let $*$ be a binary operation on S and let H be a subset of S.

The subset H is closed under $*$ if for all a, b ∈ H we also have a$*$b ∈ H.

In this case, the binary operation on H given by restricting $*$ to H is the induced operation of $*$ on H.

19

Binary Operations

Usual addition '+' on the set $\mathbb{R}$ of real numbers does not induce a binary operation on the set $\mathbb{R}\backslash\{0\}$ of nonzero real numbers because $2\in\mathbb{R}\backslash\{0\}$ and $-2\in\mathbb{R}\backslash\{0\}$, but $2+(-2)=0 \notin \mathbb{R}\backslash\{0\}$.

Thus $\mathbb{R}\backslash\{0\}$ is not closed under $+$.

20

Binary Operations

Usual multiplication '.' on the sets $\mathbb{R}$ and $\mathbb{Q}$ induces a binary operation on the sets $\mathbb{R}\backslash\{0\}$, $\mathbb{R}^+$ and $\mathbb{Q}\backslash\{0\}$, $\mathbb{Q}^+$, respectively.

21

Group Theory

Binary Operations

22

Binary Operations

- Let S be a set and $a,b\in S$.

23

Binary Operations

- Let S be a set and $a,b\in S$.
- A binary operation $*$ on S is a rule which assigns to any ordered pair (a,b) an element $a*b\in S$.

24

Binary Operations

Examples

- For $S=\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$,
  $a*b=a+b$

Binary Operations

Examples

- For $S=\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$,
  $a*b=a+b$
- For $S=\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$,
  $a*b=ab$
-

Binary Operations

Examples

- For $S=\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$,
  $a*b=a+b$
- For $S=\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$,
  $a*b=ab$
- For $S=\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$,
  $a*b=a-b$

Binary Operations

Examples

- For $S=\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$,
  $a*b=a+b$
- For $S=\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$,
  $a*b=ab$
- For $S=\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$,
  $a*b=a-b$
- For $S=\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$,
  $a*b=\min(a,b)$

Binary Operations

Examples

- For $S=\{1,2,3\}$
  $a*b=b$

Binary Operations

Examples

- For $S=\{1,2,3\}$
  $a*b=b$
- For example
  $1*2=2$,
  $1*1=1$,
  $2*3=3$.

Binary Operations

Examples

- For $S=\mathbb{Q},\ a*b=a/b$ is not everywhere defined since no rational number is assigned by this rule to the pair $(3,0)$.

Binary Operations

Examples

- For $S=\mathbb{Q},\ a*b=a/b$ is not everywhere defined since no rational number is assigned by this rule to the pair $(3,0)$.
- For $S=\mathbb{Z}^+,\ a*b=a/b$ is not a binary operation on $\mathbb{Z}^+$ since $\mathbb{Z}^+$ is not closed under $*$.

Binary Operations

Definition

- A binary operation $*$ on a set S is commutative if and only if $a*b=b*a$ for all $a,b\in S$.

Binary Operations

Definition

- A binary operation $*$ on a set S is associative if $(a*b)*c=a*(b*c)$ for all $a,b,c\in S$.

Binary Operations

Examples

- The binary operation $*$ defined by
$$a*b=a+b$$
is commutative and associative in $\mathbb{C}$.

Binary Operations

Examples

- The binary operation $*$ defined by
$$a*b=a+b$$
is commutative and associative in $\mathbb{C}$.
- The binary operation $*$ defined by
$$a*b=ab$$
is commutative and associative in $\mathbb{C}$.

Binary Operations

- The binary operation defined by $a*b=a-b$ is not commutative in $\mathbb{Z}$.

Binary Operations

- The binary operation defined by $a*b=a-b$ is not commutative in $\mathbb{Z}$.
- The binary operation given by $a*b=a-b$ is not associative in $\mathbb{Z}$.

Binary Operations

- The binary operation defined by $a*b=a-b$ is not commutative in $\mathbb{Z}$.
- The binary operation given by $a*b=a-b$ is not associative in $\mathbb{Z}$.
- For instance,

$$(a*b)*c=(4-7)-2=-5$$

but

$$a*(b*c)=4-(7-2)=-1.$$

Group Theory

Bijective Maps

Bijective Maps

Definition

- A function $f: X \to Y$ is called injective or one-to-one if
$f(x_1)=f(x_2) \Rightarrow x_1=x_2.$

Bijective Maps

Definition

- A function $f: X \to Y$ is called injective or one-to-one if
$f(x_1)=f(x_2) \Rightarrow x_1=x_2.$
or
$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2).$

Bijective Maps

Definition

- A function $f: X \to Y$ is called surjective or onto if for any $y \in Y$, there exists $x \in X$ with $y = f(x)$.

Bijective Maps

Definition

- A function $f: X \to Y$ is called surjective or onto if for any $y \in Y$, there exists $x \in X$ with $y = f(x)$. i.e. if the image $f(x)$ is the whole set Y.

Bijective Maps

Definition

- A bijective function or one-to-one correspondence is a function that is both injective and surjective.

Bijective Maps

Example

$f: \mathbb{R} \to \mathbb{R}^+, \ f(x) = 10^x$

Bijective Maps

Example

$f: \mathbb{R} \to \mathbb{R}^+, \ f(x) = 10^x$

$f(x) = f(y) \Rightarrow 10^x = 10^y \Rightarrow x = y$

Therefore, f is one-to-one.

Bijective Maps

Example

$f: \mathbb{R} \to \mathbb{R}^+, \ f(x) = 10^x$

$f(x) = f(y) \Rightarrow 10^x = 10^y \Rightarrow x = y$

Therefore, f is one-to-one.

If $r \in \mathbb{R}^+$, then $\log_{10} r \in \mathbb{R}$ such that $f(\log_{10} r) = 10^{\log_{10} r} = r$.

Bijective Maps

Example

$f:\mathbb{R}\to\mathbb{R}^+,\ \ f(x)=10^x$

$f(x)=f(y)\Rightarrow 10^x=10^y\Rightarrow x=y$

Therefore, f is one-to-one.

If $r\in\mathbb{R}^+$, then $\log_{10} r\in\mathbb{R}$ such that

$f(\log_{10} r)=10^{\log_{10} r}=r$.

It implies that f is onto.

Bijective Maps

Example

$f:\mathbb{R}\to\mathbb{R}^+,\ \ f(x)=10^x$

$f(x)=f(y)\Rightarrow 10^x=10^y\Rightarrow x=y$

Therefore, f is one-to-one.

If $r\in\mathbb{R}^+$, then $\log_{10} r\in\mathbb{R}$ such that

$f(\log_{10} r)=10^{\log_{10} r}=r$.

It implies that f is onto.

Hence f is bijective.

Bijective Maps

Example

$f:\mathbb{Z}\to\mathbb{Z},\ \ f(m)=3m$

Bijective Maps

Example

$f:\mathbb{Z}\to\mathbb{Z},\ \ f(m)=3m$

$f(m)=f(n)\Rightarrow 3m=3n\Rightarrow m=n$

Therefore, f is one-to-one.

Bijective Maps

Example

$f:\mathbb{Z}\to\mathbb{Z},\ \ f(m)=3m$

$f(m)=f(n)\Rightarrow 3m=3n\Rightarrow m=n$

Therefore, f is one-to-one.

We assume that $m\in\mathbb{Z}$ is the pre-image of $4\in\mathbb{Z}$,

then $f(m)=3m=4\Rightarrow m=4/3\notin\mathbb{Z}$.

It implies that f is not onto.

Bijective Maps

Example

$f:\mathbb{R}\to\mathbb{R},\ \ f(x)=x^2$.

Bijective Maps

Example

$f:\mathbb{R}\to\mathbb{R},\ \ f(x)=x^2.$
$f(-3)=f(3)=9$ but $-3\neq 3.$
Therefore, f is not one-to-one.

55

Bijective Maps

Example

$f:\mathbb{R}\to\mathbb{R},\ \ f(x)=x^2.$
$f(-3)=f(3)=9$ but $-3\neq 3.$
Therefore, f is not one-to-one.
We assume that $x\in\mathbb{R}$ is the pre-image of $-5\in\mathbb{R}$,
then $f(x)=x^2=-5\Rightarrow x=\sqrt{-5}\notin\mathbb{R}.$
It implies that f is not onto.

56

Bijective Maps

Definition

- Let $f:X\to Y$ be a function and let H be a subset of X. The image of H under f is given by $f[H]=\{f(h)\mid h\in H\}$.

57

Bijective Maps

Definition

- A function $f:X\to Y$ is called surjective or onto if $f[X]=Y$.

58

Bijective Maps

Example

$f:\mathbb{R}\to\mathbb{R}^+,\ \ f(x)=10^x$

59

Bijective Maps

Example

$f:\mathbb{R}\to\mathbb{R}^+,\ \ f(x)=10^x$

$f[\mathbb{R}]=\mathbb{R}^+$

Therefore, f is onto.

60

Bijective Maps

Example

$f:\mathbb{Z}\to\mathbb{Z},\ \ f(m)=3m$

Bijective Maps

Example

$f:\mathbb{Z}\to\mathbb{Z},\ \ f(m)=3m$

$f[\mathbb{Z}]=3\mathbb{Z}\neq\mathbb{Z}$

It implies that f is not onto.

Bijective Maps

Example

$f:\mathbb{R}\to\mathbb{R},\ \ f(x)=x^2$

Bijective Maps

Example

$f:\mathbb{R}\to\mathbb{R},\ \ f(x)=x^2$

$f[\mathbb{R}]=\mathbb{R}^+\cup\{0\}\neq\mathbb{R}$

So, f is not onto.

Group Theory

Inversion Theorem

Inversion Theorem

Lemma

If $f:X\to Y$ and $g:Y\to Z$ are two functions, then:

(i) If f and g are injective, $g\circ f$ is injective.

Inversion Theorem

Lemma

If $f : X \to Y$ and $g : Y \to Z$ are two functions, then:

(i) If f and g are injective, $g \circ f$ is injective.

(ii) If f and g are surjective, $g \circ f$ is surjective.

Inversion Theorem

Lemma

If $f : X \to Y$ and $g : Y \to Z$ are two functions, then:

(i) If f and g are injective, $g \circ f$ is injective.

(ii) If f and g are surjective, $g \circ f$ is surjective.

(iii) If f and g are bijective, $g \circ f$ is bijective.

Inversion Theorem

Proof

(i) Suppose that $(g \circ f)(x_1) = (g \circ f)(x_2)$ Then,

$g(f(x_1)) = g(f(x_2)) \Rightarrow f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

Inversion Theorem

Proof

(i) Suppose that $(g \circ f)(x_1) = (g \circ f)(x_2)$. Then,

$g(f(x_1)) = g(f(x_2)) \Rightarrow f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

(ii) Let $z \in Z$. Since g is surjective, there exists $y \in Y$ with $g(y) = z$.

Inversion Theorem

Proof

(i) Suppose that $(g \circ f)(x_1) = (g \circ f)(x_2)$ Then,

$g(f(x_1)) = g(f(x_2)) \Rightarrow f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

(ii) Let $z \in Z$. Since g is surjective, there exists $y \in Y$ with $g(y) = z$. Since f is also surjective, there exists $x \in X$ with $f(x) = y$.

Inversion Theorem

Proof

(i) Suppose that $(g \circ f)(x_1) = (g \circ f)(x_2)$ Then,

$g(f(x_1)) = g(f(x_2)) \Rightarrow f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

(ii) Let $z \in Z$. Since g is surjective, there exists $y \in Y$ with $g(y) = z$. Since f is also surjective, there exists $x \in X$ with $f(x) = y$. Hence,

$$(g \circ f)(x) = g(f(x)) = g(y) = z.$$

So, $g \circ f$ is surjective.

Inversion Theorem

Proof

(i) Suppose that $(g \circ f)(x_1) = (g \circ f)(x_2)$ Then,

$g(f(x_1)) = g(f(x_2)) \Rightarrow f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

(ii) Let $z \in Z$. Since g is surjective, there exists $y \in Y$ with $g(y) = z$. Since f is also surjective, there exists $x \in X$ with $f(x) = y$. Hence,

$$(g \circ f)(x) = g(f(x)) = g(y) = z.$$

So, $g \circ f$ is surjective.

(iii) This follows from parts (i) and (ii).

73

Inversion Theorem

Theorem

The function $f : X \to Y$ has an inverse if and only if f is bijective.

74

Inversion Theorem

Proof

Suppose that $h: Y \to X$ is an inverse of f.

75

Inversion Theorem

Proof

Suppose that $h: Y \to X$ is an inverse of f.

The function f is injective because

$f(x_1) = f(x_2) \Rightarrow (h \circ f)(x_1) = (h \circ f)(x_2) \Rightarrow x_1 = x_2$.

76

Inversion Theorem

Proof

Suppose that $h: Y \to X$ is an inverse of f.

The function f is injective because

$f(x_1) = f(x_2) \Rightarrow (h \circ f)(x_1) = (h \circ f)(x_2) \Rightarrow x_1 = x_2$.

The function f is surjective because if for any $y \in Y$ with $x = h(y)$, it follows that $f(x) = f(h(y)) = y$.

77

Inversion Theorem

Proof

Suppose that $h: Y \to X$ is an inverse of f.

The function f is injective because

$f(x_1) = f(x_2) \Rightarrow (h \circ f)(x_1) = (h \circ f)(x_2) \Rightarrow x_1 = x_2$.

The function f is surjective because if for any $y \in Y$ with $x = h(y)$, it follows that $f(x) = f(h(y)) = y$.

Therefore, f is bijective.

78

Inversion Theorem

Proof

Conversely, suppose that f is bijective. We define the function $h: Y \to X$ as follows.

Inversion Theorem

Proof

Conversely, suppose that f is bijective. We define the function $h: Y \to X$ as follows. For any $y \in Y$, there exists $x \in X$ with $y = f(x)$.

Since f is injective, there is only one such element x.

Inversion Theorem

Proof

Conversely, suppose that f is bijective. We define the function $h: Y \to X$ as follows. For any $y \in Y$, there exists $x \in X$ with $y = f(x)$.

Since f is injective, there is only one such element x.

Define $h(y) = x$. This function h is an inverse of f because

$f(h(y)) = f(x) = y$ and $h(f(x)) = h(y) = x$.

Group Theory

- **Isomorphic Binary Structures**

Isomorphic Binary Structures

- Let us consider a binary algebraic structure $\langle S, * \rangle$ to be a set S together with a binary operation $*$ on S.

Isomorphic Binary Structures

- Let us consider a binary algebraic structure $\langle S, * \rangle$ to be a set S together with a binary operation $*$ on S.
- Two binary structures $\langle S, * \rangle$ and $\langle S', *' \rangle$ are said to be isomorphic if there is a one-to-one correspondence between the elements x of S and the elements x' of S' such that

  $x \leftrightarrow x'$ and $y \leftrightarrow y' \Rightarrow x * y \leftrightarrow x' *' y'$.

Isomorphic Binary Structures

- Let us consider a binary algebraic structure $(S,*)$ to be a set S together with a binary operation $*$ on S.
- Two binary structures $(S,*)$ and $(S',*')$ are said to be isomorphic if there is a one-to-one correspondence between the elements x of S and the elements x' of S' such that

$$x \leftrightarrow x' \text{ and } y \leftrightarrow y' \Rightarrow x*y \leftrightarrow x'*'y'.$$

- A one-to-one correspondence exists if the sets S and S' have the same number of elements.

85

Isomorphic Binary Structures

Definition

- Let $\langle S,*\rangle$ and $\langle S',*'\rangle$ be binary algebraic structures. An isomorphism of S with S' is a one-to-one function ϕ mapping S onto S' such that

$$\phi(x*y)=\phi(x)*'\phi(y)\ \forall\ x,y\in S.$$

86

Isomorphic Binary Structures

How to show binary structures are isomorphic

- Step 1. Define the function ϕ that gives the isomorphism of S and S'.

87

Isomorphic Binary Structures

How to show binary structures are isomorphic

- Step 1. Define the function ϕ that gives the isomorphism of S and S'.
- Step 2. Show that ϕ is one-to-one.

88

Isomorphic Binary Structures

How to show binary structures are isomorphic

- Step 1. Define the function ϕ that gives the isomorphism of S and S'.
- Step 2. Show that ϕ is one-to-one.
- Step3. Show that ϕ is onto S'.

89

Isomorphic Binary Structures

How to show binary structures are isomorphic

- Step 1. Define the function ϕ that gives the isomorphism of S and S'.
- Step 2. Show that ϕ is one-to-one.
- Step3. Show that ϕ is onto S'.
- Step 4. Show that

$$\phi(x*y)=\phi(x)*'\phi(y)\ \forall\ x,y\in S.$$

90

Isomorphic Binary Structures

Example

- We show that the binary structure $\langle \mathbb{R}, + \rangle$ is isomorphic to the structure $\langle \mathbb{R}^+, . \rangle$.

Isomorphic Binary Structures

Example

- We show that the binary structure $\langle \mathbb{R}, + \rangle$ is isomorphic to the structure $\langle \mathbb{R}^+, . \rangle$.
- Step 1.
$$\phi : \mathbb{R} \to \mathbb{R}^+, \ \phi(x) = e^x$$

Isomorphic Binary Structures

Example

- We show that the binary structure $\langle \mathbb{R}, + \rangle$ is isomorphic to the structure $\langle \mathbb{R}^+, . \rangle$.
- Step 1.
$$\phi : \mathbb{R} \to \mathbb{R}^+, \ \phi(x) = e^x$$
- Step 2.
$$\phi(x) = \phi(y) \Rightarrow e^x = e^y \Rightarrow x = y.$$

Isomorphic Binary Structures

Example

- We show that the binary structure $\langle \mathbb{R}, + \rangle$ is isomorphic to the structure $\langle \mathbb{R}^+, . \rangle$.
- Step 1.
$$\phi : \mathbb{R} \to \mathbb{R}^+, \ \phi(x) = e^x$$
- Step 2.
$$\phi(x) = \phi(y) \Rightarrow e^x = e^y \Rightarrow x = y.$$
- Step3. If $r \in \mathbb{R}^+$, then $\ln(r) \in \mathbb{R}$ and
$$\phi(\ln r) = e^{\ln r} = r.$$

Isomorphic Binary Structures

Example

- We show that the binary structure $\langle \mathbb{R}, + \rangle$ is isomorphic to the structure $\langle \mathbb{R}^+, . \rangle$.
- Step 1. $\phi : \mathbb{R} \to \mathbb{R}^+, \ \phi(x) = e^x$
- Step 2. $\phi(x) = \phi(y) \Rightarrow e^x = e^y \Rightarrow x = y.$
- Step3. If $r \in \mathbb{R}^+$, then $\ln r \in \mathbb{R}$ and
$$\phi(\ln r) = e^{\ln r} = r.$$
- Step 4. $\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y) \ \forall \ x, y \in \mathbb{R}.$

Group Theory

- **Isomorphic Binary Structures**

Isomorphic Binary Structures

Example

- We show that the binary structure $\langle \mathbb{Z}, + \rangle$ is isomorphic to the structure $\langle 2\mathbb{Z}, + \rangle$.

97

Isomorphic Binary Structures

Example

- We show that the binary structure $\langle \mathbb{Z}, + \rangle$ is isomorphic to the structure $\langle 2\mathbb{Z}, + \rangle$.
- Step 1. $\phi : \mathbb{Z} \to 2\mathbb{Z},\ \phi(m) = 2m$

98

Isomorphic Binary Structures

Example

- We show that the binary structure $\langle \mathbb{Z}, + \rangle$ is isomorphic to the structure $\langle 2\mathbb{Z}, + \rangle$.
- Step 1. $\phi : \mathbb{Z} \to 2\mathbb{Z},\ \phi(m) = 2m$
- Step 2. $\phi(m) = \phi(n) \Rightarrow 2m = 2n \Rightarrow m = n.$

99

Isomorphic Binary Structures

Example

- We show that the binary structure $\langle \mathbb{Z}, + \rangle$ is isomorphic to the structure $\langle 2\mathbb{Z}, + \rangle$.
- Step 1. $\phi : \mathbb{Z} \to 2\mathbb{Z},\ \phi(m) = 2m$
- Step 2. $\phi(m) = \phi(n) \Rightarrow 2m = 2n \Rightarrow m = n.$
- Step3. If $n \in 2\mathbb{Z},$ then $m = n/2 \in \mathbb{Z}$ and
  $\phi(m) = 2(n/2) = n.$

100

Isomorphic Binary Structures

Example

- We show that the binary structure $\langle \mathbb{Z}, + \rangle$ is isomorphic to the structure $\langle 2\mathbb{Z}, + \rangle$.
- Step 1. $\phi : \mathbb{Z} \to 2\mathbb{Z},\ \phi(m) = 2m$
- Step 2. $\phi(m) = \phi(n) \Rightarrow 2m = 2n \Rightarrow m = n.$
- Step3. If $n \in 2\mathbb{Z},$ then $m = n/2 \in \mathbb{Z}$ and
  $\phi(m) = 2(n/2) = n.$
- Step 4.

$\phi(m+n) = 2(m+n) = 2m + 2n = \phi(m) + \phi(n)\ \forall\ m, n \in \mathbb{Z}.$

101

Isomorphic Binary Structures

How to show binary structures are not isomorphic

- How do we demonstrate that two binary structures $\langle S, * \rangle$ and $\langle S', *' \rangle$ are not isomorphic?

102

Isomorphic Binary Structures

How to show binary structures are not isomorphic

- How do we demonstrate that two binary structures $\langle S,*\rangle$ and $\langle S',*'\rangle$ are not isomorphic?
- There is no one-to-one function ϕ from S onto S' with the property
  $\phi(x*y)=\phi(x)*'\phi(y)\ \forall\ x,y\in S.$

103

Isomorphic Binary Structures

How to show binary structures are not isomorphic

- How do we demonstrate that two binary structures $\langle S,*\rangle$ and $\langle S',*'\rangle$ are not isomorphic?
- There is no one-to-one function ϕ from S onto S' with the property
  $\phi(x*y)=\phi(x)*'\phi(y)\ \forall\ x,y\in S.$
- In general, it is not feasible to try every possible one-to-one function mapping S onto S' and test whether it has homomorphism property.

104

Isomorphic Binary Structures

How to show binary structures are not isomorphic

- A structural property of a binary structure is one that must be shared by any isomorphic structure.

105

Isomorphic Binary Structures

How to show binary structures are not isomorphic

- A structural property of a binary structure is one that must be shared by any isomorphic structure.
- It is not concerned with names or some other nonstructural characteristics of the elements.

106

Isomorphic Binary Structures

How to show binary structures are not isomorphic

- A structural property of a binary structure is one that must be shared by any isomorphic structure.
- It is not concerned with names or some other nonstructural characteristics of the elements.
- A structural property is not concerned with what we consider to be the name of the binary operation.

107

Isomorphic Binary Structures

How to show binary structures are not isomorphic

- A structural property of a binary structure is one that must be shared by any isomorphic structure.
- It is not concerned with names or some other nonstructural characteristics of the elements.
- A structural property is not concerned with what we consider to be the name of the binary operation.
- The number of elements in the set S is a structural property of $\langle S,*\rangle$.

108

Isomorphic Binary Structures

How to show binary structures are not isomorphic

- In the event that there are one-to-one mappings of S onto S', we usually show that $\langle S, * \rangle$ is not isomorphic to $\langle S', *' \rangle$ by showing that one has some structural property that the other does not possess.

Isomorphic Binary Structures

Possible Structural Properties

- The set has four elements.

Isomorphic Binary Structures

Possible Structural Properties

- The set has four elements.
- The operation is commutative.

Isomorphic Binary Structures

Possible Structural Properties

- The set has four elements.
- The operation is commutative.
- $x * x = x$ for all $x \in S$.

Isomorphic Binary Structures

Possible Structural Properties

- The set has four elements.
- The operation is commutative.
- $x * x = x$ for all $x \in S$.
- The equation $a * x = b$ has a solution x in S for all $a, b \in S$.

Isomorphic Binary Structures

Possible Nonstructural Properties

- The number *4* is an element.

Isomorphic Binary Structures

Possible Nonstructural Properties

- The number *4* is an element.
- The operation is called "addition".

Isomorphic Binary Structures

Possible Nonstructural Properties

- The number *4* is an element.
- The operation is called "addition".
- The elements of S are matrices.

Isomorphic Binary Structures

Possible Nonstructural Properties

- The number *4* is an element.
- The operation is called "addition".
- The elements of S are matrices.
- S is a subset of $\mathbb{C}$.

Isomorphic Binary Structures

Example

- The binary structures $\langle \mathbb{Q}, + \rangle$ and $\langle \mathbb{R}, + \rangle$ are not isomorphic because $\mathbb{Q}$ has cardinality $\aleph_0$ (aleph-null) while $|\mathbb{R}| \neq \aleph_0$.

Isomorphic Binary Structures

Example

- We prove that the binary structures $\langle \mathbb{Q}, + \rangle$ and $\langle \mathbb{Z}, + \rangle$ under the usual addition are not isomorphic.

Isomorphic Binary Structures

Example

- We prove that the binary structures $\langle \mathbb{Q}, + \rangle$ and $\langle \mathbb{Z}, + \rangle$ under the usual addition are not isomorphic.
- Both $\mathbb{Q}$ and $\mathbb{Z}$ have cardinality $\aleph_0$, so there are lots of one-to-one functions mapping $\mathbb{Q}$ onto $\mathbb{Z}$.

Isomorphic Binary Structures

Example

- We prove that the binary structures $\langle \mathbb{Q}, + \rangle$ and $\langle \mathbb{Z}, + \rangle$ under the usual addition are not isomorphic.
- Both $\mathbb{Q}$ and $\mathbb{Z}$ have cardinality $\aleph_0$, so there are lots of one-to-one functions mapping $\mathbb{Q}$ onto $\mathbb{Z}$.
- The equation $x + x = c$ has a solution x for all $c \in \mathbb{Q}$ but this is not the case in $\mathbb{Z}$.

121

Isomorphic Binary Structures

Example

- We prove that the binary structures $\langle \mathbb{Q}, + \rangle$ and $\langle \mathbb{Z}, + \rangle$ under the usual addition are not isomorphic.
- Both $\mathbb{Q}$ and $\mathbb{Z}$ have cardinality $\aleph_0$, so there are lots of one-to-one functions mapping $\mathbb{Q}$ onto $\mathbb{Z}$.
- The equation $x + x = c$ has a solution x for all $c \in \mathbb{Q}$ but this is not the case in $\mathbb{Z}$.
- For example, the equation $x + x = 3$ has no solution in $\mathbb{Z}$.

122

Isomorphic Binary Structures

Example

- The binary structures $\langle \mathbb{C}, . \rangle$ and $\langle \mathbb{R}, . \rangle$ under usual multiplication are not isomorphic because the equation $x.x = c$ has solution x for all $c \in \mathbb{C}$ but $x.x = -1$ has no solution in $\mathbb{R}$.

123

Isomorphic Binary Structures

Example

- The binary structures $\langle M_2(\mathbb{R}), . \rangle$ and $\langle \mathbb{R}, . \rangle$ under usual matrix multiplication and number multiplication, respectively because multiplication of numbers is commutative, but multiplication of matrices is not.

124

Group Theory

- **Isomorphic Binary Structures**

125

Isomorphic Binary Structures

Example

- Is $\phi : \mathbb{Z} \to \mathbb{Z}$, $\phi(n) = 3n$ for $n \in \mathbb{Z}$ an isomorphism?

126

Isomorphic Binary Structures

Example
- Is $\phi:\mathbb{Z}\to\mathbb{Z},\ \phi(n)=3n$ for $n\in\mathbb{Z}$ an isomorphism?
- $\phi:\mathbb{Z}\to\mathbb{Z},\ \phi(n)=3n$

Isomorphic Binary Structures

Example
- Is $\phi:\mathbb{Z}\to\mathbb{Z},\ \phi(n)=3n$ for $n\in\mathbb{Z}$ an isomorphism?
- $\phi:\mathbb{Z}\to\mathbb{Z},\ \phi(n)=3n$
- $\phi(m)=\phi(n)\Rightarrow 3m=3n\Rightarrow m=n$

Isomorphic Binary Structures

Example
- Is $\phi:\mathbb{Z}\to\mathbb{Z},\ \phi(n)=3n$ for $n\in\mathbb{Z}$ an isomorphism?
- $\phi:\mathbb{Z}\to\mathbb{Z},\ \phi(n)=3n$
- $\phi(m)=\phi(n)\Rightarrow 3m=3n\Rightarrow m=n$
- Choose $5\in\mathbb{Z}$, $\phi(m)=3m=5$ but $m=5/3\notin\mathbb{Z}$

Isomorphic Binary Structures

Example
- Is $\phi:\mathbb{Z}\to\mathbb{Z},\ \phi(n)=3n$ for $n\in\mathbb{Z}$ an isomorphism?
- $\phi:\mathbb{Z}\to\mathbb{Z},\ \phi(n)=3n$
- $\phi(m)=\phi(n)\Rightarrow 3m=3n\Rightarrow m=n$
- Choose $5\in\mathbb{Z}$, $\phi(m)=3m=5$ but $m=5/3\notin\mathbb{Z}$

- Is $\phi:\mathbb{Z}\to\mathbb{Z},\ \phi(n)=3n$ homomorphism?

$\phi(m+n)=3(m+n)=3m+3n=\phi(m)+\phi(n)\ \forall\ m,n\in\mathbb{Z}$

Isomorphic Binary Structures

Example
- Is $\phi:\mathbb{Z}\to\mathbb{Z},\ \phi(n)=3n$ for $n\in\mathbb{Z}$ an isomorphism?
- $\phi:\mathbb{Z}\to\mathbb{Z},\ \phi(n)=3n$
- $\phi(m)=\phi(n)\Rightarrow 3m=3n\Rightarrow m=n$
- Choose $5\in\mathbb{Z}$, $\phi(m)=3m=5$ but $m=5/3\notin\mathbb{Z}$

- Is $\phi:\mathbb{Z}\to\mathbb{Z},\ \phi(n)=3n$ homomorphism?

$\phi(m+n)=3(m+n)=3m+3n=\phi(m)+\phi(n)\ \forall\ m,n\in\mathbb{Z}$

- $\langle\mathbb{Z},+\rangle\cong\langle 3\mathbb{Z},+\rangle$

Isomorphic Binary Structures

Example
- Is $\phi:\mathbb{Z}\to\mathbb{Z},\phi(n)=n+1$ for $n\in\mathbb{Z}$ an isomorphism?

Isomorphic Binary Structures

Example

- Is $\phi:\mathbb{Z}\to\mathbb{Z}, \phi(n)=n+1$ for $n\in\mathbb{Z}$ an isomorphism?
- $\phi:\mathbb{Z}\to\mathbb{Z},\ \phi(n)=n+1$

133

Isomorphic Binary Structures

Example

- Is $\phi:\mathbb{Z}\to\mathbb{Z}, \phi(n)=n+1$ for $n\in\mathbb{Z}$ an isomorphism?
- $\phi:\mathbb{Z}\to\mathbb{Z},\ \phi(n)=n+1$
- $\phi(m)=\phi(n)\Rightarrow m+1=n+1\Rightarrow m=n$

134

Isomorphic Binary Structures

Example

- Is $\phi:\mathbb{Z}\to\mathbb{Z}, \phi(n)=n+1$ for $n\in\mathbb{Z}$ an isomorphism?
- $\phi:\mathbb{Z}\to\mathbb{Z},\ \phi(n)=n+1$
- $\phi(m)=\phi(n)\Rightarrow m+1=n+1\Rightarrow m=n$
- For every $n\in\mathbb{Z}$, there exists $n-1\in\mathbb{Z}$ such that $$\phi(n-1)=n-1+1=n.$$

135

Isomorphic Binary Structures

Example

- Is $\phi:\mathbb{Z}\to\mathbb{Z}, \phi(n)=n+1$ for $n\in\mathbb{Z}$ an isomorphism?
- $\phi:\mathbb{Z}\to\mathbb{Z},\ \phi(n)=n+1$
- $\phi(m)=\phi(n)\Rightarrow m+1=n+1\Rightarrow m=n$
- For every $n\in\mathbb{Z}$, there exists $n-1\in\mathbb{Z}$ such that $$\phi(n-1)=n-1+1=n.$$
- $\phi(m+n)=m+n+1\neq\phi(m)+\phi(n)=m+n+2$

136

Isomorphic Binary Structures

Example

- Is $\phi:\mathbb{Q}\to\mathbb{Q}, \phi(x)=x/2$ for $x\in\mathbb{Q}$ isomorphism?

137

Isomorphic Binary Structures

Example

- Is $\phi:\mathbb{Q}\to\mathbb{Q}, \phi(x)=x/2$ for $x\in\mathbb{Q}$ isomorphism?
- $\phi:\mathbb{Q}\to\mathbb{Q},\ \phi(x)=x/2$

138

Isomorphic Binary Structures

Example

- Is $\phi:\mathbb{Q}\to\mathbb{Q}, \phi(x)=x/2$ for $x\in\mathbb{Q}$ isomorphism?
- $\phi:\mathbb{Q}\to\mathbb{Q},\ \phi(x)=x/2$
- $\phi(x)=\phi(y)\Rightarrow x/2=y/2\Rightarrow x=y$

Isomorphic Binary Structures

Example

- Is $\phi:\mathbb{Q}\to\mathbb{Q}, \phi(x)=x/2$ for $x\in\mathbb{Q}$ isomorphism?
- $\phi:\mathbb{Q}\to\mathbb{Q},\ \phi(x)=x/2$
- $\phi(x)=\phi(y)\Rightarrow x/2=y/2\Rightarrow x=y$
- For every $y\in\mathbb{Q}$, there exists $2y\in\mathbb{Q}$ such that $\phi(2y)=2y/2=y.$

Isomorphic Binary Structures

Example

- Is $\phi:\mathbb{Q}\to\mathbb{Q}, \phi(x)=x/2$ for $x\in\mathbb{Q}$ isomorphism?
- $\phi:\mathbb{Q}\to\mathbb{Q},\ \phi(x)=x/2$
- $\phi(x)=\phi(y)\Rightarrow x/2=y/2\Rightarrow x=y$
- For every $y\in\mathbb{Q}$, there exists $2y\in\mathbb{Q}$ such that $\phi(2y)=2y/2=y.$
- $\phi(x+y)=\frac{x+y}{2}=\frac{x}{2}+\frac{y}{2}=\phi(x)+\phi(y)$

Isomorphic Binary Structures

Example

- We prove that the binary structures $\langle\mathbb{Z},.\rangle$ and $\langle\mathbb{Z}^+,.\rangle$ under the usual multiplication are not isomorphic.

Isomorphic Binary Structures

Example

- We prove that the binary structures $\langle\mathbb{Z},.\rangle$ and $\langle\mathbb{Z}^+,.\rangle$ under the usual multiplication are not isomorphic.
- Both $\mathbb{Z}$ and $\mathbb{Z}^+$ have cardinality $\aleph_0$, so there are lots of one-to-one functions mapping $\mathbb{Z}$ onto $\mathbb{Z}^+$.

Isomorphic Binary Structures

Example

- We prove that the binary structures $\langle\mathbb{Z},.\rangle$ and $\langle\mathbb{Z}^+,.\rangle$ under the usual multiplication are not isomorphic.
- Both $\mathbb{Z}$ and $\mathbb{Z}^+$ have cardinality $\aleph_0$, so there are lots of one-to-one functions mapping $\mathbb{Z}$ onto $\mathbb{Z}^+$.
- In $\langle\mathbb{Z},.\rangle$ there are two elements x such that $x.x=x$, namely, *0* and *1*.

Isomorphic Binary Structures

Example

- We prove that the binary structures $\langle \mathbb{Z}, . \rangle$ and $\langle \mathbb{Z}^+, . \rangle$ under the usual multiplication are not isomorphic.
- Both $\mathbb{Z}$ and $\mathbb{Z}^+$ have cardinality $\aleph_0$, so there are lots of one-to-one functions mapping $\mathbb{Z}$ onto $\mathbb{Z}^+$.
- In $\langle \mathbb{Z}, . \rangle$ there are two elements x such that $x.x = x$, namely, *0* and *1*.
- However, in $\langle \mathbb{Z}^+, . \rangle$, there is only the single element *1*.

