Math103A
Modern Algebra

seraph

December 4, 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.

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

⊛

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:

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

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

1.6.1 Generating Sets & Cayley Digraphs

As previously seen. Recall that let $G = \langle a \rangle$. Then

1. $G = \{e, a, a^2, \cdots, a^{n-1}, a^{-1}, a^{-2}, \cdots, a^{-n+1}\}$

2. G is generated by a.

3. If $G \subseteq H$, (G is a subgroup of H), then G is the smallest subgroup of H containing a.

Let us generalize the idea of generating with 1 element.

Example. $\mathbb{Z}_4 = \langle 1 \rangle$ which is cyclic. But we also know Klein 4-group, let us call it V. $(V, *)$ is not cyclic.
But what about $\langle a, b \rangle$?
$V = \langle a, b \rangle = \{e, a, b, c\}$, so this set $\{a, b\}$ generates the Klein-4 group

Example. The Dihedral group D_n is the set of permutations of $\mathbb{Z}_n$ that are the rotations and reflections of a regular n-gon.
We know it is not cyclic because the operations are not communitive.
But D_n can be generated by 2 elements, $\{\rho \& \mu\}$.

Exercise. Does $\{2, 3\}$ generate $\mathbb{Z}_1 2$?

Answer. Yes, because this generates $H = \{2n + 3m : n, m \in \mathbb{Z}\}$
$H = \langle \gcd(2, 3) \rangle = \langle 1 \rangle = \mathbb{Z}_{12}$

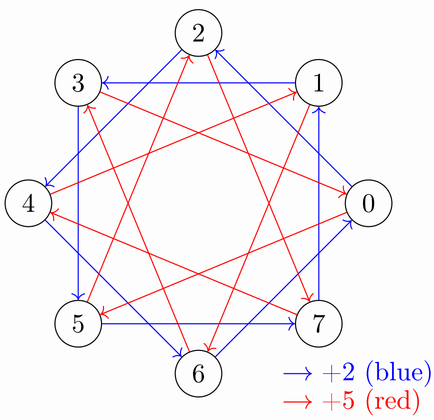
⊛

Lecture 13

Definition 1.6.3. Let G be a group. A Cayley digraph $C = (V, E)$ is a directed graph where $V = G$ and $E = \{(g, g \cdot a) : g \in G, a \in A\}$
Where A is a generating set of G.

Example. Let $G = \mathbb{Z}_8 = \{0, 1, 2, \cdots, 7\}$
Let $S = \{2, 5\}$
The Cayley digraph for G with S is shown below.

Answer.



Cayley Digraph for Z_8 with $S = \{2, 5\}$

⊛

Chapter 2

Structure & Groups

2.1 Groups of Permutations

Theorem 2.1.1 (Cayley's Theorem). Every group is isomorphic to a group of permutations.

Example. Roots of unity. Let $\omega = e^{\frac{2\pi i}{n}}$

$$U_6 = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5\}$$
$$U_3 = \{1, \omega^2, \omega^4\}$$

It is obvious that there is no isomorphism between U_6 and U_3.
But we can define a homomorphism $\phi : U_6 \to U_3$

Answer. We can define $\phi : U_6 \to U_3$ by $\phi(\omega) = \omega^2$
Let $z1, z2 \in U_6$

$$\phi(z1 \cdot z2) = (z1 \cdot z2)^2 = z1^2 \cdot z2^2 = \phi(z1) \cdot \phi(z2)$$

⊛

Lecture 14

Definition 2.1.1 (Images).

1. $\phi[a] = \{\phi(a) : a \in A\}$ This is called the image of ϕ

2. $\phi^{-1}[b] = \{a : \phi(a) = b\}$ This is called the pre-image of ϕ

Definition 2.1.2 (Properties of a homomorphism). Let G, G' to be groups.
Then ϕ is a homomorphism if $\forall a, b \in G$

$$\phi(ab) = \phi(a)\phi(b)$$

Theorem 2.1.2. Let G, G' to be groups.
Define $\phi : G \to G'$ as a homomorphism.
Then:

1. For e ∈ G, $\phi(e) = e' \in G'$
2. $[\phi(a)]^{-1} = \phi(a^{-1})$
3. If H is a subgroup of G, then $\phi[H]$ is a subgroup of G'
4. ★ If K' is a subgroup of G', then $\phi^{-1}[K']$ is a subgroup of G

Try to draw images for these for better intuition.

