Abstract Algebra

Jim Coykendall

January 5, 2021

Chapter 1

Warm Up

The notation $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ refer to the natural numbers, the integers, the rational numbers, the real numbers and the complex numbers respectively.

Let $f : A \longrightarrow B$ and $g : B \longrightarrow C$ be functions. We define $\text{im}(f) = f(A) = \{b \in B | b = f(a), a \in A\}$. If $D \subseteq B$ then $f^{-1}(D) = \{a \in A | f(a) \in D\}$. This is called the preimage of D (under f). If $b \in B$ then $f^{-1}(b)$ is called the fiber of f over b (or the preimage of b). The composite function $g \circ f$ is defined by $(g \circ f)(a) = g(f(a))$. Recall the following:

1. f is one to one or injective if $f(a_1) = f(a_2) \Longrightarrow a_1 = a_2$.
2. f is onto or surjective if $\text{im}(f) = B$.
3. f is bijective if both f is both injective and surjective.
4. f has a left (resp. right) inverse if there is an $h : B \longrightarrow A$ such that such that $h \circ f = 1_A$ (resp. $f \circ h = 1_B$).

Proposition 1.0.1. *Let $f : A \longrightarrow B$.*

1. *f is one to one if and only if f has a left inverse.*
2. *f is onto if and only if f has a right inverse.*
3. *f is bijective if and only if there is a $g : B \longrightarrow A$ such that $f \circ g = 1_B$ and $g \circ f = 1_A$.*
4. *If $|A| = |B| < \infty$ then $f : A \longrightarrow B$ is bijective if and only if f is surjective if and only if f is injective.*

Definition 1.0.2. *Let A be a nonempty set.*

a) A relation on A is a subset $R \subseteq A \times A$ and we write $a \sim b$ if and only if $(a, b) \in R$.

b) $\sim$ is said to be

1. *Reflexive if $a \sim a$ for all $a \in A$.*
2. *Symmetric if $a \sim b$ implies $b \sim a$ for all $a, b \in A$.*
3. *Transitive if $a \sim b$ and $b \sim c$ then $a \sim c$ for all $a, b, c \in A$.*

c) *If $\sim$ is symmetric, reflexive and transitive, then we say that $\sim$ is an equivalence relation.*

d) *If $\sim$ is an equivalence relation then the equivalence class of $a \in A$ is $\{x \in A | x \sim a\}$.*

e) *A partition of the set A is a collection $\{A_i\}$ of nonempty subsets of A such that $A = \bigcup_i A_i$ and $A_i \bigcap A_j = \emptyset$ is $i \neq j$.*

Example 1.0.3. *Consider the partitions of the ordinary integers $\mathbb{Z}$ (or even $\mathbb{Z}_n$).*

Proposition 1.0.4. *Let A be a nonempty set.*

a) *If $\sim$ is an equivalence relation then the set of equivalence classes form a partition of A.*

b) *If the subsets A_i of A form a partition, then there is a an equivalence relation on A such that the sets A_i form the equivalence classes.*

Here are some familiar and useful properties of the integers $\mathbb{Z}$. But first a definition.

Definition 1.0.5. *If $a, b \in \mathbb{Z}, a \neq 0$ then we say that $a|b$ (a divides b) if there is a $c \in \mathbb{Z}$ such that $b = ac$.*

Proposition 1.0.6. *Let $\mathbb{Z}$ denote the integers.*

a) *If $\emptyset \neq A \subset \mathbb{Z}^+$ then A has a least element.*

b) *Given any nonzero $a, b \in \mathbb{Z}$, there is a $d \in \mathbb{Z}$ (greatest common divisor or gcd) such that $d|a$ and $d|b$ and if d' is another common divisor of a and b then $d'|d$.*

c) *Given any nonzero $a, b \in \mathbb{Z}$, there is an $m \in \mathbb{Z}$ (least common multiple of lcm) such that $a|m$ and $b|m$ and if m' is another common multiple of a and b then $m|m'$.*

d) *Let $d = gcd(a, b)$ and $m = lcm(a, b)$, then $ab = dm$.*

e) *Given nonzero $a, b \in \mathbb{Z}$, then there exist $q, r \in \mathbb{Z}$ with $0 \leq r < |b|$ and $a = qb + r$.*

f) *Let $d = gcd(a, b)$, then there exists $x, y \in \mathbb{Z}$ such that $d = ax + by$.*

g) *(Fundamental Theorem of Arithmetic) If $n \geq 2$ is a natural number, then n can be expressed uniquely as a product of positive prime integers (for now we will take a positive prime to be an integer $p \geq 2$ that has no poitive divisors except itself and 1).*

Example 1.0.7. *You have an army that started with 2000 soldiers. After a battle you need to know how many you have left. When your remaining soldiers are organized into groups of 25, there are 5 stragglers and when you organize it into groups of 81, there are 4 stragglers. How many soldiers are left?*

Theorem 1.0.8. *(Chinese Remainder Theorem) Suppose that if $n_1, n_2, \cdots n_k$ is a collection of pairwise relatively prime positive integers and let $N = n_1 n_2 \cdots n_k$. Show that the system of congruences*

$$\begin{aligned} x \equiv & a_1 mod(n_1) \\ x \equiv & a_2 mod(n_2) \\ & \vdots \\ x \equiv & a_k mod(n_k) \end{aligned}$$

has a unique solution z such that $0 \leq z \leq N - 1$.

Proof. Exercise. Uniqueness is easier, existence depends on the fact that the numbers n_i are relatively prime. One approach might be induction on k. □

We will now look briefly at modular arithmetic from the point of view of $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ and $\equiv \mod(n)$.

Example 1.0.9. *Consider the structure on the sets $\mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^*$ with "ordinary" addition and multiplication modulo n. Note that in $\mathbb{Z}/5\mathbb{Z}$ has an "i". Look at $\mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$. Note that if $\overline{a} = \overline{b}$ as elements of $\mathbb{Z}/n\mathbb{Z}$, this is equivalent to the statement $a \equiv b mod(n)$. And to clarify this further, we say that $a \equiv b mod(n)$ if and only if $a - b$ is a multiple of n.*

Some important results concerning modular arithmetic. We have the technology to show some of this now, but many of these results will be consequences of what we will be doing presently.

We define the Euler $\phi-$function as follows.

Definition 1.0.10. *Let $n > 1$ be a natural number. If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ with p_i prime and $a_i \in \mathbb{N}$, then $\phi(n) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1)$.*

Basically, $\phi(n)$ counts the numbers between 1 and n that are relatively prime to n.

Theorem 1.0.11 (*Some Properties of Modular Arithmetic*)**.** *The relation $\equiv mod(n)$ is reflexive, symmetric, and transitive. Additionally it enjoys the following properties.*

1. *If $a \equiv b mod(n)$ then $(a + k) \equiv (b + k) mod(n)$ for all $k \in \mathbb{Z}$.*
2. *If $a \equiv b mod(n)$ then $ak \equiv bk mod(n)$ for all $k \in \mathbb{Z}$.*
3. *If $a \equiv b mod(n)$ then $f(a) \equiv f(b) mod(n)$ for all $f(x) \in \mathbb{Z}[x]$.*

4. *If* $gcd(a,n) = 1$ *and* $x \equiv y mod(\phi(n))$ *then* $a^x \equiv a^y mod(n)$.
5. *If* $gcd(a,n) = 1$ *then there is a* $c \in \mathbb{Z}$ *such that* $ac \equiv 1 mod(n)$ *and in this case, then linear congruence equation* $ax \equiv b mod(n)$ *has the unique solution given by* $x \equiv cb mod(n)$.
6. *(Fermat's Little Theorem) If* p *is a positive prime integer then for all* a *with* $gcd(a,p) = 1$, $a^{p-1} \equiv 1 mod(p)$.
7. *(Euler's Theorem) If* $gcd(a,n) = 1$, $a^{\phi(n)} \equiv 1 mod(n)$.
8. *(Wilson's Theorem)* p *is prime if and only if* $(p-1)! \equiv -1 mod(p)$.

Exercises

1. Let $k, m, n \in \mathbb{Z}$ be nonzero integers.
   a) Show that $\gcd(m,n)$ is a linear combination of m and n (that is, show that if $d = \gcd(m,n)$ then there are integers a and b such that $am + bn = d$).
   b) Show that if $\gcd(k,m) = 1$ and $\gcd(k,n) = 1$, then $\gcd(k,mn) = 1$.
   c) Show that if $\gcd(k,m) = 1$ and k divides mn, then k divides n.
2. Let $m, n \in \mathbb{Z}$ be nonzero integers, $d = \gcd(m,n)$ and $L = \text{lcm}(m,n)$. Show that $dL = mn$.
3. Let $n \in \mathbb{N}$ be a natural number, and consider $\mathbb{Z}_n$, the integers modulo n (this is the set of equivalence classes modulo the equivalence relation $\sim$ where $m_1 \sim m_2$ if and only if $n|(m_1 - m_2)$).
   a) We define the set $U(\mathbb{Z}_n) = \{\overline{a} \in \mathbb{Z}_n | \exists \overline{b} \in \mathbb{Z}_n \text{ such that } \overline{a}\overline{b} = \overline{1}\}$ (equivalently, if $a \in \mathbb{Z}$ then $\overline{a} \in U(\mathbb{Z}_n)$ if and only if there is a $b \in \mathbb{Z}$ such that $ab \equiv 1 \text{mod}(n)$). Show that if $\overline{x}, \overline{y} \in U(\mathbb{Z}_n)$ then $\overline{xy} \in U(\mathbb{Z}_n)$.
   b) Show if $\overline{a} \in U(\mathbb{Z}_n)$ then $\overline{a}^m \equiv 1 \text{mod}(n)$ for some $m \in \mathbb{N}$.
   c) Show that if $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ with each p_i prime and each $a_i \in \mathbb{N}$ then $|U(\mathbb{Z}_n)| = \prod_{i=1}^{m} (p^{a_i - 1}(p_i - 1))$.
4. (*Chinese Remainder Theorem*) Suppose that if $n_1, n_2, \cdots n_k$ is a collection of pairwise relatively prime positive integers and let $N = n_1 n_2 \cdots n_k$. Show that the system of congruences

$$\begin{aligned} x &\equiv a_1 \text{mod}(n_1) \\ x &\equiv a_2 \text{mod}(n_2) \\ &\vdots \\ x &\equiv a_k \text{mod}(n_k) \end{aligned}$$

has a unique solution z such that $0 \leq z \leq N-1$.

5. Let A be a nonempty set and $\sim$ an equivalence relation on A.

   a) Show that the set of equivalence classes of A under $\sim$ is a partition of A.

   b) Show that if $\{A_i\}_{i\in\Lambda}$ is a partition of A, then there is an equivalence relation on A such that the sets $\{A_i\}_{i\in\Lambda}$ are precisely the equivalence classes of A under this relation.

6. Prove the properties of modular arithmetic above.

Chapter 2

Groups

2.1 Basics

First some basic notions.

Definition 2.1.1. *A binary operation $\circ$ on the nonempty set G is a function $G \times G \longrightarrow G$.*

a) We say that $\circ$ is associative if $g \circ (h \circ k) = (g \circ h) \circ k$ for all $g, h, k \in G$.

b) We say that $\circ$ is commutative if $g \circ h = h \circ g$ for all $g, h \in G$.

Example 2.1.2. *Ordinary multiplication on the reals, addition on the reals, matrix multiplication, function composition.*

Definition 2.1.3. *A group G is a nonempty set equipped with a binary operation $\circ$ such that*

a) $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in G$.

b) There exists $e \in G$ such that $e \circ g = g \circ e = g$ for all $g \in G$.

c) For all $g \in G$, there is an $h \in G$ such that $g \circ h = h \circ g = e$.

From now on, we will suppress that $\circ$ notation and use juxtapostion to denote the operation. If $gh = hg$ for all $g, h \in G$, we say that G is abelian. If $|G|$ we say that G is finite.

Example 2.1.4. *$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Q}^*$, the group of rearrangements on the Rubik's cube, C_6, S_3.*

Theorem 2.1.5. *Let G be a group.*

a) $e \in G$ is unique.

b) for all $a \in G$, a^{-1} is unique.

c) $(a^{-1})^{-1} = a$ *for all* $a \in G$.

d) $(ab)^{-1} = b^{-1}a^{-1}$ *for all* $a, b \in G$.

Proof. a) Suppose that f and e are identities. Then $e = fe = f$. b) Suppose that a has x, y as inverses. Then $ax = e$ and so $y(ax) = ye = (ya)x = ex$ and hence $x = y$. c) Let $x = a^{-1}$ be the inverse of a. Since $xa = e = ax$, a is an inverse for x. By part b), $(a^{-1})^{-1} = a$. d) Note that $(ab)b^{-1}a^{-1} = e = a^{-1}b^{-1}(ab)$ and by part b) we are done. □

Definition 2.1.6. *Let G be a group, we define the order of G ($|G|$) to be the order of the underlying set G.*

Example 2.1.7. $|\mathbb{Z}_n| = n$.

Definition 2.1.8. *Let G be a group.*

a) If $a \in G$ then $\circ(a) = |a| = min\{n \in \mathbb{Z}^+ | a^n = e\}$ (and is said to be ∞ if no such n exists).

b) The exponent of G ($exp(G)$) is the smallest positive integers n such that $a^n = e$ for all $a \in G$.

2.2 Standard Examples

Here we present some classes of examples of groups.

Dihedral Groups

The dihedral group may be thought of as the group of symmetries on the $n-$gon ($n > 2$). All possible symmetries are generated by superpositions of a rotation of $\frac{2\pi}{n}$ and a flip over the $y-$axis. If we denote the rotation by r and the flip by s, one can see geometrically that $r^n = e = s^2$ and that $srs = r^{-1}$. This is often written as the presentation

$$D_n = \langle r, s | r^n = s^2 = e, srs = r^{-1} \rangle.$$

Can you show that half the elements of D_n have order 2?

Symmetric Groups

Symmetric groups may be considered the most important example here. We will study these more carefully later and we will also show that any group may be realized as a subgroup of a symmetric group. Fro now, we will outline what the symmetric groups are.

Let A be a set, we let $S_A = \{f : A \longrightarrow A | f \text{ is bijective.}\}$. Note that the bijectivity is important to ensure that ever element has an inverse. For convenience of notation we denote by the cycle

$$(a_1\ a_2\ \cdots\ a_n)$$

the function that takes a_i to a_{i+1} and a_n to a_1. It can be shown that every element fo S_n can be written as a product of disjoint cycles.

The operation here is function composition. For instance, we have

$$(1\ 2\ 5\ 6\ 4)(2\ 1\ 4\ 5)(1\ 3)(4\ 3)(3\ 6\ 2) = (1\ 3\ 4)(2\ 6)(5)$$

It is fairly easy to show that if $n \geq 3$ then S_n is nonabelian, and that disjoint cycles commute. We will look more deeply at S_n later.

See if you can realize D_n as a subgroup of an appropriate S_m.

Matrix Groups

First we recall that a field ($\mathbb{F}$) is a set with two binary operations $(+, \cdot)$ such that $(\mathbb{F}, +)$ and $(\mathbb{F} \setminus \{0\}, \cdot)$ are abelian groups and the operations come together through the distributive property

$$a(b + c) = ab + ac, \text{ for all } a, b, c \in \mathbb{F}.$$

A fact that we will show later is that if $\mathbb{F}$ is a finite field, then $|\mathbb{F}| = p^n$ where p is a positive prime number. We introduce the following notation

1. $\mathrm{M}_n(\mathbb{F})$ is the collection of $n \times n$ matrices over $\mathbb{F}$
2. $\mathrm{GL}_n(\mathbb{F})$ is the collection of $n \times n$ matrices over $\mathbb{F}$ with nonzero determinant.
3. $\mathrm{SL}_n(\mathbb{F})$ is the collection of $n \times n$ matrices over $\mathbb{F}$ with determinant 1

Note that the first is a group under matrix addition and the next two are groups under matrix multiplication.

Theorem 2.2.1. *If $\mathbb{F}$ is a finite field with $q = p^m$ elements, then*

$$|GL_n(\mathbb{F})| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$$

Proof. Let $M \in \mathrm{GL}_n(\mathbb{F})$. Think of building M constructively, row-by-row. This first row can be any $n-$vector over $\mathbb{F}$ except the zero vector. The second row can be any vector not in the span of the first vector (so there are $q^n - q$ choices). The third row can be any vector that is not in the span of the first two rows (leaving $q^n - q^2$ choices). Continuing this gives the desired result. □

The Group of Quaternions

The group of quaternions has some interesting connections with physics. The group is given by

$$\mathrm{Q}_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with the relations $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j$.

Free Groups (Words)

Given any set of symbols $\mathbb{A} = \{a_i | i \in I\}$ one can form the free group on this set, $F = F(\mathbb{A})$ where the elements are "words" formed by finite concatenations of elements of the form a_i and a_j^{-1}. So a typical element is a "word" of the form $a_{i_1}^{\epsilon_1} a_{i_2}^{\epsilon_2} \cdots a_{i_m}^{\epsilon_m}$ where each $i_k \in I$ and $\epsilon_i = \pm 1$. Verify that this collection is a group under concatenation.

2.3 Morphisms

Morphisms are functions that preserve algebraic structure. Morphisms are the key tools for comparing algebraic structures. For example, $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ are sets of the same size, but group-theoretically, they are different.

Definition 2.3.1. *Let $(G, \circ)$ and $(H, *)$ be groups. A function $\phi : G \longrightarrow H$ such that $\phi(x \circ y) = \phi(x) * \phi(y)$ for all $x, y \in G$ is called a homomorphism of groups.*

If $\phi : G \longrightarrow H$ is a homomorphism of groups, we say that ϕ is injective or a monomorphism if ϕ is one to one, we say that ϕ is an epimorphism or surjective if ϕ is onto. A homomorphism that is bijective is called an isomorphism. An isomorphism $\phi : G \longrightarrow G$ is an automorphism. These are especially important because, as we will see later, the collection of automorphisms of G forms a group in its own right (under function composition).

Given any group, G, the identity map from G to itself is an isomorphism. The map $\phi : G \longrightarrow e$ is surjective. The exponential and natural logarithm map are isomorphisms between the additive group of the reals and the multiplicative group of positive reals.

Example 2.3.2. *Consider the isomorphism between D_3 and S_3 that takes the rotation r to $(1\ 2\ 3)$ and the flip s to $(2\ 3)$.*

Theorem 2.3.3. *Let $\phi : G \longrightarrow H$ be a homomorphism.*

a) $\phi(1_G) = 1_H$.

b) $\phi(x^n) = (\phi(x))^n$ and $\phi(x^{-1}) = (\phi(x))^{-1}$.

c) If $|x| = n < \infty$ then $|\phi(x)|$ divides $|x|$ (and we have equality if ϕ is an isomorphism).

d) If ϕ is an isomorphism then $|G| = |H|$.

e) If ϕ is an isomorphism then G is abelian if and only if H is abelian.

Proof. Exercise. □

Exercises

1. . Let G be a finite group. Show that any element of G has finite order.
2. Show that any group of exponent 2 is abelian.
3. The goal of this problem is to show that any *finite* group generated by two elements of order two is dihedral (with $\mathbb{Z}_2 \times \mathbb{Z}_2$ being considered a "degenerate" dihedral group). Suppose that G is generated by the elements $x, y \in G$, both of order 2.

a) Assuming that the order of G is finite, what can you say about the order of the element $xy \in G$?

b) Show that the group generated by x and y is the same as the group generated by xy and y

c) Show that the group generated by x and y is dihedral.

4. Let G be a group. Recall that the center of G is defined by $\mathrm{Z}(G) = \{z \in G | zg = gz,\ \forall g \in G\}$. Compute $\mathrm{Z}(\mathrm{D}_n)$.

5. For this problem we consider the dihedral and symmetric groups.

a) Show that if n is odd then precisely half of the elements of D_n have order 2.

b) Find an element of the largest possible order in S_{15}.

Chapter 3

Subgroups

3.1 Basics and First Examples

Subgroups are smaller groups within an existing group. Much about the parent group can be gleaned from understanding its subgroups. At the same time, knowing the subgroups of a given groups is often quite important. For example, understanding the subgroups of the Rubik's group is important in finding optimal solutions. Additionally, algebraic objects can often be associated to geometric structures (and vice versa) and subgroups may correspond to important geometric subobjects.