145

Group Theory

- **Isomorphic Binary Structures**

146

Group Theory

Groups

147

Group Theory

Associative Binary Operation

- A binary operation $*$ is called associative if $(a*b)*c = a*(b*c)$.

148

Group Theory

Example

- Can we solve
  $3 + x = 2$
  in $\mathbb{N}$?
- The equation is unsolvable in $\mathbb{N}$ since
  $-3 \notin \mathbb{N}$.

149

Group Theory

Example

- Can we solve $3 + x = 2$ in $\mathbb{Z}$?

150

Group Theory

Example

- Can we solve $3+x=2$ in $\mathbb{Z}$?
- add -3 on both sides

$$-3+(3+x)=-3+2$$

Group Theory

Example

- Can we solve $3+x=2$ in $\mathbb{Z}$?
- add -3 on both sides

$$-3+(3+x)=-3+2$$
$$(-3+3)+x=-3+2$$

Group Theory

Example

- Can we solve $3+x=2$ in $\mathbb{Z}$?
- add -3 on both sides

$$-3+(3+x)=-3+2$$
$$(-3+3)+x=-3+2$$

- Thus

$$0+x=-3+2$$

Group Theory

Example

- Can we solve $3+x=2$ in $\mathbb{Z}$?
- add -3 on both sides

$$-3+(3+x)=-3+2$$
$$(-3+3)+x=-3+2$$

- Thus

$$0+x=-3+2$$
$$\Rightarrow \quad x=-1.$$

Group Theory

Example

- Can we solve $3+x=2$ in $\mathbb{Z}$?
- add -3 on both sides

$$-3+(3+x)=-3+2$$
$$(-3+3)+x=-3+2$$

- Thus

$$0+x=-3+2$$
$$\Rightarrow \quad x=-1.$$

1. We use associative property
2. Existence of 0 with $0+x=x$
3. Existence of -3 with $-3+3=0$

Group Theory

Group(Definition)

A group $\langle G,*\rangle$ is a set G with binary operation $*$ satisfying the following axioms for all $a,b,c\in G$:

Group Theory

Group(Definition)
A group $(G,*)$ is a set G with binary operation $*$ satisfying the following axioms for all $a,b,c \in G$:

1. For $a,b \in G$, $a*b \in G$ **(closure)**

Group Theory

Group(Definition)
A group $(G,*)$ is a set G with binary operation $*$ satisfying the following axioms for all $a,b,c \in G$:

1. For $a,b \in G$, $a*b \in G$ **(closure)**
2. $(a*b)*c = a*(b*c)$ **(associative)**

Group Theory

Group(Definition)
A group $\langle G,* \rangle$ is a set G with binary operation $*$ satisfying the following axioms for all $a,b,c \in G$:

1. For $a,b \in G$, $a*b \in G$ **(closure)**
2. $(a*b)*c = a*(b*c)$ **(associative)**
3. There exists $e \in G$ such that **(identity)**
   $e*a = a*e = a$

Group Theory

Group(Definition)
A group $(G,*)$ is a set G with binary operation $*$ satisfying the following axioms for all $a,b,c \in G$:

1. For $a,b \in G$, $a*b \in G$ **(closure)**
2. $(a*b)*c = a*(b*c)$ **(associative)**
3. There exists $e \in G$ such that **(identity)**
   $e*a = a*e = a$
4. For every $a \in G$, there exists $a^{-1} \in G$ such that
   $a^{-1}*a = a*a^{-1} = e$ **(inverse)**

Group Theory

Example

- Can we solve equations of the form $a*x = b$ in a group $\langle G,* \rangle$?

Group Theory

Example

- Can we solve equations of the form $a*x = b$ in a group $\langle G,* \rangle$?

  $a'*(a*x) = a'*b$

Group Theory

Example

- Can we solve equations of the form $a * x = b$ in a group $\langle G, * \rangle$?

$a' * (a * x) = a' * b$
$(a' * a) * x = a' * b$

Group Theory

Example

- Can we solve equations of the form $a * x = b$ in a group $\langle G, * \rangle$?

$a' * (a * x) = a' * b$
$(a' * a) * x = a' * b$
$e * x = a' * b$

Group Theory

Example

- Can we solve equations of the form $a * x = b$ in a group $\langle G, * \rangle$?

$a' * (a * x) = a' * b$
$(a' * a) * x = a' * b$
$e * x = a' * b$
$x = a' * b$

Group Theory

Examples of Groups

Group Theory

Example
$\langle \mathbb{Z}, + \rangle$

Group Theory

Example
$\langle \mathbb{Z}, + \rangle$

- Closure $\forall m, n \in \mathbb{Z}, m + n \in \mathbb{Z}$

Group Theory

Example

$\langle \mathbb{Z}, + \rangle$

- Closure $\forall m, n \in \mathbb{Z}, m+n \in \mathbb{Z}$
- Associative
  $\forall m, n, p \in \mathbb{Z}, (m+n)+p = m+(n+p)$

169

Group Theory

Example

$\langle \mathbb{Z}, + \rangle$

- Closure $\forall m, n \in \mathbb{Z}, m+n \in \mathbb{Z}$
- Associative
  $\forall m, n, p \in \mathbb{Z}, (m+n)+p = m+(n+p)$
- Identity
  For every $m \in \mathbb{Z},\ 0 \in \mathbb{Z},\ 0+m = m = m+0.$

170

Group Theory

Example

$\langle \mathbb{Z}, + \rangle$

- Closure $\forall m, n \in \mathbb{Z}, m+n \in \mathbb{Z}$
- Associative
  $\forall m, n, p \in \mathbb{Z}, (m+n)+p = m+(n+p)$
- Identity
  For every $m \in \mathbb{Z},\ 0 \in \mathbb{Z},\ 0+m = m = m+0.$
- inverse
  For every $m \in \mathbb{Z}\ \exists -m \in \mathbb{Z}$ such that
  $m+(-m) = 0 = (-m)+m.$

171

Group Theory

Example

$\langle \mathbb{Z}, - \rangle$

172

Group Theory

Example

$\langle \mathbb{Z}, - \rangle$

- closure
  $\forall m, n \in \mathbb{Z},\ m-n \in \mathbb{Z}$

173

Group Theory

Example

$\langle \mathbb{Z}, - \rangle$

- closure
  $\forall m, n \in \mathbb{Z},\ m-n \in \mathbb{Z}$
- associative
  $(2-3)-4 = -5 \neq 3 = 2-(3-4)$

174

Group Theory

Example

$\langle \mathbb{Z}, . \rangle$

Group Theory

Example

$\langle \mathbb{Z}, . \rangle$

- closure $\forall\, m, n \in \mathbb{Z}, m.n \in \mathbb{Z}$

Group Theory

Example

$\langle \mathbb{Z}, . \rangle$

- closure $\forall\, m, n \in \mathbb{Z}, m.n \in \mathbb{Z}$
- associative

  $\forall\, m, n,\, p \in \mathbb{Z}, (m.n).p = m.(n.p)$

Group Theory

Example

$\langle \mathbb{Z}, . \rangle$

- closure $\forall\, m, n \in \mathbb{Z}, m.n \in \mathbb{Z}$
- associative

  $\forall\, m, n,\, p \in \mathbb{Z}, (m.n).p = m.(n.p)$
- identity

  For every $m \in \mathbb{Z},\, 1 \in \mathbb{Z},\;\, 1.m = m = m.1.$

Group Theory

Example

$\langle \mathbb{Z}, . \rangle$

- closure $\forall\, m, n \in \mathbb{Z}, m.n \in \mathbb{Z}$
- associative

  $\forall\, m, n,\, p \in \mathbb{Z}, (m.n).p = m.(n.p)$
- identity

  For every $m \in \mathbb{Z},\, 1 \in \mathbb{Z},\;\, 1.m = m = m.1.$
- Inverse

  $2 \in \mathbb{Z}$ but $\frac{1}{2} \notin \mathbb{Z}$

Group Theory

Example

$\langle \mathbb{Q}, + \rangle$

Group Theory

Example
$\langle \mathbb{Q}, + \rangle$

- Closure $\forall r,s \in \mathbb{Q},\ r+s \in \mathbb{Q}$

Group Theory

Example
$\langle \mathbb{Q}, + \rangle$

- Closure $\forall r,s \in \mathbb{Q},\ r+s \in \mathbb{Q}$
- Associative
  $\forall r,s,t \in \mathbb{Q}, (r+s)+t = r+(s+t)$

Group Theory

Example
$\langle \mathbb{Q}, + \rangle$

- Closure $\forall r,s \in \mathbb{Q},\ r+s \in \mathbb{Q}$
- Associative
  $\forall r,s,t \in \mathbb{Q}, (r+s)+t = r+(s+t)$
- Identity
  For every $r \in \mathbb{Q}$, $0+r = r = r+0,\ 0 \in \mathbb{Q}.$

Group Theory

Example
$\langle \mathbb{Q}, + \rangle$

- Closure $\forall r,s \in \mathbb{Q},\ r+s \in \mathbb{Q}$
- Associative
  $\forall r,s,t \in \mathbb{Q}, (r+s)+t = r+(s+t)$
- Identity
  For every $r \in \mathbb{Q}$, $0+r = r = r+0,\ 0 \in \mathbb{Q}.$
- inverse
  For every $r \in \mathbb{Q}\ \exists -r \in \mathbb{Q}$ such that
  $r+(-r) = 0 = (-r)+r.$

Group Theory

Example
$\langle \mathbb{Q}, . \rangle$

Group Theory

Example
$\langle \mathbb{Q}, . \rangle$

- closure $\forall r,s \in \mathbb{Q}, r.s \in \mathbb{Q}$

Group Theory

Example

$\langle \mathbb{Q}, . \rangle$

- closure $\forall r,s \in \mathbb{Q}, r.s \in \mathbb{Q}$
- associative

  $\forall r,s,t \in \mathbb{Q}, (r.s).t = r.(s.t)$

187

Group Theory

Example

$\langle \mathbb{Q}, . \rangle$

- closure $\forall r,s \in \mathbb{Q}, r.s \in \mathbb{Q}$
- associative

  $\forall r,s,t \in \mathbb{Q}, (r.s).t = r.(s.t)$
- identity

  For every $r \in \mathbb{Q}$, $1.r = r = r.1,\ 1 \in \mathbb{Q}$.

188

Group Theory

Example

$\langle \mathbb{Q}, . \rangle$

- closure $\forall r,s \in \mathbb{Q}, r.s \in \mathbb{Q}$
- associative

  $\forall r,s,t \in \mathbb{Q}, (r.s).t = r.(s.t)$
- identity

  For every $r \in \mathbb{Q}$, $1.r = r = r.1,\ 1 \in \mathbb{Q}$.
- Inverse

  Inverse of $0 \in \mathbb{Q}$ does not exist

189

Group Theory

Examples

- $\langle \mathbb{Q} - \{0\}, . \rangle$ is a group.

190

Group Theory

Examples

- $\langle \mathbb{Q} - \{0\}, . \rangle$ is a group.
- $\langle \mathbb{R} - \{0\}, . \rangle$ is a group.

191

Group Theory

Examples

- $\langle \mathbb{Q} - \{0\}, . \rangle$ is a group.
- $\langle \mathbb{R} - \{0\}, . \rangle$ is a group.
- $\langle \mathbb{C} - \{0\}, . \rangle$ is a group.

192

Group Theory

Uniqueness of Identity and Inverse

Group Theory

Proposition

- Let $\langle G,*\rangle$ be a group. Then

Group Theory

Proposition

- Let $\langle G,*\rangle$ be a group. Then

1) G has exactly one identity element

Group Theory

Proposition

- Let $\langle G,*\rangle$ be a group. Then

1) G has exactly one identity element
2) Each element of G has exactly one inverse.

Group Theory

Proof

1) Suppose e, e' are identity elements.

Group Theory

Proof

1) Suppose e, e' are identity elements. So $e*x = x*e = x$

Group Theory

Proof

1) Suppose e, e' are identity elements. So

$$e * x = x * e = x$$

$$e' * x = x * e' = x$$

Group Theory

Proof

1) Suppose e, e' are identity elements. So

$$e * x = x * e = x$$

$$e' * x = x * e' = x$$

holds for all $x \in G$

Group Theory

Proof

1) Suppose e, e' are identity elements. So

$$e * x = x * e = x$$

$$e' * x = x * e' = x$$

holds for all $x \in G$

- In particular

$$e = e * e' = e'.$$

Group Theory

Proof

2) Let $x \in G$ and suppose x', x'' are inverses of x.

Group Theory

Proof

2) Let $x \in G$ and suppose x', x'' are inverses of x. So

$$x' * x = x * x' = e$$

Group Theory

Proof

2) Let $x \in G$ and suppose x', x'' are inverses of x. So

$$x' * x = x * x' = e$$

$$x'' * x = x * x'' = e$$

Group Theory

Proof

2) Let $x \in G$ and suppose x', x'' are inverses of x. So
$$x' * x = x * x' = e$$
$$x'' * x = x * x'' = e$$

- Then
$$x' = x' * e$$

Group Theory

Proof

2) Let $x \in G$ and suppose x', x'' are inverses of x. So
$$x' * x = x * x' = e$$
$$x'' * x = x * x'' = e$$

- Then
$$\begin{aligned} x' &= x' * e \\ &= x' * (x * x'') \end{aligned}$$

Group Theory

Proof

2) Let $x \in G$ and suppose x', x'' are inverses of x. So
$$x' * x = x * x' = e$$
$$x'' * x = x * x'' = e$$

- Then
$$\begin{aligned} x' &= x' * e \\ &= x' * (x * x'') \\ &= (x' * x) * x'' \end{aligned}$$

Group Theory

Proof

2) Let $x \in G$ and suppose x', x'' are inverses of x. So
$$x' * x = x * x' = e$$
$$x'' * x = x * x'' = e$$

- Then
$$\begin{aligned} x' &= x' * e \\ &= x' * (x * x'') \\ &= (x' * x) * x'' \\ &= e * x'' = x''. \end{aligned}$$

Group Theory

An Interesting Example of Group

An Interesting Example of Group

Example

Let $G = \{x \in \mathbb{R} \mid x \neq 1\}$ and define

$x * y = xy - x - y + 2.$

Prove that $(G, *)$ is a group.

An Interesting Example of Group

Solution
Closure:

Let a, $b \in G$, so $a \neq 1$

and $b \neq 1$.

Suppose $a * b = 1$.

Then $ab - a - b + 2 = 1$

and so $(a - 1)(b - 1) = 0$

which implies that $a = 1$

or $b = 1$, a contradiction.

An Interesting Example of Group

Associative:

$(a * b) * c$
$=(a * b)c - (a * b) - c + 2$
$= (ab - a - b + 2)c -$
$(ab - a - b + 2) - c + 2$
$= abc - ac - bc + 2c - ab$
$+ a + b - 2 - c + 2$
$= abc - ab - ac - bc + a +$
$b + c$

Similarly $a * (b * c)$ has the same value.

An Interesting Example of Group

Identity:
An identity, e, would have to satisfy:

$e * x = x = x * e$ for all x $\in$ G,

that is,

$ex - e - x + 2 = x$,

or

$(e - 2)(x - 1) = 0$ for all x.

Clearly $e = 2$ works.

An Interesting Example of Group

Inverses:

If $x * y = 2$, then

$xy - x - y + 2 = 2$.

So

$y(x - 1) = x$ and

hence
$y = x/(x - 1)$.

An Interesting Example of Group

This exists for all $x \neq 1$,

i.e. for all $x \in G$. But we

must also check that it is

itself an element of G.

This is so because

$x/(x - 1) \neq 1$

for all $x \neq 1$.

Group Theory

Topic No. 14

Group Theory

Elementary Properties of Groups

Elementary Properties of Groups

Theorem

If G is a group with binary operation * then the left and right cancellation laws hold in G, that is, $a * b = a * c$ implies $b = c$, and $b * a = c * a$ implies $b = c$ for all $a, b, c \in G$.

Elementary Properties of Groups

Proof

Suppose $a * b = a * c$.
Then, there exists $a' \in G$, and
$a'* (a* b) = a'*(a*c)$.
$(a'* a)* b = (a'* a)* c$.
So, $e * b = e * c$ implies $b = c$.
Similarly, from $b * a = c * a$ one can deduce that $b = c$ upon multiplication by $a' \in G$ on the right.

Elementary Properties of Groups

Theorem

If G is a group with binary operation *, and if a and b *are* any elements of G, then the linear equations $a * x=b$ and $y * a=b$ have unique solutions x and y in G.

Elementary Properties of Groups

Proof

First we show the existence of at least one solution by just computing that $a' * b$ is a solution of $a* x = b$.
Note that

$$a* (a'* b) =(a* a')* b= e * b= b.$$

Thus $x = a' *b$ is a solution of $a * x = b$.
In a similar fashion, $y = b * a'$ is a solution of $y *a = b$.

Group Theory

Topic No. 15

Elementary Properties of Groups

Theorem

Let G be a group. For all $a, b \in G$, we have $(a*b)' = b'*a'$.

Elementary Properties of Groups

Proof

Note that in a group G, we have

$(a*b)*(b'*a')$

$= a*(b*b')*a'$

$= (a*e)*a'$

$= a*a' = e.$

Elementary Properties of Groups

It shows that $b'*a'$ is the unique inverse of $a*b$.

That is,

$(a*b)' = b'*a'$.

Elementary Properties of Groups

Theorem

For any $n \in \mathbb{N}$, $(a^n)^{-1} = (a^{-1})^n$.

Elementary Properties of Groups

Proof

By definition, $(a^n)^{-1}$ is the unique element of G whose product with a^n in any order is e.

But by associativity,

$$a^n * (a^{-1})^n = (a^{n-1} * a) * (a^{-1} * (a^{-1})^{n-1})$$
$$= a^{n-1} * (a * (a^{-1} * (a^{-1})^{n-1}))$$
$$= a^{n-1} * ((a * a^{-1}) * (a^{-1})^{n-1})$$
$$= a^{n-1} * (e * (a^{-1})^{n-1}))$$
$$= a^{n-1} * (a^{-1})^{n-1},$$

Elementary Properties of Groups

which by induction on n equals e (the cases n = 0 and n = 1 are trivial).

Similarly, the product of a^n and $(a^{-1})^n$ in the other order is e.

This proves that $(a^{-1})^n$ is the inverse of a^n.

Group Theory

Groups of Matrices

Groups of Matrices

Is ⟨ $M_{mn}(\mathbb{R})$, + ⟩ group?

- ∀ $[a_{ij}]$, $[b_{ij}] \in M_{mn}(\mathbb{R})$, $[a_{ij}] + [b_{ij}]=[a_{ij} + b_{ij}] \in M_{mn}(\mathbb{R})$
- ∀ $[a_{ij}]$, $[b_{ij}]$, $[c_{ij}] \in M_{mn}(\mathbb{R})$,
  $([a_{ij}] + [b_{ij}])+ [c_{ij}] =[a_{ij} + b_{ij}]+ [c_{ij}]$
  $=[(a_{ij} + b_{ij})+ c_{ij}]$
  $=[a_{ij} +(b_{ij}+ c_{ij})]$
  $= [a_{ij}]+[b_{ij}+ c_{ij}]$
  $= [a_{ij}] + ([b_{ij}]+ [c_{ij}])$

Groups of Matrices

- For every $[a_{ij}] \in M_{mn}(\mathbb{R})$ and $[0] \in M_{mn}(\mathbb{R})$,
  $[a_{ij}] + [0]=[a_{ij}+0]=[a_{ij}]=[0]+[a_{ij}]$
- For every $[a_{ij}] \in M_{mn}(\mathbb{R})$ there exists $[-a_{ij}] \in M_{mn}(\mathbb{R})$ such that $[a_{ij}] + [-a_{ij}]=[a_{ij}+(- a_{ij})]= [0]= [-a_{ij}]+[a_{ij}]$

Group Theory

Groups of Matrices

Groups of Matrices

- ∀ $[a_{ij}]$, $[b_{ij}] \in M_{mn}(\mathbb{R})$,
  $[a_{ij}] + [b_{ij}]=[a_{ij} + b_{ij}]$
  $=[b_{ij}+ a_{ij}]= [b_{ij}] + [a_{ij}]$
  Therefore, ⟨ $M_{mn}(\mathbb{R})$, + ⟩ is abelian group.
- Similarly, ⟨ $M_{mn}(\mathbb{Z})$, + ⟩, ⟨ $M_{mn}(\mathbb{Q})$, + ⟩ and ⟨ $M_{mn}(\mathbb{C})$, + ⟩ are also abelian groups.

Groups of Matrices

Is ⟨ $M_{nn}(\mathbb{R})$, . ⟩ group?

- ∀ A, B ∈ $M_{nn}(\mathbb{R})$,
  AB ∈ $M_{nn}(\mathbb{R})$
- ∀ A, B, C ∈ $M_{nn}(\mathbb{R})$,
  (AB)C=A(BC)
- For every A ∈ $M_{nn}(\mathbb{R})$ and $I_n \in M_{nn}(\mathbb{R})$,
  $AI_n=A=I_nA$
- A^{-1} does not exist for all those A ∈ $M_{nn}(\mathbb{R})$ having det(A)=0

Groups of Matrices

Field

(F,+,.)

- ⟨F,+⟩ is abelian group
- ⟨F\{0},.⟩ is abelian group

∀ *a*, b, c ∈ F,

- *a*(b+c)=*a*b+*a*c
- (*a*+b)c=*a*c+bc

235

Groups of Matrices

$\langle \mathbb{Z},+\rangle$

$\langle \mathbb{Q},+\rangle$

$\langle \mathbb{Q}-\{0\},.\rangle$

$\langle \mathbb{R},+\rangle$

$\langle \mathbb{R}-\{0\},.\rangle$

$\langle \mathbb{C},+\rangle$

$\langle \mathbb{C}-\{0\},.\rangle$

236

Group Theory

Abelian Groups

237

Group Theory

- Let $F=\mathbb{R}$ or $\mathbb{C}$.

238

Group Theory

- Let $F=\mathbb{R}$ or $\mathbb{C}$.
- Let $[a_{ij}]$ be a matrix over F i.e. all $a_{ij}\in F$

239

Group Theory

- Let $F=\mathbb{R}$ or $\mathbb{C}$.
- Let $[a_{ij}]$ be a matrix over F i.e. all $a_{ij}\in F$
- Let $GL(n,F)$ denotes the set of all $n\times n$ invertible matrices over F.

240

Group Theory

- In general set of all $n \times n$ matrices is not a group under matrix multiplication.

Group Theory

- In general set of all $n \times n$ matrices is not a group under matrix multiplication.
- But $GL(n, F)$ is a group under matrix multiplication.

Group Theory

Axioms
- Let $G = GL(n, F)$.

Group Theory

Axioms
- Let $G = GL(n, F)$.
- Closure: For all $A, B \in G, AB \in G$.

Group Theory

Axioms
- Let $G = GL(n, F)$.
- Closure: For all $A, B \in G, AB \in G$.
- Associative property also holds in G.

Group Theory

Axioms
- Let $G = GL(n, F)$.
- Closure: For all $A, B \in G, AB \in G$.
- Associative property also holds in G.
- I_n is the identity matrix.

Group Theory

Axioms

- Let $G = GL(n, F)$.
- Closure: For all $A,\ B \in G,\ AB \in G.$
- Associative property also holds in $G.$
- I_n is the identity matrix.
- Since both A and A^{-1} are invertible so inverse exists.

Group Theory

Example

- Let $G = GL(2, \mathbb{R})$ and $A,\ B \in G$ such that

$$A = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Group Theory

Example

- Let $G = GL(2, \mathbb{R})$ and $A,\ B \in G$ such that

$$A = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- then

$$AB = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 2 & 0 \end{pmatrix}$$

Group Theory

Example

- Let $G = GL(2, \mathbb{R})$ and $A,\ B \in G$ such that

$$A = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- then

$$AB = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 2 & 0 \end{pmatrix}$$

$$BA = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & -1 \end{pmatrix}$$

Group Theory

Definition

- Let $\langle G, * \rangle$ be a group.
  If for all $a, b \in G,$
  $$a * b = b * a$$
  We call G an abelian group.

Group Theory

Definition

- Let $\langle G, * \rangle$ be a group.
  If for all $a, b \in G,$
  $$a * b = b * a$$
  We call G an abelian group.
- Examples
  $\langle n\mathbb{Z}, + \rangle$

Group Theory

Definition

- Let $\langle G, * \rangle$ be a group.
  If for all $a, b \in G$,
  $a * b = b * a$
  We call G an abelian group.
- Examples
  $\langle n\mathbb{Z}, + \rangle$
  $\langle \mathbb{Q} - \{0\}, . \rangle$

253

Group Theory

Examples

$\langle \mathbb{R}, + \rangle$

254

Group Theory

Examples

$\langle \mathbb{R}, + \rangle$

$\langle \mathbb{C}, + \rangle$

255

Group Theory

Examples

$\langle \mathbb{R}, + \rangle$

$\langle \mathbb{C}, + \rangle$

$\langle \mathbb{R} - \{0\}, . \rangle$

256

Group Theory

Examples

$\langle \mathbb{R}, + \rangle$

$\langle \mathbb{C}, + \rangle$

$\langle \mathbb{R} - \{0\}, . \rangle$

$\langle \mathbb{C} - \{0\}, . \rangle$

257

Group Theory

Examples

$GL(n, \mathbb{Z})$

258

Group Theory

Examples

$GL(n,\mathbb{Z})$

$$A=\begin{pmatrix}1 & -1\\ 0 & 2\end{pmatrix}$$

Group Theory

Examples

$GL(n,\mathbb{Z})$

$$A=\begin{pmatrix}1 & -1\\ 0 & 2\end{pmatrix}$$

$$A^{-1}=\frac{1}{2}\begin{pmatrix}2 & 1\\ 0 & 1\end{pmatrix}$$

Group Theory

Examples

$GL(n,\mathbb{Z})$

$$A=\begin{pmatrix}1 & -1\\ 0 & 2\end{pmatrix}$$

$$A^{-1}=\frac{1}{2}\begin{pmatrix}2 & 1\\ 0 & 1\end{pmatrix}$$

$GL(n,\mathbb{Q})$

Group Theory

Abelian Groups

Abelian Groups

Theorem

If $a * b = b * a$, then for all/any one $n \in \mathbb{Z}$, $(a * b)^n = a^n * b^n$.

Abelian Groups

Proof

If $n = 0$ or $n = 1$, this holds trivially. Now let $n > 1$.

By commutativity, $b^m * a = a * b^m$ for all $m \geq 0$.

Then by induction on n,

$(a * b)^n = (a * b)^{n-1} * (a * b) = (a^{n-1} * b^{n-1}) * (a * b)$

$= ((a^{n-1} * b^{n-1}) * a) * b = (a^{n-1} * (b^{n-1} * a)) * b$

$= (a^{n-1} * (a * b^{n-1})) * b = (a^{n-1} * a) * b^{n-1}) * b$

$= a^n * (b^{n-1} * b) = a^n * b^n$.

Thus the result holds for all $n \in \mathbb{N}$.

Abelian Groups

If n<0, then by the positive case and commutativity,

$(a * b)^n$
$= (b * a)^n$
$= ((b * a)^{-n})^{-1}$
$= (b^{-n} * a^{-n})^{-1}$
$= (a^{-n})^{-1} * (b^{-n})^{-1}$
$= a^n * b^n$

Group Theory

Modular Arithmetic

Modular Arithmetic

Definition

Let n be a fixed positive integer and a and b any two integers. We say that a is congruent to b modulo n if n divides a−b. We denote this by a ≡ b mod n.

Modular Arithmetic

Theorem

Show that the congruence relation modulo n is an equivalence relation on ℤ.

Modular Arithmetic

Proof

Write "n|m" for " n divides m," which means that there is some integer k such that m = nk.

Hence a ≡ b mod n if and only if n|(a−b).

(i) For all a ∈ ℤ, n |(a−a), so

a ≡ a mod n and the relation is reflexive.

Modular Arithmetic

(ii) If a ≡ b mod n, then n|(a−b), so n|−(a −b).

Hence n|(b−a) and b ≡ a mod n.

(iii) If a ≡ b mod n and b ≡ c mod n, then n|(a−b) and n|(b−c), so n |(a−b)+(b−c).

Therefore, n|(a−c) and a ≡ c mod n.

Hence congruence modulo n is an equivalence relation on ℤ.

Modular Arithmetic

The set of equivalence classes is called the set of integers modulo n and is denoted by $\mathbb{Z}_n$.

Modular Arithmetic

In the congruence relation modulo 3, we have the following equivalence classes:

[0]={...,−3,0,3,6,9,...} [1]={...,−2,1,4,7,10,...} [2]={...,−1,2,5,8,11,...}
[3]={...,0,3,6,9,12,...}=[0]

Any equivalence class must be one of [0], [1], or [2], so

$\mathbb{Z}_3$ ={[0],[1],[2]}.

In general, $\mathbb{Z}_n$ ={[0],[1],[2],...,[n−1]}, since any integer is congruent modulo n to its remainder when divided by n.

Group Theory

Order of a Group

Order of a Group

Definition

The number of elements of a group G is called the order of G.

We denote it as |G|.

We call G finite if it has only finitely many elements;

otherwise we call G infinite.

Order of a Group

Definition

Let G be a group and a ∈ G.
If there is a positive integer n such that a^n = e, then we call the smallest such positive integer the order of a.
If no such n exists, we say that a has infinite order.
The order of a is denoted by $|a|$.

Order of a Group

In the congruence relation modulo 4, we have the following equivalence classes:

[0]={...,−4,0,4,8,12,...} [1]={...,−3,1,5,9,13,...}

[2]={...,−2,2,6,10,14,...} [3]={...,-1,3,7,11,15,...}

Any equivalence class must be one of [0], [1], [2] or [3],

so $\mathbb{Z}_4$ ={[0],[1],[2],[3]}.

Let $+_4$ be addition modulo 4. Then, $2 +_4 3 = 1$.

Order of a Group

We can write out its Cayley table:

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

Therefore, $\langle \mathbb{Z}_4, +_4 \rangle$ is a group.

277

Order of a Group

- $|\mathbb{Z}_4|=4$
- $1+_4 1+_4 1+_4 1=4(1)=0 \Longrightarrow |[1]|=4$
- $2+_4 2=2(2)=0 \Longrightarrow |[2]|=2$
- $3+_4 3+_4 3+_4 3=4(3)=0 \Longrightarrow |[3]|=4$
- $1(0)=0 \Longrightarrow |[0]|=1$
- $\mathbb{Z}_4=\langle 1\rangle=\langle 3\rangle$

- Let $\mathbb{Z}_n=\{[0], [1], [2],\ldots,[n-1]\}$. Then, $\langle \mathbb{Z}_n, +_n \rangle$ is a group.
- $|\mathbb{Z}_n|=n$

278

Order of a Group

$$\langle \mathbb{Z},+\rangle$$
$$\langle \mathbb{Q},+\rangle$$
$$\langle \mathbb{Q}-\{0\},.\rangle$$
$$\langle \mathbb{R},+\rangle$$
$$\langle \mathbb{R}-\{0\},.\rangle$$
$$\langle \mathbb{C},+\rangle$$
$$\langle \mathbb{C}-\{0\},.\rangle$$

279

Group Theory

Finite Groups

280

Finite Groups

Let $U_4 = \{1, -1, i, -i\}$, and let "." be multiplication. Then U_4 is a group, and we can write out its multiplication table (Cayley table):

.	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

281

Finite Groups

- $|U_4|=4$
- $(-1)(-1)=(-1)^2=1 \Longrightarrow |-1|=2$
- $i.i.i.i=i^4=1 \Longrightarrow |i|=4$
- $(-i)(-i)(-i)(-i)=(-i)^4=1 \Longrightarrow |-i|=4$
- $1^1=1 \Longrightarrow |1|=1$
- $U_4=\langle i\rangle=\langle -i\rangle$

282

Finite Groups

Is $\langle U_4, .\rangle \cong \langle \mathbb{Z}_4, +_4 \rangle$?

- $1 \leftrightarrow [0]$
- $-1 \leftrightarrow [2]$
- $i \leftrightarrow [1]$
- $-i \leftrightarrow [3]$

Finite Groups

Let $U_n = \{e^{i2k\pi/n: k=0, 1, \ldots, n-1}\}$.
Then, $\langle U_n, .\rangle$ is a group.
$\langle U_n, .\rangle \cong \langle \mathbb{Z}_n, +_n \rangle$

Group Theory

Finite Groups

Finite Groups

Since a group has to have at least one element, namely, the identity, a minimal set that might give rise to a group is a one-element set { e}.
The only possible binary operation on { e} is defined by $e * e = e$.
The three group axioms hold.
The identity element is always its own inverse in every group.

Finite Groups

Let us try to put a group structure on a set of two elements.
Since one of the elements must play the role of identity element, we may as well let the set be $\{e, a\}$.
Let us attempt to find a table for a binary operation $*$ on $\{e, a\}$ that gives a group structure on $\{e, a\}$.

Finite Groups

Since e is to be the identity, so $e*x=x*e=x$ for all $x\in\{e, a\}$.
Also, a must have an inverse a' such that $a * a' = a' * a = e$.
In our case, a' must be either e or a. Since $a' =$ e obviously does not work, we must have $a' = a$.

Finite Groups

So, we have to complete the table as follows:

*	e	a
e	e	a
a	a	e

Finite Groups

$+_2$	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

We know that $\mathbb{Z}_2$ ={[0], [l]} under addition modulo 2 is a group, and by our arguments, its table must be the one above with *e* replaced by [0] and *a* by [1].

Group Theory

Finite Groups

Finite Groups

Suppose that G is any group of three elements and imagine a table for G with identity element appearing first.
Since our filling out of the table for $G = \{e, a, b\}$ could be done in only one way, we see that if we take the table for G and rename the identity *e*, the next element listed *a*, and the last element *b*, the resulting table for G gives an isomorphism of the group G with the group G' ={[0], [1], [2]}.

Finite Groups

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$+_3$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$a*b = b \Longrightarrow a=e$ not possible

$a*b = a \Longrightarrow b=e$ not possible

$a*a = a \Longrightarrow a=e$ not possible

$b*b = b \Longrightarrow b=e$ not possible

Finite Groups

Our work above can be summarized by saying that all groups with a single element are isomorphic, all groups with just two elements are isomorphic, and all groups with just three elements are isomorphic.

We may say:
There is only one group of single element (up to Isomorphism), there is only one group of two elements (up to isomorphism) and there is only one group of three elements (up to isomorphism).

Finite Groups

There are two different types of group structures of order 4.

- The group $\langle \mathbb{Z}_4, +_4 \rangle$ is isomorphic to the group U_4= { 1, i, -1, -i} of fourth roots of unity under multiplication.
- The group V=$\langle$a,b | $a^2=b^2=(ab)^2=e$ $\rangle$ is the **Klein 4-group**, and the notation V comes from the German word Vier for four.

Finite Groups

We describe Klein 4-group by its group table.

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Group Theory

Finite Groups

Finite Groups

Is $\langle \mathbb{Z}_6 \backslash \{[0]\}, \cdot_6 \rangle$ a group?

$\cdot_6$	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]
[2]	[2]	[4]	[0]	[2]	[4]
[3]	[3]	[0]	[3]	[0]	[3]
[4]	[4]	[2]	[0]	[4]	[2]
[5]	[5]	[4]	[3]	[2]	[1]

Finite Groups

Is $\langle \mathbb{Z}_5 \backslash \{[0]\}, \cdot_5 \rangle$ a group?

$\cdot_5$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

$\langle \mathbb{Z}_p \backslash \{[0]\}, \cdot_p \rangle$ is a group, where p is a prime number

Group Theory

Subgroups

Subgroups

Subgroups

- Let $\langle G, * \rangle$ be a group. A subgroup of G is a subset of G which is itself a group under $*$.