Definition 2.1.3 (Kernel). Let G, G' to be groups.
Define $\phi : G \to G'$ as a homomorphism.
We define:

$$\phi^{-1}[\{e\}] = x \in G : \phi(x) = e'$$

This is called the kernel of ϕ and is denoted by $ker(\phi)$

Example. Let $\mathbb{Q}^* = \mathbb{Q}/\{0\}$
Let $G = (\mathbb{Q}^*, \times)$
Let

$$\phi : \mathbb{Q}^* \to \mathbb{Q}^*, \phi(x) = |x|$$

Then ϕ is not a isomorphism, but it is still a homomorphism.
Then $ker(\phi) = \{-1, 1\}$

Exercise. $\mathbb{Z} = (\mathbb{Z}, +)$
$\mathbb{Z}_8 = (\mathbb{Z}_8, +)$
Let $\phi(1) = 6$ What is $ker(\phi)$?

Answer. $\phi(24) = \phi(1) + \phi(1) + \cdots + \phi(1) = 24 \cdot 6 = 144 = 0$
We notice that $ker(\phi) = \langle 4 \rangle$

⊛

Exercise. $\mathbb{Z} \times \mathbb{Z}$ is the cartesian product on the integers.
$(a, b) \in \mathbb{Z} \times \mathbb{Z}$
Let's define a cooredinate-wise addition

$$(a, b) + (c, d) = (a + c, b + d)$$

Let $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ where $\phi(0, 1) = -5, \phi(1, 0) = 3$
What is $ker(\phi)$?

Answer. Let $(a, b) \in \mathbb{Z} \times \mathbb{Z}$
$\phi(a, b) = \phi(a, 0) + \phi(0, b) = a \cdot \phi(1, 0) + b \cdot \phi(0, 1)$
$\phi(a, b) = a \cdot 3 + b \cdot -5$
$\phi(a, b) = 0 \Rightarrow 3a - 5b = 0$
$3a = 5b$
$a = 5k, b = 3k$
$ker(\phi) = \langle (5, 3) \rangle$

⊛

Lecture 15

Note. So far, all groups of permutations we've seen are equipped with the composition operation.

Example. $\mathbb{Z}_n$ is not a permtuation group. $\mathbb{Z}_n \cong$ (group of permutations).

Example. σ^i can be defined in two row notation as:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & ... & n \\ 1+i & 2+i & 3+i & 4+i & ... & n+i \end{pmatrix}$$

$\sigma^n = \sigma^0 = i$.

Also $\langle \sigma \rangle = \{e, \sigma, \sigma^2, ..., \sigma^{n-1}\}$.

Remark. $\langle \sigma \rangle \cong (\mathbb{Z}_n, +_n)$.

Exercise. Let GL(n, R) be the set of all invertible n x n matrices with real entries. Let G = (GL(n, R), $\times$).
Is this a permutation group?

Answer. Yes, because $A : \mathbb{R}^n \to \mathbb{R}^n$ is a bijection of $\mathbb{R}^n$ if and only if A is invertible.

⊛

Theorem 2.1.3 (Cayley's Theorem)**.** Every group G is isomorphic to a group of permutations.

Corollary 2.1.1. Every finite group G is isomorphic to a subgroup of S_n for a sufficiently large n.

Definition 2.1.4 (Properties of S_n)**.** Let S_n be the permutation group on $\{1, 2, ..., n\}$.
$|S_n| = n!$.
Let us define A_n and B_n as follows: A_n is the alternating group on $\{1, 2, ..., n\}$, i.e. the set of all even permutations.
B_n is the set of all odd permutations.

Definition 2.1.5. A cycle of length 2 is called a transposition.

Theorem 2.1.4. Any $\sigma \in S_n$ can be written as a product of transpositions.
Another way to think of this is any permutation can be obtained by swapping pairs

Exercise. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 2 & 8 & 4 & 7 & 6 & 1 \end{pmatrix}$.

We get $\sigma = (1, 5, 4, 8)(2, 3)(6, 7)$.
$= (1, 8)(1, 4)(1, 5)(2, 3)(6, 7)$.

Theorem 2.1.5. If $\sigma \in S_n$, then *sigma* cannot be expressed as both an even and an odd number of transpositions.