Definition 3.1.1. *Let G be a group. $H \subseteq G$ is called a subgroup if H is a group in its own right (with operation inherited from G).*

Proposition 3.1.2. *$H \subseteq G$ is a subgroup if and only if for all $x, y \in H, xy^{-1} \in H$.*

Proof. One direction (if H is a subgroup) is pretty clear. So suppose that for all $x, y \in H$ we have that $xy^{-1} \in H$. Since $x, x \in H$, $xx^{-1} = e \in H$. Now since $e \in H$, we have that $ex^{-1} = x^{-1} \in H$. Finally note that if $x, y \in H$, we have shown that $y^{-1} \in H$. So we have that $x(y^{-1})^{-1} = xy \in H$. □

Example 3.1.3. *$\mathbb{Z} \subseteq \mathbb{Q}$. Also note that D_n can be realized as a subgroup of S_n. Compare and constrast the subgroups of S_3 and $\mathbb{Z}_6$.*

We now introduce a concept that we will study more extensively later. Its utility at this juncture is to give interesting examples of subgroups.

Definition 3.1.4. *A group action of the group G on the set A is a map $G \times A \longrightarrow A$ (written $g \cdot a$) such that*

a) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, $g_1, g_2 \in G$, $a \in A$.

b) $e \cdot a = a$ for all $a \in A$.

Perhaps the easiest example of a group acting on a set is for a group G to act on itself by left multiplication($g \circ x = gx$) or by conjugation ($g \circ x = gxg^{-1}$). Invertible matrices acting on $\mathbb{R}^n$ is an example that you may have encountered in a linear algebra course. Also a very large group acts on the Rubik's cube by function composition.

Definition 3.1.5. *Let $A \subseteq G$ be a nonempty subset.*

a) $C_G(A) = \{g \in G | g^{-1}ag = a, \forall a \in A\}$, *the centralizer of A in G.*

b) $Z(G) = \{g \in G | gx = xg, \forall x \in G\}$, *the center of G.*

c) $N_G(A) = \{g \in G | g^{-1}Ag = A\}$, *the normalizer of A in G.*

Note that it is immediate that both $\mathrm{C}_G(A)$ and $\mathrm{N}_G(A)$ are groups and $\mathrm{C}_G(A) \subseteq \mathrm{N}_G(A)$. We record the following.

Theorem 3.1.6. *$C_G(A) \subseteq N_G(A)$ are subgroups of G as is $Z(G) = C_G(G)$.*

Proof. Exercise. □

Theorem 3.1.7. *Let G act on the set S. The following are subgroups of G.*

a) $G_s = \{g \in G | gs = s\}$ *(the stabilizer of s).*

b) $K = \{g \in G | gs = s, \forall s \in S\}$ *(the kernel of the action).*

Proof. a) Let $x, y \in G_s$. Since $ys = s$, $es = s = y^{-1}s$. Hence $(xy^{-1})s = x(y^{-1}s) = xs = s$ and so $xy^{-1} \in G_s$. So G_s is a subgroup of G.
b) Let $x, y \in K$. Then for all $s \in S$ $xs = s = ys$. As in the previous proof, we have that $y^{-1}s = s$ and so $xy^{-1}s = s$. □

Theorem 3.1.8. *Let $\phi : G \longrightarrow H$ be a homomorphism. The following are subgroups (of G and H respectively).*

a) $ker(\phi) = \{g \in G | \phi(g) = e_H\}$.

b) $im(\phi) = \{\phi(g) | g \in G\}$.

Proof. a) Let $x, y \in \ker(\phi)$. Since $\phi(y) = e = e^{-1} = (\phi(y))^{-1} = \phi(y^{-1})$, then $y^{-1} \in \ker(\phi)$. So $\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = e$ and so $\ker(\phi)$ is a subgroup of G.
b) Let $a, b \in \mathrm{im}(\phi)$. We write $a = \phi(x)$ and $b = \phi(y)$. Note that previous results give that $b^{-1} = \phi(y^{-1})$ and so $ab^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1})$. Hence $\mathrm{im}(\phi)$ is a subgroup of H. □

Exercise 3.1.9. *Let $\phi : G \longrightarrow H$ be a homomorphism. As an exercise, show the following.*

1. $N_G(ker(\phi)) = G$.
2. *ϕ is onto if and only if* $im(\phi) = H$.
3. *ϕ is one to one if and only if* $ker(\phi) = e$.

3.2 The Classification of Cyclic Groups

Cyclic groups are the groups that are generated by a single element. More precisely, we give the following definition.

Definition 3.2.1. *We say that G is cyclic if there is an $x \in G$ such that*

$$G = \{x^n | n \in \mathbb{Z}\}.$$

We say, in this case, that $G = \langle x \rangle$.

Note that G is not necessarily infinite, the above listed set may have an enormous amount of repetition.

Example 3.2.2. *$\mathbb{Z}_n$ and $\mathbb{Z}$ are cyclic groups. And, in a certain sense, this list is exhaustive.*

Proposition 3.2.3. *If $G = \langle x \rangle$ then $|G| = |x|$.*

Proof. (Note that in any event, $|G| \geq |x|$ and $\langle x \rangle \subseteq G$.) Suppose first that $G = \langle x \rangle$ and G is finite. It suffices to show that $|G| \leq |x|$. Since every element of G is a power of x (say $g_k = x^k$), the map $f : I \longrightarrow G$ (I is the collection of positive integers less than or equal to $|x|$) is a surjection. This establishes the proposition in the finite case. For the case where G is of infinite order, it is clear that the generator x cannot be of finite order. □

Proposition 3.2.4. *Suppose G is a group, $x \in G$ and $m, n \in \mathbb{Z}$. If $x^m = 1 = x^n$ then $x^{gcd(m,n)} = 1$.*

Proof. We know that if $d = \gcd(m, n)$ then there exist $a, b \in \mathbb{Z}$ such that $am + bn = d$. Hence $x^d = x^{am+bn} = (x^m)^a (x^n)^b = 1$. □

Theorem 3.2.5. *Any two cyclic groups of the same order are isomorphic (so an exhaustive list of the cyclic groups are $\mathbb{Z}$ and $\mathbb{Z}_n$ for $n \in \mathbb{N}$).*

Proof. (Sketch) If $G = \langle x \rangle$ is of infinite order, then the map $n \longrightarrow x^n$ from $\mathbb{Z}$ to G is an isomorphism. Use the previous result to establish the finite case (show that if G is of order n and is finite then $G \cong \mathbb{Z}_n$). □

Theorem 3.2.6. *Let G be a group and $x \in G$ of order $n \leq \infty$.*

a) If $n = \infty$ then $|x^a| = \infty$ for all $a \neq 0$

b) If $n < \infty$ then $|x^a| = \frac{n}{gcd(a,n)}$.

Proof. For the first statement, suppose that the order of x is infinite and consider $z = x^a$. If $z^m = 1$ then $x^{am} = 1$ and this is a contradiction.

For the second statement, we first note that $(x^a)^{\frac{n}{\gcd(a,n)}} = (x^n)^{\frac{a}{\gcd(a,n)}} = 1$ and hence the order of x^a is a divisor of $\frac{n}{\gcd(a,n)}$. Now suppose that $(x^a)^d = 1$. Hence ad must be a multiple of $|x| = n$ and so $nk = ad$ for some $k \in \mathbb{Z} \setminus \{0\}$. We write $a = a' \gcd(a, n)$ and note that $\gcd(a', n) = 1$. Since $nk = a' \gcd(a, n)d$, it must be the case that a' divides k (say $k = a'k'$). We now have that $nk' = \gcd(a, n)d$, and hence $\frac{n}{\gcd(a,n)}$ divides d and we are done. □

Here are a couple of theorems that round out our structural observations concerning cyclic groups,

Theorem 3.2.7. *Let $H = \langle x \rangle$.*

1. *If $|x| = \infty$ then $\langle x^a \rangle = H$ if and only if $a = \pm 1$.*
2. *if $|x| = n < \infty$ then $\langle x^a \rangle = H$ if and only if $gcd(a, n) = 1$ (and hence the number of generating elements of H is $\phi(n)$).*

Proof. 1. Suppose $|a| > 1$. If $\langle x^a \rangle = H$ then $x \in \langle x^a \rangle$. Hence $(x^a)^d = x$ for some $d \in \mathbb{Z}$. Since the order of x is infinite, we must have that $ad = \pm 1$, but $|ad| > 1$ for all $d \neq 0$, making such a solution impossible. The other direction is easier.
2. Suppose that $\langle x^a \rangle = H$. Then it must be the case that $x \in \langle x^a \rangle$. Since the order of x is n, we must have for some $d \in \mathbb{Z}$ that $ad \equiv 1 \mathrm{mod}(n)$. But we have seen that this equation is solvable if and only if $\gcd(a, n) = 1$. On the other hand, if $\gcd(a, n) = 1$ then we can find a $c \in \mathbb{Z}$ such that $ca \equiv 1 \mathrm{mod}(n)$ and so $(x^a)^c = x$. Hence $H \subseteq \langle x^a \rangle$ and the other containment is clear. □

Theorem 3.2.8. *Let $G = \langle x \rangle$ be a cyclic group.*

1. *Any subgroup of G is cyclic.*
2. *If $|G| = n$ then there is a unique subgroup of G of order a for every positive divisor a of n.*

Proof. 1. Let H be a (nonidentity) subgroup of G and let $A = \{k \in \mathbb{N} | x^k \in H\}$. If $a \in A$ is the least element, use the Euclidean algorithm to show that $H = \langle x^a \rangle$.

2. Suppose that a divides n. Let $H = \{x \in G | x^a = 1\}$. Verify that H is a subgroup of G and contains all elements of G of order a (by definition). We also note that H is cyclic and hence must be generated by an element of order a (such elements exist, for example $x^{\frac{n}{a}}$), so H has precisely a elements. For uniqueness, suppose that there is another subgroup of order a, say K. We wish to show that $H = K$. Note that $K = \langle x^k \rangle$ and $|x^k| = a$. Since the order of x^k is a, this shows that $K \subseteq H$ and since $|K| = |H|$ we have that $K = H$. □

We close out with a couple of remarks concerning intersections and generating sets for groups.

Proposition 3.2.9. *If $\{H_i | i \in \Gamma\}$ is a nonempty collection of subgroups of a group G then $\bigcap_{i \in \Gamma} H_i \leq G$.*

Proof. Let $x, y \in \bigcap_{i \in \Gamma} H_i$ then for all i, $x, y^{-1} \in H_i$. Hence $xy^{-1} \in H_i$ for all i. So $xy^{-1} \in \bigcap_{i \in \Gamma} H_i$ and hence $\bigcap_{i \in \Gamma} H_i$ is a subgroup of G. □

Definition 3.2.10. *Let $A \subseteq G$ be a subset. We define the subgroup generated by A as*

$$\langle A\rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H$$

$\langle A\rangle$ is referred to as the subgroup of G generated by the set A.

Proposition 3.2.11. *Let A be a nonempty set. Then $\langle A\rangle = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n} | a_i \in A, \epsilon_i = \pm 1\}$.*

We remark that if $S = \emptyset$ then $\langle A\rangle = \{e\}$.

Chapter 4

Quotient Groups and Homomorphisms

4.1 Normal Subgroups and Quotients

We begin with a fundamental definition.

Definition 4.1.1. *Let $N \leq G$ be a subgroup. We say that $N \trianglelefteq G$ ("N is normal in G") if and only if $g^{-1}Ng = N$ for all $g \in G$ (equivalently $g^{-1}ng \in N$ for all $n \in N, g \in G$ and also equivalently $N_G(N) = G$).*

Example 4.1.2. *Find the normal subgroups of S_3. Note that any subgroup of an abelian group is normal.*

Proposition 4.1.3. *Let G and H be groups and $\phi : G \longrightarrow H$ a homomorphism.*

1. *If G is abelian, then any subgroup of G is normal in G.*
2. *$ker(\phi) \trianglelefteq G$.*

Proof. Exercise. □

Let $H \leq G$, we now define the notion of a (right or left) coset of H in G.

Definition 4.1.4. *Let $H \leq G$ be a subgroup, and let $g \in G$. We define the left coset gH to be $gH = \{gh | h \in H\}$. Similarly, we define the right coset Hg to be $Hg = \{hg | h \in H\}$. An element of any coset (left or right) is called a representative of that coset.*

Example 4.1.5. *Look at right and left cosets of $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$ in S_3. Contrast that with what you get when you use the subgroup $\{e, (1\ 2)\}$. Count the right and left coset of the even integers as a subgroup of $\mathbb{Z}$.*

Theorem 4.1.6. *Let $H \leq G$ be a subgroup. The collection of left (resp. right) cosets of H in G form a partition of G. In other words, $G = \bigcup_{g \in G} gH$ and if $g_iH \bigcap g_jH \neq \emptyset$ then $g_iH = g_jH$.*

Remark 4.1.7. *We refer to the number of distinct cosets of H in G as the index of H in G.*

Proof. If $g \in G$ then $g \in gH$ and so $G = \bigcup_{g \in G} gH$. We now suppose that for $x, y \in G$, there is an element $z \in xH \bigcap yH$. We write $z = xh_1 = yh_2$ for $h_1, h_2 \in H$. Note that $x = yh_2h_1^{-1} \in yH$. So if $xh \in xH$ then $xh = yh_2h_1^{-1}h \in yH$. We now have that $xH \subseteq yH$ and by symmetry, we have that $yH \subseteq xH$. This establishes the theorem. □

Proposition 4.1.8. *Let $H \leq G$ be a subgroup and let $x, y \in G$. Then $xH = yH$ if and only if $x^{-1}y \in H$.*

Proof. Suppose first that $xH = yH$. Since $y \in iH = xH$, there is an $h \in H$ such that $y = xh$. Hence $x^{-1}y = h \in H$.

For the other direction, suppose that $x^{-1}y = h \in H$, then $y = xh \in xH \bigcap yH$. Since the left cosets form a partition of G, we must have $xH = yH$. □

Proposition 4.1.9. *Let $N \leq G$ be a subgroup. $N \trianglelefteq G$ if and only if $gN = Hg$ for all $g \in G$ (that is, each left coset is a right coset as well).*

Proof. Suppose first that $N \trianglelefteq G$ and let $gn \in gN$. Since N is normal in G, $gng^{-1} = n_1 \in N$. Hence $gn = n_1g \in Ng$ and so $GN \subseteq Ng$. By symmetry we have $gN = Ng$.

For the other direction, suppose that $gN = Ng$ for all $g \in G$ and consider the element $gng^{-1} = x \in G$. Since $gN = Ng$ we can write $gn = n_1g$ for some $n_1 \in N$. So $x = gng^{-1} = n_1gg^{-1} = n_1 \in N$ and so $N \trianglelefteq G$. □

Notation 4.1.10. *Let G be a group and N a normal subgroup of G. We denote the set of left (right) cosets of N in G by $G/N = \{gN | g \in G\}$.*

Theorem 4.1.11. *Let G be a group and $N \trianglelefteq G$. Then the set of left cosets of N in G, G/N forms a group with the binary operation on the set of cosets given by:*

$$(g_1N)(g_2N) = g_1g_2N$$

Remark 4.1.12. *G/N is called a quotient group or a factor group. Can you describe G/e and G/G?*

Proof. We first need to show that this operation is well defined (that is, if different coset representatives are selected, we must get the same outcome). To this end, suppose that $xN = yN$ and $uN = vN$ for elements $u, v, x, y \in G$. Since $xN = yN$, $x^{-1}y, y^{-1}x \in N$ and similarly $u^{-1}v, v^{-1}u \in N$. Note now that $v^{-1}y^{-1}xu = v^{-1}y^{-1}xvv^{-1}u = (v^{-1}y^{-1}xv)(v^{-1}u) \in N$. Hence $v^{-1}y^{-1}xu \in N$ and hence $xuN = yvN$ and the multiplication is well-defined. The rest of the verificatin is straightforward as eN is the identity, associativity is inherited from G, and $(gN)^{-1} = g^{-1}N$. □

The next result is a compact compilation of previous results, so we will omit the proof.

Theorem 4.1.13. *The following conditions are equivalent.*

1. $K \trianglelefteq G$
2. $N_G(K) = G$.
3. $gK = Kg$ *for all* $g \in G$.
4. G/K *is a group.*

Here is another interesting way to characterize normal subgroups: a subgroup of G is normal if and only if it is the kernel of some homomorphism with domain G. But first we give a first utility result and leave the proof as an exercise.

Proposition 4.1.14. *Let G be a group and N a normal subgroup. The function*

$$\pi : G \longrightarrow G/N$$

given by $\pi(g) = gN$ is a surjective homomorphism (called the natural or canonical projection).

Proposition 4.1.15. *Let N be a subgroup of G. $N \trianglelefteq G$ if and only if $N = ker(\phi)$ for some homomorphism $\phi : G \longrightarrow H$.*

Proof. Suppose first that $N \trianglelefteq G$, then N is precisely the kernel of the canonical projection $\pi : G \longrightarrow G/N$.

On the other hand, suppose that $N = \ker(\phi)$ for some homomorphism $\phi : G \longrightarrow H$. We have already seen that $\ker(\phi)$ is always normal and so the result is established. □

Exercises

1. Consider the map $\phi : G \longrightarrow G$ given by $\phi(x) = x^{-1}$.
   a) Show that ϕ is a homomorphism if and only if G is abelian.
   b) Show that if ϕ is a homomorphism, then ϕ is an automorphism (an isomorphism from G to itself).
   c) Show that if f is any homomorphism and $|x|$ is finite, then $|f(x)|$ divides $|x|$.
2. Consider the group, G, generated (multiplicatively) by the following two matrices with entries in $\mathbb{Z}$.

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

   Show, with justification, that G is isomorphic to D_n for an appropriate value of n.

3. Let G be a group. We define $\mathrm{Aut}(G) = \{\phi : G \longrightarrow G |\ \phi \text{ is an automorphism.}\}$.

   a) Show that $\mathrm{Aut}(G)$ is a group.

   b) Suppose we define $\phi_g : G \longrightarrow G$ by $\phi_g(x) = gxg^{-1}$. Show that $\phi_g \in \mathrm{Aut}(G)$.

   c) Show that the correspondence $g \longrightarrow \phi_g$ is a homomorphism from G to $\mathrm{Aut}(G)$. What is its kernal?

   d) Consider the collection of all $\phi_g,\ g \in G$ (we call this collection $\mathrm{Inn}(G)$, the inner automorphisms of G). Show that $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$. Is it a normal subgroup of $\mathrm{Aut}(G)$?

4. Let G be a group and $x, y \in G$. We say that the *commutator* of x and y (sometimes denoted $[x, y]$) is $[x, y] = x^{-1}y^{-1}xy$. Globally, we define the *commutator subgroup* of G to be

$$G' = \langle [x, y] | x, y \in G \rangle.$$

   a) Show that the elements $x, y \in G$ commute if and only if $[x, y] = 1$.

   b) Show that G' is a normal subgroup of G.

   c) Show that if N is a normal subgroup of G, then G/N is abelian if and only if N contains G'.

5. Let G be a group and $\phi : G \longrightarrow H$ be a homomorphism. Show that $\mathrm{Z}(G)$ and $\ker(\phi)$ are normal subgroups of G.

6. Let G be a group and H a subgroup of G such that $[G : H] = 2$. Show that $H \trianglelefteq G$. Is the same true if $[G : H] = 3$?

7. Let G be a group with center $\mathrm{Z}(G)$. Show that G is abelian if and only if $G/\mathrm{Z}(G)$ is cyclic.

8. In this problem we produce some examples that illustrate some things that can happen with normal subgroups.

   a) Show that every subgroup of the quaternion group Q_8 is normal.

   b) Show that if $N \trianglelefteq G$ and H is a subgroup of G then $(N \bigcap H) \trianglelefteq H$.

   c) Is it true that if $K \trianglelefteq H$ and $H \trianglelefteq G$ then $K \trianglelefteq G$? Prove or give a counterexample.

9. Let G be a group and $x, y \in G$ of orders m, n respectively.

   a) Show that $|x^{-1}| = |x|$.

   b) Show that if $x^k = e$ then m divides k.

   c) If $xy = yx$ then $|xy|$ divides $\mathrm{lcm}(m, n)$.

   d) Show if $xy = yx$ and $\langle x \rangle \bigcap \langle y \rangle = e$ then $|xy| = \mathrm{lcm}(m, n)$.

