Abstract Algebra A

soupless

May 20, 2024

Lecture 1: Sets and relations

Definition 1.1 (Cartesian product)

Let A and B be sets. The *Cartesian product* of A and B, denoted by $A \times B$, is defined as

$$A \times B \ := \ \{(a, b) \mid a \in A, \, b \in B\}.$$

Definition 1.2 (Relation)

A relation R between sets A and B is a subset of $A \times B$. That is, $R \subseteq A \times B$.

We let $aRb \equiv (a, b) \in \mathbb{R}$ for each $a \in A$ and $b \in B$ where R is a relation. It is an implicit assumption that A and B have to be nonempty, otherwise, the relation is trivial.

Theorem 1.1

If A and B are finite sets, then there are $2^{|A| \cdot |B|} - 1$ relations.

Proof: Let A and B be finite sets. Then, the question is equivalent to finding the number of subsets of $A \times B$, which is $|\mathcal{P}(A \times B)| - 1 = 2^{|A \times B|} - 1 = 2^{|A| \cdot |B|} - 1$. ■

Definition 1.3 (Function)

A function ϕ mapping X into Y is a relation between X and Y with the property that each $x \in X$ appears as the first member of exactly one ordered pair $(x, y) \in \phi$ for all $y \in Y$.

Definition 1.4 (Domain, codomain, range)

Let $\phi : X \to Y$ be a function mapping X to Y. Then,

- X is the domain of ϕ,
- Y is the codomain of ϕ,
- $\phi[X]$ is the range of ϕ such that $\phi[X] = \{\phi(x) \mid x \in X\}$.

Another notation would be $X \xrightarrow{\phi} Y$ to denote the type signature, and $x \xmapsto{\phi} y$ to denote the function definition.

Definition 1.5 (Injective function)

A function $\phi : X \to Y$ is *injective* or one-to-one (1-1) if, for all elements x_1 and x_2 of X, $\phi(x_1) = \phi(x_2)$ implies $x_1 = x_2$.

Example: Let $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = 2x + 3$ for all $x \in \mathbb{R}$. Is f injective?

Let x_1 and x_2 be arbitrary elements of $\mathbb{R}$, and suppose that $f(x_1) = f(x_2)$. Then,

$$\begin{aligned} f(x_1) &= f(x_2) \\ 2x_1 + 3 &= 2x_2 + 3 \\ 2x_1 &= 2x_2 \\ x_1 &= x_2 \end{aligned}$$

Hence, f is injective.

Example: Let $g : \mathbb{R} \to \mathbb{R}$ such that $g(x) = x^2$ for all $x \in \mathbb{R}$. Is g injective?

No, because $g(-1) = 1$, and $g(1) = 1$, but $-1 \neq 1$.

Definition 1.6 (Surjective function)

A function $\phi : X \to Y$ is surjective or onto if $\phi[X] = Y$. Equivalently, $\forall y \in Y\ \exists x \in X (\phi(x) = y)$.

Example: Let $F : \mathbb{R} \to \mathbb{R}$ defined by $F(x) = x^2$ for each $x \in \mathbb{R}$. Is F surjective?

Since $F(x) \geq 0$ for all $x \in \mathbb{R}$, then $F(x) = -1$ has no solution. Hence, F is not surjective.

Example: Let $G : \mathbb{N} \to \mathbb{N}$ such that $G(x) = x + 1$ for each $x \in \mathbb{N}$. We define $\mathbb{N} = \{1, 2, 3, \ldots\}$. Is G surjective?

No, because $G(x) = 1$ has no solution in $\mathbb{N}$. Hence, G is not surjective.

Example: Let $\phi : \mathbb{N} \to \mathbb{N}$ such that $\phi(n)$ is the nth prime number for each $n \in \mathbb{N}$. Then, ϕ is injective. However, it is not surjective, because $\phi(x) = 4$ has no solution.

Example: Let $g : \mathbb{R} \to \mathbb{R}$ such that $g(x) = x + 1$ for each $x \in \mathbb{R}$. Prove that g is surjective.

Let $y \in \mathbb{R}$ be arbitrary. Then, $g(x) = y \implies x + y = 1 \implies x = y - 1$. Since $g(y - 1) = y - 1 + 1 = y$, this means g is surjective.

Definition 1.7 (Bijective function)

If $\phi : X \to Y$ is both injective and surjective, then ϕ is bijective.

Definition 1.8 (Inverse)

Let $\phi : X \to Y$ be a bijective function. The inverse of ϕ, denoted by ϕ^{-1}, is the function $\phi^{-1} : Y \to X$ such that $\phi^{-1}(y) = x \Leftrightarrow \phi(x) = y$ for all $x \in X$ and $y \in Y$.

A representation for finite domain maps would be through a matrix representation like

$$\phi : \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ \phi(x_1) & \phi(x_2) & \cdots & \phi(x_n) \end{bmatrix}$$

Definition 1.9 (Function composition)

Let $\phi : A \to B$ and $\theta : B \to C$ be functions. The composition $\theta\phi$ is the function $\theta\phi : A \to C$ defined by $\theta\phi(a) = \theta(\phi(a))$ for each $a \in A$.

Definition 1.10 (Function equality)

Let $f : X \to Y$ and $g : X \to Y$. Then, $f = g$ if $\forall x \in X\ (f(x) = g(x))$.

Theorem 1.2

Given functions $\alpha : A \to B$, $\beta : B \to C$, and $\gamma : C \to D$, then:

1. $(\gamma\beta)\alpha = \gamma(\beta\alpha)$. That is, function composition is associative.
2. If α and β are both injective, then $\beta\alpha$ is injective.
3. If α and β are both surjective, then $\beta\alpha$ is also surjective.

Proof: We prove each property listed in the theorem:

- Suppose we have the functions $\alpha : A \to B$, $\beta : B \to C$, and $\gamma : C \to D$. Let $a \in A$ be arbitrary. Then,

$$(\gamma\beta)\alpha(a) = \gamma\beta(\alpha(a))$$

$$(\gamma\beta)\alpha(a) = \gamma\left(\beta\left(\alpha(a)\right)\right)$$

$$\begin{aligned}\gamma(\beta\alpha)(a) &= \gamma\left(\beta\alpha(a)\right)\\ \gamma(\beta\alpha)(a) &= \gamma\left(\beta\left(\alpha(a)\right)\right)\end{aligned}$$

Hence, $(\gamma\beta)\alpha(a) = \gamma(\beta\alpha)(a)$. Therefore, $(\gamma\beta)\alpha = \gamma(\beta\alpha)$.

- Let $\alpha : A \to B$ and $\beta : B \to C$ be injective functions. Then, $\beta\alpha : A \to C$. Suppose that for all $a_1, a_2 \in A$, $\beta\alpha(a_1) = \beta\alpha(a_2)$. We get the following derivation:

$$\begin{aligned}\beta\alpha(a_1) &= \beta\alpha(a_2)\\ \beta\left(\alpha(a_1)\right) &= \beta\left(\alpha(a_2)\right)\\ \alpha(a_1) &= \alpha(a_2)\\ a_1 &= a_2\end{aligned}$$

  Therefore, $\beta\alpha$ is injective.

- Let $\alpha : A \to B$ and $\beta : B \to C$ be surjective functions. Let $c \in C$ be arbitrary. Then, there exists $b \in B$ such that $\beta(b) = c$. Since α is surjective, there exists $a \in A$ such that $\alpha(a) = b$. Then, $\beta(b) = \beta(\alpha(a)) = \beta\alpha(a) = c$. Hence, there exists $a \in A$ such that $\beta\alpha(a) = c$, and so for all $c \in C$, there exists $a \in A$ such that $\beta\alpha(a) = c$. Therefore, $\beta\alpha$ is surjective. ■

Lecture 2: Sets and relations, continued

Theorem 2.1

Let $\alpha : A \to B$ be a bijective function. Then there exists a function $\theta : B \to A$ such that $\forall a \in A\,(\theta\alpha(a) = a)$ and $\forall b \in B\,(\alpha\theta(b) = b)$. The function θ is called the inverse of α and is denoted by $\theta = \alpha^{-1}$.

Proof: Suppose $\alpha : A \to B$ is a bijective function. Construct a function $\theta : B \to A$ satisfying the properties $\forall a \in A\,(\theta\alpha(a) = a)$ and $\forall b \in B\,(\alpha\theta(b) = b)$. We define $\theta : B \to A$ by $\theta(b) = a$ iff $\alpha(a) = b$.

Let $a \in A$ be arbitrary. Consider $\theta\alpha(a)$. Suppose $\alpha(a) = b$. Then, $\theta\alpha(a) = \theta\left(\alpha(a)\right) = \theta(b) = a$.

Let $b \in B$ be arbitrary. Consider $\alpha\theta(b)$. Suppose $\theta(b) = a$. Then, $\alpha\theta(b) = \alpha\left(\theta(b)\right) = \alpha(a) = b$. ■

Definition 2.1 (Identity function)

The identity function is a function having the same domain and codomain such that $x \mapsto x$ for all x in the domain.

Theorem 2.2

Let $\alpha : A \to B$ be a bijective function. Then, $\alpha^{-1} : B \to A$ is bijective.

Proof: We first prove that α^{-1} is injective. Let b_1, b_2 be arbitrary elements from B, and suppose that $\alpha^{-1}(b_1) = \alpha^{-1}(b_2)$. Then,

$$\begin{aligned}\alpha^{-1}(b_1) &= \alpha^{-1}(b_2)\\ \alpha\alpha^{-1}(b_1) &= \alpha\alpha^{-1}(b_2)\\ b_1 &= b_2\end{aligned}$$

Hence, α^{-1} is injective.

We now prove that α^{-1} is surjective. Let $a \in A$. We know that $\alpha^{-1}\alpha(a) = a$. Since $\alpha(a) \in B$, this means that there is an element $b \in B$ such that $\alpha^{-1}(b) = a$. Hence, for all $a \in A$, there exists an element $b \in B$ such that $\alpha^{-1}(b) = a$, and so α^{-1} is surjective.

Therefore, α^{-1} is surjective. ■

Definition 2.2 (Equivalence relation)

R is called an equivalence relation on a set S if R is a relation from S to S and it satisfies the following:

1. $\forall a \in S(aRa)$.
2. $\forall a, b \in S(aRb \implies bRa)$.
3. $\forall a, b, c \in S(aRb \land bRc \implies aRc)$.

Example: Define R on $\mathbb{R}^*$ such that $aRb \Leftrightarrow ab > 0$ for all $a, b \in \mathbb{R}^*$. Let $a, b, c \in \mathbb{R}^*$ be arbitrary. Since $a \in \mathbb{R}^*$, we have $a \neq 0$, and since $x^2 > 0$ for all nonzero real numbers, we get $aa > 0$ which is equivalent to aRa. Thus, R is reflexive. Now, suppose aRb. Then, $ab > 0$. Multiplication under real numbers is commutative, hence, $ba > 0$, and so bRa. This means R is symmetric. Lastly, suppose aRb and bRc. Then, $ab > 0$ and $bc > 0$. We get $ab^2c > 0$, and dividing both sides by b^2, we get $ac > 0$. Hence, aRc, and so R is transitive.

Therefore, R is an equivalence relation.

Example: Define $\sim$ on $\mathbb{Z}$ by $a \sim b \Leftrightarrow a \equiv b \pmod 4$. We verify if $\sim$ is an equivalence relation on $\mathbb{Z}$.

We have $4 \mid 0 \implies 4 \mid a - a$, and so $a \equiv a \pmod 4$. Hence, $\sim$ is reflexive. Now, suppose $a \sim b$. Then, $4 \mid a - b \implies 4 \mid (-1)(a - b) \implies 4 \mid b - a$. Hence, $b \sim a$, and $\sim$ is symmetric. Lastly, suppose $a \sim b$ and $b \sim c$. Then, $4 \mid a - b$ and $4 \mid b - c$. We have $4 \mid a - b + b - c \implies 4 \mid a - c$. Hence, aRc, and so R is transitive.

Therefore, $\sim$ is an equivalence relation on $\mathbb{Z}$.