Definition 2.1.6. $S_n = A_n \cup B_n$.
Where A_n is the set of all even permutations and B_n is the set of all odd permutations.
$|A_n| = |B_n| = \frac{n!}{2}$.

Lecture 16

2.2 Finitely Generated Abelian Groups

Note. The motivation for this section is to use known examples of abelian and non-abelian groups and construct larger groups with them via cartisian product.

Theorem 2.2.1. Suppose we have n groups $G_1, G_2, ..., G_n$. Then we calculate cartesian product $G = G_1 \times G_2 \times ... \times G_n$ s.t. $(a_1, a_2, ..., a_n) \in G$. Define $*$ on G where $(a_1, a_2, ..., a_n), (b_1, b_2, ..., b_n) \in G$ Then:

$$(a_1, a_2, ..., a_n) * (b_1, b_2, ..., b_n) = (a_1b_1, a_2b_2, ..., a_nb_n)$$

G is a group with identity $(e_1, e_2, ..., e_n)$ and inverse $(a_1, a_2, ..., a_n)^{-1} = (a_1^{-1}, a_2^{-1}, ..., a_n^{-1})$.

As previously seen. Recall two definitions of order:

1. Order of a group: $G = |G|$.
2. Order of an element: smallest positive integer n s.t. $a^n = e$. Moreover, $n = |\langle a \rangle|$.

Example. $\mathbb{Z}_2 = \{0, 1\}$, and $\mathbb{Z}_3 = \{0, 1, 2\}$.
$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}$.
$|\mathbb{Z}_2 \times \mathbb{Z}_3| = 2 \times 3 = 6$.

Remark. $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ and is cyclic. It's generator is $(1, 1)$.

Exercise. We have $|\mathbb{Z}_3 \times \mathbb{Z}_3| = 9$. Is $\mathbb{Z}_3 \times \mathbb{Z}_3$ cyclic?

Answer. Find whether there exists an element of order 9.
The answer is no. Suppose $(a, b) \in \mathbb{Z}_3 \times \mathbb{Z}_3$. Then $(a, b) + (a, b) + (a, b) = (3a, 3b) = (0, 0)$.
Therefore the maximum order is 3. ⊛

Theorem 2.2.2. The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if $\gcd(m, n) = 1$.

Corollary 2.2.1. $G = \mathbb{Z}_{m1} \times \mathbb{Z}_{m2} \times ... \times \mathbb{Z}_{mn}$ is cyclic if and only if $\gcd(m_1, m_2, ..., m_n) = 1$.

Theorem 2.2.3. $(a_1, a_2, ..., a_n) \in G = \mathbb{Z}_{m1} \times \mathbb{Z}_{m2} \times ... \times \mathbb{Z}_{mn}$.
If r_i is the order of a_i, then $|(a_1, a_2, ..., a_n)| = lcm(r_1, r_2, ..., r_n)$.

Exercise. $G = \mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{20} \times \mathbb{Z}_{24}$.

1. Is G cyclic?
2. Find the order of G.
3. $(3, 6, 12, 14) \in G$. Find the order of $(3, 6, 12, 14)$.

Answer. 1. $\gcd(4, 12, 20, 24) = 4 \neq 1$. Therefore G is not cyclic.

2. $|G| = 4 \times 12 \times 20 \times 24 = 11520$.
3. $|(3, 6, 12, 14)| = lcm(4, 2, 5, 3) = 60$.

⊛

Lecture 17

Theorem 2.2.4 (Finite version)**.** Let G be a finite abelian group. Then

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

where $p_1, \ldots, p_n$ are prime numbers (not necessarily distinct). Where $|G| = p_1^{r_1} \cdots p_n^{n_n}$.

Theorem 2.2.5 (General version)**.** Let G be some abelian group that has a finite number of generators. Let $\mathbb{Z} = \langle 1 \rangle$ be the additive group of integers. Then

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots$$

Remark.

$$\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$$

Just swap the corrdinates.

Corollary 2.2.2. If $n = p_1^{r_1} \cdots p_n^{r_n}$, then $\mathbb{Z})n = \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}}$.

Exercise. Find all abelian groups on 360 elements.

Answer.
$360 = 2^3 * 3^2 * 5$.

