MAT3004 Lecture Notes: Cyclic Groups and Subgroups

1 Recall: Subgroups

Subgroup $H \leq G$

- If $a, b \in H \implies a * b \in H$ (Closure)
- $a \in H \implies a^{-1} \in H$ (Inverse)

2 Cyclic Subgroups

Definition: The cyclic subgroup generated by g is:

$$\langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$$

2.1 Examples

1. Consider $(\mathbb{Z}_{10}, +)$ **and the subgroup** $\langle [4]_{10} \rangle$**.**

$$\begin{aligned} \langle [4] \rangle &= \{[0], [4], [4]+[4], [4]+[4]+[4], \ldots, -[4], \ldots\} \\ &= \{[0], [4], [8], [12] = [2], [16] = [6], [20] = [0]\} \\ &= \{[0], [2], [4], [6], [8]\} \end{aligned}$$

Therefore, $|\langle [4] \rangle| = 5$.

2. Consider $(\mathbb{R}, +)$**.**

$$\langle \pi \rangle = \{k\pi \mid k \in \mathbb{Z}\} \quad \text{(Integer multiples of } \pi\text{)}$$

Therefore, $|\langle \pi \rangle| = \infty$.

3. Consider $(GL(2, \mathbb{R}), \times)$**.** Let $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

$$\begin{aligned} \langle g \rangle &= \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m \middle| m \in \mathbb{Z} \right\} \\ &= \left\{ \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \middle| m \in \mathbb{Z} \right\} \end{aligned}$$

Therefore, $|\langle g \rangle| = \infty$.

4. Examples of groups of finite order.

- In a relevant group (e.g., $\mathbb{Z}^*$ or $\mathbb{R}^*$), $|\langle -1 \rangle| = 2$.
- Rotation Matrix:

$$\left| \left\langle \begin{pmatrix} \cos \frac{2\pi}{n} & -\sin \frac{2\pi}{n} \\ \sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix} \right\rangle \right| = n$$

3 Cyclic Groups

Definition: A group $(G, *)$ is called **Cyclic** if there exists $g \in G$ such that:

$$G = \langle g \rangle$$

3.1 Examples of Cyclic Groups

1. $(\mathbb{Z},+) = \langle 1 \rangle$ is cyclic. (Note: $\langle -1 \rangle$ also generates $\mathbb{Z}$).
2. $(\mathbb{Q},+)$ is **not** cyclic.
3. $(\mathbb{R},+)$ is **not** cyclic.
   - Reasoning: $(\mathbb{R},+)$ is uncountable, but any cyclic group $\langle g \rangle$ is countable (indexed by $\mathbb{Z}$). Therefore $\mathbb{R} \neq \langle g \rangle$.
4. For $(\mathbb{Z}_5^*, \times)$, consider $\langle [3] \rangle$:
$$\langle [3] \rangle = \{[3]^1 = [3], [3]^2 = [9] = [4], [3]^3 = [27] = [2], [3]^4 = [81] = [1]\}$$
   The set is $\{[1],[2],[3],[4]\} = \mathbb{Z}_5^*$. Thus, $(\mathbb{Z}_5^*, \times)$ is cyclic.
5. $(\mathbb{Z}_9,+) = \langle [1] \rangle$ is cyclic. (Also generated by $\langle [4] \rangle$ since $\gcd(4,9) = 1$).

4 Orders of Elements and Lagrange's Theorem Preview

Consider $(\mathbb{Z}_9^*, \times) = \{[1],[2],[4],[5],[7],[8]\}$. Note that $|\mathbb{Z}_9^*| = 6$. Let's look at the subgroups generated by specific elements:

- $\langle [1] \rangle = \{[1]\} \implies |\langle [1] \rangle| = 1$
- $\langle [8] \rangle = \{[1],[8]\} \implies |\langle [8] \rangle| = 2$ (since $8^2 \equiv 64 \equiv 1 \pmod 9$)
- $\langle [4] \rangle = \{[1],[4],[7]\} \implies |\langle [4] \rangle| = 3$ (since $4^2 \equiv 7, 4^3 \equiv 28 \equiv 1 \pmod 9$)

Remark: In the example above, $|\mathbb{Z}_9^*| = 6$, and the subgroup sizes $1, 2, 3$ are factors of 6. We will prove later that for all $H \leq G$, $|H|$ divides $|G|$ (**Lagrange's Theorem**).

In particular, there are **No** $g \in \mathbb{Z}_9^*$ such that $|\langle g \rangle| = 4$ or 5.

Another Example: $|\mathbb{Z}_{21}^*| = 12$. So all $k \in \mathbb{Z}_{21}^*$ must have $|\langle k \rangle| \in \{1,2,3,4,6,12\}$.