10. Consider the set of matrices given by $G := \left\{ \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \middle| \theta \in \mathbb{R} \right\}$.

    a) Show that G is a group.

    b) Show that the operation given by $M \circ \mathbf{v} = M\mathbf{v}$ for $M \in G$ and $\mathbf{v} \in \mathbb{R}^2$ is an action of G on $\mathbb{R}^2$.

    c) Explain geometrically how this action works.

4.2 Counting and Lagrange's Theorem

We first recall that if G is a group and $H \leq G$ is a subgroup then G is partitioned by the left cosets of H in G. We begin with a final simple but important observation concerning cosets.

Lemma 4.2.1. *Let $H \leq G$ be a subgroup and X, Y be two left (right) cosets of H in G. Then $|X| = |Y|$.*

Proof. We show this for left cosets only, the proof for right cosets is highly similar. Suppose that xH, yH are two (left) cosets of H in G (that is, $x, y \in G$). Consider the function $f : xH \longrightarrow yH$ given by $f(xh) = yh$. Note that if $f(xh_1) = f(xh_2)$ then $yh_1 = yh_2$ and hence $h_1 = h_2$ and so f is one to one. By symmetry we have $|xH| = |yH|$. □

Theorem 4.2.2 (Lagrange's Theorem)**.** *Let G be a finite group and $H \leq G$ a subgroup. Then $|H|$ divides $|G|$ and the quotient $\frac{|G|}{|H|}$ is the number of left (right) cosets of H in G.*

Proof. Since the left cosets of H in G partition G, we can write G as a *disjoint* union of its left cosets:

$$G = \bigcup_{i \in I}^{\bullet} g_i H$$

As the union is disjoint, $|G| = \sum_{i \in I} |g_i H|$ and as G is finite, the index set is finite (say $|I| = k$). Noting this and the previous lemma, we can refine this sum to $|G| = k|H|$. Hence the order of H divides the order of G and k is the number of distinct left cosets. □

Definition 4.2.3. *The number of distinct (left) cosets of H in G is called the index of H in G and is denoted $[G : H]$ (this is the k from the proof of the previous theorem).*

Exercise 4.2.4. *Find a formula for $[\mathbb{Z} : n\mathbb{Z}]$ where $n \in \mathbb{N}_0$.*

Corollary 4.2.5. *If G is finite and $x \in G$ then $|x|$ divides $|G|$.*

Proof. We have seen that $|x| = |\langle x \rangle|$. Apply the previous theorem. □

Corollary 4.2.6. *If $|G| = p$ where p is a positive prime, then $G \cong \mathbb{Z}_p$.*

Proof. Let $x \in G$ be a nonidentity element. Then $|x| = p$ and so $\langle x \rangle = G$ (so G is cyclic). Since $|G| = p$ and G is cyclic, we have seen that $G \cong \mathbb{Z}_p$. □

The next theorem is one of our first applications of group actions and is a fundamental result concerning the structure of groups.

Theorem 4.2.7 (Cauchy's Theorem)**.** *Let G be a finite group of order n and p a positive prime such that $p|n$, then there is an element $x \in G$ such that $|x| = p$.*

Proof. We form the set S as follows:

$$S := \{(a_1, a_2, \cdots, a_p) | a_1 a_2 \cdots a_p = e\},$$

and we first count the number of elements in S. Note that we can choose $a_1, a_2, \cdots, a_{p-1}\}$ with impunity and a_p is determined by the constraint (that is, $a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$). We let the $\mathbb{Z}_p$ act on S as follows: if $\overline{j} \in \mathbb{Z}_p$ then $\overline{j} \cdot (a_1, a_2, \cdots, a_p) = (a_{1+j}, a_{2+j}, \cdots, a_p, a_1, \cdots, a_{p+j})$ where the subscripts are taken modulo p (verify that this is indeed a group action).

Note that $|S| = |G|^{p-1} = n^{p-1}$ and the group action partitions the set S into equivalence classes. To see this we declare an equivalence relation on S via $(x_1, x_2, \cdots, x_p) \sim (y_1, y_2, \cdots, y_p)$ if and only if there is a $0 \leq j \leq p-1$ such that $y_i = x_{\overline{i+j}}$ where $\overline{i+j}$ is the integer in the interval $[0, p-1]$ equivalent to $i + j$ modulo p.

Note that $\sim$ is reflexive (take $j = 0$), symmetric ($j_2 = p - j$ reverses the j shift), and transitive. For the transitivity, suppose that $(x_1, x_2, \cdots, x_p) \sim (y_1, y_2, \cdots, y_p)$ and $(y_1, y_2, \cdots, y_p) \sim (z_1, z_2, \cdots, z_p)$. Then there exist $0 \leq j, k \leq p-1$ such that $y_i = x_{\overline{i+j}}$ and $z_i = y_{\overline{i+k}}$. Hence $z_i = x_{\overline{i+j+k}}$ and so $(x_1, x_2, \cdots, x_p) \sim (z_1, z_2, \cdots, z_p)$ and we have transitivity.

Since $\sim$ is an equivalence relation, $\sim$ partitions S into equivalence classes. We now claim that hat each equivalence class contains 1 or p elements (certainly no equivalence class can contain more than p elements). Suppose that there is an equivalence class containing $(x_1, x_2, \cdots, x_p)$ and this equivalence class contains less than p elements. Then there must be some $1 \leq j \leq p-1$ such that $x_i = x_{\overline{i+j}}$ for all $0 \leq i \leq p-1$. Hence we have that $x_1 = x_{\overline{1+j}} = x_{\overline{1+2j}} = \cdots = x_{\overline{1+(p-1)j}}$. Now observe that if $0 \leq m < k \leq p-1$ and $\overline{1+mj} = \overline{1+kj}$ then $(k-m)j \equiv 0 \mathrm{mod}(p)$, but since $1 \leq k - m, j \leq p-1$, we have a contradiction. So the listed elements are all the same and so each equivalence class has either p or 1 element.

Since S is partitioned by $\sim$, then we write $|S| = P + r$ where P is the number of elements in all equivalence classes of size p and r is the number of equivalence classes of size 1. Note $|S| \equiv P + r \mathrm{mod}(p)$. But we already know that $P, |S| \equiv 0 \mathrm{mod}(p)$. Hence $r \equiv 0 \mathrm{mod}(p)$. But $r \neq 0$ as the cycle $(e, e, \cdots, e)$ is an equivalence class of size 1. Hence there must be a nontrivial $x \in G$ such that $(x, x, \cdots, x)$ is in an equivalence class of size 1. So $x^p = e$ and we are done. □

In fact, we will see later that if G is a group and $|G| = p^a m$ with $\gcd(p, m) = 1$, then G has a subgroup of order p^a. Now on with the counting:

Definition 4.2.8. *Let $H, K \leq G$, then we define $HK = \{hk | h \in H, k \in K\}$.*

Theorem 4.2.9. *If H and K are finite subgroups of G then*

$$|HK| = \frac{|H||K|}{|H \bigcap K|}$$

Proof. Let $HK = \bigcup_{h \in H} hK$, so it is our burden to find the number of *distinct* left cosets of the form hK. To this end, suppose that for $h_1, h_2 \in H$, $h_1K = h_2K$. We have see that means that $h_2^{-1}h_1 \in K$ (and hence $h_2^{-1}h_1 \in H \bigcap K$). From this, we can conclude that $h_1(H \bigcap K) = h_2(H \bigcap K)$.

So the number of these distinct cosets in G of the form hK is the number of distinct cosets of $H \bigcap K$ in H. We now have that

$$|HK| = \frac{|H|}{|H \bigcap K|}|K| = \frac{|H||K|}{|H \bigcap K|}$$

and this concludes the proof. □

In general HK is not a subgroup of G. The following theorem characterizes when this actually does happen.

Theorem 4.2.10. *Let $H, K \leq G$ be subgroups. HK is a subgroup of G if and only if $HK = KH$.*

Proof. ($\Longrightarrow$) Suppose that HK is a subgroup of G and let $h \in H$ and $k \in K$. Since $hk \in HK$, $(hk)^{-1} \in HK$. Hence $(hk)^{-1} = k^{-1}h^{-1} \in KH$. Hence $HK \subseteq KH$. By symmetry, $KH \subseteq HK$ and we have the desired equality.

($\Longleftarrow$) Now suppose that $HK = KH$ and suppose that $h_1k_1, h_2k_2 \in HK$. Then $(h_1k_1)(h_2k_2)^{-1} = k_2^{-1}h_2^{-1}h_1k_1$. But since $k_2^{-1}h_2^{-1}h_1 \in KH = HK$ we can write $k_2^{-1}h_2^{-1}h_1 = hk$ for some $h \in H, k \in K$. So $(h_1k_1)(h_2k_2)^{-1} = hkk_1 \in HK$ and we are done. □

Corollary 4.2.11. *Let $H, K \leq G$ with $H \leq N_G(K)$ then HK is a subgroup of G (in particular, if $K \trianglelefteq G$ then $HK \leq G$).*

Proof. Suppose that $H \leq N_G(K)$. Hence for all $h \in H$, $hkh^{-1} \in K$ for all $k \in K$. Hence for all $hk \in HK$, $hkh^{-1} = k_1 \in K$ and so $hk = k_1h \in KH$ and so $HK \subseteq KH$. For the other containment, if $kh \in KH$, then write $kh = h(h^{-1}kh) \in HK$ and we are done. □

Remark 4.2.12. *If $A \subseteq N_G(K)$, we say that A normalizes K and if $A \subseteq C_G(K)$ we say A centralizes (or commutes with) K.*

Here is one last counting result. The proof is an exercise.

Theorem 4.2.13. *Let $H \leq K \leq G$ then $[G : H] = [G : K][K : H]$.*

Proof. This proof is easiest in the case where G is finite, but it is true in the general case as well. Let $\{g_jK|j \in \Lambda\}$ be the left cosets of K in G and $\{k_iH|j \in \Delta\}$ be the left cosets of H in K. we claim that the collection $\{g_jk_iH|(j,i) \in \Lambda \times \Delta\}$ is an exhaustive list of distinct cosets of H in G. Note that if $g_jk_iH = g_ak_bH$ then $k_iH = g_j^{-1}g_ak_bH$ and since $H \subseteq K$ then $g_j^{-1}g_a \in K$ and hence $g_jK = g_aK$ and so $j = a$. But then $k_iH = k_bH$ and hence $i = b$. Hence this is an exhaustive list of the cosets and since $|\Lambda \times \Delta| = |\Lambda||\Delta|$ and this proves the theorem. □

4.3 The Isomorphism Theorems

Theorem 4.3.1 (The First Isomorphism Theorem)**.** *If $\phi : G \longrightarrow H$ then $ker(\phi) \trianglelefteq G$ and ϕ induces an isomorphism*

$$\overline{\phi} : G/ker(\phi) \xrightarrow{\cong} im(\phi)$$

where $\overline{\phi}(gker(\phi)) = \phi(g)$.

Proof. We have already seen that the kernel of any homomorphism is normal. So we construct $\overline{\phi} : G/\ker(\phi) \longrightarrow \text{im}(\phi)$ via $\overline{\phi}(g\ker(\phi)) = \phi(g)$. We must first show that $\overline{\phi}$ is well-defined. To this end, suppose that $g_1\ker(\phi) = g_2\ker(\phi)$. We know that this means that $g_2^{-1}g_1 \in \ker(\phi)$ and so $\phi(g_2^{-1}g_1) = e_H = (\phi(g_2))^{-1}\phi(g_1)$. Hence we have that $\phi(g_1) = \phi(g_2)$ and so $\overline{\phi}(g_1\ker(\phi)) = \overline{\phi}(g_2\ker(\phi))$. Therefore $\overline{\phi}$ is well-defined.

To see that $\overline{\phi}$ is one to one, we suppose that $\overline{\phi}(g\ker(\phi)) = e_H$. Then, by definition, $\phi(g) = e_H$ and so $g \in \ker(\phi)$ and $g\ker(\phi) = \ker(\phi)$. So $\overline{\phi}$ is one to one.

Since ϕ is automatically onto its image, $\overline{\phi}$ must be onto. □

Theorem 4.3.2 (Second Isomorphism Theorem)**.** *Let $H, K \leq G$ and assume that $H \leq N_G(K)$, then $H \bigcap K \trianglelefteq H$ and $HK/K \cong H/(H \bigcap K)$.*

Proof. By our previous work, we know that $HK \leq G$. Also note that if $x \in H \bigcap K$ and $h \in H$, then $h^{-1}xh \in H \bigcap K$ by assumption and so $H \bigcap K \trianglelefteq H$. So show that the quotient groups are isomorphic, we start with the homomorphism $\phi : H \longrightarrow HK/K$ given by $\phi(h) = he_KK$ (verify that ϕ is a homomorphism). We now show that ϕ is onto.

For the onto part, let hkK be an arbitrary coset in HK/K. Note that $hkk^{-1} = h \in hkK \bigcap hK$ and so $\phi(h) = he_KK = hkK$ and ϕ is onto.

We finish this off with the first isomorphism. To do this we claim that $\ker(\phi) = H \bigcap K$. Note that if $h \in \ker(\phi)$ then $hK = K$ and hence $h \in K$ and so $h \in H \bigcap K$. On the other hand, if $h \in H \bigcap K$ then $\phi(h) = hK$ but since $h \in K, hK = K$ and $h \in \ker(\phi)$. So the First isomorphism Theorem guarantees that $H/\ker(\phi) \cong \text{im}(\phi)$, and so $H/(H \bigcap K) \cong HK/K$. □

Theorem 4.3.3 (Third Isomorphism Theorem)**.** *Let $N \trianglelefteq G$ be a normal subgroup. Then there is a one to one correspondence between the (normal) subgroups of G containing N and the (normal) subgroups of G/N. What is more, if $N \leq H \leq G$ and $H \trianglelefteq G$ then $(G/N)/(H/N) \cong G/H$.*

Proof. To show the correspondence, we consider a subgroup H such that $N \leq H \leq G$. Since $N \trianglelefteq H$, H/N is a group and we define $f(H) = H/N$. In a similar fashion, suppose that A is a subgroup of G/N. As A is a subset of G/N, there is a subset $H \subseteq G$ such that $hN \in A$ if and only if $h \in H$. Note that if $x, y \in H$ then $xNy^{-1}N = xy^{-1}N \in A$ and so $xy^{-1} \in H$. Hence we can write $A = H/N$ and we define $g(A) = g(H/N) = H$. Note that f, g compose to the identity function in both directions and so this correspondence between the subgroups of G/N and the subgroups of G containing N is a one to one correspondence. Also note that if $H \trianglelefteq G$ if and only if $H/N \trianglelefteq G/N$ (verify this).

Finally suppose that $N \leq H \leq G$ with $H \trianglelefteq G$. We have seen that $H/N \trianglelefteq G/N$. Consider $\phi : G/N \longrightarrow G/H$ given by $\phi(gN) = gH$. Since $N \subseteq G$ this function is well-defined and ϕ is clearly onto. Note that $\ker(\phi) = \{gN | gH = H\} = \{gN | g \in H\} = H/N$ Hence by the First Isomorphism Theorem (again) $(G/N)/(H/N) \cong H/N$. □

Exercises

1. Consider the additive group of the rationals $\mathbb{Q}$.
   a) Show that any finitely generated subgroup of $\mathbb{Q}$ is cyclic.
   b) Show that $\mathbb{Q}$ is not finitely generated.
2. Let H and K normal subgroups of G such that $H \bigcap K = 1$. Show that $hk = kh$ for all $h \in H$ and $k \in K$.
3. Classify all groups of order $2p$ where p is an odd prime.
4. Suppose that G is a group and $H \leq G$ is a subgroup of order n. Show that if H is the only subgroup of G of order n, then $H \trianglelefteq G$.
5. Suppose that G is a finite group and $N \trianglelefteq G$.
   a) Show that if H is a subgroup of G such that $\gcd(|H|, [G : N]) = 1$ then H is a subgroup of N.
   b) Show that if $\gcd(|N|, [G : N]) = 1$ then N is the unique subgroup of G of order $|N|$.

4.4 The Symmetric and Alternating Groups

Definition 4.4.1. *Let A be a set. We define the groups $S_A = \{f : A \longrightarrow A | f$ is bijective.$\}$. If A is the finite set $\{1, 2, \cdots, n\}$, we denote S_A by S_n.*

The symmetric groups are important i many senses. In particular, they are computationally useful and, as we will see later, any group can be visualized as a subgroup of an appropriate symmetric group.

Example 4.4.2. *We can identify D_5 with the subgroup of S_5 generated by* (1 2 3 4 5) *and* (2 5)(3 4)*. Do the same with $\mathbb{Z}_6$.*

Definition 4.4.3. *Let $\sigma := (a_1\ a_2\ \cdots\ a_m) \in S_n$. We say that σ is a cycle. If $m = 2$ we say that this cycle is a transpostion.*

Theorem 4.4.4. *Every element of S_n can we written as a product of:*

1. *a product of disjoint cycles (uniquely)*
2. *a product of transpositions.*

Proof. We leave the first statement as an exercise (hint: "follow the map" as an element of S_n is a bijection). The second statement follows from the first one we notice that

$$(a_1\ a_2\ \cdots\ a_m) = (a_1\ a_m)(a_1\ a_{m-1})\cdots(a_1\ a_3)(a_1\ a_2)$$

Note that the representation as a product of transpositions is not unique (e.g. (1 2) = (1 2)(1 2)(1 2). □

Definition 4.4.5. *Let $\sigma \in S_n$. We say that σ is even if σ can be written as a product of an even number of transpositions and we say that σ is odd if it can be written as an odd number of transpositions.*

We should establish that this "makes sense" (that is that there is not a $\sigma \in S_n$ that is both even and odd).

Theorem 4.4.6. *There is no $\sigma \in S_n$ that is both even and odd.*

Proof. If there is such a σ then we can write

$$\sigma = \tau_1\tau_2\cdots\tau_{2n} = \xi_1\xi_2\cdots\xi_{2m+1}$$

with each τ_i, ξ_j a transposition.

This means that we can write

$$e = \tau_{2n}\tau_{2n-1}\cdots\tau_2\tau_1\xi_1\xi_2\cdots\xi_{2m+1}$$

that is, the identity is odd. So to finish, we will assume that the identity can be written as an odd product of transpositions and obtain a contradiction. To this end we will assume that

$$e = \tau_1\tau_2\cdots\tau_{2k+1}$$

and note that $k \in \mathbb{N}$ is minimal (k cannot be 0 as it is clear that a single transposition cannot be the identity.

We will have to do some computations here, so we record some useful identities designed to "move a from right to left". We assume a, b, c, d are all distinct.

1. (a b)(a b)=e

2. (a c)(a b)=(a b c)=(a b)(b c)
3. (b c)(a b)=(a c b)=(a c)(b c)
4. (c d)(a b)=(a b)(c d)

Now suppose that $\tau_{2k+1} = (a\ b)$. Using the four above identities we can move $(a\ b)$ from right to left. Notice that whenever an identity above moves $(a\ b)$ from right to left, the new right transposition has no a. Additionally, if we never use the first identity, then after moving $(a\ b)$ all the way to the left, we obtain

$$e = \tau'_{2k+1}\tau'_1\tau'_2\cdots\tau'_{2k}$$

where $\tau'_{2k+1} = (a\ x)$ with $x \neq a$ and τ'_i is a transpostion without a (or the identity) for $1 \leq i \leq 2k$. But this cannot be the identity as this permutation takes a to x. Hence we must assume that at some point we had to use the first identity. But this collapses two of the transpositions to the identity, reducing our representation of e to a smaller odd integer, contradicting minimality. □

Definition 4.4.7. *We define the alternating group on n elements to be $A_n = \{\sigma \in S_n | \sigma$ is even$\}$.*

Theorem 4.4.8. *For all $n \geq 2, |A_n| = \frac{n!}{2}$. Additionally, $A_n \trianglelefteq S_n$.*

Proof. Consider the homomorphism $\phi : S_n \longrightarrow \{\pm 1\}$ given by

$$\phi(\sigma) = \begin{cases} 1, \text{ if } \sigma \text{ is even,} \\ -1, \text{ if } \sigma \text{ is odd.} \end{cases}$$

Since the sum of two even numbers is even, the sum of two odds is even, and the sum of an even and an odd is an odd (and the notion of even and odd permutation is well-defined), the function ϕ is a well-defined homomophism and since $n \geq 2$, ϕ is onto. The kernel of ϕ is clearly A_n and so $A_n \trianglelefteq S_n$ and by the first isomorphism theorem, $S_n/A_n \cong \{\pm 1\}$. Hence A_n is of index 2 and hence of order $\frac{n!}{2}$. □

Chapter 5

Group Actions

5.1 Groups Acting on Themselves: Basics

We recall that a group G acting on a (nonempty) set A is a function $G \times A \longrightarrow A$ that satisfies $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ and $e \cdot a = a$.