For $8 = 2^3$, we have $\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
For $9 = 3^2$, we have $\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$.
For 5, we have $\mathbb{Z}_5$.

By combinatorics, we have $3 * 2 * 1 = 6$ possibilities. ⊛

Exercise. Suppose we have $G_1 = \mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24}$ and $G_2 = \mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{40}$. Are G_1 and G_2 isomorphic?

Answer.
First step: Check orders.
$|G_1| = 8 * 10 * 24 = 1920$ and $|G_2| = 4 * 12 * 40 = 1920$.
Second step: Decompose the groups into subgroups as small as possible.
$G_1 = \mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24} = \mathbb{Z}_{2^3} \times \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
$G_2 = \mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{40} = \mathbb{Z}_{2^3} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_5$

So they are actually different because the exponents are different. ⊛

Lecture 18

Exercise. $G_1 = \mathbb{Z}_2 \times \mathbb{Z}_{12}$ and $G_2 = \mathbb{Z}_4 \times \mathbb{Z}_6$. Are these two groups isomorphic?

Answer. We can use the theorem that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ if and only if $\gcd(m, n) = 1$.
$G_1 = \mathbb{Z}_2 \times \mathbb{Z}_{43} \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$
$G_2 = \mathbb{Z}_4 \times \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$
$\Rightarrow G_1 \cong G_2$. ⊛

Theorem 2.2.6 (Finite Version). Let G be a finite abelian group. Then G is isomorphic to a direct product of cyclic groups of prime power order. That is,

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

And,

$$|G| = p_1^{n_1} \cdots p_k^{n_k}$$

where $p_1, \ldots, p_k$ are prime numbers and $n_1, \ldots, n_k$ are positive integers.
Moreover, this decomposition is unique up to the order of the factors.

Example. Find all abelian groups up to isomorphosm of order 720. $720 = 2^4 \cdot 3^2 \cdot 5$.

Answer. By the theorem above, list out the primary factor representation of a group of order 720.

2^4	3^2	5
$\mathbb{Z}_{16}$	$\mathbb{Z}_9$	$\mathbb{Z}_5$
$\mathbb{Z}_8 \times \mathbb{Z}_2$	$\mathbb{Z}_9$	$\mathbb{Z}_5$
$\mathbb{Z}_4 \times \mathbb{Z}_4$	$\mathbb{Z}_9$	$\mathbb{Z}_5$
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_9$	$\mathbb{Z}_5$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_9$	$\mathbb{Z}_5$
$\mathbb{Z}_{16}$	$\mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_5$
$\mathbb{Z}_8 \times \mathbb{Z}_2$	$\mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_5$
$\mathbb{Z}_4 \times \mathbb{Z}_4$	$\mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_5$
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_5$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_5$

⊛

Definition 2.2.1. We define torsion and torsion-free subgroups of a group as follows:

1. **Torsion Subgroup:**
   The *torsion subgroup* of a group G, denoted $T(G)$, is defined as:

   $$T(G) = \{g \in G \mid \text{there exists } n \in \mathbb{N} \text{ such that } g^n = e\}$$

   where e is the identity element in G. It consists of all elements of G with finite order.

2. **Torsion-Free Subgroup:**
   A *torsion-free subgroup* of G contains only elements with infinite order, meaning:

   $$g^n \neq e \text{ for any nonzero integer } n$$

   except for $g = e$ itself.

2.3 Cosets & the Theorem of Lagrange

Remark. Let $G \cong \mathbb{Z}_n$ and $G = \langle a \rangle$
If H is a subgroup of G, then $|H|$ divides $|G| = n$.

Proof. Let $H = \langle a^s \rangle$, then $(a^s)^{|H|} = e = a^n$.
$(a^s)^{|H|} = \underbrace{a^s a^s \cdots a^s}_{|H|} = a^{s|H|} = a^n$
So $s|H| = n$, and $|H|$ divides n. ∎

Theorem 2.3.1 (Lagrange's Theorem)**.** Let G be a finite group and H be a subgroup of G. Then $|H|$ divides $|G|$.
Moreover, the number of left cosets of H in G is $\frac{|G|}{|H|}$.

Corollary 2.3.1. Let G be a group and $|G| = p$ =prime. Then G is cyclic $\cong \mathbb{Z}_p$.

