Introduction to Group Theory Notes

paraphrased by Tyler Wright

*An important note, these notes are absolutely **NOT** guaranteed to be correct, representative of the course, or rigorous. Any result of this is not the author's fault.*

1 The Basics of Groups

1.1 Binary operations

A binary operation on a set G is a function:

$$* : G \times G \to G.$$

It's just a function that takes two values and gives a single output. Examples are addition, multiplication, and composition.

Such an operation is called **commutative** if:

$$x * y = y * x. \qquad (\forall x, y \in G)$$

1.2 Definition of a Group

A group is a set G paired with a binary operation $*$ such that they satisfy the following:

- **Associativity**: For $x, y, z \in G$, $(x * y) * z = x * (y * z)$
- **Identity**: $\exists\, e \in G$ such that $\forall g \in G$, $e * g = g * e = g$
- **Inverses**: $\forall g \in G$, $\exists\, g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$.

A group is called commutative or Abelian if all its elements commute with the given operation.

1.3 Consequences of the Definition

1.3.1 Left and right cancellation

We can left and right cancel with inverses:

$$(ax = bx) \Rightarrow (a = b) \qquad (\forall a, b, x \in G)$$
$$(xa = xb) \Rightarrow (a = b). \qquad (\forall a, b, x \in G)$$

However, $ax = xb$ does not imply $a = b$ unless the group is Abelian.

1.3.2 Uniqueness of the identity and inverses

We have uniqueness of certain elements:

- The identity of a group is unique
- The inverse of an element is unique.

1.3.3 Inverse properties

For a group G with elements x, y:

- $(x^{-1})^{-1} = x$
- $(xy)^{-1} = y^{-1}x^{-1}$.

1.3.4 Exponent properties

For a group G with an element x and $m, n \in \mathbb{Z}$:

- $x^{-n} = (x^{-1})^n$
- $(x^n)(x^m) = x^{n+m}$.

However, $(xy)^n$ may not equal $x^n y^n$ unless G is Abelian.

2 Dihedral Groups

2.1 Definition of a Dihedral Group

The dihedral group D_{2n} is the group of symmetries of an n-sided polygon. This group has order $2n$ as is defined as:

$$\begin{aligned} D_{2n} &= \langle a \rangle \cap b\langle a \rangle \\ &= e, a, a^2, \ldots, a^{n-1}, b, ba, ba^2, \ldots, ba^{n-1}. \end{aligned}$$

Where a is a rotation of $\frac{2\pi}{n}$ radians around the centre of the polygon and b is a reflection in the line through vertex 1 and the centre of the polygon.

2.2 Properties of a Dihedral Group

For the dihedral group D_{2n}:

- $a^n = e$
- $b^2 = e$
- $a^n b = ba^{-n}$

3 Subgroups

3.1 Definition of a Subgroup

A subgroup is a subset H of a group G such that H is also a group under the binary operation defined by G ($H \leq G$). If we have a subset H of a group G, we can show it is a subgroup by showing the following properties hold for H:

- **Closure**: For $x, y \in H$, $xy \in H$
- **Identity**: $\exists\, e \in H$ such that for $x \in H$, $e * x = x * e = x$
- **Inverses**: For $x \in H$, $\exists\, x^{-1} \in H$ such that $x * x^{-1} = x^{-1} * x = e$.

A consequence of this definition is that the intersection of subgroups is a subgroup.

4 The Order of Elements

4.1 The Definition of Order for Elements

For x an element in some group G, we have that the order of x is defined by:

$$\operatorname{ord}(x) = \begin{cases} n \text{ such that } x^n = e & \text{if such } n \text{ exists} \\ \infty & \text{otherwise.} \end{cases}$$

The order is the ***least*** *possible integer such that $x^n = e$. To show the order of x is n, you need to show $x^n = e$ and $x^k \neq e$ for all $k \in \{1, 2, \ldots, n-1\}$.*

4.2 Properties of the Order of Elements

Let G be a group with element x:

- $\operatorname{ord}(x) = \infty \Rightarrow$ all x^i are distinct ($i \in \mathbb{Z}$)
- $|G| < \infty \Rightarrow \operatorname{ord}(x) < \infty$
- If $\operatorname{ord}(x) = n \in \mathbb{N}$, for $i \in \mathbb{N}$, $\operatorname{ord}(x^i) = \frac{n}{\gcd(n,i)}$.

5 Cyclic Groups

5.1 Definition of a Cyclic Group

For a group G, the cyclic group generated by $x \in G$ is defined by:

$$\langle x \rangle = \{x^i : i \in \mathbb{N}\}.$$

5.2 Properties of Cyclic Groups

For a group G with element x:

- $\langle x \rangle$ is a subgroup of G
- $|\langle x \rangle| = \mathrm{ord}(x)$
- Cyclic groups are Abelian
- Subgroups of cyclic groups are cyclic
- G is cyclic $\Leftrightarrow \exists\, x \in G$ such that $\mathrm{ord}(x) = |G|$.

6 Groups from Modular Arithmetic

6.1 Congruence Classes

A congruence class $[a]$ of the set $\mathbb{Z}/n\mathbb{Z}$ is a set of integers congruent to $a \pmod n$. We define the following operations:

- **Addition**: $[a] + [b] = [a + b]$
- **Multiplication**: $[a][b] = [ab]$.

For example:

$$\mathbb{Z}/7\mathbb{Z} = \bigcup_{i=0}^{6} [i],$$

with distinct elements $0, 1, 2, 3, 4, 5, 6$.

6.2 The Set of Congruence Classes under Addition

We have that the set $\mathbb{Z}/n\mathbb{Z}$ with the operation of addition $(\mathbb{Z}/n\mathbb{Z}, +)$ is a cyclic group generated by 1.

This means it's also an Abelian group.

6.3 The Set of Congruence Classes under Multiplication

The trouble with multiplication is that certain congruence classes never have inverses and as a result, the set under multiplication can never be a group. We have that an element $[a]$ of $(\mathbb{Z}/n\mathbb{Z}, \times)$ has an inverse if:

$$\gcd(a, n) = 1.$$

We define the set U_n as follows:

$$U_n = \{a : a \in \mathbb{Z} \text{ with } \gcd(a, n) = 1\}.$$

Thus, we have $(U_n, \times)$ is an Abelian group.