Example 5.1.1. *Recall that S_5 acting on the set of symmetries of a regular pentagon by the permutations* (2 5)(3 4) *and* (1 2 3 4 5).

Theorem 5.1.2. *Let G be a group and A a nonempty set and let S_A be the group of bijections from A to A. Then there is a bijection between the actions of G on A and homomorphisms $G \longrightarrow S_A$ given by: $g \cdot a = \phi(g)(a)$ where $\phi : G \longrightarrow S_A$ is the corresponding homomorphism.*

Proof. We first suppose that $\phi : G \longrightarrow S_A$ is our homomorphism. Then $g \cdot a = \phi(g)(a)$ is a function from $G \times A \longrightarrow A$. Note that $(g_1 g_2) \cdot a = \phi(g_1 g_2)(a) = (\phi(g_1)\phi(g_2))(a) = \phi(g_1)(\phi(g_2)(a)) = g_1 \cdot (g_2 \cdot a)$. Additionally $e_G \cdot a = \phi(e_G)(a) = a$ since $\phi(e_G)$ is the identity permutation of A.

Now, if we are given the action $\cdot : G \times A \longrightarrow A$, we define $\phi : G \longrightarrow S_A$ by

$$\phi(g) = \pi_g$$

where the permutation π_g is given by $\pi_g(a) = g \cdot a$.

Since $\pi_{gh}(a) = (gh) \cdot a = g \cdot (h \cdot a) = \pi_g(\pi_h)(a)$, we have that $\pi_{gh} = \pi_g \pi_h$ and so ϕ is a homomorphism.

Now note that if we begin with the action $\cdot : G \times A \longrightarrow A$, this gives rise to the homomorphism ϕ where $\phi(g) = \pi_g$ where $\pi_g(a) = g \cdot a$. So given this ϕ we now have the action of G on A given by $\phi(g)(a) = \pi_g(a) = g \cdot a$.

And if we begin with the homomophism $\phi : G \longrightarrow S_A$, this gives the action $g \cdot a = \phi(g)(a)$. And now given this action, we have the homomorphism from $G \longrightarrow S_A$ given by $g \longrightarrow \pi_g$ where $\pi_g(a) = \phi(g)(a)$. Hence g corresponds exactly to $\phi(g)$. So this correspondence is bijective and the theorem is established. □

We also recall the following definitions.

Definition 5.1.3. *Given an action of a group G on a set A, we define*

1. *The kernel of the action is $\{g \in G | g \cdot a = a, \forall a \in A\}$.*
2. *For all $a \in A$ the stabilizer of a in G is $G_a = \{g \in G | g \cdot a = a\}$.*
3. *We say that the action is faithful if its kernel is the identity.*

Definition 5.1.4. *If G is a group that a permutation representation of G is just a homomorphism $G \longrightarrow S_A$ for some set A.*

Definition 5.1.5. *Suppose G acts on the nonempty set A.*

1. *$orb(a) = \{g \cdot a | g \in G\}$ is called the orbit of a.*
2. *We say that G acts transitively on A if there is a unique orbit on A.*

Theorem 5.1.6. *Let G be a group acting on the set A. The relation $a \sim b$ if and only if $a = g \cdot b$ for some $g \in G$ is an equivalence relation. For each $a \in A$ the number of elements in the equivalence class of a is $[G : G_a]$ (the length of the orbit of a is the index of its stabilizer).*

Proof. $a = e \cdot a$ so $a \sim a$. Also if $a \sim b$ then $a = g \cdot b$ and so $b = g^{-1} \cdot a$ and so $b \sim a$. Finally, if $a \sim b$ and $b \sim c$ then $a = g_1 \cdot b$ and $b = g_2 \cdot c$ and so $a = g_1 g_2 \cdot c$ and $a \sim c$ and hence $\sim$ is an equivalence relation.

The equivalence class of a ($[a]$) is the set of elements $[a] = \{x | x = g \cdot a, g \in G\}$. Let L be the left cosets of G_a in G and define the function $f : L \longrightarrow [a]$ by $f(gG_a) = g \cdot a$. We first note that if $g_1 G_a = g_2 G_a$ then $g_2^{-1} g_1 \in G_a$ and so $g_2^{-1} g_1 \cdot a = a$. From this we obtain that $g_1 \cdot a = g_2 \cdot a$ and so $f(g_1 G_a) = f(g_2 G_a)$ and f is well-defined. It remains to show that f is a bijection.

Suppose that $f(xG_a) = f(yG_a)$. Then $x \cdot a = y \cdot a$ and so $y^{-1} x \in G_a$. We conclude that $xG_a = yG_a$ and f is one to one.

Finally, if $b \in [a]$ then there is a $g \in G$ such that $b = g \cdot a$. Note that $b = f(gG_a)$ and so f is a bijection and the proof is complete. □

We now look at some examples of how to translate action into permutation representations.

Example 5.1.7. *Let G act on itself by left multiplication (if $g, a \in G$ then $g \cdot a = ga$). For our first concrete example, let $G = \mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Here G acts on itself by left addition. The permutation for $\overline{0}$ is merely the identity. For $\overline{1}$, this action just shifts all elements in a cycle so it induces the permutation $(\overline{0}\ \overline{1}\ \overline{2}\ \overline{3}\ \overline{4}\ \overline{5})$. $\overline{2}$ induces the permutation $(\overline{0}\ \overline{2}\ \overline{4})(\overline{1}\ \overline{3}\ \overline{5})$. $\overline{3}$ induces the permutation $(\overline{0}\ \overline{3})(\overline{1}\ \overline{4})(\overline{2}\ \overline{5})$.*

Theorem 5.1.8. *Let G be a group and $H \leq G$ a subgroup and A the set of left cosets of H in G. Suppose that G acts on A by left multiplication of the left cosets, and let π_H be the associated permutation representation of this action. Then the following hold.*

1. *G acts transitively on A.*

2. *The stabilizer in G of $H \in A$ is precisely H.*

3. *The kernel of the action is $\bigcap_{x\in G} xHx^{-1}$ and $ker(\pi_H)$ is the largest normal subgroup of G contained in H.*

Proof. 1. For $xH, yH \in A$, let $g = yx^{-1}$ and note that $g \cdot xH = yH$.

2. Clearly if $h \in H$ then $hH = H$ and so H is contained in the stabilizer. On the other hand, if $gH = H$, then $g \in H$ and we are done.

3. $\ker(\pi_H) = \{g \in G | g \cdot xH = xH, \forall x \in G\} =$
$\{g \in G | x^{-1}gxH = H, \forall x \in G\} = \{g \in G | x^{-1}gx \in H, \forall x \in G\} =$
$\{g \in G | g \in xHx^{-1}, \forall x \in G\} = \bigcap_{x\in G} xHx^{-1}$.

We now note that $\ker(\pi_H) \trianglelefteq G$ (as this is the kernel of the permutation representation and also because any group of the form $\bigcap_{x\in G} xHx^{-1}$ is normal in G). Now suppose that N is a normal subgroup of G that is contained in H. Then for all $x \in G$, $N = xNx^{-1} \leq xHx^{-1}$, and hence $N \leq \bigcap_{x\in G} xHx^{-1}$ and this establishes the theorem. □

Here is a big one that was promised earlier.

Theorem 5.1.9 (Cayley)**.** *Every group is isomorphic to a subgroup of S_A for some set A. If $|G| = n$ then G can be realized as a subgroup of S_n.*

Proof. Let H be the identity subgroup in the previous. This gives a homomorphism into S_G with trivial kernel. Hence G is a subgroup of S_A where $|A| = |G|$. The finite case follows from this easily. □

We noted in the homework that if $[G : N] = 2$ then $N \trianglelefteq G$. Here is a result that uses the previous ideas to generalize.

Corollary 5.1.10. *Let G be a finite group with $|G| = n$ and let p be the smallest prime dividing n. Then any subgroup of G of index p (if such a subgroup exists) must be normal.*

Proof. Let $H \leq G$ and suppose that $[G : H] = p$. Let π_H be the permutation representation induced by left multiplication on the left cosets of H in G. Let $K = \ker(\pi_H)$. Let $k = [H : K]$ and note that

$$[G : K] = [G : H][H : K] = pk.$$

Since H has p left cosets in G, G/K can be thought of as a subgroup of S_p (in particular, is isomorphic to the image of G under π_H by the First Isomorphism Theorem). Hence $|G/K|$ must divide $|S_p| = p!$. Hence $k|(p-1)!$ and so all prime factors of k are less than p. But since any prime factor of k must also divide $n = |G| = pk|K|$, it must be the case that $k = 1$ and hence $H = N \trianglelefteq G$. □

5.2 Conjugation Action and the Class Equation

Another useful action of G on itself is canjugation action.

Definition 5.2.1. *We say that G acts on itself by conjugation if $g \cdot x = gxg^{-1}$, $g, x \in G$.*

Definition 5.2.2. *Let G be a group. We say that the elements $a, b \in G$ are conjugate if there is a $g \in G$ such that $a = gbg^{-1}$. We say that the subset $S, T \subseteq G$ are counjugate if $S = gTg^{-1}$.*

Example 5.2.3. *You should verify that conjugation is indeed an action of G on itself. Note that if G is an abelian group of more than one element, then this action is not transitive. (Length of orbit is 1 as is the index of the stabilizer).*

Theorem 5.2.4. *Let $S \subseteq G$ be a subset of the group G. Then the number of conjugates of the set S is the index of the normalizer $[G : N_G(S)]$. If $S = s$ (a single element set) then the number of conjugates of s is equal to $[G : C_G(s)]$.*

Proof. The number of conjugates of S is the index of the stabilizer of S which is $\{g \in G | gSg^{-1} = S\} = N_G(S)$. If $S = s$ then $N_G(s) = C_G(s)$. □

Theorem 5.2.5 (The Class Equation)**.** *Let G be a finite group and $g_1, g_2, \cdots, g_r$ be representatives of the distinct conjugacy classes of G not contained in $Z(G)$. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)].$$

Proof. Note that $x \in G$ is in a conjugacy class of size 1 if and only if $x \in Z(G)$. Let $Z(G) = \{1, z_2, \cdots, z_m\}$. Let $\mathcal{C}_1, \cdots, \mathcal{C}_r$ be the conjugacy classes not contained in $Z(G)$. So we have that $|G| = |Z(G)| + \sum_{i=1}^{r} |\mathcal{C}_i|$. But each $|\mathcal{C}_i| = [G : C_G(g_i)]$ and this completes the theorem. □

Here is a super-important corollary that we make a theorem in its own right. This is a very important structural theorem for finite groups of prime power order (and hence useful for all finite groups).

Theorem 5.2.6. *If p is a positive prime and $|G| = p^a$ with $a \in \mathbb{N}$ then $Z(G) \neq 1$.*

Proof. $|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)]$. Since $|G|$ and each $[G : C_G(g_i)]$ are both divisible by p and $|Z(G)| \geq 1$ and is also divisible by p then the center is nontrivial. □

Here is another very useful corollary. But first we need a lemma that we leave as an exercise.

Lemma 5.2.7. *If G is a group and $Z(G)$ the center of G. If G/N is cyclic, then G is abelian.*

Proof. Exercise. □

Corollary 5.2.8. *If $|G| = p^a$ where $a = 1, 2$ then G is abelian.*

Proof. If $|G| = p$ then G is cyclic of order p and hence abelian. So suppose $|G| = p^2$. If $|G| = p^2$ we are done so we assume that $|Z(G)| = p$. Since $Z(G) \trianglelefteq G$ and $|G/Z(G)| = p$ (and hence is cyclic) the previous lemma shows that G is abelian.

For an alternative to the last part of the proof, you can show that G can be generated by two elements $z \in Z(G)$ and another element, say x, also of order p. Since $zx = xz$, G must be abelian. □

Exercises

1. We have seen that there is no permutation of S_n that is both even and odd. Use the information to explain why there is no rearrangement on the Rubik's Cube that swaps two corners and leaves all other pieces in their correct (geographic) position.

2. In this problem, we will count elements of various orders in S_n

   a) Find all k such that there is an element of order k in S_5, and for each such k determine how many elements of order k that there are.

   b) Let p be a positive prime. How many elements of order p are there in S_p?

   c) How many subgroups of order p are there in S_p?

3. Let G be a group and H a subgroup. We say that H is *characteristic* in G if $\phi(H) \subseteq H$ for all $\phi \in \mathrm{Aut}(G)$.

   a) Show that if H is characteristic in G, then H is normal in G.

   b) Show that an arbitrary intersection of characteristic subgroups of G is characteristic.

   c) Give an example of a group G with a normal subgroup that is not characteristic.

   d) Show that $Z(G)$ is a characteristic subgroup of G.

4. Suppose that H is a characteristic subgroup of G (so $\phi(H) \subseteq H$ for all $\phi \in \mathrm{Aut}(G)$. Is it true that $\phi(H) = H$? Prove this statement or give a counterexample.

5. Let G be a group and let G act on itself by conjugation, that is, $g \cdot x = gxg^{-1}$.

   a) Show that the above is, in fact, a group action.

   b) What is the kernal of this action?

6. Let G be a group. Show that $\mathrm{Inn}(G) \cong G/Z(G)$.

7. Show that two elements of S_n are conjugate if and only if they have the same cycle type. Then show that the number of conjugacy classes in S_n is equal to the number of partitions of the integer n.

8. Show for any prime p there is a nonabelian group of order p^3.

9. Let $H \trianglelefteq G$ be a normal subgroup.

   a) For a fixed $g \in G$, show that the function $\phi_g : H \longrightarrow H$ given by $\phi_g(h) = ghg^{-1}$ is an automorphism of H.

   b) Show that the $G-$action on H given by $g \cdot h = ghg^{-1}$ is a group action.

   c) Show that the permutation representation induced by this action gives rise to a homomorphism $G \longrightarrow \mathrm{Aut}(H)$ with kernel $C_G(H)$.

   d) Show that $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

10. Show that if $K \leq G$ is a subgroup and $g \in G$ then $K \cong gKg^{-1}$.

11. Show that if $H \leq G$ is a subgroup then $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$ (in particular, $G/Z(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(G)$).

12. Let H be a subgroup of G and let $N = \bigcap_{x \in G} xHx^{-1}$. Show that $N \trianglelefteq G$.

13. Let G be a finite $p-$group of order p^n. Show that for all $0 \leq k \leq n$, there is a subgroup of G of order p^k and each subgroup of order p^k is normal in a subgroup of order p^{k+1} $(k \leq n-1)$.

14. Let $(G, \cdot), (H, \circ)$ be groups. We define the *direct product* of the groups G and H to be the set $G \times H$ with multiplication given by $(g_1, h_1)(g_2, h_2) = (g_1 \cdot g_2, h_1 \circ h_2)$.

   a) Show that with the operation above, $G \times H$ is a group.

   b) Show that if $G' \leq G$ and $H' \leq H$ are subgroups, then $G' \times H'$ is a subgroup of $G \times H$.

   c) Is the converse of part b) true?

   d) Show that $Z(G \times H) = Z(G) \times Z(H)$.

   e) Show that $G \times H$ is abelian if and only if both G and H are abelian.

15. Let G, H be groups and $\phi : H \longrightarrow \mathrm{Aut}(G)$ a group homomorphism. We define the *semidirect product* of G and H $(G \rtimes_\phi H)$ with multiplication given by

$$(g_1, h_1)(g_2, h_2) = (g_1\phi(h_1)(g_2), h_1h_2).$$

   a) Show that the semidirect product is a group.

   b) What happens if the homomorphism $\phi : H \longrightarrow \mathrm{Aut}(G)$ is the trivial homomorphism (that is $\phi(h) = I_G$ for all $h \in G$?

c) What happens if G is cyclic of order $n \geq 3$ and H is cyclic of order 2 with
$\phi : H \longrightarrow \mathrm{Aut}(G)$ given by

$$\phi(y) = \begin{cases} I_G, \text{ if } y = e_H, \\ f, \text{ if } y \neq e_H. \end{cases}$$

where f is the automorphism of G given by $f(x) = x^{-1}$?

Chapter 6

The Sylow Theorems

6.1 The Statement and Proof

The Sylow Theorems are the most cetral and important tool in basic finite group theory and they are absolutely essential to understanding the structure of any finite group. We will jump right into the content of the theorems, but first a definition is needed.

Definition 6.1.1. *Let G be a group and p a positive prime.*

1. *A group in which every element has order p^m for some m is called a $p-$group. If our $p-$group is finite it must have order p^a for some $a \in \mathbb{N}$.*
2. *If G is a group and $|G| = p^a m$ with $gcd(p, m) = 1$ then a subgroup of G of order p^a is called a Sylow $p-$subgroup of G.*

We note here that a Sylow $p-$subgroup of G is a maximal $p-$subgroup of G. We will see that if G is any group of order $p^a m$ with $\gcd(p, m) = 1$ then G actually has a Sylow $p-$subgroup.

Theorem 6.1.2 (The Sylow Theorems)**.** *Suppose that G is a finite group with $|G| = p^a m$ and $gcd(p, m) = 1$.*

1. *G has at least one Sylow $p-$subgroup.*
2. *If P is a Sylow $p-$subgroup and Q is a $p-$subgroup of G then there is a $g \in G$ such that $Q \leq gPg^{-1}$. In particular, any two Sylow $p-$subgroups are conjugate.*
3. *If n is the number of Sylow $p-$subgroups of G then $n \equiv 1 mod(p)$. Additionally n is the index of $N_G(P)$ in G (and hence n must divide m).*

To prove this, we first establish the following the lemma.

Lemma 6.1.3. *Let P be a Sylow $p-$subgroup of G. If Q is any $p-$subgroup of G, then $Q \bigcap N_G(P) = Q \bigcap P$.*

Proof. Since $P \leq N_G(P)$ the containment $Q \bigcap P \leq Q \bigcap N_G(P)$ is clear. To establish the other containment, it will suffice to show that $Q \bigcap N_G(P) \leq P$. To this end, our strategy will be to show that $P(Q \bigcap N_G(P))$ is a $p-$subgroup of G (that contains both P and $Q \bigcap N_G(P)$). But then as P is a maximal $p-$subgroup, $P(Q \bigcap N_G(P)) = P$ and hence $Q \bigcap N_G(P) \leq P$.

To implement our strategy, we first note that as $N_G(P) \bigcap Q \leq N_G(P)$, we know that $P(N_G(P) \bigcap Q)$, we know that $P(N_G(P) \bigcap Q)$ is a subgroup of G. Hence

$$|P(N_G(P) \bigcap Q)| = \frac{|P||N_G(P) \bigcap Q|}{|P \bigcap N_G(P) \bigcap Q|}$$

and hence $P(N_G(P) \bigcap Q)$ must be a $p-$subgroup. But $P \leq P(N_G(P) \bigcap Q)$ and so by the maximality of P, we have that $P = P(N_G(P) \bigcap Q)$. □

With this in hand, we now prove the Sylow Theorems.

Proof. (Sylow Theorems) We prove 1. this by induction on $|G|$ and first note that if $|G| = 1$ then the result follows and this establishes the base case.

Inductively, we assume the existence of Sylow $p-$subgroups for all groups of order less than $r = |G|$.

If p divides $|Z(G)|$, then $Z(G)$ has a subgroup N of order p, and note that $N \trianglelefteq G$ (as N is in the center of G) and so $\overline{G} = G/N$ and so $|\overline{G}| = p^{a-1}m$. By induction $\overline{G}$ has a subgroup $\overline{P}$ of order p^{a-1}. By the correspondence theorem, there is a subgroup $N \leq P \leq G$ such that $P/N = \overline{P}$. In this case, we have that $|P| = |P/N||N| = p^a$.