Proof. $|G| = p$ is prime. Let $H = \langle a \rangle$ be a subgroup of G.
By Lagrange's Theorem, $|H|$ divides $|G| = p$.
So $|H| = 1$ or p.
So $H = G$.

The proof is based on cosets which we will see later. ∎

Definition 2.3.1. Let G be a group and H be a subgroup of G. We define a partition to have equivalence relation "$\sim$" on G as follows:

$$a \sim b \Leftrightarrow a^{-1}b \in H$$

1. Reflexive: $a \sim a$ since $a^{-1}a = e \in H$.
2. Symmetric: $a \sim b \Leftrightarrow a^{-1}b \in H \Leftrightarrow (a^{-1}b)^{-1} = b^{-1}a \in H \Leftrightarrow b \sim a$.
3. Transitive: $a \sim b$ and $b \sim c \Leftrightarrow a^{-1}b \in H$ and $b^{-1}c \in H \Leftrightarrow a^{-1}b \cdot b^{-1}c = a^{-1}c \in H \Leftrightarrow a \sim c$.

If you take an element and add other elements based on this equivalence relation, you get a subgroup. This is called a *coset*.

Lecture 19

Definition 2.3.2. Let G be a group and H be a subgroup of G. The *left coset* of H in G is defined as:

$$aH = \{ah \mid h \in H\} \subseteq G$$

for all $a \in G$. That is, all elements that is equivalent to a.
Similarly, the *right coset* of H in G is defined as:

$$Ha = \{ha \mid h \in H\} \subseteq G$$

for all $a \in G$.

Example. Let $G = \mathbb{Z}_{18} = \{0, 1, 2, \ldots, 17\}$ and $H = \langle 3 \rangle = \{0, 3, 6, 9, 12, 15\}$.

Then the left cosets of H in G are:

$$0 + H = \{0, 3, 6, 9, 12, 15\}$$

$$1 + H = \{1, 4, 7, 10, 13, 16\}$$

$$2 + H = \{2, 5, 8, 11, 14, 17\}$$

Note that $1 + H$ is not a subgroup of G.

Remark. We observe the following:

1. The left cosets of H in G partition G.
2. $|H| = |1 + H| = |2 + H| = \ldots = |a + H|$ for all $a \in G$. (partitions have the same size)

Example. Let $D_4 = \{e, \rho, \rho^2, \rho^3, \mu, \mu\rho, \mu\rho^2, \mu\rho^3\}$ be the dihedral group of permutation of a square.
Let $H = \langle \mu\rho \rangle = \{e, \mu\rho\}$.
Then the left cosets of H in D_4 are:

$$D_4 = \begin{array}{|c|c|} \hline \cdot e & \cdot \rho \\ \{e, \mu\rho\} & \{\rho, \mu\} \\ \hline \cdot \rho^2 & \cdot \rho^3 \\ \{\rho^2\mu\rho^3\} & \{\rho^3\mu\rho^2\} \\ \hline \end{array}$$

Theorem 2.3.2. Let G be a group and H be a subgroup of G. Then for all $a \in G$, $|H| = |aH|$.

Proof. Define a function $f : H \to aH$ by $f(x) = ax$. We show that f is a bijection.

1. **one-to-one**: Suppose $f(h_1) = f(h_2)$. Then $ah_1 = ah_2 \Rightarrow h_1 = h_2$.
2. **onto**: $y \in aH$ implies $y = ah$ for some $h \in H$. So $f(h) = ah = y$.

$\blacksquare$

As previously seen (Lagrange's Theorem)**.** Recall:
Let G be a finite group and H be a subgroup of G. Then $|H|$ divides $|G|$.
Moreover, the number of left cosets of H in G is $\frac{|G|}{|H|}$.

Proof. Let $G = \{a_1, a_2, \ldots, a_n\}$ and $H = \{h_1, h_2, \ldots, h_m\}$.
Then

$$G = \bigcup_{i=1}^{n} a_i H \quad \text{and} \quad a_i H \cap a_j H = \emptyset \text{ for } i \neq j.$$

So

$$|G| = \sum_{i=1}^{n} |a_i H| = n|H|.$$

Hence, $|H|$ divides $|G|$. $\blacksquare$

Example. Let $G = \mathbb{Z}_{24} = \{0, 1, 2, \ldots, 23\}$ and $H = \langle 3 \rangle = \{0, 3, 6, \cdots, 21\}$.
Then $|H| = 8$ and $|G| = 24$.
So the number of left cosets of H in G is $\frac{24}{8} = 3$.

