Math103A
Modern Algebra

seraph

October 23, 2024

Contents

Chapter 1

Group and Subgroups

Lecture 2

1.1 Binary Operators

Definition 1.1.1. A binary operation $*$ on S is a function mapping every element in $S \times S$ into S

Exercise. Let $M(\mathbb{R})$ = set of all square matrices in $\mathbb{R}$, is $+$ a binary operator on M ?

Answer. No, because different sized matrices cannot add together. ⊛

Exercise. Let $\mathbb{Z}^+ = \{1, 2, 3, ...\}$, then we define $a * b = c$ s.t. c is at least 5 more than $a + b$, is $*$ a binary operator ?

Answer. No, because the output isn't unique. $1 * 2 = \{8, 9, 10...\}$. ⊛

Definition 1.1.2. If $(S, *)$ is a binary algebraic structure, then $H \subseteq S$ is closed under this operation iff $\forall\ a, b \in H$, $a * b \in H$

Note. If $M_2(\mathbb{R})$ are all 2×2 matrices over $\mathbb{R}$, then $(M_2(\mathbb{R}), +)$ is a proper algebraic structure.

Exercise. If $H \subseteq M_2(\mathbb{R})$, $H = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$, is H closed under $+$?

Answer. Yes ⊛

Proof. $\begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} a+c & -(b+d) \\ b+d & a+c \end{bmatrix} \in$ H ■

Exercise. Let $\mathbb{C} = \{a + bi : a, b \subseteq \mathbb{R}\}$, is $\mathbb{C}$ closed under addition and multiplication?

Answer. Yes, using Euler's formula we know that $a + bi = \sqrt{a^2 + b^2} e^{i\theta}$, so it will stay complex under $+$ and $\times$. ⊛

Exercise. Let $H \subseteq \mathbb{C}$ and $H = \{a + bi : \sqrt{a^2 + b^2} = 1\}$, is H closed under additon / multiplication?

Answer. It is closed under multiplication but not addition. ⊛

Example. Let $(S, *)$ and $(S', *)$ be two algebraic structures, we want to show whether they are the same.

Answer. Need to consider basic properties: $*$ is commutative $\Leftrightarrow a * b = b * a$
Let $\mathcal{F}$ = the set of functions $f : \mathbb{R} \to \mathbb{R}$, we argue that $f \circ g$ is not commutative ⊛

Proof. $\circ$ is not commutative on $\mathcal{F}$ because lets say h = $\sin(x)$, g = e^x, then

$$h \circ g = h(g(x)) = \sin(e^x) \in \mathcal{F}$$

$$g \circ h = g(h(x)) = e^{\sin(x)} \in \mathcal{F}$$

but $\sin(e^x) \neq e^{\sin(x)}$, so back to the question, it may or may not be the same depending on what $*$ is. ■

Definition 1.1.3. If we have a structure $(\mathcal{F}, \circ)$, then $\circ$ is associative, i.e. $f \circ (g \circ h) = (f \circ g) \circ h$

Proof. Computing them shows that they are equal

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$$

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$$

■

Exercise. $\mathbb{Z}^+ = \{1, 2, 3, 4...\}$, ans define $a * b = 2^{a \cdot b}$, is $(\mathbb{Z}^+, *)$ 1. commutative, 2. associative ?

Answer.

1. Yes, $a * b = 2^{a \cdot b} = 2^{b \cdot a} = b * a$
2. No, $2 * (3 * 4) \neq (2 * 3) * 4$ ⊛

Exercise. Given $(S, *)$ where $*$ is commutative and associative. Given $H \subseteq S$ where H = $\{a \in S : a * a = a\}$, show that H is closed under $*$.

Proof. $a * a = a$ and $b * b = b$, we can show $[a * b] * [a * b] = [a * b]$ because by associativity and commutativity

$$[a * b] * [a * b] = a * b * a * b = a * a * b * b = a * b$$

■

Lecture 3

Definition 1.1.4. Let $(S, *)$ be an algebraic structure, and $e \in S$ s.t. $\forall a \in S$, $a * e = a = e * a$ Then e is called the identity element of S.