Now if it is the case that p does not divide $|Z(G)|$, we let $g_i, 1 \leq i \leq t$ be representatives of the non-central conjugacy classes and recall

$$|G| = |Z(G)| + \sum_{i=1}^{t} [G : C_G(g_i)].$$

Since p does not divide $|Z(G)|$, then for some i, p does not divide $[G : C_G(g_i)]$. For this particular g_i, we let $H = C_G(g_i)$, and note that $|H| = p^a k$ where p does not divide k and $k \leq m$. Now H centralizes g_i but g_i is not in the center of G and so H is a proper subgroup of G. By induction we have $P \leq H < G$ and $|P| = p^a$ and we are done.

We now move on to parts 2. and 3.

Let $P < G$ be a Sylow $p-$subgroup. We define

$$S = \{P_1, P_2, \cdots, P_t\} = \{gPg^{-1} | g \in G\}.$$

Let $Q \leq G$ be any $p-$subgroup. Note that G (and hence Q) acts on the set S by conjugation. We write S as the disjoint union of orbits under this Q action:

$$S = \text{orb}_1 \bigcup \text{orb}_2 \bigcup \cdots \bigcup \text{orb}_k$$

and note that $t = |\text{orb}_1| + |\text{orb}_2| + \cdots + |\text{orb}_k|$. We now renumber the elements of S so that the first k are representative of the $Q-$orbits, that is, $P_i \in \text{orb}_i, 1 \leq i \leq k$.

Note that $|\text{orb}_i| = [Q : N_Q(P_i)|$. Note that $N_Q(P_i) = N_G(P_i) \bigcap Q$, and so by the previous lemma, $N_G(P_i) \bigcap Q = P_i \bigcap Q$.

Since Q was arbitrary, we look at what happens in the special case that $Q = P_1$; in this case $|\text{orb}_1| = 1$. Now for $i > 1$, $P_i \neq P_1$ and so $P_1 \bigcap P_i < P_1$. Hence $|\text{orb}_i| = [P_1 : P_i \bigcap P_1] > 1$, but is a power of p. Hence p divides $|\text{orb}_i|$ for $2 \leq i \leq k$. This shows that $t \equiv 1 \text{mod}(p)$.

Now if Q is not contained in any P_i, then for all i, $Q \bigcap P_i < Q$ and hence $|\text{orb}_i| = [Q : Q \bigcap P_i] > 1$ for all i, which contradicts the fact that $t \equiv 1 \text{mod}(p)$. Hence $Q \leq gPg^{-1}$ for some $g \in G$.

Lastly, we note that if n is the number of Sylow $p-$subgroups, then $n = [G : N_G(P)]$. Since $N_G(P) \geq P$, n divides m. □

Corollary 6.1.4. *Let P be a Sylow $p-$subgroup of G. The following conditions are equivalent.*

1. *P is the unique Sylow $p-$subgroup.*
2. *$P \trianglelefteq G$.*
3. *P is characteristic in G.*
4. *All subgroups generated by elements of order a power of p are $p-$subgroups of G.*

Proof. Exercise. □

Definition 6.1.5. *We say that a group is simple if only the identity subgroup and the group itself are normal subgroups.*

Example 6.1.6. *A_n is simple for $n \geq 5$. $\mathbb{Z}_p$ is simple (only nonindentity abelian groups that are simple). (You may use these facts).*

Example 6.1.7. *Apply the Sylow Theorems and groups actions for the following.*

1. *Show that any group of order 15 is cyclic.*
2. *Show that no group of order 12, 80 is simple.*
3. *Show that no group of order 24, 36, 72 is simple.*

We work through the 36 example here in the notes. Suppose that $|G| = 24 = 2^2 3^2$. It will suffice to show that there is either a unique Sylow $2-$subgroup or a unique Sylow $3-$subgroup. We let n_p denote the number of Sylow $p-$subgroups. The Sylow Theorems say that $n_2 \equiv 1 mod(2)$ and must divide 9 and so our candidates are $\{1, 3, 9\}$. Also $n_3 \equiv 1 mod(3)$ and must divide 4 and so our candidates are $\{1, 4\}$. So if G is not simple then there are precisely 4 Sylow $3-$subgroups. If we consider the set of Sylow $3-$ subgroups $\{P_1, P_2, P_3, P_4\}$, we note that G acts on this set by conjugation (and the Sylow theorems say that this action is transitive as all Sylow subgroups must be conjugate). This permutation

representation gives a homomorphism $\phi : G \longrightarrow S_4$. Since $|G| = 36 > 24$ this homomophism must have a nontrivial kernel (because ϕ cannot be one to one). But if $ker(\phi) = G$ then the homomorphism (and hence the permutation action) is trivial. So $ker(\phi)$ is a nontrivial normal subgroup of G and so G is not simple.

Try this with 24 and come to the conclusion that if G is simple then $G \cong S_4$, but then S_4 has a nontrivial normal subgroup.

Example 6.1.8. *See if you can find the two nonabelian groups of order 8 and the three of order 12.*

Exercises

1. Let G be a finite group and P a Sylow $p-$subgroup. Prove the following.
   a) (5 pts) $P \trianglelefteq G$ if and only if P is the unique Sylow $p-$subgroup.
   b) (5 pts) $P \trianglelefteq G$ if and only if P is a characteristic subgroup of G.
   c) (5 pts) $P \trianglelefteq G$ if and only if all subgroups generated by elements of order a power of p are $p-$subgroups of G.
2. Let G be a finite $p-$group of order p^n. Show that for all $0 \leq k \leq n$, there is a subgroup of G of order p^k and each subgroup of order p^k is normal in a subgroup of order p^{k+1} $(k \leq n-1)$.
3. Let p and q be distinct primes with $p < q$ and $q \not\equiv 1 \mathrm{mod}(p)$. Show that if $|G| = pq$ then $G \cong \mathbb{Z}/pq\mathbb{Z}$.
4. Classify all groups of order pq where $p < q$ are positive primes and $q \equiv 1 \mathrm{mod}(p)$.
5. Let G be a group. We say that G is *simple* if G contains no normal subgroups except for G itself and the identity. Show that there is no simple group of order 80.
6. Suppose that G is a group of order 72; the goal of this problem is to show that G cannot be simple.
   a) Show that G has either 1 or 4 Sylow 3-subgroups. Conclude that if G is simple, then G must have 4 Sylow 3-subgroups.
   b) Show that if G has 4 Sylow 3-subgroups, then the conjugation action of G on the set of Sylow 3-subgroups induces a homomorphism from $G \longrightarrow \mathrm{S}_4$.
   c) Conclude that G must have a nontrivial normal subgroup (hint: the kernal of a homomorphism is always normal).
7. Let p be a prime integer. Show that any group of order p^2 is abelian.

8. Find the smallest *odd* integer such that there is a nonabelian group of order n.

9. Classify all groups of order n where n is the answer from number 2.

10. Classify all abelian groups of order 64.

11. Let G and H be groups. Show that $Z(G \times H) = Z(G) \times Z(H)$.

12. Let $p < q < r$ be primes. Show that there is no simple group of order pqr.

13. Show that no group of order 90 is simple (you may use the fact that A_n is simple for all $n \geq 5$). (This problem is rather involved).

Chapter 7

Direct Products, Semi-Direct Products, and Finitely-Generated Abelian Groups

7.1 (Semi)Direct Products

We have talked a bit about the notion of direct and semi-direct products in the exercises. We formalize here.

Definition 7.1.1. *Let $\{G_i\}_{i\in I}$ be a family of groups. We define the (external) direct product of this family to be the the group with the underlying set being $\prod_{i\in I} G_i$ and the operation being given componentwise (that is $(g_i)(h_i) = (g_i h_i)$).*

You should verify that this operation on the Cartesian product of this family results in a group structure.

Remark 7.1.2. *Observe that $|G_1 \times G_2 \times \cdots \times G_n| = \prod_{i=1}^{n} |G_i|$.*

Remark 7.1.3. *If A, B are abelian groups then we sometimes write $A \oplus B$ instead of $A \times B$ for the direct product. There is a notion of direct sum that is distinct from direct product. We will define this below.*

Definition 7.1.4. *Let $\{G_i\}_{i\in I}$ be a family of groups. We define the (external) direct sum of this family to be the the subgroup of the direct product consisting of the elements of the form $(g_i)_{\in I}$ where $g_i = e_{G_i}$ for all but finitely many i.*

Theorem 7.1.5. *Let $G_1, G_2, \cdots, G_n$ be groups and $G = G_1 \times G_2 \times \cdots G_n$ the direct product (this can be extended to the infinite case)*

1. *For all* $1 \leq i \leq n, G_i \cong (1_{G_1}, 1_{G_2}, \cdots, 1_{G_{i-1}}, G_i, 1_{G_{i+1}}, \cdots, 1_{G_n})$. *And the image of* G_i *in* G *under this map* $(\iota_i(g_i) = (1, 1, \cdots, 1, g_i, 1, \cdots, 1))$ *is normal in* G *and*

$$G/im(\iota_i) \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

2. *For all* $1 \leq i \leq n$ *we define* $\pi_i : G \longrightarrow G_i$ *by* $\pi_i(g_1, g_2, \cdots, g_n) = g_i$. π_i *is onto and* $ker(\pi_i) \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$. *Hence* $G/ker(\pi_i) \cong G_i$.

3. *If* $i \neq j$ *and* $g_i \in G_i$ *and* $g_j \in G_j$, *then* $\iota_i(g_i)\iota_j(g_j) = \iota_j(g_j)\iota_i(g_i)$.

Proof. 1. The function given by $\iota_i(g_i) = (1, 1, \cdots, 1, g_i, 1, \cdots, 1)$ is easily seen to be one to one and a homomorphism. Additionally an easy computation shows that the image of this homomoprhism is a normal subgroup of G. For the final statement consider the function $f : G \longrightarrow G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$ given by $f(g_1, g_2, \cdots, g_i, \cdots, g_n) = (g_1, g_2, \cdots, g_{i-1}, g_{i+1}, \cdots, g_n)$ is easily checked to be a group epimorphism with kernel precisely $\text{im}(\iota_i)$. Apply the first isomorphism theorem.

2. Exercise.

3. Note that if, without loss of generality, $i <$ then
$(1, 1, \cdots, 1, g_i, 1, \cdots, 1)(1, 1, \cdots, 1, g_j, 1, \cdots, 1) = (1, \cdots, 1, g_i, 1, \cdots, 1, g_j, 1, \cdots, 1) =$
$(1, 1, \cdots, 1, g_j, 1, \cdots, 1)(1, 1, \cdots, 1, g_i, 1, \cdots, 1)$. □

Example 7.1.6. *Note that the cyclic groups* $\mathbb{Z}_6$ *and* $\mathbb{Z}_{15}$ *can be decomposed into direct products.*

Here is a theorem that is important in recognizing (internal) direct products. It can be generalized easily and that will be left as an exercise.

Theorem 7.1.7. *Let* $H, K \leq G$ *be subgroups such that*

1. $H, K \trianglelefteq G$
2. $H \bigcap K = 1$

then $HK \cong H \times K$.

Proof. Form earlier results, it is immediate that HK is a subgroup of G. Also note that if $h \in H$ and $k \in K$ then $h^{-1}k^{-1}hk \in H \bigcap K = 1$, it must be that $hk = kh$.

We now define a function $f : HK \longrightarrow H \times K$ by $f(hk) = (h, k)$. We first show that this function is well defined: if $hk = h_1k_1$ then $h_1^{-1}h = k_1k^{-1} \in K \bigcap H = 1$. Hence $h = h_1$ and $k = k_1$ and so f is well-defined.

Now we note that $f(hkh_1k_1) = f(hh_1kk_1)$ since elements of H commute with elements of K. Hence $f(hh_1kk_1) = hh_1kk_1 = hkh_1k_1 = f(hk)f(h_1k_1)$ and so f is a homomorphism.

Clearly f is onto. Now suppose that $hk \in \ker(f)$. Then $hk = 1$ and so $h = k^{-1} \in H \bigcap K = 1$ and hence $h = k = 1$. This proves the theorem. □

Corollary 7.1.8. *Let $H, K \leq G$ be subgroups such that*

1. $H, K \trianglelefteq G$
2. $H \bigcap K = 1$
3. $HK = G$

then $G \cong H \times K$.

Remark 7.1.9. *If the conditions of the previous corollary are satisfied, we say that G is the internal direct product of H and K.*

Here we generalize to the so-called semidirect product notion.

Definition 7.1.10. *Let H, K be groups and $\phi : K \longrightarrow Aut(H)$ a homomorphism. We define the semidirect product $H \rtimes_\phi H = \{(h, k) | h \in H, k \in K\}$ with the operation given by $(h_1, k_1)(h_2, k_2) = (h_1\phi(k_1)(h_2), k_1k_2)$.*

We leave the proof of the next two results as an exercise.

Theorem 7.1.11. *$H \rtimes_\phi K$ is a group of order $|H||K|$. The subgroup $\{(h, 1)\} \cong H$ is normal in G. Additionally if ϕ is the trivial homomorphism (or if $K \trianglelefteq H \rtimes_\phi K$) then $H \rtimes_\phi K \cong H \times K$.*

Example 7.1.12. *Show that the dihedral groups are semidirect products.*

Theorem 7.1.13. *Suppose that G is a group and $H, K \leq G$ are subgroups such that*

1. $H \trianglelefteq G$
2. $H \bigcap K = 1$
3. $HK = G$

then $G = H \rtimes_\phi K$ for some homomorphism $\phi : K \longrightarrow Aut(H)$.

Exercises

1. Let K be the group of order 2 and H be abelian. Suppose that $\phi : K \longrightarrow \mathrm{Aut}(H)$ takes the nonidentity element to the automorphism of H that takes each element to its inverse.
   a) (5 pt) Find necessary and sufficient conditions on H so that $H \rtimes_\phi K \cong H \times K$.
   b) (5 pt) What can you say about $H \rtimes_\phi K$ in the case where H is cyclic?
   c) (5 pt) Find all groups of order 8 that cannot be written as the semidirect product of two of its proper subgroups.
2. Show that the direct sum is indeed a (normal) subgroup of the direct product.
3. Formulate and verify a generaliztion of Theorem **??**.

7.2 The Structure of Finite Abelian Groups

For abelian groups that are finite (or finitely generated) there is a nice structure theorem. Here we present it and some examples. There are many applications for this and we will see some of these now and some later.

Lemma 7.2.1. *Let G be an abelian finite group of order p^n. Then G is cyclic if and only if G contains a unique subgroup of order p.*

We remark here that the assumption "abelian" is needed as Q_8 is not cyclic but contains a unique subgroup of order 2.

Proof. If G is cyclic we already know that there is a unique subgroup for every divisor of the order of G, so we only need to show the other direction.

For this direction, we proceed by induction on n. If $n = 1$ the conclusion is immediate as any group of order p is cyclic. We now assume the conclusion for all abelian $p-$groups of order p^k with $1 \leq k \leq m$.

Suppose that $|G| = p^{m+1}$ and that G has a unique subgroup, P, of order p. Consider the homomorphism $\phi : G \longrightarrow G$ given by $\phi(x) = x^p$. Note that $\ker(\phi) = P$ and note that $\phi(G)$ is a nontrivial subgroup of G and $\phi(G) \cong G/P$ and so has order p^m. Note that $\phi(G)$ has a subgroup of order p and since this is also a subgroup of G, then it must be unique. By induction, we obtain that $\phi(G)$ is a cyclic group and G/P is cyclic of order p^m (will say that G/P is generated by the coset $x\phi(G)$ for some $x \in G$). Note that in G, $\langle x \rangle$ contains P (because $\langle x \rangle$ contains a subgroup of order p and this is in G so must be the unique P). All this shows that in G the order of x is p^{m+1} and we are done. □

Lemma 7.2.2. *Let G be an abelian $p-$group and H a cyclic subgroup of G if maximal order. Then $G = H \oplus K$ for some subgroup $K \subseteq G$.*

Proof. We go by induction on n where $|G| = p^n$ and we note that if G is cyclic then we are done. The result clearly hols for $n = 1$ and inductively we assume that the result holds for all abelian $p-$groups of order no more than p^m.

If $|G| = p^{m+1}$ and G is cyclic we are done. If not then the previous lemma shows that there are at least two subgroups of order p. Let $H \leq G$ be a cyclic subgroup of maximal order p^k where $k \leq m$ and let K be another subgroup of order p.

Note that since $H \bigcap K = 0$, it must be the case that $(H + K)/K \cong H/(H \bigcap K) \cong H$. Now given any $g \in G$, the coset $g + K$ has order dividing the order of g (and of course, $|g|$ is at most $|H|$). Hence the cyclic subgroup $(H+K)/K \cong H$ has maximal order in G/K. We apply the inductive hypothesis to obtain a group $N/K \leq G/K$ such that $G/K \cong (H + K)/K \oplus N/K$.

This means that $H + K + N = H + N = G$. Also since this is a direct product decomposition, $N \bigcap (H + K) = K$, and so $N \bigcap H = 0$ (if $z \in N \bigcap H \subseteq N \bigcap (H + K)$ then $z \in K$ and $z \in H$ and hence $z = 0$). Hence $G = H \oplus N$. □

Proposition 7.2.3. *Let G be a finite abelian $p-$group. Then G is uniquely direct product of cyclic $p-$groups.*

Proof. $|G| = p^n$ and we go by induction on n. The statement is certainly true for $n = 1$. Assume that it holds for all positive integers less than or equal to m and now suppose that $|G| = p^{m+1}$. If G is cyclic, we are done. If not, we apply the previous lemma to decompose $G = H \oplus N$ where H is a cyclic subgroup of G of maximal order and note that as G is not cyclic, $|H| < |G|$ and we apply the inductive hypothesis to the smaller $p-$group N. Uniqueness is left as an exercise. □

Corollary 7.2.4. *Any finite abelian group is a direct product (sum) of its Sylow subgroups.*

Proof. Note that if $P_1, P_2, \cdots, P_n$ are the distinct Sylow $p-$ subgroups (corresponding to the distinct prime dividing $|G|$) then each $P_i \bigcap (P_1 + P_2 \cdots P_{i-1} + P_{i+1} + \cdots + P_n = 0$ and $P_1 + P_2 + \cdots + P_n$ and hence $G = P_1 \oplus P_2 \oplus \cdots \oplus P_n$. □

Theorem 7.2.5. *Suppose that G is a finite abelian group of order n. Then G can be decomposed as follows:*

1. *A finite direct product of groups of prime power order, where n is the product of all the orders (elementary divisor decomposition where the elementary divisors are the relevant prime powers).*
2. *As a direct product of cyclic groups $C_1 \oplus C_2 \oplus \cdots \oplus C_k$ with each C_i of order m_i with $m_1 | m_2 | \cdots | m_k$, $m_1 m_2 \cdots m_k = n$ and m_k equal to the exponent of G (invariant factor decomposition where the invariant factors are the integers $m_1, m_2, \cdots, m_k$).*

Both of these decompositions are unique up to isomorphism.

Proof. Most of this is immediate from the previous. □

We present the standard generalization of the previosu without proof.

Proposition 7.2.6 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Any finitely generated abelian group, G, is isomorphic to $(\oplus_{k=1}^{n} \mathbb{Z}) \oplus F$ where F is a finite abelian group (and hence can be decomposed as in the previous).*

Remark 7.2.7. *In the previous proposition, we call F the torsion part of G and the $\oplus_{k=1}^{n} \mathbb{Z}$ is the free part. We say that n is the rank of the torsion part.*

Example 7.2.8. *Look at some examples with different decompositions.*

Exercises

1. Consider the finite abelian group

$$\mathbb{Z}_{108} \oplus \mathbb{Z}_{24} \oplus \mathbb{Z}_{1125} \oplus \mathbb{Z}_{420} \oplus \mathbb{Z}_{620}.$$

   a) Find the invariant factor decomposition for this group.

b) Find the elementary divisor decomposition for this group.

2. Find all abelian groups of order 288 up to isomorphism.

Chapter 8

Composition Series and Solvability

8.1 Series

Before we continue with series, we review some results from earlier exercises.