Exercise. Let S_5 be the permutation group of 5 elements.
Let $\sigma \in S_5$ and $\sigma = (1, 2, 5, 4)(2, 3)$.
Find $(S_5, \langle\sigma\rangle)$.

Answer. $(S_5, \langle\sigma\rangle) = \frac{|S_5|}{|\langle\sigma\rangle|} = \frac{5!}{|\langle\sigma\rangle|}$.
$|\langle\sigma\rangle| = |(1, 2, 3, 5, 4)| = 5$.
So $(S_5, \langle\sigma\rangle) = \frac{5!}{5} = 24$.

⊛

Exercise. Let $\phi : G \to G'$ be a group homomorphism.
Show that $\phi(a) = \phi(b) \Leftrightarrow a^{-1}b \in Ker(\phi)$.

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

$$\phi(a^{-1}b) = \phi(a^{-1})\phi(b) = \phi(a)^{-1}\phi(a) = e$$

So $a^{-1}b \in Ker(\phi)$.

⊛

Lecture 20

Example. When will the left and right cosets of a subgroup H of a group G coincide?

Answer. Obviously abelian groups have this property, but there are non-abelian groups that have this property as well.

⊛

Theorem 2.3.3. Let H be a subgroup, and let $\phi : G \to G'$ be a homomorphism. If $H = \ker \phi$, then the left cosets of H in G are the same as the right cosets of H in G.

Example. Let $G = GL(2, \mathbb{R})$, which are invertible 2×2 matrices. This is non abelian. Let H be 2×2 matrices with determinant 1.
Are the left and right cosets of H in G the same?

Answer. Use the theorem above:
Let $\phi : G \to (\mathbb{R}^*, \times)$ be a mapping to $e' = 1 \in \mathbb{R}^*$. Then $\ker \phi = H$.
So the left and right cosets of H in G are the same.

⊛

2.4 Homomorphisms & Factor Groups

Example. Recall $\mathbb{Z}_{12} = \{0, 1, 2, \ldots, 11\}$ with addition modulo 12.
Let $H = \{0, 3, 6, 9\}$, $1 + H = \{1, 4, 7, 10\}$, $2 + H = \{2, 5, 8, 11\}$.
Then $(0 + H) + (1 + H) = 1 + H$, $(0 + H) + (2 + H) = 2 + H$.

Definition 2.4.1. Let G be a group, and let H be a subgroup of G. If for all $a, b \in G$, $(aH)(bH) = (ab)H$, then the left cosets of H is induced by the operaetion of G

Example. When does the left cosets of H induce the operation of G?

Answer. When the left cosets are the same as the right cosets.

⊛

Definition 2.4.2. A subgroup H is called a normal subgroup of G if the left cosets of H in G are the same as the right cosets of H in G.

Theorem 2.4.1. A factor group $G/H = \{H, aH, bH, \dots\}$ is a group with the operation $(aH)*(bH) = (ab)H$.
$*$ is well defined if and only if H is a normal subgroup of G.

Example. $G = \mathbb{Z}_{50} \times \mathbb{Z}_{75}$ and $H = \langle(15, 15)\rangle$.
What is $|G/H|$?

Answer. $|G/H| = \frac{|G|}{|H|} = \frac{50\times 75}{|H|}$.
The order of 15 in $\mathbb{Z}_{50} = \frac{50}{gcd(15,50)} = 10$, and the order of 15 in $\mathbb{Z}_{75} = \frac{75}{gcd(15,75)}$ is 5.
$|H| = lcm(10, 5) = 10$.
So $|G/H| = \frac{50\times 75}{10} = 1875$.

⊛

Lecture 21

Example. The factor group G/H has left cosets equal to right cosets. We can show that $(G/N, *)$ is a group.

1. Identity: eH is the identity element.
2. Inverse: $(aH)^{-1} = a^{-1}H$.
3. It is closed under $*$
4. Associative: $(aH * bH) * cH = aH * (bH * cH)$.

