Abstract Algebra

1/5/11

- Read ahead for Friday: Chap 2, Pinter

- abstract algebra:
  Goes from familiar examples to abstract properties of those examples. Leads to new examples and theory

Ex: 1) Integers $\mathbb{Z}$ $0, \pm 1, \pm 2, \pm 3 \ldots$
Natural numbers $\mathbb{N}$ $1, 2, 3, 4 \ldots$

- Key properties of $\mathbb{Z}$
  - can add two integers and get another one
  - can multiply two integers and get another one
  - any number plus zero is just that number
  - any number plus its negative is zero

- Any abstract object satisfying such properties will be called a <u>ring</u>. You can't divide though! In particular, not by zero, Also $\frac{2}{3}$ isn't an integer.

2) Fixing Division (kind of)
Rational numbers $\mathbb{Q}$
$= \{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \}$
Real numbers $\mathbb{R}$
- "completion" of the rationals

In both cases, division (except by zero) is allowed

- If $x \neq 0$ is a real number, then $\frac{1}{x}$ is a real number, and $x \cdot \frac{1}{x} = 1$ (inverse w/respect to $*$)
- the abstraction (ring with inverses for multiplication) is called a <u>field</u>.

3) Consider all 2 x 2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$
with $a, b, c, d \in \mathbb{R}$ or $\mathbb{C}$
concentrate only on invertible matrices ($ad-bc \neq$

- If A and B are invertible (with respect to multiplication), then AB is also invertible. The inverse of AB is $B^{-1}A^{-1}$ (A^{-1} and B^{-1} are the inverses for A and B respectively)

- If A and B are invertible A + B is not always invertible!
ex: let $B = -A$
$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ $\Rightarrow A + B = 0$

- If you can multiply but not necessarily add, the abstractification is called a group

4.) Factoring polynomials (w/integer coefficients)
Let P be a polynomial and let n be its degree. Is there an algorithm for finding zeros of P?
0. $n=0$ stupid
1. $n=1$ trivial (linear)
2. $n=2$ quadratic formula
3. $n=3$ too long takes 1/2 a page
4. $n=4$ extra long takes a whole page
5. $n=5$ and higher - no formula is possible (Abel 1824) using abstract Alge

Motivation: 1/7/11

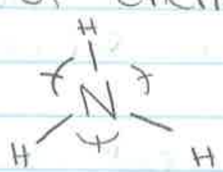
Why do abstract algebra?

Applications:

1) Quantum Mechanics
Given Shrödinger equation: $\left(-\frac{\hbar^2}{2m}\nabla^2 + V(x)\right)\Psi(x) = E\Psi(x)$

Symmetry properties (group properties) of the equation can yield understanding of solutions without explicitly solving the equation.

2) Symmetry groups of chemical compounds.
Ammonia



- rotational symmetry by 120° rotation
- reflection symmetry about vertical axis

- Can compose symmetries - the resulting output is a symmetry group
- The group has 6 elements and is denoted by S_3, D_6 (dihedral), or C_{3v} (chemistry)

3) Cryptography (code-making + code-breaking)
RSA algorithm - based on modular arithmetic
cryptography mainly utilizes finite groups

5) as a tool for doing other mathematics!

Begin Course with <u>Chapter 2</u> in Pinter

<u>Binary Operations</u>

Let S be a set.

<u>Def:</u> A (binary) operation is a function $B: S \times S \to S$
In other words, if $a, b \in S$, then
$B(a,b)$ is also in S.
Note: $B(a,b)$ isn't necessarily equal to $B(b,a)$

<u>Exs:</u> 1) addition is a binary operation on,
$\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{N}$, $\mathbb{C}$
If a, b are in any of the above sets,
then so is $B(a,b) = a+b$

2) Division is <u>not</u> a binary operation on $\mathbb{Z}$.
Define for $n, m \in \mathbb{Z}$
$B(n,m) = \frac{n}{m}$, then unless m divides n,
$\frac{n}{m} \notin \mathbb{Z}$. in particular, $\frac{n}{0}$ never defined

