

# MATH 113: Abstract Algebra

Jack Lipson

November 11, 2023

# Contents

<b>1</b>	<b>Introduction to Groups</b>	<b>2</b>
1.1	Sets and Equivalence Relations . . . . .	2
1.2	Binary Operations . . . . .	3
1.3	Groups . . . . .	4
1.4	Isomorphic Binary Structures . . . . .	5
1.5	More on Groups and Subgroups . . . . .	6
1.6	Cyclic Groups . . . . .	7
1.7	Generating Sets and Cayley Digraphs . . . . .	10
<b>2</b>	<b>Permutations, Cosets, and Direct Products</b>	<b>12</b>
2.1	Groups of Permutations . . . . .	12
2.2	Orbits, Cycles, and the Alternating Groups . . . . .	15
2.3	Cosets and the Theorem of Lagrange . . . . .	18
2.4	Finitely Generated Abelian Groups . . . . .	19
<b>3</b>	<b>Homomorphisms and Factor Groups</b>	<b>22</b>
3.1	Homomorphisms . . . . .	22
3.2	Factor Groups . . . . .	24
3.3	Simple Groups . . . . .	25
3.4	Group Action on a Set . . . . .	27
<b>4</b>	<b>Rings and Fields</b>	<b>30</b>
4.1	Rings and Fields . . . . .	30
4.2	Integral Domains . . . . .	31
4.3	Fermat's and Euler's Theorems . . . . .	33
4.4	The Field of Quotients of an Integral Domain . . . . .	34
4.5	Rings of Polynomials . . . . .	35
4.6	Factorization of Polynomials over a Field . . . . .	37
<b>5</b>	<b>Ideals and Factor Rings</b>	<b>40</b>
5.1	Homomorphisms and Factor Rings . . . . .	40
5.2	Prime and Maximal Ideals . . . . .	42
<b>6</b>	<b>Extension Fields</b>	<b>46</b>
6.1	Introduction to Extension Fields . . . . .	46

# Chapter 1

## Introduction to Groups

### 1.1 Sets and Equivalence Relations

**Note.**  $\mathbb{R}^*$  and  $\mathbb{C}^*$  represent the set of all nonzero real and complex numbers. Zero is excluded from  $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$ .

**Note.** When a set contains an element  $b$  that's algebraically or arithmetically equivalent to another element(s), our set can be partitioned into subsets  $\bar{b}$  which denote all entitites equivalent to  $b$ . e.g.  $\frac{2}{3} = \frac{4}{6}$ .

**Definition 1 (Parititon).** A *partition* of a set is a decomposition of the set into subsests s.t. every element is in exactly one subset, or *cell*.

**Definition 2 (Equivalence Relation).** For a nonempty set  $S$ ,  $\sim$  is an equivalence relation between elements of  $S$  if for all  $a, b, c \in S$ ,  $(S, \sim)$  satisfies:

1. (Reflexive)  $a \sim a$ .
2. (Symmetric)  $a \sim b \Rightarrow b \sim a$ .
3. (Transitive)  $a \sim b \wedge b \sim c \Rightarrow a \sim c$ .

Non-equivalence relations usually use  $\mathcal{R}$ .

**Note.** All relations  $\mathcal{R}$  are defined as  $\{(a, b) \text{ for } a \in A, b \in B \mid a \mathcal{R} b\} \subseteq A \times B$ . For equivalence relations,  $\sim \subseteq S \times S$ .

**Remark (Natural Parition).**  $\sim$  yields a natural partition of  $S$ :  $\bar{a} = \{x \in S \mid x \sim a\}$  for all  $a \in S$ .

**Explanation.** For any  $a \in S$ ,  $a \in \bar{a}$ . So each element of  $S$  is in at least one cell. To show that  $a$  is in exactly one cell, let  $a \in \bar{b}$  as well. We must show

$\bar{a} = \bar{b}$ .  $\Rightarrow$ : If  $x \in \bar{a}$  then  $x \sim a$ . From our assumption  $a \sim b$  so by (3),  $x \sim b$  so  $x \in \bar{b}$  thus,  $\bar{a} \subseteq \bar{b}$ .  $\Leftarrow$ : If  $x \in \bar{b}$ ,  $x \sim b$ . From our assumption,  $a \sim b$  so, by (2),  $b \sim a$  meaning  $x \sim a$  via (3) implying  $x \in \bar{a}$  s.t.  $\bar{b} \subseteq \bar{a}$ . This completes the proof.

**Definition 3 (Equivalence Class).** Each cell  $\bar{a}$  in a natural partition given by an equivalence relation is called an equivalence class.

**Definition 4 (Congruence Modulo  $n$ ).** Let  $h, k$  be distinct integers and  $n \in \mathbb{Z}^+$ . We say  $h$  congruent to  $k$  modulo  $n$ , written  $h \equiv k \pmod{n}$  if  $n \mid h - k$  s.t.  $h - k = ns$  for some  $s \in \mathbb{Z}$ .

**Definition 5 (Residue Classes Modulo).** Equivalence classes for congruence modulo  $n$  are *residue classes modulo  $n$* .

**Remark.** Each residue class modulo  $n \in \mathbb{Z}^+$  contains an infinite number of elements.

**Definition 6 (Irreducible).** An irreducible polynomial  $h(x)$  is one that cannot be factored into polynomials in  $\mathcal{P}(\mathbb{R})$  all of lower degree than  $h(x)$ .

## 1.2 Binary Operations

**Definition 7 (Binary Operation).** A *binary operation*  $*$  on a set  $S$  is a rule that assigns to each ordered pair  $(a, b)$  of elements of  $S$  another element of  $S$  generally denoted  $a * b$  or formally  $*(a, b)$ . To be *well-defined*,  $*$  must assign a value to every possible  $a * b$ .

**Definition 8 (Closure under  $*$ ).** A set  $S$  is *closed under  $*$*  if for all  $a, b \in S$ ,  $a * b \in S$ . If a subset  $H$  of  $S$  is also closed under  $*$ , this is referred to as the *induced operation  $*$  on  $H$* .

**Definition 9 (Commutative Operation).** A binary operation  $*$  on a set  $S$  is *commutative* iff  $a * b = b * a$  for all  $a, b \in S$ .

**Definition 10 (Associative operation).** A binary operation  $*$  on a set  $S$  is *associative* iff  $(a * b) * c = a * (b * c)$  for all  $a, b, c \in S$ .

**Note.** Associativity of function composition follows.

**Remark.** A binary operation on a set, typically finite, can be represented

as follows:

$*$	$a$	$b$	$c$
$a$	$b$	$b$	$b$
$b$	$a$	$c$	$b$
$c$	$c$	$b$	$a$

### 1.3 Groups

**Definition 11 (Group).** A group  $\langle G, * \rangle$  is a set  $G$  combined with a binary operation  $*$  on  $G$  which satisfies the following axioms:

- ( $\mathcal{G}_1$ )  $*$  is associative.
- ( $\mathcal{G}_2$ ) There exists a **unique identity** element  $e$  on  $G$  s.t.  $e * x = x * e$  for all  $x \in G$ .
- ( $\mathcal{G}_3$ ) For each  $a \in G$ , there exists an  $a' \in G$  s.t.  $a' * a = a * a' = e$ . This  $a'$  is called the *inverse* of  $a$  with respect to the operation  $*$ .
- ( $\mathcal{G}_4$ ) (optional if part of binary operation definition)  $G$  is closed under  $*$ .

**Theorem 1 (Left/Right Cancellation).** If  $G$  is a group with binary operation  $*$ , then the *left and right* cancellation laws hold s.t.  $a * b = a * c \Rightarrow b = c$  and  $b * a = c * a \Rightarrow b = c$  for all  $a, b, c \in G$ .

**Proof.** The right cancellation proof is identical to that below.

$$\begin{array}{ll}
 a * b = a * c & \because \text{by supposition} \\
 a' * (a * b) = a' * (a * c) & \because \text{inverse axiom.} \\
 (a' * a) * b = (a' * a) * c & \because \text{associativity axiom} \\
 e * b = e * c & \because \text{inverse axiom} \\
 b = c & \square \text{ identity axiom}
 \end{array}$$

□

**Theorem 2.** Trivially, in a group  $G$ ,  $(ab)' = b'a'$  for all  $a, b \in G$ .

**Remark.** Note that the solutions  $x, y$  to  $a * x = b$  and  $y * a = b$  have unique solutions in  $G$  for any  $a, b \in G$ . Similarly,  $e$  is unique.

**Note (Idempotent for  $*$ ).** An element  $x$  of  $S$  is *idempotent for  $*$*  if  $x * x = x$ . This is always in the identity element.

**Definition 12 (Abelian Group).** A group  $G$  is *abelian* if its binary operation is commutative.

**Definition 13 (Roots of Unity).** Call the elements of the set  $U_n := \{z \in \mathbb{C} \mid z^n = 1\}$  the  $n^{\text{th}}$  roots of unity, usually listed as  $1 = \zeta^0, \zeta^1, \zeta^2, \dots, \zeta^{n-1}$ .

**Remark.** Let the unit circle  $U := \{z \in \mathbb{C} \mid |z| = 1\}$ . Clearly, for any  $z_1, z_2 \in U$ ,  $|z_1 z_2| = |z_1| |z_2| = 1$  such that  $z_1 z_2 \in U$  implying  $U$  is closed under  $\cdot$ . Note then that  $\langle U, \cdot \rangle \simeq \langle R_{2\pi}, +_{2\pi} \rangle$ . Similarly,  $\langle U_n, \cdot \rangle \simeq \langle \mathbb{Z}_n, +_n \rangle$  for  $n \in \mathbb{Z}^+$ .

**Definition 14 (Addition Modulo  $n$ ).** We respectively write  $\mathbb{Z}_n$  and  $\mathbb{R}_c$  to denote  $[0, 1, \dots, n-1]$  and  $[0, c]$ . Addition modulo  $n/c$  is written  $+_n$  or  $+_c$ .

## 1.4 Isomorphic Binary Structures

**Definition 15 (Binary Algebraic Structures).** For two *binary algebraic structures*  $\langle S, * \rangle$  and  $\langle S', *' \rangle$  to be structurally alike, we would need a one-to-one correspondence between the elements  $x \in S$  and  $x' \in S'$  s.t. if  $x \leftrightarrow x'$  and  $y \leftrightarrow y'$  then  $x * y \leftrightarrow x' *' y'$ .

**Remark (Homomorphism Property).** This last condition is called the *homomorphism property*. If the function  $\phi$  is NOT one-to-one, it is a homomorphism only.

**Definition 16 (Isomorphism).** An *isomorphism* of  $S$  with  $S'$  is a one-to-one function  $\phi$  mapping  $S$  onto  $S'$  such that  $\phi(x * y) = \phi(x) *' \phi(y)$  for all  $x, y \in S$ .

If such a map exists,  $S$  and  $S'$  are called *isomorphic binary structures* denoted  $S \simeq S'$ .

**Note (Show Binary Algebraic Structures are Isomorphic).**

(Step 1) Define the function  $\phi$  which defines  $\phi(s)$  for all  $s \in S$  and gives the isomorphism from  $S \rightarrow S'$ .

(Step 2) Show  $\phi$  is one-to-one.

(Step 3) Show  $\phi$  is onto.

(Step 4) Show  $\phi(x * y) = \phi(x) *' \phi(y)$  for all  $x, y \in S$ .

**Example.** Take the isomorphism  $\phi: \mathbb{R} \rightarrow \mathbb{R}^+: x \mapsto e^x$  from  $\langle \mathbb{R}, + \rangle$  to  $\langle \mathbb{R}^+, \cdot \rangle$ . Clearly,  $\forall x \in \mathbb{R}, \phi(x) \in \mathbb{R}^+$  and  $\phi$  is bijective. Last, for  $x, y \in \mathbb{R}$ ,  $\phi(x + y) = e^{x+y} = e^x e^y = \phi(x) \cdot \phi(y)$ .

**Definition 17 (Structural Property).** A structural property is any property of a binary structure that is invariant to any isomorphic structure. These, like cardinality, are used to show no such isomorphism exists between structures.

**Example.** Although  $\langle \mathbb{Q}, + \rangle$  and  $\langle \mathbb{Z}, + \rangle$  both have cardinality  $\aleph_0$  and have many one-to-one functions between them, the equation  $x + x = c$  has a solution  $x \in \mathbb{Q}$  for all  $c \in \mathbb{Q}$ , but this is not true for  $\mathbb{Z}$  if, say,  $c = 3$ . This structural property distinguishes these binary structures and thus they are not isomorphic under the usual addition.

**Theorem 3.** Suppose  $\langle S, * \rangle$  has an identity element  $e$  for  $*$ . If  $\phi: S \rightarrow S'$  is an isomorphism to  $\langle S', *' \rangle$  then  $\phi(e)$  is an identity element for  $'$  on  $S'$ .

**Proof.** Because an isomorphism exists from  $S \rightarrow S'$ , for any element  $s' \in S'$ , there exists exactly one element  $s \in S$  s.t.  $\phi(s) = s'$ . By the definition of an isomorphism  $s' = \phi(s) = \phi(s * e) = \phi(s) *' \phi(e) = s' *' \phi(e)$  for an arbitrary element  $s'$  of  $S$ . This implies  $\phi(e)$  is the identity element for  $S'$ .  $\square$

## 1.5 More on Groups and Subgroups

**Definition 18 (Semigroup).** A semigroup is an algebraic structure combining a set with an associative binary operation.

**Definition 19 (Monoid).** A monoid is a semigroup that has an identity element corresponding to its binary operation.

**Definition 20 (Subgroup).** If a subset  $H$  of a group  $G$  is closed under the binary operation of  $G$  and is itself a group,  $H$  is a *subgroup* of  $G$ . This is denoted  $H \leq G$ .  $H < G \Rightarrow H \neq G$ .

**Example.**  $\langle \mathbb{Z}, + \rangle < \langle \mathbb{R}, + \rangle$ , but  $\langle \mathbb{Q}, \cdot \rangle$  is *not* a subgroup of  $\langle \mathbb{R}, - \rangle$ .

**Definition 21 (Proper and trivial subgroups).** If  $G$  is a group, the subgroup consisting of  $G$  itself is the *improper subgroup* of  $G$ . All other subgroups are *proper subgroups*. The subgroup  $\{e\}$  is the *trivial subgroup* of  $G$  and all other subgroups are nontrivial.

**Theorem 4.** A subset  $H$  of a group  $G$  is a subgroup of  $G$  if and only if:

1.  $H$  is closed under the binary operation of  $G$ .
2. the identity  $e$  of  $G$  is in  $H$ .

3. for all  $a \in H$ ,  $a^{-1} \in H$  also.

**Proof.**  $\Rightarrow$ : Let  $H$  be a subgroup of  $G$ . By definition,  $H$  is closed under  $G$ 's binary operation (1).  $H$  must have an identity element because it is a group. Because  $a * x = a$  and  $y * a = a$  have unique solutions,  $H$ 's identity element must be the same in  $H$  group as  $G$  group (2). (3) is trivial because  $H$  is a group.

$\Leftarrow$ : Let (1), (2), (3) be true. Then  $H$  has a unique identity element on its binary operation ( $\mathcal{G}_2$ ), each element of  $H$  has a unique inverse in  $H$  ( $\mathcal{G}_3$ ), and  $H$  is closed under the binary operation of  $G$  (optional  $\mathcal{G}_4$ ). To satisfy ( $\mathcal{G}_1$ ), the binary operation on  $H$  must be associative s.t., for all  $a, b, c \in H$ ,  $(ab)c = a(bc)$ . But this clearly holds in  $G$  so ( $\mathcal{G}_1$ ) is satisfied and  $H$  is a subgroup of  $G$ .  $\square$

## 1.6 Cyclic Groups

**Theorem 5.** Let  $G$  be a group and  $a \in G$ . Then

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of  $G$  and the *smallest* subgroup of  $G$  that contains  $a$ .

**Proof.** Let's first check  $H$  is indeed a subgroup of  $G$ . (1) For any  $r, s \in \mathbb{Z}$ ,  $a^r * a^s = \overbrace{(a * \dots * a)}^{a \text{ } r \text{ times}} * \overbrace{(a * \dots * a)}^{a \text{ } s \text{ times}} = a^{r+s} \in H$  so we have closure. (2) Let  $e := a^0 \in H$  so for all  $r \in \mathbb{Z}$ ,  $a^r * a^0 = a^r$ . (3) For all  $r \in \mathbb{Z}$ ,  $a^r \in H$  so  $\exists a^{-r} \in H$  such that  $a^r * a^{-r} = a^0 = e$ . Thus,  $H \leq G$ .