Example. Let $G = \mathbb{Z}_3 \times \mathbb{Z}_6$ and $|G| = 18$.
Let $H = \langle(1, 1)\rangle = \{(0, 0), (1, 1), (2, 2), (0, 3), (1, 4), (2, 5)\}$.
$G/H = \{H, (1, 0) + H, (2, 0) + H\} \cong \mathbb{Z}_3$.
What is the order of $(1, 4) + H$?
What is the order of $(2, 1) + H$?

Answer. We need to find the minimum n such that $[(1, 4) + H]^n = H$.
$(1, 4) + H = H$, which is the identity in G/H, so the order is 1.
$(2, 1) + H$ has order 3.

⊛

Theorem 2.4.2. The following 4 equivalent conditions are required for subgroup H in G to be normal

1. $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.
2. $gHg^{-1} = \{ghg^{-1} : h \in H\} = H$ for all $g \in G$.
3. $\exists \phi : G \to G'$ such that $H = \ker \phi$.
4. $gH = Hg$ for all $g \in G$ (normal group).

Example. Let G be a finite group, and let H be a subgroup of G.
H is the only subgroup of G with $|H| = d$. Prove that H is normal in G.

Proof. By the above theorem, it suffices to show that $gHg^{-1} = H$ for all $g \in G$.
For sake of contradiction, $\exists g \in G$ such that $gHg^{-1} \neq H$.
If we can show that gHg^{-1} is a subgroup of G, and $|gHg^{-1}| = |H|$, then we have a contradiction.
By the automorphism $\phi : gtogHg^{-1}$, we know $|gHg^{-1}| = |H|$ because ϕ is bijective.
Now we need to show that gHg^{-1} is a subgroup of G.

1. Closure: $g(xy)g^{-1} = (gxg^{-1})(gyg^{-1})$.
2. Identity: $e \in H$, so $geg^{-1} = e \in gHg^{-1}$.
3. Inverse: $g(x^{-1})g^{-1} = (gxg^{-1})^{-1}$.

■

Definition 2.4.3 (Automorphism). An automorphism $\phi : G \to G$ is an isomorphism from G to G.
We can define the mapping as $g(x) = gxg^{-1}$.

1. Bijective: Suppose $g(x) = g(y)$, then $gxg^{-1} = gyg^{-1}$, so $x = y$.
2. Onto: For all $y \in G$, $\exists x \in G$ such that $g(x) = y$. Choose $y = g^{-1}yg$, then $g(g^{-1}yg) = y$.

Lecture 22

Remark. Here are some facts about factor groups:
$|H| = |aH|$ for all $a \in G$
If we have a factor group $G/H = \{H, 1+H, 2+H\}$ on $\mathbb{Z}_12$, its equal to $\{3+H, 7+H, 8+H\}$. The index of H in G is the number of cosets of H in $G = |G|/|H|$.

Theorem 2.4.3 (Fundemental Homomorphism Theorem). Let $\phi : G \to G'$ be a homomorphism. Then for $H = \ker(\phi)$, we have $G/H \cong G'$.

Example. For a group $\mathbb{Z}_{12}$, we have a homomorphism $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_3$ where $\phi(x) = x \mod 3$.

Example. Let $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ and $H = \{(0,0),(0,1)\}$, we can see there are 4 cosets of H in G.
Then we have a homomorphism $\phi((a,b)) = a$

Example. Let $\mathbb{C}^*$ be the group of non-zero complex numbers under multiplication.
Let $H = \{z \in \mathbb{C}^* | |z| = 1\}$, then H is a subgroup of $\mathbb{C}^*$.
Find the factor group $\mathbb{C}^*/H$.

Answer. Let $\phi(x) = |x|$ be a homomorphism from $\mathbb{C}^*$ to $\mathbb{R}^*$.
Then $H = \ker(\phi)$.

⊛

Lecture 25

2.5 Factor Group Computation & Simple Groups

Note. Computing factor groups: We will classify according to the fundamental theorem of finitely generated abelian groups.

As previously seen. Recall that if G is an abelian group with finitely many generators, then $G \cong \mathbb{Z}_{{p_1}^{n_1}} \times \cdots \times \mathbb{Z}_{{p_k}^{n_k}} \times \mathbb{Z}^r$ for some primes $p_1, \ldots, p_k$ and $n_1, \ldots, n_k, r \in \mathbb{N}$.