Subgroups

Examples

- $\langle \mathbb{Z}, + \rangle$ is a subgroup of $\langle \mathbb{R}, + \rangle$

Subgroups

Examples

- $\langle \mathbb{Z}, + \rangle$ is a subgroup of $\langle \mathbb{R}, + \rangle$
- $\langle \mathbb{Q} - \{0\}, . \rangle$ is not a subgroup of $\langle \mathbb{R}, + \rangle$

Subgroups

Examples

- $\langle \mathbb{Z}, + \rangle$ is a subgroup of $\langle \mathbb{R}, + \rangle$
- $\langle \mathbb{Q} - \{0\}, . \rangle$ is not a subgroup of $\langle \mathbb{R}, + \rangle$
- $\langle \{1, -1\}, . \rangle$ is a subgroup of $\langle \{1, -1, i, -i\}, . \rangle$

Subgroups

Examples

- $\langle \mathbb{Z}, + \rangle$ is a subgroup of $\langle \mathbb{R}, + \rangle$
- $\langle \mathbb{Q} - \{0\}, . \rangle$ is not a subgroup of $\langle \mathbb{R}, + \rangle$
- $\langle \{1, -1\}, . \rangle$ is a subgroup of $\langle \{1, -1, i, -i\}, . \rangle$
- $\langle \{1, \ i\}, . \rangle$ is not a subgroup of $\langle \{1, \ -1, i, -i\}, . \rangle$

Subgroups

Proposition

- Let G be a group. Let $H \subseteq G$. Then H is a subgroup of G if the following are true:

Subgroups

Proposition
- Let G be a group. Let $H \subseteq G$. Then H is a subgroup of G if the following are true:

1) $e \in H$

Subgroups

Proposition
- Let G be a group. Let $H \subseteq G$. Then H is a subgroup of G if the following are true:

1) $e \in H$
2) if $h, k \in H$ then $hk \in H$

Subgroups

Proposition
- Let G be a group. Let $H \subseteq G$. Then H is a subgroup of G if the following are true:

1) $e \in H$
2) if $h, k \in H$ then $hk \in H$
3) if $h \in H$ then $h^{-1} \in H$

Subgroups

Example
- Let $G = GL(2, \mathbb{R})$
- Let $H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \middle| \ n \in \mathbb{Z} \right\}$

Subgroups

Example
- Let $G = GL(2, \mathbb{R})$
- Let $H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \middle| \ n \in \mathbb{Z} \right\}$

1) $e \in H$

Subgroups

Example
- Let $G = GL(2, \mathbb{R})$
- Let $H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \middle| \ n \in \mathbb{Z} \right\}$

1) $e \in H$
2) let $h = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, k = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$

then $hk = \begin{pmatrix} 1 & p+n \\ 0 & 1 \end{pmatrix} \in H.$

Subgroups

Example

3) let $h = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

Then

$$h^{-1} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \in \mathrm{H}.$$

Subgroups

Example

3) let $h = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

Then

$$h^{-1} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \in \mathrm{H}.$$

Hence H is a subgroup of G.

Group Theory

Examples of Subgroups

Groups of Matrices

If F is a field **GL(*n, F*)** denotes the group of all invertible $n \times n$ matrices over F under multiplication. This group is called the **general linear group of degree *n* over *F***.

We know that the associative law holds for matrix multiplication. Checking the closure law requires us to know that the product of two invertible matrices is invertible. And we need to know more than just the fact that every invertible matrix has an inverse. We need to observe that such an inverse is itself invertible.

Groups of Matrices

An interesting subgroup of GL(n, F) is **T$^+$(*n, F*)** the set of all $n \times n$ **upper- triangular matrices** over F, that is, $n \times n$ matrices of the form:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & a_{22} & a_{23} & \dots & a_{2n} \\ 0 & 0 & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_{nn} \end{bmatrix}$$

where each diagonal component is non-zero.

Groups of Matrices

Then there are the **lower triangular matrices T$^-$(*n, F*)** which are the transposes of the upper triangular ones.

$$\begin{bmatrix} a_{11} & 0 & 0 & \dots & 0 \\ a_{12} & a_{22} & 0 & \dots & 0 \\ a_{13} & a_{23} & a_{33} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_{1n} & a_{2n} & a_{3n} & \dots & a_{nn} \end{bmatrix}$$

Groups of Matrices

Diagonal matrices D(n, F). It's closed under multiplication, identity and inverses simply because each of $T^+(n, F)$ and $T^-(n, F)$ are.

This is a special case of the general fact that: **The intersection of any collection of subgroups is itself a subgroup.**

$$\begin{bmatrix} a_{11} & 0 & 0 & \dots & 0 \\ 0 & a_{22} & 0 & \dots & 0 \\ 0 & 0 & a_{33} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_{nn} \end{bmatrix}$$

Groups of Matrices

Within D(n, F) we have the non-zero **scalar matrices S(n, F).** These are simply the diagonal matrices that have the same non-zero entry down the diagonal, that is, non-zero scalar multiples of the identity matrix.

$$\begin{bmatrix} \lambda & 0 & 0 & \dots & 0 \\ 0 & \lambda & 0 & \dots & 0 \\ 0 & 0 & \lambda & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \lambda \end{bmatrix} = \lambda \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix} = \lambda I_n,\ \lambda \neq 0$$

Groups of Matrices

Another interesting subgroup of $T^+(n, F)$ is the group of **uni-upper-triangular matrices UT^+(n, F).**

These are the upper-triangular matrices with 1's down the diagonal:

$$\begin{bmatrix} 1 & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & 1 & a_{23} & \dots & a_{2n} \\ 0 & 0 & 1 & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}$$

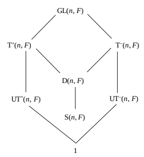
Groups of Matrices

And inside $T^-(n, F)$ we have the **uni-lower-triangular matrices UT^-(n, F).**

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ a_{12} & 1 & 0 & \dots & 0 \\ a_{13} & a_{23} & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_{1n} & a_{2n} & a_{3n} & \dots & 1 \end{bmatrix}$$

Groups of Matrices

We can summarize the connections between these subgroups in a "lattice diagram":



Groups of Matrices

Another very important subgroup of GL(n, F) is **SL(n, F)** consisting of all the matrices with determinant 1.

It's called **the special linear group of degree *n* over *F*.**

Group Theory

Topic No. 28

Group Theory

The Two Step Subgroup Test

The Two Step Subgroup Test

Theorem

A subset H of a group G is a subgroup of G if and only if

1. H is closed under the binary operation $*$ of G,
2. for all $a \in H$ it is true that $a^{-1} \in H$ also.

The Two Step Subgroup Test

Proof

The fact that if H is subgroup of G then conditions 1 and 2 must hold follows at once from the definition of a subgroup.

Conversely, suppose H is a subset of a group G such that conditions 1 and 2 hold.

By 1 we have at once that closure property is satisfied. The inverse law is satisfied by 2.

Therefore, for every $a \in H$ there exists $a^{-1} \in H$ such that $e = a * a^{-1} \in H$ by 1. So, $e * a = a * e = a$ by 1.

The Two Step Subgroup Test

It remains to check the associative axiom.
But surely for all *a, b, c* ∈ H it is true that
$(ab)c = a(bc)$
in H, for we may actually view this as an equation in G, where the associative law holds.

Group Theory

Topic No. 29

Group Theory

Examples on Subgroup Test

Examples on Subgroup Test

Recall
Let **G** be a group and **H** a nonempty subset of **G**. If $a*b$ is in **H** whenever a and b are in **H**, and a^{-1} is in **H** whenever a is in **H**, then **H** is a subgroup of **G**.

Examples on Subgroup Test

To Apply the Two Step Subgroup Test:

- Note that **H** is nonempty
- Show that **H** is closed with respect to the group operation
- Show that **H** is closed with respect to inverses.
- Conclude that **H** is a subgroup of **G**.

Examples on Subgroup Test

Example
Show that **3Q*** is a subgroup of **Q***, the non-zero rational numbers.

3Q* is non-empty because 3 is an element of **3Q***.
For a, b in **3Q***, a=3i and b=3j where i, j are in **Q***.
Then $ab=3i3j=3(3ij)$, an element of **3Q*** (closed)
For a in **3Q***, $a=3i$ for i an element in **Q***.
Then $a^{-1}=(i^{-1}3^{-1})$, an element of **3Q***. (inverses)
Therefore **3Q*** is a subgroup of **Q*.**

Group Theory

Topic No. 30

Group Theory

The One Step Subgroup Test

The one Step Subgroup Test

Theorem

If S is a subset of the group G, then S is a subgroup of G if and only if S is nonempty and whenever a, b $\in$ S, then $ab^{-1} \in$ S.

The one Step Subgroup Test

Proof

If S is a subgroup, then of course S is nonempty and whenever a, b $\in$ S, then $ab^{-1} \in$ S.

The one Step Subgroup Test

Conversely suppose S is a nonempty subset of the Group G such that whenever a, b $\in$ S, then $ab^{-1} \in$ S.
Let a $\in$ S, then $e = aa^{-1} \in S$ and so $a^{-1} = ea^{-1} \in S$.
Finally, if a, b $\in$ S, then $b^{-1} \in S$ by the above and so $ab = a(b^{-1})^{-1} \in S$.

Group Theory

Topic No. 31

Group Theory

Examples on Subgroup Test

Examples on Subgroup Test

Recall

Suppose **G** is a group and **H** is a non-empty subset of **G**.
If, whenever a and b are in **H**, ab^{-1} is also in **H**, then **H** is a subgroup of **G**.

Or, in additive notation:
If, whenever a and b are in **H**, a - b is also in **H**, then **H** is a subgroup of **G**.

Examples on Subgroup Test

To apply this test:

- Note that **H** is a non-empty subset of **G**.
- Show that for any two elements a and b in **H**, ab^{-1} is also in **H**.
- Conclude that **H** is a subgroup of **G**.

Examples on Subgroup Test

Example
Show that the even integers are a subgroup of the Integers.
Note that the even integers is not an empty set because 2 is an even integer.
Let a and b be even integers.
Then a = 2j and b = 2k for some integers j and k.
a + (-b) = 2j + 2(-k) = 2(j-k) = an even integer
Thus a - b is an even integer
Thus the even integers are a subgroup of the integers.

Examples on Subgroup Test

Example
For a, b in **3Q***, a=3i and b=3j where i, j are in **Q***
Then
$ab^{-1}=3i(3j)^{-1}=3i(j^{-1}3^{-1})=3(ij^{-1}3^{-1})$, an element of **3Q***

Group Theory

Topic No. 32

Group Theory

The Finite Subgroup Test

The finite Subgroup Test

Theorem
If S is a subset of the finite group G, then S is a subgroup of G if and only if S is nonempty and whenever $a, b \in S$, then $ab \in S$.

The finite Subgroup Test

Proof

If S is a subgroup then obviously S is nonempty and whenever a, b ∈ S, then ab ∈ S.
Conversely suppose S is nonempty and whenever a, b ∈ S, then ab ∈ S.
Then let a ∈ S. The above property says that $a^2=aa \in S$ and so $a^3=aa^2 \in S$ and so $a^4=aa^3 \in S$ and so on and on and on.

The finite Subgroup Test

That is $a^n \in S$ for all integers $n > 0$.
But G is finite and thus so is S.
Consequently the sequence, $a, a^2, a^3, a^4, \ldots, a^n, \ldots$ cannot continue to produce new elements.
That is there must exist $m<n$ such that $a^m=a^n$.
Thus $e= a^{n-m} \in S$.

The finite Subgroup Test

Therefore for all a ∈ S, there is a smallest integer $k > 0$ such that $a^k = e$.
Moreover, $a^{-1} = a^{k-1} \in S$.
Finally if a, b ∈ S, then $b^{-1} \in S$ by the above and so by the assume property we have $a b^{-1} \in S$.
Therefore S is a subgroup as desired.

Group Theory

Topic No. 33

Group Theory

Examples on Subgroup Test

Examples on Subgroup Test

Example

- ({1,−1, i,−i}, ・)
- {1,i}
- {1,-i}
- {1,−1}
- {1,-1,i}
- {1,-1,-i}

Examples on Subgroup Test

Example

- ({[0], [1], [2], [3], [4], [5]}, $+_6$)
- {[0], [1]} or {[0], [4]} or {[0], [5]} or {[0], [2]}
- {[0], [3]}
- {[0], [2], [4]}
- {[0], [2], [3], [4]}

Group Theory

- **Cyclic Groups**

Cyclic Groups

Definition

Let G be a group and let $a \in G$.

Then the subgroup

$H=\{a^n \mid n \in \mathbb{Z}\}$

of G is called the cyclic subgroup of G generated by a, and denoted by $\langle a \rangle$.

Cyclic Groups

Definition

- An element a of a group G generates G and is a generator for G if $\langle a \rangle$=G.
- A group G is cyclic if there is some element a in G that generates G.

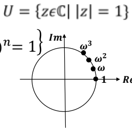
Cyclic Groups

- Let a be an element of a group G.
- If the cyclic subgroup $\langle a \rangle$ is finite, then the order of a is the order $|\langle a \rangle|$ of this cyclic subgroup.
- Otherwise, we say that a is of infinite order.

Cyclic Groups

Example

- For each positive integer n, *let U_n be the multiplicative group of the nth roots of unity in $\mathbb{C}$.*
- *These elements of U_n can be represented geometrically by equally spaced points on a circle about the origin.*
- $U_n = \left\langle \omega \mid \omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \right\rangle < U = \{z\epsilon\mathbb{C} \mid |z| = 1\}$
  $= \left\{\omega, \omega^2, \dots, \omega^{n-1}, \omega^n = (e^{i\frac{2\pi}{n}})^n = 1\right\}$



Group Theory

- **Examples of Cyclic Groups**

Examples of Cyclic Groups

Cyclic groups may be finite:

- In $\mathbb{Z}_4$, $\langle\bar{1}\rangle = \{\bar{1}, \bar{2}, \bar{3}, \bar{0}\} = \mathbb{Z}_4 = \langle\bar{3}\rangle \neq \langle\bar{2}\rangle$
- $\mathbb{Z}_4$ is cyclic.
- In $\mathbb{Z}_5$, $\langle\bar{1}\rangle = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{0}\} = \mathbb{Z}_5 = \langle\bar{2}\rangle = \langle\bar{3}\rangle = \langle\bar{4}\rangle$
- $\mathbb{Z}_5$ is cyclic.
- In $\mathbb{Z}_6$, $\langle\bar{1}\rangle = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{0}\} = \mathbb{Z}_6 = \langle\bar{5}\rangle$
- $\mathbb{Z}_6$ is cyclic.
- In $\mathbb{Z}_n$, $\langle\bar{1}\rangle = \{\bar{1}, \bar{2}, \dots, \overline{n-1}, \bar{0}\} = \mathbb{Z}_n = \langle\bar{m}\rangle$ if $g.c.d(m,n) = 1$ for $m = 1,2,\dots,n-1$.

Examples of Cyclic Groups

Cyclic groups may be infinite:

- In $\mathbb{Z}$, $\langle 1\rangle = \{\dots, -2, -1, 0, 1, 2, \dots\} = \mathbb{Z} = \langle -1\rangle$
- $\dots,\ -2(1) = -2,\ -1(1) = -1,\ 0(1) = 0,\ 1(1) = 1,\ 2(1) = 2,\ \dots$
- $\dots,\ -2(-1) = 2,\ -1(-1) = 1,\ 0(-1) = 0,\ 1(-1) = -1,\ 2(-1) = -2,\ \dots$
- In $\mathbb{Z}$, $\langle 2\rangle = \{\dots, -4, -2, 0, 2, 4, \dots\} = 2\mathbb{Z} = \langle -2\rangle$
- In $\mathbb{Z}$, $\langle n\rangle = \{\dots, -2n, -n, 0, n, 2n, \dots\} = n\mathbb{Z} = \langle -n\rangle$ for $n \in \mathbb{Z}$

Examples of Cyclic Groups

Cyclic groups may be infinite:

- In $\mathbb{Q} - \{0\}$, $\langle 2\rangle = \left\{\dots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \dots\right\} = \left\langle \frac{1}{2} \right\rangle$
- In $\mathbb{Q} - \{0\}$, $\langle r\rangle = \left\{\dots, \frac{1}{r^3}, \frac{1}{r^2}, \frac{1}{r}, 1, r, r^2, r^3, \dots\right\} = \left\langle \frac{1}{r} \right\rangle$ for $r \in \mathbb{Q}$.
- In $GL(2,\mathbb{R})$, $\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} : n \in \mathbb{Z} \right\}$

Group Theory

- **Elementary Properties of Cyclic Groups**

Elementary Properties of Cyclic Groups

Theorem

Every cyclic group is abelian.

Elementary Properties of Cyclic Groups

Proof

- Let G be a cyclic group and let a be a generator of G so that
  $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.
- If g_1 and g_2 are any two elements of G, there exists integers r and s such that $g_1 = a^r$ and $g_2 = a^s$.
- Then
  $g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = g_2 g_1$.
- So, G is abelian.

367

Elementary Properties of Cyclic Groups

- U_n
- $\mathbb{Z}_n$
- $n\mathbb{Z}$
- In $\mathbb{Q} - \{0\}$, $\langle r \rangle = \left\{\dots, \frac{1}{r^3}, \frac{1}{r^2}, \frac{1}{r}, 1, r, r^2, r^3, \dots\right\} = \left\langle \frac{1}{r} \right\rangle$ for $r \in \mathbb{Q}$.
- In $GL(2, \mathbb{R})$, $\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} : n \epsilon \mathbb{Z} \right\}$

368

Elementary Properties of Cyclic Groups

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-2} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}$$

369

Group Theory

- **Elementary Properties of Cyclic Groups**

370

Group Theory

- **Elementary Properties of Cyclic Groups**

371

Elementary Properties of Cyclic Groups

Definition: G is cyclic if G = <a> for some a in G.

Theorem

- If $|a| = \infty$, $a^i = a^j$ iff i = j
- If $|a| = n$, $a^i = a^j$ iff $n \mid i - j$
- $\langle a \rangle = \{a, a^2, \dots a^{n-1}, e\}$

Corollary 1: $|a| = |\langle a \rangle|$

Corollary 2: $a^k = e$ implies $|a| \mid k$

Example: $U_5 = \langle \omega \mid \omega^5 = 1 \rangle = \langle \omega^2 \rangle = \langle \omega^3 \rangle = \langle \omega^4 \rangle$, $\omega = e^{i(2\pi/5)}$

$\omega^2 \neq \omega^4$ $\quad 5 \nmid 4 - 2$; $\quad \omega^5 = \omega^{10}$ $\quad 5 \mid 10 - 5$

372

Elementary Properties of Cyclic Groups

Example

$U_6 = \langle \omega \mid \omega^6 = 1 \rangle = \{\omega, \omega^2, \omega^3, \omega^4, \omega^5, 1\}$ with $\omega = e^{i(2\pi/6)}$

$(\omega^5)^2 = \omega^{10} = \omega^6\omega^4 = \omega^4$

$(\omega^5)^3 = \omega^{15} = (\omega^6)^2\omega^3 = \omega^3$

$(\omega^5)^4 = \omega^{20} = (\omega^6)^3\omega^2 = \omega^2$

$(\omega^5)^5 = \omega^{25} = (\omega^6)^4\omega = \omega$

$(\omega^5)^6 = \omega^{30} = (\omega^6)^5 = 1$

$U_6 = \langle \omega^5 \rangle = \{\omega^5, \omega^4, \omega^3, \omega^2, \omega, 1\}$

373

Elementary Properties of Cyclic Groups

Example

$U_6 = \langle \omega \mid \omega^6 = 1 \rangle = \{\omega, \omega^2, \omega^3, \omega^4, \omega^5, 1\}$ with $\omega = e^{i(2\pi/6)}$

$\langle \omega^2 \rangle = \{\omega^2, \omega^4, 1\} < U_6$

$\langle \omega^3 \rangle = \{\omega^3, 1\} < U_6$

$\langle \omega^4 \rangle = \{\omega^4, \omega^2, 1\} = \langle \omega^2 \rangle$

374

Group Theory

- **Elementary Properties of Cyclic Groups**

375

Elementary Properties of Cyclic Groups

Theorem 1

If $|a| = n$, then

- $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$
- $|a^k| = n/\gcd(n,k)$

376

Elementary Properties of Cyclic Groups

To prove the $|a^k| = n/\gcd(n,k)$, we begin with a little lemma.

Prove: If $d \mid n = |a|$, then $|a^d| = n/d$.

Proof: Let $n = dq$. Then $e = a^n = (a^d)^q$.

So $|a^d| \leq q$.

If $0 < i < q$, then $0 < di < dq = n = |a|$

so $(a^d)^i \neq e$

Hence, $|a^d| = q$ which is n/d as required.

377

Elementary Properties of Cyclic Groups

Now, we prove that $|a^k| = n/\gcd(n,k)$.

Let $d = \gcd(n,k)$. Then, we have

$\lvert a^k \rvert = \lvert \langle a^k \rangle \rvert$	by Corollary 1
$= \lvert \langle a^d \rangle \rvert$	by Part 1 of Theorem 1
$= \lvert a^d \rvert$	by Corollary 1
$= n/d$	by above Lemma.

This concludes the proof.

378

Elementary Properties of Cyclic Groups

Example

- Suppose G = $\langle a \rangle$ with $|a| = 30$.
  Find $|a^{21}|$ and $\langle a^{21} \rangle$.
- By Theorem 1, $|a^{21}| = 30/\gcd(30,21) = 10$
- Also $\langle a^{21} \rangle = \langle a^3 \rangle$
  $= \{a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}, a^{24}, a^{27}, e\}$

379

Group Theory

- **Elementary Properties of Cyclic Groups**

380

Elementary Properties of Cyclic Groups

Theorem 1

If $|a| = n$, then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n,k)$.

Corollaries to Theorem 1

1.In a finite cyclic group, the order of an element divides the order of the group.

2.Let $|a| = n$ in any group. Then

a) $\langle a^i \rangle = \langle a^j \rangle$ iff gcd(n,i) = gcd(n,j)

b) $|a^i| = |a^j|$ iff gcd(n,i) = gcd(n,j)

381

Elementary Properties of Cyclic Groups

Corollaries to Theorem 1

3. Let $|a| = n$.
   Then $\langle a^i \rangle = \langle a^j \rangle$ iff gcd(n,i) = gcd(n,j)
4. An integer k in $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ iff gcd(n,k) =1

382

Elementary Properties of Cyclic Groups

Example

Find all the generators of U(50) = ⟨3⟩.

U(50) ={1,3,7,9,11,13,17,19,21,23,27,29,31,33,
37,39,41,43,47,49} |U(50)| = 20

The numbers relatively prime to 20 are 1, 3, 7, 9, 11, 13, 17, 19

The generators of U(50) are therefore

$3^1, 3^3, 3^7, 3^9, 3^{11}, 3^{13}, 3^{17}, 3^{19}$

i.e. 3, 27, 37, 33, 47, 23, 13, 17

383

Group Theory

- **Fundamental Theorem of Cyclic Groups**

384

Fundamental Theorem of Cyclic Groups

Fundamental Theorem of Cyclic Groups

a) Every subgroup of a cyclic group is cyclic.
b) If $|a|$ = n, then the order of any subgroup of $<a>$ is a divisor of n
c) For each positive divisor k of n, the group $<a>$ has exactly one subgroup of order k, namely $<a^{n/k}>$

385

Fundamental Theorem of Cyclic Groups

Subgroups are cyclic

Proof: Let G = $<a>$ and suppose H ≤ G. If H is trivial, then H is cyclic.

Suppose H is not trivial.

Let m be the smallest positive integer with a^m in H.

(Does m exist?) ________

386

Fundamental Theorem of Cyclic Groups

By closure, $<a^m>$ is contained in H.

We claim that H = $<a^m>$. To see this,

choose any b = a^k in H. There exist integers q,r with

0≤ r < m such that

$a^k = a^{qm+r}$ (Why?) ___________

387

Fundamental Theorem of Cyclic Groups

Since $b = a^k = a^{qm}a^r$, we have

$a^r = (a^m)^{-q}\, b$

Since b and a^m are in H, so is a^r.

But r < m (the smallest power of a in H)

so r = 0.

Hence $b = (a^m)^q$ and b is in H.

It follows that H = $<a^m>$ as required.

388

Fundamental Theorem of Cyclic Groups

|H| is a divisor of |*a*|

Proof: Given $|<a>|$ = n and H ≤ $<a>$. We showed H = $<a^m>$ where m is the smallest positive integer with a^m in H.

Now $e = a^n$ is in H, so as we just showed, n = mq for some q.

Now $|a^m|$ = q is a divisor of n as required.

389

Fundamental Theorem of Cyclic Groups

Exactly one subgroup for each divisor k of n

- (**Existence**) Given $|<a>|$ = n. Let k | n.
  Say n = kq. Note that gcd(n,q) = q
  So $|a^q|$ = n/gcd(n,q) = n/q = k.
  Hence there exists a subgroup of order k, namely $<a^{n/q}>$

390

Fundamental Theorem of Cyclic Groups

- (**Uniqueness**) Let H be any subgroup of $<a>$ with order k. We claim H = $<a^{n/k}>$

  From (a), H = $<a^m>$ for some m.

  From (b), m | n so gcd(n,m) = m.

  So k = $|a^m|$ = n/gcd(n,m) by Theorem 1

  = n/m

  Hence m = n/k

  So H = $<a^{n/k}>$ as required.

391

Group Theory

- **Subgroups of Finite Cyclic Groups**

392

Subgroups of Finite Cyclic Groups

Theorem

Let G be a cyclic group with n elements and generated by a. Let $b \in G$ and let $b=a^k$. Then b generates a cyclic subgroup H of G containing n/d elements, where d = gcd (n, k).

Also $<a^k> = <a^s>$ if and only if gcd (k, n) = gcd (s, n).

393

Subgroups of Finite Cyclic Groups

Example

using additive notation, consider in $\mathbb{Z}_{12}$, with the generator a=1.

- 3 = 3·1, gcd(3, 12)=3, so $\langle 3 \rangle$ has 12/3=4 elements.

  $\langle 3 \rangle$={0, 3, 6, 9}
- Furthermore, $\langle 3 \rangle = \langle 9 \rangle$ since gcd(3, 12)=gcd(9, 12).

394

Subgroups of Finite Cyclic Groups

Example

- 8= 8·1, gcd (8, 12)=4, so $\langle 8 \rangle$ has 12/4=3 elements.

  $\langle 8 \rangle$={0, 4, 8}
- 5= 5·1, gcd (5, 12)=1, so $\langle 5 \rangle$ has 12 elements.

  $\langle 5 \rangle = \mathbb{Z}_{12}$.

395

Subgroups of Finite Cyclic Groups

Corollary

If a is a generator of a finite cyclic group G of order n, then the other generators of G are the elements of the form a^r, where r is relatively prime to n.

396

Subgroups of Finite Cyclic Groups

Example

Find all subgroups of $\mathbb{Z}_{18}$ and give their subgroup diagram.

- All subgroups are cyclic
- By above Corollary is the generator of Z_{18}, so is 5, 7, 11, 13, and 17.
- Starting with 2, $\langle 2 \rangle$={0, 2, 4, 6, 8, 10, 12, 14, 16 }is of order 9, and gcd(2, 18)=2=gcd(k, 18) where k is 2, 4, 8, 10, 14, and 16. Thus 2, 4, 8, 10, 14, and 16 are all generators of $\langle 2 \rangle$.

397

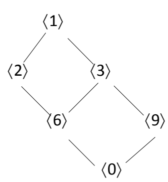
Subgroups of Finite Cyclic Groups

Example

- $\langle 3 \rangle$={0, 3, 6, 9, 12, 15} is of order 6, and gcd(3, 18)=3=gcd(k, 18) where k=15
- $\langle 6 \rangle$={0, 6, 12} is of order 3, so is 12
- $\langle 9 \rangle$={0, 9} is of order 2

398

Subgroups of Finite Cyclic Groups



399

Group Theory

Theorem on Cyclic Group

400

Theorem on Cyclic Group

Theorem

Let G be a cyclic group with generator a.

If the order of G is infinite, then G is isomorphic to $(\mathbb{Z}, +)$.

If G has finite order n, then G is isomorphic to $(\mathbb{Z}_n, +_n)$.

401

Theorem on Cyclic Group

Proof

Case 1

For all positive integers m, $a^m \neq e$.

In this case we claim that no two distinct exponents h and k can give equal elements a^h and a^k of G.

Suppose that $a^h = a^k$ and say $h > k$.

Then $a^h a^{-k} = a^{h-k} = e$, contrary to our Case 1 assumption.

402

Theorem on Cyclic Group

Case 1

Hence every element of G can be expressed as a^m for a unique m $\in \mathbb{Z}$.

The map $\varphi : G \to \mathbb{Z}$ given by $\varphi(a^i) = i$ is thus well defined, one to one, and onto $\mathbb{Z}$.

403

Theorem on Cyclic Group

Case 1

Also,

$\varphi(a^i a^j)=\varphi(a^{i+j})$

$=i+j$

$=\varphi(a^i)+\varphi(a^j)$,

so the homomorphism property is satisfied and φ is an isomorphism.

404

Theorem on Cyclic Group

Case 2

$a^m = e$ for some positive integer m.

Let n be the smallest positive integer such that

$a^n = e$.

If $s \in \mathbb{Z}$ and $s = nq + r$ for $0 < r < n$, then

$a^s = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r$.

As in Case 1, if $0 < k < h < n$ and

$a^h = a^k$, then $a^{h-k} = e$ and $0 < h-k < n$, contradicting our choice of n.

405

Theorem on Cyclic Group

Case 2

Thus the elements

$a^0=e, a, a^2, a^3, \cdots, a^{n-1}$ are all distinct and comprise all elements of G.

The map $\Psi : G \to \mathbb{Z}_n$ given by $\Psi(a^i) = i$ for $i = 0, 1, 2, \cdots, n - 1$ is thus well defined, one to one, and onto $\mathbb{Z}_n$.

406

Theorem on Cyclic Group

Case 2

Because $a^n = e$, we see

that $a^i a^j = a^k$

where $k = i +_n j$.

Thus $\Psi(a^i a^j) = i +_n j$

$= \Psi(a^i) +_n \Psi(a^j)$,

so the homomorphism property is satisfied and Ψ is an isomorphism.

407

Group Theory

Permutation Groups

408

Permutation Groups

Definition

A permutation of a set A is a function from A to A that is both one to one and onto.

409

Permutation Groups

Array Notation

- Let A = {1, 2, 3, 4}
- Here are two permutations of A:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\alpha(2) = 3 \qquad \beta(4) = 3$$
$$\alpha(4) = 4 \qquad \beta(1) = 2$$
$$\beta\alpha(2) = \beta(3) = 4$$

410

Permutation Groups

Composition in Array Notation

$$\beta\alpha = \begin{pmatrix} 1 & \boxed{2} & 3 & 4 \\ 2 & \boxed{1} & 4 & 3 \end{pmatrix}\begin{pmatrix} \boxed{1} & 2 & 3 & 4 \\ \boxed{2} & 3 & 1 & 4 \end{pmatrix}$$
$$= \begin{pmatrix} \boxed{1} & 2 & 3 & 4 \\ \boxed{1} & & & \end{pmatrix}$$

411

Permutation Groups

Composition in Array Notation

$$\beta\alpha = \begin{pmatrix} 1 & 2 & \boxed{3} & 4 \\ 2 & 1 & \boxed{4} & 3 \end{pmatrix}\begin{pmatrix} 1 & \boxed{2} & 3 & 4 \\ 2 & \boxed{3} & 1 & 4 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & \boxed{2} & 3 & 4 \\ 1 & \boxed{4} & & \end{pmatrix}$$

412

Permutation Groups

Composition in Array Notation

$$\beta\alpha = \begin{pmatrix} \boxed{1} & 2 & 3 & 4 \\ \boxed{2} & 1 & 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & \boxed{3} & 4 \\ 2 & 3 & \boxed{1} & 4 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & \boxed{3} & 4 \\ 1 & 4 & \boxed{2} & \end{pmatrix}$$

413

Permutation Groups

Composition in Array Notation

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & \boxed{4} \\ 2 & 1 & 4 & \boxed{3} \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & \boxed{4} \\ 2 & 3 & 1 & \boxed{4} \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & \boxed{4} \\ 1 & 4 & 2 & \boxed{3} \end{pmatrix}$$

414

Permutation Groups

Composition in Array Notation

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

415

Permutation Groups

Definition

A permutation group of a set A is a set of permutations of A that forms a group under function composition.

416

Permutation Groups

Example

- The set of all permutations on {1,2,3} is called the symmetric group on three letters, denoted S_3
- There are 6 permutations possible:

$$\begin{pmatrix} 1 & 2 & 3 \\ \_\_ & \_\_ & \_\_ \end{pmatrix}$$
$$3 \times 2 \times 1 = 6$$

417

Group Theory

Examples of Permutation Groups

418

Examples of Permutation Groups

S_3

- The permutations of {1,2,3}:

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \alpha^2\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

419

Examples of Permutation Groups

Is S_3 a group?

- Composition of functions is always associative.
- Identity is ε.
- Since permutations are one to one and onto, there exist inverses (which are also permutations).
- Therefore, S_3 is group.

420

Examples of Permutation Groups

Computations in S_3

$$\alpha^3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \varepsilon$$

$$\beta^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \varepsilon$$

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \alpha^2\beta$$

421

Examples of Permutation Groups

Simplified Computations in S_3

- $\alpha\beta\alpha^2\beta = \alpha(\beta\alpha)\alpha\beta = \alpha(\alpha^2\beta)\alpha\beta$
  $= \alpha^3(\beta\alpha)\beta = \varepsilon(\alpha^2\beta)\beta$
  $= \alpha^2\beta^2$
  $= \alpha^2$
- Double the exponent of α when switching with β.
- We can simplify any expression in S_3!

422

Group Theory

Examples of Permutation Groups

423

Examples of Permutation Groups

Symmetric Groups, S_n

- Let A = {1, 2, … n}. The symmetric group on n letters, denoted S_n, is the group of all permutations of A under composition.
- S_n is a group for the same reasons that S_3 is group.
- $|S_n| = n!$

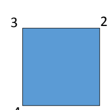
424

Examples of Permutation Groups

Symmetries of a Square, D_4

$$R_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad H = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$R_{90} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad V = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$



$$R_{180} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad D = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$$R_{270} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \quad D' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$D_4 \le S_4$

425

Examples of Permutation Groups

Why do we care?

- Every group turns out to be a permutation group on some set! (To be proved later).

426

Group Theory

Permutation Groups

Permutation Groups

Definition

Let $f : A \rightarrow B$ be a function and let H be a subset of A. The **image** of H **under** f is

$\{f(h) \mid h \in H\}$ and is denoted by f[H].

Permutation Groups

Lemma

Let G and G' be groups and let $\varphi : G \rightarrow G'$ be a one-to-one function such that $\varphi(xy) = \varphi(x)\varphi(y)$

for all $x, y \in G$.

Then $\varphi[G]$ is a subgroup of G' and φ provides an isomorphism of G with $\varphi[G]$.

Permutation Groups

Proof

Let $x', y' \in \varphi[G]$. Then there exist $x, y \in G$ such that $\varphi(x) = x'$ and $\varphi(y) = y'$.

By hypothesis, $\varphi(xy) = \varphi(x)\varphi(y) = x'y'$, showing that $x'y' \in \varphi[G]$.

We have shown that $\varphi[G]$ is closed under the operation of G'.

Permutation Groups

Let e' be the identity of G'.

Then

$e'\varphi(e) = \varphi(e)$

$= \varphi(ee)$

$= \varphi(e)\varphi(e)$.

Cancellation in G' shows that $e' = \varphi(e)$ so $e' \in \varphi[G]$.

Permutation Groups

For $x' \in \varphi[G]$ where $x' = \varphi(x)$, we have

$e'=\varphi(e)$

$= \varphi(xx^{-1})$

$= \varphi(x)\, \varphi(x^{-1})$

$= x'\, \varphi(x^{-1})$

which shows that

$x'^{-1} = \varphi(x^{-1}) \in \varphi[G]$.

Therefore, $\varphi[G]<G'$.

Permutation Groups

Note that φ provides an isomorphism of G with $\varphi[G]$ follows at once because φ provides a one-to-one map of G onto $\varphi[G]$ such that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$.

433

Group Theory

Cayley's Theorem

434

Cayley's Theorem

Theorem

Every group is isomorphic to a group of permutations.

435

Cayley's Theorem

Proof

Let G be a group.

We show that G is isomorphic to a subgroup of S_G.

We Need only to define a one-to-one function

φ: $G \rightarrow S_G$ such that

$\varphi(xy) = \varphi(x)\varphi(y)$

for all $x, y \in G$.