<u>Properties of Binary operations:</u>

- first, if $a, b \in S$ and B is a binary operation,
shorthand $B(a,b)$ as $a * b$

- Denote S with binary operation B by $(S, *)$
1) $(S, *)$ is associative if for all $a, b, c \in S$,
$(a * b) * c = a * (b * c)$
[perenthesis don't matter]

2) $(S, *)$ is commutative if for all $a, b \in S$
$a * b = b * a$ (order of operations doesn't matter)

3) $(S, *)$ has an identity element e if for all $a \in S$, $e * a = a * e = a$

4) If $(S, *)$ has an identity element then $a \in S$ is <u>invertible</u> w/ respect to "$*$" if there exists $a^{-1} \in S$ such that
$$a^{-1} * a = a * a^{-1} = e$$

call a^{-1} the inverse of a.

<u>Exs:</u> Given a set S with binary operation "$*$", which of the preceding four properties (associativity, commutative, identity, + inverses) does $(S, *)$ posses?

1) $S = \mathbb{R}$
a) $* = +$
$(\mathbb{R}, +)$ is associative and commutative)
Identity $= 0$, Inverse of $x \in \mathbb{R} = -x$
b) throw out $x = 0$, consider $* = \cdot$ $(\mathbb{R} \setminus \{0\})$
$(\mathbb{R} \setminus \{0\}, \cdot)$ is associative and commutative
Identity $= 1$, inverse of $x \in \mathbb{R} \setminus \{0\} = 1/x$

2) Multiplication $= *$ on $S = \mathbb{Z} \setminus \{0\}$, $S \subseteq \mathbb{R} \setminus \{0\}$, so $(\mathbb{Z} \setminus \{0\}, \cdot)$ is associative, commutative, with identity 1.
However, only two elements $(x = \pm 1)$ have inverse

3) $S =$ 2×2 matrix with real coefficients.
$* =$ matrix multiplication $(S, *)$ is associative since "$*$" is function composition, but not commutative, Identity $= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has an inverse iff $ad - bc \neq 0$

← cont.

1/10/11

Exs:

- $\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$
  consider $\langle \mathbb{Z}, \cdot \rangle$

- matrix mult. on $M_2(\mathbb{R})$.
  consider $\langle M_2(\mathbb{R}), * \rangle$
  set $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$
  - Identity is $e = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
  - Not commutative: Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$
    Then $AB \neq BA$
  - inverse DNE
    consider $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

- Table on a finite set
  $S = \{a, b, c\}$
  Table:

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

This is a group →

Commutative:
$b * c = a$
$c * b = a$
associative:
yes

Identity element $= a$
inverse: $b^{-1} = c$, $c^{-1} = b$, $a^{-1} = a$

Chapter 3

The Definition of a Group:

Def: A group is a set G with operation $*$ that satisfies the following:

(G1) $*$ is associative

(G2) $\exists$ an element $e \in G \ni a * e = a$ and $e * a = a \ \forall a \in G$

(G3) $\forall$ element $a \in G \ \exists \ a^{-1} \in G \ni a * a^{-1} = e$ and $a^{-1} * a = e$

A group is often denoted by $\langle G, * \rangle$ or simply G

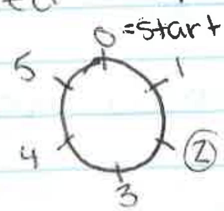
$Q^* =$ non-zero rational numbers

Exs:

$$\left.\begin{array}{ll} \text{i)} & \langle \mathbb{Z}, + \rangle \\ \text{ii)} & \langle \mathbb{Q}, + \rangle \\ \text{iii)} & \langle \mathbb{R}, + \rangle \\ \text{iv)} & \langle \mathbb{Q}^*, \cdot \rangle \\ \text{v)} & \langle \mathbb{R}^*, \cdot \rangle \\ \text{vi)} & \langle \mathbb{Q}^{pos}, \cdot \rangle \\ \text{vii)} & \langle \mathbb{R}^{pos}, \cdot \rangle \end{array}\right\} \text{examples of groups.}$$

Ex: The group of integers of modulo 6.
$S = \{0, 1, \dots, 5\}$ and the operation of addition modulo 6.
For $h, k \in S$, defined $h +_6 k =$ remainder of: $h+k$ divided by 6

ex/ $5 +_6 3 = 2$



Ex: The group of integers modulo 3.