Example.
$(\mathbb{Z}, +)$ has identity element 0.
$(\mathbb{Z}^+, \times)$ has identity element 1.
$(\mathbb{Z}^+, +)$ has no identity element.

Theorem 1.1.1. If (S, *) has an identity element, it is unique.

Proof. For sake of contradiction, suppose e and e' are both identity elements of S. Then $e = e * e' = e'$. ■

Definition 1.1.5. Let $(S, *)$ be an algebraic structure, and $x \in S$. If $\exists\, x' \in S$ s.t. $x * x' = x' * x = e$, then x' is called the inverse of x.

Example.
$(\mathbb{Z}, +)$, the inverse of a is $-a$.
$(\mathbb{Z}^+, +)$, has no inverses
$(\mathbb{Z}, \times)$, the inverse of a is $\frac{1}{a}$ if $a \neq 0$.

1.2 Groups

Definition 1.2.1. A group is an algebraic structure $(G, *)$ if:

1. $*$ is associative.
2. $\exists$ an identity element $e \in G$.
3. $\forall a \in G$, $\exists$ an inverse $a' \in G$.

Example. G $= \{e, a, b\}$ where

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad a = \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}, \quad b = \begin{bmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$$

$(G, \times)$ where $\times$ is standard matrix multiplication is a group.
$(G, +)$ where $+$ is standard matrix addition is not a group because it is not closed under addition.

Definition 1.2.2. A group $(G, *)$ is **abelian** if $\forall a, b \in G$, $a * b = b * a$.

Example. Consider $(\mathbb{Q}^+, *)$ where $*$ is defined by $a * b = \frac{ab}{2}$.
Associativity: For any $a, b, c \in \mathbb{Q}^+$,

$$(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{\left(\frac{ab}{2}\right) c}{2} = \frac{abc}{4} = a * (b * c)$$

Thus, $*$ is associative.
Identity element: We need $e \in \mathbb{Q}^+$ such that $\forall a \in \mathbb{Q}^+$,

$$a * e = \frac{ae}{2} = a \quad \text{and} \quad e * a = \frac{ea}{2} = a$$

Solving $\frac{ae}{2} = a$ gives $e = 2$. Thus, 2 is the identity element.
Inverses: For any $a \in \mathbb{Q}^+$, we need $a' \in \mathbb{Q}^+$ such that

$$a * a' = \frac{aa'}{2} = 2 \quad \text{and} \quad a' * a = \frac{a'a}{2} = 2$$

Solving $\frac{aa'}{2} = 2$ gives $a' = \frac{4}{a}$. Thus, every element has an inverse.
Therefore, $(\mathbb{Q}^+, *)$ is a group.
Commutativity: For any $a, b \in \mathbb{Q}^+$,

$$a * b = \frac{ab}{2} = \frac{ba}{2} = b * a$$

Thus, $(\mathbb{Q}^+, *)$ is an abelian group.

Theorem 1.2.1. Let $(G, *)$ be a group. Then

1. The identity element is unique (Theorem 1.1.1).
2. Every element has a unique inverse .

Proof. Let a, a', a'' be inverses of $a \in G$. Then $a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$. ∎

Corollary 1.2.1. Let $(G, *)$ be a group and $a, b \in G$. If $a * b \in G$, then the inverse of $(a * b)$ is $b' * a'$, where b' is the inverse of b and a' is the inverse of a.

Proof.

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

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

∎

Lecture 4

1.3 Abelian Groups

Example. $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ is an albelian group under addition.

Example. Let $\mathbb{R}^2 = \left\{ \begin{bmatrix} a \\ b \end{bmatrix} : a, b \in \mathbb{R} \right\}$, $(\mathbb{R}^2, +)$ is an albelian group.

Example. Let $\mathbb{P}_1 = \{ax + b : a, b \in \mathbb{R}\}$. , $(\mathbb{P}_1, +)$ is an albelian group.

Definition 1.3.1. A **group isomorphism** is a bijective group homomorphism. Specifically, if $(G, *_1)$ and $(H, *_2)$ are groups, a function $\phi : G \to H$ is called a group isomorphism if:

1. ϕ is a homomorphism, i.e., $\forall a, b \in G, \phi(a *_1 b) = \phi(a) *_2 \phi(b)$.
2. ϕ is bijective, i.e., ϕ is both injective (one-to-one) and surjective (onto).