Definition 8.1.1. *If G is a group and $x, y \in G$ then the commutator of x and y is defined as $[x, y] = x^{-1}y^{-1}xy$. Additionally the group $G' = G^{(1)} = \langle [x, y] | x, y \in G \rangle$ is called the commutator subgroup of G.*

Theorem 8.1.2. *Let G be a group, $x, y \in G$ and $H \leq G$.*

1. *$xy = yx$ if and only if $[x, y] = 1$.*
2. *$H \trianglelefteq G$ if and only if $[H, G] = \langle [h, g] | h \in H, g \in G \rangle \leq H$.*
3. *$f([x, y]) = [f(x), f(y)]$ for any homomorphism on G (hence G' is characteristic in G and hence is normal in G).*
4. *G/G' is the largest abelian quotient of G (if $H \trianglelefteq G$ and G/H is abelian then $G' \leq H$ and conversely if $G' \leq H$ then $H \trianglelefteq G$ and G/H is abelian).*

Proof. Exercise. □

We will be defining various types of series used in group theory.

Definition 8.1.3. *Here we define some types of series.*

1. *A central series is a sequence of groups $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ such that $[G, G_{k+1}] \leq G_k$ for all k. If G has a central series, we say that G is nilpotent.*
2. *An upper central series of a group, G, is a sequence of the form $1 = Z_0 \trianglelefteq Z_1 \trianglelefteq \cdots \trianglelefteq Z_k \trianglelefteq \cdots$ where $Z_{k+1} = \{x \in G |$ for all $g \in G, [x, g] \in Z_k\}$. If this sequence terminates at G, we say that G is nilpotent.*

3. *A lower central series is a sequence of subgroups of G of the form $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_k \trianglerighteq \cdots$ where $G_{k+1} = [G, G_k]$.*

4. *The derived series for G is a sequence of subgroups $G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \cdots \trianglerighteq G^{(k)} \trianglerighteq \cdots$ where $G^{(k+1)} = [G^{(k)}, G^{(k)}]$. If this series terminates at 1 then we say that G is solvable.*

We define this type of series separately.

Definition 8.1.4. *Let G be a group we say that the sequence of groups*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

where each G_{k+1}/G_k is simple. We say that each G_{k+1}/G_k is a composition factor.

Here are a couple of important theorems.

Lemma 8.1.5. *Any subgroup of a solvable group is solvable.*

Proof. Exercise. □

Theorem 8.1.6. *Let G be a group and N a normal subgroup. If both N and G/N are solvable then G is solvable.*

Proof. Since G/N is solvable its derived series terminate in N/N. We write its derived series as

$$G/N = G_0/N \trianglerighteq G_1/N \trianglerighteq \cdots \trianglerighteq G_k/N \trianglerighteq N/N.$$

Note that each $(G_m/N)/(G_{m+1}/N)$ is abelian and hence G_m/G_{m+1} is abelian and hence $[G_m, G_m] \leq G_{m+1}$. So in the derived series for G, we have inductively that $G^{(m+1)} \leq [G^{(m)}, G^{(m)}]$. In particular $[G^{(k)}, G^{(k)}] \leq N$. Since N is solvable, the previous lemma finishes the proof. □

The following theorem underscores why the quest for finite simple groups was so important. we will not prove it here.

Theorem 8.1.7 (Jordan-Hölder Theorem)**.** *Any two composition series for a group G have the same length and composition factors.*

Example 8.1.8. *Look at different composition series of $\mathbb{Z}_{36}$ and other examples.*

Exercises

1. Show that S_n is not solvable if $n \geq 5$ (you may use the fact that A_n is simple if $n \geq 5$).

2. Let $|G| = p^n$. Describe the composition series for G.

3. Let G be a finite group.

a) Show that if G is a $p-$group then G is solvable.

b) Show that any group of order 675 is solvable.

4. Let G be a solvable group.

a) Show that any subgroup of G is solvable.

b) Show that if $N \trianglelefteq G$ then G/N is solvable.

Chapter 9

Ring Theory

9.1 The Basics

We spent time looking at groups, which have a single binary operation. We will look at structures that have two operations. The prototype is the integers $\mathbb{Z}$.

Definition 9.1.1. *A ring, $(R, +, \cdot)$ is a nonempty set R with two binary operations $+$ and $\cdot$ satisfying:*

1. *$(R, +)$ is an abelian group.*
2. *$\cdot$ is associative.*
3. *$\forall a, b, c \in R, a \cdot (b + c) = a \cdot b + a \cdot b$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.*

Additionally we say that R is commutative if $a \cdot b = b \cdot a$ for all $a, b \in R$ and we say R has an identity if there is an element $1_R \in R$ such that $1_R \cdot x = x \cdot 1_R = x$ for all $x \in R$.

Example 9.1.2. *Of course the integers $\mathbb{Z}$. Also the fields $\mathbb{Q}, \mathbb{R}, mathbbC$. Continuous functions on an interval to $\mathbb{R}$. $M_n(R)$ for any ring R. $\mathbb{Z}_n$, $F[[x]]$ and $F[x]$.*

Example 9.1.3. *In a commutative ring we have the famous binomial theorem. That is, if $x, y \in R$ and $N \in \mathbb{N}$ then*

$$(x + y)^N = \sum_{k=0}^{N} \binom{N}{k} x^{N-k} y^k.$$

Proposition 9.1.4. *Let R be a ring.*

1. *$0 \cdot a = a \cdot 0 = 0$ for all $a \in R$.*
2. *$-a(b) = a(-b) = -(ab)$ for all $a, b \in R$.*

3. *$(-a)(-b) = ab$ for all $a, b \in R$.*

4. *If R has an identity then it is unique and $-a = (-1)a$.*

5. *If $m, n \in \mathbb{Z}$ and $r, s \in R$ then $(mr)(ns) = mnrs$ (here mr means adding r to itself m times if $m \geq 0$ and the additive inverse of $-mr$ if m is negative).*

Proof.

1. $0 \cdot a - 0 \cdot a = 0$ and hence $(0 - 0) \cdot a = 0 \cdot a = 0$. The other one is similar.

2. $(-a)b + ab = (-a + a)b = 0$ and hence $(-a)b = -(ab)$. The other one is similar.

3. By the previous, $(-a)(-b) = a(-(-b)) = ab$.

4. Suppose that I and J are identities. Then $I = IJ = J$ (which we will rename to 1). Additionally $a + (-1)a = (1 - 1)a = 0$ and hence $(-1)a = -a$.

5. We prove the case for $m, n \in \mathbb{N}$ here and leave the general case as an exercise. To this end, we proceed by induction on m. If $m = 1$, we have $r(ns) = r(s + s + \cdots + s) = rs + rs + \cdots + rs$, n times, hence $r(ns) = nrs$. Now assume that the result holds for m and consider $((m + 1)r)(ns) = (mr + r)(ns) = (mr)(ns) + r(ns) = mnrs + nrs = (mn + n)rs = (m + 1)nrs$ and we are done by induction.

□

Definition 9.1.5. *Let R be a ring and $a \in R$.*

1. *We say that a is a left zero-divisor if there is a nonzero $b \in R$ such that $ab = 0$. We sasy that a is a right zero-divisor if there is a nonzero $b \in R$ such that $ba = 0$. a is a zero-divisor if it is both a left and right zero-divisor.*

2. *We say that a is nilpotent if there is an $n \in \mathbb{N}$ such that $a^n = 0$.*

3. *If $1 \in R$, we say that $u \in R$ is a unit if there is a $v \in R$ such that $uv = vu = 1$.*

Example 9.1.6. *Find the units in $M_2(\mathbb{R})$. Find the zero-divisors, units, and nilpotents in $\mathbb{Z}_n$.*

Proposition 9.1.7. *If R has an identity then $U(R) = \{u \in R | u \text{ is a unit}\}$ is a group under multiplication.*

Proof. Exercise. □

Proposition 9.1.8. *Let R be commutative and suppose that $u \in U(R)$ and $x, y \in R$ are nilpotent. Then $u + x \in U(R)$ and $x + y$ is nilpotent.*

Proof. Exercise. You should see why commutativity is necessary in general. □

Definition 9.1.9. *A ring R such that $R \setminus \{0\}$ is a group under multiplication (that is, every nonzero element of R is a unit) is called a division ring. A commutative division ring is called a field.*

Example 9.1.10. *The quaternions, $\mathbb{Q}$, $\mathbb{R}$, and the quotient field of a polynomial ring with two noncommutting variables.*

Definition 9.1.11. *A commutative ring with 1 is called an (integral) domain if the only zero-divisor is 0 (so $ab = 0 \Longrightarrow a = 0$ or $b = 0$).*

Proposition 9.1.12. *Any field is an integral domain.*

Proof. Suppose that $a \neq 0$ and $ab = 0$. Since R is a field there is an $x \in R$ such that $xa = 1$, and so $xab = 0 = b$. □

The next theorem demonstrates an intimate relation between fields and integral domains. Integral domains have the so-called cancellation property. We state the result in slighty more generality.

Theorem 9.1.13. *If R is a ring with no nonzero zero-divisors and $ab = ac$ for $a, b, c \in R, a \neq 0$ then $b = c$.*

Proof. We have that $a(b - c) = 0$. Since $a \neq 0$ and R has no nonzero zero-divisors, $b - c = 0$ and hence $b = c$. □

Theorem 9.1.14. *Let R be a finite commutative ring and $a \in R$. Then a is either a unit or a zero-divisor.*

We contrast this with most rings, like $\mathbb{Z}$ for example, that contain elements (in this case any element that is no ± 1 or 0 that is neither a unit nor a zero divisor.

Proof. Consider the set of powers of a: $\{a, a^2, a^3, \cdots\}$. Since R is a finite ring, the pigeon-hole principle gives that there are positive integers $1 < m < n$ such that $a^m = a^n$ (note that if $m = 1$ we can multiply this equation by a to obtain that $m > 1$. Hence we have the equation $a^{m-1}(a - a^{n-m+1}) = 0$. If a is not a zero divisor then neither is a^{m-1}.

So if a is not a zero divisor, then $a^{n-m+1} = a$. We now claim that a^{n-m} is the identity for this ring and this will complete the proof (since a power of a is a unit implies that a is a unit). Let $b \in R$ and note that $ba^{n-m+1} = ba$ and so $(ba^{n-m} - b)a = 0$. Since a is not a zero-divisor, we have $ba^{n-m} = b$ for all $b \in R$. So $a^{n-m} = 1$ and hence a is a unit. □

Corollary 9.1.15. *Any finite integral domain is a field.*

Proof. Let $x \in R \setminus \{0\}$. Since R is a domain, then x is not a zero-divisor and so, by the previous, $x \in U(R)$ and hence R is a field. □

Definition 9.1.16. *Let R be a ring. A subring of R is a subgroup $T \subseteq R$ that is closed under multiplication (sometimes we will demand that if R has an identity 1_R, then $1_R \in T$).*

Example 9.1.17. $\mathbb{Z} \subseteq \mathbb{R}$ *or* $\mathbb{Z}[x]$. *Perhaps* $2\mathbb{Z} \subseteq \mathbb{Z}$.

Exercises

1. Let R be a commutative ring with identity and let $x, y \in R$ be nilpotent elements.

   a) Show that $x + y$ and xy are nilpotent elements.

   b) Show that if u is a unit of R and x is nilpotent, then $u + x$ is a unit.

   c) Show that if R is not commutative, neither of the above necessarily holds ($x + y$ is not necessarily nilpotent and $u + x$ is not necessarily a unit).

2. Find all subrings of $\mathbb{Z}$ and prove that your list is complete.

3. Give examples or prove the following.

   a) A ring with a left identity but no right identity.

   b) Show that if R has a left identity that is not a right identity, then it has more than one left identity.

   c) Show that if R has a left and right identity, then it is unique.

4. Let R be a ring. We say that the characteristic of R ($\text{char}(R)$) is $n \in \mathbb{N}$ if $nr = 0$ for all $r \in R$ and n is minimal with respect to this property (and we say that the $\text{char}(R) = 0$ if no such n exists.

   a) Show that if R has identity 1_R then $\text{char}(R) = n \in \mathbb{N}$ if and only if $n1_R = 0$ and n is minimal with respect to this property.

   b) Show that if R is an integral domain then $\text{char}(R)$ is either a positive prime or 0.

5. (*The Freshman's Dream*) Show that if R is a commutative ring with 1 such that $\text{char}(R) = p$ where p is a prime then $(a + b)^{p^n} = a^{p^n} + b^{p^n}$.

6. We define a Boolean ring to be a ring R such that $x^2 = x$ for all $x \in R$.

   a) Show that a Boolean ring is commutative and of characteristic 2.

   b) If R is the set of subsets of a set U and $A, B \in R$ and we define $A + B = (A \setminus B) \bigcup (B \setminus A)$ and $AB = A \bigcap B$, show that R is a Boolean ring.

7. Let R be a ring and $\phi : R \longrightarrow T$ a nonzero homomorphism. Show that if T has no nonzero zero divisors and R has an identity then $f(1_R) = 1_T$.

8. Let R be a ring with the property that for all $a \in R$ there exists unique $b \in R$ such that $aba = a$. Prove the following.

   a) R has no nonzero zero divisors.

   b) $bab = b$.

   c) R has an identity.

d) R is a division ring.

9. Let R be a ring. We define the opposite ring R^{op} to be the abelian group $(R, +)$ and new multiplicative operation $\circ$ defined by $x \circ y = yx$. We also define the center of the ring R to be $Z(R) = \{x \in R | xy = yx \text{ for all } y \in R\}$.

   a) Show that R^{op} is a ring and $(R^{op})^{op} \cong R$.

   b) Show $Z(R) = Z(R^{op})$ and show that $R = R^{op}$ (as rings) if and only if R is commutative.

   c) Show that R has identity if and only if R^{op} has an identity.

   d) Show that R is a division ring if and only if R^{op} is a division ring.

   e) Show that $R \cong S$ if and only if $R^{op} \cong S^{op}$.

9.2 Ideals and Homomorphisms

The "ideal" concept is the analog of "normal subgroup" that we encountered before and the notion of homomoprhism is the analog in the case of rings. We begin with this concept.

Definition 9.2.1. *Let R, T be rings. A function $f : R \longrightarrow T$ is a homomorphism (of rings) if*

1. *$f(x + y) = f(x) + f(y)$ for all $x, y \in R$ (so is a homomorphis of abelian groups) and*
2. *$f(xy) = f(x)f(y)$ for all $x, y \in R$.*

Definition 9.2.2. *Let $f : R \longrightarrow T$ be a homomorphism of rings. Then $ker(f) = \{x \in R | f(x) = 0\}$.*

Remark 9.2.3. *The previous adjectives apply. for instance, a homomorphism is an isomorphism if it is one to one and onto etc.*

The concept of homomorphism and ideal is intimately connected as it is for groups (recall a normal subgroup is the kernel of a homomorphism and the analog will be true for rings). Our first definition will distinguish the case for rings which are not necessarily commutative.

Definition 9.2.4. *A (left) ideal $I \subseteq R$ is a subgroup of R such that $rI \subseteq I$ for all $r \in R$. The left ideal is an (two sided) ideal if $Ir \subseteq I$ for all $r \in R$ as well. We say that the ideal is proper if $I \subsetneq R$.*

Proposition 9.2.5. *Let R, T be rings and $f : R \longrightarrow T$ a homomorphism.*

1. *$im(f)$ is a subring of T.*
2. *$ker(f)$ is an ideal of R*

Proof. The proof of 1. will be left as an exercise. For 2. note that we already know that $\ker(f)$ is a (normal) subgroup of R. It suffice to show that rI and Ir are both contained in I. To this end, let $x \in \ker(f)$ and note that for all $r \in R$ $f(rx) = f(r)f(x) = 0 = f(x)f(r) = f(xr)$. □

The next lemma is a simple observation, but will prove useful later.

Lemma 9.2.6. *Let R be a ring with identity and $I \subseteq R$ a left ideal. If $1 \in I$ then $I = R$.*

Proof. Clearly $I \subseteq R$. Now suppose that $a \in I$ and let $r \in R$. Since I is a left ideal and $1 \in I$, $r \cdot 1 = r \in I$ and hence $R = I$. □

Just like for groups, we can form a quotient structure (quotient ring) as follows.

Proposition 9.2.7. *Let R be a ring and $I \subseteq R$ an ideal. Then $R/I = \{r+I | r \in R\}$, the quotient group, can be made into a ring with the operations*

1. $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$
2. $(r_1 + I)(r_2 + I) = r_1 r_2 + I$.

Proof. We leave most of this as an exercise. Note that the fact that R/I is an abelian group is known to us from the work we did in group theory. We will show first that the multiplication is well-defined. Suppose that $a+I = x+I$ and $b+I = y+I$. Hence $a-x, b-y \in I$. Since I is a right ideal, $ab-xb \in I$ and since it is a left ideal, $xb-xy \in I$. Hence $ab-xb+xb-xy \in I$ and so $ab+I = xy+I$. The associate and distributive properties follow pretty easily. □

Remark 9.2.8. *If R is commutative, then so is R/I. Additionally, if R has an identity 1_R then R/I has identity $1_R + I$.*

We now give the analog of the isomorphism theorems.

Theorem 9.2.9 (First Isomorphism Theorem)**.** *If $f : R \longrightarrow T$ is a homomorphism then $ker(f)$ is an ideal of R, $im(f)$ is a subring of T and*

$$R/ker(f) \cong im(f).$$

Also, given any ideal $I \subseteq R$ there is an epimorphism $\pi_I : R \longrightarrow R/I$ given by $\pi_I(r) = r + I$.

Proof. We know that the relation $\overline{f} : R/\ker(f) \longrightarrow \text{im}(f)$ given by $\overline{f}(r + \ker(f)) = f(r)$ is a well-defined function and is, in fact an isomorphism of groups. We only need to show that this function preserves multiplication to finish the result. Letting $K = \ker(f)$, we note that $\overline{f}((r_1 + K)(r_2 + K)) = \overline{f}(r_1 r_2 + K) = f(r_1 r_2) = f(r_1)f(r_2) = \overline{f}(r_1 + K)\overline{f}(r_2 + K)$. We leave the final remark as an exercise. □

The next application is a nice example of this.

Example 9.2.10. *We wish to show that the Diophantine equation $x^2-10y^2=2$ has no solutions for $x,y\in\mathbb{Z}$. To the contrary, we suppose that the integers a,b satisfy $a^2-10b^2=2$. Consider the epimorphism*

$$\phi : Z \longrightarrow \mathbb{Z}_5$$

given by $\phi(n)=\overline{n}$ where $\overline{n}$ is the reduction of n modulo 5. It is an easy exercise to see that ϕ is an onto homomorphism. If $a^2-10b^2=2$ then applying ϕ, we obtain the equation in $\mathbb{Z}_5$

$$\overline{a}^2-\overline{10}\overline{b}^2=\overline{a}^2=\overline{2}$$

and since $\mathbb{Z}_5$ is a finite field, it is easy to check that $\overline{2}$ is not a square. Since there is no solution in $\mathbb{Z}_5$ there cannot be a solution in $\mathbb{Z}$.

It should be noted that this example is not trivial. The equation $x^2-94y^2=1$ has solution $x=\pm1$ and $y=0$, but also has nontrivial solutions, the smallest of which is $x=2143295$ and $y=221064$

Theorem 9.2.11 (Second Isomorphism Theorem)**.** *Let A be a subring of R and B an ideal of R. Then $A+B:=\{a+b|a\in A,b\in B\}$ is a subring of R and $A\bigcap B$ is an ideal of A,and*

$$(A+B)/B\cong A/(A\bigcap B).$$

Proof. We leave as an exercise that $A+B$ is a subring and that $A\bigcap B$ is an ideal of A. To establish the isomorphism we consider $f:A\longrightarrow(A+B)/B$ given by $f(a)=(a+0)+B=a+B$ we have seen that this is a group homomorphism with kernel precisely equal to $A\bigcap B$. It suffices to show that f respects the multiplication. To this end $f(xy)=xy+B=(x+B)(y+B)=f(x)f(y)$ and this completes the proof. □

Theorem 9.2.12 (Third Isomorphism Theorem)**.** *Let $I,J\subseteq R$ be ideals with $I\subseteq J$. Then J/I is an ideal of R/I and $(R/I)/(J/I)\cong R/J$. What is more there is a one to one correspondence between the ideals (resp. subrings) of R containing I and the ideals (resp. subrings) of R/I*

Proof. The fact that $(R/I)/(J/I)\cong R/J$ as groups has been established and the verification for rings is an exercise (show the homomphism used before in the Third Isomorphism Theorem is a ring homomorphism in this context. We will concentrate on the correspondence.