436

Cayley's Theorem

For $x \in G$, let $\lambda_x : G \rightarrow G$ be defined by $\lambda_x(g) = xg$ for all $g \in G$. (We think of λ_x as performing left multiplication by x.)

The equation $\lambda_x(x^{-1}c) = x(x^{-1}c) = c$ for all $c \in G$ shows that λ_x maps G onto G. If $\lambda_x(a) = \lambda_x(b)$, then $xa = xb$ so $a = b$ by cancellation. Thus λ_x is also one to one, and is a permutation of G.

437

Cayley's Theorem

We now define φ: $G \rightarrow S_G$ by defining $\varphi(x) = \lambda_x$ for all $x \in G$.

To show that φ is one to one, suppose that

$\varphi(x) = \varphi(y)$.

Then $\lambda_x = \lambda_y$ as functions mapping G into G.

In particular $\lambda_x(e) = \lambda_y(e)$, so $xe = ye$ and $x = y$.

Thus φ is one to one.

438

Cayley's Theorem

It only remains to show that $\varphi(xy) = \varphi(x)\varphi(y)$,
that is, $\lambda_{xy} = \lambda_x \lambda_y$.
Now for any $g \in G$, we have $\lambda_{xy}(g) = (xy)g$.
Permutation multiplication is function composition, so $(\lambda_x \lambda_y)(g) = \lambda_x(\lambda_y(g)) = \lambda_x(yg) = x(yg)$.
Thus by associativity, $\lambda_{xy} = \lambda_x \lambda_y$.

439

Group Theory

Examples of Permutation Groups

440

Examples of Permutation Groups

There is a natural correspondence between the elements of S_3 and the ways in which two copies of an equilateral triangle with vertices 1, 2, and 3 can be placed, one covering the other with vertices on top of vertices.

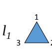
For this reason, S_3 is also the **group D_3 of symmetries of an equilateral triangle.** We used ρ, for rotations and μ; for mirror images in bisectors of angles. The notation D_3 stands for the third dihedral group.

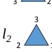
The **nth dihedral group** D_n is the group of symmetries of the regular n-gon.

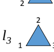
441

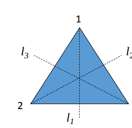
Examples of Permutation Groups

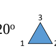
ρ_0 = do nothing

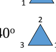
μ_1 = reflect in line l_1 

μ_2 = reflect in line l_2 

μ_3 = reflect in line l_3 



ρ_1 = rotate anticlockwise 120° 

ρ_2 = rotate anticlockwise 240° 

442

Examples of Permutation Groups

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$
$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$\mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$
$$\mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

443

Group Theory

Examples of Permutation Groups

444

Examples of Permutation Groups

Recall

We form the dihedral group D_4 of permutations corresponding to the ways that two copies of a square with vertices 1, 2, 3, and 4 can be placed, one covering the other with vertices on top of vertices.

D_4 is the **group of symmetries of the square.**

It is also called the **octic group.**

445

Examples of Permutation Groups

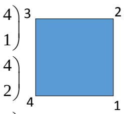
Symmetries of a Square, D_4

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

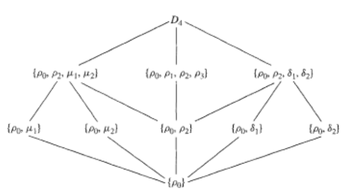
$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \quad \delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$



$D_4 \leq S_4$

446

Examples of Permutation Groups



447

Group Theory

Orbits

448

Orbits

Definition

An orbit of a permutation p is an equivalence class under the relation:

a ~ b $\Leftrightarrow$ b = $p^n(a)$,

for some n in $\mathbb{Z}$.

449

Orbits

Find all orbits of $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$

Method:

Let S be the set that the permutation works on.

0) Start with an empty list

1) If possible, pick an element of the S not already visited and apply permutation repeatedly to get an orbit.

2) Repeat step 1 until all elements of S have been visited.

450

Orbits

- Look at what happens to elements as a permutation is applied.
- $$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

$\alpha(1)=2, \alpha^2(1)=3, \alpha^3(1)=1$ {1,2,3}

$\alpha(4)=5, \alpha^2(4)=4$ {4,5}

451

Group Theory

Orbits

452

Orbits

Theorem

Let p be a permutation of a set S.

The following relation is an equivalence relation:
a ~ b ⇔ b $=p^n(a)$,
for some n in $\mathbb{Z}$.

453

Orbits

Proof

1) reflexive:
 a = $p^0(a)$ ⇒ a~a

2) symmetric:
 a~b ⇒ b = $p^n(a)$, for some n in $\mathbb{Z}$
⇒ a = $p^{-n}(b)$,
 with -n in $\mathbb{Z}$
⇒ b~a

454

Orbits

3) transitive:
 a~b and b~c
⇒ b = $p^{n_1}(a)$ and c = $p^{n_2}(b)$, for some n_1 and n_2 in $\mathbb{Z}$
⇒ c = $p^{n_2}(p^{n_1}(a))$, for some n_1 and n_2 in $\mathbb{Z}$
⇒ c = $p^{n_2+n_1}(a)$, with $n_2 + n_1$ in $\mathbb{Z}$
⇒ a~c

455

Group Theory

Cycles

456

Cycles

Definition

A permutation is a cycle if at most one of its orbits is nontrivial (has more than one element).

457

Cycles

Definition

A cycle of length 2 is called a transposition.

458

Cycles

Example

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

=(1, 2, 3)(4, 5)

=(1,3)(1,2)(4,5)

459

Cycles

Composition in cycle notation

$\alpha\beta$ = (1 2 3)(1 2)(3 4)

= (1 3 4)(2)

= (1 3 4)

$\beta\alpha$ = (1 2)(3 4)(1 2 3)

= (1)(2 4 3)

= (2 4 3)

460

Group Theory

Disjoint Cycles

461

Disjoint Cycles

Definition

Two permutations are disjoint if the sets of elements moved by the permutations are disjoint.

462

Disjoint Cycles

Symmetries of a Square, $D_4 \leq S_4$

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1\ 2)(1\ 2)$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2)$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\ 3)(2\ 4)$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1\ 4\ 3\ 2) = (1\ 2)(1\ 3)(1\ 4)$$

463

Disjoint Cycles

Symmetries of a Square, $D_4 \leq S_4$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 4)$$

$$\mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1\ 4)(2\ 3)$$

$$\delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (2\ 4)$$

$$\delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (1\ 3)$$

464

Group Theory

Cycle Decomposition

465

Cycle Decomposition

Theorem:

Every permutation of a finite set is a product of disjoint cycles.

466

Cycle Decomposition

Proof:

Let σ be a permutation.

Let $B_1, B_2, \ldots, B_r$ be the orbits.

Let μ_i be the cycle defined by $\mu_i(x) = \sigma(x)$ if x in B_i and x otherwise.

Then $\sigma = \mu_1 \mu_2 \ldots \mu_r$.

Note: Disjoint cycles commute.

467

Cycle Decomposition

Lemma

Every cycle is a product of transpositions.

Proof

Let $(a_1, a_2, \ldots, a_n)$ be a cycle, then

$(a_1, a_n)(a_1, a_{n-1}) \ldots (a_1, a_2) = (a_1, a_2, \ldots, a_n)$.

468

Cycle Decomposition

Theorem

Every permutation can be written as a product of transpositions.

Proof

Use the lemma plus the previous theorem.

Group Theory

Parity of Permutation

Parity of a Permutation

Definition

The parity of a permutation is said to be even if it can be expressed as the product of an **even** number of transpositions, and **odd** if it can be expressed as a product of an odd number of transpositions.

Parity of a Permutation

Theorem

The parity of a permutation is even or odd, but not both.

Parity of a Permutation

Proof

We show that for any positive integer n, parity is a homomorphism from S_n to the group $\mathbb{Z}_2$, where 0 represents **even**, and 1 represents **odd**.
These are alternate names for the equivalence classes $2\mathbb{Z}$ and $2\mathbb{Z}+1$ that make up the group $\mathbb{Z}_2$.
There are several ways to define the parity map.
They tend to use the group {1, -1} with multiplicative notation instead of {0, 1} with additive notation.

Parity of a Permutation

One way uses linear algebra: For the permutation π define a map from R^n to R^n by switching coordinates as follows

$$L_\pi(x_1, x_2, \ldots, x_n) = (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}).$$

Then L_π is represented by a n x n matrix M_π whose rows are the corresponding permutation of the rows of the n x n identity matrix.
The map that takes the permutation π to Det (M_π) is a homomorphism from S_n to the multiplicative group {-1, 1}.

Parity of a Permutation

Another way uses the action of the permutation on the polynomial

$P(x_1, x_2, \ldots, x_n) = \text{Product}\{(x_i - x_j) \mid i < j\}$.

Each permutation changes the sign of P or leaves it alone.

This determines the parity: change sign = odd parity, leave sign = even parity.

475

Group Theory

Alternating Group

476

Alternating Group

Definition

The alternating group on n letters consists of the even permutations in the symmetric group of n letters.

477

Alternating Group

Definition

The alternating group on n letters consists of the even permutations in the symmetric group of n letters.

478

Alternating Group

Theorem

If n≥2, then the collection of all even permutations of

{1, 2, …, n}

forms a subgroup of order n!/2 of the symmetric group S_n.

479

Alternating Group

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (12)(12)$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3) = (1\ 3)(1\ 2)$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2) = (1\ 2)(1\ 3)$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3)$$

$$\mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3)$$

$$\mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2)$$

480

Alternating Group

A_3={(1), (1 2 3), (1 3 2)}

	(1)	(1 2 3)	(1 3 2)
(1)	(1)	(1 2 3)	(1 3 2)
(1 2 3)	(1 2 3)	(1 3 2)	(1)
(1 3 2)	(1 3 2)	(1)	(1 2 3)

Group Theory

Direct Products

Direct Products

Definition

The Cartesian product of sets $S_1, \ldots, S_n$ is the set of all n-tuples $(a_1,\cdots, a_n)$, where $a_i \in S_i$ for $i = 1,\cdots, n$. The Cartesian product is denoted by either $S_1 \times \ldots \times S_n$ or by $\prod_{i=1}^{n} S_i$.

Direct Products

Let $G_1, \cdots, G_n$ be groups, and let us use multiplicative notation for all the group operations. Regarding the G as sets, we can form $\prod_{i=1}^{n} G_i$.
Let us show that we can make $\prod_{i=1}^{n} G_i$ into a group by means of a binary operation of multiplication by components.

Direct Products

Theorem

Let $G_1, \ldots, G_n$ be groups.
For $(a_1, \ldots, a_n)$ and $(b_1,\ldots, b_n)$ in $\prod_{i=1}^{n} G_i$, define $(a_1, \ldots, a_n)(b_1,\ldots, b_n)$ to be the element $(a_1 b_1, \ldots, a_n b_n)$.
Then $\prod_{i=1}^{n} G_i$ is a group, the direct product of the groups G_i, under this binary operation.

Direct Products

Proof

Note that since $a_i, b_i \in G_i$ and G_i is a group, we have $a_ib_i \in G$.
Thus the definition of the binary operation on $\prod_{i=1}^{n} G_i$ given in the statement of the theorem makes sense, that is, $\prod_{i=1}^{n} G_i$ is closed under the binary operation.

Direct Products

The associate law in

$\prod_{i=1}^{n} G_i$ is thrown back onto the associative law in each component as follows:

$(a_1,\cdots, a_n)[(b_1,\cdots, b_n)(c_1,\cdots, c_n)]$

$=(a_1, \cdots, a_n)(b_1c_1,\cdots, b_nc_n)= (a_1(b_1c_1),\cdots, a_n(b_nc_n))$

$= ((a_1b_1)c_1,\cdots, (a_nb_n)c_n)=(a_1b_1,\dots,a_nb_n)(c_1,\dots,c_n)$

$=[(a_1,\dots,a_n)(b_1,\dots,b_n)](c_1,\dots,c_n)$

487

Direct Products

If e_i is the identity element in G_i, then clearly, with multiplication by components, $(e_1,\cdots,e_n)$ an identity in $\prod_{i=1}^{n} G_i$.

Finally, an inverse of $(a_1,\cdots, a_n)$ is $(a_1^{-1},\cdots, a_n^{-1})$; compute the product by components.

Hence $\prod_{i=1}^{n} G_i$ is a group.

488

Group Theory

Direct Products

489

Direct Products

In the event that the operation of each G_i is commutative, we sometimes use additive notation in $\prod_{i=1}^{n} G_i$, and refer to $\prod_{i=1}^{n} G_i$ as the direct sum of the groups G_i. The notation $\bigoplus_{i=1}^{n} G_i$ is sometimes used in this case in place of $\prod_{i=1}^{n} G_i$, especially with abelian groups with operation +. The direct sum of abelian groups G_1, $G_2,\cdots, G_n$ may be written as $G_1 \oplus \dots \oplus G_n$.

490

Direct Products

Proposition

A direct product of abelian groups is abelian.

491

Direct Products

Proof

Let $G_1, \dots, G_n$ be abelian groups. For $(a_1, \dots, a_n)$ and $(b_1,\dots, b_n)$ in $\prod_{i=1}^{n} G_i$,

$(a_1, \dots, a_n)(b_1,\dots, b_n)$

$=(a_1 b_1, \dots, a_n b_n)$

$=(b_1a_1,\dots,b_na_n)$

$=(b_1,\dots, b_n) (a_1, \dots, a_n)$.

492

Direct Products

If the S_i has r_i elements for i =1,⋯,n, then $\prod_{i=1}^{n} S_i$ has $r_1 \ldots r_n$ elements, for in an n-tuple, there are r_1 choices for the first component from S_1, and for each of these there are r_2 choices for the next component from S_2, and so on.

493

Group Theory

Direct Products

494

Direct Products

Example

Consider the group $\mathbb{Z}_2 \times \mathbb{Z}_3$, which has 2·3=6 elements, namely (0, 0), (0, 1), (0, 2), (l, 0), (1, 1), and (1, 2). We claim that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic. It is only necessary to find a generator. Let us try (1, 1). Here the operations in $\mathbb{Z}_2$ and $\mathbb{Z}_3$ are written additively, so we do the same in the direct product $\mathbb{Z}_2 \times \mathbb{Z}_3$.

495

Direct Products

- 1(1, 1) = (1, 1)
- 2(1. 1) = (l, l) + (1, 1) = (0, 2)
- 3(1, 1) = (1, 1) + (1, 1) + (1, 1) = (1, 0)
- 4(1, 1) = 3(1. 1) + (1, 1) = (1, 0) + (1. 1) = (0, 1)
- 5(1, 1) = 4(1, 1) + (1, 1) = (0, 1) + (1, 1) = (1, 2)
- 6(1, 1) = 5(1. 1) + (1, 1) = (1, 2) + (1, 1) = (0, 0)

Thus (1, 1) generates all of $\mathbb{Z}_2 \times \mathbb{Z}_3$. Since there is, up to isomorphism, only one cyclic group structure of a given order, we see that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is isomorphic to $\mathbb{Z}_6$.

496

Direct Products

Example

Consider $\mathbb{Z}_3 \times \mathbb{Z}_3$. This is a group of nine elements. We claim that $\mathbb{Z}_3 \times \mathbb{Z}_3$ is *not* cyclic.

Since the addition is by components, and since in $\mathbb{Z}_3$ every element added to itself three times gives the identity, the same is true in $\mathbb{Z}_3 \times \mathbb{Z}_3$. Thus no element can generate the group, for a generator added to itself successively could only give the identity after nine summands. We have found another group structure of order 9. A similar argument shows that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic. Thus $\mathbb{Z}_2 \times \mathbb{Z}_2$ must be isomorphic to the Klein 4-group.

497

Group Theory

Direct Products

498

Direct Products

Theorem

The group $\mathbb{Z}_m$ x $\mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{mn}$ if and only if *m* and *n* are relatively prime, that is, the gcd of *m* and *n* is 1.

499

Direct Products

Proof

Consider the cyclic subgroup of $\mathbb{Z}_m$ x $\mathbb{Z}_n$ generated by (1,1). The order of this cyclic subgroup is the smallest power of (1,1) that gives the identity (0,0). Here taking a power of (1,1) in our additive notation will involve adding (1,1) to itself repeatedly. Under addition by components, the first component $1 \in \mathbb{Z}_m$ yields 0 only after m summands, 2m summands, and so on, and the second component $1 \in \mathbb{Z}_n$ yields 0 only after n summands, 2n summands, and so on.

500

Direct Products

For them to yield 0 simultaneously, the number of summands must be a multiple of both m and n. The smallest number that is a multiple of both *m* and *n* will be mn if and only if the gcd of m and n is 1; in this case, (1,1) generates a cyclic subgroup of order mn, which is the order of the whole group. This shows that $\mathbb{Z}_m$ x $\mathbb{Z}_n$ is cyclic of order mn, and hence isomorphic to $\mathbb{Z}_{mn}$ if m and n are relatively prime.

501

Direct Products

For the converse, suppose that the gcd of m and n is *d* > 1. The mn/d is divisible by both m and n. Consequently, for any (r, s) in $\mathbb{Z}_m$x $\mathbb{Z}_n$, we have

$\underbrace{(r,s) + \cdots + (r,s)}_{mn/d \text{ summands}} = (0,0).$

Hence no element (r, s) in $\mathbb{Z}_m$ x $\mathbb{Z}_n$ can generate the entire group, so $\mathbb{Z}_m$ x $\mathbb{Z}_n$ is not cyclic and therefore not isomorphic to $\mathbb{Z}_{mn}$.

502

Direct Products

Corollary

The group $\prod_{i=1}^{n}\mathbb{Z}_{m_i}$ is cyclic and isomorphic to $\mathbb{Z}_{m_1 \ldots m_n}$ if and only if the numbers m_i for i = 1,…, n are such that the gcd of any two of them is 1.

503

Direct Products

Example

If *n* is written as a product of powers of distinct prime numbers, as in $n = p_1^{n_1} \ldots p_r^{n_r}$

then $\mathbb{Z}_n$ is isomorphic to

$\mathbb{Z}_{p_1^{n_1}}$ x … x$\mathbb{Z}_{p_r^{n_r}}$.

In particular, $\mathbb{Z}_{72}$ is isomorphic to $\mathbb{Z}_8$ x $\mathbb{Z}_9$.

504

Group Theory

Direct Products

Direct Products

We remark that changing the order of the factors in a direct product yields a group isomorphic to the original one. The names of elements have simply been changed via a permutation of the components in the n-tuples.

Direct Products

It is straightforward to prove that the subset of $\mathbb{Z}$ consisting of all integers that are multiples of both r and s is a subgroup of $\mathbb{Z}$, and hence is cyclic group generated by the least common multiple of two positive integers r and s.
Likewise, the set of all common multiples of n positive integers $r_1,\cdots, r_n$ is a subgroup of $\mathbb{Z}$, and hence is cyclic group generated by the least common multiple of n positive integers $r_1,\cdots, r_n$.

Direct Products

Definition
Let $r_1,\cdots, r_n$ be positive integers. Their least common multiple (abbreviated lcm) is the positive generator of the cyclic group of all common multiples of the r_i, that is, the cyclic group of all integers divisible by each r_i, for $i = 1,\cdots, n$.

Direct Products

Theorem
Let $(a_1,\cdots, a_n)\in \prod_{i=1}^{n} G_i$. If a_i is of finite order r_i in G_i, then the order of $(a_1,\cdots,a_n)$ in $\prod_{i=1}^{n} G_i$ is equal to the least common multiple of all the r_i.

Direct Products

Proof
This follows by a repetition of the argument used in the proof of previous Theorem. For a power of $(a_1,\cdots, a_n)$ to give $(e_1, \cdots,e_n)$, the power must simultaneously be a multiple of r_1 so that this power of the first component a_1 will yield e_1, a multiple of r_2, so that this power of the second component a_2 will yield e_2, and so on.

Group Theory

Direct Products

Direct Products

Example

Find the order of (8, 4, 10) in the group $\mathbb{Z}_{12}$ x $\mathbb{Z}_{60}$ x $\mathbb{Z}_{24}$.

Solution

Since the gcd of 8 and 12 is 4, we see that 8 is of order 3 in $\mathbb{Z}_{12}$. Similarly, we find that 4 is of order 15 in $\mathbb{Z}_{60}$ and 10 is of order 12 in $\mathbb{Z}_{24}$. The lcm of 3, 15, and 12 is 3·5·4 = 60, so (8, 4,10) is of order 60 in the group $\mathbb{Z}_{12}$ x $\mathbb{Z}_{60}$ x $\mathbb{Z}_{24}$.

Direct Products

Example

The group $\mathbb{Z}$ x $\mathbb{Z}_2$ is generated by the elements (1, 0) and (0, 1). More generally, the direct product of n cyclic groups, each of which is either $\mathbb{Z}$ or $\mathbb{Z}_m$ for some positive integer m, is generated by then n-tuples

(1, 0,⋯, 0), (0, 1,⋯, 0),…,(0, 0,⋯, 1). Such a direct product might also be generated by fewer elements. For example, $\mathbb{Z}_3$ x $\mathbb{Z}_4$ x $\mathbb{Z}_{35}$ is generated by the single element (1, 1, 1).

Group Theory

Fundamental Theorem of Finitely Generated Abelian Groups

Fundamental Theorem of Finitely Generated Abelian Groups

Theorem

Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form

$\mathbb{Z}_{{p_1}^{r_1}}$ x … x $\mathbb{Z}_{{p_n}^{r_n}}$ x $\mathbb{Z}$ x … x $\mathbb{Z}$

where the p_i are primes, not necessarily distinct, and the r_i are positive integers. The direct product is unique except for possible rearrangement of the factors; that is, the number (Betti number of G) of factors $\mathbb{Z}$ is unique and the prime powers ${p_i}^{r_i}$ are unique.

Fundamental Theorem of Finitely Generated Abelian Groups

Example

Find all abelian groups, up to isomorphism, of order 360. The phrase *up to isomorphism* signifies that any abelian group of order 360 should be structurally identical (isomorphic) to one of the groups of order 360 exhibited.

Fundamental Theorem of Finitely Generated Abelian Groups

Solution

Since our groups are to be of the finite order 360, no factors $\mathbb{Z}$ will appear in the direct product shown in the statement of the fundamental theorem of finitely generated abelian groups.

First we express 360 as a product of prime powers $2^3.3^2.5$.

517

Fundamental Theorem of Finitely Generated Abelian Groups

Then, we get as possibilities

1. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

2. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

3. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

4. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

5. $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

6. $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

Thus there are six different abelian groups (up to isomorphism) of order 360.

518

Group Theory

Applications

519

Applications

Definition

A group G is **decomposable** if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise G is **indecomposable.**

520

Applications

Theorem

The finite indecomposable abelian groups are exactly the cyclic groups with order a power of a prime.

521

Applications

Proof

Let G be a finite indecomposable abelian group. Then, G is isomorphic to a direct product of cyclic groups of prime power order. Since G is indecomposable, this direct product must consist of just one cyclic group whose order is a power of a prime number.

Conversely, let p be a prime. Then $\mathbb{Z}_{p^r}$ is indecomposable, for if $\mathbb{Z}_{p^r}$ were isomorphic to $\mathbb{Z}_{p^i} \times \mathbb{Z}_{p^j}$, where i + j = r, then every element would have an order at most $p^{max\{i,j\}} < p^r$.

522

Group Theory

Applications

Applications

Theorem

If m divides the order of a finite abelian group G, then G has a subgroup of order m.

Applications

Proof

We can think of G as being

$\mathbb{Z}_{p_1^{r_1}}$ X ... X $\mathbb{Z}_{p_n^{r_n}}$ where not all primes p_i need be distinct. Since $p_1^{r_1} \ldots p_n^{r_n}$ is the order of G, then m must be of the form $p_1^{s_1} \ldots p_n^{s_n}$, where $0 \leq s_i \leq r_i$.

$p_i^{r_i - s_i}$ generates a cyclic subgroup of $\mathbb{Z}_{p_i^{r_i}}$ of order equal to the quotient of $p_i^{r_i}$ by the gcd of $p_i^{r_i}$ and $p_i^{r_i - s_i}$. But the gcd of $p_i^{r_i}$ and $p_i^{r_i - s_i}$ is $p_i^{r_i - s_i}$. Thus $p_i^{r_i - s_i}$ generates a cyclic subgroup $\mathbb{Z}_{p_i^{r_i}}$ of order $[p_i^{r_i}]/[p_i^{r_i - s_i}] = p_i^{s_i}$.

Applications

Recalling that <a> denotes the cyclic subgroup generated by a, we see that

$< p_1^{r_1 - s_1} >$ x ... x $< p_n^{r_n - s_n} >$

is the required subgroup of order m.

Group Theory

Applications

Applications

Theorem

If m is a square free integer, that is, m is not divisible by the square of any prime, then every abelian group of order m is cyclic.

Applications

Proof

Let G be an abelian group of square free order m. Then, G is isomorphic to

$\mathbb{Z}_{p_1{}^{r_1}}$ x … x $\mathbb{Z}_{p_n{}^{r_n}}$,

where m= ${p_1}^{r_1}$ … ${p_n}^{r_n}$. Since m is square free, we must have all r_i = 1 and all p_i distinct primes. Then, G is isomorphic to $\mathbb{Z}_{p_1 \dots p_n}$, so G is cyclic.

529

Group Theory

Cosets

530

Cosets

Definition

Let H be a subgroup of a group G, which may be of finite or infinite order and *a* in G.

The *left coset of H containing a* is the set

*a*H = {*a*h | h in H}

The *right coset of H containing a* is the set

H*a* = {h*a* | h in H}

In additive groups, we use *a*+H and H+*a* for left and right cosets, respectively.

531

Cosets

Example

We exhibit the left cosets and the right cosets of the subgroup 3ℤ of ℤ.

0+3ℤ= 3ℤ ={…, -6, -3, 0, 3, 6, … }

1+3ℤ={…, -5, -2, 1, 4, 7, … }

2+3ℤ={…, -4, -1, 2, 5, 8, … }

ℤ= 3ℤ⊔1+3ℤ ⊔ 2+3ℤ

So, these three left cosets constitute the partition of ℤ into left cosets of 3ℤ.

532

Cosets

Example

3ℤ+0= 3ℤ ={…, -6, -3, 0, 3, 6, … }=0+3ℤ

3ℤ+1={…, -5, -2, 1, 4, 7, … }=1+3ℤ

3ℤ+2={…, -4, -1, 2, 5, 8, … }=2+3ℤ

ℤ= 3ℤ⊔3ℤ+1 ⊔ 3ℤ+2

So, the partition of ℤ into right cosets is the same.

533

Group Theory

Cosets

534

Group Theory

Topic No. 67

Group Theory

Partitions of Groups

Partitions of Groups

Let H be a subgroup of a group G, which may be of finite or infinite order.
We exhibit two partitions of G by defining two equivalence relations, $\sim_L$ and $\sim_R$ on G.

Partitions of Groups

Theorem
Let H be a subgroup of a group G.
Let the relation $\sim_L$ be defined on G by $a \sim_L b$ iff $a^{-1}b \in H$.
Let $\sim_R$ be defined by $a \sim_R b$ iff $ab^{-1} \in H$.
Then $\sim_L$ and $\sim_R$ are both equivalence relations on G.

Partitions of Groups

Proof
Reflexive
Let $a \in G$.
Then $a^{-1}a = e \in H$
since H is a subgroup.
Thus $a \sim_L a$.

Partitions of Groups

Symmetric
Suppose $a \sim_L b$.
Then $a^{-1}b \in H$.
Since H is a subgroup,
$(a^{-1}b)^{-1} = b^{-1}a \in H$.
It implies that $b \sim_L a$.

Partitions of Groups

Transitive

Let $a \sim_L b$ and $b \sim_L c$.

Then $a^{-1}b \in H$ and $b^{-1}c \in H$.

Since H is a subgroup,

$(a^{-1}b)(b^{-1}c)=a^{-1}c \in H$.

So, $a \sim_L c$.

Partitions of Groups

- a is called the coset representative of aH.
- Similarly, $aHa^{-1} = \{aha^{-1} \mid h \text{ in } H\}$

Group Theory

Topic No. 68

Group Theory

Examples of Cosets

Examples of Cosets

Vectors under addition are a group:

- $(a,b) + (c,d) = (a+c,b+d) \in \mathbb{R}^2$
- Identity is $(0,0) \in \mathbb{R}^2$
- Inverse of (a,b) is $(-a,-b)$ in $\mathbb{R}^2$
- $((a,b)+(c,d))+(e,f)=(a+c,b+d)+(e,f)=((a+c)+e,(b+d)+f) =(a+(c+e),b+(d+f))=(a,b)+(c+e,d+f)=(a,b)+((c,d)+(e,f))$

H = $\{(2t,t) \mid t \in \mathbb{R}\}$ is a subgroup of $\mathbb{R}^2$.

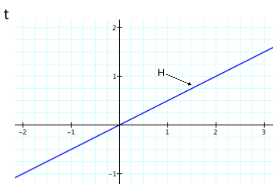
Proof: $(2a,a) - (2b,b) = (2(a-b),a-b) \in H$

Examples of Cosets

Visualizing H=$\{(2t,t) \mid t \in \mathbb{R}\}$

- Let x = 2t, y = t
- Eliminate t:

  y = x/2



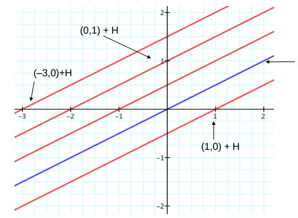
Examples of Cosets

Cosets of H={(2t,t) | t ∈ $\mathbb{R}$}
(a,b) + H = {(a+2t,b+t)}
Set x = a+2t, y = b+t and eliminate t:
y = b + (x-a)/2
The subgroup H is the line y = x/2.
The cosets are lines parallel to y = x/2 !

547

Examples of Cosets

H and some cosets



548

Group Theory

Examples of Cosets

549

Group Theory

Topic No. 69

550

Group Theory

Examples of Cosets

551

Examples of Cosets

Left Cosets of <(23)> in S_3
Let H = <(23)> {ε, (23)}
εH = {ε, (23)}=H
(123)H = {(123), (12)}
(132)H = {(132), (13)}
S_3= H ⊔ (123)H ⊔ (132)H

552

Examples of Cosets

Right Cosets of <(23)> in S_3
Let H = <(23)> {ε, (23)}
H ε = {ε, (23)}=H
H(123) = {(123), (13)}
H(132) = {(132), (12)}
S_3= H ⊔ H(123) ⊔ H(132)

553

Examples of Cosets

Left Cosets of <(123)> in A_4
Let H = <(123)> {ε, (123), (132)}
εH = {ε, (123), (132)}
(12)(34)H = {(12)(34), (243), (143)}
(13)(24)H = {(13)(24), (142), (234)}
(14)(23)H = {(14)(23), (134), (124)}

554

Group Theory

Examples of Cosets

555

Group Theory

Topic No. 70

556

Group Theory

Properties of Cosets

557

Properties of Cosets

Proposition

Let H be a subgroup of G, and *a*,b in G.

1. *a* belongs to *a*H
2. *a*H = H iff *a* belongs to H

558

Properties of Cosets

1. a belongs to aH

Proof: $a = ae$ belongs to aH.

2. aH=H iff a in H

Proof: (⇒) Given aH = H.
By (1), a is in aH = H.

559

Properties of Cosets

(⇐) Given a belongs to H. Then
(i) aH is contained in H by closure.
(ii) Choose any h in H.
Note that a^{-1} is in H since a is.
Let b = a^{-1}h. Note that b is in H. So
h = (aa^{-1})h = $a(a^{-1}$h) = ab is in aH
It follows that H is contained in aH
By (i) and (ii), aH = H

560

Group Theory

Properties of Cosets

561

Group Theory

Topic No. 71

562

Group Theory

Properties of Cosets

563

Properties of Cosets

Proposition
Let H be a subgroup of G, and a,b in G.
3. aH = bH iff a belongs to bH
4. aH and bH are either equal or disjoint
5. aH = bH iff a^{-1}b belongs to H

564

Properties of Cosets

3. aH = bH iff a in bH

Proof: (⇒) Suppose aH = bH. Then

a = ae in aH = bH.

(⇐) Suppose a is in bH. Then

a = bh for some h in H.

so aH = (bh)H = b(hH) = bH by (2).

565

Properties of Cosets

4. aH and bH are either disjoint or equal.

Proof: Suppose aH and bH are not disjoint. Say x is in the intersection of aH and bH.

Then aH = xH = bH by (3).

Consequently, aH and bH are either disjoint or equal, as required.

566

Properties of Cosets

5. aH = bH iff a^{-1}b in H

Proof: aH = bH

⇔ b in aH by (3)

⇔ b = ah for some h in H

⇔ a^{-1} b = h for some h in H

⇔ a^{-1} b in H

567

Group Theory

Properties of Cosets

568

Group Theory

Topic No. 72

569

Group Theory

Properties of Cosets

570

Properties of Cosets

Proposition

Let H be a subgroup of G, and a in G.

6. $|aH| = |bH|$
7. $aH = Ha$ iff $H = aHa^{-1}$
8. $aH \leq G$ iff a belongs to H

571

Properties of Cosets

6. $|aH| = |bH|$

Proof: Let $\phi: aH \to bH$ be given by

$\phi(ah) = bh$ for all h in H.

We claim ϕ is one to one and onto.

If $\phi(ah_1) = \phi(ah_2)$, then $bh_1 = bh_2$

so $h_1 = h_2$. Therefore $ah_1 = ah_2$.

Hence ϕ is one-to-one.

ϕ is clearly onto.

It follows that $|aH| = |bH|$ as required.

572

Properties of Cosets

7. $aH = Ha$ iff $H = aHa^{-1}$

Proof: $aH = Ha$

$\Leftrightarrow$ each $ah = h'a$ for some h' in H

$\Leftrightarrow$ $aha^{-1} = h'$ for some h' in H

$\Leftrightarrow$ $H = aHa^{-1}$.

573

Properties of Cosets

8. $aH \leq G$ iff a in H

Proof: ($\Rightarrow$) Suppose $aH \leq G$.

Then e in aH.

But e in eH, so eH and aH are not disjoint. By (4), aH =eH =H.

($\Leftarrow$) Suppose a in H.

Then $aH = H \leq G$.

574

Group Theory

Properties of Cosets

575

Group Theory

Lagrange's Theorem

576

Lagrange's Theorem

Lagrange's Theorem

Statement

If G is a finite group and H is a subgroup of G, then |H| divides |G|.

Lagrange's Theorem

Proof

The right cosets of H in G form a partition of G, so G can be written as a disjoint union

$G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k$

for a finite set of elements $a_1, a_2, \ldots, a_k \in G$.

The number of elements in each coset is |H|.

Hence, counting all the elements in the disjoint union above, we see that |G| = k|H|.

Therefore, |H| divides |G|.

Lagrange's Theorem

Subgroups of $\mathbb{Z}_{12}$

$|\mathbb{Z}_{12}|=12$

The divisors of 12 are 1, 2, 3, 4, 6 and 12.

The subgroups of $\mathbb{Z}_{12}$ are

$H_1=\{[0]\}$

$H_2=\{[0],[6]\}$

$H_3=\{[0],[4],[8]\}$

$H_4=\{[0],[3],[6],[9]\}$

$H_5=\{[0],[2],[4],[6],[8],[10]\}$

Group Theory

Applications of Lagrange's Theorem

Applications of Lagrange's Theorem

Corollary

Every group of prime order is cyclic.

Applications of Lagrange's Theorem

Proof

Let G be of prime order p, and let a be an element of G different from the identity.

Then the cyclic subgroup <a> of G generated by *a* has at least two elements, a and e.

But the order m≥2 of <a> must divide the prime p.

Thus we must have m = p and <a>=G, so G is cyclic.

Applications of Lagrange's Theorem

Since every cyclic group of order p is isomorphic to $\mathbb{Z}_p$, we see that there is only one group structure, up to isomorphism, of a given prime order p.

Applications of Lagrange's Theorem

Theorem

The order of an element of a finite group divides the order of the group.

Applications of Lagrange's Theorem

Proof

Remembering that the order of an element is the same as the order of the cyclic subgroup generated by the element, we see that this theorem follows directly from Lagrange's Theorem.

Group Theory

Indices of Subgroups

Indices of Subgroups

Definition

Let H be a subgroup of a group G.