Next, to show it's the smallest possible subgroup, just take the set  $\{a\}$ . To have closure, we must add  $a^n \forall n \in \mathbb{Z}^+$ . To have inverses, we must have  $a^{-n}$  so our set becomes  $\{a^n \mid n \in \mathbb{Z} \setminus \{0\}\}$ . To have an identity, we must have  $a^0$  and this completes the proof.  $\square$

**Definition 22 (Cyclic Subgroup of  $G$ ).** For any  $a \in G$ , define  $\langle a \rangle$  to be the set  $\{a^n \mid n \in \mathbb{Z}\}$ . This is called the *cyclic subgroup of  $G$  generated by  $a$* . An element  $a$  of a group  $G$  *generates  $G$*  and is a *generator for  $G$*  if  $\langle a \rangle = G$ .

**Definition 23 (Cyclic Group).** A group is *cyclic* if there is some element  $a$  in  $G$  that generates  $G$ .

**Example.**  $\langle 1 \rangle = \langle 3 \rangle = \mathbb{Z}_4$  so  $\mathbb{Z}_4$  is cyclic and both 1 and 3 are generators.

**Example.** The group  $\langle \mathbb{Z}, + \rangle$  is a cyclic group generated ONLY by 1 and -1.



**Remark (Subgroup Diagrams).** Lattice, or *subgroup diagrams*, can be drawn such that lines run down from a group  $G$  to a group  $H$  if  $H < G$ .

**Example.** Take two group structures of order 4:  $\mathbb{Z}_4$  and the Klein 4-group *Vierergruppe* defined as follows:

	+	0	1	2	3
	0	0	1	2	3
$\mathbb{Z}_4 :$	1	1	2	3	0
	2	2	3	0	1
	3	3	0	1	2

	*	e	a	b	c
	e	e	a	b	c
$V :$	a	a	e	c	b
	b	b	c	e	a
	c	c	b	a	e

$\mathbb{Z}_4$   
 $\downarrow$   
 $\{0, 2\}$   
 $\downarrow$   
 $\{0\}$

$V$   
 $\swarrow \quad \downarrow \quad \searrow$   
 $\{e, a\} \quad \{e, b\} \quad \{e, c\}$   
 $\swarrow \quad \downarrow \quad \searrow$   
 $\{e\}$

We can map these as:      and      .

**Definition 24 (Order).** If the cyclic subgroup  $\langle a \rangle$  of  $G$  is finite, we say the order of  $a$  is the order  $|\langle a \rangle|$ . Otherwise,  $a$  is of *infinite order*.

**Theorem 6.** Every cyclic group is abelian.

**Theorem 7 (Division Algorithm for  $\mathbb{Z}$ ).** If  $m \in \mathbb{Z}^+$  and  $n \in \mathbb{Z}$ , then there exist unique integers  $q, r$  such that

$$n = mq + r \quad \text{and} \quad 0 \leq r < m.$$

**Proof.** From the archimedean property, there is a unique  $q$  such that  $qm \leq n < (q+1)m$ . Then,  $0 \leq r = n - mq < m$  is unique. We regard  $q$  and  $r$  as the quotient and nonnegative remainder respectively when  $n$  is divided by  $m$ .  $\square$

**Theorem 8.** A subgroup of a cyclic group is cyclic.

**Proof.** Take a cyclic group  $G$  with subgroup  $H$ . If  $H = \langle e \rangle$  then  $H$  is cyclic and the proof is complete.

Otherwise,  $H \neq \langle e \rangle$  so there exists  $b \in H, b \neq e$ . Because  $G$  is cyclic, there must exist  $a \in G$  such that  $a$  generates  $G$ , i.e. for all  $n \in \mathbb{Z}^+$ ,  $a^n$  spans every value of  $G$  including every element of  $H$ . Let  $c := a^m$  where  $m$  is the least positive integer such that  $c \in H$ . Now, for all  $b \in H$ , take  $n$  such that  $b = a^n$ . From division algorithm, there exist integers  $q, r$  such that  $n = mq + r$  so  $a^n = a^{mq+r} = (a^m)^q a^r$  which implies, because  $a^m \in H$  and

$H$  is a group so  $a^{-m} \in H$ ,  $a^n(a^m)^{-q} = a^r$ .  $H$  is a group so this implies  $a^r \in H$ . Because  $0 \leq r < m$  and  $m$  is the least positive integer such that  $a^m \in H$ ,  $r = 0$  such that  $n = mq$  for all  $b = a^n = (a^m)^q \in H$ .  $\langle c \rangle = H$  so  $H$  is cyclic.  $\square$

**Definition 25 (Greatest Common Divisor).** The positive generator  $d$  of the cyclic group  $H = \{nr + ms \mid n, m \in \mathbb{Z}\}$  under addition is called the *greatest common divisor* of  $r$  and  $s$ , written  $d = \gcd(r, s)$ .

**Definition 26.** Two integers are *relatively prime* if their gcd is 1.

**Theorem 9.** Let  $G$  be a cyclic group with generator  $a$ . If the order of  $G$  is infinite, then  $G$  is isomorphic to  $\langle \mathbb{Z}, + \rangle$ . If  $G$  has finite order  $n$ , then  $G$  is instead isomorphic to  $\langle \mathbb{Z}_n, +_n \rangle$ .

**Proof.** Take the following two cases. **Case 1:** For all positive integers  $m$ ,  $a^m \neq e$ . Suppose  $a^h = a^k$  and  $h > k$ . Thus,  $a^h a^{-k} = a^{h-k} = e$  which contradicts our assumption. Therefore, each element of  $G$  can be uniquely expressed as  $a^m$  for a unique  $m \in \mathbb{Z}$ . The map  $\phi : G \rightarrow \mathbb{Z}$  defined as  $\phi(a^i) = i$  is then well-defined and bijective on  $\mathbb{Z}$ . Last,  $\phi(a^i a^j) = \phi(a^{i+j}) = i + j = \phi(a^i) + \phi(a^j)$  so the homomorphism property is satisfied and  $\phi$  is an isomorphism to  $\langle \mathbb{Z}, + \rangle$ .

**Case 2:**  $a^m = e$  for some  $m \in \mathbb{Z}^+$ . Let  $n$  be the smallest positive integer so  $a^n = e$ . If  $s \in \mathbb{Z}$  and  $s = q + r$  for  $0 \leq r < n$ , then  $a^s = a^{nq+r} = (a^n)^q a^r = a^r$ . Like in case 1, if  $0 < k < h < n$  and  $a^h = a^k$ , then  $a^{h-k} = e$  and  $0 < h - k < n$  contradicting our assumption that  $n$  is the smallest positive integer possible. Hence,  $a^0, a^1, a^2, \dots, a^{n-1}$  are all distinct and comprise all elements of  $G$ . We can then make the map  $\psi : G \rightarrow \mathbb{Z}_n$  defined by  $\psi(a^i) = i$  for  $i = 0, 1, \dots, n-1$  is well-defined and bijective on  $\mathbb{Z}_n$ . Also, because  $a^n = e$ ,  $a^i a^j = a^k$  whenever  $k = i +_n j$ . Therefore,  $\psi(a^i a^j) = i +_n j = \psi(a^i) +_n \psi(a^j)$  satisfying the homomorphism property so  $\psi$  is an isomorphism to  $\langle \mathbb{Z}_n, +_n \rangle$ .  $\square$

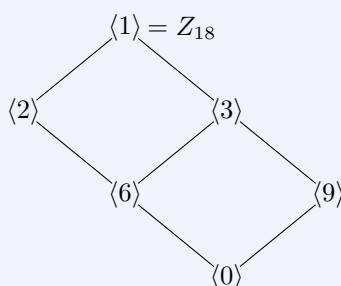
**Theorem 10.** Let  $G$  be a cyclic group generated by  $a$  with  $n$  elements. Let  $b \in G$  and  $b = a^s$ . Then,  $b$  generates a cyclic subgroup  $H$  of  $G$  containing  $n/d$  elements where  $d$  is the greatest common divisor of  $n$  and  $s$ . Also,  $\langle a^s \rangle = \langle a^n \rangle \Leftrightarrow \gcd(s, n) = \gcd(t, n)$ .

**Proof.** We already know  $b$  generates a cyclic subgroup  $H$  of  $G$ . And that because it is finite, it has only as many elements as the smallest power  $m$  of  $b$  so  $b^m = e$ . This and  $b = a^s$  implies  $(a^s)^m = e$  if and only if  $n$  divides  $ms$  because  $a^n = e$  because  $G$  is of finite order  $n$ . Let  $d = \gcd(n, s)$  such that we want to find the smallest  $m$  so  $\frac{ms}{n} = \frac{m(s/d)}{(n/d)}$  is an integer. This implies  $(n/d)$  divides  $m$  so the smallest  $m$  we can pick is  $n/d$ . Thus,  $H$  has order  $n/d$ .

We know  $G$  is isomorphic to  $\langle \mathbb{Z}_n, +_n \rangle$  so taking cyclic subgroup  $\langle d \rangle$  of  $\mathbb{Z}_n$  where  $d$  divides  $n$  implies  $\langle d \rangle$  has  $n/d$  elements and contains all positive integers  $m$  less than  $n$  such that  $\gcd(m, n) = d$ . Thus, there is only one subgroup of  $\mathbb{Z}_n$  of order  $n/d$ . It immediately follows that  $\langle a^s \rangle = \langle a^t \rangle$  if and only if  $\gcd(s, n) = \gcd(t, n)$ .  $\square$

**Corollary.** If  $a$  is a generator of a finite cyclic group  $G$  of order  $n$ , then the other generators of  $G$  are the elements of the form  $a^r$ , where  $r$  is relatively prime to  $n$ .

**Example.** For instance, we can derive the subgroup diagram for  $Z_{18}$  as:



## 1.7 Generating Sets and Cayley Digraphs

**Example.** The Klein 4-group  $V = \{e, a, b, c\}$  is generated by  $\{a, b\}$  since  $ab = c$ . It is similarly generated by  $\{a, c\}$ ,  $\{b, c\}$ , and  $\{a, b, c\}$ .

**Theorem 11.** The intersection of some subgroups  $H_i$  of a group  $G$  for  $i \in I$  is again a subgroup of  $G$  where  $I$  is the set of indices.

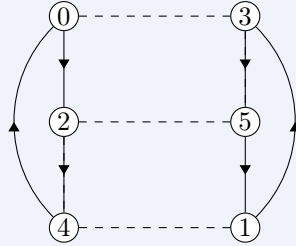
**Proof.** First, closure. For any  $a, b \in \bigcap_{i \in I} H_i$ , because each  $H_i$  has closure,  $a, b \in H_i \Rightarrow ab \in H_i$  so  $ab \in \bigcap_{i \in I} H_i$ . Similarly, because the identity element of  $G$  is in  $H_i$  for all  $i \in I$ ,  $e \in \bigcap_{i \in I} H_i$ . Last, for all  $a \in \bigcap_{i \in I} H_i$ , because  $H_i$  is a group,  $a^{-1} \in H_i$ . Thus, for any  $a \in \bigcap_{i \in I} H_i$ ,  $a \in H_i$  for all  $i$  so  $a^{-1} \in H_i$  for all  $i$  so  $a^{-1} \in \bigcap_{i \in I} H_i$ .  $\square$

**Definition 27 (Subgroup generated by  $\{a_i \mid i \in I\}$ ).** Let  $G$  be a group and  $a_i \in G$  for  $i \in I$ . The smallest subgroup of  $G$  containing  $\{a_i \mid i \in I\}$  is the *subgroup generated by  $\{a_i \mid i \in I\}$* . If this subgroup is all of  $G$  then the set *generates  $G$*  and the  $a_i$  are the *generators of  $G$* . If there is a finite set that generates  $G$ , we say  $G$  is *finitely generated*.

**Definition 28 (Digraph).** A directed graph, abbreviated as *digraph*, consists of a finite number of points, or *vertices* and some *arcs* denoted by an arrowhead joining them together.

**Definition 29 (Cayley Digraphs).** Cayley digraphs draw arcs of different types between each element of  $G$  demonstrating what each element is generated by. Of course, if  $x \rightarrow y$  means  $xa = y$  then  $ya^{-1} = x$ . Traveling opposite to arrow direction implies this second equality.

**Example.** For instance, we can create the digraph for  $Z_6$  with generator



set  $S = \{2, 3\}$  as:

with solid (2) and dashed (3) lines. Dashed lines have no arrowhead because 3 is its own inverse.

## Chapter 2

# Permutations, Cosets, and Direct Products

### 2.1 Groups of Permutations

**Definition 30 (Permutation of a set).** A *permutation of a set*  $A$  is a function  $\phi: A \rightarrow A$  that is both one to one and onto.

**Remark (Permutation Multiplication).** Function composition  $\circ$  is a binary operation on the collection of all permutations of a set  $A$ . We call this operation *permutation multiplication*.

**Remark.** Let  $\sigma, \tau$  be permutations of a set  $A$  so  $\sigma, \tau$  are both one-to-one function mapping  $A$  onto  $A$ . then,  $\sigma \circ \tau$ , or simply  $\sigma\tau$  is a permutation as long as it is one-to-one.

For any  $a_1, a_2 \in A$ , if  $(\sigma\tau)(a_1) = (\sigma\tau)(a_2)$  gives  $(\sigma(\tau(a_1))) = (\sigma(\tau(a_2)))$ . Because  $\sigma$  is injective,  $\tau(a_1) = \tau(a_2)$ . Because  $\tau$  is injective,  $a_1 = a_2$  so  $\sigma\tau$  is injective.

For any  $a \in A$ , there exists some  $b \in A$  so  $\sigma(b) = a$  because  $\sigma$  is onto  $A$ . Because  $\tau$  is onto  $A$ , there exists some  $c \in A$  so  $\tau(c) = b$ . Thus,  $a = (\sigma\tau)(c)$  so  $\sigma\tau$  is onto  $A$ .

**Example.** Given a set  $A = \{1, 2, 3, 4, 5\}$ , we can write a permutation  $\sigma$  as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}.$$

so  $\sigma(1) = 4$ , etc.

**Theorem 12.** Let  $A$  be a nonempty set, and  $S_A$  be the collection of all permutations of  $A$ . Then,  $S_A$  is a group under permutation multiplication.

**Proof.** Because the composition of two permutations of  $A$  results in a permutation, we have closure under  $\circ$ . For any functions  $f, g, h$ ,  $((f \circ g) \circ h)(x) = (f(g)) \circ (h)(x) = f(g(h))(x) = f(g \circ h)(x)$  so  $\mathcal{G}_1$  is easily satisfied. The permutation  $\iota$  defined as  $\iota(a) = a$  for all  $a \in A$  is the identity ( $\mathcal{G}_2$ ). Last, for any permutation  $\sigma$ ,  $\sigma^{-1}$  reverse the direction of the mapping  $\sigma$  such that  $\sigma^{-1}(a)$  is the element  $a'$  of  $A$  so  $\sigma(a') = a$ . This exists because  $\sigma$  is bijective. For any  $a \in A$ ,  $\iota(a) = a = \sigma(a') = \sigma(\sigma^{-1}(a')) = (\sigma\sigma^{-1})(a)$  and  $\iota(a') = a' = \sigma^{-1}(a) = \sigma^{-1}(\sigma(a')) = (\sigma^{-1}\sigma)(a')$  satisfying  $\mathcal{G}_3$ .  $\square$

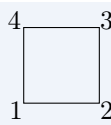
**Remark.** To define an isomorphism  $\phi: S_A \rightarrow S_B$ , we let  $f: A \rightarrow B$  have one-to-one function mapping  $A$  onto  $B$  so  $A$  and  $B$  have the same cardinality so for  $\sigma \in S_A$ , let  $\phi(\sigma) = \bar{\sigma} \in S_B$  so that for all  $a \in A$ ,  $\bar{\sigma}(f(a)) = f(\sigma(a))$ .

**Definition 31 (Symmetric Group on  $n$  Letters).** Let  $A$  be the finite set  $\{1, 2, \dots, n\}$ . The group of all permutations of  $A$  is the *symmetric group on  $n$  letters*  $S_n$ . Note that  $S_n$  has  $n!$  elements.