If such a function ϕ exists, we say that G and H are **isomorphic** and write $G \cong H$.

Exercise. Let $(\mathbb{Z}, +)$ and $(2\mathbb{Z}, +)$ be groups under addition. Define the function $\phi : \mathbb{Z} \to 2\mathbb{Z}$ by $\phi(n) = 2n$ for all $n \in \mathbb{Z}$. Do we have an isomorphism between $(\mathbb{Z}, +)$ and $(2\mathbb{Z}, +)$?

Answer.

1. ϕ is a homomorphism: For all $a, b \in \mathbb{Z}$,

$$\phi(a + b) = 2(a + b) = 2a + 2b = \phi(a) + \phi(b).$$

2. ϕ is bijective:
   - Injective: Suppose $\phi(a) = \phi(b)$. Then $2a = 2b$, which implies $a = b$. (For an output check if the input are the same)
   - Surjective: For any $m \in 2\mathbb{Z}$, there exists $n \in \mathbb{Z}$ such that $m = 2n$. Hence, $\phi(n) = m$.

Therefore, ϕ is an isomorphism, and $(\mathbb{Z}, +) \cong (2\mathbb{Z}, +)$. ⊛

Lecture 5

1.3.1 More Abelian Examples

Example. $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ where $+_n$ is addition modulo n. When a, b $\in \mathbb{Z}_n$, $a +_n b = (a+b)$ mod n.
• Many groups are isomorphic to $\mathbb{Z}_n$.

Remark (Fact). Any group of size 1 is isomorphic to $\mathbb{Z}_1$.

Exercise. If we have a group $\mathbb{Z}_2 = 0, 1$ equipped with $(\mathbb{Z}_2, +)$ and an abstract group $G = \{e, a\}$. Do these groups have the same structure?

Answer. We can check its operation table.

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \cong \quad \begin{array}{c|cc} * & \text{e} & \text{a} \\ \hline \text{e} & \text{e} & \text{a} \\ \text{a} & \text{a} & \text{e} \end{array}$$

⊛

Remark (Fact). Any group of size 2 is isomorphic to $\mathbb{Z}_2$.

Exercise. Let $G = \{I, A, B\}$ where I is the identity matrix, $A = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$, and $B = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$.
Is this group isomorphic to $\mathbb{Z}_3$?

Answer. This is also isomorphic to $\mathbb{Z}_3$.
We can check it using the same method as above. ⊛

Remark (Fact). All groups on 3 elements is isomorphic to $\mathbb{Z}_3$.

Theorem 1.3.1. Let $(G, *)$ be a group. If we fix $a, b \in G$, then:

1. $a * x = b$ has a unique solution for x.
2. $y * a = b$ has a unique solution for y.

Example. $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ and the Klein 4-group $V_4 = \{e, a, b, c\}$ with their operation tables:

$$\begin{array}{c|cccc} + & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array} \quad \ncong \quad \begin{array}{c|cccc} * & \text{e} & \text{a} & \text{b} & \text{c} \\ \hline \text{e} & \text{e} & \text{a} & \text{b} & \text{c} \\ \text{a} & \text{a} & \text{e} & \text{c} & \text{b} \\ \text{b} & \text{b} & \text{c} & \text{e} & \text{a} \\ \text{c} & \text{c} & \text{b} & \text{a} & \text{e} \end{array}$$

Proof. Check the diagonals and it is clear that they are not isomorphic. ■

Theorem 1.3.2. Every group on 4 elements is isomorphic to either $(\mathbb{Z}_4, +)$ or $(V, *)$.

Partial proof. Generate all possible tables and check if they are isomorphic to $(\mathbb{Z}_4, +)$ or $(V, *)$. Turns out they will only be isomorphic to one of these two groups. ■

Lecture 6

1.3.2 Circle Algrbra

Example. Define $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$. Then $(\mathbb{C}, +)$ is an abelian group.

Remark. $(\mathbb{C}, \times)$ is not abelian group because 0 does not have an inverse.