$S = \{0, 1, 2\}$ $\quad \langle S, +_3 \rangle$

group table:

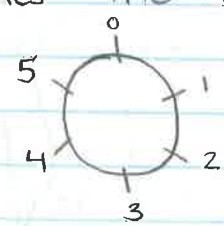
$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\varphi(0) = a$
$\varphi(1) = b$
$\varphi(2) = c$
$\varphi(n +_3 m) = \varphi(n) * \ell(m)$

1/12/11

Further examples of groups

1) Recall $\mathbb{Z}_6$ denotes the cyclic group of order 6 "clock" form

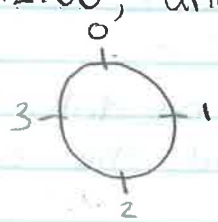


rotations by multiples of $60°$

Generalize to $\mathbb{Z}_n$

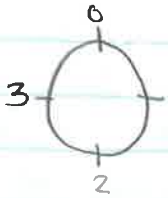
- n hash marks around the circle, identity at 12:00, and hashes are spaced at $\frac{360}{n}$ degrees

ex: $\mathbb{Z}_4$



- Consider as rotations about the circle's center, multiples of $\frac{360°}{n}$
- This is a binary operation (composition of rotations)
- Check:
  - Associativity
  - identity
  - inverse.

ex: $\mathbb{Z}_4$



- identity: rotation at $0°$ (don't move)
- Inverse: rotate by multiple m of $\frac{360°}{n}$, is there a way to get back to 12:00 by some multiple of $\frac{360°}{n}$?

Rotate by $\frac{360°}{n} \cdot m$

Inverse would be: $\frac{360}{n} \cdot (n-m)$

m rotations of $\frac{360°}{n}$ followed by $(n-m)$ rotations of $\frac{360°}{n}$ is: $m + (n-m) = n$ rotations of $\frac{360°}{n}$

$= 360°$ (12:00)

- Associativity: rotate: $\left(\frac{360°}{n} \cdot m\right)$ then $\left(\frac{360°}{n} \cdot k\right)$ finally $\left(\frac{360°}{n} \cdot l\right)$

① $\left(\frac{360°}{n} \cdot l\right)\left(\left(\frac{360°}{n} \cdot m\right)\left(\frac{360°}{n} \cdot k\right)\right)$

Same as

② $\left(\left(\frac{360°}{n} \cdot l\right)\left(\frac{360°}{n} \cdot m\right)\right)\left(\frac{360°}{n} \cdot k\right)$? YES

① 1st do $\frac{360°}{n}(k+m)$ rotations, then do $\frac{360°}{n} \cdot l$ rotations, for a total of $\frac{360°}{n}(k+m+l)$.

② exactly $\frac{360°}{n}(k+m+l)$

So associativity holds.

Note: $\mathbb{Z}_n$ is commutative

Think of $\mathbb{Z}_n$ as $\{0,1,2 \ldots n-1\}$ with additive structure

Using same structure, when is $\mathbb{Z}_n \setminus \{0\}$ a group under multiplication?

ex: let S be any set.

A bijection from S to itself is a map $\phi : S \to S$ such that the range of ϕ is all of S (surjectivity) and if $\phi(t) = \phi(r)$ for $t, r \in S$, then $t = 3$ (injective)

($S = \mathbb{R}$ $\phi(x) = x$ is a bijection but $\phi(x) = x^2$ is not)

let G be the set of all bijections on S.

Binary operation: function composition "$\circ$"

Claim: $\langle G, \circ \rangle$ is a group.