The number of left (or right) cosets of H in G is the index (G:H) of H in G.

Indices of Subgroups

The index (G:H) just defined may be finite or infinite.

If G is finite, then obviously (G:H) is finite and (G:H)=IGI/IHI, since every coset of H contains IHI elements.

Indices of Subgroups

Example

$\mu=(1,2,4,5)(3,6)$
$\mu^2=(2,5)(1,4)$
$\mu^3=(1,5,4,2)(3,6)$
$\mu^4=\varepsilon$
$<\mu> < S_6$
$(S_6:<\mu>)=|S_6|/|<\mu>|$
$=6!/4=6.5.3.2=180.$

589

Indices of Subgroups

Example

Find the right cosets of $H = \{e, g^4, g^8\}$ in $C_{12} = \{e, g, g^2, \ldots, g^{11}\}$.

590

Indices of Subgroups

Solution

$H=\{e, g^4, g^8\}$ itself is one coset.

Another is $Hg = \{g, g^5, g^9\}$.

These two cosets have not exhausted all the elements of C_{12}, so pick an element, say g^2, which is not in H or Hg.

A third coset is $Hg^2 = \{g^2, g^6, g^{10}\}$ and a fourth is $Hg^3 =\{g^3, g^7, g^{11}\}$.

Since $C_{12} = H \cup Hg \cup Hg^2 \cup Hg^3$, these are all the cosets. Therefore, $(C_{12}:H)=12/3=4$.

591

Indices of Subgroups

Theorem

Suppose H and K are subgroups of a group G such that $K \leq H \leq G$, and suppose (H:K) and (G:H) are both finite. Then (G:K) is finite, and (G:K)=(G:H)(H:K).

592

Group Theory

Converse of Lagrange's Theorem

593

Converse of Lagrange's Theorem

Lagrange's Theorem shows that if there is a subgroup H of a finite group G, then the order of H divides the order of G.

594

Converse of Lagrange's Theorem

Is the converse true?

That is, if *G* is a group of order n, and m divides n, is there always a subgroup of order m?

We will see next that this is true for abelian groups.

595

Converse of Lagrange's Theorem

However, A_4 can be shown to have no subgroup of order 6, which gives a counterexample for nonabelian groups.

596

Converse of Lagrange's Theorem

A_4 = {(1), (1, 2)(3, 4),
(1, 3)(2, 4),(1, 4)(2, 3),
(1, 2, 3), (1, 3, 2),
(1, 3, 4), (1, 4, 3),
(1, 2, 4),(1, 4, 2),
(2, 3, 4), (2, 4, 3)}

597

Group Theory

An Interesting Example

598

An Interesting Example

Example

A translation of the plane $\mathbb{R}^2$ in the direction of the vector (a, b) is a function f :$\mathbb{R}^2 \rightarrow \mathbb{R}^2$ defined by

f (x, y) = (x + a, y + b).

599

An Interesting Example

The composition of this translation with a translation g in the direction of (c, d) is the function

f g:$\mathbb{R}^2 \rightarrow \mathbb{R}^2$, where

f g(x, y) = f (g(x, y))

= f (x + c, y + d)

= (x + c + a, y + d + b).

This is a translation in the direction of (c + a, d + b).

600

An Interesting Example

It can easily be verified that the set of all translations in $\mathbb{R}^2$ forms an abelian group, under composition.

An Interesting Example

A translation of the plane $\mathbb{R}^2$ in the direction of the vector (0, 0) is an identity function $1_{\mathbb{R}}{}^2:\mathbb{R}^2 \to \mathbb{R}^2$ defined by $1_{\mathbb{R}}{}^2(x, y)=(x+0, y+0)=(x, y)$.

An Interesting Example

The inverse of the translation of the plane $\mathbb{R}^2$ in the direction of the vector (a, b) is an inverse function $f^{-1}:\mathbb{R}^2 \to \mathbb{R}^2$ defined by

$f^{-1}(x, y) = (x - a, y - b)$

such that

$f\,f^{-1}(x, y)=(x, y)=f^{-1}\,f(x, y)$.

An Interesting Example

The inverse of the translation in the direction (a, b) is the translation in the opposite direction (−a,−b).

Group Theory

Homomorphism of Groups

Homomorphism of Groups

Structure-Relating Maps

Let G and G' be groups. We are interested in maps from G to G' that relate the group structure of G to the group structure of G'.

Such a map often gives us information about one of the groups from known structural properties of the other.

Homomorphism of Groups

Structure-Relating Maps

An isomorphism ϕ: G → G', if one exists, is an example of such a structure-relating map. If we know all about the group G and know that ϕ is an isomorphism, we immediately know all about the group structure of G', for it is structurally just a copy of G.

Homomorphism of Groups

Structure-Relating Maps

We now consider more general structure-relating maps, weakening the conditions from those of an isomorphism by no longer requiring that the maps be one to one and onto. We see, those conditions are the purely *set-theoretic portion* of our definition of an isomorphism, and have nothing to do with the binary operations of G and of G'.

Homomorphism of Groups

Definition

If (G, ・) and (H, ∗) are two groups, the function f :G → H is called a *group homomorphism* if

f(a ・ b)=f(a)∗f(b)

for all a, b ∈ G.

Homomorphism of Groups

- We often use the notation

  f : (G, ・) → (H, ∗)

  for such a homorphism.
- Many authors use *morphism* instead of *homomorphism*.

Homomorphism of Groups

Definition

A *group isomorphism* is a bijective group homomorphism.

If there is an isomorphism between the groups (G, ・) and (H,∗), we say that

(G, ・) and (H,∗) are *isomorphic* and write

(G, ・) ≅ (H, ∗).

Homomorphism of Groups

Example

Let ϕ: G → G' be a group homomorphism of G *onto* G'. We claim that if G is abelian, then G' must be abelian. Let *a', b'* ∈ G'. We must show that a' b' = b' a'. Since ϕ is onto G', there exist a, b ∈ G such that ϕ(a)= a' and ϕ(b) = b', Since G is abelian,

we have *ab*= *ba*. Using homomorphism property, we have *a'b'* = ϕ(a) ϕ(b) = ϕ(ab)= ϕ(ba) =

ϕ(b) ϕ(a) = b' a', so G' is indeed abelian.

Group Theory

Examples of Group Homomorphisms

Homomorphism of Groups

Example

The function $f : \mathbb{Z} \to \mathbb{Z}_n$, defined by f (x) = [x] is the group homomorphism, for if $i, j \in \mathbb{Z}$, then

$f(i+j)=[i+j]$
$=[i]+_n[j]$
$=f(i)+_nf(j)$.

Examples of Group Homomorphisms

Example

Let be $\mathbb{R}$ the group of all real numbers with operation addition, and let $\mathbb{R}^+$ be the group of all positive real numbers with operation multiplication. The function $f : \mathbb{R} \to \mathbb{R}^+$, defined by $f(x) = e^x$, is a homomorphism, for if $x, y \in \mathbb{R}$, then

$f(x + y) = e^{x+y} = e^x e^y = f(x) f(y)$.

Examples of Group Homomorphisms

Now f is an isomorphism, for its inverse function $g : \mathbb{R}^+ \to \mathbb{R}$ is ln x.

Therefore, the additive group $\mathbb{R}$ is isomorphic to the multiplicative group $\mathbb{R}^+$.

Note that the inverse function g is also an isomorphism:

$g(x\,y) = ln(x\,y) = ln x + ln y = g(x) + g(y)$.

Group Theory

Examples of Group Homomorphisms

Examples of Group Homomorphisms

Example

Let S_n be the symmetric group on n letters, and let : $\phi: S_n \to \mathbb{Z}_2$ be defined by

$\phi(\sigma) = 0$ if σ is an even permutation,

$= 1$ if σ is an odd permutation.

Show that ϕ is a homomorphism.

Examples of Group Homomorphisms

Solution

We must show that $\phi(\sigma, \mu) = \phi(\sigma) + \phi(\mu)$ for all choices of $\sigma, \mu \in S_n$. Note that the operation on the right-hand side of this equation is written additively since it takes place in the group $\mathbb{Z}_2$. Verifying this equation amounts to checking just four cases:

- σ odd and μ odd,
- σ odd and μ even,
- σ even and μ odd,
- σ even and μ even.

619

Examples of Group Homomorphisms

Checking the first case, if σ and μ can both be written as a product of an odd number of transpositions, then $\sigma\mu$ can be written as the product of an even number of transpositions. Thus $\phi(\sigma, \mu) = 0$ and $\phi(\sigma) + \phi(\mu) = 1 + 1 = 0$ in $\mathbb{Z}_2$. The other cases can be checked similarly.

620

Group Theory

Properties of Homomorphisms

621

Properties of Homomorphisms

Proposition

Let $\phi : G \to H$ be a group morphism, and let e_G and e_H be the identities of G and H, respectively.

Then

(i) $\phi(e_G) = e_H$.

(ii) $\phi(a^{-1}) = \phi(a)^{-1}$ for all $a \in G$.

622

Theorems on Group Homomorphisms

Proof

(i) Since ϕ is a morphism,

$\phi(e_G)\,\phi(e_G)$

$= \phi(e_G\, e_G)$

$= \phi(e_G)$

$= \phi(e_G)e_H$

Hence (i) follows by cancellation in H.

623

Theorems on Group Homomorphisms

Proof

(ii) $\phi(a)\,\phi(a^{-1})$

$= \phi(a\ a^{-1})$

$= \phi(e_G)$

$= e_H$ by (i).

Hence $\phi(a^{-1})$ is the unique inverse of $\phi(a)$; that is $\phi(a^{-1}) = \phi(a)^{-1}$.

624

Group Theory

Properties of Homomorphisms

Properties of Homomorphisms

We tum to some structural features of G and G' that are preserved by a homomorphism

$\phi: G \to G'$.

First we review set-theoretic definitions.

Properties of Homomorphisms

Definition

Let ϕ be a mapping of a set X into a set Y, and let $A \subseteq X$ and $B \subseteq Y$. The image $\phi[A]$ of A in Y under ϕ is $\{\phi(a) \mid a \in A\}$. The set $\phi[X]$ is the range of ϕ. The inverse image $\phi^{-1}[B]$ of B in X is $\{x \in X \mid \phi(x) \in B\}$.

Properties of Homomorphisms

Theorem

Let ϕ be a homomorphism of a group G into a group G'.

1. If H is a subgroup of G, then $\phi[H]$ is a subgroup of G'.

2. If K' is a subgroup of G', then $\phi^{-1}[K']$ is a subgroup of G.

Properties of Homomorphisms

Proof

(1) Let H be a subgroup of G, and let $\phi(a)$ and $\phi(b)$ be any two elements in $\phi[H]$. Then $\phi(a)\,\phi(b) = \phi(ab)$, so we see that $\phi(a)\,\phi(b) \in \phi[H]$; thus, $\phi[H]$ is closed under the operation of G'. The fact that $\phi(e_G) = e_{G'}$ and $\phi(a^{-1}) = \phi(a)^{-1}$ completes the proof that $\phi[H]$ is a subgroup of G'.

Properties of Homomorphisms

Proof

(2) Let K' be a subgroup of G'. Suppose a and b are in $\phi^{-1}[K']$. Then $\phi(a)\phi(b) \in K'$ since K' is a subgroup. The equation $\phi(ab) = \phi(a)\,\phi(b)$ shows that $ab \in \phi^{-1}[K']$. Thus $\phi^{-1}[K']$ is closed under the binary operation in G.

Properties of Homomorphisms

Also, K' must contain the identity element $e_{G'}$= $\phi(e_G)$, so $e_G \in \phi^{-1}[K']$. If $a \in \phi^{-1}[K']$, then $\phi(a) \in K'$, so $\phi(a)^{-1} \in K'$. But $\phi(a)^{-1} = \phi(a^{-1})$, so we must have $a^{-1} \in \phi^{-1}[K']$.

Hence $\phi^{-1}[K']$ is a subgroup of G.

631

Group Theory

Properties of Homomorphisms

632

Properties of Homomorphisms

Theorem: Let h be a homomorphism from a group G into a group G'. Let K be the kernel of h. Then

a K = {x in G | h(x) = h(a)} = h^{-1}[{h(a)}]

and also

K a = {x in G | h(x) = h(a)} = h^{-1}[{h(a)}]

633

Properties of Homomorphisms

Proof

h^{-1}[{h(a)}] = {x in G | h(x) = h(a)} directly from the definition of inverse image.

Now we show that: a K = {x in G | h(x) = h(a)} :

x in a K ⇔ x = a k, for some k in K

⇔ h(x) = h(a k) = h(a) h(k) = h(a) , for some k in K

⇔ h(x) = h(a)

Thus, a K = {x in G | h(x) = h(a)}.

Likewise, K a = {x in G | h(x) = h(a)}.

634

Properties of Homomorphisms

Suppose: h: X → Y is any map of sets. Then h defines an equivalence relation $\sim_h$ on X by:

$x \sim_h y \Leftrightarrow h(x) = h(y)$

The previous theorem says that when h is a homomorphism of groups then the cosets (left or right) of the kernel of h are the equivalence classes of this equivalence relation.

635

Group Theory

Properties of Homomorphisms

636

Properties of Homomorphisms

Definition

If ϕ: G → G' is a group morphism, the *kernel* of ϕ , denoted by Ker ϕ, is defined to be the set of elements of G that are mapped by f to the identity of G'. That is, Ker f ={g ∈ G|f (g) = e' }.

637

Properties of Homomorphisms

Corollary

Let ϕ: G → G' be a group morphism. Then, ϕ is injective if and only if Ker ϕ = {e}.

638

Properties of Homomorphisms

Proof

If Ker(ϕ) = {e}, then for every a ∈ G, the elements mapped into ϕ(a) are precisely the elements of the left coset a { e} = {a}, which shows that ϕ is one to one.

Conversely, suppose ϕ is one to one. Now, we know that ϕ(e)=*e'*, the identity element of G'. Since ϕ is one to one, we see that *e* is the only element mapped into *e'* by ϕ, so Ker(ϕ)= {e}.

639

Properties of Homomorphisms

Definition

To Show ϕ: G → G' is an Isomorphism

Step 1 Show ϕ is a homomorphism.

Step 2 Show Ker(ϕ)= {e}.

Step 3 Show ϕ maps G onto G'.

640

Group Theory

Normal Subgroups

641

Normal Subgroups

Normal Subgrops

Let G be a group with subgroup H. The *right cosets* of H in G are equivalence classes under the relation a ≡ b mod H, defined by ab^{-1} ∈ H. We can also define the relation L on G so that a L b if and only if $b^{-1}a$ ∈ H. This relation, L, is an equivalence relation, and the equivalence class containing a is the *left coset* aH = {ah|h ∈ H}. As the following example shows, the left coset of an element does not necessarily equal the right coset.

642

Normal Subgroups

Example

Find the left and right cosets of $H = A_3$ *and* $K = \{(1), (12)\}$ *in* S_3.

Normal Subgroups

Solution

We calculated the right cosets of $H = A_3$.

Right Cosets

H = {(1), (123), (132)}; H(12) = {(12), (13), (23)}

Left Cosets

H = {(1), (123), (132}; (12)H = {(12), (23), (13)}

In this case, the left and right cosets of H are the same.

Normal Subgroups

However, the left and right cosets of K are not all the same.

Right Cosets

K = {(1), (12)} ; K(13) = {(13), (132)} ; K(23) = {(23), (123)}

Left Cosets

K = {(1), (12)};(23)K = {(23), (132)}; (13)K = {(13), (123)}

Group Theory

Normal Subgroups

Normal Subgroups

Definition

A subgroup H of a group G is called a *normal subgroup* of G if $g^{-1}hg \in H$ for all $g \in G$ and $h \in H$.

Normal Subgroups

Proposition

$Hg = gH$, for all $g \in G$, if and only if H is a normal subgroup of G.

Normal Subgroups

Proof
Suppose that $Hg = gH$.
Then, for any element $h \in H$, $hg \in Hg = gH$.
Hence $hg = gh_1$ for some $h_1 \in H$ and
$g^{-1}hg = g^{-1}gh_1 = h_1 \in H$.
Therefore, H is a normal subgroup.

649

Normal Subgroups

Conversely, if H is normal, let $hg \in Hg$ and
$g^{-1}hg = h_1 \in H$.
Then $hg = gh_1 \in gH$ and $Hg \subseteq gH$.
Also, $ghg^{-1} = (g^{-1})^{-1}hg^{-1} = h_2 \in H$, since H is normal, so $gh = h_2g \in Hg$. Hence, $gH \subseteq Hg$, and so $Hg = gH$.

650

Group Theory

Theorem on Normal Subgroup

651

Theorem on Normal Subgroup

If N is a normal subgroup of a group G, the left cosets of N in G are the same as the right cosets of N in G, so there will be no ambiguity in just talking about the cosets of N in G.

652

Theorem on Normal Subgroup

Theorem
If N is a normal subgroup of $(G, \cdot)$, the set of cosets $G/N = \{Ng \mid g \in G\}$ forms a group $(G/N, \cdot)$, where the operation is defined by
$(Ng_1) \cdot (Ng_2) = N(g_1 \cdot g_2)$.
This group is called the quotient group or factor group of G by N.

653

Theorem on Normal Subgroup

Proof. The operation of multiplying two cosets, Ng_1 and Ng_2, is defined in terms of particular elements, g_1 and g_2, of the cosets. For this operation to make sense, we have to verify that, if we choose different elements, h_1 and h_2, in the same cosets, the product coset $N(h_1 \cdot h_2)$ is the same as
$N(g_1 \cdot g_2)$. In other words, we have to show that multiplication of cosets is well defined.

654

Theorem on Normal Subgroup

Since h_1 is in the same coset as g_1, we have $h_1 \equiv g_1$ mod N. Similarly, $h_2 \equiv g_2$ mod N.
We show that $Nh_1h_2 = Ng_1g_2$.
We have $h_1g_1^{-1} = n_1 \in N$ and $h_2g_2^{-1} = n_2 \in N$, so $h_1h_2(g_1g_2)^{-1} = h_1h_2g_2^{-1}g_1^{-1} = n_1g_1n_2g_2g_2^{-1}g_1^{-1} = n_1g_1n_2g_1^{-1}$.
Now N is a normal subgroup, so $g_1n_2g_1^{-1} \in N$ and $n_1g_1n_2g_1^{-1} \in N$. Hence $h_1h_2 \equiv g_1g_2$ mod N and $Nh_1h_2 = Ng_1g_2$.
Therefore, the operation is well defined.

655

Theorem on Normal Subgroup

- The operation is associative because $(Ng_1 \cdot Ng_2) \cdot Ng_3 = N(g_1g_2) \cdot Ng_3 = N(g_1g_2)g_3$ and also $Ng_1 \cdot (Ng_2 \cdot Ng_3) = Ng_1 \cdot N(g_2g_3) = Ng_1(g_2g_3) = N(g_1g_2)g_3$.
- Since $Ng \cdot Ne = Nge = Ng$ and $Ne \cdot Ng = Ng$, the identity is $Ne = N$.
- The inverse of Ng is Ng^{-1} because $Ng \cdot Ng^{-1} = N(g \cdot g^{-1}) = Ne = N$ and also $Ng^{-1} \cdot Ng = N$.
- Hence $(G/N, \cdot)$ is a group.

656

Group Theory

Example on Normal Subgroup

657

Example on Normal Subgroup

Example
$(\mathbb{Z}_n, +)$ is the quotient group of $(\mathbb{Z},+)$ by the subgroup $n\mathbb{Z} = \{nz | z \in \mathbb{Z}\}$.

658

Example on Normal Subgroup

Solution
Since $(\mathbb{Z},+)$ is abelian, every subgroup is normal. The set $n\mathbb{Z}$ can be verified to be a subgroup, and the relationship $a \equiv b$ mod $n\mathbb{Z}$ is equivalent to $a - b \in n\mathbb{Z}$ and to $n|a - b$. Hence $a \equiv b$ mod $n\mathbb{Z}$ is the same relation as $a \equiv b$ mod n. Therefore, $\mathbb{Z}_n$ is the quotient group $\mathbb{Z}/n\mathbb{Z}$, where the operation on congruence classes is defined by $[a] + [b] = [a + b]$.

659

Example on Normal Subgroup

$(\mathbb{Z}_n,+)$ is a cyclic group with 1 as a generator. When there is no confusion, we write the elements of $\mathbb{Z}_n$ as 0, 1, 2, 3, . . . , n − 1 instead of [0], [1], [2], [3], . . . , [n − 1].

660

Group Theory

Morphism Theorem for Groups

Morphism Theorem for Groups

Theorem

Let K be the kernel of the group morphism

$f: G \to H$. Then G/K is isomorphic to the image of f, and the isomorphism

$\psi: G/K \to \mathrm{Im}\, f$

is defined by

$\psi(Kg) = f(g)$.

Morphism Theorem for Groups

This result is also known as the **first isomorphism theorem.**

Proof. The function ψ is defined on a coset by using one particular element in the coset, so we have to check that ψ is well defined;

that is, it does not matter which element we use.

Morphism Theorem for Groups

$\psi: G/K \to \mathrm{Im}\, f$, $\psi(Kg)=f(g)$.

If $Kg'=Kg$, then $g' \equiv g \bmod K$

so $g'g^{-1} = k \in K = \mathrm{Ker}\, f$.

Hence $g'=kg$ and so

$f(g') = f(kg)$

$= f(k)f(g)$

$= e_H f(g) = f(g)$.

Thus ψ is well defined on cosets.

Morphism Theorem for Groups

The function ψ is a morphism because

$\psi(Kg_1Kg_2)$

$= \psi(Kg_1g_2)$

$= f(g_1g_2)$

$= f(g_1)f(g_2)$

$= \psi(Kg_1)\psi(Kg_2)$.

Morphism Theorem for Groups

If $\psi(Kg) = e_H$, then

$f(g) = e_H$ and $g \in K$.

Hence the only element in the kernel of ψ is the identity coset K, and

ψ is injective.

Morphism Theorem for Groups

Finally, Im ψ = Im f, that is,
$\psi^{-1}(f(g))=Kg$, by the definition of ψ.
Therefore, ψ is the required isomorphism between G/K and Im f.

Group Theory

Application of Morphism Theorem

Application of Morphism Theorem

Example

Show that the quotient group $\mathbb{R}/\mathbb{Z}$ is isomorphic to the circle group
W = $\{e^{i\theta} \in \mathbb{C} \mid \theta \in \mathbb{R}\}$.

Application of Morphism Theorem

Solution

The set W= $\{e^{i\theta} \in \mathbb{C} \mid \theta \in \mathbb{R}\}$ consists of points on the circle of complex numbers of unit modulus, and forms a group under multiplication.
Define the function $f : \mathbb{R} \to W$ by $f(x) = e^{2\pi ix}$.
This is a morphism from $(\mathbb{R},+)$ to $(W, \cdot)$ because
$f(x + y) = e^{2\pi i(x+y)}$
$= e^{2\pi ix} \cdot e^{2\pi iy}$
$= f(x) \cdot f(y)$.

Application of Morphism Theorem

The morphism $f : \mathbb{R} \to W$ is clearly surjective, and its kernel is
$\{x \in \mathbb{R} \mid e^{2\pi ix} = 1\} = \mathbb{Z}$.
Therefore, the morphism theorem implies that
$\mathbb{R}/\mathbb{Z} \cong W$.

Group Theory

Normality of Kernel of a Homomorphism

Normality of Kernel of a Homomorphism

Right Cosets

Let (G, ·) be a group with subgroup H. For a, b ∈ G, we say that a is ***congruent to b modulo H***, and write **a ≡ b mod H** if and only if $ab^{-1} \in H$.

Normality of Kernel of a Homomorphism

Proposition

The relation a ≡ b mod H is an equivalence relation on G.

The equivalence class containing a can be written in the form Ha = {ha|h ∈ H}, and it is called a right coset of H in G. The element a is called a representative of the coset Ha.

Normality of Kernel of a Homomorphism

Theorem

Let φ be a homomorphism function from group

(G, *) to group (G',.). Then, (Kerφ,*) is a normal subgroup of (G,*).

Normality of Kernel of a Homomorphism

Proof

i) Kerφ is a subgroup of G

$\forall a,b \in Ker\varphi$, $\varphi(a)=e_{G'}$, $\varphi(b)=e_{G'}$.

Then, $\varphi(a*b)=\varphi(a)\varphi(b)=e_{G'}$.

Therefore, $a*b \in Ker\varphi$.

Inverse element:

$\forall a \in Ker\varphi$, $\varphi(a)=e_{G'}$.

Then, $\varphi(a^{-1})=\varphi(a)^{-1}=e_{G'}$. Therefore, $a^{-1} \in Ker\varphi$.

Normality of Kernel of a Homomorphism

ii) $\forall g \in G, a \in Ker\varphi$, $\varphi(a)=e_{G'}$.

Then,

$\varphi(g^{-1}*a*g)$

$= \varphi(g^{-1})\,\varphi(a)\,\varphi(g)$

$= \varphi(g)^{-1}\,e_{G'}\,\varphi(g)$

$= e_{G'}$

Therefore,

$g^{-1}*a*g \in Ker\varphi$.

Group Theory

Example of Normal Group

Example of Normal Group

Definition

A subgroup H of a group is a normal subgroup if $gH=Hg$ for $\forall g\in G$.

Example of Normal Group

Example

- Any subgroups of Abelian group are normal subgroups
- S_3={(1),(1,2,3), (1,3,2), (2,3), (1,3), (1,2)}.
- H_1={(1), (2,3)}; H_2={(1), (1,3)}; H_3={(1), (1,2)};
- (1,3)H_1={(1,3),(1,2)} H_1(1,3)={(1,3),(1,2)}
- (1,2,3)H_1={(1,2,3),(1,2)} H_1(1,2,3)={(1,2,3),(1,3)}

Example of Normal Group

- H_4={(1), (1,2,3), (1,3,2)} are subgroups of S_3.
- H_4 is a normal subgroup.

Example of Normal Group

(1)Hg=gH, it does not imply hg=gh.

(2) If Hg=gH, then there exists $h'\in H$ such that hg=gh' for $\forall h\in H$.

Example of Normal Group

- Let H be a subgroup of a group G. When is
  (a H) (b H) = a b H?
- This is true for abelian groups, but not always when G is nonabelian.
- Consider S_3: Let H = $\{\rho_0, \mu_1\}$. The left cosets are
  $\{\rho_0, \mu_1\}, \{\rho_1, \mu_3\}, \{\rho_2, \mu_2\}$.

  If we multiply the first two together, then

  $$\{\rho_0, \mu_1\}, \{\rho_1, \mu_3\} = \{\rho_0 \rho_1, \rho_0 \mu_3, \mu_1 \rho_1, \mu_1 \mu_3\}$$
  $$= \{\rho_1, \mu_3, \mu_2, \rho_2\}$$

  This has four distinct elements, not two!

Group Theory

Factor Group

Factor Group

Definition

Let (H,*) be a normal subgroup of the group (G,*). (G/H,⊗) is called quotient group, where the operation ⊗ is defined on G/H by

$Hg_1 \otimes Hg_2 = H(g_1 * g_2)$.

If G is a finite group, then G/H is also a finite group, and |G/H|=|G|/|H|.

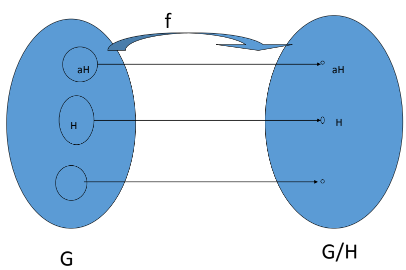
685

Factor Group

- The product of two sets is define as follow
  SS' = {xx'|x∈S and x'∈S}
- {aH|a∈G, H is normal} is a group, denote by G/H and called it factor groups of G.
- A mapping f: G→G/H is a homomorphism, and call it canonical homomorphism.

686

Factor Group



687

Factor Group

Consider S_3: Let H = $\{\rho_0, \rho_1, \rho_2\}$. The left cosets are

$\{\rho_0, \rho_1, \rho_2\}, \{\mu_1, \mu_2, \mu_3\}$

If we multiply the first two together, then

$\{\rho_0, \rho_1, \rho_2\}\{\mu_1, \mu_2, \mu_3\} = \{\rho_0\mu_1, \rho_0\mu_2, \rho_0\mu_3, \rho_1\mu_1, \rho_1\mu_2, \rho_1\mu_3, \rho_2\mu_1, \rho_2\mu_2, \rho_2\mu_3\} = \{\mu_1, \mu_2, \mu_3, \mu_3, \mu_1, \mu_2, \mu_2, \mu_3, \mu_1\} = \{\mu_1, \mu_2, \mu_3\}$

This is one of the cosets. Likewise,

$\{\rho_0, \rho_1, \rho_2\}\{\rho_0, \rho_1, \rho_2\} = \{\rho_0, \rho_1, \rho_2\}$

$\{\mu_1, \mu_2, \mu_3\}\{\rho_0, \rho_1, \rho_2\} = \{\mu_1, \mu_2, \mu_3\}$

$\{\mu_1, \mu_2, \mu_3\}\{\mu_1, \mu_2, \mu_3\} = \{\rho_0, \rho_1, \rho_2\}$

Note that the cosets of $\{\rho_0, \rho_1, \rho_2\}$ with this binary operation form a group isomorphic to $\mathbb{Z}_2$.

688

Factor Group

Note that there is a natural map from S_3 to $\{\{\rho_0, \rho_1, \rho_2\}, \{\mu_1, \mu_2, \mu_3\}\}$ that takes any element to the coset that contains it. This gives a homomorphism called the cannonical homomorphism.

689

Group Theory

Coset Multiplication and Normality

690

Coset Multiplication and Normality

Theorem
Let H be a subgroup of a group G.
Then H is normal if and only if
(a H)(b H) = (a b) H,
for all a, b in G

Coset Multiplication and Normality

Proof
Suppose
(a H)(b H) = (a b) H,
for all a, b in G.
We show that aH = H a,
for all a in H.
We do this by showing:
a H $\subseteq$ H a and Ha$\subseteq$ aH,
for all a in G.

Coset Multiplication and Normality

a H $\subseteq$ H a: First observe that aHa^{-1}$\subseteq$ (aH)(a^{-1}H) =(aa^{-1})H = H.
Let x be in a H. Then x = a h, for some h in H. Then x a^{-1} = a h a^{-1}, which is in = a H a^{-1} , thus in H. Thus x a^{-1} is in H. Thus x is in H a.
H a $\subseteq$ a H: H a $\subseteq$ H a H = (e H)(a H) = (e a) H = a H.
This establishes normality.

Coset Multiplication and Normality

For the converse, assume H is normal.
(a H)(b H) $\subseteq$ (a b) H: For a, b in G, x in (a H)(b H) implies that x = a h_1 b h_2, for some h_1 and h_2 in H.
But h_1 b is in H b, thus in b H. Thus h_1 b = b h_3 for some h_3 in H. Thus x = a b h_3 h_2 is in a b H.
(a b) H $\subseteq$ (a H)(b H): x in (a b) H ⇒ x = a e b h, for some h in H.
Thus x is in (a H) (b H).

Group Theory

Examples on Kernel of a Homomorphism

Examples on Kernel of a Homomorphism

Let h: G→G' be a homomorphism and let e′ be the identity element of G'. Now {e'} is a subgroup of G', so h^{-1}[{e'}] is a subgroup K of G. This subgroup is critical to the study of homomorphisms.

Examples on Kernel of a Homomorphism

Definition

Let h: G→G' be a homomorphism of groups. The subgroup $h^{-1}[\{e'\}]=\{x\in G \mid h(x)=e'\}$ is the **kernel** of h, denoted by Ker(h).

697

Examples on Kernel of a Homomorphism

Example

Let $\mathbb{R}^n$ be the additive group of column vectors with n real-number components. (This group is of course isomorphic to the direct product of $\mathbb{R}$ under addition with itself for n factors.) Let A be an m x n matrix of real numbers. Let $\phi: \mathbb{R}^n \to \mathbb{R}^m$ be defined by $\phi(v)=Av$ for each column vector $v\in\mathbb{R}^n$.

698

Examples on Kernel of a Homomorphism

Example

Then ϕ is a homomorphism, since v, $w\in\mathbb{R}^n$, matrix algebra shows that $\phi(v+w)=A(v+w)$

$=Av+Aw=\phi(v)+\phi(w)$

In linear algebra, such a map computed by multiplying a column vector on the left by a matrix A is known as a **linear transformation.**

699

Examples on Kernel of a Homomorphism

Ker(h) is called the null space of A. It consists of all $v \in \mathbb{R}^n$ such that

Av = 0, the zero vector.

700

Group Theory

Examples on Kernel of a Homomorphism

701

Examples on Kernel of a Homomorphism

Example

Let GL(n, $\mathbb{R}$) be the multiplicative group of all invertible n x n matrices. Recall that a matrix A is invertible if and only if its determinant, det(A), is nonzero.

702

Examples on Kernel of a Homomorphism

Recall also that for matrices A, B ∈GL(n, ℝ) we have det(AB)=det(A)det(B). This means that det is a homomorphism mapping GL(n, ℝ) into the multiplicative group ℝ* of nonzero real numbers.

Ker(det)

= {A∈ GL(n, ℝ)|det(A)=1}.

703

Examples on Kernel of a Homomorphism

Homomorphisms of a group G into itself are often useful for studying the structure of G. Our next example gives a nontrivial homomorphism of a group into itself.

704

Examples on Kernel of a Homomorphism

Example

Let r∈ℤ and let ϕ_r: ℤ→ℤ be defined by ϕ_r(n)=rn for all n∈ℤ. For all m, n∈ℤ, we have ϕ_r(m+n)=*r(m + n)* =rm+rn=ϕ_r(m)+ϕ_r(n) so ϕ_r is a homomorphism.

705

Examples on Kernel of a Homomorphism

Note that ϕ_0 is the trivial homomorphism, ϕ_1 is the identity map, and ϕ_{-1} maps ℤ onto ℤ. For all other r in ℤ, the map ϕ_r is not onto ℤ.

Ker(ϕ_0)= ℤ
Ker(ϕ_r)= {0} for r≠0

706

Group Theory

Examples on Kernel of a Homomorphism

707

Examples on Kernel of a Homomorphism

Example (Reduction Modulo n)

Let y be the natural map of ℤ into $\mathbb{Z}_n$ given by y(m) = r, where r is the remainder given by the division algorithm when m is divided by n. Show that *y* is a homomorphism. Find Ker(y).

708

Examples on Kernel of a Homomorphism

Solution

We need to show that y(s+t)=y(s)+y(t) for s, t ∈ $\mathbb{Z}$. Using the division algorithm, we let

$s=q_1n+r_1$ (1) and

$t=q_2n+r_2$ (2) where $0\le r_i<n$ for i=1, 2.

If $r_1+r_2=q_3n+r_3$ (3) for $0\le r_3<n$ then adding Eqs. (1) and (2) we see that $s + t = (q_1 + q_2 + q_3)n + r_3$, so that $y(s+t)=r_3$. From Eqs. (1) and (2) we see that

$y(s) =r_1$ and $y(t)=r_2$. Equation (3) shows that

the sum r_1+r_2 in $\mathbb{Z}_n$ is equal to r_3 also.

709

Examples on Kernel of a Homomorphism

Consequently

y(s+t)=y(s)+y(t),

so we do indeed have a homomorphism.

Ker(y)=n$\mathbb{Z}$

710

Group Theory

Kernel of a Homomorphism

711

Kernel of a Homomorphism

Theorem

Let h be a homomorphism from a group G into a group G'. Let K be the kernel of h. Then

a K = {x in G | h(x) = h(a)}

= h^{-1}[{h(a)}] and also

K a = {x in G | h(x) = h(a)}

= h^{-1}[{h(a)}]

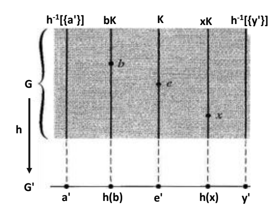
712

Kernel of a Homomorphism

Let K=Ker(h) for a homomorphism h:G→G'. We think of h as "collapsing" K down onto e'. Above Theorem shows that for g ∈ G, the cosets gK and Kg are the same, and are collapsed onto the single element h(g) by h. That is h^{-1}[{h(g)}]=gK=Kg. We have attempted to symbolize this collapsing in Fig. below, where the shaded rectangle represents G, the solid vertical line segments represent the cosets of K= Ker(h), and the horizontal line at the bottom represents G'.