> **Note.** So we come up with a notation $\mathbb{C}^* = \mathbb{C} - \{0\}$. $(\mathbb{C}^*, \times)$ is an abelian group.

Note (Euler's Formula). z $\in \mathbb{C}^*$, $z = a + bi$. Then $z = |z|e^{i\theta}$. where $|z| = \sqrt{a^2 + b^2}$ and $\theta = \arctan(\frac{b}{a})$.

Example. 1. Let $u = \{z \in \mathbb{C}^*, |z| = 1\}$. Then $(u, \times)$ is an abelian group.

Example (Roots of Unity). Let $n \in \mathbb{N}$. Then $u_n = \{z \in \mathbb{C}^*, z^n = 1\}$.

1. $u_1 = \{1\}$.
2. $u_2 = \{1, -1\}$.
3. $u_3 = \{1, e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}\}$.
4. $u_4 = \{1, i, -1, -i\}$.
5. $u_n = \{e^{\frac{2\pi ik}{n}} \mid k = 0, 1, 2, \ldots, n-1\}$.

> **Note.** $(u_n, \times)$ is an abelian group of order n. Also, $u_n \cong \mathbb{Z}_n$.

1.4 Non Abelian Groups

1.4.1 Permutation Groups

Note (Notation). From now on, if $(G, *)$ is a group, we will write a*b as ab.
a^k means $a * a * \ldots * a$ (k times).
a^{-k} means $a^{-1} * a^{-1} * \ldots * a^{-1}$ (k times).
Operator should be clear from context so most of the time we will omit it.

Definition 1.4.1. The order of a group G is the number of elements in G.

Definition 1.4.2. Let A be a set. A permutation of A is a bijection $\phi : A \to A$.

Example. Let $A = 1, 2, 3, 4, 5$
Let σ be a permutation of A. Then $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}$.

Definition 1.4.3. Let's define a composite operator on S_A. Let $\sigma, \tau \in S_A$. Then $\sigma \circ \tau$ is a permutation of A defined by $(\sigma \circ \tau)(x) = \sigma(\tau(x))$.

Theorem 1.4.1. A set $(S_A, \circ)$ is a group.

Proof.

1. Associativity: Let $\sigma, \tau, \rho \in S_A$. Then $(\sigma \circ \tau) \circ \rho = \sigma \circ (\tau \circ \rho)$.
2. Identity: The identity element is the identity permutation $id(x) = x$.
3. Inverse: Let $\sigma \in S_A$. Then σ^{-1} is the inverse of σ. This reverse the mapping of σ.

■

Lecture 7

Example (Finite Setting)**.** Let $A = \{1, 2, 3, \cdots, n\}$.
$S_A = S_n =$ the symmetric group on n letters. $(S_n, \circ)$ is a group.

Remark. $|S_n| = n!$.

Example. Let $\sigma \in S_6$ and we define σ with the two row notation as follows:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 2 & 5 & 1 \end{pmatrix}$$

Example (Disjoint Cycles)**.** There is a notion that is 1. shorter and 2. more "natural":

$$\sigma = (1, 3, 6)(2, 4)$$

Definition 1.4.4 (Dihedral Group)**.** Let $D_n \in S_n$.
$P_n =$ regular n-gon in the plane with vertices $0, 1, 2, \cdots n-1$ in counter-clockwise order with origin at $(1, 0)$.

$$D_n = \{e, \rho, \rho^2, \rho^3, \ldots, \rho^{n-1}, \mu, \mu\rho, \ldots, \mu\rho^{n-1}\}$$

where ρ is a counter-clockwise rotation and μ is a horizontal reflection.

Definition 1.4.5. D_n is the set of permutations (bijections) $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ such that ϕ preserves the distance between vertices of P_n.

Theorem 1.4.2. D_n are reflections and rotations of P_n. $|D_n| = 2n$.

Theorem 1.4.3. D_n is a group under composition.

Lecture 8

1.5 Subgroups

As previously seen. If $\mathbb{C}^*$ is a nonzero complex number, then $(\mathbb{C}^*, \times)$ is a group. We also know that $(U_n, \times)$ is a group and $(U_n, \times) \in \mathbb{C}^*$.

Definition 1.5.1. Let G be a group. If $H \in G$, and H is a group under the same operator as G, then H is called a subgroup of G.