**Remark.**  $S_3$  is also the 3rd dihedral group  $D_3$  of *symmetries of an equilateral triangle* where  $\rho_i$  is rotations and  $\mu_i$  is mirror images in bisectors of angles such that  $D_3$  is made up of:

$$\left\{ \begin{array}{l} \rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \mu_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \\ \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \\ \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \end{array} \right\}$$

**Definition 32 ( $n$ th Dihedral Group  $D_n$ ).** The  $n$ th *dihedral group*  $D_n$  is the group of symmetries of the regular  $n$ -gon.



**Example (Octic Group  $D_4$ ).** Given a square: ,  $D_4$  is the set of:

$$\left\{ \begin{array}{l} \rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \mu_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \\ \rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \\ \rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \delta_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \\ \rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \quad \delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}. \end{array} \right\}$$

where  $\rho_i, \mu_i, \delta_i$  represent rotations, mirror images in perpendicular bisectors of sides, and diagonal flips respectively.

**Definition 33 (Image of  $H$  under  $f$ ).** Let  $f: A \rightarrow B$  be a function and  $H$  be a subset of  $A$ . The *image of  $H$  under  $f$*  is the set  $\{f(h) \mid h \in H\}$  and is denoted  $f[H]$ .

**Lemma 1.** Let  $G, G'$  be groups and  $\phi: G \rightarrow G'$  be a one-to-one function such that for all  $x, y \in G$ ,  $\phi(xy) = \phi(x)\phi(y)$ . Thus  $\phi[G]$  is a subgroup of  $G'$  and  $\phi$  provides an isomorphism of  $G$  with  $\phi[G]$ .

**Proof.** We simply prove the subgroup requirements. For any  $x', y' \in \phi[G]$ , there exist  $x, y \in G$  so  $\phi(x) = x'$  and  $\phi(y) = y'$ . By hypothesis,  $\phi(xy) = \phi(x)\phi(y)$  so  $x'y' \in \phi[G]$  so  $\phi[G]$  is closed under the operation of  $G'$ . Next, say  $e'$  is the identity of  $G'$ . Then,  $e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e)$ . Cancellation in  $G'$  shows  $e' = \phi(e)$  so  $e' \in \phi[G]$ . Last, for any  $x' \in \phi[G]$ ,  $e' = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1}) = x'\phi(x^{-1})$  implying  $x'^{-1} = \phi(x^{-1}) \in \phi[G]$ . Thus  $\phi[G]$  is a subgroup of  $G'$ . We already showed  $\phi$  is onto and therefore an isomorphism of  $G$  with  $\phi[G]$ .  $\square$

**Theorem 13 (Cayley's Theorem).** Every group is isomorphic to a group of permutations.

**Proof.** Let  $G$  be a group. We want to show  $G$  is isomorphic to a subgroup of  $S_G$ . By the previous lemma, we need only define a universal one-to-one function  $\phi: G \rightarrow S_G$  with the homomorphism property. For any  $x, g \in G$ , let's define left multiplication by  $x$  via  $\lambda_x: G \rightarrow G$  as  $\lambda_x(g) = xg$ . For all  $c \in G$ ,  $\lambda_x(x^{-1}c) = x(x^{-1}c) = c$  so clearly  $\lambda_x$  maps  $G$  onto  $G$ . Also, for any  $a, b \in G$ ,  $\lambda_x(a) = \lambda_x(b) \Rightarrow xa = xb \Rightarrow a = b$  through left cancellation. Thus,  $\lambda_x$  is one-to-one, onto, and a permutation of  $G$ . Now, we define  $\phi: G \rightarrow S_G$  as  $\phi(x) = \lambda_x$  for all  $x \in G$ .

To satisfy our lemma, we now only show  $\phi$  is one-to-one and has the homo-

morphism property. Let  $e$  be the identity on  $G$  so that  $\phi(x) = \phi(y)$  implies  $\lambda_x = \lambda_y$  so  $\lambda_x(e) = \lambda_y(e) \Rightarrow xe = ye \Rightarrow x = y$ . Last, for any  $x, y, g \in G$ ,  $\lambda_{xy}(g) = (xy)g = x(yg) = \lambda_x(\lambda_y(g)) = \lambda_x\lambda_y(g)$  so  $\phi(xy) = \phi(x)\phi(y)$  satisfying the homomorphism property.  $\square$

**Definition 34 (Left/Right Regular Representation).** The map  $\phi: G \rightarrow S_G$  defined as above is the *left regular representation* of  $G$  and the map  $\mu: G \rightarrow S_G$  defined by  $\mu(x) = \rho_{x^{-1}}$  where  $\rho_x(g) = gx$  for all  $x, g \in G$  is the *right regular representation* of  $G$ .

## 2.2 Orbits, Cycles, and the Alternating Groups

**Definition 35 (Orbit of  $a$  under  $\sigma \in S_A$ ).** Let  $A$  be a set and  $\sigma \in S_A$ . For a fixed  $a \in A$ , the set  $\mathcal{O}_{a,\sigma} = \{\sigma^n(a) \mid n \in \mathbb{Z}\}$  is the *orbit of  $a$  under  $\sigma$* .

**Remark.** Let  $\sigma$  be a permutation of a set  $A$ . The equivalence classes in  $A$  are determined by the following equivalence class:

For  $a, b \in A$ , let  $a \sim b$  if and only if  $b = \sigma^n(a)$  for some  $n \in \mathbb{Z}$ .

These are called the *orbits of  $\sigma$* .

**Explanation.**  $\sim$  is an equivalence relation because it is:

1. **reflexive:**  $a \sim a$  clearly because  $a = \iota(a) = \sigma^0(a)$ .
2. **symmetric:** If  $a \sim b$ , then  $b = \sigma^n(a)$  for some  $n \in \mathbb{Z}$  so  $a = \sigma^{-n}(b)$  and  $-n \in \mathbb{Z}$  so  $b \sim a$ .
3. **transitive:** If  $a \sim b, b \sim c$ , then  $b = \sigma^n(a)$  and  $c = \sigma^m(b)$  for some  $n, m \in \mathbb{Z}$ . This implies  $c = \sigma^m(\sigma^n(a)) = \sigma^{n+m}(a)$  so  $a \sim c$ .

**Example.** The orbits of  $\iota$  are the singleton subsets of  $A$ .

**Example.** Given the permutation  $\sigma$  of a finite set  $A$  defined as:

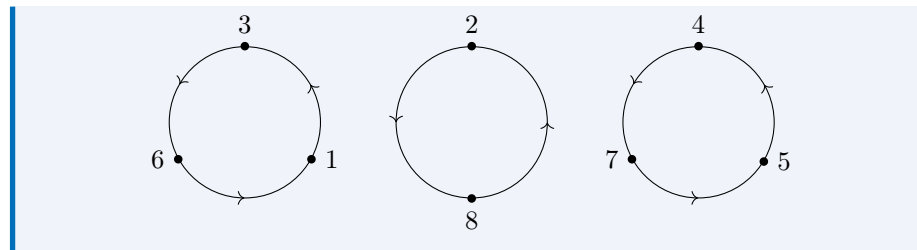
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix},$$

the complete list of orbits of  $\sigma$  are

$$\{1, 3, 6\}, \{2, 8\}, \text{ and } \{4, 5, 7\},$$

which we can map in the following way:





**Definition 36.** A permutation  $\sigma \in S_n$  is a *cycle* if it has at most one orbit containing more than one element. The *length* of a cycle is the number of elements in its largest orbit.

**Remark.** We can use *cyclic notation* to simply denote  $\mu = (1, 3, 6)$ .

**Remark.** Cycles are *disjoint*. That is, no integer appears in the notations of 2 different cycles. Note that multiplication of disjoint cycles *is* commutative.

**Theorem 14.** Every permutation  $\sigma$  of a finite set is a product of disjoint cycles.

**Proof.** Let  $B_1, B_2, \dots, B_r$  be the orbits of  $\sigma$  and define the cycle  $\mu_i$  as:

$$\mu_i(x) = \begin{cases} \sigma(x) & x \in B_i \\ x & \text{otherwise.} \end{cases}$$

Clearly,  $\sigma = \mu_1 \mu_2 \cdots \mu_r$ . Because the orbits  $B_1, B_2, \dots, B_r$  are disjoint equivalence-classes, the cycles  $\mu_1, \mu_2, \dots, \mu_r$  are disjoint also.  $\square$

**Example.** Take the disjoint cycles  $\sigma = (1, 3, 5, 2)$  and  $\tau = (2, 5, 6)$ . To find  $\sigma\tau$  ( $\tau$  first), begin with 1 so  $\sigma\tau = (1, \dots)$ .  $\tau$  doesn't map 1 but  $\sigma$  maps it to 3 so we get  $(1, 3, \dots)$ . Following this cycle, 3 isn't mapped anywhere by  $\tau$  but is mapped to 5 so  $(1, 3, 5, \dots)$ . 5 is mapped to 6 but 6 isn't mapped anywhere so it stays fixed as  $(1, 3, 5, 6, \dots)$ . Beginning a new cycle, 2 is mapped to 5 then back to 2 so it becomes  $(1, 3, 5, 6)(2)$ . Finally, 4 isn't mapped anywhere by either so it stays as 4. Thus,  $(1, 3, 5, 2)(2, 5, 6) = (1, 3, 5, 6)(2)(4) = (1, 3, 5, 6)$ .

**Definition 37 (Transposition).** A cycle of length 2 is a *transposition*.

**Corollary.** Any permutation of a finite set of at least 2 elements is a product of transpositions. The identity, for  $S_n$  with  $n \geq 2$  is  $(1, 2)(1, 2)$ .

**Theorem 15.** No permutation in  $S_n$  can be expressed both as a product of an even and odd number of transpositions.

**Proof.** (Linear Algebra) Recall  $S_A \sim S_B$  if  $A, B$  have the same cardinality. Permutations work with  $n$  rows of the  $n \times n$   $I_n$  which has determinant 1. Interchanging any two rows changes the sign of the determinant. If  $C$  is a matrix obtained by some permutation  $\sigma$  of  $I_n$  and  $C$  could be obtained by an even and odd number of transpositions of rows, then its determinant would be both 1 and -1.  $\square$

**Proof.** (Orbits) Let  $\sigma \in S_n$  and  $\tau = (i, j)$  be a transposition in  $S_n$ .

**Case I:** Suppose the orbits of  $\sigma$  and  $\tau\sigma$  differ by 1. Suppose  $i, j$  are in different orbits of  $\sigma$ . Writing  $\sigma$  as a product of disjoint cycles with the first containing  $j$  and the second containing  $i$ , e.g.  $(b, j, \times, \times, \times)(a, i, \times, \times)$  implies that  $\tau\sigma = (i, j)\sigma = (i, j)(b, j, \times, \times, \times)(a, i, \times, \times)$  after calculating is  $(a, j, \times, \times, \times, b, i, \times, \times)$ . This is because  $a$  feeds into  $i$  now  $j$  feeds into  $\times, \times, \times$  and  $b$  feeds into  $j$  now  $i$  into  $\times, \times$ . This is now a single orbit.

**Case II:** Suppose instead that  $i, j$  are in the same orbit of  $\sigma$  so  $\sigma$  can be written as the product of disjoint cycles so the first cycle is of form  $(a, i, \times, \times, \times, b, j, \times, \times)$ .  $\tau\sigma = (i, j)\sigma$  gives  $(a, j, \times, \times)(b, i, \times, \times, \times)$ . This single orbit has been split into two.

These cases show the number of orbits of  $\tau\sigma$  differs from the number of orbits of  $\sigma$  by 1. The identity permutation  $\iota$  has exactly  $n$  orbits because each element is the only member of its orbit. So the orbits of a permutation  $\sigma \in S_n$  must differ from  $n$  by an even or odd number. Each new transposition multiplied with the identity trying to create  $\sigma$  must then change that product's orbits by 1. So, there cannot be 2 sequences of different size because that would imply  $\sigma$  has different numbers of orbits.  $\square$

**Definition 38.** Even/Odd Permutation A permutation of a finite set is known as *even* or *odd* depending on whether it can be written the product of an even or odd number of transpositions.

**Example.** The identity permutation  $\iota \in S_n$  is even because it is  $(1, 2)(1, 2)$ .

**Theorem 16.** If  $n \geq 2$ , the collection of even permutations of  $\{1, 2, 3, \dots, n\}$  forms a subgroup of order  $n!/2$  of the symmetric group  $S_n$ . Note the set of odd permutations is of the same size.

**Proof.** Take the set of even and odd ( $A_n$  and  $B_n$ ) permutations in  $S_n$ . Let  $\tau$  be any fixed transposition in  $S_n$ . Because  $n \geq 2$ , we might as well suppose  $\tau = (1, 2)$ . Take the function  $\lambda_\tau: A_n \rightarrow B_n$  defined as  $\lambda_\tau(\sigma) = \tau\sigma$  for  $\sigma \in A_n$ .  $\sigma$  is even so  $(1, 2)\sigma$  can be expressed as an odd number of transpositions so  $\tau\sigma \in B_n$ . Because  $S_n$  is a group, for any  $\sigma, \mu \in A_n$ ,  $\lambda_\tau(\sigma) = \lambda_\tau(\mu)$  implies  $\sigma = \mu$  so  $\lambda_\tau$  is injective. Note also that  $\tau = \tau^{-1}$  so

if  $\rho \in B_n$ , then  $\tau^{-1}\rho \in A_n$  and  $\lambda_\tau(\tau^{-1}(\rho)) = \tau(\tau^{-1}(\rho)) = \rho$  implying  $\lambda_\tau$  is onto  $B_n$ . So  $B_n$  and  $A_n$  are of the same size because they are finite. The fact the set of even permutations is a subgroup is trivial.  $\square$

**Definition 39 (Alternating Group  $A_n$  on  $n$  Letters).** The subgroup  $S_n$  consisting of the even permutations of  $n$  letters is the *alternating group  $A_n$  on  $n$  letters*.

## 2.3 Cosets and the Theorem of Lagrange

**Theorem 17.** Let  $H$  be a subgroup of  $G$ . Let the relation  $\sim_L$  be defined on  $G$  by

$$a \sim_L b \text{ if and only if } a^{-1}b \in H.$$

Let  $\sim_R$  be defined on  $G$  by

$$a \sim_R b \text{ if and only if } ab^{-1} \in H.$$

Then  $\sim_L, \sim_R$  are both equivalence relations on  $G$ .

**Proof.** (Just  $\sim_L$ ) For any  $a \in G$ ,  $a^{-1}(a) = e \in H$  so  $\sim_L$  is reflexive. For any  $a, b \in G$ , suppose  $a^{-1}b \in H$ . Because this is a subgroup,  $(a^{-1}b)^{-1} \in H$  so that  $b^{-1}a \in H$  and thus  $b \sim_L a$  so  $\sim_L$  is symmetric. Lastly, if  $a \sim_L b, b \sim_L c$  for some  $a, b, c \in G$ , then  $a^{-1}b, b^{-1}c \in H$ . By closure  $a^{-1}bb^{-1}c = a^{-1}c \in H$  so  $a \sim_L c$  implying  $\sim_L$  is transitive. Thus,  $\sim_L$  is an equivalence relation.  $\square$

**Definition 40 (Left/Right Cosets).** Let  $H$  be a subgroup of group  $G$ . The subset  $aH = \{ah \mid h \in H\}$  of  $G$  is the *left coset* of  $H$  containing  $a$  while the subset  $Ha = \{ha \mid h \in H\}$  is the *right coset* of  $H$  containing  $a$ .

**Example.** Take the subgroup  $3\mathbb{Z}$  of  $\mathbb{Z}$ . Using additive notation, the left coset of  $3\mathbb{Z}$  containing  $m$  is  $m + 3\mathbb{Z}$ . When  $m = 0$ ,  $3\mathbb{Z} = \{\dots, -3, 0, 3, \dots\}$  so  $3\mathbb{Z}$  is itself such a left coset. Similarly,  $1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}$  are left cosets. Together, these partition  $\mathbb{Z}$ . Because  $\mathbb{Z}$  is abelian, left coset  $m + 3\mathbb{Z}$  is the same as right coset  $3\mathbb{Z} + m$ .

**Lemma 2.** Take the one-one map  $\phi: H \rightarrow gH$  so  $\phi(h) = gh$  for each  $h \in H$ . This is onto  $gH$  by definition. Next, suppose  $\phi(h_1) = \phi(h_2)$  for some  $h_1, h_2 \in H$ . Thus,  $gh_1 = gh_2$  so by cancellation in  $G$ ,  $h_1 = h_2$  implying  $\phi$  is bijective. If  $H$  is of finite order, then  $\phi$  and a similar function for right cosets have equal numbers of elements to  $H$ .