713

Kernel of a Homomorphism



Cosets of K collapsed by h

714

Kernel of a Homomorphism

We view h as projecting the elements of G, which are in the shaded rectangle, straight down onto elements of G', which are on the horizontal line segment at the bottom. Notice the downward arrow labeled h at the left, starting at G and ending at G'. Elements of K=Ker(h) thus lie on the solid vertical line segment in the shaded box lying over e', as labeled at the top of the figure.

Group Theory

Kernel of a Homomorphism

Kernel of a Homomorphism

Example

We have $|z_1z_2|=|z_1||z_2|$ for complex numbers z_1 and z_2. This means that the absolute value function $|\ |$ is a homomorphism of the group $\mathbb{C}^*$ of nonzero complex numbers under multiplication onto the group $\mathbb{R}^+$ of positive real numbers under multiplication.

Kernel of a Homomorphism

Since {1} is a subgroup of $\mathbb{R}^+$, the complex numbers of magnitude 1 form a subgroup U of $\mathbb{C}^*$. Recall that the complex numbers can be viewed as filling the coordinate plane, and that the magnitude of a complex number is its distance from the origin. Consequently, the cosets of U are circles with center at the origin. Each circle is collapsed by this homomorphism onto its point of intersection with the positive real axis.

Group Theory

Kernel of a Homomorphism

Kernel of a Homomorphism

Theorem

Let h be a homomorphism from a group G into a group G’. Let K be the kernel of h. Then

a K = {x in G | h(x) = h(a)} = h^{-1}[{h(a)}] and also

K a = {x in G | h(x) = h(a)} = h^{-1}[{h(a)}]

Kernel of a Homomorphism

Above theorem shows that the kernel of a group homomorphism h:G→G' is a subgroup K of G whose left and right cosets coincide, so that gK=Kg for all g ∈ G. When left and right cosets coincide, we can form a coset group G/K. Furthermore, we have seen that K then appears as the kernel of a homomorphism of G onto this coset group in a very natural way. Such subgroups K whose left and right cosets coincide are very useful in studying normal group.

721

Kernel of a Homomorphism

Example

Let D be the additive group of all differentiable functions mapping ℝ into ℝ, and let F be the additive group of all functions mapping ℝ into ℝ Then differentiation gives us a map ϕ: D→F, where ϕ(f)=f' for f∈F. We easily see that ϕ is a homomorphism, for ϕ(f+g)=(f+g)'=f'+g'=ϕ(f)+ϕ(g); the derivative of a sum is the sum of the derivatives.

722

Kernel of a Homomorphism

Now Ker(ϕ) consists of all functions f such that f'=0. Thus Ker(ϕ) consists of all constant functions, which form a subgroup C of F. Let us find all functions in G mapped into x^2 by ϕ, that is, all functions whose derivative is x^2. Now we know that $x^3/3$ is one such function. By previous theorem, all such functions form the coset $x^3/3+C$.

723

Group Theory

Examples of Group Homomorphisms

724

Examples of Group Homomorphisms

Example (Evaluation Homomorphism)

Let F be the additive group of all functions mapping ℝ into ℝ, let ℝ be the additive group of real numbers, and let c be any real number. Let

ϕ: F→ℝ be the **evaluation homomorphism** defined by $\phi_c(f)= f(c)$ for f∈F. Recall that, by definition, the sum of two functions f and g is the function f + g whose value at x is f (x) + g(x). Thus we have

$\phi_c(f+g)=(f+g)(c)=f(c)+g(c)=\phi_c(f)+\phi_c(g)$, so we have a homomorphism.

725

Examples of Group Homomorphisms

Composition of group homomorphisms is again a group homomorphism. That is, if

ϕ: G→G' and *y*: G'→G" are both group homomorphisms then their composition

(y∘ϕ): G→G", where (y∘ϕ)(g) = y(ϕ(g)) for g ∈ G, is also a homomorphism.

726

Group Theory

Examples of Group Homomorphisms

Examples of Group Homomorphisms

Example

Let $G=G_1 \times \cdots \times G_i \times \cdots \times G_n$ be a direct product of groups. The **projection map** $\pi_i: G \to G_i$ where $\pi_i(g_1, \cdots, g_i, \cdots, g_n) = g_i$ is a homomorphism for each $i=1, \cdots, n$.

This follows immediately from the fact that the binary operation of G coincides in the ith component with the binary operation in G_i.

Examples of Group Homomorphisms

Example

Let F be the additive group of continuous functions with domain [0, 1] and let $\mathbb{R}$ be the additive group of real numbers. The map $\sigma: F \to \mathbb{R}$ defined by $\sigma(f)=\int_0^1 f(x)dx$ for $f \in F$ is a homomorphism, for $\sigma(f+g)=\int_0^1 (f+g)(x)dx=\int_0^1 [f(x)+g(x)]dx= \int_0^1 f(x)dx+\int_0^1 g(x)dx=\sigma(f)+\sigma(g)$ for all $f, g \in F$.

Examples of Group Homomorphisms

Each of the homomorphisms in the preceding two examples is a many-to-one map. That is, different points of the domain of the map may be carried into the same point. Consider, for illustration, the homomorphism $\pi_1: \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_2$ We have

$\pi_1(0, 0)=\pi_1(0, 1)= \pi_1(0, 2)= \pi_1(0, 3)=0$, so four elements in $\mathbb{Z}_2 \times \mathbb{Z}_4$ are mapped into 0 in $\mathbb{Z}_2$ by π_1.

Group Theory

Factor Groups from Homomorphisms

Factor Groups from Homomorphisms

Let G be a group and let S be a set having the same cardinality as G. Then there is a one-to-one correspondence $\leftrightarrow$ between S and G. We can use $\leftrightarrow$ to define a binary operation on S, making S into a group isomorphic to G. Naively, we simply use the correspondence to rename each element of G by the name of its corresponding (under $\leftrightarrow$) element in S. We can describe explicitly the computation of xy for $x, y \in S$ as follows:

if $x \leftrightarrow g_1$ and $y \leftrightarrow g_2$ and $z \leftrightarrow g_1g_2$, then $xy=z$ (1)

Factor Groups from Homomorphisms

The direction → of the one-to-one correspondence $s \leftrightarrow g$ between $s \in S$ and $g \in G$ gives us a one-to-one function μ mapping S onto G. The direction ← of ↔ gives us the inverse function μ^{-1}. Expressed in terms of μ, the computation (1) of xy for x, y ∈ S becomes

if $\mu(x)=g_1$ and $\mu(y)=g_2$ and $\mu(z)=g_1g_2$, then xy=z (2)

The map μ: S→G now becomes an isomorphism mapping the group S onto the group G. Notice that from (2), we obtain $\mu(xy)=\mu(z)=g_1g_2=\mu(x)\mu(y)$, the required homomorphism property.

Group Theory

Factor Groups from Homomorphisms

Factor Groups from Homomorphisms

Let G and G' be groups, let h: G→G' be a homomorphism, and let K=Ker(h). The previous theorem shows that for a∈G, we have $h^{-1}[\{h(a)\}]=aK=Ka$. We have a one-to-one correspondence aK ↔h(a) between cosets of K in G and elements of the subgroup h[G] of G'.

Factor Groups from Homomorphisms

Remember that if x∈aK, so that x=ak for some k∈*K*, then h(x)=h(ak)=h(a)h(k)=h(a)e'

=h(a), so the computation of the element of h[G]

corresponding to the coset aK=xK is the same whether we compute it as h(a) or as h(x). Let us denote the set of all cosets of K by G/K. (We read G/K as "G over K" or as "G modulo K" or as "G mod K," but never as "G divided by K.")

Factor Groups from Homomorphisms

We started with a homomorphism h: G→G' having kernel K, and we finished with the set G/K of cosets in one-to-one correspondence with the elements of the group h[G]. In our work above that, we had a set S with elements in one-to-one correspondence with a those of a group G, and we made S into a group isomorphic to G with an isomorphism μ.

Factor Groups from Homomorphisms

Replacing S by G / H and replacing G by h[G] in that construction, we can consider G/K to be a group isomorphic to h[G] with that isomorphism μ. In terms of G/K and h[G], the computation (2) of the product (xK)(yK) for xK, yK ∈ G/K becomes if

$\mu(xK)=h(x)$ and $\mu(yK)=h(y)$ and $\mu(zK)=h(x)h(y)$, then (xK)(yK)=zK. (3)

Factor Groups from Homomorphisms

But because h is a homomorphism, we can easily find $z \in G$ such that $\mu(zK)=h(x)h(y)$; namely, we take $z=xy$ in G, and find that $\mu(zK)=\mu(xyK)=h(xy)=h(x)h(y)$.

This shows that the product $(xK)(yK)$ of two cosets is the coset $(xy)K$ that contains the product xy of x and y in G. While this computation of $(xK)(yK)$ may seem to depend on our choices x from xK and y from yK, our work above shows it does not. We demonstrate it again here because it is such an important point. If $k_1, k_2 \in K$ so that xk_1 is an element of xK and yk_2 is an element of yK, then there exists $h_3 \in K$ such that $k_1y = yk_3$ because $Ky = yK$ by previous Theorem.

739

Factor Groups from Homomorphisms

Thus we have

$(xk_1)(yk_2)=x(k_1y)k_2=x(yk_3)k_2=(xy)(k_3k_2) \in (xy)K$,

so we obtain the same coset. Computation of the product of two cosets is accomplished by choosing an element from each coset and taking, as product of the cosets, the coset that contains the product in G of the choices. Any time we define something (like a product) in terms of choices, it is important to show that it is well defined, which means that it is independent of the choices made.

740

Group Theory

Factor Groups from Homomorphisms

741

Factor Groups from Homomorphisms

Theorem

Let $h: G \to G'$ be a group homomorphism with kernel K. Then the cosets of K form a factor group, G/K. where $(aK)(bK)=(ab)K$. Also, the map μ: $G/H \to h[G]$

defined by $\mu(aK)=h(a)$ is an isomorphism. Both coset multiplication and μ are well defined, independent of the choices a and b from the cosets.

742

Factor Groups from Homomorphisms

Example

Consider the map $\gamma: \mathbb{Z} \to \mathbb{Z}_n$, where $\gamma(m)$ is the remainder when m is divided by n in accordance with the division algorithm. We know that γ is a homomorphism. Of course, $Ker(\gamma) = n\mathbb{Z}$. By above Theorem, we see that the factor group $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$. The cosets of $n\mathbb{Z}$ are the residue classes modulo n.

743

Factor Groups from Homomorphisms

For example, taking n = 5, we see the cosets of $5\mathbb{Z}$ are

$5\mathbb{Z}=\{\ldots, -10, -5, 0, 5, 10,\ldots\}$,

$1+5\mathbb{Z} = \{\ldots, -9, -4, 1, 6, 11,\ldots\}$,

$2+5\mathbb{Z} = \{\ldots, -8, -3, 2, 7, 12,\ldots\}$,

$3+5\mathbb{Z} = \{\ldots, -7, -2, 3, 8, 13,\ldots\}$

$4+5\mathbb{Z} = \{\ldots, -6, -1, 4, 9, 14,\ldots\}$.

Note that the isomorphism $\mu: \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}_5$ of previous Theorem assigns to each coset of $5\mathbb{Z}$ its smallest nonnegative element. That is, $\mu(5\mathbb{Z})=0$, $\mu(1+5Z) = 1$, etc.

744

Group Theory

Factor Groups from Homomorphisms

Factor Groups from Homomorphisms

It is very important that we learn how to compute in a factor group. We can multiply (add) two cosets by choosing any two representative elements, multiplying (adding) them and finding the coset in which the resulting product (sum) lies.

Factor Groups from Homomorphisms

Example

Consider the factor group $\mathbb{Z}/5\mathbb{Z}$ with the cosets shown in precious example. We can add $(2+5\mathbb{Z})+(4+5\mathbb{Z})$ by choosing 2 and 4, finding 2+4=6, and noticing that 6 is in the coset $1+5\mathbb{Z}$. We could equally well add these two cosets by choosing 27 in $2+5\mathbb{Z}$ and -16 in $4+5\mathbb{Z}$; the sum 27+(-16)=11 is also in the coset $1+5\mathbb{Z}$.

Factor Groups from Homomorphisms

The factor groups $\mathbb{Z}/n\mathbb{Z}$ in the preceding example are classics. Recall that we refer to the cosets of $n\mathbb{Z}$ as residue classes modulo n. Two integers in the same coset are congruent modulo n. This terminology is carried over to other factor groups. A factor group G/H is often called the factor group of G modulo H. Elements in the same coset of H are often said to be congruent modulo H. By abuse of notation, we may sometimes write $\mathbb{Z}/n\mathbb{Z}=\mathbb{Z}_n$ and think of $\mathbb{Z}_n$ as the additive group of residue classes of $\mathbb{Z}$ modulo n.

Group Theory

Factor Groups from Normal Subgroups

Factor Groups from Normal Subgroups

So far, we have obtained factor groups only from homomorphisms. Let G be a group and let H be a subgroup of G. Now H has both left cosets and right cosets, and in general, a left coset aH need not be the same set as the right coset Ha.

Factor Groups from Normal Subgroups

Suppose we try to define a binary operation on left cosets by defining (aH)(bH)=(ab)H as in the statement of previous theorem. The above equation attempts to define left coset multiplication by choosing representatives a and b from the cosets. The above equation is meaningless unless it gives a well-defined operation, independent of the representative elements a and b chosen from the cosets. In the following theorem, we have proved that the above equation gives a well-defined binary operation if and only if H is a normal subgroup of G.

751

Factor Groups from Normal Subgroups

Theorem

Let H be a subgroup of a group G.

Then H is normal if and only if

(a H)(b H) = (a b) H,

for all a, b in G

752

Factor Groups from Normal Subgroups

Above theorem shows that if left and right cosets of H coincide, then the equation

(aH)(bH)=(ab)H, for all a, b in G

gives a well-defined binary operation on cosets.

753

Factor Groups from Normal Subgroups

Theorem

If N is a normal subgroup of $(G, \cdot)$, the set of cosets $G/N = \{Ng \mid g \in G\}$ forms a group $(G/N, \cdot)$, where the operation is defined by $(Ng_1)\cdot(Ng_2)=N(g_1\cdot g_2)$.

754

Factor Groups from Normal Subgroups

Example

Since $\mathbb{Z}$ is an abelian group, $n\mathbb{Z}$ is a normal subgroup. Above theorem allows us to construct the factor group $\mathbb{Z}/n\mathbb{Z}$ with no reference to a homomorphism. As we already observed, $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$.

755

Group Theory

Factor Groups from Normal Subgroups

756

Factor Groups from Normal Subgroups

Example

Consider the abelian group $\mathbb{R}$ under addition, and let $c \in \mathbb{R}^+$. The cyclic subgroup <c> of $\mathbb{R}$ contains as elements

$\cdots$ -3c, -2c, -c, 0, *c*, 2c, 3c,$\cdots$.

Factor Groups from Normal Subgroups

Every coset of <c> contains just one element of x such that $0 \leq x < c$. If we choose these elements as representatives of the cosets when computing in $\mathbb{R}$/ <c>, we find that we are computing their sum modulo c in $\mathbb{R}_c$. For example, if c = 5.37, then the sum of the cosets 4.65+<5.37> and 3.42+<5.37> is the coset 8.07+<5.37>, which contains 8.07-5.37 = 2.7, which is $4.65+_{5.37}3.42$.

Factor Groups from Normal Subgroups

Working with these coset elements x where $0 \leq x < c$, we thus see that the group $\mathbb{R}_c$ is isomorphic to $\mathbb{R}$ / <c> under an isomorphism μ where μ(x) =x+<c> for all $x \in \mathbb{R}_c$. Of course, $\mathbb{R}$ / <c> is then also isomorphic to the circle group U of complex numbers of magnitude 1 under multiplication.

Group Theory

Kernel of an Injective Homomorphism

Kernel of an Injective Homomorphism

Theorem

A homomorphism $h: G \to G'$ is injective if and only if Ker h={e}.

Kernel of an Injective Homomorphism

Proof

Suppose h is injective,

and let $x \in$ Ker h.

Then h(x)=e'=h(e).

Hence x=e.

Kernel of an Injective Homomorphism

Conversely, suppose Ker h={e}.
Then h(x)=h(y)
$\Rightarrow h(xy^{-1})=h(x)h(y^{-1})$
$=h(x)h(y)^{-1}=e'$
$\Rightarrow xy^{-1}\in \text{Ker } h$
$\Rightarrow xy^{-1}=e$
$\Rightarrow x=y.$
Hence, h is injective.

763

Group Theory

Factor Groups from Normal Subgroups

764

Factor Groups from Normal Subgroups

Theorem

Let K be a normal subgroup of G.

Then y: G→G/K given by y(g)=gK is a homomorphism with kernel K.

765

Factor Groups from Normal Subgroups

Proof

Let $g_1, g_2 \in G$. Then
$y(g_1g_2)=(g_1g_2)K$
$=(g_1K)(g_2K)=y(g_1)y(g_2)$,
so y is a homomorphism.
Since $g_1K= K$ if and only if
$g_1\in K$, we see that the kernel of y is indeed K.

766

Factor Groups from Normal Subgroups

We have proved that if h:G→G' is a homomorphism with kernel K, then μ:G/K→h[G] where μ(gK) = h(g) is an isomorphism.

Above theorem shows that y:G→G/K defined by y(g)= gK is a homomorphism.

767

Factor Groups from Normal Subgroups

$$\begin{tikzcd} G \arrow[rr, "h"] \arrow[dr, "y"'] & & h[G] \\ & G/K \arrow[ur, "\mu"'] & \end{tikzcd}$$

We show these groups and maps in the figure. We see that the homomorphism h can be factored, h = μy,

where y is a homomorphism and μ is an isomorphism of G/K with h[G].

768

Group Theory

Example on Morphism Theorem of Groups

Example on Morphism Theorem of Groups

Theorem

Let K be the kernel of the group morphism

h :G → G'. Then G/K is isomorphic to the image of h, h[G], and the isomorphism

μ: G/K → Im h

is defined by

$\mu(Kg) = h[g]$.

Example on Morphism Theorem of Groups

Example

Classify the group

$(\mathbb{Z}_4 x\mathbb{Z}_2) /(\{0\}x\ \mathbb{Z}_2)$ according to the fundamental theorem of finitely generated abelian groups.

Example on Morphism Theorem of Groups

Solution

The projection map

π_1: $\mathbb{Z}_4 x\mathbb{Z}_2 \rightarrow \mathbb{Z}_4$ given by

$\pi_1(x,y) = x$ is a homomorphism of $\mathbb{Z}_4 x\mathbb{Z}_2$ onto $\mathbb{Z}_4$ with kernel $\{0\}x\mathbb{Z}_2$. By fundamental theorem of homomorphism, we know that the given factor group is isomorphic to $\mathbb{Z}_4$.

Example on Morphism Theorem of Groups

The projection map

π_1: $\mathbb{Z}_4 x\mathbb{Z}_2 \rightarrow \mathbb{Z}_4$ given by

$\pi_1(x,y) = x$.

$K = \text{Ker } \pi_1 = \{0\}x\mathbb{Z}_2$

$=\{(0,0),(0,1)\}$.

$(1,0)+K=\{(1,0),(1,1)\}$

$(2,0)+K=\{(2,0),(2,1)\}$

$(3,0)+K=\{(3,0),(3,1)\}$

Group Theory

Normal Groups and Inner Automorphisms

Normal Groups and Inner Automorphisms

We derive some alternative characterizations of normal subgroups, which often provide us with an easier way to check normality than finding both the left and the right coset decompositions.

775

Normal Groups and Inner Automorphisms

Theorem

The following are three equivalent conditions for a subgroup H of a group G to be a normal subgroup of G.

1. $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.

2. $gHg^{-1} = H$ for all $g \in G$.

3. $gH = Hg$ for all $g \in G$.

776

Normal Groups and Inner Automorphisms

Condition (2) of above Theorem is often taken as the definition of a normal subgroup H of a group G.

777

Normal Groups and Inner Automorphisms

Proof

Suppose that $gH = Hg$ for all $g \in G$. Then $gh = h_1 g$, so $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$.

Then $gHg^{-1} = \{ghg^{-1} \mid h \in H\} \subseteq H$ for all $g \in G$.

We claim that actually $gHg^{-1} = H$. We must show that $H \subseteq gHg^{-1}$ for all $g \in G$. Let $h \in H$. Replacing g by g^{-1} in the relation $ghg^{-1} \in H$, we obtain

$g^{-1}h(g^{-1})^{-1} = g^{-1}hg = h_1$ where $h_1 \in H$.

Consequently, $gHg^{-1} = H$ for all $g \in G$.

778

Normal Groups and Inner Automorphisms

Conversely, if $gHg^{-1} = H$ for all $g \in G$, then $ghg^{-1} = h_1$ so

$gh = h_1 g \in Hg$, and $gH \subseteq Hg$. But also, $g^{-1}Hg = H$ giving

$g^{-1}hg = h_2$, so that $hg = gh_2$ and $Hg \subseteq gH$.

779

Group Theory

Normal Groups and Inner Automorphisms

780

Normal Groups and Inner Automorphisms

Example

Every subgroup H of an abelian group G is normal.

We need only note that $gh = hg$ for all $h \in H$ and all $g \in G$, so, of course, $ghg^{-1} = h \in H$ for all $g \in G$ and all $h \in H$.

Normal Groups and Inner Automorphisms

Example

The map $i_g: G \rightarrow G$ defined by $i_g(x) = gxg^{-1}$ is a homomorphism of G into itself.

$i_g(xy) = gxyg^{-1}$

$= (gxg^{-1})(gyg^{-1})$

$= i_g(x)i_g(y)$

Normal Groups and Inner Automorphisms

We see that

$i_g(x) = i_g(y)$

$\Rightarrow gxg^{-1} = gyg^{-1}$

$\Rightarrow x = y$,

so i_g is injective.

Since for any x in G

$i_g(g^{-1}xg) = g(g^{-1}xg)g^{-1} = x$,

we see that i_g is onto G, so it is an isomorphism of G with itself.

Group Theory

Inner Automorphisms

Inner Automorphisms

Definition

An isomorphism $\phi: G \rightarrow G$ of a group G with itself is an **automorphism** of G. The automorphism $i_g: G \rightarrow G$, where $i_g(x) = gxg^{-1}$ for all $x \in G$, is the **inner automorphism of** G by g, denoted by Inn (G). Performing i_g on x is called **conjugation of** x by g.

Inner Automorphisms

Theorem

The following are three equivalent conditions for a subgroup H of a group G to be a normal subgroup of G.

1. $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.

2. $gHg^{-1} = H$ for all $g \in G$. **3.** $gH = Hg$ for all $g \in G$.

The equivalence of conditions (2) and (3) shows that $gH = Hg$ for all $g \in G$ if and only if $i_g[H] = H$ for all $g \in G$, that is, if and only if H is **invariant** under all inner automorphisms of G.

Inner Automorphisms

It is important to realize that $i_g[H] = H$ is an equation in sets; we need not have $i_g(h) = h$ for all $h \in H$.

That is i_g may perform a nontrivial permutation of the set H.

We see that the normal subgroups of a group G are precisely those that are invariant under all inner automorphisms.

A subgroup K of G is a **conjugate subgroup** of H if $K = i_g[H]$ for some $g \in G$.

787

Group Theory

Inner Automorphisms

788

Inner Automorphisms

Lemma

The set of all inner automorphisms of G is a subgroup of Aut(G).

789

Inner Automorphisms

Proof

(1) Let $i_a, i_b \in$ Inn (G).

Then $i_a(i_b(x)) = a(i_b(x))a^{-1} = abxb^{-1}a^{-1}$

$= abx(ab)^{-1} = i_{ab} \in$ Inn (G).

Hence the conjugation by b composed by conjugation by a is conjugation by ab.

(2) The inverse of i_a is conjugation by $a' = a^{-1}$.

$i_a((i_{a'})(x)) = i_a(a'x(a')^{-1}) = aa'xa'^{-1}a^{-1} = aa'x(aa')^{-1} = x$.

Thus Inn (G) is a subgroup.

790

Group Theory

Example on Automorphism

791

Inner Automorphisms

Example

Prove that $\mathrm{Aut}(\mathbb{Z}_n) \cong U_n$.

792

Inner Automorphisms

Solution

An automorphism $\varphi:\mathbb{Z}_n\to\mathbb{Z}_n$ is determined by $\varphi(1)$ as for any integer k,

$\varphi(k)=\varphi(1+\ldots+1)=\varphi(1)+\ldots+\varphi(1)= k\varphi(1)$.

Since isomorphisms preserve order, $\varphi(1)$ must be a generator of $\mathbb{Z}_n$.

We have proved that the generators of $\mathbb{Z}_n$ are those integers $k \in \mathbb{Z}_n$ for which $\gcd(k, n) = 1$. But these k are precisely the elements of

$U_n=\{1, \omega,\ldots, \omega^{n-1} \mid \omega=e^{2\pi i/n}\}$.

Inner Automorphisms

In this way, each element a of U_n gives a distinct automorphism φ_a which is multiplication by a, and these are all the automorphisms of $\mathbb{Z}_n$.

Furthermore, μ: $\mathrm{Aut}(\mathbb{Z}_n)\to U_n$ given by $\mu(\varphi_a)=a$ is a group isomorphism.

- $\mu(\varphi_{ab})=ab=\mu(\varphi_a)\,\mu(\varphi_b)$
- $\mu(\varphi_a)=\mu(\varphi_b)\Rightarrow a=b$
- $\mu(\varphi_a)=a$

Group Theory

Theorem on Factor Group

Theorem on Factor Group

Theorem

A factor group of a cyclic group is cyclic.

Theorem on Factor Group

Proof

Let G be cyclic with generator a, and let N be a normal subgroup of G. We claim the coset aN generates G / N. We must compute all powers of aN. But this amounts to computing, in G, all powers of the representative a and all these powers give all elements in G. Hence the powers of aN certainly give all cosets of N and G / N is cyclic.

Group Theory

Example on Factor Group

Example on Factor Group

Example

Let us compute the factor group $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0, 2)\rangle$. Now (0, 2) generates the subgroup

$H=\{(0,0), (0, 2),(0,4)\}$

of $\mathbb{Z}_4 \times \mathbb{Z}_6$ of order 3.

799

Example on Factor Group

Here the first factor $\mathbb{Z}_4$ of $\mathbb{Z}_4 \times \mathbb{Z}_6$ is left alone. The $\mathbb{Z}_6$ factor, on the other hand, is essentially collapsed by a subgroup of order 3, giving a factor group in the second factor of order 2 that must be isomorphic to $\mathbb{Z}_2$. Thus $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0, 2)\rangle$ is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$.

800

Group Theory

Factor Group Computations

801

Factor Group Computations

Let N be a normal subgroup of G. In the factor group G / N, the subgroup N acts as identity element. We may regard N as being collapsed to a single element, either to 0 in additive notation or to e in multiplicative notation.

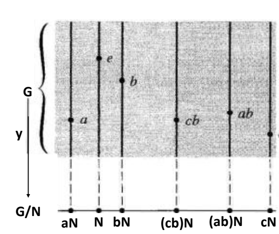
802

Factor Group Computations

This collapsing of N together with the algebraic structure of G require that other subsets of G, namely, the cosets of N, also collapse into a single element in the factor group. A visualization of this collapsing is provided by Figure.

803

Factor Group Computations



804

Factor Group Computations

Recall that γ: G→G/N defined by γ(a)=aN for a ∈ G is a homomorphism of G onto G / N. We can view the "line" G / N at the bottom of the figure as obtained by collapsing to a point each coset of N in another copy of G. Each point of G / N thus corresponds to a whole vertical line segment in the shaded portion, representing a coset of N in G. It is crucial to remember that multiplication of cosets in G / N can be computed by multiplying in G, using any representative elements of the cosets.

805

Group Theory

Factor Group Computations

806

Factor Group Computations

Additively, two elements of G will collapse into the same element of G/N if they differ by an element of N. Multiplicatively, a and b collapse together if ab^{-1} is in N. The degree of collapsing can vary from nonexistent to catastrophic. We illustrate the two extreme cases by examples.

807

Factor Group Computations

Example

The trivial subgroup

N = {0} of $\mathbb{Z}$ is, of course, a normal subgroup.

Compute $\mathbb{Z}$ /{0}.

808

Factor Group Computations

Solution

Since N={0} has only one element, every coset of N has only one element. That is, the cosets are of the form {m} for m ∈ $\mathbb{Z}$. There is no collapsing at all, and consequently, $\mathbb{Z}$ /{0} ≅ $\mathbb{Z}$. Each m ∈ $\mathbb{Z}$ is simply renamed {m} in $\mathbb{Z}$ /{0}.

809

Factor Group Computations

Example

Let n be a positive integer. The set

$n\mathbb{R} = \{nr \mid r \in \mathbb{R}\}$ is a subgroup of $\mathbb{R}$ under addition, and it is normal since $\mathbb{R}$ is abelian.

Compute $\mathbb{R}/n\mathbb{R}$.

810

Factor Group Computations

Solution

Actually $n\mathbb{R} = \mathbb{R}$, because each $x \in \mathbb{R}$ is of the form $n(x/n)$ and $x/n \in \mathbb{R}$. Thus $\mathbb{R}/n\mathbb{R}$ has only one element, the subgroup $n\mathbb{R}$. The factor group is a trivial group consisting only of the identity element.

811

Group Theory

Factor Group Computations

812

Factor Group Computations

As illustrated in above Examples for any group G, we have $G/\{e\} \cong G$ and $G/G \cong \{e\}$, where $\{e\}$ is the trivial group consisting only of the identity element e. These two extremes of factor groups are of little importance.

813

Factor Group Computations

We would like knowledge of a factor group G/N to give some information about the structure of G.

If $N=\{e\}$, the factor group has the same structure as G and we might as well have tried to study G directly.

814

Factor Group Computations

If N = G, the factor group has no significant structure to supply information about G.

815

Factor Group Computations

If G is a finite group and $N \neq \{e\}$ is a normal subgroup of G, then G/N is a smaller group than G, and consequently may have a more simple structure than G.

816

Factor Group Computations

The multiplication of cosets in G/N reflects the multiplication in G, since products of cosets can be computed by multiplying in G representative elements of the cosets.

817

Factor Group Computations

In next module, we give example showing that even when G/N has order 2, we may be able to deduce some useful results.

If G is a finite group and G/N has just two elements, then we must have $|G|=2|N|$.

818

Group Theory

Factor Group Computations

819

Factor Group Computations

Note that every subgroup H containing just half the elements of a finite group G must be a normal subgroup, since for each element a in G but not in H, both the left coset aH and the right coset Ha must consist of all elements in G that are not in H.

820

Factor Group Computations

Thus the left and right cosets of H coincide and H is a normal subgroup of G.

821

Factor Group Computations

Example

Because $|S_n| = 2|A_n|$, we see that A_n is a normal subgroup of S_n, and S_n/A_n has order 2.

Let σ be an odd permutation in S_n, so that

$S_n/A_n = \{A_n, \sigma A_n\}$.

822

Factor Group Computations

Renaming the element A_n "even" and the element σA_n "odd," the multiplication in S_n/A_n shown in Table becomes

(even)(even)=even, (even)(odd)=odd, (odd)(even)=odd, (odd)(odd)=even.

Thus the factor group reflects these multiplicative properties for all the permutations in S_n.

	A_n	σA_n
A_n	A_n	σA_n
σA_n	σA_n	A_n

823

Factor Group Computations

Above example illustrates that while knowing the product of two cosets in G/N does not tell us what the product of two elements of G is, it may tell us that the product in G of two types of elements is itself of a certain type.

824

Group Theory

Factor Group Computations

825

Factor Group Computations

The theorem of Lagrange states if H is a subgroup of a finite group G, then the order of H divides the order of G.

We show that it is false that if d divides the order of G, then there must exist a subgroup H of G having order d.

826

Factor Group Computations

Example

We show that A_4, which has order 12, contains no subgroup of order 6.

Suppose that H were a subgroup of A_4 having order 6.

As observed before in previous example, it would follow that H would be a normal subgroup of A_4.

827

Factor Group Computations

Then A_4/H would have only two elements, H and σH for some $\sigma \epsilon A_4$ not in H. Since in a group of order 2, the square of each element is the identity, we would have HH=H and $(\sigma H)(\sigma H)$=H. Now computation in a factor group can be achieved by computing with representatives in the original group. Thus, computing in A_4, we find that for each $\alpha \epsilon H$ we must have $\alpha^2 \epsilon H$ and for each $\beta \epsilon \sigma H$ we must have $\beta^2 \epsilon H$. That is, the square of every element in A_4 must be in H.

828

Factor Group Computations

But in A_4, we have

$(1, 2, 3) = (1, 3, 2)^2$ and $(1, 3, 2) = (1, 2, 3)^2$

so (1, 2, 3) and (1, 3, 2) are in H.

A similar computation shows that (1, 2, 4), (1, 4, 2), (1, 3, 4), (1, 4, 3), (2, 3, 4), and (2, 4, 3) are all in H.

This shows that there must be at least 8 elements in H, contradicting the fact that H was supposed to have order 6.

829

Group Theory

Factor Group Computations

830

Factor Group Computations

We now turn to several examples that compute factor groups. If the group we start with is finitely generated and abelian, then its factor group will be also. Computing such a factor group means classifying it according to the fundamental theorem of finitely generated abelian groups.

831

Factor Group Computations

Example

Let us compute the factor group $(\mathbb{Z}_4 x \mathbb{Z}_6)/\langle(0, 1)\rangle$. Here $\langle(0, 1)\rangle$ is the cyclic subgroup H of $\mathbb{Z}_4 x \mathbb{Z}_6$ generated by (0, 1). Thus

H = {(0, 0), (0, 1), (0. 2), (0, 3), (0, 4), (0, 5)}.

Since $\mathbb{Z}_4 x \mathbb{Z}_6$ has 24 elements and H has 6 elements, all cosets of H must have 6 elements, and $(\mathbb{Z}_4 x\ \mathbb{Z}_6)/H$ must have order 4. Since $\mathbb{Z}_4 x \mathbb{Z}_6$ is abelian, so is $(\mathbb{Z}_4 x\ \mathbb{Z}_6)/H$. Remember, we compute in a factor group by means of representatives from the original group.

832

Factor Group Computations

In additive notation, the cosets are

H=(0, 0)+H, (1,0)+H, (2, 0)+H, (3, 0)+H.

Since we can compute by choosing the representatives (0, 0), (1, 0), (2, 0), and (3, 0), it is clear that $(\mathbb{Z}_4 x \mathbb{Z}_6)/H$ is isomorphic to $\mathbb{Z}_4$. Note that this is what we would expect, since in a factor group modulo H, everything in H becomes the identity element; that is, we are essentially setting everything in H equal to zero. Thus the whole second factor $\mathbb{Z}_6$ of $\mathbb{Z}_4 x \mathbb{Z}_6$ is collapsed, leaving just the first factor $\mathbb{Z}_4$.

833

Group Theory

Factor Group Computations

834

Factor Group Computations

The last example is a special case of a general theorem that we now state and prove. We should acquire an intuitive feeling for this theorem in terms of collapsing one of the factors to the identity element.

Factor Group Computations

Theorem

Let G = H x K be the direct product of groups H and K. Then $\overline{H}$={(h, e)| h ϵ H} is a normal subgroup of G. Also G/$\overline{H}$ is isomorphic to K in a natural way. Similarly, G / $\overline{K}$ ≃ H in a natural way.

Factor Group Computations

Proof

Consider the map π_2: H x K → K given by

$\pi_2(h, k) = k$. The map π_2 is homomorphism since

$\pi_2(h_1h_2,k_1k_2)=k_1k_2= \pi_2(h_1,k_1)\ \pi_2(h_2,k_2)$.

Because Ker(π_2) = $\overline{H}$, we see that $\overline{H}$ is a normal subgroup of H x K. Because π_2 is onto K, Fundamental Theorem of Homomorphism tells us that (H x K)/ $\overline{H}$ ≃ K.

