Rice University
Department of Mathematics

Introduction to Groups, Rings, and Fields

A first exposure to core concepts in abstract algebra

Author
Gabriel Gress

December 2, 2021

Contents

Chapter 1

Divisibility, Congruences, Euler's Function

All numbers are assumed to be $\mathbb{Z}$

$$a \mid b := \quad \exists c \text{ s.t. } ac = b$$

Definition 1.0.1

We say that $a \equiv b \pmod{m}$ (a is equivalent to b) if $m|a-b$

Definition 1.0.2: Euler's Function

$\varphi(n)$ is defined as the number of integers coprime to n in $\{1, 2, \ldots, n\}$. In other words, it is the magnitude of $\{c \mid 1 \leq c \leq n, (c, n) = 1\}$

Note that if p is prime, then $\varphi(p) = p - 1$.

Theorem 1.0.1

$n = p_1^{k_1} \cdot \ldots \cdot_r^{k_r}$, $p_i \neq p_j$, p prime, $k_i > 0 \implies \varphi(n) = (p_1^{k_1-1} - p_1^{k_1-1}) \cdot \ldots \cdot (p_r^{k_r} - p_r^{k_r-1})$

Theorem 1.0.2: Euler-Fermat Theorem

If c, m are coprime, then $c^{\varphi(m)} \equiv 1 \pmod{m}$.

Theorem 1.0.3: Linear Congruence

A linear congruence $ax \equiv b \pmod{m}$ is solvable if and only if $(a, m) \mid b$. Furthermore, the number of pairwise incongruent solutions is (a, m).

Definition 1.0.3: Linear Diophantine equation

A linear Diophantine equation in two variables is $Ax + By = C$ where A, B, C are given integers, A, B not both zero, with integer solutions for x, y.

A linear Diophantine equation is solvable if and only if $(A, B) \mid C$, in which case there are infinite solutions.
Note that a linear Diophantine equation can be transformed into a linear congruence $Ax \equiv C \pmod{|B|}$ or $By \equiv C \pmod{|A|}$

Definition 1.0.4: Binary Operation

A binary operation assigns every ordered pair of a set $(a, b) \in S \times S$ a unique element $c \in S$, which can have the following properties:

- For every $a, b, c \in S$, $a(bc) = (ab)c$ (associative)
- For every $a, b \in S$, we have $ab = ba$ (commutative)
- There is an element $e \in S$ satisfying $ea = ae = a$ for every $a \in S$
- If S has an identity e, then there is an inverse of $a \in S$, or a^{-1} satisfying $aa^{-1} = a^{-1}a = e$ (left and right inverses, in particular)

Chapter 2

Groups

2.1 Fundamentals of Groups

Definition 2.1.1: Group

A **group** is a set G that has an associative operation with an identity e and inverses for all elements. If the operation is commutative, then we say G is **abelian**.

Definition 2.1.2: Order

Let $g \in G$. The **order of g**, denoted by $o(g)$, is the smallest positive integer k satisfying $g^k = e$. If there is no such k, then we say that $o(g) = \infty$.

In the finite case, the powers of g are periodic, and so the order is the smallest period.

Definition 2.1.3: Subgroup

A set $H \subset G$ is a **subgroup** of G if it is a group under the operation of G. We denote this by $H \leq G$.

$H \leq G$ if and only if it contains the identity of G and is closed under the operation in G, and for inverses. We can reduce these conditions to requiring that H satisfies the criterion

$$xy^{-1} \in H \quad \forall x, y \in H$$

Proposition 2.1.1

Let $\mathcal{A}$ be a nonempty collection of subgroups of G. Then their intersection is a subgroup:

$$K = \bigcap_{H \in \mathcal{A}} H \leq G.$$

This leads us to the following definition.

Definition 2.1.4: Generated Subgroup

Let $A \subset G$ be a subset of the group G. We define

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

to be the **subgroup of G generated by A**.

Alternatively, we define $\overline{A}$ to be the (finite product) closure of A under the group operation of G. One should check that $\langle A \rangle = \overline{A}$.