Definition 2.3 (Equivalence class)

Let $\sim$ be an equivalence relation on S. Let $a \in S$, The equivalence containing a, denoted by $[a]$, is the set defined by

$$[a] := \{x \in S \mid a \sim x\}.$$

Example: We have shown that R is an equivalence relation on $\mathbb{R}^*$. Finding the equivalence class containing 2,

$$[2] = \{x \in \mathbb{R}^* \mid 2Rx\}$$
$$[2] = \{x \in \mathbb{R}^* \mid 2x > 0\}$$
$$[2] = \{x \in \mathbb{R}^* \mid x > 0\}$$
$$[2] = \mathbb{R}^+$$

Finding the equivalence class containing $\sqrt{2}$,

$$[\sqrt{2}] = \{x \in \mathbb{R}^* \mid \sqrt{2}Rx\}$$
$$[\sqrt{2}] = \{x \in \mathbb{R}^* \mid \sqrt{2}x > 0\}$$
$$[\sqrt{2}] = \{x \in \mathbb{R}^* \mid x > 0\}$$
$$[\sqrt{2}] = \mathbb{R}^+$$

Finding the equivalence class containing $-e$,

$$[-e] = \{x \in \mathbb{R}^* \mid -eRx\}$$
$$[-e] = \{x \in \mathbb{R}^* \mid -ex > 0\}$$
$$[-e] = \{x \in \mathbb{R}^* \mid x < 0\}$$
$$[-e] = \mathbb{R}^-$$

Example: We have shown that $\sim$ is an equivalence relation on $\mathbb{Z}$ where $a \sim b \Leftrightarrow a \equiv b \pmod 4$.

Finding the equivalence class containing a,

$$[a] = \{x \in \mathbb{Z} \mid x \sim a\}$$
$$[a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod 4\}$$
$$[a] = \{x \in \mathbb{Z} \mid 4 \mid x - a\}$$
$$[a] = \{x \in \mathbb{Z} \mid 4 \mid x - a\}$$
$$[a] = \{x \in \mathbb{Z} \mid 4k = x - a, k \in \mathbb{Z}\}$$
$$[a] = \{x \in \mathbb{Z} \mid 4k + a = x, k \in \mathbb{Z}\}$$
$$[a] = \{4k + a \mid k \in \mathbb{Z}\}$$

Hence, the equivalence class containing 0 is just $\{4k \mid k \in \mathbb{Z}\}$. The equivalence class containing 1 is $\{4k + 1 \mid k \in \mathbb{Z}\}$, $\{4k + 2 \mid k \in \mathbb{Z}\}$ for the equivalence class containing 2, and $\{4k + 3 \mid k \in \mathbb{Z}\}$ for the equivalence class containing 3. The equivalence class containing 5 is just $[1]$ since $5 \in [1]$. Finally, $\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3]$.

Definition 2.4 (Partition, cells)

A partition P of a set S is a collection of nonempty disjoint subsets of S whose union is S. Each element of P is called a *cell*.

Example: In $\mathbb{Z}$, one such partition is $\left\{\mathbb{Z}^-, \mathbb{Z}^+, \{0\}\right\}$

Example: Let $S = \{1, 2, 3, 4, 5\}$. One partition would be $P_1 = \{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}\}$. Another partition would be $P_2 = \{\{1, 2\}, \{3\}, \{4\}, \{5\}\}$. The number of 2-cell partitions of S would be $\binom{5}{2}$.

Theorem 2.3

The equivalence classes of an equivalence relation on a set S constitute a partition of S.

Proof: Let $\sim$ be an equivalence relation on S. For any $a \in S$, we have $a \in [a]$. Let $a, b \in S$ such that $[a] \neq [b]$. There will be two cases:

- The intersection of $[a]$ and $[b]$ is nonempty. This means that there exists an element x in both $[a]$ and $[b]$. Then, $x \sim a$ and $x \sim b$, so $a \sim b$. Let $y \in S$ be arbitrary. Suppose $y \in [a]$. Then, $y \sim a$. Since $a \sim b$, then $y \sim b$, so $y \in [b]$. Hence, $[a] \subseteq [b]$. Similarly, suppose $y \in [b]$. Then, $y \sim b$. Then, $a \sim b$ implies $b \sim a$, so $y \sim a$. Hence, $y \in [a]$, and so $[b] \subseteq [a]$. Hence, $[a] = [b]$. This contradicts our assumption that $[a] \neq [b]$. Hence, $[a] \cap [b] = \varnothing$.
- The intersection of $[a]$ and $[b]$ is empty. Hence, $[a] \cap [b] = \varnothing$.

In either case, we get $[a] \cap [b] = \varnothing$.

Since each equivalence class is disjoint to another, and every element belongs to an equivalence class containing it, this means that the collection of all equivalence classes of S is a partition of S. ■

Lecture 3: Introduction to groups

Definition 3.1 (Binary operation)

> A binary operation $*$ on a set S is a function $*: S \times S \to S$.

We let $a * b \equiv *((a, b))$ for each $a, b \in S$.

Definition 3.2 (Closure)

> If $*$ is a binary operation on S, then S is closed under $*$.

Example :

- $+$ is a binary operation on $\mathbb{R}$ because the signature of $+$ is $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$.
- $-$ is a binary operation on $\mathbb{R}$ since $- : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$.
- $\div$ is not a binary operation on $\mathbb{R}$ since $a \div 0$ is not in $\mathbb{R}$. However, $\div$ is a binary operation on $\mathbb{R} \backslash \{0\}$.
- Define θ on $\mathbb{R}^+$ by $a\theta b = a^b$. Then, θ is a binary operation on $\mathbb{R}^+$.
- Define ϕ on $\mathbb{R}$ by $a\phi b = \sqrt{ab}$. Then, ϕ is not a binary operation on $\mathbb{R}$ since if $ab < 0$, then $\sqrt{ab} \notin \mathbb{R}$.

Note 3.1 (Ordinary addition, ordinary multiplication)

> We call $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ as ordinary addition, and $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$.

Definition 3.3 (Commutative binary operation)

> A binary operation $*$ on S is commutative iff $\forall a, b \in S \, (a * b = b * a)$.

Definition 3.4 (Set of $m \times n$ matrices)

> We define $M_{mn}(\mathbb{R})$ as the set of all $m \times n$ matrices whose entries belong to $\mathbb{R}$.

Definition 3.5 (General linear matrix set)

> We define $GL(n, \mathbb{R})$ as the set of $n \times n$ nonsingular matrices with real entries.

Example :

- In $M_{mn}(\mathbb{R})$, matrix addition is a binary operation. It is also commutative.
- In $GL(n, \mathbb{R})$, matrix multiplication is a binary operation but it is not commutative. Matrix addition is not a binary operation, i.e., $I_n + (-1)I_n$ is not in $GL(n, \mathbb{R})$.

Definition 3.6 (Associative binary operation)

> A binary operation $*$ on S is an associative binary operation iff $\forall a, b, c \in S \, (a*(b*c) = (a*b)*c)$.

Example : Define the operation $*$ on $\mathbb{R}$ by $a * b = a + b + ab$. Is $*$ an associative binary operation?

It is trivial that $*$ is a binary operation. Checking if it is associative,

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

We see that $a * (b * c) = (a * b) * c$. Hence, $*$ is an associative binary operation.

Example: Let $S = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \middle| a, b \in \mathbb{R} \right\}$. Let $*$ be matrix multiplication. Verify if $*$ is a commutative or associative binary operation on S.

Let $A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ where $a, b \in \mathbb{R}$, and $B = \begin{bmatrix} c & -d \\ d & c \end{bmatrix}$ where $c, d \in \mathbb{R}$. Then,

$$AB = \begin{bmatrix} a & -b \\ -b & a \end{bmatrix} * \begin{bmatrix} c & -d \\ d & c \end{bmatrix}$$
$$AB = \begin{bmatrix} ac - bd & -ad - bc \\ ad + bc & ac - bd \end{bmatrix}$$
$$AB = \begin{bmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{bmatrix}$$

This means $AB \in S$. Solving for BA,

$$BA = \begin{bmatrix} c & -d \\ d & c \end{bmatrix} * \begin{bmatrix} a & -b \\ -b & a \end{bmatrix}$$
$$BA = \begin{bmatrix} ac - bd & -bc - ad \\ ad + bc & -bd + ac \end{bmatrix}$$
$$BA = \begin{bmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{bmatrix}$$

This also means that $BA \in S$. Note that $AB = BA$. Hence, matrix multiplication is commutative. It is also associative, since the general matrix multiplication is associative.

Example: Let $S = \{a, b, c\}$. Define $*$ on S by

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

.

Is $*$ a binary operation? If it is, is it commutative and/or associative?

The operation $*$ is a binary operation since every output of $*$ is in S. It is not commutative, since $a * c \neq c * a$. Checking if it is associative is left for the reader.

Theorem 3.1

There are n^{n^2} binary operations on a set S such that $|S| = n$.

Proof: We have n choices for each cell in the table. There are n^2 cells in the matrix, so there will be n^{n^2} combinations for the matrix. Hence, there are n^{n^2} binary operations on a set S such that $|S| = n$. ■

Definition 3.7 (Group)

A group $\langle G, * \rangle$ is a set G, closed under the binary operation $*$ such that the following axioms hold:

- $\mathcal{G}_1 : \forall a, b, c \in G (a * (b * c) = (a * b) * c)$.
- $\mathcal{G}_2 : \exists e \in G \ \forall a \in G (e * a = a * e = a)$.
- $\mathcal{G}_3 : \forall a \in G \ \exists a' \in G (a * a' = a' * a = e)$.

In the third axiom, a' is called the inverse of a. We let $a^{-1} \equiv a'$ for each $a \in G$.

Example :

- Is $\langle \mathbb{R}, + \rangle$ a group?

  Yes, $\langle \mathbb{R}, +$ is a group because:

  - $+$ is associative,
  - $+$ has an identity element which is 0,
  - An arbitrary element a from $\mathbb{R}$ has an inverse $-a$ such that $a + (-a) = 0$.
- Is $GL(2, \mathbb{R})$ a group? Yes, $GL(2, \mathbb{R})$ is a group because:
  - Matrix multiplication is associative,
  - $+$ has an identity element which is I_2,
  - A nonsingular 2×2 matrix has a nonsingular inverse, which is in $GL(2, \mathbb{R})$.

Lecture 4: Introduction to groups, continued

Definition 4.1 (Set of integers modulo n)

We define $\mathbb{Z}_n$ be the set of integers modulo n, such that

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

Note that $a \pmod{n}$ is the remainder when a is divided by n.

Example: Let $*$ be the binary operation on $\mathbb{Z}_n$ defined by $a * b = (a+b) \pmod{n}$. The table for $*$ on $\mathbb{Z}_4$ is

$*$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Theorem 4.1

$\langle \mathbb{Z}_n, * \rangle$ is a group.

Proof: This is because it satisfies the group axioms:

- The operation $*$ is a binary operation in $\mathbb{Z}_n$.
- The binary operation $*$ is associative on $\mathbb{Z}_n$.
- The binary operation $*$ has an identity element which is 0.
- If $a \in \mathbb{Z}_n$, then $a^{-1} = n - a \pmod{n}$. ■

Definition 4.2 (Set of integers relatively prime to n)

We define U_n to be the set of integers relatively prime to n. That is,

$$U_n = \{x \mid 1 \leq x \leq n \wedge \gcd(n, x) = 1\}.$$

Theorem 4.2

$\langle U_n, * \rangle$ is a group.

Proof: $\langle U_n, * \rangle$ satisfies the group axioms:

- U_n is closed under $*$.

  Let $a, b \in U_n$. Then, $\gcd(a, n) = \gcd(b, n) = 1$. Suppose $\gcd(ab, n) \neq 1$. Then, there exists an integer p such that $p \mid n$ and $p \mid ab$. Let d be such a number. Then, by Euclid's lemma, if $p \mid ab$, then $p \mid a$ or $p \mid b$. Suppose $p \mid a$. Then, $\gcd(a, n) \geq p$ which contradicts our assumption that $\gcd(a, n) = 1$. Similarly, if $p \mid b$, then $\gcd(b, n) \geq p$ which also contradicts our assumption that $\gcd(b, n) = 1$. Regardless of the case, we have a contradiction.

  Hence, $\gcd(ab, n) = 1$.