Group Theory

Factor Group Computations

Factor Group Computations

Example

Let us compute the factor group ($\mathbb{Z}_4$ x $\mathbb{Z}_6$)/ ⟨(2, 3)⟩. Be careful! There is a great temptation to say that we are setting the 2 of $\mathbb{Z}_4$ and the 3 of $\mathbb{Z}_6$ both equal to zero, so that $\mathbb{Z}_4$ is collapsed to a factor group isomorphic to $\mathbb{Z}_2$ and $\mathbb{Z}_6$ to one isomorphic to $\mathbb{Z}_3$, giving a total factor group isomorphic to $\mathbb{Z}_2$ x $\mathbb{Z}_3$. This is wrong!

Note that H = ⟨(2, 3)⟩ = {(0, 0), (2, 3)} is of order 2, so ($\mathbb{Z}_4$ x $\mathbb{Z}_6$)/⟨(2, 3)⟩ has order 12, not 6.

Factor Group Computations

Setting (2, 3) equal to zero does not make (2, 0) and (0, 3) equal to zero individually, so the factors do not collapse separately.

The possible abelian groups of order 12 are

$\mathbb{Z}_4$ x $\mathbb{Z}_3$ and $\mathbb{Z}_2$ x $\mathbb{Z}_2$ x $\mathbb{Z}_3$, and we must decide to which one our factor group is isomorphic. These two groups are most easily distinguished in that $\mathbb{Z}_4$ x $\mathbb{Z}_3$ has an element of order 4, and

$\mathbb{Z}_2$ x $\mathbb{Z}_2$ x $\mathbb{Z}_3$ does not.

Factor Group Computations

We claim that the coset (1, 0) + H is of order 4 in the factor group ($\mathbb{Z}_4 \times \mathbb{Z}_6$)/H.

To find the smallest power of a coset giving the identity in a factor group modulo H, we must, by choosing representatives, find the smallest power of a representative that is in the subgroup H. Now, 4(1,0)=(1, 0)+(1,0)+(1,0)+(1,0)=(0,0) is the first time that (1,0) added to itself gives an element of H. Thus $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(2, 3)\rangle$ has an element of order 4 and is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_3$ or $\mathbb{Z}_{12}$.

841

Group Theory

Factor Group Computations

842

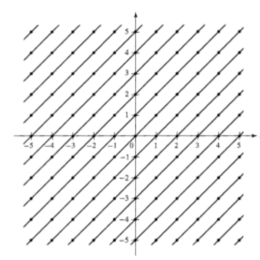
Factor Group Computations

Example

Let us compute (that is, classify as in Fundamental Theorem of Abelian Groups the group $(\mathbb{Z}\times\mathbb{Z})/\langle(1, 1)\rangle$. We may visualize $\mathbb{Z} \times \mathbb{Z}$ as the points in the plane with both coordinates integers, as indicated by the dots in Fig. below. The subgroup $\langle(1, 1)\rangle$ consists of those points that lie on the 45° line through the origin, indicated in the figure. The coset $(1, 0) + \langle(1, 1)\rangle$ consists of those dots on the 45° line through the point (1, 0), also shown in the figure.

843

Factor Group Computations



844

Factor Group Computations

Continuing, we see that each coset consists of those dots lying on one of the 45° lines in the figure. We may choose the representatives

⋯, (-3,0), (-2,0), (-1,0), (0,0), (1,0), (2,0), (3,0),⋯

of these cosets to compute in the factor group. Since these representatives correspond precisely to the points of $\mathbb{Z}$ on the x-axis, we see that the factor group $(\mathbb{Z} \times \mathbb{Z}) /\langle(1, 1)\rangle$ is isomorphic to $\mathbb{Z}$.

845

Simple Groups

One feature of a factor group is that it gives crude information about the structure of the whole group.

Of course, sometimes there may be no nontrivial proper normal subgroups.

846

Simple Groups

For example, Lagrange's Theorem shows that a group of prime order can have no nontrivial proper subgroups of any sort.

Simple Groups

Definition

A group is **simple** if it is nontrivial and has no proper nontrivial normal subgroups.

Simple Groups

Example

The cyclic group $G=\mathbb{Z}/5\mathbb{Z}$ of congruence classes modulo 5 is simple.

If H is a subgroup of this group, its order must be a divisor of the order of G which is 5.

Since 5 is prime, its only divisors are 1 and 5, so either H is G, or H is the trivial group.

Group Theory

Simple Groups

Simple Groups

Example

The cyclic group $G=\mathbb{Z}/p\mathbb{Z}$ of congruence classes

modulo p is simple, where p is a prime number.

Simple Groups

Example

On the other hand, the group $G = \mathbb{Z}/12\mathbb{Z}$ is not simple.

The set H={0, 4, 8} of congruence classes of 0, 4, and 8 modulo 12 is a subgroup of order 3, and it is a normal subgroup since any subgroup of an abelian group is normal.

Simple Groups

Example

The additive group $\mathbb{Z}$ of integers is not simple; the set of even integers $2\mathbb{Z}$ is a non-trivial proper normal subgroup.

Simple Groups

Theorem

The alternating group A_n is simple for $n \geq 5$.

Group Theory

Simple Groups

Simple Groups

Theorem

Let ϕ: G → G' be a group homomorphism. If N is a normal subgroup of G, then $\phi[N]$ is a normal subgroup of $\phi[G]$. Also, if N' is a normal subgroup of $\phi[G]$, then $\phi^{-1}[N']$ is a normal subgroup of G.

Simple Groups

Proof

Let ϕ: G → G' be a group homomorphism. If N is a normal subgroup of G, then $gng^{-1} \in N$ for all $g \in G$ and $n \in N$. It implies that $\phi(gng^{-1})=$

$\phi(g)\phi(n)\phi(g)^{-1} \in \phi[N]$.

Therefore, $\phi[N]$ is a normal subgroup of $\phi[G]$.

Simple Groups

Proof

Also, if N' is a normal subgroup of $\phi[G]$, then $\phi(g)n'\phi(g)^{-1} \in N'$ for every $\phi(g) \in \phi[G]$ and $n' \in N'$.

By definition, there exist $n \in N$ such that $\phi(n) = n'$. Therefore, $\phi(g)n'\phi(g)^{-1} = \phi(gng^{-1})$.

Hence $\phi^{-1}[N']$ is a normal subgroup of G.

Group Theory

Simple Groups

Simple Groups

The last Theorem should be viewed as saying that a homomorphism $\phi: G \to G'$ preserves normal subgroups between G and $\phi[G]$.

It is important to note that $\phi[N]$ may not be normal in G', even though N is normal in G.

Simple Groups

Example

For example, $\phi: \mathbb{Z}_2 \to S_3$, where

$\phi(0) = \rho_0$ and $\phi(1) = \mu_1$ is a homomorphism, and $\mathbb{Z}_2$ is a normal subgroup of itself, but $\{\rho_0, \mu_1\}$ is not a normal subgroup of S_3.

(1 3)(2 3)=(2 1 3)

(2 3)(1 3)=(1 2 3)

Group Theory

Maximal Normal Subgroups

Maximal Normal Subgroups

We characterize when G/N is a simple group.

Definition

A maximal normal subgroup of a **group** G is a normal subgroup M not equal to G such that there is no proper normal subgroup N of G properly containing M.

Maximal Normal Subgroups

Theorem

M is a maximal normal subgroup of G if and only if G / M is simple.

Maximal Normal Subgroups

Proof

Let M be a maximal normal subgroup of G. Consider the canonical homomorphism

y: G→G/M. Now y^{-1} of any nontrivial proper normal subgroup of G/M is a proper normal subgroup of G properly containing M. But M is maximal, so this can not happen. Thus G/M is simple.

865

Maximal Normal Subgroups

Conversely, if N is a normal subgroup of G properly containing M, then y[N] is normal in G/M. If also N≠G, then y[N]≠G/M and y[N]≠ {M}.

Thus, if G/M is simple so that no such y[N] can exist, no such N can exist, and M is maximal.

866

Group Theory

The Center Subgroup

867

The Center Subgroup

Definition

The center Z(G) is defined by

Z(G)={z ∈ G| zg=gz for all g ∈ G}.

868

The Center Subgroup

Exercise

Show that Z(G) is a normal and an abelian subgroup of G.

869

The Center Subgroup

Solution

For each g ∈ G and

z∈Z(G) we have

$gzg^{-1}=zgg^{-1}=ze=z$, we see at once that Z(G) is a normal subgroup of G. It implies that gz=zg for g ∈ G and z∈Z(G).

870

The Center Subgroup

If G is abelian, then
Z(G) = G;
in this case, the center is not useful.

Group Theory

Example on Center Subgroup

Example on Center Subgroup

Example

$\rho_0\,(123) = (123)\rho_0$

$\rho_0\,(132) = (132)\rho_0$

$\rho_0\,(23) = (23)\rho_0$

$\rho_0\,(13) = (13)\rho_0$

$\rho_0\,(12) = (12)\rho_0$

Example on Center Subgroup

$(132)(123) = \rho_0 = (123)(132)$
$(123)(23) = (12), (23)(123) = (13)$
$(132)(13) = (12), (13)(132) = (23)$
$(13)(12) = (123), (12)(13) = (132)$

$Z(S_3)=\{\rho_0\}$, so the center of S_3 is trivial.

Group Theory

Example on Center Subgroup

Example on Center Subgroup

The center of a group G always contains the identity element e.

It may be that Z(G)={e}, in which case we say that **the center of** G is **trivial.**

Example on Center Subgroup

Example

$S_3 \times \mathbb{Z}_5$={(ρ_0,0), (ρ_0,1), (ρ_0,2), (ρ_0,3), (ρ_0,4),
(ρ_1,0), (ρ_1,1), (ρ_1,2), (ρ_1,3), (ρ_1,4),
(ρ_2,0), (ρ_2,1), (ρ_2,2), (ρ_2,3), (ρ_2,4),
(μ_1,0), (μ_1,1), (μ_1,2), (μ_1,3), (μ_1,4),
(μ_2,0), (μ_2,1), (μ_2,2), (μ_2,3), (μ_2,4),
(μ_3,0), (μ_3,1), (μ_3,2), (μ_3,3), (μ_3,4)}

Example on Center Subgroup

The center of $S_3 \times \mathbb{Z}_5$ must be $\{\rho_0\} \times \mathbb{Z}_5$, which is isomorphic to $\mathbb{Z}_5$.

Group Theory

The Commutator Subgroup

The Commutator Subgroup

Every nonabelian group G has two important normal subgroups,

the center Z(G) of G and the commutator subgroup C of G.

The Commutator Subgroup

Turning to the commutator subgroup, recall that in forming a factor group of G modulo a normal subgroup N, we are essentially putting every element in G that is in N equal to e, for N forms our new identity in the factor group.

This indicates another use for factor groups.

The Commutator Subgroup

Suppose, for example, that we are studying the structure of a nonabelian group G.

Since Fundamental Theorem of Abelian Groups gives complete information about the structure of all sufficiently small abelian groups, it might be of interest to try to form an abelian group as much like G as possible, an abelianized version of G, by starting with G and then requiring that ab=ba for all a and b in our new group structure.

The Commutator Subgroup

To require that ab=ba is to say that $aba^{-1}b^{-1}=e$ in our new group.

An element $aba^{-1}b^{-1}$ in a group is a **commutator of the group.**

Thus we wish to attempt to form an abelianized version of G by replacing every commutator of G by e.

We should then attempt to form the factor group of G modulo the smallest normal subgroup we can find that contains all commutators of G.

883

The Commutator Subgroup

Theorem

Let G be a group.

The set of all commutators $aba^{-1}b^{-1}$ for a, b ∈ G generates a subgroup C of G.

884

The Commutator Subgroup

Proof

Let a, b ∈ G. Then,

$(aba^{-1}b^{-1})(aba^{-1}b^{-1})^{-1}$

$=aba^{-1}b^{-1}bab^{-1}a^{-1}$

$=e \in C$

since $e = eee^{-1}e^{-1}$ is a commutator.

885

The Commutator Subgroup

Definition

The set of all commutators $aba^{-1}b^{-1}$ for a, b ∈ G generates a subgroup C of G is called the **commutator subgroup**.

886

Group Theory

Generating Sets

887

Generating Sets

Let G be a group, and let a ∈ G. We have described the cyclic subgroup <a> of G, which is the smallest subgroup of G that contains the element a.

Suppose we want to find as small a subgroup as possible that contains both a and b for another element b in G.

888

Generating Sets

We see that any subgroup containing a and b must contain a^n and b^m for all m, n ∈ $\mathbb{Z}$, and consequently must contain all finite products of such powers of a and b.

Generating Sets

For example, such an expression might be $a^2b^4a^{-3}b^2a^5$.

Note that we cannot "simplify" this expression by writing first all powers of a followed by the powers of b, since G may not be abelian. However, products of such expressions are again expressions of the same type.

Furthermore, e = a^0 and the inverse of such an expression is again of the same type.

Generating Sets

For example, the inverse of $a^2b^4a^{-3}b^2a^5$ is $a^{-5}b^{-2}a^3b^{-4}a^{-2}$.

This shows that all such products of integral powers of a and b form a subgroup of G, which surely must be the smallest subgroup containing both a and b. We call a and b generators of this subgroup.

If this subgroup should be all of G, then we say that {a, b} generates G.

We could have made similar arguments for three, four, or any number of elements of G, as long as we take only finite products of their integral powers.

Generating Sets

Example

The Klein 4-group V = {e, a, b, c} is generated by {a,b} since ab=c.

It is also generated by {a,c}, {b,c }, and {a,b,c}.

If a group G is generated by a subset S, then every subset of G containing S generates G.

Group Theory

Generating Sets

Generating Sets

Example

The group $\mathbb{Z}_6$ is generated by {1} and {5}.

It is also generated by {2,3} since 2+3=5, so that any subgroup containing 2 and 3 must contain 5 and must therefore be $\mathbb{Z}_6$.

Generating Sets

It is also generated by {3,4}, {2,3,4}, {1,3}, and {3,5}.

But it is not generated by {2, 4} since

<2> = {0, 2, 4}

contains 2 and 4.

895

Generating Sets

We have given an intuitive explanation of the subgroup of a group G generated by a subset of G.

What follows is a detailed exposition of the same idea approached in another way, namely via intersections of subgroups.

896

Generating Sets

Definition

Let $\{S_i | i \in I\}$ be a collection of sets.

Here I may be any set of indices.

The intersection $\bigcap_{i\in I} S_i$ of the sets S_i is the set of all elements that are in all the sets S_i; that is,

$\bigcap_{i\in I} S_i = \{x | x \in S_i \text{ for all } i \in I\}$.

If I is finite, $I = \{1, 2,\ldots,n\}$, we may denote $\bigcap_{i\in I} S_i$ by $S_1 \cap \ldots \cap S_n$.

897

Group Theory

Generating Sets

898

Generating Sets

Theorem

The intersection of some subgroups H_i of a group G for $i \in I$ is again a subgroup of G.

899

Generating Sets

Proof

Let us show closure. Let $a \in \bigcap_{i\in I} H_i$ and $b \in \bigcap_{i\in I} H_i$, so that $a \in H_i$ for all $i \in I$ and $b \in H_i$ for all $i \in I$. Then $ab \in H_i$ for all $i \in I$, since H_i is a group. Thus $ab \in \bigcap_{i\in I} H_i$.

Since H_i is a subgroup for all $i \in I$, we have $e \in H_i$ for all $i \in I$, and hence $e \in \bigcap_{i\in I} H_i$.

Finally, for $a \in \bigcap_{i\in I} H_i$, we have $a \in H_i$ for all $i \in I$, so $a^{-1} \in H_i$ for all $i \in I$, which implies that $a^{-1} \in \bigcap_{i\in I} H_i$.

900

Generating Sets

Let G be a group and let $a_i \in G$ for $i \in I$.

There is at least one subgroup of G containing all the elements a_i for $i \in I$, namely G is itself.

The above theorem assures us that if we take the intersection of all subgroups of G containing all a_i for $i \in I$, we will obtain a subgroup H of G.

This subgroup H is the smallest subgroup of G containing all the a_i for $i \in I$.

901

Group Theory

Generating Sets

902

Generating Sets

Definition

Let G be a group and let $a_i \in G$ for $i \in I$.

The smallest subgroup of G containing $\{a_i \mid i \in I\}$ is the subgroup generated by $\{a_i \mid i \in I\}$.

If this subgroup is all of G, then $\{a_i \mid i \in I\}$ generates G and the a_i are generators of G.

903

Generating Sets

Definition

If there is a finite set

$\{ a_i \mid i \in I\}$

that generates G, then G is finitely generated.

904

Generating Sets

Note that this definition is consistent with our previous definition of a generator for a cyclic group.

Note also that the statement a is a generator of G may mean either that G = <a> or that a is a member of a subset of G that generates G.

Our next theorem gives the structural insight into the subgroup of G generated by $\{a_i \mid i \in I\}$ that we discussed for two generators in the beginning of these modules.

905

Generating Sets

Theorem

If G is a group and $a_i \in G$ for $i \in I$, then the subgroup H of G generated by $\{ a_i \mid i \in I\}$ has as elements precisely those elements of G that are finite products of integral powers of the a_i, where powers of a fixed a_i may occur several times in the product.

906

Generating Sets

Proof

Let K denote the set of all finite products of integral powers of the a_i. Then $K \subseteq H$.

We need only observe that K is a subgroup and then, since H is the smallest subgroup containing a_i for $i \in I$, we will be done.

Observe that a product of elements in K is again in K. Since $(a_i)^0=e$, we have $e \in K$.

907

Generating Sets

For every element k in K, if we form from the product giving k a new product with the order of the a, reversed and the opposite sign on all exponents, we have k^{-1} which is thus in K.

908

Group Theory

The Commutator Subgroup

909

The Commutator Subgroup

Theorem

Let G be a group.

Then, the commutator subgroup C of G is a normal subgroup of G.

910

The Commutator Subgroup

Proof

We must show that C is normal in G.

The last theorem then shows that C consists precisely of all finite products of commutators.

For $x \in C$, we must show that $g^{-1}xg \in C$ for all $g \in G$, or that if x is a product of commutators, so is

$g^{-1}xg$ for all $g \in G$.

911

The Commutator Subgroup

By inserting $e = gg^{-1}$ between each product of commutators occurring in x, we see that it is sufficient to show for each commutator $cdc^{-1}d^{-1}$ that $g^{-1}(cdc^{-1}d^{-1})g$ is in C.

But $g^{-1}(cdc^{-1}d^{-1})g = (g^{-1}cdc^{-1})(e)(d^{-1}g)$

$= (g^{-1}cdc^{-1})(gd^{-1}dg^{-1})(d^{-1}g)$

$= [(g^{-1}c)d(g^{-1}c)^{-1}d^{-1}][dg^{-1}d^{-1}g]$, which is in C.

Thus C is normal in G.

912

Group Theory

The Commutator Subgroup

The Commutator Subgroup

Theorem

If N is a normal subgroup of G, then G/N is abelian if and only if $C \leq N$.

The Commutator Subgroup

Proof

If N is a normal subgroup of G and G/N is abelian, then

$(a^{-1}N)(b^{-1}N)=(b^{-1}N)(a^{-1}N)$; that is, $aba^{-1}b^{-1}N=N$,

so $aba^{-1}b^{-1} \in N$, and

$C \leq N$.

The Commutator Subgroup

Finally, if $C \leq N$, then

$(aN)(bN)=abN$

$=ab(b^{-1}a^{-1}ba)N$

$= (abb^{-1}a^{-1})baN$

$= baN$

$= (bN)(aN)$.

Group Theory

The Commutator Subgroup

The Commutator Subgroup

Example

For the group S_3, we find that one commutator is

$\rho_1\mu_1\, \rho_1^{-1}\mu_1^{-1} = \rho_1\mu_1\, \rho_2\mu_1 = \mu_3\mu_2 = \rho_2$.

(12)(13)=(132)

We similarly find that

$\rho_2\mu_1\, \rho_2^{-1}\mu_1^{-1} = \rho_2\mu_1\, \rho_1\mu_1 = \mu_2\mu_3 = \rho_1$.

(13)(12)=(123)

The Commutator Subgroup

Thus the commutator subgroup C of S_3 contains A_3. Since A_3 is a normal subgroup of S_3 and

S_3/A_3 is abelian, above theorem shows that $C=A_3$.

919

Group Theory

Automorphisms

920

Automorphisms

Recall that an automorphism of a group G is an isomorphism of G onto G.
The set of all automorphisms of G is denoted by Aut(G).

921

Automorphisms

We have seen that every $g \in G$ determines an automorphism i_g of G (called an inner automorphism)given by $i_g(x)=gxg^{-1}$. The set of all inner automorphisms of G is denoted by Inn(G).

922

Automorphisms

Theorem
The set Aut(G) of all automorphisms of a group G is a group under composition of mappings, and $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$. Moreover, $G/Z(G) \simeq \mathrm{Inn}(G)$.

923

Automorphisms

Proof
Clearly, Aut(G) is nonempty. Let $\sigma, \tau \in \mathrm{Aut}(G)$.
Then for all $x, y \in G$, $\sigma\tau(xy)=\sigma((\tau(x)\,\tau(y)) = (\sigma\tau(x))(\sigma\tau(y))$.
Hence, $\sigma\tau \in \mathrm{Aut}(G)$. Again,
$\sigma(\sigma^{-1}(x)\sigma^{-1}(y))=$
$\sigma\sigma^{-1}(x)\sigma\sigma^{-1}(y)=xy$.
Hence $\sigma^{-1}(x)\sigma^{-1}(y)= \sigma^{-1}(xy)$. Therefore, $\sigma^{-1} \in \mathrm{Aut}(G)$. This proves that Aut(G) is a subgroup of the symmetric group S_G and, hence, is itself a group.

924

Group Theory

Automorphisms

Automorphisms

Theorem
The set Aut(G) of all automorphisms of a group G is a group under composition of mappings, and $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$. Moreover, $G/Z(G) \simeq \mathrm{Inn}(G)$.

Automorphisms

Consider the mapping $\phi: G \to \mathrm{Aut}(G)$ given by $\phi(a)=i_a=axa^{-1}$ for all $x \in G$.
For any $a, b \in G$, $i_{ab}(x)= abx(ab)^{-1}= a(bxb^{-1})a^{-1} = i_a i_b(x)$ for all $x \in G$.
Hence, ϕ is a homomorphism, and, therefore, $\mathrm{Inn}(G)=\mathrm{Im}\ \phi$ is a subgroup of Aut(G).

Automorphisms

Further, i_a is the identity automorphism if and only if $axa^{-1}= x$ for all $x \in G$. Hence, $\mathrm{Ker}\ \phi = Z(G)$, and by the fundamental theorem of homomorphisms $G/Z(G) \simeq \mathrm{Inn}(G)$.

Finally, for any $\sigma \in \mathrm{Aut}(G)$,
$(\sigma i_a \sigma^{-1})(x) = \sigma(a\sigma^{-1}(x)a^{-1})$
$= \sigma(a)x\,\sigma(a)^{-1}$
$= i_{\sigma(a)}(x)$; hence $\sigma i_a \sigma^{-1}=i_{\sigma(a)} \in \mathrm{Inn}(G)$.
Therefore, $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

Automorphisms

It follows from above theorem that if the center of a group G is trivial, then $G \simeq \mathrm{Inn}(G)$. A group G is said to be complete if $Z(G) = \{e\}$ and every automorphism of G is an inner automorphism; that is, $G \simeq \mathrm{Inn}(G)=\mathrm{Aut}(G)$.

When considering the possible automorphisms σ of a group G, it is useful to remember that, for any $x \in G$, x and $\sigma(x)$ must be of the same order.

Group Theory

Examples on Automorphisms

Examples on Automorphisms

Example
The symmetric group S_3 has a trivial center {e}. Hence, $Inn(S_3) \simeq S_3$. We have seen that $S_3= \{e,a,a^2,b,ab,a^2b\}$ with the defining relations $a^3= e= b^2$, $ba = a^2b$. The elements a and a^2 are of order 3, and b, ab, and a^2b are all of order 2.

931

Examples on Automorphisms

Hence, for any $\sigma \in Aut(S_3)$, $\sigma(a)= a$ or a^2, $\sigma(b)= b, ab,$ or a^2b. Moreover, when $\sigma(a)$ and $\sigma(b)$ are fixed, $\sigma(x)$ is known for every $x \in S_3$. Hence, σ is completely determined.

932

Examples on Automorphisms

Thus, there cannot be more than six automorphisms of S_3. Hence $Aut(S_3)=Inn(S_3) \simeq S_3$. Therefore, S_3 is a complete group.

933

Group Theory

Examples on Automorphisms

934

Examples on Automorphisms

Example
Let G be a finite abelian group of order n, and let m be a positive integer relative prime to n. Then the mapping $\sigma: x \rightarrow x^m$ is an automorphism of G.

935

Examples on Automorphisms

Solution
$(m,n) = 1 \Rightarrow$ there exist integers u and v such that $mu + nv = 1 \Rightarrow$ for all $x \in G$, $x^{mu+nv}=x^{mu}x^{nv}=x^{um}$ since $o(G)=n$. Now for all $x \in G$, $x=(x^u)^m$ implies that σ is onto. Further, $x^m=e \Rightarrow x^{mu}=e \Rightarrow x = e$, showing that σ is 1-1.

936

Examples on Automorphisms

That σ is a homomorphism follows from the fact that G is abelian. Hence, σ is an automorphism of G.

Group Theory

Examples on Automorphisms

Examples on Automorphisms

Example
A finite group G having more than two elements and with the condition that $x^2 \neq e$ for some $x \in G$ must have a nontrivial automorphism.

Examples on Automorphisms

When G is abelian, then $\sigma : x \mapsto x^{-1}$ is an automorphism, and, clearly, σ is not an identity automorphism. When G is not abelian, there exists a nontrivial inner automorphism.

Examples on Automorphisms

Example
Let $G = \langle a \mid a^n = e \rangle$ be a finite cyclic group of order n. Then the mapping $\sigma : a \rightarrow a^m$ is an automorphism of G iff $(m,n) = 1$.

Examples on Automorphisms

Solution
If $(m,n) = 1$, then it has been shown in Example of last module that σ is an automorphism. So let us assume now that σ is an automorphism. Then the order of $\sigma(a) = a^m$ is the same as that of a, which is n.

Examples on Automorphisms

Further, if (m,n)=d, then $(a^m)^{n/d}=(a^n)^{m/d} = e$. Thus, the order of a^m divides n/d; that is, n|n/d. Hence, d = 1, and the solution is complete.

Group Theory

Group Action on a Set

Group Action on a Set

We define a binary operation * on a set S to be a function mapping SxS into S. The function * gives us a rule for "multiplying" an element s_1 in S and an element s_2 in S to yield an element $s_1 * s_2$ in S.

Group Action on a Set

More generally, for any sets A, B, and C, we can view a map *: A x B→C as defining a "multiplication," where any element a of A times any element b of B has as value some element c of C. Of course, we write a* b = c, or simply ab= c.

Group Action on a Set

In these modules, we will be concerned with the case where X is a set, G is a group, and we have

a map *: G x X→ X. We shall write *(g, x) as g * x or gx.

Group Action on a Set

Definition

Let X be a set and G a group. An **action of G on** X is a map *: G x X → X such that

1. ex = x for all x ∈ X,

2. $(g_1g_2)(x) = g_1(g_2x)$ for all x ∈ X and all g_1, g_2 ∈ G. Under these conditions,

X is a G-set.

Group Action on a Set

Example

Let X be any set, and let H be a subgroup of the group S_x of all permutations of X.

Then X is an H -set, where the action of $\sigma \in H$ on X is its action as an element of S_x, so that $\sigma x = \sigma(x)$ for all $x \in X$.

949

Group Theory

Group Action on a Set

950

Group Action on a Set

Condition 2 is a consequence of the definition of permutation multiplication as function composition, and Condition 1 is immediate from the definition of the identity permutation as the identity function. Note that, in particular,

$\{1, 2, 3, \cdots, n\}$ is an S_n set.

951

Group Action on a Set

Our next theorem will show that for every G-set X and each $g \in G$, the map σ_g: X→X defined by $\sigma_g = gx$ is a permutation of X, and that there is a homomorphism $\phi: G \to S_x$ such that the action of G on X is essentially the above Example action of the image subgroup $H = \phi[G]$ of S_x on X.

952

Group Action on a Set

So actions of subgroups of S_x on X describe all possible group actions on X. When studying the set X, actions using subgroups of S_x suffice. However, sometimes a set X is used to study G via a group action of G on X. Thus we need the more general concept given by above Definition.

953

Group Action on a Set

Theorem

Let X be a G-set. For each $g \in G$, the function σ_g: X→X defined by $\sigma_g(x) = gx$ for $x \in X$ is a permutation of X. Also, the map $\phi: G \to S_x$ defined by $\phi(g) = \sigma_g$ is a homomorphism with the property that $\phi(g)(x) = gx$.

954

Group Action on a Set

Proof

To show that σ_g is a permutation of X, we must show that it is a one-to-one map of X onto itself. Suppose that $\sigma_g(x_1) = \sigma_g(x_2)$ for $x_1, x_2 \in X$. Then $gx_1 = gx_2$ Consequently, $g^{-1}(gx_1) = g^{-1}(gx_2)$. Using Condition 2 in Definition, we see that $(g^{-1}g)x_1 = (g^{-1}g)x_2$, so $ex_1 = ex_2$. Condition 1 of the definition then yields $x_1 = x_2$, so σ_g is one to one. The two conditions of the definition show that for $x \in X$, we have $\sigma_g(g^{-1}x) = g(g^{-1})x = (gg^{-1})x = ex = x$, so σ_g maps X onto X. Thus σ_g is indeed a permutation.

955

Group Theory

Group Action on a Set

956

Group Action on a Set

Theorem

Let X be a G-set. For each $g \in G$, the function σ_g: $X \to X$ defined by $\sigma_g(x) = gx$ for $x \in X$ is a permutation of X. Also, the map ϕ: $G \to S_x$ defined by $\phi(g) = \sigma_g$ is a homomorphism with the property that $\phi(g)(x) = gx$.

957

Group Action on a Set

To show that ϕ: $G \to S_x$ defined by $\phi(g) = \sigma_g$ is a homomorphism, we must show that $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$. We show the equality of these two permutations in S_x by showing they both carry an $x \in X$ into the same element. Using the two conditions in above Definition and the rule for function composition, we obtain

$\phi(g_1g_2)(x) = \sigma_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = g_1\,\sigma_{g_2}(x) = \sigma_{g_1}(\sigma_{g_2}(x)) = (\sigma_{g_1} \circ \sigma_{g_2})(x) = (\sigma_{g_1}\sigma_{g_2})(x) = (\,\phi(g_1)\,\phi(g_2)\,)(x).$

958

Group Action on a Set

Thus ϕ is a homomorphism.

The stated property of ϕ follows at once since by our definitions, we have $\phi(g)(x) = \sigma_g(x) = gx$.

959

Group Theory

Group Action on a Set

960

Group Action on a Set

Definition

Let X be a set and G a group. An **action of G on** X is a map $*: G \times X \to X$ such that

1. $ex = x$ for all $x \in X$,

2. $g_1(g_2x)=(g_1g_2)(x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

Under these conditions, X is a G-set.

961

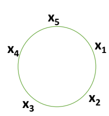
Group Action on a Set

Example

Let G be the additive group $\mathbb{R}$, and X be the set of complex numbers z such that $|z| = 1$. Then X is a G-set under the action $\gamma * c = e^{i\gamma}c$, where $\gamma \in \mathbb{R}$ and $c \in X$. Here the action of γ is the rotation through an angle $\theta=\gamma$ radians, anticlockwise.

962

Group Action on a Set



Example

Let $G=S_5$, and $X=\{x_1, x_2, x_3, x_4, x_5\}$ be a set of beads forming a circular ring. Then X is a G-set under the action $G*x_i=x_{g(i)}$, $g\in S_5$.

963

Group Action on a Set

Example

Let $G=D_4$ and X be the vertices 1, 2, 3, 4 of a square. X is a G-set under the action

$g * i = g(i)$, $g \in D_4$, $i \in \{1, 2, 3, 4\}$.

964

Group Action on a Set

Example

Let G be a group. Define $a*x = ax$, $a \in G$, $x \in G$.

Then, clearly, the set G is a G-set.

This action of the group G on itself is called translation.

965

Group Theory

Group Action on a Set

966

Group Action on a Set

Example

Let G be a group.

Define

$a*x = axa^{-1}$, $a \in G$, $x \in G$.

We show that G is a G-set.

Let a, b ∈ G. Then

$(ab)*x = (ab)x(ab)^{-1}$

$= a(bxb^{-1})a^{-1} = a(b*x)a^{-1}$

$= a*(b*x)$.

Also, $e*x = x$.

967

Group Action on a Set

This proves G is a G-set.
This action of the group G on itself is called conjugation.

968

Group Action on a Set

Example

Let G be a group and $H<G$. Then the set G/H of left cosets can be made into a G-set defining

$a*xH = axH$, $a \in G$, $xH \in G/H$.

969

Group Action on a Set

Example

Let G be a group and $H \triangleleft G$.
Then the set G/H of left cosets is a G-set if we define $a*xH = axa^{-1}H$, $a \in G$, $xH \in G/H$.

970

Group Action on a Set

To see this, let $a, b \in G$ and $xH \in G/H$. Then

$(ab)*xH = abxb^{-1}a^{-1}H$

$= a*bxb^{-1}H = a*(b*xH)$.

Also, $e*xH = xH$.

Hence, G/H is a G-set.

971

Group Theory

Group Action on a Set

972

Group Action on a Set

Theorem
Let G be a group and let X be a set.
(i) If X is a G-set, then the action of G on X induces a homomorphism
$\phi: G \to S_X$.
(ii) Any homomorphism $\phi: G \to S_X$ induces an action of G onto X.

973

Group Action on a Set

Proof
(i) We define $\phi: G \to S_X$ by $(\phi(a))(x)=ax$, $a \in G$, $x \in X$.
Clearly $\phi(a) \in S_X$, $a \in G$. Let a, $b \in G$. Then
$(\phi(ab))(x)=(ab)x=a(bx)=a((\phi(b))(x)) = (\phi(a))((\phi(b))(x))=(\phi(a)\phi(b))x$ for all $x \in X$.
Hence, $\phi(ab)= \phi(a)\, \phi(b)$.
(ii) Define $a*x=(\phi(a))(x)$; that is, $ax=(\phi(a))(x)$. Then
$(ab)x = (\phi(ab))(x)=(\phi(a)\phi(b))(x)= \phi(a)(\phi(b)(x))= \phi(a)(bx)=a(bx)$. Also, $ex=(\phi(e))(x)=x$.
Hence, X is a G-set.

974

Group Theory

Stabilizer

975

Stabilizer

Definition
Let G be a group acting on a set X, and let $x \in X$. Then the set
$G_x= \{g \in G \mid gx = x\}$,
which can be shown to be a subgroup, is called the stabilizer (or isotropy) group of x in G.

976

Stabilizer

Example
Let G be a group. Define $a*x = axa^{-1}$, $a \in G$, $x \in G$.
This action of the group G on itself is called conjugation.
Then, for $x \in G$, $G_x = \{a \in G \mid axa^{-1}=x\}=N(x)$, the normalizer of x in G.
Thus, in this case the stabilizer of any element x in G is the normalizer of x in G.

977

Stabilizer

Example
Let G be a group and H<G. We define action of G on the set G/H of left cosets by
$a*xH=axH$, $a \in G$, $xH \in G/H$.
Here the stabilizer of a left coset xH is the subgroup
$\{g \in G \mid gxH=xH\} = \{g \in G \mid x^{-1}gx \in H\}$
$= \{g \in G \mid g \in xHx^{-1}\} = xHx^{-1}$

978

Group Theory

Stabilizer

Stabilizer

Theorem

Let X be a G-set.

Then G_x is a subgroup of G for each $x \in X$.

Stabilizer

Proof

Let $x \in X$ and let $g_1, g_2 \in G_x$. Then $g_1x=x$ and $g_2x=x$. Consequently, $(g_1g_2)x=g_1(g_2x)=g_1x=x$, so $g_1g_2 \in G_x$, and G_x is closed under the induced operation of G.

Of course $ex=x$, so $e \in G_x$.

If $g \in G_x$, then $gx = x$, so $x=ex=(g^{-1}g)x= g^{-1}(gx)=g^{-1}x$, and consequently $g^{-1} \in G_x$.