**Theorem 18 (Theorem of Lagrange).** Let  $H$  be a subgroup of a finite group  $G$ . Then the order of  $H$  is a divisor of the order of  $G$ .

**Proof.** Let  $n$  be the order of  $G$  and  $H$  have order  $m$ . Every coset (left or right) of a subgroup  $H$  of a group  $G$  has the same number of elements as  $H$ , namely  $m$ . Let  $G$  be partitioned into  $r$  left cosets of  $H$  so  $n = rm$  implying  $m$  is a divisor of  $n$ .  $\square$

**Corollary.** Every group of prime order is cyclic.

**Proof.** Let  $G$  be of prime order  $P$  and  $a \in G, a \neq e$ . Thus,  $\langle a \rangle$  of  $G$  has at least 2 elements. But by Lagrange's Theorem, the order  $m \geq 2$  of  $a$  must divide the prime  $p$  implying  $m = p$  so  $\langle a \rangle = G$  so  $G$  is cyclic.  $\square$

**Definition 41.** Let  $H$  be a subgroup of a group  $G$ . The number of left cosets of  $H$  in  $G$  is the *index*  $(G : H)$  of  $H$  in  $G$ . The index may be infinite or finite.

**Theorem 19.** Suppose  $H$  and  $K$  are subgroups of a group  $G$  so  $K \leq H \leq G$  and suppose  $(H : K)$  and  $(G : H)$  are both finite. Then  $(G : K) = (G : H)(H : K)$  is finite.

## 2.4 Finitely Generated Abelian Groups

**Theorem 20 (Direct Product of Groups).** Let  $G_1, G_2, \dots, G_n$  be groups. For  $(a_1, a_2, \dots, a_n)$  and  $(b_1, b_2, \dots, b_n)$  in  $\prod_{i=1}^n G_i$ . Define  $(a_1, a_2, \dots, a_n)$  times  $(b_1, b_2, \dots, b_n)$  as the element  $(a_1 b_1, a_2 b_2, \dots, a_n b_n)$ . This is the *direct product of the groups*  $G_i$  under this binary operation.

**Proof.** Closure is trivial. Take the element  $(e_1, e_2, \dots, e_n)$  as the identity. And for any  $(a_1, a_2, \dots, a_n)$ , its inverse is  $(a_1^{-1}, a_2^{-1}, \dots, a_n^{-1})$ . Thus,  $\prod_{i=1}^n G_i$  is a group.  $\square$

**Remark (Direct Sum of Groups).** In the case the binary operation of each  $G_i$  is commutative, we replace  $\prod_{i=1}^n G_i$  with the *direct sum of the groups*  $G_i$ , denoted  $\oplus_{i=1}^n G_i$ . We may also write it  $G_1 \oplus G_2 \oplus \dots \oplus G_n$ .

**Example.** The group  $\mathbb{Z}_2 \times \mathbb{Z}_3$  obviously is of order 6. However, via the generator  $(1,1)$ , we can show it is cyclic as:

- $1(1,1) = (1,1)$
- $2(1,1) = (0,2)$
- $3(1,1) = (1,0)$
- $4(1,1) = (0,1)$
- $5(1,1) = (1,2)$
- $6(1,1) = (0,0)$

Because there is only one cyclic group structure of a given order, we see  $\mathbb{Z}_2 \times \mathbb{Z}_3$  is isomorphic to  $\mathbb{Z}_6$ .

In contrast, however,  $\mathbb{Z}_3 \times \mathbb{Z}_3$  is a group of 9 elements but every 3 opera-

tionsd generates the identity and thus it is not cyclic. The same goes for  $\mathbb{Z}_2 \times \mathbb{Z}_2$  which must be isomorphic, then, to the Klein 4-group.

**Theorem 21.** The group  $\mathbb{Z}_m \times \mathbb{Z}_n$  is cyclic and isomorphic to  $\mathbb{Z}_{mn}$  if and only if  $m, n$  are relatively prime.

**Proof.**  $\Rightarrow$ : Consider the cyclic subgroup of  $\mathbb{Z}_m \times \mathbb{Z}_n$  generated by  $(1,1)$ . Clearly, the smallest number that is a multiple of both  $m$  and  $n$  will be  $mn$  if and only if  $\gcd(m, n) = 1$ . It is at this number of summands that  $(1,1)$  yields the identity and implies  $mn$  is the order of  $\mathbb{Z}_m \times \mathbb{Z}_n$  and  $\mathbb{Z}_{mn}$ . Because  $\langle(1, 1)\rangle$  is cyclic, they are isomorphic.

$\Leftarrow$ : Suppose  $\gcd(m, n) = d > 1$ . Then,  $mn/d$  is divisible by both  $m$  and  $n$  so for any  $(r, s) \in \mathbb{Z}_m \times \mathbb{Z}_n$ ,  $\square$

**Corollary.** The group  $\prod_{i=1}^n \mathbb{Z}_{m_i}$  is cyclic and isomorphic to  $\mathbb{Z}_{m_1 m_2 \dots m_n}$  if and only if any two of the numbers  $m_i$  for  $i = 1, \dots, n$  are coprime.

**Example.** Thus, if  $n = (p_1)^{n_1} (p_2)^{n_2} \dots (p_r)^{n_r}$  for distinct primes, then  $\mathbb{Z}_n$  is isomorphic to  $\mathbb{Z}_{(p_1)^{n_1}} \times \mathbb{Z}_{(p_2)^{n_2}} \times \dots \times \mathbb{Z}_{(p_r)^{n_r}}$ . In particular,  $\mathbb{Z}_72$  is isomorphic to  $\mathbb{Z}_8 \times \mathbb{Z}_9$ .

**Example.** The order of  $(8,4,10)$  in  $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$  is the least common multiple of  $(\frac{12}{\gcd(8,12)}, \frac{60}{\gcd(4,60)}, \frac{24}{\gcd(10,24)}) = 3 \cdot 5 \cdot 4 = 60$ .

**Theorem 22.** Let  $(a_1, a_2, \dots, a_n) \in \prod_{i=1}^n G_i$ . If  $a_i$  is of finite order  $r_i$  in  $G_i$ , then the order of  $(a_1, a_2, \dots, a_n)$  in  $\prod_{i=1}^n G_i$  is equal to the least common multiple of all the  $r_i$ .

**Proof.** Only for the power  $\text{lcm}(r_1, r_2, \dots, r_n)$  does  $(a_1, a_2, \dots, a_n)$  give the identity  $(e_1, e_2, \dots, e_n)$ .  $\square$

**Theorem 23 (Fundamental Theorem of Finitely Generated Abelian Groups).** Every finitely generated abelian group  $G$  is isomorphic to a direct product of cyclic groups in form

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \dots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z}$$

where  $p_i$  are primes, not necessarily distinct, and  $r_i \in \mathbb{Z}^+$ . The direct product is unique except for possible rearrangement. In other words, the *Betti number* of  $G$  of factors  $\mathbb{Z}$  is unique and the prime power  $(p_i)^{r_i}$  are unique.

We call the left part the *torsion part* and *free part*.

**Example.** We can decompose every group of order  $360 = 2^3 3^2 5$  through separating groups into groups of coprime orders. Then,  $\mathbb{Z}_4 \mathbb{Z}_6 \mathbb{Z}_{15}$  is equivalent to  $\mathbb{Z}_4 \mathbb{Z}_2 \mathbb{Z}_3 \mathbb{Z}_3 \mathbb{Z}_5 = \mathbb{Z}_3 \mathbb{Z}_{12} \mathbb{Z}_{10}$ .

**Definition 42 (Decomposable).** A group  $G$  is *decomposable* if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise  $G$  is *indecomposable*.

**Theorem 24.** The finite indecomposable abelian groups are exactly the cyclic groups with order a power of a prime.

**Proof.**  $\Rightarrow$ : Let  $G$  be a finite indecomposable abelian group. Thus,  $G$  is isomorphic to a direct product of cyclic groups of a prime power. Since  $G$  is indecomposable, this direct product must consist of just one cyclic group whose order is a power of a prime number.

$\Leftarrow$ : Let  $p$  be a prime number so  $\mathbb{Z}_{p^r}$  is indecomposable such that if  $\mathbb{Z}_{p^r}$  were isomorphic to  $\mathbb{Z}_{p^i} \times \mathbb{Z}_{p^j}$  where  $i + j = r$ , then every element would have an order at most  $p^{\max(i,j)} < p^r$ .  $\square$

**Theorem 25.** If  $m$  divides the order of a finite abelian group  $G$ , then  $G$  has a subgroup of order  $m$ .

**Proof.**  $G$  finite so it can be written as  $\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}}$  where not all primes  $p_i$  need be distinct. This implies  $(p_1)^{r_1} (p_2)^{r_2} \cdots (p_n)^{r_n}$  is the order of  $G$ . So  $m = (p_1)^{s_1} (p_2)^{s_2} \cdots (p_n)^{s_n}$  where  $0 \leq s_i \leq r_i$ . This implies  $(p_i)^{r_i - s_i}$  generates a cyclic subgroup of  $\mathbb{Z}_{(p_i)^{r_i}}$  of order  $(p_i)^{s_i}$ . This implies that  $\langle (p_1)^{r_1 - s_1} \rangle \times \langle (p_2)^{r_2 - s_2} \rangle \times \cdots \times \langle (p_n)^{r_n - s_n} \rangle$  is the required subgroup of order  $m$ .  $\square$

**Theorem 26.** If  $m$  is a square free integer, that is,  $m$  is not divisible by the square of any prime, then every abelian group of order  $m$  is cyclic.

**Proof.** Let  $G$  be an abelian group of square free order  $m$  so  $G$  finite and isomorphic to  $\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}}$  where  $m = (p_1)^{r_1} (p_2)^{r_2} \cdots (p_n)^{r_n}$ . Because  $m$  is square free, all  $r_i = 1$  and all  $p_i$  distinct primes implying  $G$  isomorphic to  $\mathbb{Z}_{p_1 p_2 \cdots p_n}$  so  $G$  cyclic.  $\square$

## Chapter 3

# Homomorphisms and Factor Groups

### 3.1 Homomorphisms

**Definition 43 (Homomorphism).** A map  $\phi$  of a group  $G$  into a group  $G'$  is a *homomorphism* if the homomorphism property that  $\phi(ab) = \phi(a)\phi(b)$  for all  $a, b \in G$  holds.

**Remark (Trivial Homomorphism).** There is at least always the homomorphism  $\phi: G \rightarrow G'$  defined as  $\phi(g) = e'$  for all  $g \in G$  is called the *trivial homomorphism*.

**Example.** Let  $S_n$  be the symmetric group on  $n$  letters and let  $\phi: S_n \rightarrow \mathbb{Z}_n$  be defined by:

$$\phi(\sigma) = \begin{cases} 0 & \sigma \text{ even permutation} \\ 1 & \sigma \text{ odd permutation.} \end{cases}$$

Clearly,  $\sigma$  is a homomorphism.

**Example (Evaluation Homomorphism).** Let  $F$  be the additive group of all functions mapping  $R$  into  $R$  and  $R$  be the additive group of all reals and  $c \in \mathbb{R}$ . Then,  $\phi_c: F \rightarrow \mathbb{R}$  is the *evaluation homomorphism* defined as  $\phi_c(f) = f(c)$  for  $f \in F$ .

**Example.** The *projection map*  $\pi_i: G \rightarrow G_i$  where  $G = G_1 \times G_2 \times \cdots \times G_i \times \cdots \times G_n$  and  $\pi_i(g_1, g_2, \cdots, g_i, \cdots, g_n) = g_i$  for each  $i = 1, 2, \cdots, n$ .

**Definition 44 (Image, Range, Preimage).** Let  $\phi$  be a mapping on a set  $X$  into a set  $Y$  and  $A \subseteq X, B \subseteq Y$ . The *image*  $\phi[A]$  of  $A$  in  $Y$  under  $\phi$  is

$\{\phi(a) \mid a \in A\}$ .

The set  $\phi[X]$  is the *range* of  $\phi$ .

The *inverse image*  $\phi^{-1}[B]$  of  $B$  in  $X$  is  $\{x \in X \mid \phi(x) \in B\}$ .

**Theorem 27.** Let  $\phi$  be a homomorphism of a group  $G$  into a group  $G'$ . Then,

1. If  $e$  is the identity element in  $G$ ,  $\phi(e)$  is the identity element  $e' \in G'$ .
2. If  $a \in G$ , then  $\phi(a^{-1}) = \phi(a)^{-1}$ .
3. If  $H$  is a subgroup of  $G$ , then  $\phi[H]$  is a subgroup of  $G'$ .
4. If  $K'$  is a subgroup of  $G'$ , then  $\phi^{-1}[K']$  is a subgroup of  $G$ .

**Definition 45 (Kernel).** Let  $\phi: G \rightarrow G'$  be a homomorphism of groups. The subgroup  $\phi^{-1}[\{e'\}] = \{x \in G \mid \phi(x) = e'\}$  is the *kernel* of  $\phi$ , denoted by  $\ker(\phi)$ .

**Theorem 28.** Let  $\phi: G \rightarrow G'$  be a group homomorphism and  $H = \ker(\phi)$ . For  $a \in G$ , the set

$$\phi^{-1}[\{\phi(a)\}] = \{x \in G \mid \phi(x) = \phi(a)\}$$

is the left coset  $aH$  and right coset  $aH$  of  $H$ . Thus, the partitions of  $G$  into left cosets and right cosets are the same.

**Proof.** We want to show  $\{x \in G \mid \phi(x) = \phi(a)\} = aH$ , i.e. they are subsets of one another.

$\subseteq$ : If  $\phi(x) = \phi(a)$ , then  $e' = \phi(a)^{-1}\phi(x) = \phi(a^{-1})\phi(x) = \phi(a^{-1}x)$  so  $a^{-1}x \in H = \ker(\phi)$ . Thus,  $a^{-1}x = h$  for some  $h \in H$  so  $x = ah \in aH$  so  $\{x \in G \mid \phi(x) = \phi(a)\} = aH$ .

$\supseteq$ : Say  $y \in aH$  so  $y = ah$  for some  $h \in H$ . Thus,  $\phi(y) = \phi(ah) = \phi(a)\phi(h) = \phi(a)e' = \phi(a)$  so  $y \in \{x \in G \mid \phi(x) = \phi(a)\}$ .  $\square$

**Corollary.** A group homomorphism  $\phi: G \rightarrow G'$  is injective  $\Leftrightarrow \ker(\phi) = \{e\}$ .

**Proof.**  $\Rightarrow$ : If  $\ker(\phi) = \{e\}$ , then the elements mapped to  $\phi(a)$  are exactly the elements of the left coset  $a\{e\} = \{e\}$  showing that  $\phi$  is injective.  $\Leftarrow$ : If  $\phi$  is injective, then simply  $e$  can be the only element mapped to  $e'$ .  $\square$

**Note (Show  $\phi: G \rightarrow G'$  Is an Isomorphism).**

(Step 1) Show  $\phi$  homomorphism.

(Step 2) Show  $\ker(\phi) = \{e\}$ .



(Step 3) Show  $\phi$  is surjective.

**Definition 46 (Normal Subgroup).** A subgroup  $H$  of a group  $G$  is normal if its left and right cosets coincide, that is, if  $gH = Hg$  for all  $g \in G$ . Normal subgroups are denoted as  $H \triangleleft G$ .

**Note.** All subgroups of abelian groups are normal.

**Corollary.** If  $\phi: G \rightarrow G'$  is a group homomorphism, then  $\ker(\phi)$  is a normal subgroup of  $G$ .

## 3.2 Factor Groups

**Theorem 29.** Let  $\phi: G \rightarrow G'$  be a group homomorphism with kernel  $H$ . Then the cosets of  $H$  form a *factor group*  $G/H$  where  $(aH)(bH) = (ab)H$ . Also, the map  $\mu: G/H \rightarrow \phi[G]$  defined by  $\mu(aH) = \phi(a)$  is an isomorphism.

A factor group  $G/H$  is also called the *factor group of  $G$  modulo  $H$*  and elements in the same coset are said to be *congruent modulo  $H$* .

**Example.** The isomorphism  $\mu: \mathbb{Z}/5\mathbb{Z} \rightarrow \mathbb{Z}_5$  assigns to each coset of  $5\mathbb{Z}$  its smallest nonnegative element, i.e.  $\mu(5\mathbb{Z}) = 0, \mu(1 + 5\mathbb{Z}) = 1$ , etc.