- Associativity follows from the fact that function composition is associative

- Identity: for $t \in S$ define $\phi(t) = t$

  If $\psi \in G$, is it true that:

  $(\psi \circ \phi)(t) = (\phi \circ \psi)(t) = \psi(t)$?

  check: $(\psi \circ \phi)(t)$

  $= \psi(\phi(t)) = \psi(t)$

  and $(\phi \circ \psi)(t)$

  $= \phi(\psi(t)) = \psi(t)$ ✓

- Inverse: Let $\psi \in G$. Need to find $\psi^{-1} \ni$

  $(\psi \circ \psi^{-1})(t) = (\psi^{-1} \circ \psi)(t) = t$

  Define ψ^{-1} as follows:

  let $t \in S$. Since ψ is bijective, there is a ! element $r \in S$ with $\psi(r) = t$

  Define $\psi^{-1}(t) = r$

  check: $(\psi \circ \psi^{-1})(t) = \psi(\psi^{-1}(t)) = \psi(r) = t$

  and $(\psi^{-1} \circ \psi)(t) = t$

Note: ψ^{-1} is bijective since ψ is bijective

If $|S| = n$ (number of elements in S is n)
then denote $\langle G, \circ \rangle$ by S_n

What is $|S_n|$?
$n = 3$
$S = \{a, b, c\}$
$\varphi: S \to S$ is a bijection
- How many choices do you have for $\varphi(a)$? 3
- After that choice, How many choices are left for $\varphi(b)$? Two - anywhere not equal to $\varphi(a)$
- only one choice for $\varphi(c)$

That is $3 \cdot 2 \cdot 1 = 3!$ choices for bijections
$\Rightarrow |S_n| = n!$

1/14/11

Mentoring Hours:	
MW	1:30 - 3:30
F	11:30 - 1:30

MLC silent study room
2070

How to show a group is not commutative:

ex: G = all invertible 2×2 matrices, usual matrix multiplication, entries in $\mathbb{R}$.
Is the multiplication commutative? NO

$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$

$\det(A) \neq 0 \neq \det(B)$

$AB = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$

$BA = \begin{pmatrix} b_{11}a_{11} + b_{12}a_{21} & b_{11}a_{12} + b_{12}a_{22} \\ b_{21}a_{11} + b_{22}a_{21} & b_{21}a_{12} + b_{22}a_{22} \end{pmatrix}$

In order for AB to equal BA, we need every entry of AB to equal the corresponding entry in BA

Entry in 1^{st} row & 1^{st} column
AB entry $a_{11}b_{11} + a_{12}b_{21}$
BA entry $b_{11}a_{11} + b_{12}a_{21}$
If these were equae,
$\cancel{a_{11}b_{11}} + a_{12}b_{21} = b_{11}a_{11} + b_{12}a_{21}$
$= \cancel{a_{11}b_{11}} + b_{12}a_{21}$
Need $a_{12}b_{21} = b_{12}a_{21}$,
does this always happen?
Find an invertible matrix A and B
with $a_{12}b_{21} \neq b_{12}a_{21}$
ex: $A = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}$ is invertible
$a_{12} = a_{21} = 1$
$B = \begin{pmatrix} 2 & 4 \\ 6 & 8 \end{pmatrix}$ is invertible
$b_{12} = 4 \quad b_{21} = 6$
so, $a_{12}b_{21} = 6$
$a_{21}b_{12} = 4$ } $6 \neq 4$ so the matrices A + B do not commute ☒

How to show a binary operation does not have an identity:

ex: $S = \mathbb{N}$
(Binary) operation $*$
$n, m \in \mathbb{N}$, $n * m = 2^{n+m}$
"$*$" is commutative
since, $m * n = 2^{m+n} = 2^{n+m} = n*m$
This is a binary operation, is there an identity?
Suppose there is an identity e.
If e is an identity for '$*$', then $n*e = e*n = n \ \forall n$
$n*e = 2^{n+e}$
Choose $n=1$, need $1*e = 1$, but $1*e = 2^{1+e}$ →

so we need $2^{1+e} = 1$, so we would have to have $e = -1$ but $-1 \notin \mathbb{N}$
So there is no identity in the $\mathbb{N}$ $\blacksquare$

To show no identity at all;

$3 * e = 3$

$\quad 2^{3+e}$

from previous calculation, with $n=1$, $e=-1$
so then,

$$3 = 2^{3-1} = 2^2 = 4$$

$\therefore 3 \neq 4$ $\therefore$ no identity possible

GROUP PROPERTIES

Proposition: Let $\langle G, * \rangle$ be a group.

