MATH 320 Lecture 8

Deepak Jassal

October 2$^{\text{nd}}$, 2025

1 Matrix Groups

In this section we will be looking into non-Abelian groups, namely Matrix Groups. The set

$$GL_n(F) = \{A \in M_n(F) : \det A \neq 0\}$$

of all invertible $n \times n$ matrices with entries in a field F forms a group under matrix multiplication.
A field is the smallest algebraic structure in which we can perform the usual arithmetic operations, including division by non-zero elements. In particular, every non-zero element in a field has a multiplicative inverse.

Definition 1.1: Field

A *field* is a set F with two binary operations $+$ and $\cdot$ such that

(i) $(F, +)$ is an abelian group with identity element 0;
(ii) $F\times := F \setminus 0$ is an abelian group under $\cdot$ with identity element 1;
(iii) Distributivity holds: for all $a, b, c \in F$, one has $a(b + c) = ab + ac$.

Example.

Common examples of fields include $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, and finite fields $\mathbb{Z}/p\mathbb{Z}$ where p is prime.

Remark.

1. In any field F, one has $a \cdot 0 = 0$ for all $a \in F$.
2. We write $F^\times$ for the multiplicative group of nonzero elements of a field F.

Theorem 1.2

If F is a finite field, then $|F| = p^n$, for some prime p and integer $n \geq 1$.

Proposition 1.3

Let F be a field. The set $GL_n(F)$ of all invertible $n \times n$ matrices with entries in F forms a group under matrix multiplication. It is called the general linear group of degree n over F.

The following material is covered in Chapter 1 Section 6 of the Dummit and Foote textbook

2 Group Homomorphisms and Isomorphisms

Definition 2.1: Group Homomorphisms

Let $(G, *)$ and $(H, \circ)$ be groups. A map $\varphi : G \to H$ is a *homomorphisms* is

$$\varphi(a * b) = \varphi(a) \circ \varphi(b) \quad \forall a, b \in G.$$

Definition 2.2: Group Isomorphisms

A map $\varphi : G \to H$ is an *isomorphism* if it is a bijective homomorphism. In this case we say that G and H are *isomorphic* and write $G \cong H$. More precisely, an isomorphism φ from a group $(G, *)$ to a group $(H, \circ)$ is a **one-to-one** mapping from G **onto** H **that preserves the group operation**. That isomorphism

$$\varphi(a * b) = \varphi(a) \circ \varphi(b).$$

From now on, we shall write $\varphi(ab) = \varphi(a)\varphi(b)$ and it will be understood that for ab we are using the operation of G, while for $\varphi(a)\varphi(b)$ we are using the operation of H.
How do we prove that two groups are isomorphic?

1. Find a candidate mapping for the isomorphism. That is a function $\varphi : G \to H$.
2. Prove that φ is one-to-one.
3. Prove that φ is onto.
4. Prove that φ is operation preserving.

Example.

(Automorphisms). Every group G is isomorphic to itself via the identity map 1_G. An isomorphism $G \to G$ is called an *automorphism* of G.

Example.

[The exponention isomorphism of additive and multiplicative groups of $\mathbb{R}$]
Consider $\exp : (\mathbb{R}, +) \to (\mathbb{R}, \times)$. then

$$\exp(a + b) = \exp(a)\exp(b) \quad \text{(homomorphism)}.$$

It is injective because $\exp(a) = \exp(b)$ implies $a = b$, and surjective onto $\mathbb{R}_{>0}$ since for any $y > 0$ there exists $a = \log y$ with $\exp(a) = y$. Thus $(\mathbb{R}, +) \cong (\mathbb{R}, \times)$

Example.

Later we will prove that any non-abelian group of order 6 is isomorphic to the symmetric group S3 giving a first illustration of group classification by structure rather than by presentation. Hence, $D6 \cong S_3$ and $GL_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$.

test