Remark. From the previous definition, we can see that $(U_n, \times)$ is a subgroup of $(\mathbb{C}^*, \times)$.

Example. Let G be a group. If $G = \{e, \cdots\}$ and $H = e$, then H is a subgroup of G. H is called the trivial subgroup.

Proof.

1. H is closed under the same operator as G.
2. H is associative under the same operator as G.
3. H has an identity element under the same operator as G.
4. H has an inverse element under the same operator as G.

■

Exercise. Let $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ and $+_4$ is addition mod 4. Analyze the subgroups of this group.

Answer. Let H $= \{0, 1\}$, then H is NOT a subgroup of G. Because H is not closed under $+_4$. However, if $H = \{0, 2\}$, then H is a subgroup of G. We also have the trivial subgroup $H = \{0\}$. ⊛

As previously seen. Recall that there are exactly two 2 non-isomporphic groups of size 4. One is $\mathbb{Z}_4$ and the other is the Klein 4-group.

Note.

Subgroup Diagram of $\mathbb{Z}_4$

$$\begin{tikzcd}
\mathbb{Z}_4 \arrow[d] \\
\{0, 2\} = H \arrow[d] \\
\{0\}
\end{tikzcd}$$

Subgroup Diagram of Klein 4-group

$$\begin{tikzcd}
 & V \arrow[dl] \arrow[d] \arrow[dr] & \\
\{e, a\} = H_1 \arrow[dr] & \{e, b\} = H_2 \arrow[d] & \{e, c\} = H_3 \arrow[dl] \\
 & \{e\} &
\end{tikzcd}$$

Theorem 1.5.1. Let G be a group. If $H \in G$, then H is a subgroup of G if and only if:

1. H is closed under the same operator as G.
2. H has an identity element under the same operator as G.
3. H has an inverse element under the same operator as G.

Remark. If $H \in G$ is finite, then it's easier to check if H is a subgroup of G.

Theorem 1.5.2. If G is a group and we have a finite subset $H \in G$. Then it is a subgroup of G if and only if it is closed under the same operator on G.

Proof.
($\Rightarrow$) If H is a subgroup of G, then by definition of being a subgroup, H is closed under this operator.
($\Leftarrow$) H is finite, and $|H| = n$. We know H is closed under the same operator as G. We can check the properties:

1. H is closed under the same operator as G. (Given)
2. Identity: $|H| = n$, and $H = \{a^1, a^2, \cdots, a^n, a^{n+1}\}$. By pigeonhole principle, there exists 2 elements a^i, a^j and $i < j$ that are the same.

$$a^{-i}a^i = a^{-i}a^j$$

$$e = \underbrace{a^{-1}a^{-1}\dots a^{-1}}_{i \text{ times}}\underbrace{aaa\dots a}_{i \text{ times}} = \underbrace{a^{-1}a^{-1}\dots a^{-1}}_{i \text{ times}}\underbrace{aaa\dots a}_{j \text{ times}} = a^{j-i}$$

Therefore e is in H.

3. Inverse: Let $a \in H$, we need to find $a^{-1} \in H$. $|H| = n$, and $H = \{a^1, a^2, \cdots, a^n, a^{n+1}\}$. By pigeonhole principle, there exists 2 elements a^i, a^j and $i < j$ that are the same.

Case 1: Suppose $j - i = 1$, then $a = a^{-1} = e \in H$.
Case 2: Suppose $j - 1 \geq 2$, then we multiply a^{-1} to both sides of $e = a^{j-i}$. Then by construction of the list:
$$a^{-1} = a^{-1}e = a^{-1}a^{j-i} = a^{j-i-1} \in H$$

■

Lecture 9

1.5.1 Cyclic Subgroups

Exercise. Let $\mathbb{Z}_{12} = \{0, 1, 2, \cdots, 11\}$ and H is the trivial subgroup. What is the smallest subgroup of $\mathbb{Z}_{12}$ that contains 3?