Let T be a subring of R/I. The group theory assures us that T is of the form A/I for some subgroup A of R containing I. Since $T=A/I$ is a subring then for all $x,y\in A$, $(x+I)(y+I)=xy+I\in T$ and hence $xy\in A$ and so A a subring of R containing I. Additionally if T is an ideal of R/I then (again) we can write $T=A/I$ and since for all $r+I\in R/I$, $(r+I)T\subseteq T=A/I$, $ra\in A$ for all $r\in R$ and hence A is an ideal of R containing I.

On the other hand, suppose that A is a subring of R containing I, then as I is an ideal of R, it is an ideal of A and hence A/I is a subring of R/I. Additionally if A is an ideal, then it is easy to see that A/I is an ideal of R/I. □

9.3 Ideal Types and Constructions

The ideals themselves have an algebraic structure. Here are some basic constructions. But we begin with a basic theorem that will prove very useful.

Proposition 9.3.1. *If R is commutative with 1, then $I \subseteq R$ is an ideal if and only if for all $x, y \in I$ and $r \in R$, $x + ry \in I$.*

Proposition 9.3.2 (Sums and Products)**.** *Let $I, J \subseteq R$ be ideals. The following are also ideals of R.*

1. $I \bigcap J$
2. $I + J = \{x + y | x \in I, y \in J\}$.
3. $IJ = \{\sum_{i=1}^{n} a_i b_i | a_i \in I, b_i \in J\}$.
4. $I^m = \{\sum_{i=1}^{n} a_{1,i} a_{2,i} \cdots a_{m,i} | a_{j,i} \in I\}$.

The ideal $I + J$ is the smallest ideal of R containing both I and J. Also $IJ \subseteq I \bigcap J$.

Definition 9.3.3. *Let R be a ring and $A \subseteq R$ a subset. We define the ideal generated by A to be the smallest ideal of R that contains A (we write $\langle A \rangle = \bigcap_{A \subseteq I} I$ where the intersection is taken over all ideals containing A). If $|A| < \infty$ we say that $\langle A \rangle$ is finitely generated and if $|A| = 1$ then we say that it is principal.*

Note that if $A = \emptyset$ then $\langle A \rangle = 0$.

Remark 9.3.4. *In general, if R has identity, the left ideal generated by A is $RA = \{\sum r_i a_i | r_i \in R, a_i \in I\}$ and the right ideal $AR = \{\sum a_i r_i | r_i \in R, a_i \in I\}$ and the two-sided ideal generated by A is $RAR = \{\sum r_i a_i s_i | r_i, s_i \in R, a_i \in I\}$. In the commutative setting (with identity) these are all the same set. Without identity, these ideals become a bit more complicated. For example, if $a \in R$ and R is not assumed to have an identity or commutative, then a general element of $\langle a \rangle$ is of the form $t_1 a + a t_2 + \sum_{i=1}^{k} r_i a r_i' + na$ where $t_i, r_i, r_i' \in R$ and $n \in \mathbb{Z}$. If R is commutative, then we can reduce this to $ra + na, r \in R, n \in \mathbb{Z}$, if R has an identity, we can reduce this to $\sum_{i=1}^{k} r_i a r_i'$ with $r_i, r_i' \in R$ and if R is commutative with 1, then this further reduces to $ra, r \in R$.*

The last remark shows why shortly we will begin looking mostly at commutative rings with 1.

Lemma 9.3.5. *Suppose that R is a ring with identity and $I \subseteq R$ is an ideal.*

1. *$I = R$ if and only if I contains a unit in R.*
2. *If R is commutative then R is a field if and only if 0 is the only proper ideal.*

Proof. For the first statement, if $I = R$ then $1 \in I$ and this direction is complete. On the other hand if there is a $u \in U(R)$ that is in I then $uu^{-1} = 1 \in I$ and since $1 \in I$ then $r \cot 1 \in I$ for all $r \in R$ and hence $R = I$.

If R is a field and I is a proper ideal, we suppose that $x \in I$ if $x \neq 0$ then $xx^{-1} = 1 \in I$ and hence $I = R$ by the previous. Hence $I = 0$. Conversely suppose that 0 is the only proper ideal. Let $0 \neq x \in R$. Then $(x) = R$ and hence $1 \in (x)$. Hence there is a $y \in R$ such that $xy = 1$ and hence R is a field. □

Definition 9.3.6. *An ideal $M \subsetneq R$ is said to be maximal if it is proper and if N is an ideal such that $M \subseteq N \subseteq R$, then either $N = M$ or $N = R$. A proper ideal $P \subsetneq R$ is prime if for all ideals $A, B \subseteq R$, if $AB \subseteq P$ the either $A \subseteq P$ or $B \subseteq P$.*

Proposition 9.3.7. *If R is commutative ring with 1, then $P \subsetneq R$ is prime if and only if for all $a, b \in R$, $ab \in P \implies a \in P$ or $b \in P$.*

Proof. Suppose that P is prime. Since $ab \in P$, $(ab) \subseteq P$. Since P is prime then we can say WLOG that $(a) \subseteq P$ and hence $a \in P$.

We now suppose that if $ab \in P$ then $a \in P$ or $b \in P$. Let $AB \subseteq P$ and suppose that B is not contained in P. Then there is a $b \in B$ that is not in B. Since $AB \subseteq P$ then for all $a \in A, ab \in AB \subseteq P$. Hence, since $b \notin P$, then $a \in P$ for all $a \in A$ and so $A \subseteq P$. □

Definition 9.3.8. *Let R be commutative ring with 1, and $I \subseteq R$. We define the radical of I to be $\sqrt{I} = \{x \in R | x^n \in I,$ for some $n \in \mathbb{N}\}$. We say that I is a radical ideal if $I = \sqrt{I}$.*

We now need a result that is equivalent to the Axiom of Choice.

Axiom 9.3.9 (Zorn's Lemma)**.** *If S is a nonempty partially ordered set with the property that every chain has an upper bound in S. Then S has a maximal element.*

Theorem 9.3.10. *If R is a ring with 1 and $I \subseteq R$ an ideal. Then I is contained in a maximal ideal (in particular, any ring with identity has a maximal ideal).*

Proof. Let $I \subsetneq R$ and let S be the collection of all proper ideals of R containing I. This set is partially ordered by inclusion. Now let C be a chain in S and let $J = \bigcup_{A \in C} A$. We show that J is an upper bound for the chain C. Note that J contains every A in C so we only need to show that A is an element of S. To see that S is an ideal, we suppose that $x, y \in J$. Then $x \in A$ and $y \in B$ for $A, B \in C$. we will assume without loss of generality that $A \subseteq B$. Hence $x + y \in B \subseteq J$.

Also if $r \in R$ and $x \in J$ then $x \in A$ for some $A \in C$. Hence $ra, ar \in A \subseteq C$. It remains to see that J is proper, but we have seen that J is proper if and only if $1 \notin J$. But if $1 \in J$ then $1 \in A$ for some $A \in C$ which is a contradiction. So Zorn's Lemma gives that S has a maximal element and hence I is contained in a maximal ideal. □

Example 9.3.11. *If R does not have an identity, it might or might not have a maximal ideal. Consider, for example, all polynomials over $\mathbb{R}$ with real exponents. To see that Zorn's Lemma is actually doing something, consider the maximal ideal of $\prod_{n\in\mathbb{N}}\mathbb{Z}_2$ that contains $\oplus_{n\in\mathbb{N}}\mathbb{Z}_2$*

Here is an important connection.

Theorem 9.3.12. *Let R be commutative with 1 and $M \subseteq R$ a maximal ideal. Then M is prime.*

Proof. Suppose that $ab \in M$ and that neither a nor b is in M. Since M is maximal, both (M, a) and (M, b) are all of R. Hence there are $m_1, m_2 \in M$ and $r_1, r_2 \in R$ such that $m_1 + r_1a = 1$ and $m_2 + r_2b = 1$. Multiplying, we obtain that $1 = m_1m_2 + r_2m_1b + r_1m_2a + r_1r_2ab \in M$, which is our desired contradiction. □

Example 9.3.13. *Look at some primes in $\mathbb{Z}$ and $\mathbb{Z}[x]$.*

Definition 9.3.14. *We say that R is reduced if R has no nonzero nilpotents.*

We now characterize these types of ideals in terms of quotients. This theorem can be very useful in applications. The proof is fairly straightforward and is a good exercise.

Theorem 9.3.15. *Let R be a commutative ring with 1 and $I \subsetneq R$ a proper ideal.*

1. *I is maximal if and only if R/I is a field.*
2. *I is prime if and only if R/I is an integral domain.*
3. *I is radical if and only if R/I is reduced.*

In preparation for the Chinese Reainder Theorem (and for the good of mathematics in general) we introduce the notion of direct product. This is exactly the analog of direct product in groups that you might think and it is a central construction in ring theorey (and a rich way to make new rings from old).

Definition 9.3.16. *Let $\{R_i\}_{i\in\Lambda}$ be a family of rings. We define the direct product of this family of rings to be the ring with underlying group $\prod_{i\in\Lambda} R_i$ and multiplication componentwise (that is $(r_i) \cdot (r_i') = (r_ir_i')$).*

Definition 9.3.17. *We say that the ideals $I, J \subseteq R$ are comaximal if $I+J = R$.*

With this definition in hand, we now give the celebrated Chinese Remainder Theorem.

Theorem 9.3.18 (Chinese Remainder Theorem)**.** *Let $I_1, I_2, \cdots, I_k$ be ideals of R. Then the function*

$$f : R \longrightarrow R/I_1 \times R/I_2 \times \cdots \times R/I_k$$

given by

$$f(r) = (r + I_1, r + I_2, \cdots, r + I_k)$$

is a ring homomorpism with kernel $I_1 \bigcap I_2 \bigcap \cdots \bigcap I_k$.

If in addition, the ideals are pairwise comaximal, then $I_1 \bigcap I_2 \bigcap \cdots \bigcap I_k = I_1 I_2 \cdots I_k$ *and*

$$R/I_1 I_2 \cdots I_k \cong R/I_1 \times R/I_2 \times \cdots \times R/I_k.$$

Proof. Consider the function $f(r) = (r + I_1, r + I_2, \cdots, r + I_k)$. Because of the rules of cosets addition and multiplication, this is homomorphism (check this). If $r \in \ker(f)$ then $(r+I_1, r+I_2, \cdots, r+I_k) = (0+I_1, 0+I_2, \cdots, 0+I_k)$ and hence $r \in \bigcap_{i=1}^{k} I_i$. And conversely, if $r \in \bigcap_{i=1}^{k} I_i$ then $f(r) = (0+I_1, 0+I_2, \cdots, 0+I_k)$ and the second statement is established.

For the second statement we use induction with the base case being $k = 2$. For convenience of notation, we will write $I = I_1$ and $J = I_2$. We first show that if I, J are comaximal then $I \bigcap J = IJ$. Note that it is easy to see that $IJ \subseteq I \bigcap J$. For the other containment, we let $a \in I \bigcap J$. Since I and J are comaximal, there are elements $x \in I$ and $y \in J$ such that $x + y = 1$. So $a = ax + ay$ but both terms on the right side are in $I \bigcap J$ and we have the other containment.

For the other statement, we consider the function $f : R \longrightarrow R/I \times R/J$ given by $f(r) = (r + I, r + J)$. It is easy to verify that this is a ring homomorphism. We now use the fact that I and J are comaximal to show that f is onto.

Suppose that $(r_1 + I, r_2 + J) \in R/I \times R/J$ is arbitrary. Since $I + J = R$ there are $\alpha \in I$ and $\beta \in J$ such that $r_1 - r_2 = \alpha + \beta$, and so $z := r_1 - \alpha = r_2 + \beta$. Note now that $f(z) = (z + I, z + J) = (r_1 - \alpha + I, r_2 + \beta + J) = (r_1 + I, r_2 + J)$. Hence f is onto. By the first isomorphism and the previous paragraph, we have that

$$R/IJ \cong R/I \times R/J.$$

We now assume for some $m \in \mathbb{N}$, $m \geq 2$, the statement of the theorem holds. We now suppose that we have $m + 1$ pairwise comaximal ideals $I_1, I_2, \cdots, I_m, I_{m+1}$. Letting $J := I_1 I_2 \cdots I_m$, we first note that $I := I_{m+1}$ and J are comaximal. If this is not the case, there is a maximal (and hence prime) ideal, M, of R such that M contains both I and J. But since M contains J and is prime, then for some $1 \leq k \leq m$, M contains I_k and M contains $I = I_{m+1}$ which is a contradiction.

By induction $J = \bigcap_{i=1}^{m} I_i$ and by the base case $J \bigcap I = JI$. Hence $\bigcap_{i=1}^{m+1} I_i = J \bigcap I = JI = \prod_{i=1}^{m+1} I_i$.

Also by the base case, we have that $R/IJ \cong R/I \times R/J$ and by the inductive step,

$$R/(\prod_{i=1}^{m+1} I_i) \cong R/IJ \cong R/J \times R/I \cong \prod_{i=1}^{m} R/I_i \times R/I_{m+1} \cong \prod_{i=1}^{m+1} R/I_i$$

□

Example 9.3.19. *Count the units in $\mathbb{Z}_{360}$. Also look at te old Chinese army trick.*

9.4 Multiplicative Sets and Localization ("Fractions")

In this section, R will be a commutative ring with 1 unless specified otherwise.

Definition 9.4.1. *Let R be commutative with 1. A multiplicatively closed subset $S \subseteq R$ is a set satisfying $s, t \in S \implies ab \in S$ (we usually take the convention that $0 \notin S$).*

Example 9.4.2. *$U(R)$ is such a set. So is the nonzero even integers and the odd integers in $\mathbb{Z}$. So are the nonzero polynomials in $\mathbb{Z}[x]$. Also the compliment of a prime ideal in R has this property (and this is central to the notion).*

Definition 9.4.3. *A (multiplicatively closed) set $S \subseteq R$ is said to be saturated if it contains its divisors. More precisely, we say that S is saturated if $st \in S \implies s, t \in S$.*

Example 9.4.4. *The complement of an ideal is saturated and is multiplicatively closed if and only if R is prime. The units are multiplicatively closed and saturated (although rarely the complement of a single prime).*

The next theorem is a very important one. The proof is not super hard, but is very instructive and is left for an exercise. This is the first in a line of theorems that have to do with maximality properties. Before the theorem, we have a definition.

Definition 9.4.5. *We say that the ideal I is maximal with respect to the property $\mathbb{P}$ if I has the property $\mathbb{P}$ and any ideal properly containing I does not have the property $\mathbb{P}$. For example, if S is a multiplicatively closed set and I is maximal with respect to the property that $I \bigcap S = \emptyset$ then any ideal strictly containing I must intersect S nontrivially.*

Theorem 9.4.6. *Let $S \subset R$ be a multiplicatively closed set and $I \subseteq R$ and ideal maximal with respect to the exclusion of S (maximal with respect to the property that $I \bigcap S = \emptyset$). Then I is prime.*

Proof. Exercise. □

Of course the question is: "given a multiplicatively closed set $S \subset R$ does there exist an ideal I that is maximal with respect to the exclusion of S?" The answer (via Zorn's Lemma again) is "yes".

Theorem 9.4.7. *If $I \bigcap S = \emptyset$ then there is an ideal $J \supseteq I$ such that J is maximal with respect to the exclusion of I.*

Proof. Once again we will have a Zorn's Lemma strategy. Let $\Gamma = \{A \subsetneq R | I \subseteq A \text{ and } A \bigcap S = \emptyset\}$ and partially order Γ by set-theoretic inclusion. Let $\mathcal{C} = \{I_\alpha\}_{\alpha \in \Lambda}$ be a chain in Γ. We let $B = \bigcup_{\alpha \in \Lambda} I_\alpha$ and claim that B is an upper bound for $\mathcal{C}$. certainly it is the case that every element of the chain is in B and that B contains I, so it remains to show that B is a proper ideal. If $x, y \in B$ and $r \in R$ then $x \in I_\alpha$ and $y \in I_\beta$ for some $\alpha, \beta \in \Lambda$. Without loss of generality, we will say that $I_\alpha \subseteq I_\beta$ and hence $x + ry \in I_\beta \subseteq B$. So B is an ideal and since $1 \notin B$, it is a proper ideal.

Finally note that if $B \bigcap S$ is not empty then there is some $b \in B$ that is also in S. Since B is the unioin of the chain, then b is in some I_α and hence $I_\alpha \bigcap S$ is not empty and this is our desired contradiction. □

We put this together:

Corollary 9.4.8. *Let $I \subsetneq R$ be an ideal and S a multiplicatively closed subset of R such that $S \bigcap I = \emptyset$. Then we can expand I to a (prime) ideal that is maximal with respect to the exclusion of S.*

Corollary 9.4.9. *If R is a commutative ring with 1 and $I \subsetneq R$ is an ideal then I is contained in a maximal ideal (in particular, any commmutative ring with 1 contains a maximal ideal).*

Proof. If $I \subsetneq R$ is an ideal then $I \bigcap U(R) = \emptyset$. Apply the previous and note that any ideal that is maximal with respect to the exclusion of the units must be maximal. □

Here is another very important result concerning multiplicative sets.

Theorem 9.4.10. *Let $S \subseteq R$ be a multiplicative set (with 0 not in S). The following are equivalent.*

1. *S is multiplicatively closed and saturated.*
2. *S^c is a union of prime ideals.*

Proof. (2. $\implies$ 1.) Let $a, b \in S$. Since a, b is in the complement of the union of the primes $\{P_i | i \in I\}$, then for all $i \in I$, $a, b \notin P_i$ and hence $ab \notin P_i$ as each P_i is prime. Hence $ab \in S$. Additionally we suppose that $ab \in S$, and we will suppose that $a \in P_i$ for some $i \in I$. Then as P_i is an ideal, $ab \in P_i$ and hence $a \notin P_i$ for all i and hence $a \in S$. Similarly, $b \in S$ and so S is saturated.

(1. $\implies$ 2.) Let $x \in S^c$ then (x) is disjoint form S as S is saturated. We exapnd (x) to a prime ideal P_x containing x such that $P_x \bigcap S = \emptyset$. $x \in P_x$ and so $S^c = \bigcap_{x \in S^c} P_x$. □

So what are these animlas (multiplicatively closed sets) actually for? One of the important applications is to use them to make "fractions". This general construction is called a localization.

Definition 9.4.11. *Let R be a commutative ring and $S \subset R$ a multiplicatively closed set. We define and equivalence relation on the set $R \times S$ by*

$$(r_1, s_1) \sim (r_2, s_2) \iff \exists s \in S \text{ such that } s(r_1 s_2 - r_2 s_1) = 0.$$

The set of equivalence classes $(R \times S)/\sim = S^{-1}R = R_S$ is called the localization of R at the set S.

You should verify that this is indeed an equivalence relation. It should also be noted that the definition of the relation is much easier in the case where R has no nonzero zero-divisors as it collapses to

$$(r_1, s_1) \sim (r_2, s_2) \iff (r_1 s_2 - r_2 s_1) = 0.$$

We also often write the equivalence class $[(r, s)]$ in the form $\frac{r}{s}$ (familiar fraction notation). We finally note that if $0 \in S$ then $R_S = 0$.

Proposition 9.4.12. *The set R_S of equivalence classes forms a ring with the operations*

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$$

and

$$(\frac{r_1}{s_1})(\frac{r_2}{s_2}) = \frac{r_1 r_2}{s_1 s_2}$$

form a ring with identity s/s for $s \in S$.

