MA2202 — Algebra I

Liew Zhao Wei

Semester 2, 2022-2023

---

1 Preface

This is a set of (incomplete) notes for a course on basic group theory.

2 Groups

We start by introducing groups.

Definition 2.1 (Group)
A *group* is a set G together with a law of composition that satisfies the following properties:

- *Identity*: There is an element $e \in G$ such that for all $a \in G$, $ae = ea = a$.
- *Associativity*: For all $a, b, c \in G$, $(ab)c = a(bc)$.
- *Inverses*: For all $a \in G$, there exists $b \in G$ such that $ab = ba = e$.

Definition 2.2 (Abelian group)
A group G is *abelian* if its law of composition is commutative, that is, for all $a, b \in G$, $ab = ba$.

Remark 2.3 (Identity and inverse are unique). *The identity and inverse of an element in a group are unique. We denote the identity by e, and the inverse of a by a^{-1}.*

Example 2.4 (Examples and non-examples of groups)
Some examples of groups include:

- $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}$, and $\mathbb{Z}/n\mathbb{Z}$ are groups under addition.
- Removing the zero element, $\mathbb{R}*, \mathbb{C}*$, and $\mathbb{Q}^*$ are groups under addition
- $\mathbb{N}$ is not a group because inverses do not exist for any non-zero element.

Example 2.5 (General/special linear group)
The *general linear group* and *special linear group* are groups of invertible matrices over a ring R under matrix multiplication, denoted $\mathrm{GL}_n\, R$ and $\mathrm{SL}_n\, R$ respectively. $\mathrm{GL}_n\, R$ has non-zero determinant, while $\mathrm{SL}_n\, R$ has determinant 1.

3 Symmetric Groups

3.1 Symmetric Groups

Definition 3.1 (Permutation)
A *permutation* of a set S is a bijective map p from S to itself. That is, $p\colon S \to S$.

Definition 3.2
The set of all permutations of the indices $\{1, 2, \ldots, n\}$ is called the *symmetric group* on n elements, denoted by S_n.

Definition 3.3
Let X be a set. The set of all permutations of X is called the *symmetric group* on X, denoted by S_X.

Proposition 3.4
$(S_n, \circ)$ and $(S_X, \circ)$ are isomorphic groups.

3.2 Permutation Matrices

A *permutation matrix* is associated to any permutation.

Definition 3.5 (Permutation matrix)
An $n \times n$ permutation matrix is an $n \times n$ matrix P whose columns are a permutation of the standard basis $e_1, e_2, \ldots, e_n$.

Proposition 3.6
Let $S_n^{''}$ denote the set of all $n \times n$ permutation matrices. Let $\times$ denote matrix multiplication. Then, $(S_n^{''}, \times)$ is a group and is isomorphic to $(S_n, \circ)$.

3.3 Cyclic Notations

We can express permutations as a product of disjoint cycles. This notation is called the *cyclic notation* and is more compact compared to the tabular notation.

Example 3.7
The permutation $p = (34)(12) \in S_4$ contains the following disjoint cycles: $1 \mapsto 2$, $2 \mapsto 1$, $3 \mapsto 4$, $4 \mapsto 3$, and $5 \mapsto 5$.

In fact, we can think of a cycle as a permutation.

Definition 3.8
Consider a permutation $p \in S_n$ with a cycle $(x_1 x_2 \cdots x_r)$. The cycle is a permutation $h \in S_n$ such that $h(x_1) = x_2, h(x_2) = x_3, \ldots, h(x_r) = h(x_1)$ and $h(y) = y$ for any y not in the cycle.

Then, a product of disjoint cycles simply refers to the composition of the corresponding permutations.

Proposition 3.9
Every permutation can be factorized into a product of disjoint cycles. The factorization is unique up to an ordering of the product of cycles.

3.4 Transpositions

Definition 3.10
A *transposition* is a cycle of the form $h = (ij)$.

Proposition 3.11
Any cycle can be written as a product of transpositions.

Proof sketch. Let $h = (i_1, \ldots, i_r)$. Then, $(i_1 i_r)(i_1 i_{r-1}) \cdots (i_1 i_2)$ is an equivalent permutation. $\square$

Since any permutation can be expressed as a product of disjoint cycles, we can also express any permutation as a product of transpositions.

Proposition 3.12
Every permutation can be expressed as a product of transpositions.

3.5 The Sign Character

Lemma 3.13
For any permutation matrices F and H in $S_n^{''}$, we have $\det(FH) = \det(F)\det(H)$ and $\det(F) = \pm 1$.

Since permutations in S_n are isomorphic to permutation matrices in $S_n^{''}$, observe the *sign* of a permutation is equivalent to the determinant of its corresponding permutation matrix.

Example 3.14 (Sign of a Permutation)
Let p be a permutation in S_n and φ be an isomorphism between S_n and $S_n^{''}$. Then, the *sign* of p is $\mathsf{sgn}(p) = \det(\varphi(p))$.

However, the determinant of a matrix is typically defined in terms of its sign, so we define the sign in an alternative fashion.

Definition 3.15
Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ be n variables.

Define $P(\mathbf{x}) = P(x_1, \ldots, x_n) = \prod\limits_{1 \le i < j \le n} (x_i - x_j)$.

Then, for each permutation $f \in S_n$, define $P_f(x_1, \ldots, x_n) = P(x_{f(1)}, x_{f(2)}, \ldots, x_{f(n)}) = \prod\limits_{1 \le i < j \le n} (x_{f(i)} - x_{f(j)})$.

Proposition 3.16
For any permutation $f \in S_n$, $P_f(x_1, \ldots, x_n) = \pm P(x_1, \ldots, x_n)$. We call the sign of P_f the *sign character* of f.

Proposition 3.17
For any permutations $f, h \in S_n$, $\mathsf{sgn}(f \circ h) = \mathsf{sgn}(f)\mathsf{sgn}(h)$.

Definition 3.18
A permutation $f \in S_n$ is *even* if $\mathsf{sgn}(f) = 1$. Otherwise, it is *odd*.

Theorem 3.19
Let $f \in S_n$ be a permutation. f is even iff f is a product of an even number of transpositions.

Proposition 3.20
The set of all even permutations in S_n is a subgroup of S_n.

4 Cayley's Theorem

Theorem 4.1 (Cayley's Theorem)
Every finite group of order n is isomorphic to a subgroup of the symmetric group S_n.

Cayley's Theorem gives a way of realizing an abstract group as a subgroup of a more concrete group S_n. However, it is difficult to use in practice because the order of S_n is usually too large in comparison to n. If $|G| = n$, then $|S_n| = n!$.

5 Cosets

Definition 5.1 (Coset)
Let H be a subgroup of G and $g \in G$ be an element of G. Then, a **left coset** is the subset

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

A **right coset** is the subset

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

Note that $eH = He = H$.