Answer. Let H $= \{0, 3, 6, 9\}$, we can see that this is the smallest because we use 3 to generate the other numbers. Additionally, H is isomorphic to $\mathbb{Z}_4$. ⊛

Remark. If G is a group and H is a subgroup of G.
If $a \in H$ then $a^n \in H \quad \forall \quad n \in \mathbb{Z}$. where $a^0 = e$ is the identity element.

Theorem 1.5.3. Let G be a group and $a \in G$ and set H $= \{a^n : n \in \mathbb{Z}\}$, then H is a subgroup, and it's the smallest subgroup of G that contains a.

Proof.

1. H is closed: Given $a^r, a^s \in H$, then $(a^r)(a^s) = a^{r+s} \in H$.
2. H has an identity element: $e = a^0 \in H$.
3. H has an inverse element: $a^r \in H$, take $a^{-r} \in H$ such that $a^r(a^{-r}) = a^{-r}(a^r) = e$.

■

Definition 1.5.2. Let G be a group and $a \in G$. If $H = \{a^n : n \in \mathbb{Z}\}$, then H is called the cyclic subgroup generated by a. We denote $H = \langle a \rangle$.

Definition 1.5.3. A group G is cyclic if $G = \langle a \rangle$ for some $a \in G$.

Example. $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ is a cyclic group $= \langle 1 \rangle$.

Example. $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ is a cyclic group $= \langle 1 \rangle$. 1 is a generator for $\mathbb{Z}_4$. We can see 3 is also a generator for $\mathbb{Z}_4$. But 2 is not a generator for $\mathbb{Z}_4$.

Example. $U_n =$ the n^{th} roots of unity.

$$U_n = \{e^{2\pi ik/n} : k = 0, 1, 2, \cdots, n-1\}$$

So this is a cyclic group generated by $e^{2\pi i/n}$. So $U_n = \langle e^{2\pi i/n} \rangle$.

Exercise. S_{10} is a permutation on $A = \{1, 2, \cdots, 10\}$. $\sigma = (1, 10)(2, 9)(3, 8)(4, 7)(5, 6)$
Compute $|\langle \sigma \rangle|$.

Answer. $\sigma \circ \sigma = (1, 10)(2, 9)(3, 8)(4, 7)(5, 6) \circ (1, 10)(2, 9)(3, 8)(4, 7)(5, 6) = (1)(2)(3) \cdots (10) = i$
So $|\langle \sigma \rangle| = 2$. ⊛

1.6 Cyclic Groups

Theorem 1.6.1. Every cyclic group is abelian.

Proof. Let $G = \langle a \rangle$ be a cyclic group.
Let $a^r, a^s \in G$.
Then

$$(a^r)(a^s) = a^{r+s} = a^{s+r} = (a^s)(a^r)$$

So G is abelian. ■

Example. Let $\mathbb{Z}_{10} = \{0, 1, 2, \cdots, 9\}$.

$$\langle 2 \rangle = \{0, 2, 4, 6, 8\}$$

did not generate all of $\mathbb{Z}_{10}$.

$$\langle 3 \rangle = \{0, 3, 6, 9, 2, 5, 8, 1, 4, 7\}$$

generated all of $\mathbb{Z}_{10}$.
You can check if they have a common divisor or not to determine if they generate all of $\mathbb{Z}_{10}$.

Theorem 1.6.2 (Division Algorithm)**.** $n = qm + r$

Theorem 1.6.3. Let G be a cyclic group. Then any subgroup of G is also cyclic.

Lecture 10

Theorem 1.6.4. If $G = \langle a \rangle$

1. If $|G| = \infty \implies G \cong (\mathbb{Z}, +)$
2. If $|G| = n \implies G \cong (\mathbb{Z}_n, +_n)$

Proof. Case 1:
Suppose $|G| = \infty$, For all positive $m \geq 1$, $a^m \neq e$
Goal is show that $G \cong (\mathbb{Z}, +)$
We need to check all elements in G are distinct. For sake of contradiction, suppose there exists i $<$ j such that:

$$a^i = a^j \Rightarrow e = a^{j-i}$$

But j-i is a positive integer. This contradicts the assumption that $a^m \neq e$ for all positive m, so every element in G is distinct.
So we can define:

$$\phi : G \to \mathbb{Z}, \phi(a^i) = i$$

This is a bijection.
Case 2:
There exists positive $m > 0$ such that $a^m = e$.
Again we define $\phi : G \to \mathbb{Z}_m$ by $\phi(a^i) = i \mod m$