**Theorem 30.** Let  $H$  be a subgroup of a group  $G$ . Then left coset multiplication is well defined by  $(aH)(bH) = (ab)H$  if and only if  $H$  is a normal subgroup of  $G$ .

**Proof.**  $\Rightarrow$ : Suppose  $(aH)(bH) = (ab)H$  is a well-defined operation on left cosets. Then, we want to show  $aH$  and  $Ha$  are the same set. Let  $x \in aH$ . Picking representatives  $x \in aH$  and  $a^{-1} \in a^{-1}H$ , we get  $(xH)(a^{-1}H) = (xa^{-1})H$ . This must be equal to  $(aH)(a^{-1}H) = (eH) = H$  so  $xa^{-1} = h \in H$ . Thus,  $x = ha \Rightarrow x \in Ha$  so  $aH \subseteq Ha$ . The symmetric proof is also true so  $aH = Ha$ .

$\Leftarrow$ : Suppose  $H$  is a normal subgroup of  $G$ . Take  $a, ah_1 \in aH, b, bh_2 \in bH$  so  $h_1b \in Hb = bH$  so  $h_1b = bh_3$  for some  $h_1, h_2, h_3 \in H$ . Thus,

$$(ah_1)(bh_2) = a(h_1b)(h_2) = a(bh_3)h_2 = (ab)(h_3h_2) \in (ab)H.$$

Going the other direction, if  $x \in (ab)H \Rightarrow x = abh = (ae)(bh) \in (aH)(bH)$ .  $\square$

**Definition 47 (Factor/Quotient Group).** Let  $H \triangleleft G$ . Then the cosets of  $H$  form a group  $G/H$  under the binary operation  $(aH)(bH) = (ab)H$ . This group is called the *factor, or quotient, group of  $G$  by  $H$* .

**Example.** Because  $\mathbb{Z}$  is an abelian group,  $n\mathbb{Z}$  is a normal subgroup so  $\mathbb{Z}/n\mathbb{Z}$  is isomorphic to  $\mathbb{Z}_n$ .

**Theorem 31.** Let  $H \triangleleft G$ . Then  $\gamma: G \rightarrow G/H$  given by  $\gamma(x) = xH$  is a homomorphism with kernel  $H$ .

**Proof.** Let  $x, y \in G$ . Clearly,  $\gamma(a)\gamma(b) = (aH)(bH) = (ab)H = \gamma(ab)$  so it is a homomorphism. Plus, if  $\gamma(x) \in eH$ , then  $xH = eH$  so clearly  $x \in H$ . Thus,  $\ker(\gamma) = H$ .  $\square$

**Theorem 32 (The Fundamental Homomorphism Theorem).** Let  $\phi: G \rightarrow G'$  be a group homomorphism with kernel  $H$ . Then  $\phi[G]$  is a group and  $\mu: G/H \rightarrow \phi[G]$  given by  $\mu(gH) = \phi(g)$  is an isomorphism. If  $\gamma: G \rightarrow G/H$  is the homomorphism given by  $\gamma(g) = gH$ , then  $\phi(g) = \mu\gamma(g)$  for each  $g \in G$ .  $\mu$  is the *natural, or canonical isomorphism*.

**Theorem 33.** The following are 3 equivalent conditions for a subgroup  $H$  of a group  $G$  to be a normal subgroup of  $G$ :

1.  $ghg^{-1} \in H$  for all  $g \in G, h \in H$ .
2.  $gHg^{-1} = H$  for all  $g \in G$
3.  $gH = Hg$  for all  $g \in G$ .

**Definition 48 ((Inner) Automorphism).** An isomorphism  $\phi: G \rightarrow G$  of a group  $G$  with itself is a *automorphism of  $G$* . The automorphism  $i_g: G \rightarrow G$  where  $i_g(x) = gxg^{-1}$  for all  $x \in G$  is the *inner automorphism of  $G$  by  $g$* .

**Definition 49 (Conjugate Subgroup).** Performing  $i_g$  on  $x$  is called the *conjugation of  $x$  by  $g$* . A subgroup  $K$  of  $G$  is a *conjugate subgroup of  $H$*  if  $K = i_g[H]$  for some  $g \in G$ .

### 3.3 Simple Groups

**Remark.** For a normal subgroup  $N$  of  $G$ , the factor group  $G/N$  collapses  $N$  to a single element, namely the identity.

**Example.** The trivial subgroup  $N = \{0\}$  of  $\mathbb{Z}$  is obviously normal and has factor group isomorphic to  $\mathbb{Z}$ .

**Example.** We can show the falsity of the converse of Lagrange's Theorem. That is,  $A_4$  has order 12 yet has no subgroup of order 6.

Suppose  $H < A_4$  and  $H$  was of order 6. It would follow that  $H$  is a normal subgroup of  $A_4$  so  $A_4/H$  would only have 2 elements,  $H$  and  $\sigma H$  for some  $\sigma \in A_4/H$ . Because it's a group of order 2, the square of this element but be the identity so  $(\sigma H)(\sigma H) = H$ . Thus, the square of every element in  $A_4$  must be in  $H$ . However, this is 8 elements so  $H$  cannot have order 6.

**Theorem 34.** Let  $G = H \times K$  be the direct product of groups  $H$  and  $K$ . Then  $\bar{H} = \{(h, e) \mid h \in H\} \triangleleft G$ . Also,  $G/\bar{H} \simeq K$  and  $G/\bar{K} \simeq H$  in natural ways.

**Proof.** Take the homomorphism  $\pi_2: H \times K \rightarrow K$  where  $\pi_2(h, k) = k$ . Because  $\ker(\pi_2) = \bar{H}$ ,  $\bar{H} \triangleleft H \times K$ . Because  $\pi_2$  is onto  $K$ ,  $(H \times K)/\bar{H} \simeq K$ .  $\square$

**Theorem 35.** A factor group of a cyclic group is cyclic.

**Proof.** Let  $G$  be a cyclic group generated by  $a$  with normal subgroup  $N$ . To compute all powers of  $aN$  means computing all powers of the representative  $a$  which gives all elements in  $G$  such that  $aN$  gives all cosets of  $N$  such that  $G/N$  is cyclic.  $\square$

**Example.** To find the factor group of  $\mathbb{Z}_4 \times \mathbb{Z}_6 / \langle (2, 3) \rangle$ , note that  $\langle (2, 3) \rangle$  has order 2 and  $\mathbb{Z}_4 \times \mathbb{Z}_3$  has order 24 implying the factor group has order 12 which is either of form, up to isomorphism,  $\mathbb{Z}_4 \times \mathbb{Z}_3$  or  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ . However, note that  $(1, 0) + \langle (2, 3) \rangle$  is of order 4 in the factor group  $(\mathbb{Z}_4 \times \mathbb{Z}_6) / \langle (2, 3) \rangle$  so the group must be isomorphic to  $\mathbb{Z}_4 \times \mathbb{Z}_3$  or equivalently  $\mathbb{Z}_{12}$ .

**Definition 50 (Simple Groups).** A group is *simple* if it is nontrivial and has no proper nontrivial normal subgroups.

**Remark.** The alternating group  $A_n$  is simple for  $n \geq 5$ .

**Theorem 36.** Let  $\phi: G \rightarrow G'$  be a group homomorphism. If  $N \triangleleft G$ , then  $\phi[N] \triangleleft \phi[G]$ . Also, if  $N'$  is a normal subgroup of  $\phi[G]$ , then  $\phi^{-1}[N'] \triangleleft G$ . Note that  $\phi[N]$  may not be normal in  $G'$ .

**Definition 51 (Maximal Normal Subgroup of a Group  $G$ ).** A *maximal normal subgroup* of a group  $G$  is a normal subgroup  $M$  not equal to  $G$  such that there is no proper normal subgroup  $N$  of  $G$  properly containing  $M$ .

**Theorem 37.**  $M$  is a *maximal normal subgroup* of  $G$  if and only if  $G/M$  is simple.

**Proof.**  $\Rightarrow$ : Let  $M$  be a maximal normal subgroup of  $G$ . Take the canonical homomorphism  $\gamma: G \rightarrow G/M$ . Now,  $\gamma^{-1}$  of any nontrivial proper normal subgroup of  $G/M$  is a proper normal subgroup of  $G$  properly containing  $M$ . But  $M$  is maximal so this isn't possible. So  $G/M$  is simple.

$\Leftarrow$ : If  $N$  is a normal subgroup of  $G$  properly containing  $M$ , then  $\gamma[N]$  is normal in  $G/M$ . If  $N \neq G$ , then  $\gamma[N] \neq G/M$  and  $\gamma[N] \neq \{M\}$ . If  $G/M$  is simple, no such  $\gamma[N]$  and thus no such  $N$  can exist so  $M$  is maximal.  $\square$

**Definition 52 (Center of  $G$ ).** Every nonabelian group has a *center*  $Z(G)$  such that

$$Z(G) = \{z \in G \mid zg = gz \forall g \in G\}.$$

The center always contains the identity, but if it only contains this then it is trivial.

**Definition 53 (Commutator).** To abelianize  $G$ , we will find all elements such that  $ab = ba$ , or that  $aba^{-1}b^{-1} = e$ . This element is a *commutator of the group*.

**Theorem 38.** Let  $G$  be a group. The set of all commutators  $aba^{-1}b^{-1}$  for  $a, b \in G$  generates the *commutator subgroup*  $C$  of  $G$ . This is a normal subgroup of  $G$ . Furthermore, if  $N$  is a normal subgroup of  $G$ , then  $G/N$  is abelian if and only if  $C \leq N$ .

**Proof.** The commutators surely generate a subgroup  $C$  from  $e$ , inverses, and closure. Now, for any  $x \in C$ , and any  $g \in G$ ,  $x = cdc^{-1}d^{-1}$  for some  $c, d \in G$  such that  $g^{-1}xg = (g^{-1}cdc^{-1})(e)(d^{-1}g)$ . This becomes  $(g^{-1}cdc^{-1})(gd^{-1}g^{-1})(d^{-1}g) = [(g^{-1}c)d(g^{-1}c)^{-1}d^{-1}][dg^{-1}d^{-1}g] \in C$  so  $C \triangleleft G$ .

Next, if  $N \triangleleft G$ , then  $\Rightarrow$ : If  $G/N$  abelian,  $(a^{-1}N)(b^{-1}N) = (b^{-1}N)(a^{-1}N)$  so  $aba^{-1}b^{-1}N = N$  so  $aba^{-1}b^{-1} \in N \Rightarrow C \leq N$ .

$\Leftarrow$ : If  $C \leq N$ , then  $(aN)(bN) = abN = ab(b^{-1}a^{-1}ba)N = baN = (bN)(aN)$ .  $\square$

### 3.4 Group Action on a Set

**Definition 54 (Group Action).** Let  $X$  be a set and  $G$  a group. An *action of  $G$  on  $X$*  is a map  $*$ :  $G \times X \rightarrow X$  such that:

1.  $ex = x$  for all  $x \in X$
2.  $(g_1g_2)(x) = g_1(g_2x)$  for all  $x \in X$  and all  $g_1, g_2 \in G$ .

In this case, we call  $X$  a  *$G$ -set*.

**Theorem 39.** Let  $X$  be a  $G$ -set. For each  $g \in G$ , the function  $\sigma_g: X \rightarrow X$  defined by  $\sigma_g(x) = gx$  for  $x \in X$  is a permutation of  $X$ . Also, the map  $\phi: G \rightarrow S_X$  defined by  $\phi(g) = \sigma_g$  is a homomorphism with the property that  $\phi(g)(x) = gx$ .

**Proof.** To show  $\sigma_g$  is a permutation of  $X$ , we must show it is bijective. (i) If  $\sigma_g(x_1) = \sigma_g(x_2)$ , then  $gx_1 = gx_2$  so  $g^{-1}(gx_1) = g^{-1}(gx_2)$  so  $(g^{-1}g)(x_1) = (g^{-1}g)(x_2)$  from the second condition of group actions so  $e(x_1) = e(x_2)$  so  $x_1 = x_2$  from the first condition. Next, for any  $x \in X$ ,  $\sigma_g(g^{-1}x) = g(g^{-1}x) = (gg^{-1})x = ex = x$  so  $\sigma_g$  is onto and 1-1 making it a permutation.

Next,  $\phi: G \rightarrow S_X$  defined by  $\phi(g) = \sigma_g$  is a homomorphism because  $\sigma(g_1g_2)(x) = (g_1g_2)x = g_1(g_2x) = g_1\sigma_{g_2}(x) = \sigma_{g_1}(\sigma_{g_2}(x)) = (\sigma_{g_1} \circ \sigma_{g_2})(x) = (\sigma_{g_1g_2})(x) = (\phi(g_1)\phi(g_2))(x)$ .  $\square$

**Definition 55 (Acting Faithfully, Transitive).** Note that the subset of  $G$  leaving each element of  $X$  fixed is a normal subgroup  $N$  of  $G$ . We say  $G$  *acts faithfully* on  $X$  if  $N = \{e\}$ .

We say  $G$  is *transitive* on a  $G$ -set  $X$  if and only if the subgroup  $\phi[G]$  of  $S_X$  is transitive on  $X$ , that is, if for each  $x_1, x_2 \in X$ , there exists some  $g \in G$  so that  $gx_1 = x_2$ .

**Remark.** Every group is itself a  $G$ -set.

**Theorem 40.** Let  $X$  be a  $G$ -set. Then  $G_x$  is a subgroup of  $G$  for each  $x \in X$ .

**Note.** As notation, for  $G$ -set  $X$  with  $x \in X, g \in G$ , we say

$$X_g = \{x \in X \mid gx = x\} \quad \text{and} \quad G_x = \{g \in G \mid gx = x\}.$$

**Proof.** Let  $x \in X, g_1, g_2 \in G_x$ . So  $g_1x = g_2x = x$  so  $g_1x = x = g_2x$ . Thus,  $(g_1g_2)x = g_1(g_2x) = g_1x = x$  so  $g_1, g_2 \in G_x$  and  $G_x$  closed under the induced operation of  $G$ . Clearly,  $e \in G_x$ . And  $g \in G_x$  implies  $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x$  so  $g^{-1} \in G_x$ . Thus  $G_x \leq G$ .  $\square$

**Definition 56 (Isotropy Subgroup).** Let  $X$  be a  $G$ -set and  $x \in X$ . The subgroup  $G_x$  is the *isotropy subgroup* of  $x$ .

**Theorem 41.** Let  $X$  be a  $G$ -set. For  $x_1, x_2 \in X$ , say  $x_1 \sim x_2$  if and only if there exists  $g \in G$  so  $gx_1 = x_2$ .  $\sim$  is an equivalence relation on  $X$ .

**Proof.** (i) For any  $x \in X$ ,  $ex = x$  so  $x \sim x$ . (ii) For any  $x_1, x_2 \in X$ , if  $x_1 \sim x_2$ , then  $gx_1 = x_2$  so  $g^{-1}x_2 = g^{-1}(gx_1) = (g^{-1}g)(x_1) = ex_1 = x_1$  so  $x_2 \sim x_1$ . (iii) Last, if  $x_1 \sim x_2, x_2 \sim x_3$ , then  $g_1x_1 = x_2, g_2x_2 = x_3$  for

some  $g_1, g_2 \in G$  so  $(g_2 g_1)(x_1) = g_2(g_1 x_1) = g_2(x_2) = x_3$  so  $x_1 \sim x_3$ .  $\square$

**Definition 57 (Orbit of  $x$ ).** Let  $X$  be a  $G$ -set. Each cell in the partition of the equivalence relation is described as a *orbit in  $X$  under  $G$* . For  $x \in X$ , the cell containing  $x$  is the *orbit of  $x$* . This is  $Gx$ .

**Theorem 42.** Let  $X$  be a  $G$ -set,  $x \in X$ . Then  $|Gx| = (G : G_x)$ . If  $|G|$  is finite, then  $|Gx|$  is a divisor of  $|G|$ .

**Proof.** Let's define the 1-1 map  $\psi$  from  $G_X$  onto the collection of left cosets of  $G_x$  in  $G$ . Let  $x_1 \in Gx$ . Then, there exists  $g_1 \in G$  so  $g_1 x = x_1$ . Say  $\psi(x_1)$  is the left coset  $g_1 G_x$  of  $G_x$ . To show this is well defined, if  $g'_1 x = x_1$ , then  $g_1 x = g'_1 x$  so  $g_1^{-1}(g_1 x) = g_1^{-1}(g'_1 x)$  implying  $x = g(g_1^{-1} g'_1)x$  so  $g_1^{-1} g'_1 \in G_x$  so  $g'_1 \in g_1 G_x$  and  $g_1 G_x = g'_1 G_x$ .