- $*$ is associative.

  Multiplying integers in modular arithmetic is associative. Since U_n has a binary operation utilizing modular arithmetic, this means $*$ is associative.

- U_n has an identity element under $*$.

  Let $a, e \in U_n$. Then, we must have $ae = a$, or equivalently, $ae \equiv a \pmod{n}$. Then, $n \mid ae - a$ which is the same as $n \mid a(e-1)$. By Euclid's lemma, either $n \mid a$ or $n \mid e - 1$, which is the same as $e \equiv 1 \pmod{n}$. Clearly, $\gcd(1, n) = 1$, so our identity element is 1.

- Every element in U_n has an inverse.

  We are to find $x \in U_n$ such that $ax \equiv 1 \pmod{n}$ for every $a \in U_n$. This is the same as finding x such that $nk = ax - 1 \Leftrightarrow ax - nk = 1$. By Bezout's lemma, there exists an x satisfying the equation. Hence, a has an inverse in U_n. ■

Example:

- The table for $\mathbb{Z}_6$ is

$*$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

- The table for U_9 is

$*$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

- Let $G = \{e, a, b, c, d\}$ where e is the identity in G under $*$. Complete the table below:

$*$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

Example: Define $*$ on $\mathbb{R}$ by $a * b = a + b + ab$. Verify if $\langle \mathbb{R}, * \rangle$ is a group.

We can see that $a+b+ab = (a+1)(b+1)-1$. Since $a, b \in \mathbb{R}$, then $a*b \in \mathbb{R}$. We also know that $*$ is associative. Consider $a * e = a$. Solving for the identity,

$$\begin{aligned} a + e + ae &= a \\ e + ae &= 0 \\ e(1+a) &= 0 \end{aligned}$$

This means $e = 0$. To check if every element in $\mathbb{R}$ has an inverse under $*$, suppose $b = a^{-1}$. Then, $a * b = 0$. Solving for b in terms of a,

$$\begin{aligned} a + b + ab &= 0 \\ b + ab &= -a \end{aligned}$$

$$\begin{aligned} b(1+a) &= -a \\ b &= \frac{-a}{1+a} \end{aligned}$$

We can see that b exists only if $a \neq 1$. Hence, not all elements have an inverse, so $\langle \mathbb{R}, * \rangle$ is not a group.

Note 4.1

Let G be a group. For any $a, b \in G$, we define ab as $a * b$ where $*$ is the binary operation of G, if $*$ is not stated.

Theorem 4.3

The identity element in a group is unique.

Proof: Suppose e_1 and e_2 are both identities of a group. Then, $e_1e_2 = e_1$ since e_2 is an identity. Similarly, $e_1e_2 = e_2$ since e_1 is an identity. By transitivity, we have $e_1 = e_2$. ■

Theorem 4.4

Let $a, b, c \in G$ where G is a group. Then,

(i) $ac = bc \implies a = b$. This is called right cancellation.

(ii) $ca = cb \implies a = b$. This is called left cancellation.

Proof: Let $a, b, c \in G$ be arbitrary. We prove each item:

(i) Suppose that $ac = bc$. Then, $acc^{-1} = bcc^{-1}$. Since the binary operation in G is associative, we have $a(cc^{-1}) = b(cc^{-1})$, which simplifies to $a = b$.

(ii) Suppose that $ca = cb$. Then, $c^{-1}ca = c^{-1}cb$. Since the binary operation in G is associative, we have $(c^{-1}c)a = (c^{-1}c)b$, which simplifies to $a = b$. ■

Theorem 4.5

Let G be a group. The inverse of any element in G is unique.

Proof: Let $g \in G$ be arbitrary. Let $a, b \in G$ be inverses of g. Then, $ag = ga = e$, and $bg = gb = e$, where e is the identity in G. Consider agb. We have $a(gb) = b$, and $(ag)b = a$. Since G is associative, then $a = b$. ■

Theorem 4.6

Let G be a group and let $a \in G$. Then, $(a^{-1})^{-1} = a$.

Proof: Since the inverse of a is a^{-1} and by the uniqueness of inverses, the inverse of a^{-1}, $(a^{-1})^{-1}$, is a. ■

Theorem 4.7

Let G be a group. If $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof: Let G be a group, and let $a, b \in G$ be arbitrary. Then,

$$\begin{aligned} ab(ab)^{-1} &= e \\ a^{-1}ab(ab)^{-1} &= a^{-1}e \\ eb(ab)^{-1} &= a^{-1} \end{aligned}$$

$$
\begin{aligned}
b^{-1}eb(ab)^{-1} &= b^{-1}a^{-1} \\
b^{-1}b(ab)^{-1} &= b^{-1}a^{-1} \\
(ab)^{-1} &= b^{-1}a^{-1}
\end{aligned}
$$

■

Theorem 4.8

Let G be a group. Let $a_1, a_2, \ldots, a_n \in G$. Then, $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}$.

Proof: Let $n \in \mathbb{N}$ be arbitrary, and suppose that for all $i \in \mathbb{N}$ less than n, $(a_1 a_2 \cdots a_i)^{-1} = a_i^{-1} a_{i-1}^{-1} \cdots a_2^{-1} a_1^{-1}$.

$$
\begin{aligned}
(a_1 a_2 \cdots a_n)^{-1} &= a_n^{-1}(a_1 a_2 \cdots a_{n-1})^{-1} \\
(a_1 a_2 \cdots a_n)^{-1} &= a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}
\end{aligned}
$$

Hence, $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}$. ■

Lecture 5: Groups, continued

Definition 5.1

Let G be a group, and let $x \in G$. Let $n \in \mathbb{Z}^+$. We define x^n as $\underbrace{x \cdot x \cdots x}_{n \text{ times}}$.

Theorem 5.1

Let G be a group, and let $x \in G$. Let $n \in \mathbb{Z}^+$. Then, $(x^n)^{-1} = (x^{-1})^n$.

This is a corollary of finding the inverse of a product.

Theorem 5.2

Let G be a group with $x \in G$. Let $m, n \in \mathbb{Z}$. Then,

(i) $x^m x^n = x^{m+n}$.

(ii) $(x^m)^n = x^{mn}$.

The proof is trivial.

Example: Let G be a group, and let $a, b, c \in G$. Then,

- $(a^2b^{-1}c^{-3})^{-1}$ can be simplified as follows:

$$(a^2b^{-1}c^{-3})^{-1} = (c^{-3})^{-1}(b^{-1})^{-1}(a^2)^{-1}$$
$$(a^2b^{-1}c^{-3})^{-1} = c^3ba^{-2}$$

- $(a^2b^{-1}c^{-1})^{-2}$ is equivalent to the following:

$$(a^2b^{-1}c^{-1})^{-2} = \left[(a^2b^{-1}c^{-1})^{-1}\right]^2$$
$$(a^2b^{-1}c^{-1})^{-2} = \left[(c^{-1})^{-1}(b^{-1})^{-1}(a^2)^{-1}\right]^2$$
$$(a^2b^{-1}c^{-1})^{-2} = \left[cba^{-2}\right]^2$$

Definition 5.2 (Abelian groups)

A commutative group is called an abelian group.

Theorem 5.3

Let G be a group and let $H = \{x^{-1} \mid x \in G\}$. Prove that $H = G$.

Proof: We first prove that $H \subseteq G$. Let $y \in H$ be arbitrary. Then, $y^{-1} \in G$. This means that $(y^{-1})^{-1} = y \in G$. Hence, $H \subseteq G$. We now prove that $G \subseteq H$. Let $y \in G$ be arbitrary. Then, $y^{-1} \in G$, so $y \in H$. Hence, $G \subseteq H$. Therefore, $H = G$. ■

Seatwork :

1. Show that $\{5, 15, 25, 35\}$ is a group under multiplication modulo 40.

   We first construct the table:

$*$	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

   - Multiplication of integers in modular arithmetic is closed, hence, $*$ is closed.
   - Associativity also holds since we are dealing with a specific modulus.
   - We have an identity element which is 25.
   - Each element has an inverse, in this case, the inverse of an element is itself.

   Hence, $\{5, 15, 25, 35\}$ is a group under multiplication modulo 40.

2. For any integer $n \geq 2$, show that there are at least two elements in U_n that satisfy $x^2 = 1$.

   Clearly, 1 satisfies the condition since $1^2 = 1$. Another element satisfying the condition is $n - 1$, since:

$$(n-1)^2 \equiv (n^2 - 2n + 1) \pmod{n}$$
$$(n-1)^2 \equiv 1 \pmod{n}$$

   Hence, there are at least two elements in U_n that satisfy $x^2 = 1$.

3. Prove that G is abelian iff $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

   Let G be a group, and let $a, b \in G$ be arbitrary.

   ($\Rightarrow$) Suppose that G is abelian. Then,

$$\begin{aligned} (ab)^{-1} &= b^{-1}a^{-1} && \text{by inverse of product} \\ (ab)^{-1} &= a^{-1}b^{-1} && \text{since } G \text{ is abelian} \end{aligned}$$

   ($\Leftarrow$) Suppose that $(ab)^{-1} = a^{-1}b^{-1}$. Then,

$$\begin{aligned} (ab)^{-1} &= a^{-1}b^{-1} \\ \left((ab)^{-1}\right)^{-1} &= (a^{-1}b^{-1})^{-1} \\ ab &= (b^{-1})^{-1}(a^{-1})^{-1} \\ ab &= ba \end{aligned}$$

   Therefore, G is abelian iff $(ab)^{-1} = a^{-1}b^{-1}$.

4. Prove that for any integer n, $(a^{-1}ba)^n = a^{-1}b^n a$ for any elements a and b from a group.

   Let $n \in \mathbb{Z}^+$ be arbitrary, and suppose that for all $i \in \mathbb{Z}^+$ less than n, $(a^{-1}ba)^i = a^{-1}b^i a$. Then,

$$\begin{aligned} (a^{-1}ba)^n &= (a^{-1}ba)(a^{-1}ba)^{n-1} \\ (a^{-1}ba)^n &= a^{-1}baa^{-1}b^{n-1}a \\ (a^{-1}ba)^n &= a^{-1}bb^{n-1}a \\ (a^{-1}ba)^n &= a^{-1}b^n a \end{aligned}$$

   Hence, $(a^{-1}ba)^n = a^{-1}b^n a$. Now, consider the case when $n \in \mathbb{Z}^-$. Let $k \in \mathbb{Z}^+$ such that $n = -k$. Then,

$$\begin{aligned} (a^{-1}ba)^n &= (a^{-1}ba)^{-k} \\ (a^{-1}ba)^n &= \left[(a^{-1}ba)^k\right]^{-1} \end{aligned}$$

$$\begin{aligned}(a^{-1}ba)^n &= (a^{-1}b^ka)^{-1}\\ (a^{-1}ba)^n &= a^{-1}(b^k)^{-1}(a^{-1})^{-1}\\ (a^{-1}ba)^n &= a^{-1}b^{-k}a\\ (a^{-1}ba)^n &= a^{-1}b^na\end{aligned}$$

And when $n = 0$, we have $(a^{-1}ba)^0 = e$ and $a^{-1}b^0a = a^{-1}a = e$. Therefore, $(a^{-1}ba)^n = a^{-1}b^na$ for any elements a and b from a group and for any integer n.

5. Prove that in a group, $(ab)^2 = a^2b^2$ iff $ab = ba$.

(⇒) Suppose that $(ab^2) = a^2b^2$. Then,

$$\begin{aligned}(ab)^2 &= a^2b^2\\ (ab)^2 &= aabb\\ (ab)^2 &= abab\\ aabb &= abab\\ ab &= ba\end{aligned}$$

(⇐) Suppose that $ab = ba$. Then,

$$\begin{aligned}abab &= abba\\ (ab)^2 &= ab^2a\\ (ab)^2 &= aab^2\\ (ab)^2 &= a^2b^2\end{aligned}$$

Therefore, $(ab)^2 = a^2b^2$ iff $ab = ba$ for all elements a, b in the group.

6. Let G be a group such that $x^2 = e$ for all $x \in G$ with e as the identity in G. Show that G is abelian.

Let $a, b \in G$. Then, $a^2 = b^2 = e$. Also, $(ab)^2 = e$. Hence, $abab = a^2b^2$ and by cancellations, we get $ab = ba$. Therefore, G is abelian.