1) there is only one identity element
2) every $g \in G$ has only one inverse

ie.: identity and inverse are unique.

Proof: see Pinter page 36

Interesting: External Direct Products

Thm: Let $\langle G, * \rangle$ and $\langle H, \star \rangle$ be two groups with identities e_G and e_H respectively. Consider the set $G \times H$ = all ordered pairs of the form (g, h) with $g \in G$ and $h \in H$. Define a binary operation "$\cdot$" on $G \times H$ by
$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 \star h_2)$
$\forall g_1, g_2 \in G$ and $h_1, h_2 \in H$
Then $\langle G \times H, \cdot \rangle$ is also a group $\rightarrow$

Proof: $(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2 , h_1 \star h_2)$
This is a binary operation since, $g_1 * g_2 \in G$ and $h_1 \star h_2 \in H$ as $\langle G, * \rangle$ and $\langle H, \star \rangle$ are groups.
Hence, $(g_1 * g_2 , h_1 \star h_2) \in G \times H$

Associativity:

let $g_3 \in G$, $h_3 \in H$

$(g_1, h_1) \cdot ((g_2, h_2) \cdot (g_3, h_3))$
$= (g_1, h_1) \cdot ((g_2 * g_3 , h_2 \star h_3))$
$= (g_1 * (g_2 * g_3), h_1 \star (h_2 \star h_3))$
$= ((g_1 * g_2) * g_3 , (h_1 \star h_2) \star h_3)$
[Since G + H are associative]
$= (g_1 * g_2 , h_1 \star h_2) \cdot (g_3 , h_3)$
$= ((g_1, h_1) \cdot (g_2, h_2)) \cdot (g_3, h_3)$ ✓

Identity:

$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2 , h_1 \star h_2)$
Recall, e_G, e_H are the identities of G + H
Claim: $e = (e_G , e_H)$ is the identity of $\langle G \times H , \cdot \rangle$
let $g \in G$ and $h \in H$, then
$(e_G, e_H) \cdot (g, h)$
$= (e_G * g , e_H \star h)$
$= (g, h)$
$(g, h) \cdot (e_G , e_H)$
$= (g * e_G , h \star e_H)$
$= (g , h)$ ✓

Inverse:

$(g, h)^{-1} = (g^{-1}, h^{-1})$
Check: $(g, h) \cdot (g^{-1}, h^{-1})$
$= (g * g^{-1}, h \star h^{-1}) = (e_G, e_H)$
and $(g^{-1}, h^{-1}) \cdot (g, h)$
$= (g^{-1} * g , h^{-1} \star h) = (e_G , e_H)$

Terminology & Notation

1/19/11

1) The notation $(G, \cdot)$ will denote a group G with binary operation "$\cdot$".
Warning: "$\cdot$" is not necessarily multiplication

2) If $(G, \cdot)$ is commutative, we say $(G, \cdot)$ (or simply G) is abelian after Neils Henrik Abel.

examples:

- $(\mathbb{R}, +)$ or $\mathbb{Z}_n$ are abelian groups
- invertible 2×2 matrices with real or complex entries is not abelian
- S_3 (bijections on a 3 element set) is not abelian.