To show  $\psi$  is one-one,  $x_1, x_2 \in Gx$  gives  $\psi(x_1) = \psi(x_2)$  so there exists  $g_1, g_2 \in G$  so  $x_1 = g_1 x, x_2 = g_2 x$  where  $g_2 \in g_1 Gx$  giving  $g_2 = g_1 g$  for some  $g \in G_x$ . Thus,  $x_2 = g_2 x = g_1(gx) = g_1 x = x_1$ .

To show it's onto, for any left coset of  $G_x$   $g_1 G_x$  in  $G$ , if  $g_1 x = x_1$  then  $g_1 G_x = \psi(x_1)$ . This map is bijective so  $|Gx| = (G : G_x)$ . If  $|G|$  finite, then clearly,  $|Gx|$  divides  $|G|$ .  $\square$

## Chapter 4

# Rings and Fields

### 4.1 Rings and Fields

**Definition 58 (Ring).** A *ring*  $\langle R, +, \cdot \rangle$  is a set  $R$  together with two binary operations  $+$  and  $\cdot$  which we call *addition* and *multiplication* defined on  $R$  such that the following are satisfied:

( $\mathcal{R}_1$ )  $\langle R, + \rangle$  is an abelian group.

( $\mathcal{R}_2$ ) Multiplication is associative.

( $\mathcal{R}_3$ ) For all  $a, b, c \in R$ , the *left and right distributive laws*  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$  and  $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$  hold.

**Example.**  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  are all rings with addition and multiplication. In fact, these axioms hold for any subset of the complex numbers that is a group under addition and closed under multiplication.

**Example.** For any ring  $R$ , the collection of all  $n \times n$  matrices having elements of  $R$  as entries,  $M_n(R)$ , is an abelian additive group. Note, in particular, that (matrix) multiplication is not commutative for these.

**Theorem 43.** If  $R$  is a ring with additive identity  $0$ , then for any  $a, b \in R$ , we have:

1.  $0a = a0 = 0$ .
2.  $a(-b) = (-a)b = -(ab)$ .
3.  $(-a)(-b) = ab$ .

**Proof.** (i)  $a0 + a0 = a(0 + 0) = a0 = 0 + a0$  so  $a0 = 0$ . (ii)  $a(-b) + ab = a(0) = 0$  so  $a(-b) = -(ab)$ . The same goes for  $(-a)b$ . (iii)  $-(-a(-b)) = -(-(ab))$  so  $(-a)(-b) = ab$ .  $\square$

**Definition 59 (Ring Homomorphism).** For rings  $R$  and  $R'$ , a map  $\phi: R \rightarrow R'$  is a homomorphism if both  $\phi(a + b) = \phi(a) + \phi(b)$  and  $\phi(ab) = \phi(a)\phi(b)$ .  $\phi$  is one-to-one if and only if its kernel ( $\{a \in R \mid \phi(a) = 0'\}$ ) is just the subset  $\{0\}$  of  $R$ . This gives rise to a factor group as well as a factor ring.

**Definition 60 (Ring Isomorphism).** A ring isomorphism is a homomorphism  $\phi: R \rightarrow R'$  that is bijective. Group isomorphisms do not necessarily extend to ring isomorphisms.

**Definition 61 (Unity).** A ring with a multiplicative identity element, denoted by  $1$ , is a *ring with unity*.  $1$  is the "unity."

**Definition 62 (Commutative Ring).** A ring in which multiplication is commutative is a *commutative ring*.

**Example.** For integers  $r, s$  where  $\gcd(r, s) = 1$ , the rings  $\mathbb{Z}_{rs}$  and  $\mathbb{Z}_r \times \mathbb{Z}_s$  are isomorphic.  $\phi: \mathbb{Z}_{rs} \rightarrow \mathbb{Z}_r \times \mathbb{Z}_s$  defined by  $\phi(n \cdot 1) = n \cdot (1, 1)$  is an additive group isomorphism. Also,  $\phi(nm) = (nm) \cdot (1, 1) = [n \cdot (1, 1)][m \cdot (1, 1)] = \phi(n)\phi(m)$  so it is a ring isomorphism as well.

**Definition 63 (Multiplicative Inverse).** A *multiplicative inverse* of an element  $a$  in a ring  $R$  with unity  $1 \neq 0$  is an element  $a^{-1} \in R$  so  $aa^{-1} = a^{-1}a = 1$ .

**Remark.** Only the ring  $\{0\}$  has both the multiplicative and additive inverse as the same element.

**Definition 64 (Unit, Division Rings).** Let  $R$  be a ring with  $1 \neq 0$ . An element  $u \in R$  is a *unit* of  $R$  if it has a multiplicative inverse in  $R$ . If every nonzero element is a unit, then  $R$  is a *division ring* or *skew field*.

**Definition 65 (Field).** A *field* is a commutative division ring. A noncommutative division ring is a *strictly skew field*.

**Definition 66 (Subring and Subfield).** A *subring* is a subset of a ring with under induced operations. A subfield is defined similarly.

**Note.** *Unit* denotes an element with a multiplicative inverse and *unity* denotes the actual multiplicative identity element  $1$ .

## 4.2 Integral Domains



**Definition 67 (Divisors of 0).** If  $a$  and  $b$  are two nonzero elements of a ring  $R$  so that  $ab = 0$ , then  $a$  and  $b$  are *divisors of 0*.

**Theorem 44.** In the ring  $\mathbb{Z}_n$ , the divisors of 0 are the nonzero elements that are *not* relatively prime to  $n$ .

**Proof.** Let  $m \in \mathbb{Z}_n, m \neq 0$  and  $d = \gcd(m, n) \neq 1$ . Thus,  $m(\frac{n}{d}) = (\frac{m}{d})n$  so  $(\frac{m}{d})n$  is 0 in  $\mathbb{Z}_n$  so  $m(n/d)$  is 0 in  $\mathbb{Z}_n$  also but neither  $m, n/d = 0$  so  $m$  is a divisor of 0.

On the other hand, if  $m \in \mathbb{Z}_n, \gcd(m, n) = 1$  and  $ms = 0$  for some  $s \in \mathbb{Z}_n$ , then  $n \mid ms$ . But,  $\gcd(m, n) = 1$  so  $n \mid s$  but  $s \in \mathbb{Z}_n$  so  $s = 0$  in  $\mathbb{Z}_n$  meaning  $m$  is not a divisor.  $\square$

**Corollary.** If  $p$  is prime, then  $\mathbb{Z}_p$  has no divisors of 0.

**Theorem 45.** The multiplicative cancellation laws hold in a ring  $R$  if and only if  $R$  has no divisors of 0.

**Proof.** Say  $R$  is a ring with cancellation laws and  $ab = 0$  for some  $a, b \in R$ . If  $a \neq 0$ , then  $ab = a0$  implies  $b = 0$  via cancellation, WLOG. Conversely, if  $R$  has no divisors of 0 and  $ab = ac, a \neq 0$  for any  $a, b, c \in R$ , then  $0 = ab - ac = a(b - c)$ .  $a = 0$  and  $R$  has no divisors of 0 so  $b = c$  and we can do cancellation. The same goes for right cancellation.  $\square$

**Definition 68 (Integral Domain).** A *integral domain*  $D$  is a commutative ring with unity  $1 \neq 0$  that has *NO* divisors of 0.

**Theorem 46.** Every field  $F$  is an integral domain.

**Proof.** For any  $a, b \in F$ , if  $a \neq 0$  and  $ab = 0$  then  $b = 1b = (a^{-1}a)b = a^{-1}0 = 0$ . So no divisors of 0 in  $F$  exist (from commutativity for other direction).  $\square$

**Theorem 47.** Every finite integral domain is a field.

**Proof.** Take the finite domain  $D$  with finite elements  $0, 1, a_1, \dots, a_n$ . We must show that for any  $a \in D, a \neq 0, \exists b \in D$  so  $ab = 1$ . If all elements of  $D$  are distinct and all nonzero (no divisors of 0), then we find  $a1, aa_1, \dots, aa_n$  can contain no 0 elements but must all be distinct as if they weren't, by cancellation laws,  $aa_i = aa_j \Rightarrow a_i = a_j$ . Thus, this must be some permutation of  $0, 1, a_1, \dots, a_n$  so some  $a_k$  must be the multiplicative inverse of 1.  $\square$

**Corollary.** If  $p$  is prime, then  $\mathbb{Z}_p$  is a field.

**Definition 69 (Characteristic of a Ring).** The *characteristic of a ring*  $R$  is the least positive integer  $\min\{n \in \mathbb{Z}^+ \mid n \cdot a = 0 \text{ for all } a \in R\}$ . If none exists, the characteristic of  $R$  is 0.

**Example.** The ring  $\mathbb{Z}_n$  has characteristic  $n$  while  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  all have characteristic 0.

**Theorem 48.** Let  $R$  be a unital ring. If  $n \cdot 1 \neq 0$  for all  $n \in \mathbb{Z}^+$ , then  $R$  has characteristic 0. But, if  $n \cdot 1 = 0$  then the smallest such integer  $n$  is the characteristic of  $R$ .

**Proof.** If  $n \cdot 1 \neq 0$  for all  $n \in \mathbb{Z}^+$ , then surely we cannot have  $n \cdot a = 0$  for all positive integers  $n$  so  $R$  has characteristic 0. Otherwise, if  $n \cdot 1 = 0$  for some  $n \in \mathbb{Z}^+$ , then for any  $a \in R$ ,  $n \cdot a = a + \cdots + a = a(1 + \cdots + 1) = a(n \cdot 1) = a0 = 0$ .  $\square$

### 4.3 Fermat's and Euler's Theorems

**Remark.** For any field, the nonzero elements form a group under the field multiplication.

**Theorem 49.** Fermat's Little Theorem If  $a \in \mathbb{Z}$  and  $p$  is a prime *not* dividing  $a$ , then  $p$  divides  $a^{p-1}$  so  $a^{p-1} \equiv 1 \pmod{p}$  for  $a \not\equiv 0 \pmod{p}$ .

**Corollary.** If  $a \in \mathbb{Z}$ , then for any prime  $p$ ,  $a^p \equiv a \pmod{p}$ .

**Example.**  $8^{103} \div 13$  gives  $(8^{12})^8(8^7) \equiv (1^8)(8^7) \equiv (-5)^7 \equiv (25)^3(-5) \equiv (-1)^3(-5) \equiv 5 \pmod{13}$ .

**Theorem 50.** The set  $G_n$  of nonzero elements of  $\mathbb{Z}_n$  that are not 0 divisors forms a group under multiplication mod  $n$ .

**Proof.** For any  $a, b \in G_n$ , if  $ab \notin G_n$  then there would exist some  $c \neq 0$  in  $\mathbb{Z}_n$  so  $(ab)c = 0$ . But, this implies  $a(bc) = 0$ . Because  $b$  is not a 0 divisor,  $bc \neq 0$  but then  $a \notin G_n$ . Contradiction, so  $ab \in G_n$  so  $G_n$  has closure.  $1 \in G_n$  obviously and multiplication mod  $n$  is associative.

To show the existence of an inverse, we can use a proof by counting. For any  $a \in G_n$ , given distinct elements of  $G_n$ :  $1, a_1, \dots, a_r$ , the elements  $a1, aa_1, \dots, aa_r$  must also be distinct as  $aa_i = aa_j \Rightarrow a(a_i - a_j) = 0$  but  $a$  is not a divisor of 0 so  $a_i = a_j$ . Because of closure, these products must cover  $G_n$  so there exists some  $a_k$  so  $aa_k = 1$ .  $\square$

**Remark (Euler's Totient/Phi Function  $\phi(n)$ ).**  $\phi(n)$  is equal to the number of positive integers less than or equal to  $n$  and relatively prime to  $n$ . Note  $\phi(1) = 1$ . This is equal to the number of nonzero elements of  $\mathbb{Z}_n$  that are not divisors of 0.

**Theorem 51 (Euler's Theorem).** If  $a$  is an integer relatively prime to  $n$ , then  $a^{\phi(n)} - 1$  is divisible by  $n$ . I.e.  $a^{\phi(n)} \equiv 1 \pmod{n}$ .

**Proof.** If  $a$  is coprime with  $n$  then the coset  $a + n\mathbb{Z}$  of  $n\mathbb{Z}$  containing  $a$  contains an integer  $b < n$  also coprime to  $n$ . Because multiplication mod  $n$  of representatives is well-defined,  $a^{\phi(n)} \equiv b^{\phi(n)} \pmod{n}$ .  $b$  can then be viewed as an element of  $G_n$  of order  $\phi(n)$  consisting of the  $\phi(n)$  elements of  $\mathbb{Z}_n$  coprime to  $n$  so  $b^{\phi(n)} \equiv 1 \pmod{n}$ .  $\square$

**Theorem 52.** Let  $m \in \mathbb{Z}^+, a \in \mathbb{Z}_m$  so  $\gcd(a, m) = 1$ . For each  $b \in \mathbb{Z}_m$ , the equation  $ax = b$  has a unique solution in  $\mathbb{Z}_m$ .

**Proof.**  $a$  is a unit in  $\mathbb{Z}_m$  by the previous theorem so  $s = a^{-1}b$  is a solution of this equation. multiplying both sides of  $ax = b$  by  $a^{-1}$  reveals this indeed is the only solution.  $\square$

**Theorem 53.** Let  $m \in \mathbb{Z}^+$  and  $a, b \in \mathbb{Z}_m$ . Let  $d = \gcd(a, m)$ . The equation  $ax = b$  has a solution in  $\mathbb{Z}_m$  iff  $d \mid b$ . If so, the equation has exactly  $d$  solutions in  $\mathbb{Z}_m$ .

**Proof.** Suppose  $s \in \mathbb{Z}_m$  is a solution to  $ax = b$ . Then  $as - b = qm$  for some  $q \in \mathbb{Z}$  so  $b = as - qm$ .  $d$  divides  $a, m$  so  $d$  must also divide the LHS so a solution  $s$  only exists if  $d \mid b$ .

Next, if  $d \mid b$ , let  $a = a_1d, b = b_1d, m = m_1d$  so  $as - b = qm$  can be rewritten as  $d(a_1s - b_1) = dqm_1$  so  $as - b$  is a multiple of  $m$  if and only if  $a_1s - b_1$  is also a multiple of  $m_1$ . This yields the solutions  $s \in \mathbb{Z}_m$  of  $ax = b$  as precisely  $s, s + m_1, s + 2m_1, \dots, s + (d - 1)m_1$ . Thus,  $d$  solutions to the equation exist in  $\mathbb{Z}_m$ .  $\square$

**Example.** Take the congruence  $12x \equiv 27 \pmod{18}$ . The greatest common divisor of 12 and 18 is 6, but 6 is not a divisor of 27 so no such solutions exist.

For  $15x \equiv 27 \pmod{18}$ , however, their gcd is 3 which divides 27 so this has 3 solutions,  $3 + 18\mathbb{Z}, 9 + 18\mathbb{Z}, 15 + 18\mathbb{Z}$ .

## 4.4 The Field of Quotients of an Integral Domain

**Remark.** Let's think of the rationals as the formal quotient  $(a, b)$  within  $D \times D$  for integral domain  $D = \mathbb{Z}$ .

**Definition 70 (Equivalent).** Let  $S = \{(a, b) \mid a, b \in D, b \neq 0\}$  for an integral domain  $D$ . Two elements  $(a, b)$  and  $(c, d)$  in  $S$  are *equivalent*, denoted as  $(a, b) \sim (c, d)$  if and only if  $ad = bc$ .

**Lemma 3.** The relation  $\sim$  on the set  $S$  is an equivalence relation. (i)  $ab = ba \Rightarrow (a, b) \sim (b, a)$ . (ii)  $(a, b) \sim (c, d) \Rightarrow ad = bc \Rightarrow cb = da \Rightarrow (c, d) \sim (b, a)$ . (iii)  $(a, b) \sim (c, d), (c, d) \sim (e, f) \Rightarrow ad = bc, cf = ed$  so  $acf/e = bc$  so  $af = be$  implying  $(a, b) \sim (e, f)$ . (Note division is simply shorthand for cancellation which is allowed because of integral domain).

**Note.** This chapter discusses the formation of field  $F$  from  $D \times D$ . Proof shows addition and multiplication well defined and has field axioms and contains  $D$ .