Lecture 6: Order and subgroups

Definition 6.1 (Order of a group)

Let G be a group. The number of elements in G, denoted by $|G|$, is called the order of G.

Example:

$$\begin{aligned} |\mathbb{Z}_{10}| &= 10 \\ |U_5| &= |\{1,2,3,4\}| = 4 \\ |\mathbb{Z}| &= \infty \\ |\mathbb{Z}_n| &= n \\ |U_n| &= \phi(n) \end{aligned}$$

Definition 6.2 (Order of a group element)

Let G be a group and let $g \in G$. The order of g, denoted by $|g|$, is the smallest positive integer k such that $g^k = e$, where e is the identity in G. If no such k exists, we say that $|g|$ is infinite.

Example:

1. G is a group, and e is the identity in G. Hence, $|e| = 1$, since $e^1 = e$.
2. $U_9 = \{1,2,4,5,7,8\}$. We have $\phi(9) = 6$, so $|U_9| = 6$.

Example: Determine the order of each element in U_9.

Theorem 6.1

If $g \in G$ where G is a group, and if $g^k = e$, and $k \in \mathbb{Z}^+$, then $|g| \leq k$.

Proof: We check the cases of the relationship between $|g|$ and k:

Case 1: $|g| < k$.

Assume that $|g| = j < k$. Then, $|g| \leq k$.

Case 2: $|g| = k$.

Then, $|g| \leq k$.

Case 3: $|g| > k$.

This is a contradiction, since we already have $g^k = e$. ■

Definition 6.3 (Subgroup)

Let $H \subseteq G$, and $H \neq \varnothing$, and G be a group. H is called a subgroup of G, denoted $H \leq G$, if H itself is a group under the binary operation in G.

Example: Consider $\mathbb{Z}_{12}$, and let $H_1 = \{0,2,4,6,8,10\}$, $H_2 = \{0,3,6,9\}$, $H_3 = \{0,4,8\}$, $H_4 = \{0,6\}$, and $H_5 = \{0\}$.

All sets H_i can be proved to be subgroups of $\mathbb{Z}_{12}$.

Theorem 6.2 (Two-Step Subgroup Test)

Let G be a group and let H be a non-empty subset of G. If $ab \in H$ whenever $a, b \in H$ and $a^{-1} \in H$ whenever $a \in H$, then $H \leq G$.

Proof: Suppose that H is a non-empty subset of G where H is closed under the binary operation of G, and H is closed under taking inverses. Then, by hypothesis, closure and inverse conditions are already proved. Associativity of the binary operation of G is inherited by H, since it is a subset. To prove that an identity element exists, we know that for any element $h \in H$, $h^{-1} \in H$. Since the operation is closed in H, $hh^{-1} = e \in H$.

Hence, H is a group. Since H is a subset of G, this means that H is a subgroup of G. ■

Example: Let G be an abelian group, and let $H = \{x \mid x \in G \wedge |x| \text{ is finite}\}$.

We first prove that $H \neq \varnothing$. Since G is a group, this means that G has an identity element. We let e to be this identity element. Since $|e| = 1$, then $e \in H$, and so $H \neq \varnothing$.

We now show that H is closed. Let $a, b \in H$ be arbitrary. This means that $|a|$ and $|b|$ are finite. Let $|a| = k$ and let $|b| = j$. Consider $(ab)^{jk}$. Then, $(ab)^{jk} = a^{jk}b^{jk} = (a^k)^j(b^j)^k = e^je^k = e$. Hence, $(ab)^{jk} = e$ means that the order of ab is at most jk, and is finite.

To prove that H is closed under taking inverses, let $h \in H$ be arbitrary. This means that $|h|$ is finite. Let $|h| = k$. Then,

$$\begin{aligned}
h^k &= e \\
(h^k)^{-1} &= e^{-1} \\
(h^{-1})^k &= e \\
|h^{-1}| &\leq k \\
|h^{-1}| &\text{ is finite.} \\
|h^{-1}| &\in H.
\end{aligned}$$

By the two-step subgroup test, $H \leq G$.

Theorem 6.3 (One-step subgroup test)

Let G be a group and H be a nonempty subset of G. If, for any $a, b \in H$, $ab^{-1} \in H$, then $H \leq G$.

Proof: Let $H \neq \varnothing$ and $H \subseteq G$ where G is a group. Suppose that for any two elements $a, b \in H$, $ab^{-1} \in H$. First, we show that $e \in H$ where e is the identity in G. Since H is nonempty, this implies the existence of some element in H, let a be such an element. Then, $aa^{-1} = e \in H$. Hence, the identity element exists in H.

Let $a, b \in H$ be arbitrary. Since $e \in H$, then $eb^{-1} = b^{-1} \in H$. Hence, H is closed upon taking inverses. Now, $a(b^{-1})^{-1} = ab \in H$. Hence, H is closed.

By the two-step subgroup test, $H \leq G$. ■

Lecture 7: Order and subgroups, continued

Example : Let G be an abelian group. and let $H, K \subseteq G$ be subgroups. Show that the set $HK := \{hk \mid h \in H, k \in K\} \subseteq G$.

We prove this claim using the one-step subgroup test. Let $a, b \in HK$. Then, $a = h_1k_1$ and $b = h_2k_2$, so

$$\begin{aligned} ab^{-1} &= h_1k_1(h_2k_2)^{-1} \\ ab^{-1} &= h_1k_1h_2^{-1}k_2^{-1} \\ ab^{-1} &= h_1h_2^{-1}k_1k_2^{-1} \end{aligned}$$

Since $h_1h_2^{-1} \in H$, and $k_1k_2^{-1} \in K$, then $ab^{-1} \in HK$.

Theorem 7.1 (Finite subgroup test)

Let H be a nonempty finite subset of a group G. If H is closed, then $H \subseteq G$.

Proof: By hypothesis, $H \neq \varnothing$ and H is closed. We need to show that for all $h \in H$, $h^{-1} \in H$. Suppose H is finite. Let $h \in H$ be arbitrary. Consider the following cases:

Case 1: $h = e$.

Hence, $h^{-1} = e^{-1} = e$.

Case 2: $h \neq e$.

Consider the set $T = \{h^k \mid k \in \mathbb{Z}^+\}$. If each power of h is unique, then T is an infinite set. However, we know that H is finite, hence, a contradiction. Therefore, T is a finite set.

This means that there exists $i, j \in \mathbb{Z}^+$ such that $h^i = h^j$ and $i \neq j$. Without loss of generality, let $i > j$. Since $h^k \in H$ for all $k \in \mathbb{Z}$, then $T \subseteq H$. We then have

$$\begin{aligned} h^i &= h^j \\ h^ih^{-j} &= h^jh^{-j} \\ h^{i-j} &= e \end{aligned}$$

We claim that $i - j \geq 2$. Suppose that $i - j < 2$. If $i - j = 0$, then $i = j$ which contradicts our proof that $i \neq j$. If $i - j = 1$, then $h^{i-j} = h^1 = h = e$, which contradicts our assumption that $h \neq e$. Hence, $i - j \geq 2$.

Then,

$$\begin{aligned} h^{i-j} &= e \\ hh^{i-j-1} &= e \end{aligned}$$

This means that $h^{-1} = h^{i-j-1}$. Hence, the inverse of h exists.

By the two-step subgroup test, $H \leq G$. ■

Definition 7.1 (Subgroup generated by an element)

Let $g \in G$ where G is a group. Then, $\langle g \rangle$ is the subgroup generated by g, and is defined as $\{g^k \mid k \in \mathbb{Z}\}$.

Definition 7.2 (Centralizer)

Let G be a group, and let $a \in G$. Then, $C(a)$ is the centralizer of a, defined as the set $\{x \mid x \in G \wedge ax = xa\}$.

Example : Let G be a group, and let $a \in G$. Show that $C(a) \leq G$.

- We can use the two-step subgroup test. It is obvious that $C(a)$ is nonempty, since $e \in C(a)$. To prove closure, let $x, y \in C(a)$ be arbitrary. We then have $axy = xay = xya$, which implies $xy \in C(a)$. And to prove that inverses exist,

$$\begin{gathered} ax = xa \\ x^{-1}axx^{-1} = x^{-1}xax^{-1} \\ x^{-1}a = ax^{-1} \end{gathered}$$

which implies $x^{-1} \in C(a)$. By the two-step subgroup test, this means $C(a) \leq G$.

Definition 7.3 (Center)

Let G be a group. Then, $Z(G)$ is the center of G, defined as the set

$$Z(G) = \{x \mid x \in G \land \forall a \in G(ax = xa)\}.$$

Lecture 8: Sample problems on order

1. Let G be a group, and let $a, b \in G$ be arbitrary. Show that:

   (i) $|a| = |a^{-1}|$

   We consider two cases, one where a is of infinite order and one where it is of finite order.

   - $|a|$ is infinite.

     Suppose $|a^{-1}|$ is finite. Let $k = |a^{-1}|$. Then,

     $$\begin{aligned}(a^{-1})^k &= e\\ a^{-k} &= e\\ a^k a^{-k} &= a^k\\ e &= a^k\\ |a| &\leq k\end{aligned}$$

     which contradicts our assumption that $|a|$ is infinite. Hence, $|a| = |a^{-1}|$.

   - $|a|$ is finite.

     Let $|a| = k$. Then,

     $$\begin{aligned}a^k &= e\\ (a^k)^{-1} &= e^{-1}\\ a^{-k} &= e\\ (a^{-1})^k &= e\\ |a^{-1}| &\leq k\end{aligned}$$

     Suppose $|a^{-1}| < k$. Let $|a^{-1}| = m$. Then,

     $$\begin{aligned}(a^{-1})^m &= e\\ a^{-m} &= e\\ (a^m)^{-1} &= e\\ ((a^m)^{-1})^{-1} &= e^{-1}\\ a^m &= e\\ |a| &\leq m\\ k &\leq m\end{aligned}$$

     This contradicts the statement we obtained that $m < k$. Hence, $|a^{-1}| = k$, so $|a| = |a^{-1}|$.

   (ii) $|a| = |bab^{-1}|$

   A similar proof from the previous item will be used. Suppose that $|a|$ is infinite. If $|bab^{-1}|$ is finite, say k, then

$$\begin{aligned}(bab^{-1})^k &= e\\ ba^kb^{-1} &= e\\ b^{-1}ba^kb^{-1}b &= b^{-1}eb\\ a^k &= e\\ |a| &\leq k\end{aligned}$$

which contradicts our assumption that $|a|$ is infinite. Hence, $|a| = |bab^{-1}|$. Now, suppose that $|a|$ is finite, say k. Then,

$$\begin{aligned}(bab^{-1})^k &= ba^kb^{-1}\\ (bab^{-1})^k &= beb^{-1}\\ (bab^{-1})^k &= bb^{-1}\\ (bab^{-1})^k &= e\\ |bab^{-1}| &\leq k\end{aligned}$$

Suppose $|bab^{-1}| < k$, say m. Then,

$$\begin{aligned}(bab^{-1})^m &= e\\ ba^mb^{-1} &= e\\ b^{-1}ba^mb^{-1}b &= b^{-1}eb\\ a^m &= b^{-1}b\\ a^m &= e\\ |a| &\leq m\\ k &\leq m\end{aligned}$$

which contradicts our obtained statement $m < k$. Hence, $|bab^{-1}| = k$, so $|a| = |bab^{-1}|$.

2. Prove that if a and b are group elements of the same group such that $ab \neq ba$, then $aba \neq e$.

   Let a, b be arbitrary elements of a group. Suppose that $aba = e$ where e is the identity element. Then,

$$\begin{aligned}abaa^{-1} &= ea^{-1} & \qquad a^{-1}aba &= a^{-1}e\\ ab &= a^{-1} & ba &= a^{-1}\end{aligned}$$

   And by transitivity, $ab = ba$. This contradicts our assumption that $ab \neq ba$. Hence, $aba \neq a$.