Theorem 2.5.1. Let G be a finite cyclic group and H is a subgroup. If G is abelian, then H is normal and thus $|G/H| = |G|/|H|$. $G/H \cong \mathbb{Z}_{|G|/|H|}$, which is also cyclic.

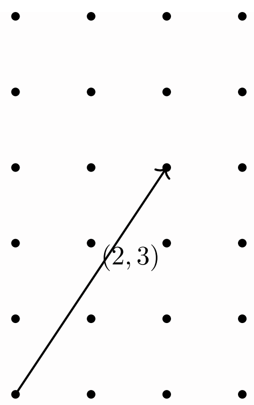
Theorem 2.5.2 (First Isomorphism Theorem)**.** If there exists a homomorphism $\varphi : G \to G'$ and $H = \ker(\varphi)$, then $G/H \cong G'$.

Example. $G = \mathbb{Z}_{100}$ and $H = \langle 25 \rangle$. Then $|G| = 100$ and $|H| = 4$. Thus $|G/H| = 100/4 = 25$. $G/H \cong \mathbb{Z}_{25}$.

Example. $G = \mathbb{Z}_4 \times \mathbb{Z}_6$ (not cyclic). Let $H = \langle (0, 1) \rangle$. Then $|G| = 4 \times 6 = 24$ and $|H| = 6$. Thus $|G/H| = 24/6 = 4$. $G/H \cong \mathbb{Z}_4$.
Define $\phi : \mathbb{Z}_4 \times \mathbb{Z}_6 \to \mathbb{Z}_4$ by $\phi(a, b) = a$. Then $\ker(\phi) = H$. It is indeed a homomorphism because $\phi((a + c, b + d)) = a + c = \phi(a, b) + \phi(c, d)$. Thus by the first isomorphism theorem, $\mathbb{Z}_4 \times \mathbb{Z}_6/\langle (0, 1) \rangle \cong \mathbb{Z}_4$.

Example. $G = \mathbb{Z}_4 \times \mathbb{Z}_6$ and $H = \langle (2, 3) \rangle = \{(0, 0), (2, 3)\}$. Then $|G| = 24$ and $|H| = 2$. Thus $|G/H| = 24/2 = 12$.
This time we have two possible choices however, $\mathbb{Z}_{12}$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

Answer. Intuition: draw a lattice diagram and draw a line from the origin to the generator.



It is not hard to see that the line only intersect 2 points, so imagine 12 parrallel lines, which is the 12 cosets of G, so $G/H \cong \mathbb{Z}_{12}$ and the G/H is cyclic.
Now we use the first isomorphism theorem:
Define

$$\phi : \mathbb{Z}_4 \times \mathbb{Z}_6 \to \mathbb{Z}_{12} = \phi(a, b) = 3a - 2b$$

Then $\ker(\phi) = H$
It is indeed a homomorphism because

$$\phi((a + c, b + d)) = 3(a + c) - 2(b + d) = 3a - 2b + 3c - 2d = \phi(a, b) + \phi(c, d)$$

Thus by the first isomorphism theorem, $\mathbb{Z}_4 \times \mathbb{Z}_6/\langle(2, 3)\rangle \cong \mathbb{Z}_{12}$. ⊛

Example. $G = \mathbb{Z}_4 \times \mathbb{Z}_6$ and $H = \langle(0, 2)\rangle = \{(0, 0), (0, 2), (0, 4)\}$. Then $|G| = 24$ and $|H| = 3$. Thus $|G/H| = 24/3 = 8$.
Now G/H could be isomorphic to $\mathbb{Z}_8$ or $\mathbb{Z}_4 \times \mathbb{Z}_2$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Answer. Again, draw the lattice diagram, but we will omit here: intuitively, we see that $G/H \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.
Now we use the first isomorphism theorem:
Define

$$\phi(a, b) = (a, b \mod 2)$$

Then $\ker(\phi) = H$
It is indeed a homomorphism because

$$\phi((a + c, b + d)) = (a + c, b + d \mod 2) = (a, b \mod 2) + (c, d \mod 2) = \phi(a, b) + \phi(c, d)$$

Thus by the first isomorphism theorem, $\mathbb{Z}_4 \times \mathbb{Z}_6/\langle(0, 2)\rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2$. ⊛

Lecture 26

Lecture 27

Lecture 28