**Lemma 4.** To show that  $F$  contains  $D$ , we simply construct an isomorphism  $i: D \rightarrow F$  as given by  $i(a) = [(a, 1)]$  with a subring of  $F$ .

**Proof.** For any  $a, b \in D$ ,  $i(a + b) = [(a + b, 1)] = [(a1 + b1, 1)] = [(a, 1)] + [(b, 1)] = i(a) + i(b)$ . Also,  $i(ab) = [(ab, 1)] = [(a, 1)][(b, 1)] = i(a)i(b)$ . Thus,  $i$  is a ring homomorphism. Next, if  $i(a) = i(b)$ , then  $[(a, 1)] = [(b, 1)] \Rightarrow (a, 1) \sim (b, 1) \Rightarrow a1 = 1b \Rightarrow a = b$  so  $i$  is injective. Because it is of the same size as  $D$ , this is an isomorphism of  $D$  with  $i[D]$ . So  $i[D]$  is a subdomain of  $F$ .  $\square$

**Theorem 54 (Field of Quotients of  $D$ ).** Any integral domain  $D$  can be enlarged to or embedded in a field  $F$  so each element of  $F$  can be expressed as a quotient of two elements of  $D$ . Here, a field  $F$  is a *field of quotients* of  $D$ .

**Proof.**  $[(a, b)] = [(a, 1)][(1, b)] = [(a, 1)]/[(b, 1)] = i(a)/i(b)$ .  $\square$

**Theorem 55.** Let  $F$  be a field of quotients of  $D$  and  $L$  be any field containing  $D$ . Then, there exists a map  $\psi: F \rightarrow L$  which gives an isomorphism of  $F$  with a subfield of  $L$  so  $\psi(a) = a$  for all  $a \in D$ .

**Proof.** Proof omitted.  $\square$

**Corollary.** Every field  $L$  containing an integral domain  $D$  contains a field of quotients of  $D$ .

**Corollary.** Any two fields of quotients of an integral domain  $D$  are isomorphic.

## 4.5 Rings of Polynomials

**Note.** We call  $x$  an *indeterminate* rather than a variable in the ring  $\mathbb{Z}[x]$ .

**Definition 71** (Polynomial  $f(x)$  with Coefficients in  $R$ ). Let  $R$  be a ring. A polynomial  $f(x)$  with coefficients in  $R$  is an infinite formal sum  $\sum_{i=0}^{\infty} a_i x^i$  where  $a_i \in R$  and  $a_i = 0$  for all but a finite number of values of  $i$ . The largest such value of  $i$  is the *degree* of  $f(x)$  while  $a_i$  are the coefficients.

**Note.** An element of  $R$  is a *constant polynomial*.

**Theorem 56.** The set  $R[x]$  of all polynomials in an indeterminate  $x$  with coefficients in a ring  $R$  is a ring under polynomial addition and multiplication. If  $R$  is commutative, then so is  $R[x]$  and  $R$  has unity  $1 \neq 0$  so  $1$  is also a unity for  $R[x]$ .

**Proof.** Clearly  $\langle R[x], + \rangle$  is an abelian group. The associative law for multiplication and the distributive laws are clear as well.  $\square$

**Example.** In  $\mathbb{Z}_2[x]$ ,  $(x+1)^2 = (x+1)(x+1) = x^2 + (1+1)x + 1 = x^2 + 1$  while  $(x+1) + (x+1) = 0x$ .

**Example.** We can even form the ring  $(R[x])[y]$ , i.e. the ring of polynomials in  $y$  with coefficients that are polynomials in  $x$ . This is naturally isomorphic to  $(R[y])[x]$ . Thus, we can denote the ring  $R[x, y]$  as the ring of polynomials in two indeterminates  $x$  and  $y$  with coefficients in  $R$ . In fact the ring  $R[x_1, \dots, x_n]$  of polynomials in  $n$  indeterminates  $x_i$  with coefficients in  $R$  is similarly defined.

Given integral domain  $D$ ,  $D[x]$  is also an integral domain. If  $F$  is a field,  $F[x]$  is a field but *not* a field as  $x$  is not a unit in  $F[x]$ . However, we can do same goes for  $F(x_1, \dots, x_n)$  or the field of rational functions with  $n$  indeterminates over field  $F$ .

**Theorem 57** (The Evaluation Homomorphisms for Field Theory). Let  $F$  be a subfield of a field  $E$ ,  $\alpha \in E$ , and  $x$  be the indeterminate. Define the map  $\phi_\alpha: F \rightarrow E$  as  $\phi_\alpha(a_0 + a_1x + \dots + a_nx^n) = a_0 + a_1\alpha + \dots + a_n\alpha^n$  is a homomorphism of  $F[x]$  into  $E$ . Note that  $\phi_\alpha(x) = \alpha$  so  $\phi_\alpha$  maps  $F$  isomorphically by the identity map such that  $\phi_\alpha(a) = a$  for any  $a \in F$ . This map is the *evaluation homomorphism at  $\alpha$* .

**Proof.** This map is obviously well-defined. Next, for any  $f(x) = a_0 + a_1x + \dots + a_nx^n$ ,  $g(x) = b_0 + b_1x + \dots + b_mx^m$ , let  $h(x) = f(x) + g(x) = c_0 + c_1x + \dots + c_rx^r$ . Thus,  $\phi_\alpha(f(x) + g(x)) = \phi_\alpha(h(x)) = c_0 + c_1\alpha + \dots + c_r\alpha^r = a_0 + a_1\alpha + \dots + a_n\alpha^n + b_0 + b_1\alpha + \dots + b_m\alpha^m = \phi_\alpha(f(x)) + \phi_\alpha(g(x))$ . Multiplication works similarly by definition of polynomial multiplication  $d_j = \sum_{i=0}^j a_i b_{j-i}$ . Thus,  $\phi_\alpha$  is a homomorphism.  $\square$

**Example.** Let  $F = \mathbb{Q}, E = \mathbb{R}$  and apply the evaluation homomorphism  $\phi_0: \mathbb{Q}[x] \rightarrow \mathbb{R}$  such that each polynomial is mapped onto its constant term.

**Example.** Let  $F = \mathbb{Q}, E = \mathbb{C}$ , we can apply the evaluation homomorphism from  $\mathbb{Q}[x] \rightarrow \mathbb{C}$  at  $i$  so  $\phi(x^2 + 1) = 0$  so  $x^2 + 1$  is in the kernel of  $\phi_i$ .

**Remark.** A more interesting example uses the same evaluation homomorphism from  $\mathbb{Q}[x] \rightarrow \mathbb{R}$  but at  $\pi$ . Because  $\pi$  is transcendental, no algebraic solution exists for  $a_0 + a_1\pi + \cdots + a_n\pi^n = 0$  as this implies  $a_i = 0$  so the kernel of  $\phi_\pi$  is  $\{0\}$  implying it is an injective map and thus ring isomorphic to  $\mathbb{Q}[x]$ .

**Definition 72 (Zero of  $f(x)$ ).** Take subfield  $F$  of field  $E$ ,  $\alpha \in E$  and let  $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ . Given evaluation homomorphism  $\phi_\alpha: F[x] \rightarrow E$ , we say  $\alpha$  is a *zero* of  $f(x)$  if  $f(\alpha) = 0$ .

**Theorem 58.** The polynomial  $x^2 - 2$  has no zeroes in the rational numbers. Thus  $\sqrt{2} \notin \mathbb{Q}$ .

**Proof.** Take  $m/n$  for  $m, n \in \mathbb{Z}$  such that  $(m/n)^2 = 2$  and we simplify so that  $\gcd(m, n) = 1$ . Then,  $m^2 = 2n^2$  but this implies 2 is a factor of  $2n^2$  and therefore must be a factor of  $m^2$  as well. But, if this is the case,  $m^2$  is a multiple of 4 so  $n^2$  must have a multiple of 2 as well. But this implies their greatest common divisor is not 1. Contradiction.  $\square$

## 4.6 Factorization of Polynomials over a Field

**Theorem 59 (Division Algorithm for  $F[x]$ ).** Let  $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$  and  $g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_0$  be two elements of  $F[x]$  with nonzero  $a_n, b_m \in F, m > 0$ . Then there exist unique polynomials  $q(x), r(x)$  in  $F[x]$  so  $f(x) = g(x)q(x) + r(x)$  where either  $r(x) = 0$  or its degree is less than the degree  $m$  of  $g(x)$ .

**Theorem 60 (Factor Theorem).** An element  $a \in F$  is a zero of  $f(x) \in F[x]$  if and only if  $x - a$  is a factor of  $f(x)$  in  $F[x]$ .

**Proof.**  $\Rightarrow$ : Suppose that  $f(a) = 0$  for some  $a \in F$ . Then, there exists a  $q(x), r(x) \in F[x]$  so  $f(x) = (x - a)q(x) + r(x)$  where  $r(x) = 0$  or the degree of  $r(x) < 1$ . Thus,  $r(x)$  must equal  $c$  for  $c \in F$  such that  $f(x) = (x - a)q(x) + c$ . Applying the evaluation homomorphism  $\phi_a: F[x] \rightarrow F$ , we get  $0 = f(a) = 0q(a) + c$  implying  $c = 0$ . Therefore,  $x - a \mid f(x)$ .

$\Leftarrow$ : If  $x - a$  is a factor of  $f(x) \in F[x]$ , then clearly,  $f(x) = (x - a)q(x)$  for  $q(x) \in F[x]$  so  $f(a) = (0)q(a) = 0$   $\square$

**Corollary.** A nonzero polynomial  $f(x) \in F[x]$  of degree  $n$  can have at most  $n$  zeros in a field  $F$ .

**Corollary.** If  $G$  is a finite subgroup of the multiplicative group  $(F^*, \cdot)$  for a field  $F$ , then  $G$  is cyclic.

**Proof.** If  $G$  is a finite abelian group, it must be isomorphic to  $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r}$  where each  $d_i$  is a power of a prime. Thinking of each  $\mathbb{Z}_{d_i}$  as a multiplicative cyclic group, take  $m = \text{lcm}(d_1, d_2, \dots, d_r)$  so  $m \leq d_1 d_2 \cdots d_r$ . Note that, for any  $\alpha \in G$ ,  $\alpha^m = 1$  so every element of  $G$  is a zero of  $x^m - 1$ . Because  $G$  has  $d_1 d_2 \cdots d_r$  elements yet  $x^m - 1$  has at most  $m$  zeros,  $m \geq d_1 d_2 \cdots d_r$  so  $m = d_1 d_2 \cdots d_r$ . Therefore, the primes involved in the prime powers are distinct implying the group  $G$  is isomorphic to the cyclic group  $\mathbb{Z}_m$ .  $\square$

**Definition 73 (Irreducible Polynomial in  $F[x]$ ).** A nonconstant polynomial  $f(x) \in F[x]$  is *irreducible over  $F$*  if  $f(x) = g(x)h(x)$  for  $g, h \in F[x]$  both of lower degree than  $f(x)$ . Otherwise  $f(x)$  is *reducible over  $F$* .

**Example.** Note that  $x^2 - 2$  has no zeros in  $\mathbb{Q}$  and is therefore not irreducible over  $\mathbb{Q}$  but clearly has roots in  $\mathbb{R}$  over which it is reducible.

**Theorem 61.** Let  $f(x) \in F[x]$  and let  $f(x)$  have degree 2 or 3. Then, it is reducible over  $F$  if and only if it has a zero in  $F$ .

**Proof.** If  $f(x)$  is reducible and therefore  $f(x) = g(x)h(x)$ , we can say  $g(x)$ , WLOG, has degree 1. Thus,  $g(x)$  is of the form  $x - a$  so  $g(a) = 0$  so  $f(a) = 0$  implying  $f(x)$  indeed must have a zero in  $F$ . Conversely, if  $f(a) = 0$  for some  $a \in F$ , then  $x - a \mid f(x)$  making  $f(x)$  reducible.  $\square$

**Theorem 62.** If  $f(x) \in \mathbb{Z}[x]$ , then  $f(x)$  factors into a product of two polynomials of lower degrees  $r, s \in \mathbb{Q}[x]$  if and only if it has such a factorization with polynomials of the same degree  $r, s \in \mathbb{Z}[x]$ .

**Corollary.** If  $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$  with  $a_0 \neq 0$ , and if  $f(x)$  has a zero in  $\mathbb{Q}$ , then it has a zero  $m$  in  $\mathbb{Z}$  and  $m$  must divide  $a_0$ .

**Theorem 63 (Einstein Criterion).** Let  $p \in \mathbb{Z}$  be a prime. Suppose  $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$  and  $a_n \not\equiv 0 \pmod{p}$ , but  $a_i \equiv 0 \pmod{p}$  for all  $i < n$ , with  $a_0 \not\equiv 0 \pmod{p^2}$ . Then  $f(x)$  is irreducible over  $\mathbb{Q}$ .

**Proof.** We need only show  $f(x)$  does not factor into polynomials of lower degree in  $\mathbb{Z}[x]$ . If  $f(x) = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0)$  is such a factorization with  $b_r, c_s \neq 0$  and  $r, s < n$ , then  $a_0 \not\equiv 0 \pmod{p^2}$  implies  $b_0, c_0$  are not both congruent to 0 mod  $p$ . Supposing  $b_0 \not\equiv 0 \pmod{p}$  but

$c_0 = 0(\text{mod } p)$ . This then implies, because  $a_n \neq 0(\text{mod } p)$ , that  $b_r, c_s \neq 0(\text{mod } p)$ . Because  $a_n = b_r c_s$ , if  $m$  is the smallest value of  $K$  so  $c_k \neq 0(\text{mod } p)$ , then  $a_m = b_0 + b_1 c_{m-1} + \cdots + \begin{cases} b_m c_0 & \text{if } r \geq m \\ b_r c_{m-r} & \text{if } r < m \end{cases}$ . The fact neither  $b_0$  nor  $c_m$  are congruent to 0 modulo  $p$  while  $c_{m-1}, \dots, c_0$  are all congruent to 0 modulo  $p$  implies that  $a_m \neq 0(\text{mod } p)$  so  $m = n$ . Hence,  $s = n$  so  $s$  is not less than  $n$  against our assumption meaning this factorization was nontrivial.  $\square$

**Corollary** ( $p^{\text{th}}$  Cyclotomic Polynomial). The polynomial  $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$  is irreducible over  $\mathbb{Q}$  for any prime  $p$ .  $\Phi_p(x)$  is the  $p^{\text{th}}$  cyclotomic polynomial.

**Theorem 64.** Let  $p(x)$  be an irreducible polynomial in  $F[x]$ . If  $p(x)$  divides  $r(x)s(x)$  for  $r, s \in F[x]$ , then either  $p(x)$  divides  $r(x)$  or  $s(x)$ .

**Theorem 65.** If  $F$  is a field, then every nonconstant polynomial  $f(x) \in F[x]$  can be factored in  $F[x]$  into a product of irreducible polynomials which are unique except for order and for unit (nonzero constant) factors in  $F$ .



## Chapter 5

# Ideals and Factor Rings

### 5.1 Homomorphisms and Factor Rings

**Theorem 66.** Let  $\phi$  be a homomorphism of a ring  $R$  into a ring  $R'$ . These qualities follow: (a) If 0 is the additive identity in  $R$ , then  $\phi(0) = 0'$  is the additive identity in  $R'$ . (b) If  $a \in R$ , then  $\phi(-a) = -\phi(a)$ . (c) If  $S$  is a subring of  $R$ , then  $\phi[S]$  is a subring of  $R'$ . (d) If  $S'$  is a subring of  $R'$  then  $\phi^{-1}[S']$  is a subring of  $R$ . Finally, if  $R$  has unity 1, then  $\phi(1)$  is the unity for  $\phi[R]$ .

**Theorem 67.** For ring homomorphism  $\phi: R \rightarrow R'$  with kernel  $H$ , if  $a \in R$ , then  $\phi^{-1}[\phi(a)] = a + H = H + a$  where  $a + H = H + a$  is the coset containing  $a$  of the commutative additive group  $\langle H, + \rangle$ .

**Remark.** Ring homomorphism  $\phi: R \rightarrow R'$  is injective iff  $\ker(\phi) = \{0\}$ .

**Theorem 68.** Given ring homomorphism  $\phi: R \rightarrow R'$  with kernel  $H$ , the additive cosets of  $H$  form a ring  $R/H$  which have addition and multiplication defined with

$$(a + H) + (b + H) = (a + b) + H, \quad (a + H)(b + H) = (ab) + H.$$

Also the map  $\mu: R/H \rightarrow \phi[R]$  defined via  $\mu(a + H) = \phi(a)$  is an isomorphism.