3. Let G be a group, and let $x \in G$ be arbitrary such that $|x| = 7$. Show that x is a cube of some element in G.

   Since $|x| = 7$,

$$x^7 = e$$

$$\begin{aligned}(x^7)^2 &= e^2\\ x^{14} &= e\\ x^{14}x &= ex\\ x^{15} &= x\\ (x^5)^3 &= x\end{aligned}$$

Since $x^5 \in G$, we can let $g = x^5$. Then, $g^3 = x$ for some g in G. Hence, x is a cube of some element in G.

4. Let G be a group, and let $g \in G$ be arbitrary. Prove that $C(g) = C(g^{-1})$.

Let $x \in C(g)$ be arbitrary. Then,

$$\begin{aligned}gx &= xg\\ g^{-1}gxg^{-1} &= g^{-1}xgg^{-1}\\ xg^{-1} &= g^{-1}x\end{aligned}$$

which implies that $x \in C(g^{-1})$. This means $C(g) \subseteq C(g^{-1})$. Now, let $x \in C(g^{-1})$ be arbitrary. Then,

$$\begin{aligned}g^{-1}x &= xg^{-1}\\ gg^{-1}xg &= gxg^{-1}g\\ xg &= gx\end{aligned}$$

which implies $x \in C(g)$, so $C(g^{-1}) \subseteq C(g)$. Therefore, $C(g) = C(g^{-1})$.

5. Let G be a group. Prove that $Z(G) = \bigcap\limits_{g \in G} C(g)$.

Let $x \in Z(G)$ be arbitrary. Then, $\forall g \in G(xg = gx)$. Let $g \in G$ be arbitrary. Then $xg = gx$, which implies $x \in C(g)$. Since g is arbitrary, it must be that $x \in \bigcap\limits_{g\in G} C(g)$, so $Z(G) \subseteq \bigcap\limits_{g\in G} C(g)$. Now, let $x \in \bigcap\limits_{g\in G} C(g)$ be arbitrary. By definition of set intersection, this is equivalent to $\forall g \in G(x \in C(g))$. Let $g \in G$ be arbitrary. Then, $x \in C(g)$, which implies $xg = gx$. This means $\forall g \in G(xg = gx)$, and by definition of center, $x \in Z(G)$. Hence, $\bigcap\limits_{g\in G} C(g) \subseteq Z(G)$. Therefore, $Z(G) = \bigcap\limits_{g\in G} C(g)$.

6. Let G be a group, and let $g \in G$ such that $|g| = n$. Prove that if $d > 0$ and $d \mid n$, then $|g^d| = n/d$.

Since $d|n$, this means $n = dk$ for some integer k. By manipulating this equality, we get $k = n/d$. Then,

$$\begin{aligned}g^n &= e\\ g^{dk} &= e\\ (g^d)^k &= e\\ |g^d| &\leq k\\ |g^d| &\leq \frac{n}{d}.\end{aligned}$$

If $|g^d| < n/d$, say i, then

$$\begin{aligned} (g^d)^i &= e \\ g^{di} &= e \\ |g| &\leq di \end{aligned}$$

Since $i < k$, then $di < dk = n$, so $|g| \leq di < n$ which gives us $n < n$, a contradiction. Hence, $|g^d| = n/d$.

Lecture 9: Cyclic groups

Definition 9.1 (Cyclic groups)

Let G be a group. G is cyclic if there exists $g \in G$ such that $G = \langle g \rangle$. We say that g is called a generator of G. If G has no generator, then G is called acyclic.

Example: Consider U_9. The subgroups generated by each element are the following:

$$\begin{aligned}\langle 1 \rangle &= \{1\}\\ \langle 2 \rangle &= \{2,4,8,7,5,1\}\\ \langle 4 \rangle &= \{4,7,1\}\\ \langle 5 \rangle &= \{5,7,8,4,2,1\}\\ \langle 7 \rangle &= \{7,4,1\}\\ \langle 8 \rangle &= \{8,1\}\end{aligned}$$

This means that the generators of U_9 are 2 and 5.

Example: The infinite group $\mathbb{Z}$ is cyclic, since 1 generates $\mathbb{Z}$.

Theorem 9.1

Let G be a group and let $a \in G$. If a has infinite order, then $a^i = a^j$ iff $i = j$.

Proof: Let G be a group and let $|a| = \infty$.

($\Leftarrow$) Trivial.

($\Rightarrow$) Suppose $a^i = a^j$. Without loss of generality, let $i > j$. Then,

$$\begin{aligned}a^i &= a^j\\ a^i a^{-j} &= e\\ a^{i-j} &= e\end{aligned}$$

Hence, $|a| \leq i - j$, contradicting our assumption that the order of a is infinite. Therefore, $i = j$. ■

Theorem 9.2

Let G be a group and let $a \in G$. If $|a| = n < \infty$, then $\langle a \rangle = \{e, a, a^2, a^3, \ldots, a^{n-1}\}$.

Proof: Suppose $|a| = n$. Clearly, $\{e, a, a^2, \ldots, a^{n-1}\} \subseteq \langle a \rangle$ since $a^k \in \langle a \rangle$ for any $k \in \mathbb{Z}$.

To show the converse, let $a^k \in \langle a \rangle$. Using the division algorithm on k, there exists nonnegative integers q, r such that $k = nq + r$ where $0 \leq r \leq n$. Then,

$$\begin{aligned}a^k &= a^{nq+r}\\ a^k &= a^{nq}a^r\\ a^k &= (a^n)^q a^r\\ a^k &= (e)^q a^r\\ a^k &= ea^r\\ a^k &= ea^r\end{aligned}$$

$$a^k = a^r \in \{e, a, a^2, a^3, \ldots, a^{n-1}\}$$
$$a^k \in \{e, a, a^2, a^3, \ldots, a^{n-1}\}$$

Now, all elements in $\{e, a, \ldots, a^{n-1}\}$ must be unique. If not, then there must be integers s, t, without loss of generality, $s < t$, such that $a^t = a^s$ when $0 \leq s, t < n$. This means $a^{t-s} = e$, so $|a| \leq t - s$ which contradicts the fact that $t - s < n$.

Hence, $\langle a \rangle \subseteq \{e, a, a^2, a^3, \ldots, a^{n-1}\}$. Therefore, $\langle a \rangle = \{e, a, a^2, a^3, \ldots, a^{n-1}\}$ ■

Theorem 9.3

Let G be a group and let $a \in G$. If $|a| = n < \infty$, then $a^i = a^j$ iff $n \mid i - j$.

Proof: We prove the two directions as follows:

($\Longrightarrow$) Suppose $a^i = a^j$. Then, $a^{i-j} = e$. By the division algorithm, there exists integers q, r such that $i - j = nq + r$ where $0 \leq r < n$. Then, $a^{i-j} = a^{nq+r} = a^r = e$. If $0 < r$, then $|a| \leq r$ which implies $n \leq r$, contradicting $r < n$. This forces r to be zero. Hence, $i - j = nq$, and so $n \mid i - j$.

($\Longleftarrow$) Suppose $n \mid i - j$. There exists an integer k such that $i - j = nk$. Then,

$$\begin{aligned} a^{i-j} &= a^{nk} \\ a^{i-j} &= (a^n)^k \\ a^{i-j} &= e^k \\ a^{i-j} &= e \\ a^{i-j}a^j &= ea^j \\ a^i &= a^j \end{aligned}$$

■

Corollary 9.1

For any group element a, $|a| = |\langle a \rangle|$.

Proof: We consider two cases, one where the order of a is finite and the other is infinite.

- The order is finite.

  Suppose $|a| = n$. Since $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$ and $|\langle a \rangle| = n$, then $|a| = |\langle a \rangle|$.
- The order is infinite.

  Since $\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$, then $|\langle a \rangle| = |\mathbb{Z}| = \infty$ which implies $|a| = |\langle a \rangle|$. ■

Corollary 9.2

Let G be a group and let $a \in G$ with $|a| = n$. If $a^k = e$, then $n \mid k$ for some $k \in \mathbb{Z}$.

Proof: Let G be a group and let $a \in G$ with $|a| = n$. Since $a^k = e$, then $a^k = a^0$. This is iff $n \mid k - 0$, which simplifies $n \mid k$. ■

Theorem 9.4

Let a be a group element of order n and let k be a particular integer. Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n, k)$.

Proof: Let a be a group element of G such that $|a| = n$. Let $d = \gcd(k, n)$. First, we show that $\langle a^k \rangle = \langle a^d \rangle = \langle a^{\gcd(n,k)} \rangle$. We show $\langle a^d \rangle \subseteq \langle a^k \rangle$.

Note that for all integers i, $a^{ki} = a^{ds}$ for some integer s. Since $d = \gcd(n, k)$, by Bézout's lemma, there exists integers s, t such that $ns + kt = d$. Then,

$$\begin{aligned} a^d &= a^{ns+kt} \\ a^d &= a^{ns}a^{kt} \\ a^d &= (a^n)^s a^{kt} \\ a^d &= e^s a^{kt} \\ a^d &= a^{kt} \end{aligned}$$

Since $a^{kt} \in \langle a^k \rangle$, this means $\langle a^d \rangle \subseteq \langle a^k \rangle$.

Now, we show that $\langle a^k \rangle \subseteq \langle a^d \rangle$. Let $x \in \langle a^k \rangle$. Then, x will be of the form a^{ki} for some integer i. Since $d \mid k$, then $k = dj$ for integer j. This means that $x = a^{ki} = a^{dji} = (a^d)^{ji}$ which implies $x \in \langle a^d \rangle$. Hence, $\langle a^k \rangle = \langle a^d \rangle = \langle a^{\gcd(n,k)} \rangle$.

To prove that $|a^k| = n/\gcd(n, k)$, we find the order of a^k. It is the smallest positive integer m such that $(a^k)^m = e$. Since n is the smallest positive integer such that $a^n = e$, then it must be that $n \mid km - n$ (by Theorem 9.3) which implies $n \mid km$. We then get

$$\frac{n}{\gcd(n,k)} \,\Bigg|\, \frac{k}{\gcd(n,k)} m$$

and since

$$\begin{aligned} \gcd(n,k) &= \gcd(n,k) \\ \gcd\left(\frac{n}{\gcd(n,k)}, \frac{k}{\gcd(n,k)}\right) &= 1, \end{aligned}$$

then by Euclid's lemma, $n/\gcd(n, k) \mid m$. Hence, $n/\gcd(n, k) \leq m$. The smallest value of m satisfying the inequality is if $m = n/\gcd(n, k)$. Hence, $|a^k| = n/\gcd(n, k)$. ■

Example: Suppose that $|a| = 100$. Find $|a^{28}|$.

Using the previous theorem,

$$\begin{aligned} |a^{28}| &= \frac{|a|}{\gcd(|a|, 28)} \\ |a^{28}| &= \frac{100}{\gcd(100, 28)} \\ |a^{28}| &= \frac{100}{4} \\ |a^{28}| &= 25 \end{aligned}$$

Example: Suppose $|a| = 12$. Find $|a^8|$ and $\langle a^8 \rangle$.

Using the previous theorem,

$$\begin{aligned} |a^8| &= \frac{|a|}{\gcd(|a|, 8)} \\ |a^8| &= \frac{12}{\gcd(12, 8)} \\ |a^8| &= \frac{12}{4} \\ |a^8| &= 3 \end{aligned}$$

$$\begin{aligned} \langle a^8 \rangle &= \langle a^{\gcd(12,8)} \rangle \\ \langle a^8 \rangle &= \langle a^4 \rangle \\ \langle a^8 \rangle &= \langle a^4, a^8, e \rangle \end{aligned}$$

Lecture 10: Cyclic groups, continued

Theorem 10.1 (Fundamental Theorem of Cyclic Groups)

Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a\rangle| = n$, then the order of any subgroup of $\langle a\rangle$ is a divisor of n, and for each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order k, namely $\langle a^{n/k}\rangle$.

