

# 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:

$$* : G \times G \rightarrow G.$$

*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:

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

## 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:

$$\begin{aligned} (ax = bx) &\Rightarrow (a = b) & (\forall a, b, x \in G) \\ (xa = xb) &\Rightarrow (a = b). & (\forall a, b, x \in G) \end{aligned}$$

*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  $x^ny^n$  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:

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

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  $D_{2n}$ :

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

## 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:

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

*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  $k \in \{1, 2, \dots, n-1\}$ .*

### 4.2 Properties of the Order of Elements

Let  $G$  be a group with element  $x$ :

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

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

## 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.

## 6.4 The Set of Congruence Classes under the Direct Product

For  $m, n$  positive integers with  $\gcd(m, n) = 1$ , we have:

$$U_m \times U_n \cong U_{mn}.$$

# 7 Isomorphisms

## 7.1 Definition of an Isomorphisms

For  $(G, *)$ ,  $(H, \circ)$  groups, an isomorphism  $\phi : G \rightarrow H$  is a bijective function such that:

$$\phi(x * y) = \phi(x) \circ \phi(y). \quad (\forall x, y \in G)$$

## 7.2 Properties of an Isomorphism

For the groups  $G, H, K$  and an isomorphism  $\phi : G \rightarrow H$ :

- $\phi^{-1}$  is an isomorphism
- $G$  and  $H$  are isomorphic ( $G \cong H$ )
- If there exists an isomorphism  $\psi : H \rightarrow K$  then  $G \cong K$  (transitive)
- $\phi(e_G) = e_H$
- $\phi(x^{-1}) = \phi(x)^{-1}$
- $\phi(x^i) = \phi(x)^i$  ( $i \in \mathbb{Z}$ )
- $\text{ord}_G(x) = \text{ord}_H(\phi(x))$
- $|G| = |H|$
- $G$  is Abelian  $\Leftrightarrow H$  is Abelian
- $G$  is cyclic  $\Leftrightarrow H$  is cyclic

## 8 Direct Products

### 8.1 Definition of the Direct Product

For  $G, H$  groups,  $G \times H$  is the Cartesian product of  $G$  and  $H$  with the binary operation:

$$(x, y)(a, b) = (x * a, y * b). \quad (\forall x, a \in G, y, b \in H)$$

This is itself a group.

### 8.2 Properties of the Direct Product

For  $H, K$  groups,  $G = H \times K$ :

- $G$  is finite  $\Leftrightarrow H$  and  $K$  are finite (in this case  $|G| = |H||K|$ )
- $G$  is Abelian  $\Leftrightarrow H$  and  $K$  are Abelian
- $G$  is cyclic  $\Rightarrow H$  and  $K$  are cyclic.

### 8.3 The Direct Product and Cyclic Groups

#### 8.3.1 Order of elements

For  $H, K$  groups,  $G = H \times K$ ,  $(x, y) \in G$ :

$$\text{ord}(x, y) = \text{lcm}(\text{ord}_H(x), \text{ord}_K(y)).$$

### 8.3.2 Condition for a cyclic direct product

For  $H, K$  groups,  $G = H \times K$ ,  $G$  is cyclic if and only if  $\gcd(|H|, |K|) = 1$ .

### 8.3.3 The direct product of cyclic groups

We denote the cyclic group of order  $n$  as  $C_n$ . We have that for  $C_n, C_m$  cyclic groups:

$$C_n \times C_m \cong C_{mn} \Leftrightarrow \gcd(m, n) = 1.$$

## 9 Lagrange's Theorem

### 9.1 Definition of Lagrange's Theorem

For a finite group  $G$  with  $H \leq G$  a subgroup. We have that  $|H|$  divides  $|G|$ .

### 9.2 Cyclic Subgroups

For  $G$  a finite group with order  $n$ , for  $x \in G$ ,  $\text{ord}(x)$  divides  $n$  (this is because  $\langle x \rangle \leq G$ ).

### 9.3 Cosets

#### 9.3.1 Definition of a coset

For a group  $G$  with  $H \leq G$  and  $x \in G$ , the left coset  $xH$  is and right coset  $Hx$  are the sets:

$$xH = \{xh : h \in H\}, Hx = \{hx : h \in H\}.$$

*While this is a subset of  $G$ , it is not necessarily a subgroup.*

#### 9.3.2 A bijection from a subgroup to its left coset

For a group  $G$  with  $H \leq G$ ,  $x \in G$ , and left coset  $xH$ , there exist a bijection from  $H$  to  $xH$ . This implies that their order is the same.

#### 9.3.3 The intersection of cosets

For a group  $G$  with  $H \leq G$ ,  $x, y \in G$ :

$$xH \cap yH \neq \emptyset \Leftrightarrow xH = yH.$$

*Cosets are distinct unless they are equal.*



### 9.3.4 Index of a subgroup

For a group  $G$  with  $H \leq G$  and  $x \in G$ , the index of  $H$  in  $G$   $|G : H|$  is the number of left cosets of  $H$  in  $G$ . So, since all cosets of  $H$  are distinct, we have:

$$|G| = |H||G : H|.$$

## 9.4 Consequences of Lagrange's Theorem

### 9.4.1 Intersection of subgroups

For a group  $G$  with  $H, K \leq G$ ,  $\gcd(|H|, |K|) = 1$  implies  $H \cap K = \{e\}$ .

### 9.4.2 Prime order groups

For  $G$  a group with  $|G| = p \in \mathbb{P}$  (prime):

- $G$  is cyclic
- Every element of  $G$  except the identity has order  $p$  (and generates  $G$ )
- The only subgroups of  $G$  are  $G$  and  $\{e\}$ .

## 10 Fermat-Euler Theorem

### 10.1 Euler's $\phi$ Function

We define the Euler  $\phi$  function over the naturals by:

$$\phi(n) = |\{a : a \in \mathbb{N}, \gcd(a, n) = 1\}|.$$

We have that  $\phi(n)$  is the order of  $U_n$  (the group of congruence classes under multiplication). Also, for  $p \in \mathbb{P}$  (prime),  $\phi p = p - 1$ .

*This is the number of values less than or equal to an integer that don't divide it.*

### 10.2 Fermat-Euler Theorem

For  $a, n \in \mathbb{N}$  with  $\gcd(a, n) = 1$ , we have that:

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

So, for  $p \in \mathbb{P}$  (prime):

$$a^{p-1} \equiv 1 \pmod{p}.$$