5 Order of an Element

Definition: The order of an element $g \in G$ is:
$$\operatorname{ord}(g) = |\langle g \rangle|$$

Examples:

1. $G = GL(2,\mathbb{R})$.
$$\operatorname{ord}\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = \infty$$
$$\operatorname{ord}\left(\begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}\right) = n$$
2. $G = \mathbb{Z}_9^*$.
$$\operatorname{ord}([1]) = 1, \quad \operatorname{ord}([8]) = 2, \quad \operatorname{ord}([4]) = 3$$

6 Proposition on Element Order

Proposition: Let $g \in G$. Then $\operatorname{ord}(g)$ is the smallest positive integer k such that $g^k = e$.

Proof: Suppose $\operatorname{ord}(g) = k$. Therefore $\langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$ has k elements.

For all $i \in \mathbb{N}$, consider $g^1, g^2, \ldots, g^k \in \langle g \rangle$.

Claim 1: If I pick these, the elements are distinct.

Proof of Claim 1: Suppose on the contrary that $g^a = g^b$ for $1 \leq a < b \leq k$. Then:
$$g^b \cdot g^{-a} = e \implies g^{b-a} = e$$

Write $l = b - a$. Note that $l < k$ (since $b \leq k$). So we have $g^l = e$ for some $l < k$.

Then for all $m \in \mathbb{Z}$, by the division algorithm, we can write $m = ql + r$ where $0 \leq r < l$.

$$g^m = g^{ql+r} = (g^l)^q \cdot g^r = e^q \cdot g^r = g^r$$

This implies:

$$\langle g \rangle = \{g^r \mid 0 \leq r < l\} = \{e, g^1, \dots, g^{l-1}\}$$

This means $|\langle g \rangle| \leq l < k$. But we assumed $\text{ord}(g) = |\langle g \rangle| = k$. This is a contradiction.

Therefore, $g^1, g^2, \dots, g^k$ are distinct elements in $\langle g \rangle$. Since $|\langle g \rangle| = k$, it follows that $\langle g \rangle = \{g^1, g^2, \dots, g^k\}$. Consequently, g^k must be the identity (or relates to the closure such that the sequence cycles back), proving the proposition regarding the smallest integer power.

Proof Regarding Order of Elements

Proof: Suppose on the contrary that:

$$g^a = g^b \quad \text{for } 1 \leq a < b \leq k$$

Then:

$$g^{b-a} = e$$

Write $l = b - a < k$, so that $g^l = e$.

Then for all $m \in \mathbb{Z}$, by the division algorithm (m divided by l):

$$m = ql + r, \quad 0 \leq r < l$$

$$\Rightarrow g^m = g^{ql+r} = g^{ql} \cdot g^r$$

$$\Rightarrow g^m = (g^l)^q \cdot g^r$$

Since $g^l = e$:

$$g^m = e^q \cdot g^r = g^r$$

Therefore, $\langle g^m \rangle = \{g^r \mid 0 \leq r < l\}$. This implies $|\langle g^m \rangle| \leq l < k$, which is a contradiction.

$\therefore g^1, g^2, \dots, g^k$ are k distinct elements in $\langle g \rangle$.

$$\Rightarrow \langle g \rangle = \{g^1, g^2, \dots, g^k\}$$

$$e = g^j \text{ for some } j = 1, 2, \dots, k$$

Claim 2: $g^k = e$ (Exercise).

(and $g^j \neq e$ for $j < k$).

So the Prop is proved.

1.4 Permutation / Symmetric Group

Definition: Let

$$S_n = \{\sigma : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\} \mid \sigma \text{ is bijective}\}$$

e.g. $n = 3$

Mapping examples:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{where } \sigma(1) = 2, \sigma(2) = 1, \sigma(3) = 3$$

The permutation (or symmetric) group is $(S_n, \circ)$, where "$\circ$" is the composition of (bijective) maps.

e.g. for $\sigma, \tau \in S_3$: Applying $\tau \circ \sigma$ means calculating $\tau(\sigma(x))$.

Remark

1. **Check the axioms of groups for $(S_n, \circ)$:**

   - $(\sigma \circ \tau) \circ \gamma = \sigma \circ (\tau \circ \gamma)$ is automatic by the associativity of map composition.
   - $e \in S_n$ is given by:
   $$e : \{1, \dots, n\} \to \{1, \dots, n\}$$
   $$e(1) = 1, e(2) = 2, \dots, e(n) = n$$
   $$\left(\text{or } \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}\right)$$
   - For $\sigma \in S_n$, $\sigma^{-1} \in S_n$ is taken as the inverse map of σ.

2. $|S_n| = n!$

3. S_n is <u>NOT</u> abelian for $n \geq 3$, i.e., $\sigma \circ \tau \neq \tau \circ \sigma$ in general.