Proof: We prove the theorem by parts:

- We first show that any subgroup of a cyclic group is cyclic. Let G be a cyclic group. Then, $G = \langle a\rangle$. Let $H \leq G$. If H is generated by e, then H is trivially cyclic. Suppose H is not generated by e. There exists an element of the form a^t in H such that $a^t \neq e$ for some $t > 0$. Since $a^t \in H$ iff $a^{-t} \in H$, choose $\min\{t : a^t \in H, t > 0\}$. Let m be this number. We claim that $H = \langle a^m\rangle$.
- Clearly, $\langle a^m\rangle \subseteq H$ by closure. We show that $H \subseteq \langle a^m\rangle$. Let $a^k \in H$. By the division algorithm, there exists a $0 \leq r < m$ such that $k = mq + r$. Then, $a^k = a^{mq+r}$, so $a^k a^{-mq} = a^r$. Observe that $a^k \in H$ and $a^{-mq} \in H$, so $a^r \in H$. If $0 < r < m$, then we get a contradiction since we have m as the minimal exponent. Hence, $r = 0$. Thus, $a^k = a^{mq} = (a^m)^q$, so $a^k \in \langle a^m\rangle$. Hence, $H \subseteq \langle a^m\rangle$, so $H = \langle a^m\rangle$.
- Let $|\langle a\rangle| = n$, and let k be a positive divisor of n. We show that there is a unique subgroup of order k, namely $\langle a^{n/k}\rangle$.

  We first show existence. Consider $\langle a^{n/k}\rangle$. Then, $|\langle a^{n/k}\rangle| = |a^{n/k}| = n/\gcd(n, n/k) = n/(n/k) = k$. We now show uniqueness. Let $H \leq \langle a\rangle$ such that $|H| = k$. Then, there exists an $m \in \mathbb{Z}^+$ such that $H = \langle a^m\rangle$. This means $|H| = |a^m| = n/\gcd(n, m) = n/m$. Since $|H| = k$, then $k = n/m$, so $m = n/k$. Therefore, the subgroup is unique. ■

A corollary would about subgroups of $\mathbb{Z}_n$. For each positive divisor k of n, the group $\langle n/k\rangle$ is the unique subgroup of order k.

Theorem 10.2

If d is a positive divisor of n, the number of elements of order d is $\phi(d)$.

Lecture 11: Permutation group

Definition 11.1 (Permutation of a set)

A permutation of a set S is a bijective function from S to S.

Example: Let $S = \{1, 2, 3\}$. Then, permutations $\sigma_i : S \to S$ would be

$$\sigma_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \qquad \sigma_2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} \qquad \sigma_3 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

$$\sigma_4 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \qquad \sigma_5 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \qquad \sigma_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

Theorem 11.1

Let $n = |S|$. The number of permutations of a set S is $n!$.

Theorem 11.2

If σ is a permutation of S, then $\sigma \cdot \mathrm{id} = \mathrm{id} \cdot \sigma = \sigma$ where id is the identity permutation.

Definition 11.2 (Symmetric group of degree n)

Let $S = \{1, 2, \dots, n\}$. We define S_n to be the set of permutations of a set with n elements. This is called the symmetric group of degree n.

Theorem 11.3

S_n is a group.

Proof: We prove that S_n satisfies the group axioms:

- Closure: $\sigma, \tau \in S_n \implies \sigma\tau \in S_n$.
- Associativity: Trivial.
- Identity: Define $\mathrm{id} : S \to S$ by $\mathrm{id}(i) = i$ for all $i \in S$. Then id is the identity in S_n.
- Inverse: If $\sigma \in S_n$, we let σ^{-1} be the mapping such that $\sigma(i) = j$ iff $\sigma^{-1}(j) = i$. ■

Definition 11.3 (Identity mapping)

We define $\mathrm{id} : S \to S$ such that $\mathrm{id}(i) = i$.

Corollary 11.1

If σ is a permutation in S, then $\sigma \cdot \mathrm{id} = \mathrm{id} \cdot \sigma = \sigma$.

Proof: Let $i \in S$. Then,

$$\sigma \cdot \mathrm{id}(i) = \sigma(i)$$
$$\mathrm{id} \cdot \sigma(i) = \sigma(i)$$

Hence, $\sigma \cdot \mathrm{id} = \mathrm{id} \cdot \sigma = \sigma$. ■

Definition 11.4 (Dihedral group of degree n)

The group of symmetries of a regular n-gon is called the dihedral group of degree n.

The cardinality of D_n is $2n$, since we have n turns and n flips.

Lecture 12: Cycle form of permutations

Definition 12.1

Let S be a nonempty finite set. Let $\sigma = (a_1, a_2, \dots, a_k)$ be a permutation of S. We call σ a k-cycle of length k.

For example, in $\sigma = (1, 2, 3)$, $\sigma(1) = 1$, $\sigma^2(1) = 3$, and $\sigma^3(1) = 1$.

Note 12.1

Cycles are said to be equal if they can be rewritten as another cycle by moving the first i elements to the last element.

Theorem 12.1

Let σ be a k-cycle. Then, $|\sigma| = k$.

Proof: Let $\sigma = (a_1, a_2, \dots, a_k)$. From the remark, $\sigma^j(a_1) = a_{j+1}$ for $1 \leq j < k$. Then, $\sigma^j(a_1) \neq a_1$. But $\sigma^k(a_i) = a_i$ for all $1 \leq i \leq k$. Hence, $\sigma^k = \epsilon$, so $|\sigma| = k$. ■

Definition 12.2

A 2-cycle is called a transposition.

Theorem 12.2

The inverse of a 2-cycle is itself.

Theorem 12.3

Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Proof: Let σ be a permutation of a set $S = \{1, 2, \dots, n\}$. The first subcycle would be

$$(a_1, \sigma(a_1), \sigma^2(a_1), \dots, \sigma^{k_1}(a_1)).$$

The next subcycle would take elements from $S \setminus \{a_1, \sigma(a_1), \sigma^2(a_1), \dots, \sigma^{k_1}(a_1)\}$. It is evident that the cardinality of S decreased. By repeatedly constructing subcycles from this new set and removing the used elements, it is guaranteed that S is exhausted. Since we removed the elements the previous cycle used, the next subcycle to be written will be disjoint from the previous one. The permutation is then, the product of all the subcycles we formed. ■

Theorem 12.4

If the pair of cycles $\alpha = (a_1, a_2, \dots, a_m)$ and $\beta = (b_1, b_2, \dots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

Proof: Let α, β be permutations of $S = \{1, 2, \dots, n\}$ where $\alpha = (a_1, a_2, \dots, a_m)$ and $\beta = (b_1, b_2, \dots, b_n)$, and α and β have no entries in common. Let $A = \{a_1, a_2, \dots, a_m\}$ and $B = \{b_1, b_2, \dots, b_n\}$.

There are three cases where $x \in S$ belongs in a subset. Either it is in A, B, or neither. For the first case, this implies that $x \notin B$. Hence,

$$\begin{aligned} \alpha\beta(x) &= \alpha(\beta(x)) & \qquad \beta\alpha(x) &= \beta(\alpha(x)) \\ \alpha\beta(x) &= \alpha(x) & \qquad \beta\alpha(x) &= \alpha(x) \end{aligned}$$

which we can conclude that $\alpha\beta(x) = \beta\alpha(x)$. For the second case where $x \in B$, it is clear that $x \notin A$. Then,

$$\begin{aligned} \alpha\beta(x) &= \alpha(\beta(x)) & \beta\alpha(x) &= \beta(\alpha(x)) \\ \alpha\beta(x) &= \beta(x) & \beta\alpha(x) &= \beta(x) \end{aligned}$$

to which we derive the same conclusion. For the last case, since x is neither in A nor in B, then $\alpha\beta(x) = x = \beta\alpha(x)$. Therefore, $\alpha\beta = \beta\alpha$ if α and β have no entries in common. ■

Theorem 12.5 (Order of a Permutation)

The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.

Proof: Let σ be a permutation of a finite set S. Set $\sigma = \alpha_1\alpha_2 \ldots \alpha_n$ where σ is a product of disjoint cycles. Define $|\alpha_i| = m_i$ for $i = 1, 2, \ldots, n$. Suppose $|\sigma| = r$. Then, $\sigma^r = \text{id}$ and

$$\begin{aligned} \sigma^r &= \alpha_1^r \alpha_2^r \cdots \alpha_n^r \\ \alpha_i^r &= \text{id} \\ |\alpha_i| &\mid r \\ m_i &\mid r \end{aligned}$$

This means $m_1 \mid r, m_2 \mid r, \ldots, m_n \mid r$. Since r is the order, it must be the smallest integer such that $\sigma^r = \text{id}$. The divisibility constraints is the definition of the least common multiple, so $r = \text{lcm}(m_1, m_2, \ldots, m_n)$ ■

Definition 12.3 (Permutation parity)

A permutation is even if it can be written as a product of even number of 2-cycles.

Theorem 12.6

A k-cycle is even iff k is odd.

Lecture 13: Permutations, continued

Theorem 13.1

If $\epsilon = \beta_1\beta_2\cdots\beta_r$ where ϵ is the identity function and β_i is a 2-cycle for $i = 1, 2, \ldots, r$, then r is even.

Theorem 13.2

Let α be a permutation in S_n, $n > 1$. Suppose α can be written as $\beta_1\beta_2\cdots\beta_s$ and $\gamma_1\gamma_2\cdots\gamma_t$ where β_i and γ_j are 2-cycles. Then, s and t are either both even or both odd.

Proof: Let α be a permutation in S_n for $n > 1$, and suppose that it can be written as a product of 2-cycles $\beta_1\beta_2\cdots\beta_s$ and $\gamma_1\gamma_2\cdots\gamma_t$. Then,

$$\begin{aligned}\beta_1\beta_2\cdots\beta_s &= \gamma_1\gamma_2\cdots\gamma_t\\(\beta_1\beta_2\cdots\beta_s)(\beta_1\beta_2\cdots\beta_s)^{-1} &= (\gamma_1\gamma_2\cdots\gamma_t)(\beta_1\beta_2\cdots\beta_s)^{-1}\\\text{id} &= \gamma_1\gamma_2\cdots\gamma_t\beta_s\cdots\beta_2\beta_1\end{aligned}$$

The right-hand side is composed of $s + t$ transpositions, and the left-hand side is an identity permutation. Hence, $s + t$ must be even, which is only possible if both s and t are odd, or both of them are even. ■

Theorem 13.3

The set of even permutations in S_n, $n > 1$, is a subgroup of S_n.

Proof: Let $H = \{\sigma \in S_n \mid \sigma \text{ is an even permutation}\}$. We show that $H_n \leq S_n$ using the finite subgroup test.

Let $\rho, \tau \in H$. Then ρ has $2j$ 2-cycles, and τ has $2j$ 2-cycles. Hence, $\rho\tau$ has $2j + 2k$ 2-cycles, which implies $\rho\tau \in H$. Therefore, $H \leq S_n$. ■

Definition 13.1 (Alternating group)

The group of even permutations on n symbols is denoted by A_n and is called the alternating group of degree n.

Theorem 13.4

For $n > 1$, the number of even permutations in S_n is equal to the number of odd permutations, hence, $|A_n| = n!/2$.

Proof: We use the bijective principle. Construct the function $f : A_n \to B_n$ where A_n and B_n each contains all even and odd permutations, respectively. Choose a transposition σ from S_n. We define f as $f(\tau) = \tau\sigma$. Clearly, f is injective since

$$\begin{aligned}f(\tau_1) &= f(\tau_2)\\\tau_1\sigma &= \tau_2\sigma\\\tau_1 &= \tau_2\end{aligned}$$

It is also surjective. Fix $\rho \in B_n$, and we need to find $\tau \in A_n$ such that $f(\tau) = \rho$. We can choose $\tau = \rho\sigma$, since $f(\rho\sigma) = \rho\sigma\sigma = \rho$. Hence, f is bijective, and so $|A_n| = |B_n|$. Since $|S_n| = |A_n \cup B_n|$ and A_n and B_n are disjoint, then $|S_n| = 2|A_n| \implies 2|A_n| = n! \implies |A_n| = n!/2$. ■

Lecture 14: Cosets

Definition 14.1 (Coset)

Let G be a group, let H be a subgroup, and let $g \in G$. Then we define the left coset of H, denoted by gH, as

$$gH = \{gh \mid h \in H\}$$

and the right coset of H, denoted by Hg, as

$$Hg = \{hg \mid h \in H\}.$$

We call g as the coset representative.

Note 14.1

If G is abelian, then the left and right cosets of a subgroup coincide.