Thus G_x is a subgroup of G.

Group Theory

Orbits

Orbits

Theorem

Let X be a G-set. For $x_1, x_2 \in X$, let $x_1 \sim x_2$ if and only if there exists $g \in G$ such that $gx_1=x_2$. Then $\sim$ is an equivalence relation on X.

Orbits

Proof

For each $x \in X$, we have $ex=x$, so $x \sim x$ and $\sim$ is reflexive.

Suppose $x_1 \sim x_2$, so $gx_1=x_2$ for some $g \in G$. Then $g^{-1}x_2=g^{-1}(gx_1) =(g^{-1}g)x_1=ex_1=x_1$, so $x_2 \sim x_1$, and $\sim$ is symmetric.

Finally, if $x_1 \sim x_2$ and $x_2 \sim x_3$, then $g_1x_1=x_2$ and $g_2x_2=x_3$ for some $g_1, g_2 \in G$. Then $(g_2g_1)x_1= g_2(g_1x_1)= g_2x_2=x_3$, so $x_1 \sim x_3$ and $\sim$ is transitive.

Orbits

Definition
Let G be a group acting on a set X, and let $x \in X$. Then the set
$Gx = \{ax \mid a \in G\}$
is called the orbit of x in G.

Orbits

Example
Let G be a group. Define
$a*x = ax$, $a \in G$, $x \in G$.
The orbit of $x \in G$ is
$Gx=\{ax \mid a \in G\}=G$.

Orbits

Example
Let G be a group.
Define
$a*x = axa^{-1}$, $a \in G$, $x \in G$.
The orbit of $x \in G$ is
$Gx = \{axa^{-1} \mid a \in G\}$, called the conjugate class of x and denoted by C(x).

Group Theory

Conjugacy and G-Sets

Conjugacy and G-Sets

Theorem
Let X be a G-set and let $x \in X$. Then $|Gx|=(G:G_x)$.
If $|G|$ is finite, then $|Gx|$ is a divisor of $|G|$.
If X is a finite set, $|X|=\sum_{x\in C}(G:G_x)$,
where C is a subset of X containing exactly one element from each orbit.

Conjugacy and G-Sets

Proof
We define a one-to-one map ψ from Gx onto the collection of left cosets of G_x in G.
Let $x_1 \in Gx$. Then there exists $g_1 \in G$ such that $g_1x=x_1$. We define $\psi(x_1)$ to be the left coset g_1G_x of G_x.
We must show that this map ψ is well defined, independent of the choice of $g_1 \in G$ such that $g_1x=x_1$. Suppose also that $g_1'x=x_1$. Then, $g_1x=g_1'x$, so $g_1^{-1}(g_1x)= g_1^{-1}(g_1'x)$, from which we deduce $x=(g_1^{-1}g_1')x$. Therefore $g_1^{-1}g_1' \in G_x$, so $g_1' \in g_1G_x$, and $g_1G_x=g_1'G_x$. Thus the map ψ is well defined.

Group Theory

Conjugacy and G-Sets

Conjugacy and G-Sets

Theorem

Let X be a G-set and let $x \in X$. Then $|Gx|=(G:G_x)$.

If $|G|$ is finite, then $|Gx|$ is a divisor of $|G|$.

If X is a finite set, $|X|=\sum_{x\in C}(G: G_x)$,
where C is a subset of X containing exactly one element from each orbit.

Conjugacy and G-Sets

To show the map ψ is one to one, suppose $x_1, x_2 \in Gx$, and $\psi(x_1)=\psi(x_2)$. Then there exist $g_1, g_2 \in G$ such that $x_1=g_1x$, $x_2=g_2x$, and $g_2 \in g_1G_x$. Then $g_2=g_1g$ for some $g \in G_x$, so $x_2=g_2x=g_1(gx)=g_1x=x_1$. Thus ψ is one to one.

Finally, we show that each left coset of G_x in G is of the form $\psi(x_1)$ for some $x_1 \in Gx$. Let g_1G_x be a left coset. Then if $g_1x=x_1$, we have $g_1G_x=\psi(x_1)$.

Thus ψ maps Gx one to one onto the collection of left cosets so $|Gx|=(G:G_x)$.

Conjugacy and G-Sets

If $|G|$ is finite, then the equation $|G|=|G_x|(G:G_x)$ shows that $|Gx|=(G:Gx)$ is a divisor of $|G|$.

Since X is the disjoint union of orbits Gx, it follows that if X is finite, then $|X|=\sum_{x\in C}(G: G_x)$.

Group Theory

Isomorphism Theorems

Isomorphism Theorems

There are several theorems concerning isomorphic factor groups that are known as the isomorphism theorems of group theory.

Isomorphism Theorems

Theorem

Let ϕ: $G \to G'$ be a homomorphism with kernel K, and let

y_K: $G \to G/K$ be the canonical homomorphism. There is a unique isomorphism

μ: $G/K \to \phi[G]$ such that $\phi(x) = \mu(y_K(x))$ for each $x \in G$.

Isomorphism Theorems

The first isomorphism theorem is diagrammed in Figure below.

$$\begin{tikzcd} G \arrow[rr, "\phi"] \arrow[dr, "y_K"'] & & \phi[G] \\ & G/K \arrow[ur, "\mu"'] & \end{tikzcd}$$

Isomorphism Theorems

Lemma

Let N be a normal subgroup of a group G and let y: $G \to G/N$ be the canonical homomorphism. Then the map ϕ from the set of normal subgroups of G containing N to the set of normal subgroups of G/N given by $\phi(L)=y[L]$ is one to one and onto.

Isomorphism Theorems

Proof

If L is a normal subgroup of G containing N, then $\phi(L)=y[L]$ is a normal subgroup of G/N.

Because $N \leq L$, for each $x \in L$ the entire coset xN in G is contained in L. Thus, $y^{-1}[\phi(L)]=L$. Consequently, if L and M are normal subgroups of G, both containing N, and if $\phi(L)= \phi(M) = H$, then $L=y^{-1}[H]=M$. Therefore ϕ is one to one.

Isomorphism Theorems

If H is a normal subgroup of G/N, then $y^{-1}[H]$ is a normal subgroup of G. Because $N \in H$ and

$y^{-1}[\{N\}]=N$, we see that $N \subseteq y^{-1}[H]$. Then

$\phi(y^{-1}[H])=y[y^{-1}[H]]=H$.

This shows that ϕ is onto the set of normal

subgroups of G/N.

Group Theory

Isomorphism Theorems

Isomorphism Theorems

If H and N are subgroups of a group G, then we let

HN={hn| h ∈ H, n ∈ N}.

We define the **join** H V N of H and N as the intersection of all subgroups of G that contain HN; thus H V N is the smallest subgroup of G containing HN.

Isomorphism Theorems

Of course H V N is also the smallest subgroup of G containing both H and N, since any such subgroup must contain HN. In general, HN need not be a subgroup of G.

Isomorphism Theorems

Lemma

If N is a normal subgroup of G, and if H is any subgroup of G, then

H V N=HN=NH.

Furthermore, if H is also normal in G, then HN is normal in G.

Isomorphism Theorems

Proof

We show that HN is a subgroup of G, from which

H V N=HN follows at once. Let $h_1, h_2 \in H$ and $n_1, n_2 \in N$. Since N is a normal subgroup, we have $n_1h_2=h_2n_3$ for some $n_3 \in N$. Then $(h_1n_1)(h_2n_2)=h_1(n_1h_2)n_2=h_1(h_2n_3)n_2=(h_1h_2)(n_3n_2) \in HN$, so HN is closed under the induced operation in G. Clearly e=ee is in HN. For $h \in H$ and $n \in N$, we have $(hn)^{-1}=n^{-1}h^{-1}= h^{-1}n_4$ for some $n_4 \in N$, since N is a normal subgroup. Thus $(hn)^{-1} \in HN$, so

HN $\leq$G.

Isomorphism Theorems

A similar argument shows that NH is a subgroup, so NH=H V N=HN.

Now suppose that H is also normal in G, and let h ∈ H, n ∈ N, and g ∈ G. Then

$ghng^{-1}=(ghg^{-1})(gng^{1}) \in HN$, so HN is indeed normal in G.

Group Theory

Second Isomorphism Theorem

Second Isomorphism Theorem

Theorem

Let H be a subgroup of G and let N be a normal subgroup of G. Then $(HN)/N \simeq H/(H \cap N)$.

Second Isomorphism Theorem

Proof

Let $y: G \to G/N$ be the canonical homomorphism and let $H \leq G$. Then $y[H]$ is a subgroup of G/N. Now the action of y on just the elements of H (called y **restricted to** H) provides us with a homomorphism mapping H onto $y[H]$, and the kernel of this restriction is clearly the set of elements of N that are also in H,

that is, the intersection $H \cap N$. By first isomorphism theorem, there is an isomorphism

$\mu_1: H/(H \cap N) \to y[H]$.

Second Isomorphism Theorem

On the other hand, y restricted to HN also provides a homomorphism mapping HN onto $y[H]$, because $y(n)$ is the identity N of G/N for all $n \in N$. The kernel of y restricted to HN is N. The first isomorphism theorem then provides us with an isomorphism

$\mu_2: (HN)/N \to y[H]$.

Because $(HN)/N$ and $H/(H \cap N)$ are both isomorphic to $y[H]$, they are isomorphic to each other. Indeed,

$\phi: (HN)/N \to H/(H \cap N)$ where $\phi = \mu_1^{-1}\mu_2$ will be an isomorphism. More explicitly,

$\Phi((hn)N) = \mu_1^{-1}(\mu_2((hn)N)) = \mu_1^{-1}(hN) = h(H \cap N)$.

Group Theory

Isomorphism Theorems

Isomorphism Theorems

Example

Let G be a group such that for some fixed integer

$n > 1$, $(ab)^n = a^n b^n$ for all $a, b \in G$. Let $G_n = \{a \in G \mid a^n = e\}$ and $G^n = (a^n \mid a \in G\}$.

Then $G_n \lhd G$, $G^n \lhd G$, and $G/G_n \simeq G^n$.

Isomorphism Theorems

Solution

Let $a, b \in G_n$ and $x \in G$. Then $(ab^{-1})^n = a^n(b^n)^{-1} = e$, so $ab^{-1} \in G_n$. Also, $(xax^{-1})^n = (xax^{-1})\ldots(xax^{-1}) = xa^nx^{-1} = e$ implies $xax^{-1} \in G_n$. Hence, $G_n \lhd G$.

Let $a, b, x \in G$. Then $a^n(b^n)^{-1} = (ab^{-1})^n \in G^n$.

Also, $xa^nx^{-1} = (xax^{-1})\ldots(xax^{-1}) = (xax^{-1})^n \in G^n$. Therefore, $G^n \lhd G$.

Group Theory

Isomorphism Theorems

Isomorphism Theorems

Example

Let G be a group such that for some fixed integer

n >1, $(ab)^n = a^n b^n$ for all a, b∈G. Let $G_n=\{a\in G | a^n=e\}$ and $G^n=\{a^n | a\in G\}$.

Then $G_n \lhd G$, $G^n \lhd G$, and $G/G_n \simeq G^n$.

Isomorphism Theorems

Define a mapping f: $G\to G^n$ by $f(a) = a^n$.

Then, for all a, b ∈ G, $f(ab)=(ab)^n=a^n b^n=f(a)f(b)$. Thus, f is a homomorphism.

Now Ker $f=\{a | a^n = e\}=G_n$. Therefore, by the first isomorphism theorem $G/G_n \simeq G^n$.

Isomorphism Theorems

Example

Let $G=\mathbb{Z}x\ \mathbb{Z}x\mathbb{Z}$, $H=\mathbb{Z}x\mathbb{Z}x\{0\}$, and $N=\{0\}x\mathbb{Z}x\mathbb{Z}$. Then clearly $HN=\mathbb{Z}x\mathbb{Z}x\mathbb{Z}$ and $H\cap N=\{0\}x\mathbb{Z}x\{0\}$. We have $(HN)/N\simeq \mathbb{Z}$ and we also have $H/(H\cap N)\simeq \mathbb{Z}$.

Group Theory

Third Isomorphism Theorem

Third Isomorphism Theorem

If H and K are two normal subgroups of G and $K\leq H$, then H/K is a normal subgroup of G/K.

The third isomorphism theorem concerns these groups.

Third Isomorphism Theorem

Theorem

Let H and K be normal subgroups of a group G with $K \leq H$.

Then $G/H \simeq (G/K)/(H/K)$.

Third Isomorphism Theorem

Proof

Let $\phi: G \to (G/K)/(H/K)$ be given by $\phi(a) = (aK)(H/K)$ for $a \in G$.

Clearly ϕ is onto $(G/K)/(H/K)$, and for $a, b \in G$,

$\phi(ab) = [(ab)K](H/K)$

$= [(aK)(bK)](H/K)$

$= [(aK)(H/K)][(bK)(H/K)] = \phi(a)\,\phi(b)$,

so ϕ is a homomorphism.

Third Isomorphism Theorem

The kernel consists of those $x \in G$ such that $\phi(x) = H/K$.

These x are just the elements of H.

Then first isomorphism theorem shows that $G/H \simeq (G/K)/(H/K)$.

Group Theory

Third Isomorphism Theorem

Third Isomorphism Theorem

A nice way of viewing third isomorphism theorem is to regard the canonical map $\gamma_H: G \to G/H$ as being factored via a normal subgroup K of G, $K \leq H \leq G$, to give

$\gamma_H = \gamma_{H/K}\gamma_K$, up to a natural isomorphism, as illustrated in Figure.

Third Isomorphism Theorem

$$
\begin{tikzcd}
G \arrow[r, "\gamma_H"] \arrow[d, "\gamma_K"'] & G/H \\
G/K \arrow[r, "\gamma_{H/K}"'] & (G/K)/(H/K) \arrow[u, "\text{Natural Isomorphism}"']
\end{tikzcd}
$$

Third Isomorphism Theorem

Another way of visualizing this theorem is to use the subgroup diagram in Figure, where each group is a normal subgroup of G and is contained in the one above it.

G
|
H
|
K

1027

Third Isomorphism Theorem

The larger the normal subgroup, the smaller the factor group.

Thus we can think of G collapsed by H, that is, G/H, as being smaller than G collapsed by K.

Third isomorphism theorem states that we can collapse G all the way down to G/H in two steps.

First, collapse to G/K, and then, using H/K, collapse this to (G/ K)/(H/K). The overall result is the same (up to isomorphism) as collapsing G by H.

1028

Group Theory

Third Isomorphism Theorem

1029

Third Isomorphism Theorem

Theorem

Let H and K be normal subgroups of a group G with K≤H.

Then $G/H \simeq (G/K)/(H/K)$.

1030

Third Isomorphism Theorem

Example

Consider

$K = 6\mathbb{Z} < H = 2\mathbb{Z} < G = \mathbb{Z}$.

Then $G/H = \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}_2$.
Now $G/K = \mathbb{Z}/6\mathbb{Z}$ has elements $6\mathbb{Z}$, $1+6\mathbb{Z}$, $2+6\mathbb{Z}$, $3+6\mathbb{Z}$, $4+6\mathbb{Z}$, and $5+6\mathbb{Z}$.

Of these six cosets, $6\mathbb{Z}$, $2+6\mathbb{Z}$, and $4+6\mathbb{Z}$ lie in $2\mathbb{Z}/6\mathbb{Z}$.

1031

Third Isomorphism Theorem

Thus $(\mathbb{Z}/6\mathbb{Z})/(2\mathbb{Z}/6\mathbb{Z})$ has two elements and is isomorphic to $\mathbb{Z}_2$ also.
Alternatively, we see that $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}_6$, and $2\mathbb{Z}/6\mathbb{Z}$ corresponds under this isomorphism to the cyclic subgroup $<2>$ of $\mathbb{Z}_6$.

Thus $(\mathbb{Z}/6\mathbb{Z})/(2\mathbb{Z}/6\mathbb{Z})$

$\simeq \mathbb{Z}_6/<2> \simeq \mathbb{Z}_2 \simeq \mathbb{Z}/2\mathbb{Z}$.

1032

Group Theory

Sylow Theorems

Sylow Theorems

The fundamental theorem for finitely generated abelian groups gives us complete information about all finite abelian groups. The study of finite nonabelian groups is much more complicated. The Sylow theorems give us some important information about them.

Sylow Theorems

We know the order of a subgroup of a finite group G must divide |G|. If G is abelian, then there exist subgroups of every order dividing |G|.

We showed that A_4, which has order 12, has no subgroup of order 6.

Thus a nonabelian group G may have no subgroup of some order d dividing |G|; the "converse of the theorem of Lagrange" does not hold.

Sylow Theorems

The Sylow theorems give a weak converse. Namely, they show that if d is a power of a prime and d divides |G|, then G does contain a subgroup of order d.

Note that 6 is not a power of a prime. The Sylow theorems also give some information concerning the number of such subgroups and their relationship to each other.

We will see that these theorems are very useful in studying finite nonabelian groups.

Sylow Theorems

Proofs of the Sylow theorems give us another application of action of a group on a set. This time, the set itself is formed from the group; in some instances the set is the group itself, sometimes it is a collection of cosets of a subgroup, and sometimes it is a collection of subgroups.

Group Theory

Sylow Theorems

Sylow Theorems

Let X be a finite G-set. Recall that for $x \in X$, the orbit of x in X under G is $Gx=\{gx \mid g \in G\}$. Suppose that there are r orbits in X under G, and let $\{x_1, x_2, \cdots, x_r\}$ contain one element from each orbit in X. Now every element of X is in precisely one orbit, so

$|X|=\sum_{i=1}^{r}|Gxi|$·

1039

Sylow Theorems

There may be one-element orbits in X.

Let $X_G=\{x \in X \mid gx=x \text{ for all } g \in G\}$.

Thus X_G is precisely the union of the one-element orbits in X.

Let us suppose there are s one-element orbits, where $0 \leq s \leq r$. Then $|X_G|=s$, and reordering the x_i if necessary, we may rewrite above equation as

$|X|=|X_G|+\sum_{i=s+1}^{r}|Gx_i|$.

Most of the results of these modules will flow from above equation.

1040

Sylow Theorems

Theorem

Let G be a group of order p^n and let X be a finite G-set. Then

$|X| \equiv |X_G| \pmod{p}$.

1041

Sylow Theorems

Proof

Recall $|X|=|X_G|+\sum_{i=s+1}^{r}|Gx_i|$.

In the notation of above Equation, we know that

$|Gx_i|$ divides $|G|$.

Consequently p divides $|Gx_i|$ for $s + 1 \leq i \leq r$. Above equation then shows that $|X|-|X_G|$ is divisible by p, so $|X| \equiv |X_G| \pmod{p}$.

1042

Sylow Theorems

Definition

Let p be a prime. A group G is a **p-group** if every element in G has order a power of the prime p.

A subgroup of a group G is a **p-subgroup of** G if the subgroup is itself a p-group.

1043

Group Theory

Cauchy's Theorem

1044

Cauchy's Theorem

Our goal in these modules is to show that a finite group G has a subgroup of every prime-power order dividing |G|.

As a first step, we prove Cauchy's theorem, which says that if p divides |G|, then G has a subgroup of order p.

1045

Cauchy's Theorem

Cauchy's Theorem

Let p be a prime. Let G be a finite group and let p divide |G|.

Then G has an element of order p and, consequently, a subgroup of order p.

1046

Cauchy's Theorem

Proof

We form the set X of all p-tuples $(g_1, g_2, \cdots, g_p)$ of elements of G having the property that the product of the coordinates in G is e. That is,

$X=\{(g_1, g_2, \cdots, g_p) \mid g_i \in G \text{ and } g_1 g_2 \cdots g_p = e\}$.

1047

Cauchy's Theorem

We claim p divides |X|. In forming a p-tuple in X, we may let $g_1, g_2, \cdots, g_{p-1}$ be any elements of G, and g_p is then uniquely determined as

$(g_1 g_2 \ldots g_{p-1})^{-1}$.

Thus $|X| = |G|^{p-1}$ and since p divides |G|, we see that p divides |X|. Let σ be the cycle (1, 2, 3,…, p) in S_p.

1048

Cauchy's Theorem

We let σ act on X by $\sigma(g_1, g_2, \ldots, g_p)$

$=(g_{\sigma(1)}, g_{\sigma(2)}, \ldots, g_{\sigma(p)}) = (g_2, g_3, \ldots, g_p, g_1)$.

Note that $(g_2, g_3, \ldots, g_p, g_1) \in X$, for $g_1(g_2 g_3 \ldots g_p)=e$ implies that $g_1 = (g_2 g_3 \ldots g_p)^{-1}$, so $(g_2 g_3 \ldots g_p) g_1 = e$ also. Thus σ acts on X, and we consider the subgroup $<\sigma>$

of S_p to act on X by iteration in the natural way.

1049

Cauchy's Theorem

Now $|<\sigma>| = p$, so we may apply above Theorem, and we know that $|X| \equiv |X_{<\sigma>}| \pmod{p}$. Since p divides |X|, it must be that p divides $|X_{<\sigma>}|$ also. Let us examine $X_{<\sigma>}$.

Now $(g_1, g_2, \ldots, g_p)$ is left fixed by σ, and hence by $<\sigma>$, if and only if $g_1 = g_2 = \ldots = g_p$. We know at least one element in $X_{<\sigma>}$, namely (e, e, …, e). Since p divides $|X_{<\sigma>}|$, there must be at least p elements in $X_{<\sigma>}$. Hence there exists some element $a \in G$, $a \neq e$, such that $(a, a, \ldots, a) \in X_{<\sigma>}$ and hence $a^p = e$, so a has order p. Of course, <a> is a subgroup of G of order p.

1050

Group Theory

Sylow Theorems

Sylow Theorems

Corollary

Let G be a finite group. Then G is a p-group if and only if |G| is a power of p.

Sylow Theorems

Let G be a group, and let $\mathcal{S}$ be the collection of all subgroups of G.

We make $\mathcal{S}$ into a G-set by letting G act on $\mathcal{S}$ by conjugation.

That is, if $H \in \mathcal{S}$ so $H \leq G$ and $g \in G$, then g acting on H yields the conjugate subgroup gHg^{-1}.

Sylow Theorems

Now $G_H=\{g \in G \mid gHg^{-1}=H\}$ is easily seen to be a subgroup of G, and H is a normal subgroup of G_H. Since G_H consists of all elements of G that leave H invariant under conjugation, G_H is the largest subgroup of G having H as a normal subgroup.

Sylow Theorems

Definition

The subgroup

$G_H = \{g \in G \mid gHg^{-1}=H\}$

is the normalizer of H in G and is denoted by N[H].

Sylow Theorems

Lemma

Let H be a p-subgroup of a finite group G. Then $(N[H]:H) \equiv (G:H) \pmod{p}$.

Sylow Theorems

Proof

Let $\mathcal{L}$ be the set of left cosets of H in G, and let H act on $\mathcal{L}$ by left translation, so that h(xH) = (hx)H. Then $\mathcal{L}$ becomes an H-set. Note that $|\mathcal{L}|$=(G:H).

Let us determine $\mathcal{L}_H$, that is, those left cosets that are fixed under action by all elements of H.

Now xH= h(xH) if and only if H=x^{-1}hxH, or if and only if $x^{-1}hx \in$ H.

1057

Sylow Theorems

Thus xH=h(xH) for all h∈H if and only if $x^{-1}hx$ $=x^{-1}h(x^{-1})^{-1}\in$H for all h∈H, or if and only if $x^{-1}\in$N[H], or if and only if x∈N[H]. Thus the left cosets in $\mathcal{L}_H$ are those contained in N[H]. The number of such cosets is (N[H]:H), so $|\mathcal{L}_H|$ = (N[H]:H).

Since H is a p-group, it has order a power of p. Then $|\mathcal{L}| \equiv |\mathcal{L}_H|$ (mod p), that is,

(G:H) ≡ (N[H]:H) (mod p).

1058

Group Theory

First Sylow Theorem

1059

First Sylow Theorem

Theorem

Let G be a finite group and let $|G| = p^n m$ where $n\geq 1$ and where p does not divide m. Then

1. G contains a subgroup of order p^i for each i where $1\leq i\leq n$,

2. Every subgroup H of G of order p^i is a normal subgroup of a subgroup of order p^{i+1} for $1 \leq i < n$.

1060

First Sylow Theorem

Proof

We know G contains a subgroup of order p by Cauchy's theorem.

We use an induction argument and show that the existence of a subgroup of order p^i for $i<n$ implies the existence of a subgroup of order p^{i+1}.

1061

First Sylow Theorem

Let H be a subgroup of order p^i. Since i < n, we see p divides (G:H). We then know p divides (N[H]:H).

Since H is a normal subgroup of N[H], we can form N[H]/H, and we see that p divides |N[H]/H|.

By Cauchy's theorem, the factor group N[H]/H has a subgroup K which is of order p.

If γ:N[H]→N[H]/H is the canonical homomorphism, then $\gamma^{-1}[K]=\{x\in N[H] \mid \gamma(x)\in K\}$ is a subgroup of N[H] and hence of G. This subgroup contains H and is of order p^{i+1}.

1062

First Sylow Theorem

2. We repeat the construction in part 1 and note that $H < \gamma^{-1}[K] \leq N[H]$ where $|\gamma^{-1}[K]| = p^{i+1}$.

Since H is normal in N[H], it is of course normal in the possibly smaller group $\gamma^{-1}[K]$.

1063

First Sylow Theorem

Definition

A Sylow p-subgroup P of a group G is a maximal

p-subgroup of G,

that is,

a p-subgroup contained in no larger p-subgroup.

1064

Group Theory

Second Sylow Theorem

1065

Second Sylow Theorem

Let G be a finite group, where $|G|=p^n m$ as in first Sylow theorem.

The theorem shows that the Sylow p-subgroups of G are precisely those subgroups of order p^n.

If P is a Sylow p-subgroup, every conjugate gPg^{-1} of P is also a Sylow p-subgroup.

1066

Second Sylow Theorem

The second Sylow theorem states that every Sylow p-subgroup can be obtained from P in this fashion; that is, any two Sylow p-subgroups are conjugate.

1067

Second Sylow Theorem

Theorem

Let P_1 and P_2 be Sylow p-subgroups of a finite group G.

Then P_1 and P_2 are conjugate subgroups of G.

1068

Second Sylow Theorem

Proof

Here we will let one of the subgroups act on left cosets of the other. Let $\mathcal{L}$ be the collection of left cosets of P_1, and let P_2 act on $\mathcal{L}$ by $z(xP_1)=(zx)P_1$ for $z \in P_2$. Then $\mathcal{L}$ is a P_2-set. We have $|\mathcal{L}_{P_2}| \equiv |\mathcal{L}|$ (mod p), and $|\mathcal{L}|=(G: P_1)$ is not divisible by p, so $|\mathcal{L}_{P_2}| \neq 0$. Let $xP_1 \in \mathcal{L}_{P_2}$.

Then $zxP_1=xP_1$ for all $z \in P_2$, so $x^{-1}zxP_1=P_1$ for all $z \in P_2$. Thus $x^{-1}zx \in P_1$ for all $z \in P_2$, so $x^{-1}P_2x \leq P_1$.

Since $|P_1|=|P_2|$, we must have $P_1=x^{-1}P_2x$, so P_1 and P_2 are indeed conjugate subgroups.

1069

Group Theory

Third Sylow Theorem

1070

Third Sylow Theorem

The final Sylow theorem gives information on the number of Sylow p-subgroups.

Theorem

If G is a finite group and p divides |G|, then the number of Sylow p-subgroups is congruent to 1 modulo p and divides |G|.

1071

Third Sylow Theorem

Proof

Let P be one Sylow p-subgroup of G. Let $\mathcal{S}$ be the set of all Sylow p-subgroups and let P act on $\mathcal{S}$ by conjugation, so that $x \in P$ carries $T \in \mathcal{S}$ into xTx^{-1}.

We have $|\mathcal{S}| \equiv |\mathcal{S}_P|$(mod p). Let us find $\mathcal{S}_P$.

If $T \in \mathcal{S}_P$, then $xTx^{-1}=T$ for all $x \in P$. Thus $P \leq N[T]$.

Of course $T \leq N[T]$ also.

Since P and T are both Sylow p-subgroups of G, they are also Sylow p-subgroups of N[T].

But then they are conjugate in N[T] by second Sylow theorem.

1072

Third Sylow Theorem

Since T is a normal subgroup of N[T], it is its only conjugate in N[T]. Thus T=P.

Then $\mathcal{S}_P=\{P\}$. Since $|\mathcal{S}| \equiv |\mathcal{S}_P|=1$ (mod p), we see the number of Sylow p-subgroups is congruent to 1 modulo p.

Now let G act on $\mathcal{S}$ by conjugation. Since all Sylow p-subgroups are conjugate, there is only one orbit in $\mathcal{S}$ under G.

If $P \in \mathcal{S}$ then $|\mathcal{S}|=|\text{orbit of } P|=(G:G_P)$. G_P is, in fact, the normalizer of P. But $(G:G_P)$ is a divisor of |G|, so the number of Sylow p-subgroups divides |G|.

1073

Group Theory

Sylow Theorems

1074

Sylow Theorems

Example

The Sylow 2-subgroups of S_3 have order 2.

The subgroups of order 2 in S_3 are

$\{\rho_0, \mu_1\}$, $\{\rho_0, \mu_2\}$, $\{\rho_0, \mu_3\}$.

Note that there are three subgroups and that

$3 \equiv 1 \pmod 2$.

1075

Sylow Theorems

Also, 3 divides 6, the order of S_3.

We can readily check that

$i_{\rho_2}[\{\rho_0, \mu_1\}]=\{\rho_0, \mu_3\}$ and $i_{\rho_1}[\{\rho_0, \mu_1\}]=\{\rho_0, \mu_2\}$

where $i_{\rho_j}(x)=\rho_j x \rho_j^{-1}$, illustrating that they are all conjugate. For instance, $i_{\rho_2}(\mu_1)=\rho_2\mu_1\rho_2^{-1}=\rho_2\mu_1\rho_1=$ $(1,3,2)(2,3)(1,2,3)=(1,2)=$ μ_3.

1076

Sylow Theorems

Example

Let us use the Sylow theorems to show that no group of order 15 is simple. Let G have order 15.

We claim that G has a normal subgroup of order 5.

By first Sylow theorem G has at least one subgroup of order 5, and by third Sylow theorem the number of such subgroups is congruent to 1 modulo 5 and divides 15. Since 1, 6, and 11 are the only positive numbers less than 15 that are congruent to 1 modulo 5, and since among these only the number 1 divides 15, we see that G has exactly one subgroup P of order 5.

1077

Sylow Theorems

But for each $g \in G$, the inner automorphism i_g of G with $i_g(x)=gxg^{-1}$ maps P onto a subgroup gPg^{-1}, again of order 5.

Hence we must have

$gPg^{-1}=P$ for all $g \in G$, so P is a normal subgroup of G.

Therefore, G is not simple.

1078

Group Theory

Application of Sylow Theory

1079

Application of Sylow Theory

Let X be a finite G-set where G is a finite group. Let $X_G=\{x \in X \mid gx=x \text{ for all } g \in G\}$. Then

$|X|=|X_G|+\sum_{i=s+1}^{r}|Gx_i|$, where x_i is an element in the ith orbit in X.

1080

Application of Sylow Theory

Consider now the special case of above equation, where X=G and the action of G on G is by conjugation, so $g \in G$ carries $x \in X = G$ into gxg^{-1}.
Then $X_G=\{x \in G \mid gxg^{-1}=x \text{ for all } g \in G\}$

$= \{x \in G \mid xg=gx \text{ for all } g \in G\}=Z(G)$, the center of G.

If we let $c=|Z(G)|$ and $n_i=|Gx_i|$ in above equation, then we obtain $|G|=c+n_{c+1}+\ldots+n_r$, where n_i is the number of elements in the ith orbit of G under conjugation by itself.

Note that n_i divides $|G|$ for $c+1\le i \le r$ since we know $|Gx_i|=(G: G_{x_i})$, which is a divisor of $|G|$.

Application of Sylow Theory

Definition

The equation $|G|=c+n_{c+1}+\ldots+n_r$, where $c=|Z(G)|$ and n_i is the number of elements in the ith orbit of G under conjugation by itself, is the class equation of G.

Each orbit in G under conjugation by G is a conjugate class in G.

Application of Sylow Theory

Example

$i_{\rho_1}(\rho_0)=\rho_1\rho_0\rho_1^{-1}=\rho_0$ $\quad i_{\mu_1}(\rho_1)=\mu_1\rho_1\mu_1^{-1}=\rho_2$

$i_{\mu_1}(\rho_2)=\mu_1\rho_2\mu_1^{-1}=\mu_1\rho_2\mu_1=\rho_1$

$i_{\rho_1}(\mu_1)=\rho_1\mu_1\rho_1^{-1}=(1,2,3)(2,3)(1,3,2)=(1,3)=\mu_2$

$i_{\rho_1}(\mu_2)=\rho_1\mu_2\rho_1^{-1}=\mu_3$ $\quad i_{\rho_1}(\mu_3)=\rho_1\mu_3\rho_1^{-1}=\mu_1$

Therefore, the conjugate classes of S_3 are

$\{\rho_0\}$, $\{\rho_1, \rho_2\}$, $\{\mu_1, \mu_2, \mu_3\}$.

The class equation of S_3 is $6 = 1+2+3$.

Application of Sylow Theory

Theorem

The center of a finite nontrivial p-group G is nontrivial.

Application of Sylow Theory

Proof

We have $|G|=c+n_{c+1}+\ldots+n_r$, where n_i is the number of elements in the ith orbit of G under conjugation by itself.

For G, each n_i divides $|G|$ for $c+1\le i\le r$, so p divides each n_i, and p divides $|G|$. Therefore p divides c. Now $e\in Z(G)$, so $c\ge 1$. Therefore $c\ge p$, and there exists some $a\in Z(G)$ where $a\ne e$.

Group Theory

Application of Sylow Theory

Application of Sylow Theory

Lemma

Let G be a group containing normal subgroups H and K such that $H \cap K = \{e\}$ and

$H \vee K = G$. Then G is isomorphic to $H \times K$.

Application of Sylow Theory

Proof

We start by showing that hk=kh for $k \in K$ and $h \in H$. Consider the commutator

$hkh^{-1}k^{-1}=(hkh^{-1})k^{-1}=h(kh^{-1}k^{-1})$.

Since H and K are normal subgroups of G, the two groupings with parentheses show that $hkh^{-1}k^{-1}$ is in both K and H.

Since $K \cap H=\{e\}$, we see that $hkh^{-1}k^{-1}=e$, so hk=kh.

Application of Sylow Theory

Let $\phi: H \times K \rightarrow G$ be defined by $\phi(h,k) = hk$.

Then $\phi((h, k)(h', k'))=\phi(hh', kk')=hh'kk'= hkh'k'$

$=\phi(h, k)\, \phi(h', k')$, so ϕ is a homomorphism.

If $\phi(h, k)=e$, then $hk=e$, so $h = k^{-1}$, and both h and k are in $H \cap K$. Thus $h=k=e$, so $Ker(\phi)=\{(e, e)\}$ and ϕ is one to one.

We know that $HK=H \vee K$, and $H \vee K = G$ by hypothesis.

Thus ϕ is onto G, and $H \times K \simeq G$.

Group Theory

Application of Sylow Theory

Application of Sylow Theory

Theorem

For a prime number p, every group G of order p^2 is abelian.

Application of Sylow Theory

Proof

If G is not cyclic, then every element except e must be of order p.

Let a be such an element. Then the cyclic subgroup <a> of order p does not exhaust G.

Also let $b \in G$ with $b \notin \langle a \rangle$. Then $\langle a \rangle \cap \langle b \rangle=\{e\}$, since an element c in $\langle a \rangle \cap \langle b \rangle$ with $c \neq e$ would generate both <a> and <b>, giving $\langle a \rangle=\langle b \rangle$, contrary to construction.

Application of Sylow Theory

From first Sylow theorem, <a> is normal in some subgroup of order p^2 of G, that is, normal in all of G. Likewise <b> is normal in G.

Now <a> V <b> is a subgroup of G properly containing <a> and of order dividing p^2.

Hence <a> V <b> must be all of G.

Thus the hypotheses of last lemma are satisfied, and G is isomorphic to <a> x <b> and therefore abelian.

1093