**Proof.** Addition of cosets is well-defined from group theory. For multiplication, given  $h_1, h_2 \in H$ ,  $a + h_1 \in a + H$ ,  $b + h_2 \in b + H$  say  $c = (a + h_1)(b + h_2) = ab + ah_2 + h_1b + h_1h_2$ .  $c$  will lie in  $ab + H$  if  $\phi(c) = \phi(ab)$  where  $ab + H = \phi^{-1}[\phi(ab)]$ . Because  $\phi(h) = 0'$  for  $h \in H$ , we get  $\phi(c) = \phi(ab) + \phi(ah_2) + \phi(h_1b) + \phi(h_1h_2) = \phi(ab)$ , making multiplication well-defined.

We are left to show  $R/H$  is a ring. This requires associative property for multiplication and the distributive laws which follow from the representatives of  $R$ . An earlier theorem then shows  $\mu$  is well-defined and bijective onto  $\phi[R]$  and satisfies the multiplicative property of a homomorphism. Multiplicatively,  $\mu[(a+H)(b+H)] = \mu(ab+H) = \phi(a)\phi(b) = \mu(a+H)\mu(b+H)$ . So  $\mu$  is an isomorphism.  $\square$

**Theorem 69.** Given subring  $H$  of ring  $R$ , multiplication of additive cosets of  $H$  is well-defined  $((a+H)(b+H) = ab+H)$  if and only if  $ah \in H$  and  $hb \in H$  for all  $a, b \in R, h \in H$ .

**Definition 74 (Ideal).** An additive subgroup  $N$  of a ring  $R$  for which  $aN \subseteq N$  and  $Nb \subseteq N$  for all  $a, b \in R$  is an *ideal*.

**Example.**  $n\mathbb{Z}$  is an ideal for the ring  $\mathbb{Z}$ .

**Corollary.** Let  $N$  be an ideal of ring  $R$ . Then the additive cosets of  $N$  form a ring  $R/N$  with binary operations  $(a+N) + (b+N) = (a+b) + N$  and  $(a+N)(b+N) = ab + N$ .

**Definition 75 (Factor Ring).** The ring  $R/N$  is the *factor ring*, or *quotient ring* of  $R$  by  $N$ .

**Theorem 70 (Fundamental Homomorphism Theorem).** Given ring homomorphism  $\phi: R \rightarrow R'$  with kernel  $N$ ,  $\phi[R]$  is a ring and the map  $\mu: R/N \rightarrow \phi[R]$  given by  $\mu(x+N) = \phi(x)$  is an isomorphism. Moreover, if  $\gamma: R \rightarrow R/N$  is the homomorphism given by  $\gamma(x) = x+N$ , then for all  $x \in R$ ,  $\phi(x) = \mu\gamma(x)$ .

**Proof.** This follows from previous theorems.  $\square$

**Example.** As an example, take ideal  $n\mathbb{Z}$  of  $\mathbb{Z}$  so we can take the factor ring  $\mathbb{Z}/n\mathbb{Z}$ . We therefore have the ring homomorphism  $\phi: \mathbb{Z} \rightarrow \mathbb{Z}_n$  where  $\phi(m)$  is the remainder of  $m \bmod n$  such that  $\ker(\phi) = n\mathbb{Z}$ . This implies  $\mu: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}_n$  where  $\mu(m+n\mathbb{Z})$  is the remainder of  $m \bmod n$  is well-defined and an isomorphism.

**Remark.** An ideal in ring theory is analogous to a normal subgroup in group theory. Both structures allow us to form a factor structure like  $R/N$  which give rise to a certain homomorphism.

Similarly,  $\phi[N]$  is an ideal of  $\phi[R]$  though not necessarily of  $R'$  and if  $N'$  is an ideal of either  $\phi[R]$  or  $R'$  then  $\phi^{-1}[N']$  is indeed an ideal of  $R$ .

## 5.2 Prime and Maximal Ideals

**Example.** Take the following examples:

- (a) The ring  $\mathbb{Z}_p$  is a field for prime  $p$  implying a factor ring  $(\mathbb{Z}/p\mathbb{Z})$  of an integral domain may be a field.
- (b) While  $\mathbb{Z} \times \mathbb{Z}$  is not an integral domain as  $(0, 1)(1, 0) = (0, 0)$ ,  $N = \{(0, n) \mid n \in \mathbb{Z}\}$  is an ideal of  $\mathbb{Z} \times \mathbb{Z}$  where  $(\mathbb{Z} \times \mathbb{Z})/N$  is isomorphic to  $\mathbb{Z}$ . This implies a factor ring of a ring may be an integral domain even though the original ring isn't.
- (c) The subset  $N = \{0, 3\} \subset \mathbb{Z}_6$  is an ideal and has factor ring of 3 elements. Thus, even if  $R$  is not an integral domain,  $R/N$  can still be a field.
- (d) Finally,  $\mathbb{Z}$  is an integral domain but  $\mathbb{Z}/6\mathbb{Z}$  isn't so a factor ring isn't necessarily 'better.'

**Remark (Improper/Trivial Ideals).** Every nonzero ring has the *improper ideal*  $R$  itself and the trivial ideal  $\{0\}$ . These have factor rings isomorphic to  $\{0\}$  and  $R$  itself.

**Theorem 71.** Given unital ring  $R$ , if its ideal  $N$  contains a unit, then  $N = R$ .

**Proof.** With unit  $u \in N$ , the condition  $rN \subseteq N$  for all  $r \in R$  so taking  $r = u^{-1}$  implies  $1 = u^{-1}u \in N$  meaning  $rN \subseteq N$  for all  $r \in R$  so  $N = R$ .  $\square$

**Corollary.** A field contains no proper nontrivial ideals.

**Definition 76.** A *maximal ideal* of a ring  $R$  is an ideal  $M$  different from  $R$  such that there is no proper ideal  $N$  of  $R$  properly containing  $M$ .

**Theorem 72.** Given unital commutative ring  $R$ ,  $M$  is a maximal ideal of  $R$  if and only if  $R/M$  is a field.

**Proof.**  $\Rightarrow$ : Suppose  $M$  is a maximal ideal of  $R$ . If  $R$  is commutative with unity, then  $R/M$  is also a nonzero commutative ring with unity. Now, we must show every nonzero element is a unit. Since  $M \neq R$  because  $M$  maximal, say  $(a + M) \in R/M$  with  $a \notin M$  so  $a + M$  is not the additive identity element of  $R/M$ . If  $a + M$  has no multiplicative inverse, then the set  $(R/M)(a + M)$  does not contain  $1 + M$ . It's then clear,  $(R/M)(a + M)$  is an ideal of  $R/M$ . It's nontrivial because  $a \notin M$  and proper because it doesn't contain  $1 + M$ . Thus, if  $\gamma: R \rightarrow R/M$  is the canonical homomorphism, then  $\gamma^{-1}[(R/M)(a + M)]$  is a proper ideal of  $R$  properly containing  $M$  making  $M$  not the maximal ideal so  $a + M$  must indeed have a multiplicative inverse

in  $R/M$ , making  $R/M$  a field.

$\Leftarrow$ : Conversely, if  $R/M$  is a field and  $N$  is an ideal of  $R$ , then  $M \subset N \subset R$  by canonical homomorphism  $\gamma$  of  $R$  onto  $R/M$ . This implies  $\gamma[N]$  is an ideal of  $R/M$  not equal to  $R/M$  but larger than  $\{0 + M\}$ . But this contradicts the earlier corollary that  $R/M$  contains no proper nontrivial ideals so if  $R/M$  is a field, then  $M$  must be maximal.  $\square$

**Example.** Since  $\mathbb{Z}/n\mathbb{Z}$  is isomorphic to  $\mathbb{Z}_n$  and  $\mathbb{Z}_n$  is a field iff  $n$  is prime, the maximal ideals of  $\mathbb{Z}$  are precisely the ideals  $p\mathbb{Z}$  for prime  $p$ .

**Corollary.** A commutative unital ring is a field iff it has no proper nontrivial ideals.

**Proof.** The earlier corollary shows a field has no proper nontrivial ideals. Conversely, if a commutative ring  $R$  with unity has no proper nontrivial ideals, then  $\{0\}$  is a maximal ideal and  $R/\{0\}$  isomorphic to  $R$  must be a field.  $\square$

**Remark.** The factor ring  $R/N$  will be an integral domain if and only if  $(a + N)(b + N) = N$  implies  $a + N = N$  or  $b + N = N$ , i.e.  $R/N$  has no divisors of 0. This condition amounts to saying  $ab \in N \Rightarrow a \in N \vee b \in N$ .

**Definition 77 (Prime Ideal).** An ideal  $N \neq R$  in a commutative ring  $R$  is a *prime ideal* if  $ab \in N$  implies either  $a \in N$  or  $b \in N$  for  $a, b \in R$ . Note  $\{0\}$  is a prime ideal in any integral domain.

**Theorem 73.** Let  $R$  be a commutative unital ring so  $N \neq R$  is an ideal in  $R$ . Then  $R/N$  is an integral domain if and only if  $N$  is a prime ideal in  $R$ .

**Corollary.** Every maximal ideal in a commutative ring  $R$  with unity is a prime ideal.

**Remark.** We can summarize the above with the following: for a commutative unital ring  $R$ :

1. An ideal  $M$  of  $R$  is maximal iff  $R/M$  is a field.
2. An ideal  $N$  of  $R$  is prime iff  $R/N$  is an integral domain.
3. Every maximal ideal of  $R$  is a prime ideal.

**Theorem 74.** If  $R$  is a ring with unity 1, then there exists a homomorphism  $\phi: \mathbb{Z} \rightarrow R$  given by  $\phi(n) = n \cdot 1$  for  $n \in \mathbb{Z}$ .

**Proof.**  $\phi(n + m) = (n + m) \cdot 1 = (n \cdot 1) + (m \cdot 1) = \phi(n) + \phi(m)$ . Next,

$$\phi(nm) = (nm) \cdot 1 = (n \cdot 1)(m \cdot 1) = \phi(n)\phi(m). \quad \square$$

**Corollary.** If  $R$  is a unital ring with characteristic  $n > 1$ , then  $R$  contains a subring isomorphic to  $\mathbb{Z}_n$ . If  $R$  has characteristic 0, then  $R$  contains a subring isomorphic to  $\mathbb{Z}$ .

**Proof.** The homomorphism  $\phi: \mathbb{Z} \rightarrow R$  given by  $\phi(m) = m \cdot 1$  for  $m \in \mathbb{Z}$  has kernel of form  $s\mathbb{Z}$  ideal in  $\mathbb{Z}$  for some  $s \in \mathbb{Z}$ . If  $R$  has characteristic  $n > 0$ , then the kernel of  $\phi$  is  $n\mathbb{Z}$  with image  $\phi[\mathbb{Z}] \leq R$  isomorphic to  $\mathbb{Z}/n\mathbb{Z} \sim \mathbb{Z}_n$ . If  $R$  has characteristic 0, then  $m \cdot 1 \neq 0$  for all  $m \neq 0$  so the kernel of  $\phi$  is just  $\{0\}$  implying the image of  $\phi[\mathbb{Z}] \leq R$  is isomorphic to  $\mathbb{Z}$ .  $\square$

**Theorem 75.** A field  $F$  is either of prime characteristic  $p$  and contains a subfield isomorphic to  $\mathbb{Z}_p$  or of characteristic 0 and contains a subfield isomorphic to  $\mathbb{Q}$ .

**Proof.** If the characteristic of  $F$  is not 0, then the above corollary shows  $F$  contains a subring isomorphic to  $\mathbb{Z}_n$ . Thus,  $n$  must be a prime  $p$  or else  $F$  must contain a subring isomorphic to  $\mathbb{Z}$  in which case  $F$  must contain a field of quotients which must be isomorphic to  $\mathbb{Q}$ .  $\square$

**Definition 78 (Prime Fields).** The fields  $\mathbb{Z}_p, \mathbb{Q}$  are *prime fields*.

**Definition 79 (Principal Ideal).** If  $R$  is a commutative unital ring and  $a \in R$ , the ideal  $\{ra \mid r \in R\}$  of all multiples of  $a$  is the *principal ideal generated by  $a$*  denoted by  $\langle a \rangle$ . An ideal  $N$  of  $R$  is a *principal ideal* if  $N = \langle a \rangle$  for some  $a \in R$ .

**Example.** Every ideal of the ring  $\mathbb{Z}$  is of the form  $n\mathbb{Z}$  generated by  $N$  so every ideal of  $\mathbb{Z}$  is a principal ideal.

**Example.** The ideal  $\langle x \rangle$  in  $F[x]$  consists of all polynomials in  $F[x]$  with zero constant terms.

**Theorem 76.** If  $F$  is a field, then every ideal in  $F[x]$  is *principal*.

**Proof.** For ideal  $N$  of  $F[x]$ , if  $N = \{0\}$ , then  $N = \langle 0 \rangle$ . Otherwise, say  $g(x)$  is a nonzero element of  $N$  of minimal degree. If the degree of  $g(x)$  is 0, then  $g(x) \in F$  and is a unit so  $N = F[x] = \langle 1 \rangle$  so  $N$  is principal. If the degree of  $g(x) \geq 1$ , say  $f(x) \in N$  such that  $f(x) = g(x)q(x) + r(x)$  where the degree of  $r(x)$  is either 0 or less than that of  $g(x)$ . Thus,  $f(x), g(x) \in N$  imply  $f(x) - g(x)q(x) = r(x) \in N$  by definition of an ideal such that  $g(x)$  is a nonzero element of minimal degree in  $N$  so  $r(x) = 0$  and finally  $f(x) = g(x)q(x)$  so  $N = \langle g(x) \rangle$ .  $\square$

**Theorem 77.** An ideal  $\langle p(x) \rangle \neq \{0\}$  of  $F[x]$  is maximal iff  $p(x)$  is irreducible over  $F$ .

**Proof.**  $\Rightarrow$ : Suppose  $\langle p(x) \rangle \neq \{0\}$  is a maximal ideal of  $F[x]$ . Then  $\langle p(x) \rangle \neq F[x]$  so  $p(x) \notin F$ . Thus, if  $p(x) = f(x)g(x)$ , because  $\langle p(x) \rangle$  is a maximal ideal and hence also a prime ideal,  $(f(x)g(x)) \in \langle p(x) \rangle$  implies either  $f(x)$  or  $g(x) \in \langle p(x) \rangle$  so either  $f(x)$  or  $g(x)$  have  $p(x)$  as a factor. But, the degrees of both  $f(x), g(x)$  cannot be less than the degree of  $p(x)$  implying  $p(x)$  is irreducible over  $F$ .

$\Leftarrow$ : Conversely, if  $p(x)$  is irreducible over  $F$ , suppose  $N$  is an ideal such that  $\langle p(x) \rangle \subseteq N \subseteq F[x]$ . If  $N$  is a principal ideal, then  $N = \langle g(x) \rangle$  for some  $g(x) \in N$ . Therefore,  $p(x) \in N$  implies  $p(x) = g(x)q(x)$  for some  $q(x) \in F[x]$ . But,  $p(x)$  is irreducible so either  $g(x), q(x)$  are of degree 0. If  $g(x)$  is of degree 0, then it's a nonzero constant and consequently a unit in  $F[x]$  so  $\langle g(x) \rangle = N = F[x]$ . If  $q(x)$  is of degree 0, then  $q(x) = c \in F$  so  $g(x) = (1/c)p(x)$  is in  $\langle p(x) \rangle$  meaning  $N = \langle p(x) \rangle$  is maximal.  $\square$

**Example.**  $x^3 + 3x^2 + 2$  is irreducible in  $\mathbb{Z}_5[x]$  and therefore  $\mathbb{Z}_5[x]/\langle x^3 + 3x^2 + 2 \rangle$  is a field. Similarly,  $x^2 - 2$  irreducible in  $\mathbb{Q}[x]$  so  $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$  is a field.

**Theorem 78.** Let  $p(x)$  be an irreducible polynomial in  $F[x]$ . If  $p(x)$  divides  $r(x)s(x)$  for  $r(x), s(x) \in F[x]$ , then either  $p(x)$  divides  $r(x)$  or  $s(x)$ .

## Chapter 6

# Extension Fields

### 6.1 Introduction to Extension Fields

**Definition 80** (Extension Field). A field  $E$  is an *extension field* of a field  $F$  if  $F \leq E$ .