Theorem 14.1

Let $H \leq G$, $a, b \in G$. Then,

1. $a \in aH$ and $a \in Ha$.
2. $aH = H$ iff $a \in H$.
3. $(ab)H = a(bH)$ and $H(ab) = (Ha)b$.
4. $aH = bH$ iff $a \in bH$.
5. $aH = bH$ or $aH \cap bH = \varnothing$.
6. $aH = bH$ iff $a^{-1}b \in H$.
7. $|aH| = |bH|$.
8. $aH = Ha$ iff $H = aHa^{-1}$.

Proof: We prove each of the following statements provided the given statements:

1. Since $e \in H$, then $ae \in aH$. Since $a = ae$, this means $a \in aH$. Similarly, $ea \in Ha$, and since $a = ea$, this implies $a \in Ha$.
2. For the forward direction, suppose $aH = H$. Let $h \in H$. Then, $ah \in aH$, which implies $ah \in H$. This means that there is an element $h' \in H$ such that $ah = h'$. Since both h and h' are in H, then $h'h^{-1}$ is also in H. We then have $ahh^{-1} = h'h^{-1}$ which simplifies to $a = h'h^{-1}$, and so $a \in H$.

   For the backward direction, suppose $a \in H$. Let $h \in H$ be arbitrary. Then, $ah \in aH$ by the definition of a left coset. Also, $ah \in H$ by closure. Hence, $ah \in H \implies ah \in aH$, and $ah \in aH \implies ah \in H$, so $aH \subseteq H$ and $H \subseteq aH$. Therefore, $aH = H$.
3. Using the definition,

$$\begin{aligned}(ab)H &= \{(ab)h \mid h \in H\}\\ (ab)H &= \{a(bh) \mid h \in H\}\\ (ab)H &= a(bH).\end{aligned}$$

   A similar proof can be written for the right coset.
4. For the forward direction, suppose $aH = bH$. Let $h \in H$ be arbitrary. Then,

$$\begin{aligned}ah \in aH &\implies ah \in bH\\ ah \in aH &\implies ah = bh' \qquad (\exists h' \in H)\\ ah \in aH &\implies \ \ a = bh'h^{-1}\end{aligned}$$

And since $h'h^{-1} \in H$, then $bh'h^{-1} \in bH$. Hence, $a \in bH$.

And for the backward direction, suppose $a \in bH$. Then, $a = bh$ for some $h \in H$, and so

$$\begin{aligned} aH &= (bh)H \\ aH &= b(hH) \\ aH &= bH \end{aligned}$$

5. Suppose $aH \cap bH \neq \varnothing$. Let $x \in aH \cap bH$. Then, $x = ah_1 = bh_2$ for some $h_1, h_2 \in H$, and so

$$\begin{aligned} (ah_1)H &= (bh_2)H \\ a(h_1H) &= b(h_2H) \\ aH &= bH \end{aligned}$$

6. For the forward direction, suppose $aH = bH$. Then,

$$\begin{aligned} a^{-1}(aH) &= a^{-1}(bH) \\ (a^{-1}a)H &= (a^{-1}b)H \\ eH &= (a^{-1}b)H \\ H &= (a^{-1}b)H \end{aligned}$$

This implies $a^{-1}b \in H$. And for the backward direction, suppose that $a^{-1}b \in H$. Then,

$$\begin{aligned} H &= a^{-1}bH \\ aH &= aa^{-1}bH \\ aH &= bH \end{aligned}$$

7. We prove that $|aH| = |bH|$ using the bijective principle. Define $\rho : aH \to bH$ where $\rho(ah) = bh$. To prove that ρ is injective, suppose $\rho(ah_1) = \rho(ah_2)$. Then,

$$\begin{aligned} \rho(ah_1) &= \rho(ah_2) \\ bh_1 &= bh_2 \\ h_1 &= h_2 \\ ah_1 &= ah_2 \end{aligned}$$

And to show that ρ is surjective, let $x \in bH$ be arbitrary. Then, $x = bh$ for some $h \in H$. It is obvious that $\rho(ah) = bh$, so there exists some element in aH that ρ maps to bh.

Therefore, ρ is bijective. By the bijective principle, $|aH| = |bH|$.

8. For the forward direction, suppose $aH = Ha$. Then,

$$\begin{aligned} aHa^{-1} &= Haa^{-1} \\ aHa^{-1} &= H. \end{aligned}$$

For the backward direction, suppose $H = aHa^{-1}$. ■

Theorem 14.2

If H is a subgroup and $a \notin H$, then aH is not a subgroup.

Proof: Suppose that aH is a subgroup. Then, $aH \cap H \neq \varnothing$ since the identity element is both in aH and H.

Also, since $a \notin H$, this means $aH \neq H$. This contradicts the second coset property, so aH must not be a subgroup. ■

Theorem 14.3 (Lagrange's Theorem)

If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $|G|/|H|$.

Proof: Suppose G is a finite group and $H \leq G$. Let $a_1H, a_2H, \ldots, a_kH$ be the distinct left cosets of H in G. Every element must belong to some coset, as $g \in gH$. We then have

$$\bigcup_{i=1}^{k} a_iH = G$$
$$\left|\bigcup_{i=1}^{k} a_iH\right| = |G|$$

And since cosets are distinct, we can split the cardinality of the union to a sum of cardinalities:

$$\sum_{i=1}^{k} |a_iH| = |G|$$
$$\sum_{i=1}^{k} |H| = |G|$$
$$k|H| = |G|$$

Hence, the order of H divides the order of G as desired. Also, we declared k to be the number of distinct left cosets. By solving for k from the last line, we get $k = |G|/|H|$. ■

Definition 14.2 (Index of a subgroup)

The index of H in G, denoted by $[G : H]$, is the number of distinct left (right) cosets of H in G defined as
$$[G : H] = \frac{|G|}{|H|}.$$

Note 14.2

The more important part of Definition 14.2 is the number of distinct cosets, not the division of orders. This is because it will fail for infinite groups, i.e., $[\mathbb{Z} : 2\mathbb{Z}]$ which is 2, but both $\mathbb{Z}$ and $2\mathbb{Z}$ are of infinite order.

Theorem 14.4

In a finite group, the order of each group element divides the order of the group.

Proof: Each element $a \in G$ can be used to generate a subgroup $\langle a \rangle$. Since $|a| = |\langle a \rangle|$ and $|\langle a \rangle|$ divides[1] $|G|$, then $|a|$ divides $|G|$. ■

Theorem 14.5

A group of prime order is cyclic.

Proof: Let the order of a group be p where p is a prime number. The divisors of a prime number p is 1 and itself. Only the identity element is of order 1, hence the order of all other elements a must be p. This implies that a generates the entire group. Hence, $\langle g \rangle = G$. ■

Theorem 14.6

Let G be a finite group, and let $a \in G$. Then, $a^{|G|} = e$.

Proof: By Theorem 14.4, $|G|$ is a multiple of $|a|$. This means $|G| = k|a|$ for some integer k. Then, $a^{|G|} = a^{k|a|} = (a^{|a|})^k = e^k = e$. ■

Lecture 15: Normal subgroups and group homomorphisms

Definition 15.1 (Normal subgroup)

A subgroup H of a group G is normal in G, written $H \trianglelefteq G$, if $gH = Hg$ for all $g \in G$.

Example :

- If G is abelian and $H \leq G$, then $H \trianglelefteq G$.
- Let $n > 1$. Then, $A_n \triangleleft S_n$.

Example : Let G be a group and $H < G$ such that $[G : H] = 2$. Then, $H \triangleleft G$.

Proof : Since $[G : H] = 2$, then H has two cosets, namely H and xH for some $x \notin H$. If $a \in H$, then $aH = Ha = H$. If not, notice that $xH = G \backslash H$ and $Hx = G \backslash H$, so $xH = Hx$.

This means that $H \triangleleft G$. ■

Theorem 15.1 (Normal subgroup test)

Let G be a group and let H be a subgroup of G. Then $H \trianglelefteq G$ iff $xHx^{-1} \subseteq H$ for all $x \in G$.

Proof :

($\Longrightarrow$) Assume $H \trianglelefteq G$. Then, $xH = Hx$ for all $x \in G$. This implies $xHx^{-1} = H \subseteq H$.

($\Longleftarrow$) Suppose $xHx^{-1} \subseteq H$ for all $x \in G$. Then,

$$\begin{aligned} xHx^{-1} &\subseteq H \\ xH &\subseteq Hx \end{aligned}$$

$$\begin{aligned} x^{-1}Hx &\subseteq H \\ Hx &\subseteq xH \end{aligned}$$

Hence, $xH = Hx$ so $H \trianglelefteq G$. ■

Theorem 15.2

Let $H \trianglelefteq G$ and $K \leq G$. Then

$$HK = \{hk \mid h \in H, k \in K\}$$

is a subgroup of G.

Proof : $HK \neq \varnothing$ since $ee = e \in HK$. Let $h_1k_1, h_2k_2 \in HK$ where $h_1, h_2 \in H$ and $k_1, k_2 \in K$. We show that HK is a subgroup using the one-step subgroup test. Then,

$$\begin{aligned} (h_1k_1)(h_2k_2)^{-1} &= h_1k_1k_2^{-1}h_2^{-1} \\ (h_1k_1)(h_2k_2)^{-1} &= h_1k_1k_2^{-1}h_2^{-1}k_2k_2^{-1} \\ (h_1k_1)(h_2k_2)^{-1} &= h_1k_1(k_2^{-1}h_2^{-1}k_2)k_2^{-1} \end{aligned}$$

We can see that $k_2^{-1}h_2^{-1}k_2 \in H$. Let this be equal to h_3. Then, $(h_1k_1)(h_2k_2)^{-1} = h_1k_1h_3k_2^{-1}$. ■

Theorem 15.3

If $H \leq G$, then $xHx^{-1} \leq G$ for all $x \in G$.

Proof: It is trivial that $xHx^{-1} \neq \varnothing$ since $xex^{-1} = e \in xHx^{-1}$. Let $xh_1x^{-1}, xh_2x^{-1} \in xHx^{-1}$. Then,

$$(xh_1x^{-1})(xh_2x^{-1})^{-1} = xh_1x^{-1}xh_2x^{-1}$$
$$(xh_1x^{-1})(xh_2x^{-1})^{-1} = xh_1h_2^{-1}x^{-1}$$

Since $h_1, h_2 \in H$, then $h_1h_2^{-1} \in H$. This means $xh_1h_2^{-1}x^{-1}$ is in xHx^{-1}. Hence, $xHx^{-1} \leq G$ ■

Theorem 15.4

If $H \leq H$, then $|xHx^{-1}| = |H|$ for all $x \in G$.

A sketch of proof for this theorem is to use the bijective principle using the mapping $\rho : xHx^{-1} \to H$ defined by $\rho(xhx^{-1}) = h$.

Theorem 15.5

Let G be a group and H is a unique subgroup of finite order. Then $H \trianglelefteq G$.

Proof: Let $x \in G$. Assume $H \leq G$. By Theorem 15.3, $xHx^{-1} \leq G$. By Theorem 15.4, $|xHx^{-1}| = |H|$. Since H is the unique subgroup of order H, then $xHx^{-1} = H$ for all $x \in G$. This implies $xH = Hx$, so $H \trianglelefteq G$. ■

Theorem 15.6 (Factor Group/Quotient Group)

Let G be a group and let $H \trianglelefteq G$. The set of all left (right) cosets of H in G forms a group under the operation $(aH)(bH) = (ab)H$.

The factor group is denoted by G/H.

Note 15.1

G/H means G modulo H.

Proof: We will show that G/H is a group. First, we need to establish that the operation is well-defined. Let $aH = a'H$ and $bH = b'H$. Then, $a' = ah_1$ and $b' = bh_2$ for some h_1 and h_2 in H.

We show that $(ab)H = (a'b')H$.

$$(a'H)(b'H) = (a'b')H$$
$$(a'H)(b'H) = ah_1bh_2H$$
$$(a'H)(b'H) = ah_1bH$$
$$(a'H)(b'H) = ah_1Hb$$
$$(a'H)(b'H) = aHb$$
$$(a'H)(b'H) = abH$$

Hence, the operation is well-defined. Checking that the operation satisfies the group axioms is trivial, hence G/H is a group. ■

Definition 15.2 (Group homomorphism)

Let G and G' be groups. A homomorphism ϕ is a function $\phi : G \to G'$ that preserves group operations, that is,

$$\phi(a * b) = \phi(a) \cdot \phi(b)$$

for all $a, b \in G$.