■

Example. Let $\mathbb{Z}_{12} = \{0, 1, 2, \cdots, 11\}$ equipped with addition modulo 12.
Let $\langle 3 \rangle$ = the subgroup of $\mathbb{Z}_{12}$ generated by 3.
We get $\langle 3 \rangle = \{0, 3, 6, 9\}$
$|\langle 3 \rangle| = 4$
$\langle 8 \rangle = \{0, 8, 4\}$
$|\langle 8 \rangle| = 3$

Remark. The size of a subgroup of a finite cyclic group depends on the divisors.

Definition 1.6.1 (Greatest Common Divisor)**.** Fix integers r and s. gcd(r, s) is the largest positive integer that divides both r and s.

Definition 1.6.2. Fix r and s. The gcd(r, s) is the generator of the cyclic subgroup of

$$H = \{n \cdot r + m \cdot s : n, m \in \mathbb{Z}\} \leq \mathbb{Z}$$

$H = \langle \gcd(r, s) \rangle$

Corollary 1.6.1. Fix r and s. If there exists $m, n \in \mathbb{Z}$ such that $n \cdot r + m \cdot s = 1$, then $\gcd(r, s) = 1$. So r and s are coprime.

Proof.

> **As previously seen.** Recall that let $G = \langle a \rangle$. If G is a cyclic group generated by a, then ANY subgroup of G is also cyclic.

$(\mathbb{Z}, +) = \langle 1 \rangle$
Fix r and s. $H \subseteq \mathbb{Z}$ and $H = \{m \cdot r + n \cdot s : m, n \in \mathbb{Z}\}$

By the above theorem, $(H, +)$ is cyclic because it is a subgroup of a cyclic group.
Now we also show that H is a subgroup:

1. H is closed under addition: $m_1 \cdot r + n_1 \cdot s + m_2 \cdot r + n_2 \cdot s = (m_1 + m_2) \cdot r + (n_1 + n_2) \cdot s$
2. Identity: $0 \cdot r + 0 \cdot s = 0$
3. H is closed under inverses: $m \cdot r + n \cdot s \Rightarrow -m \cdot r + -n \cdot s$, and $(mr + ns) + (-mr - ns) = 0$

■

Example. $\mathbb{Z}_4 = \{0, 1, 2, 3\}$
All subgroups of $\mathbb{Z}_4$ are cyclic.
$\langle 0 \rangle = \{0\}$
$\langle 1 \rangle = \{0, 1, 2, 3\} \cong \mathbb{Z}_4$
$\langle 2 \rangle = \{0, 2\} \cong \mathbb{Z}_2$
$\langle 3 \rangle = \{0, 1, 2, 3\} \cong \mathbb{Z}_4$

Theorem 1.6.5. Let $G = \langle a \rangle$ be a cyclic group of order n.
$G = \{e, a, a^2, \cdots, a^{n-1}\}$

1. Let $a^s \in G$, then $|H| = |\langle a^s \rangle| = \frac{n}{\gcd(n,s)}$
2. Moreover, $a^s, a^t \in G$, if $gcd(s, n) = d = gcd(t, n)$, then $\langle a^s \rangle = \langle a^t \rangle$

Proof. Let m be the smalllest positive integer such that $(a^s)^m = e$.
We want to show that $|H| = m = \frac{n}{d}$.
If $(a^s)^m = e$, then $a^{sm} = e = (a^{s \cdot m})$
Which will have some multiple of n on the exponent.
Let d = gcd(s, n).
We know $d = u \cdot n + v \cdot s$ for some integers u, v $\in \mathbb{Z}$.

$$1 = u(\frac{n}{d}) + v(\frac{s}{d})$$

$(\frac{n}{d})$ and $(\frac{s}{d})$ are coprime from the corollary above.
We know $s \cdot m$ is a multiple of n. It follows that $(\frac{sm}{n}) = (\frac{m\frac{s}{d}}{\frac{n}{d}})$ is an integer.
Hence, $(\frac{n}{d})$ must divide m. ■

Lecture 11