Pf: recall that S_3 has $3! = 6$ elements.
recall also that the group operation is function composition.
let our 3 element set be $\{1, 2, 3\}$
define an element $\varphi \in S_3$ by
$\varphi(1) = 2$, $\varphi(2) = 3$, $\varphi(3) = 1$
define $\psi \in S_3$ by:
$\psi(1) = 2$, $\psi(2) = 1$, $\psi(3) = 3$
If $\psi \circ \varphi = \varphi \circ \psi$, then
$(\psi \circ \varphi) n = (\varphi \circ \psi)(n) \quad \forall n \in \{1, 2, 3\}$
Try $n = 2$, $(\psi \circ \varphi)(2)$
$= \psi(\varphi(2))$
$= \psi(3) = 3$
and $(\varphi \circ \psi)(2)$
$= \varphi(\psi(2)) = \varphi(1) = 2$
Since $2 \neq 3$, $\varphi \circ \psi \neq \psi \circ \varphi$

- We will show later in class that S_3 is the smallest group which is not abelian.

Chapter 9 in Pinter : Isomorphism

Def: let $(G, \cdot)$ and $(H, *)$ be groups.
A map $\varphi : G \to H$ is called an isomorphism if φ is bijective and for all $g_1, g_2 \in G$,
$\varphi(g_1 \cdot g_2) = \varphi(g_1) * \varphi(g_2)$

If there exists an isomorphism $\varphi : (G, \cdot) \to (H, *)$, we say that $(G, \cdot)$ and $(H, *)$ are isomorphic.

Examples

1). let $\{a, b, c, d\}$ be a four-element set. create 2 group structures using two tables of operation

	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	d	b
d	d	c	b	a

	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

call the first table $(G, \cdot)$ and the second $(G, *)$
Define an isomorphism $\varphi : (G, \cdot) \to (G, *)$ by:

$\varphi(a) = a$
$\varphi(b) = b$ clearly φ is a bijection.
$\varphi(c) = d$
$\varphi(d) = c$

for any element $n \in \{a, b, c, d\}$,
$\varphi(n \cdot a) = \varphi(n) = \varphi(n) \cdot a = \varphi(n) \cdot \varphi(a)$
can check in general that, $\varphi(n \cdot m) = \varphi(n) * \varphi(m)$ for all $n, m \in \{a, b, c, d\}$

2) Consider an operation table on $\{a, b, c, d\}$

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Lets show that $\{a, b, c, d\}$ with this operation is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.
Write the elements of $\mathbb{Z}_2$ as $\{0, 1\}$
then $\mathbb{Z}_2 \times \mathbb{Z}_2$ is:

$(0, 0)$, $(1, 0)$, $(0, 1)$, $(1, 1)$

with addition on coordinates, convention $1+1=0$.

$(1, 0) + (1, 0) = (1+1, 0) = (0, 0)$

Similarly, $(0, 1)$ and $(1, 1)$ are their own inverses. Define $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \{a, b, c, d\}$

$\varphi((0,0)) = a$ $\qquad$ $\varphi((0,1)) = c$

$\varphi((1,0)) = b$ $\qquad$ $\varphi((1,1)) = d$

Then check if this is an isomophism.

<u>Proposition</u>: let $\varphi : (G, \circ) \to (H, *)$ be an isomorphism. Let e_G and e_H be the identities of $(G, \cdot)$ and $(H, *)$ representivly, and let $g \in G$, Then:

- $\varphi(e_G) = e_H$
- $\varphi(g^{-1}) = \varphi(g)^{-1}$

<u>Proof</u>:

Recall for $g_1, g_2 \in G$, $\varphi(g_1 \cdot g_2) = \varphi(g_1) * \varphi(g_2)$
Then if $g \in G$, $\varphi(g) = \varphi(g \cdot e_G) = \varphi(g) * \varphi(e_G)$
Similarly, $\varphi(e_G) * \varphi(g) = \varphi(g)$. $\rightarrow$

Proof con't:

Since φ is bijective, $\varphi(g)$ can be any element in H. Hence, for all $h \in H$, there is a $g \in G$ with $\varphi(g) = h$.

Rewriting we have,

$h = h * \varphi(e_G) * h$

By uniqueness, $\varphi(e_G) = e_H$