Example : Consider the mapping $\phi : \mathbb{R}^* \to \mathbb{R}^*$ defined by $\phi(x) = |x|$. We claim that ϕ is a homomorphism.

Let $a, b \in \mathbb{R}^*$. Then,

$$\begin{aligned} \phi(ab) &= |ab| \\ \phi(ab) &= |a||b| \\ \phi(ab) &= \phi(a)\phi(b) \end{aligned}$$

Hence, ϕ is a homomorphism.

Example : The mapping $\theta : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\theta(x) = x \pmod n$ is a homomorphism.

Let $a, b \in \mathbb{Z}$. Then,

$$\begin{aligned} \theta(a+b) &= (a+b) \pmod n \\ \theta(a+b) &= a \pmod n \oplus b \pmod n \\ \theta(a+b) &= \theta(a) \oplus \theta(b) \end{aligned}$$

Hence, θ is a homomorphism.

Definition 15.3 (Kernel of homomorphism)

The kernel of a homomorphism $\phi : G \to G'$, denoted by $\ker \phi$, is defined as

$$\ker \phi = \{x \in G \mid \phi(x) = e'\}$$

where e' is the identity element in G'.

Example : To find the kernel for the previous examples,

$$\begin{aligned} \phi(x) &= 1 \\ |x| &= 1 \\ x &= \pm 1 \end{aligned}$$

Hence, $\ker \phi = \{-1, 1\}$.

$$\begin{aligned} \theta(x) &= 0 \\ x &\equiv 0 \pmod n \\ x - 0 &= nk \quad (\exists k \in \mathbb{Z}) \\ x &= nk \end{aligned}$$

This means that x is of the form nk where k is a particular integer. But notice that $\theta(nk) = nk \pmod n = 0$, so it doesn't matter which k is used. Therefore, $\ker \theta = \{nk \mid k \in \mathbb{Z}\}$.

Lecture 16: Properties of homomorphisms, and isomorphisms

Theorem 16.1

Let $\phi : G \to G'$ be a group homomorphism, and $g \in G$. Then,

1. $\phi(e) = e'$ where e and e' are the identity elements of G and G', respectively,
2. $\phi(g^n) = \phi(g)^n$ for all integers n,
3. If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$,
4. $\ker \phi \leq G$,
5. $\phi(a) = \phi(b)$ iff $a \ker \phi = b \ker \phi$,
6. If $\phi(g) = g'$, then $\phi^{-1}(g') = g \ker \phi$ where $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\}$.

Proof: We prove each item as follows:

1. Let $g \in G$ be arbitrary. We consider $\phi(ge)$ as follows:

$$\begin{aligned} \phi(ge) &= \phi(g) \\ \phi(g)\phi(e) &= \phi(g) \\ (\phi(g))^{-1}\phi(g)\phi(e) &= (\phi(g))^{-1}\phi(g) \\ \phi(e) &= e'. \end{aligned}$$

2. We first prove that $\phi(g^{-1}) = \phi(g)^{-1}$. We consider $\phi(gg^{-1})$ as follows:

$$\begin{aligned} \phi(gg^{-1}) &= \phi(e) \\ \phi(g)\phi(g^{-1}) &= e' \\ (\phi(g))^{-1}\phi(g)\phi(g^{-1}) &= \phi(g)^{-1} \\ \phi(g^{-1}) &= \phi(g)^{-1} \end{aligned}$$

There are two cases for n, and the first one is if $n \geq 0$. Then,

$$\begin{aligned} \phi(g^n) &= \phi(\underbrace{g \cdot g \cdots g}_{n \text{ times}}) \\ \phi(g^n) &= \underbrace{\phi(g) \cdot \phi(g) \cdots \phi(g)}_{n \text{ times}} \\ \phi(g^n) &= \phi(g)^n \end{aligned}$$

And if $n < 0$, then

$$\begin{aligned} \phi(g^n) &= \phi(g^{-|n|}) \\ \phi(g^n) &= \phi((g^{-1})^{|n|}) \\ \phi(g^n) &= \phi(g^{-1})^{|n|} \\ \phi(g^n) &= (\phi(g)^{-1})^{|n|} \\ \phi(g^n) &= \phi(g)^{-|n|} \\ \phi(g^n) &= \phi(g)^n \end{aligned}$$

3. Let $|g| = n$. Then, $g^n = e$. It follows that

$$\begin{aligned} \phi(g^n) &= \phi(e) \\ \phi(g)^n &= e' \end{aligned}$$

Hence, $|\phi(g)|$ divides n, so $|\phi(g)|$ divides $|g|$.

4. Let $a, b \in \ker\phi$. Then,

$$\begin{aligned}\phi(ab^{-1}) &= \phi(a)\phi(b^{-1}) \\ \phi(ab^{-1}) &= e'e' \\ \phi(ab^{-1}) &= e'\end{aligned}$$

Hence, $ab^{-1} \in \ker\phi$. By the one-step subgroup test, $\ker\phi \leq G$.

5. Suppose $\phi(a) = \phi(b)$. Then,

$$\begin{aligned}\phi(a) &= \phi(b) \\ \phi(b)^{-1}\phi(a) &= \phi(b)^{-1}\phi(b) \\ \phi(b^{-1})\phi(a) &= e' \\ \phi(b^{-1a}) &= e' \\ b^{-1}a &\in \ker\phi \\ b^{-1}a\ker\phi &= \ker\phi \\ bb^{-1}a\ker\phi &= b\ker\phi \\ a\ker\phi &= b\ker\phi\end{aligned}$$

The backward direction can be proven by simply doing the proof of the forward direction in reverse.

6. Suppose $\phi(g) = g'$. Let $y \in \phi^{-1}(g')$ be arbitrary. Then,

$$\begin{aligned}y &\in \phi^{-1}(g') \\ \phi(y) &= g' \\ \phi(y) &= \phi(g) \\ \phi(g)^{-1}\phi(y) &= e' \\ \phi(g^{-1})\phi(y) &= e' \\ \phi(g^{-1}y) &= e' \\ g^{-1}y &\in \ker\phi \\ g^{-1}y\ker\phi &= \ker\phi \\ y\ker\phi &= g\ker\phi\end{aligned}$$

Since $y \in y\ker\phi$, this implies $y \in g\ker\phi$. Hence, $\phi^{-1}(g') \subseteq g\ker\phi$.

Now, let $z \in g\ker\phi$ be arbitrary. Then,

$$\begin{aligned}z &= ga \qquad (\exists a \in \ker\phi) \\ \phi(z) &= \phi(ga) \\ \phi(z) &= \phi(g)\phi(a) \\ \phi(z) &= g'e' \\ \phi(z) &= g'\end{aligned}$$

which means $z \in \phi^{-1}(g')$. Hence, $g\ker\phi \in \phi^{-1}(g')$, and so $\phi^{-1}(g') = g\ker\phi$. ■

The last item gives us information about which elements also map to g', provided we know at least one element $g \in G$.

Note 16.1

Given a homomorphism $\phi : G \to G'$ and $H \leq G$, we define $\phi(H)$ as $\{\phi(h) \mid h \in H\}$.

Theorem 16.2

Let $\phi : G \to G'$ be a group homomorphism and let $H \leq G$. Then,

1. $\phi(H) \leq G'$.
2. If H is cyclic, then $\phi(H)$ is cyclic.
3. If H is abelian, then $\phi(H)$ is abelian.
4. If H is normal, then $\phi(H)$ is normal.
5. If $|\ker \phi| = n$, then ϕ is an n-to-1 mapping from G onto $\phi(G)$.
6. If $|H| = n$, then $|\phi(H)|$ divides n.

Proof:

1. Checking that $\phi(H)$ is nonempty is trivial, since the identity element of H is mapped onto $\phi(H)$. Let $h_1, h_2 \in H$. Then,

$$\phi(h_1)\phi(h_2)^{-1} = \phi(h_1)\phi(h_2^{-1})$$
$$\phi(h_1)\phi(h_2)^{-1} = \phi(h_1 h_2^{-1})$$

Since $h_1 h_2^{-1} \in H$, then $\phi(h_1 h_2^{-1} \in \phi(H))$. By the one-step subgroup test, $\phi(H) \leq G$.

2. Suppose H is cyclic. Then, there is an element $a \in H$ such that $H = \langle a \rangle$. We claim that $\phi(a)$ generates $\phi(H)$. Let $h \in H$ such that $\phi(h) \in \phi(H)$. Since H is cyclic, we can find an integer k such that $h = a^k$. Then,

$$h = a^k$$
$$\phi(h) = \phi(a^k)$$
$$\phi(h) = \phi(a)^k$$
$$\phi(H) \leq \langle \phi(a) \rangle.$$

Clearly, $\langle \phi(a) \rangle \leq \phi(H)$. Hence, $\phi(H) = \langle \phi(a) \rangle$, so $\phi(H)$ is cyclic.

3. Suppose H is abelian. Let $h_1, h_2 \in H$. Then,

$$\phi(h_1)\phi(h_2) = \phi(h_1 h_2)$$
$$\phi(h_1)\phi(h_2) = \phi(h_2 h_1)$$
$$\phi(h_1)\phi(h_2) = \phi(h_2)\phi(h_1)$$

Hence, $\phi(H)$ is abelian.

4. Suppose H is normal in G. Let $h \in H$, $g \in G$. We consider $\phi(g)\phi(h)\phi(g)^{-1}$:

$$\phi(g)\phi(h)\phi(g)^{-1} = \phi(g)\phi(h)\phi(g^{-1})$$
$$\phi(g)\phi(h)\phi(g)^{-1} = \phi(ghg^{-1})$$

Since H is normal, there is an $h_1 \in H$ such that $h_1 = ghg^{-1}$. Then,

$$\phi(g)\phi(h)\phi(g)^{-1} = \phi(h_1)$$
$$\phi(g)\phi(h)\phi(g)^{-1} \in \phi(H)$$

Therefore, $\phi(H)$ is normal in $\phi(G)$.

5. If $\phi(g) = g'$, then $\phi^{-1}(g') = g \ker \phi$. Since $|g \ker \phi| = |\ker \phi| = n$, then there are n elements mapped to g' where $g' \in \phi(G)$.
6. Trivial. ■

Theorem 16.3

Let $\phi : G \to G'$ be a homomorphism of groups. Then, $\ker \phi \trianglelefteq G$.

Proof: Let $g \in G$ and $x \in \ker \phi$. Consider gxg^{-1}:

$$\begin{aligned} \phi(gxg^{-1}) &= \phi(g)\phi(x)\phi(g^{-1}) \\ \phi(gxg^{-1}) &= \phi(g)e'\phi(g)^{-1} \\ \phi(gxg^{-1}) &= \phi(g)\phi(g)^{-1} \\ \phi(gxg^{-1}) &= e' \end{aligned}$$

Hence, $gxg^{-1} \in \ker \phi$, so $\ker \phi \trianglelefteq G$. ■

Definition 16.1 (Isomorphism)

Let $\phi : G \to G'$ be a homomorphism of groups. If ϕ is bijective, then ϕ is called an isomorphism.

Example: Let G be an abelian group. Let $\theta : G \to G$ where $\theta(g) = g^{-1}$. Then,

$$\begin{aligned} \theta(g_1g_2) &= (g_1g_2)^{-1} \\ \theta(g_1g_2) &= g_2^{-1}g_1^{-1} \\ \theta(g_1g_2) &= g_1^{-1}g_2^{-1} \\ \theta(g_1g_2) &= \theta(g_1)\theta(g_2) \end{aligned}$$

So θ is a homomorphism. We can see that θ is injective since

$$\begin{aligned} \theta(g_1) &= \theta(g_2) \\ g_1^{-1} &= g_2^{-1} \\ (g_1^{-1})^{-1} &= (g_2^{-1})^{-1} \\ g_1 &= g_2 \end{aligned}$$

And it is also surjective. Choose any $g \in G$. We can find an element in G that θ maps to g, and this is g^{-1}: $\theta(g^{-1}) = (g^{-1})^{-1} = g$.