MAT3004 Lecture 2 Notes

1 Recall: Groups

Definition 1. $(G, *)$ *is a group if:*

(i) ***Associativity:*** $(a * b) * c = a * (b * c)$ *for all* $a, b, c \in G$.

(ii) ***Identity:*** *There exists* $e \in G$ *such that* $a * e = e * a = a$ *for all* $a \in G$.

(iii) ***Inverse:*** *For every* $a \in G$, *there exists* $a^{-1} \in G$ *such that* $a * a^{-1} = a^{-1} * a = e$.

Remark 1. *For* $m \in \mathbb{N}$, *we write:*

$$g^m = \underbrace{g * g * \cdots * g}_{m \text{ times}}$$

Also, note that in general, $a * b \neq b * a$ *(groups are not necessarily abelian).*

Example 1. *Consider* $GL_n(\mathbb{R})$, *the General Linear Group.*

$$\begin{cases} A \cdot I_n = I_n \cdot A = A \\ A \cdot A^{-1} = A^{-1} \cdot A = I_n \end{cases}$$

Note: We do not have $AB = BA$ in general. To prove inverses in matrices, we typically need to prove $AA^{-1} = I_n$ and $A^{-1}A = I_n$ separately, though for square matrices one implies the other.

2 Uniqueness Properties

Theorem 1. *Let* $(G, *)$ *be a group.*

1. *The identity element* $e \in G$ *is unique.*
2. *For all* $a \in G$, *the inverse* $a^{-1} \in G$ *is unique.*

Proof. **Uniqueness of Identity:** Suppose e and e' both satisfy the identity property. Then $e * e' = e'$ (treating e as identity). Also $e * e' = e$ (treating e' as identity). Therefore, $e = e'$.

Uniqueness of Inverse: Suppose b and c are both inverses of a.

$$\begin{aligned} c &= c * e \\ &= c * (a * b) \quad \text{(since } a * b = e\text{)} \\ &= (c * a) * b \quad \text{(associativity)} \\ &= e * b \quad \text{(since } c \text{ is an inverse of } a\text{)} \\ &= b \end{aligned}$$

Thus, $c = b$. □

3 Cayley Tables

Definition 2. *Let $(G, *)$ be a finite group. The **Cayley Table** of G is the "multiplication table" of G, whose rows and columns are labeled by elements of G, and the (g, h)-entry is equal to $g * h$.*

Example 2. $(\mathbb{Z}_4, +)$

$+$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

Proposition 1 (Latin Square Property)**.** *The elements of G show up **exactly once** in each row and each column of the Cayley Table.*

Equivalently: For any $a \in G$, the set $\{a * g \mid g \in G\}$ has no repetitions (it has $|G|$ elements). Similarly for $\{g * a \mid g \in G\}$.

Proof. Suppose on the contrary that there exist $g \neq g'$ in G such that:

$$a * g = a * g'$$

Multiply by a^{-1} on the left:

$$\begin{aligned} a^{-1} * (a * g) &= a^{-1} * (a * g') \\ (a^{-1} * a) * g &= (a^{-1} * a) * g' \quad \text{(associativity)} \\ e * g &= e * g' \\ g &= g' \end{aligned}$$

This contradicts $g \neq g'$. Thus, all entries in a row must be distinct. Since the group is finite, every element must appear exactly once. $\square$

4 Subgroups

4.1 Definition

Definition 3. *Let $(G, *)$ be a group. A subset $H \subseteq G$ is called a **subgroup** of G (written $H \leq G$) if:*

1. *For all $h, h' \in H$, $h * h' \in H$ (Closure).*
2. *For all $h \in H$, $h^{-1} \in H$ (Inverse).*

Example 3. $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$.

4.2 Notation Convention

If our binary operation is $+$, we write mg instead of g^m:

$$mg = \underbrace{g + g + \cdots + g}_{m \text{ times}}$$

The inverse is denoted $-g$.

4.3 Examples and Non-Examples

Example 4. *Let $k\mathbb{Z} = \{$all multiples of $k\}$. $k\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$.*

Example 5. *Consider $2\mathbb{Z}+1$ (the odd integers). $(2\mathbb{Z}+1, +)$ is **not** a subgroup of $\mathbb{Z}$ because closure fails:*

$$\textit{odd} + \textit{odd} = \textit{even} \notin (2\mathbb{Z}+1).$$

Example 6. *If $W \subseteq V$ is a vector subspace, then $(W, +) \leq (V, +)$ is a subgroup.*

Example 7 (Special Linear Group)**.**

$$SL_n(\mathbb{R}) = \{A \in M_{n\times n}(\mathbb{R}) \mid \det(A) = 1\} \leq (GL_n(\mathbb{R}), \cdot)$$

Proof Sketch: If $A, B \in SL_n(\mathbb{R})$, then $\det(A) = 1$ and $\det(B) = 1$.

$$\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1 \implies AB \in SL_n(\mathbb{R}).$$

Also, $\det(A^{-1}) = \frac{1}{\det(A)} = 1$, so inverses are in the set.

Example 8. *Consider the group $G = (\mathbb{Z}_9^\times, \times)$ (Units modulo 9). Elements: $\{[1], [2], [4], [5], [7], [8]\}$.*

- *Let $H_1 = \{[1], [4]\}$. Check closure: $[4] \times [4] = [16] = [7]$. Since $[7] \notin H_1$, this is **not** a subgroup.*
- *Let $H_2 = \{[1], [8]\}$. Check closure: $[8] \times [8] = [64] = [1] \in H_2$. Inverse of $[8]$ is $[8]$. This **is** a subgroup.*

4.4 Properties of Subgroups

Proposition 2. *If H is a subgroup of $(G, *)$, then $(H, *)$ is also a group.*

Proof. We check the group axioms for H:

1. **Associativity:** For $a, b, c \in H$, $(a * b) * c = a * (b * c)$ holds because it holds for all elements in G.
2. **Identity:** For any $a \in H$, we know $a^{-1} \in H$ (by subgroup definition). By closure, $a * a^{-1} \in H$. Since $a * a^{-1} = e$, the identity $e \in H$.
3. **Inverse:** Direct from the subgroup definition.

□

4.5 Types of Subgroups

1. A **proper subgroup** is any subgroup $H \leq G$ such that $H \neq G$.
2. The **trivial subgroup** is $\{e\}$.
3. Any subgroup H such that $\{e\} \neq H \leq G$ is called a **nontrivial** subgroup.

Definition 4 (Cyclic Subgroup)**.** *For any $g \in G$,*

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

*is the **cyclic subgroup generated by** g.*

[**Exercise: <u>Check</u>**

$$g^m \cdot g^n = g^{m+n}$$

by cases:

$$\begin{cases} m \geq 0 \\ m < 0 \end{cases} \quad \text{and} \quad \begin{cases} n \geq 0 \\ n < 0 \end{cases} \qquad)$$