Proof. This is an exercise in bookkeeping. We must make sure that the multiplication and addition are well-defined and that the associativity and all that jazz works out. Please attempt this. □

Proposition 9.4.13. *Let s be a fixed element of S, then there is a homomorphism $f : R \longrightarrow R_S$ given by $f(r) = \frac{rs}{s}$. Additionally $ker(f) = \{x \in R | tx = 0, \text{ some } t \in S\}$ and so if R has no nonzero zero-divisors then f is one to one (and so in this case R may be viewed as a subring of R_S).*

Proof. Note that $f(r_1 + r_2) = \frac{s(r_1+r_2)}{s} = f(r_1) + f(r_2)$ and $f(r_1 r_2) = \frac{s(r_1 r_2)}{s} = \frac{sr_1}{s}\frac{sr_2}{s}$. Now note that if $tx = 0$ for some $t \in S$ then $f(x) = \frac{sx}{s}$ and this "fraction" is equivalent to 0. On the other hand if $\frac{sx}{s} = 0$ then there is a $t \in S$ such that $tsx = 0$ and hence x has the property claimed. □

Example 9.4.14. *If R is an integral domain the $S = R \backslash \{0\}$ is a multiplicatively closed set and R_S is a field (called the quotient field of R. more generally if S is the complement of a prime ideal P then R_S is written as R_P (unfortunate notation). $R_P = \{\frac{r}{s} | s \in R \setminus P\}$.*

Definition 9.4.15. *A ring with only one maximal ideal is called quasilocal and a ring with only finitely many maximal ideals is called semiquasilocal.*

Example 9.4.16. *If P is a prime ideal of R then R_P is quasilocal.*

Theorem 9.4.17. *Let $0 \neq S \subset R$ be a multiplicatively closed subset, then there is a one to one correspondence between the (prime) ideals of R that miss S and the prime ideals of R_S (given by $P \longleftrightarrow P_S$).*

Proof. We first note that if I is an ideal of R then I_S is an ideal of R_S. By the addition rule, this clearly forms a subgroup and if $\frac{\alpha}{s} \in I_S$ and $\frac{r}{s'} \in R_S$ then $\frac{r\alpha}{ss'} \in I_S$.

We now observe that P_S is prime if and only if P is prime in R. First suppose that P is prime and that $\frac{r}{s}\frac{x}{t} = \frac{p}{u} \in P_S$ with $s,t,u \in S, p \in P$. So there is an $s' \in S$ such that $s'[urx - stp] = 0 \in P$. Since $s', u \notin P$, we get that $rx \in P$ hence either r or x (and hence either $\frac{r}{s}$ or $\frac{x}{t}$ is in P_S). On the other hand if P_S is prime and $rx \in P$ then $\frac{r}{s}\frac{x}{s} \in P_S$ and we conclude without loss of generality that $\frac{r}{s} \in P_S$. So $\frac{r}{s} = \frac{p}{t}$ with $p \in P$ and $t \in S$. Hence there is $s' \in S$ such that $s'[rt - ps] = 0$. Since $s', t \notin P$, $r \in P$.

So the (prime) ideal P corresponds to the (prime) ideal P_S. We now suppose that $\mathfrak{P}$ is a (prime) ideal of R_S and let $P = \{p \in R | \frac{p}{s} \in \mathfrak{P}$ for some $s \in S\}$. It is easy to show that P is an ideal of R. Now suppose that $\mathfrak{P}$ is prime and $xy \in P$. So there is an $s \in S$ such that $\frac{xy}{s} = \frac{xs}{s}\frac{y}{s} \in \mathfrak{P}$. Suppose that $\frac{xs}{s} \in \mathfrak{P}$. In this case, $\frac{xs}{s}\frac{s}{s^2} = \frac{x}{s} \in \mathfrak{P}$ and so $x \in P$. If $\frac{y}{s} \in \mathfrak{P}$ then the fact that $y \in P$ is immediate.

Note that $\mathfrak{P} = P_S$ and if you start with the prime $P \subset R$ you return to P after two of these operations. This establishes the theorem. □

Chapter 10

Polynomial and Power Series Rings

10.1 The Basics

Polynomial and power series rings are fundamental constructions in algebra that lend themselves to many applications all over the map. We begin by defining these objects. We have seen these used previously for examples. Here will will introduce some of their properties as a formal listing. Most of the proofs are fairly routine and left as exercises.

Definition 10.1.1. *Let R be a commutative ring with 1. We define the ring of polynomials over R to be $R[x] = \{\sum_{k=0}^{n} r_k x^k | r_k \in R\}$. Addition is given by $\sum_{k=0}^{n} r_k x^k + \sum_{k=0}^{n} r'_k x^k = \sum_{k=0}^{n} (r_k + r'_k) x^k$ and multiplication given by $(\sum_{k=0}^{n} r_k x^k)(\sum_{k=0}^{m} r'_k x^k) = \sum_{k=0}^{n+m} c_k x^k$ where $c_k = \sum_{i=0}^{k} r_i r'_{k-i}$.*

For polynomials we have the notion of "degree" which is especially useful in the case where R is an integral domain.

Definition 10.1.2. *If $f(x) = \sum_{k=0}^{n} r_k x^k$ and $r_n \neq 0$ we say that the degree of $f(x)$, $deg(f(x)) = n$.*

Here is a fundamental theorem concerning properties of polynomial rings. The proof is an exercise.

Theorem 10.1.3. *Let R be a commutative ring with 1.*

1. *If R is an integral domain, then $deg(f(x)g(x)) = deg(f(x)) + deg(g(x))$.*
2. *If R is an integral domain, then so is $R[x]$.*
3. *If R is an integral domain, then $U(R) = U(R[x])$.*
4. *If $I \subset R$ is an ideal then $I[x] = \{\sum_{k=0}^{n} \alpha_k x^k | \alpha_k \in I\}$ is an ideal of $R[x]$.*

5. *$R[x]/I[x] \cong (R/I)[x]$ and $R[x]/(I,x) \cong R/I$.*

6. *I is prime if and only if $I[x]$ is prime if and only if (I,x) is prime.*

Power series are (very loosely speaking) polynomial that may continue indefinitely.

Definition 10.1.4. *Let R be a commutative ring with 1. We define the ring of formal power series over R to be $R[[x]] = \{\sum_{k=0}^{\infty} r_k x^k | r_k \in R\}$. Addition is given by $\sum_{k=0}^{\infty} r_k x^k + \sum_{k=0}^{\infty} r'_k x^k = \sum_{k=0}^{\infty} (r_k + r'_k) x^k$ and multiplication given by $(\sum_{k=0}^{\infty} r_k x^k)(\sum_{k=0}^{\infty} r'_k x^k) = \sum_{k=0}^{\infty} c_k x^k$ where $c_k = \sum_{i=0}^{k} r_i r'_{k-i}$.*

Theorem 10.1.5. *Let R be a commutative ring with 1.*

1. *R is an integral domain if and only if $R[[x]]$ is an integral domain.*

2. *$U(R[[x]]) = \{u + xf(x) | u \in U(R), f(x) \in R[[x]]\}$.*

3. *If $I \subset R$ is an ideal then $I[[x]] = \{\sum_{k=0}^{\infty} \alpha_k x^k | \alpha_k \in I\}$ is an ideal of $R[[x]]$.*

4. *$I \subset R$ be an ideal, then $R[[x]]/I[[x]] \cong (R/I)[[x]]$ and $R[[x]]/(I,x) \cong R/I$.*

5. *$I \subset R$ is prime if and only if $I[[x]]$ is prime if and only if (I,x) is prime.*

6. *$\mathfrak{M} \subseteq R[[x]]$ is a maximal ideal if and only $\mathfrak{M} = (M,x)$ for some maximal ideal $M \subset R$ of R.*

Polynomials in multiple variable can be defined inductively. This can be extended to infinitely many variables for polynomials (but this is not so easy for power series).

With these in hand we move on to factorization.

Chapter 11

Factorization

11.1 Basic Definitions and Properties

In this section, R will be an integral domain unless specifically noted otherwise.

Definition 11.1.1. *Let R be an integral domain.*

1. *A nonzero nounit $\pi \in R$ is irreducible if $\pi = ab$ implies that a or b is a unit.*

2. *A nonunit $p \in R$ is said to be prime if $p|ab$ implies that $p|a$ or $p|b$.*

Example 11.1.2. *In $\mathbb{Z}[x]$ the elements $2, x, 1+x$ is prime. In $\mathbb{Z}[[x]]$ the elements $2, x$ are prime, but $1+x$ is a unit. In $\mathbb{Z}[\sqrt{-5}]$ the elements $2, 3, 1 \pm \sqrt{-5}$ are all irreducible but not prime (but in this ring 0 and $6+\sqrt{-5}$ are prime).*

Example 11.1.3. *In the ring $\mathbb{R}[x^2, x^3] = \{a_0 + a_2x^2 + a_3x^3 + a_4x^4 + \cdots + a_nx^n | a_i \in \mathbb{R}\}$, the elements x^2, x^3 are irreducible and we have the nonunique factorizations of differing lengths:*

$$x^6 = (x^2)(x^2)(x^2) = (x^3)(x^3).$$

The following results give a better characterization of the notion of prime and give a relationship between the notions of "irreducible" and "prime".

Lemma 11.1.4. *Let R be an integral domain and $x \in R$ a nonunit. Then x is prime if and only if (x) is a prime ideal.*

Proof. Suppose first tha (x) is a prime ideal and x divides ab. Since $rx = ab \in (x)$, then either a or b is in (x) since (x) is prime. This is equivalent to the statement that x divides a or x divides b.

On the other hand, suppose that x is a prime element and suppose that $ab \in (x)$. This is equivalent to the existence of $r \in R$ such that $rx = ab$. Since $x|ab$, it is the case that $x|a$ or $x|b$ and so $a \in (x)$ or $b \in (x)$. □

Theorem 11.1.5. *Let R be an integral domain and suppose that $x \in R$ is a nonzero nonunit. Then if x is prime, then x is irreducible.*

Proof. we have seen this before in a more specific situation. The proof here is essentially identical. □

It is an important situation when you can actually factor elements into irreducibles. The following definition highlights this situation.

Definition 11.1.6. *We say that the integral domain R is atomic if every nonzero nonunit in R can be decomposed into a product of atoms (irreducibles).*

Example 11.1.7. *Any field has this property (in a very silly way). So does $\mathbb{Z}, \mathbb{Z}[x], \mathbb{Z}[x,y], \mathbb{R}[x^2, x^3], \mathbb{Z}[\sqrt{-5}]$. It is more difficult at this point to think of examples which do not have this property. For this kind of non-example, consider $\mathbb{Z}$ or $\mathbb{Z} + x\mathbb{R}[x] = \{n + xf(x) | n \in \mathbb{Z}, f(x) \in \mathbb{R}[x]\}$.*

11.2 Unique Factorization, PIDs, and Euclidean Domains

Definition 11.2.1. *We say that R is a Euclidean domain if there is a function $\phi : R \setminus \{0\} \longrightarrow \mathbb{N}_0$ that satisfies the following properties:*

1. *$\phi(xy) \geq \phi(x)$ for all $x, y \in R \setminus \{0\}$.*
2. *For all $x, y \in R \setminus \{0\}$, there exists $q, r \in R$ such that $y = qx + r$ with $r = 0$ or $\phi(r) < \phi(x)$.*

Example 11.2.2. *Examples are $\mathbb{Z}$ with standard absolute value and $F[x], F[[x]]$ with F a field and ϕ the degree function for $F[x]$ and the order (or "least degree") function for $F[[x]]$.*

The next definition is a bit of a tandem. The concept of Noetherianess is central in commutative algebra. It is a natural finiteness condition to impose on commutative rings with identity that makes fancier theorems possible and computations more accessible.

Definition 11.2.3. *We say that R is Noetherian if every ideal is finitely generated. We say that R is a principal ideal domain (PID) if every ideal is principal.*

Finally we introduce the notion that is the weakest that guarantees the fundamental theorem of arithmetic.

Definition 11.2.4. *We say that R is a unique factorization domain (UFD) if R is atomic and given the irreducible factorizations*

$$\pi_1 \pi_2 \cdots \pi_n = \xi_1 \xi_2 \cdots \xi_m$$

then

1. $n = m$ *and*

2. *there is a* $\sigma \in S_n$ *such that* $\pi_i = u_i \xi_{\sigma(i)}$, *for* $u_i \in U(R)$.

We remark here that this first condition asserts that the length of the irreducible factorizations are the same and the second states that you can "pair off" the irreducibles up to units.

We now produce a couple of results that will allow us to compare these types of domains.

Proposition 11.2.5. *R is a PID (resp. Noetherian) if and only if every prime ideal of R is principal (resp. finitely generated).*

Proof. We only prove the result for PIDs and leave the Noetherian as a (very good) exercise.

It is clear that if R is a PID then every prime is finitely generated (as every ideal is finitely generated by definition). For the other direction, we will show that if there is an ideal $I \subset R$ that is not principal then there must also be a prime ideal that is not principal and this will establish the other direction. Suppose that I is R is an ideal that is not principal, we first claim that there is an ideal that is maximal with respect to being not principal. To this end, we consider the set $\Gamma = \{J \supseteq I | J \text{ is not principal}\}$ and partially order it by inclusion. Let $\{I_\alpha\}_{\alpha \in \Lambda}$ be a chain in Γ and let $A = \bigcup_{\alpha \in \Lambda} I_\alpha$. A is clearly an upper bound if it is the case that $A \in \Gamma$. Since the union is taken over a chain, then A is an ideal (the proof is almost the same as we have seen before) and clearly A contains I. Finally, note that if A is principal, then $A = (x)$ for some $x \in A = \bigcup_{\alpha \in \Lambda} I_\alpha$ and so $x \in I_\alpha$ for some α and hence $I_\alpha = (x)$ which is a contradiction. So by Zorn's Lemma there is an ideal P containing I that is maximal with respect to being nonprincipal.

To see that P must be prime, we suppose that we can find $a, b \in R \setminus P$ such that $ab \in P$. We now consider the ideal $A = (P, a)$. Since A strictly contains P, $A = (y)$ is principal. Now let $J = \{z \in R | zy \in P\}$. Since y must be of the form $y = p + ra$, $p \in P$ and $r \in R$, J must contain all of P and b as well so, again, by the maximality of P, $J = (x)$ must be principal. We now claim that $JA = P$. The containment $JA \subseteq P$ is by the definition of J and A. For the other containment, we let $p \in P \subseteq A$. We write $p = ry$ for some $r \in R$ and note that by the definition of J, $r \in J$. So $P = JA = (xy)$ is principal. This contradiction shows that P is prime.

We conclude by (re)stating that if R is not a PID, then there is a prime ideal that is not principal. This establishes the proposition. □

Here are some similar statements for the UFD situation.

Lemma 11.2.6. *R is a UFD if and only if every nonzero nonunit is a product of primes.*

Proof. This result shows essentially that factorization into primes is always unique. This is an easy exercise in inductively using the "prime" property that $p|ab$ implies that $p|a$ or $p|b$. □

Proposition 11.2.7. *Let R be an integral domain. The following conditions are equivalent.*

1. *R is a UFD.*
2. *Every nonzero prime ideal of R contains a nonzero prime element.*

Proof. Suppose that R is a UFD and $0 \neq P$ a prime ideal. Let $0 \neq x \in P$ and factor $x = p_1 p_2 \cdots p_n$ with each p_i a prime. Since this product is in P and P is prime, some $p_i \in P$ and this establishes the first direction.

Now suppose that 2. holds. Let S be the multiplicative set generated by the units and primes in R (so an element of S is either a unit or of the form $up_1p_2 \cdots p_m$ with u a unit and each p_i nonzero prime). Since R is a domain, S does not contain 0, and so we note that R is a UFD if and only if $S = R \setminus \{0\}$. If there is a nonzero (nonunit) element, x, of R that is not in S, we consider (x). Note that $(x) \bigcap S = \emptyset$. Indeed if rx is a product of primes then we can show by induction on the length of the factorization that x is a product of primes. If rx is prime then r must be a unit and x is prime. We will assume that if rx is a product of n primes then x is a product of primes. Now suppose that $rx = p_1 p_2 \cdots p_n p_{n+1}$. If none of these primes divide r then r must be a unit and we are done. So we assume without loss of generality that p_1 divides r and hence if $r = r'p_1$ then $r'x = p_2 p_3 \cdots p_{n+1}$ and we are done by induction. So we conclude that $(x) \bigcap S = \emptyset$ and so we expand (x) to a prime P_x such that $P_x \bigcap S = \emptyset$. But since S contains all nonzero primes, then P_x is a prime that contains no nonzero prime element. This contradiction shows that R is a UFD. □

Here is a big thereom that ties these concepts together.

Theorem 11.2.8. *Let R be an integral domain. For the following conditions, we have* 1. $\implies$ 2. $\implies$ 3. *and noe of the implications are reversible in general.*

1. *R is a Euclidean domain.*
2. *R is a PID.*
3. *R is a UFD.*

Proof. 1. $\implies$ 2.: Let $I \subseteq R$ be an ideal. Consider $\{\phi(z) | z \in I\}$. Let $t \in I$ be such that $\phi(t)$ is minimal. We claim that $I = (t)$. Certainly $(t) \subseteq I$, for the other containment, let $\alpha \in I$. Write $\alpha = qt + r$ with $q, r \in R$ and either $r = 0$ or $\phi(r) < \phi(t)$. But since $r = \alpha - qt \in I$, it cannot be the case that $\phi(r) < \phi(t)$ and hence $r = 0$ and $I = (t)$.

2. $\implies$ 3.: Let R be a PID. To show that R is a UFD, it suffices to show that every nonzero prime ideal contains a prime element. Let $P \subset R$ be a prime ideal. Since R is a PID, then $P = (p)$ and $p \in P$ is our requisite nonzero prime element. □

Example 11.2.9. *$\mathbb{Z}[x]$ is a UFD that is not a PID (look at the ideal $(2, x)$. A more general statement can be found below. The domain $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$.*

Now we look at a very famous result that shows that unique factorization is preserved in polynomial extensions. But first a lemma

Lemma 11.2.10. *Let $p \in R$ be a prime element, then p is also prime in $R[x]$.*

Proof. $R[x]/(p) \cong R/(p)[x]$ is an integral domain. So p is prime in $R[x]$. □

Theorem 11.2.11. *If R is a UFD then so is $R[x]$.*

Proof. It suffices to show that any prime $\mathfrak{P}$ in $R[x]$ has a prime element. Consider $\mathfrak{P} \bigcap R = P$. This is a prime of R and if P is not zero, it must contain a nonzero prime element p which is also prime in $R[x]$ and we are done.

So suppose that $P = 0$. In this case, if S is the set of nonzero elements of R, then $\mathfrak{P}_S$ is a prime ideal of $R[x]_S = K[x]$ where K is the quotient field of R. Since $K[x]$ is Euclidean, it is a PID and so $\mathfrak{P}_S = (f(x))$ where we can assume that $f(x)$ is a polynomial in $R[x]$ where the greatest common divisor of the coefficients of f is 1. It will suffice to show that $f(x)$ is prime in $R[x]$. To this end, suppose that $a(x)b(x) = f(x)r(x)$ where $a(x), b(x), r(x) \in R[x]$. Without loss of generality, $a(x) = f(x)g(x)$ with $g(x) \in K[x]$. We wish to show that $g(x) \in R[x]$. We write $g(x) = \frac{h(x)}{r}$ with $r \in R$. This gives the equation $ra(x) = f(x)h(x)$. If p is a prime dividing r in R then note that p is prime in $R[x]$ and must divide $h(x)$. Continuing inductively gives that $g(x) \in R[x]$ and we are done. □

So it follows by induction that $R[x_1, x_2, \cdots, x_n]$ is a UFD for all n. This is also true for *any* collection of indeterminates (even infinite sets of any size). The same is not true in general for power series (not even for one variable), but the example is beyond the scope of what we are doing here.

Theorem 11.2.12 (Eisenstein's Irreducibility Criterion)**.** *Let R be an integral domain and $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. If $0 \neq p \in R$ is a prime such that p does not divide a_n, p does divide a_k for all $0 \leq k \leq n-1$ and p^2 does not divide a_0 then the only possible proper factors of $f(x)$ have degree 0. Additionally if R is a UFD with quotient field K, then $f(x)$ is irreducible in $K[x]$*

Example 11.2.13. *Consider the polynomial $x^5 - 4x^3 + 6x^2 + 18$. This is irreducible in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$. Consider the polynomial $x^4 + x^3 + x^2 + x + 1$. This is irreducible over $\mathbb{Q}[x]$ (do the change of variables $x \mapsto x + 1$).*

Theorem 11.2.14. *If R is Noetherian, then so are $R[x]$ and $R[[x]]$.*