In short, we can generate a subgroup on a set by looking for the smallest subgroup that contains the set. This is a unique minimal element. This will also be the exact same subgroup formed by taking the closure of A under the group operations of G.

Definition 2.1.5: Coset

Let $H \leq G$ and $g \in G$. Then $gH = \{gh \mid h \in H\}$ is a **left coset**, and $Hg = \{hg \mid h \in H\}$ is a **right coset**.

Two left cosets are either disjoint or equal, and every coset is of the same size.

Proposition 2.1.2

Let $H \leq G$ be a subgroup of G. Then the set of left cosets of H form a partition of G. That is,

$$G = \bigcup_{g \in G} gH.$$

Furthermore, for all $g, g' \in G$, $gH = g'H$ if and only if $g'^{-1}g \in H$. In other words, g and g' are representatives of the same coset.

The set of left cosets form a group by the operation

$$gH \cdot g'H = (gg')H$$

provided that $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$. We will soon give this property a name. But first, we will state and prove a fundamental theorem for groups.

Theorem 2.1.1: Lagrange's Theorem

Let H be a subgroup of a finite group G. Then $|H| \mid |G|$, and te number of left cosets of H in G is $\dfrac{|G|}{|H|}$.

This gives a new perspective on subgroups– we can view subgroups as a means of partitioning a group.

Definition 2.1.6: Index

If G is a group and $H \leq G$, the number of left cosets of H in G is called the **index** of H in G. We denote this by $|G : H|$.

Lagrange's Theorem gives us a lot of really nice results. For example, we can immediately see that $|g| \mid |G|$ for $g \in G$ in a finite group, and moreover $g^{|G|} = 1$ for all $g \in G$.

We will define a way to compose two subgroups of a group that can sometimes be convenient.

Definition 2.1.7

Let $H, K \leq G$ be subgroups of G. We define

$$HK := \{hk \mid h \in H, k \in K\}.$$

Proposition 2.1.3

If $H, K \leq G$ are finite subgroups of G, then

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

This equation becomes nicer when H, K are disjoint (with the exception of identity of course), as it implies that $|HK| = |H|\,|K|$. However, one needs to be careful– this product isn't necessarily a subgroup, as it may not contain inverses.

Proposition 2.1.4

Let $H, K \leq G$ be subgroups of G. HK is a subgroup if and only if

$$HK = KH.$$

If this holds, then inverses will be contained within HK, and hence it will be closed under group operations.

2.1.1 Normal Subgroups

Cosets are such a vital construction to visualize subgroups, as they will become key to understanding quotient groups. However, we notice one flaw that makes this characterization difficult– left and right cosets of a subgroup are not necessarily equivalent. This property is important enough to earn itself a name.

Definition 2.1.8: Normal Subgroup

A subgroup N of G is **normal** if the left and right cosets are the same; i.e.

$$N \leq G \text{ and } gN = Ng$$

for every $g \in G$. We denote this by $N \triangleleft G$.

We can also think of this as $Ng \subset gN$ and $gN \subset Ng$, or in other words, $g^{-1}ng \in N$ and $gng^{-1} \in N$.

$$N \triangleleft G \iff N \leq G \text{ and } g^{-1}ng \in N \text{for every } g \in G, n \in N$$

We call $g^{-1}ng$ a **conjugate** of n.

Observe that, because the trivial subgroups are trivially normal, then all subgroups H of index 2 are normal.

Theorem 2.1.2

Let $N \leq G$ be a subgroup of a group G. The following are equivalent:

- $N \triangleleft G$
- $gN = Ng$ for all $g \in G$
- The left cosets of N in G form a group by the natural group operation

$$gN \cdot g'N = (gg')N$$

- $gNg^{-1} \subset N$ for all $g \in G$

Every group also has a special normal subgroup called the **center**.

Definition 2.1.9: Center

The **center** of a group is the normal subgroup given by

$$Z(G) = \{g \in G \mid xg = gx \text{ for every } x \in G\}.$$

Every subgroup of the center is normal.

2.1.2 Quotient Groups

Definition 2.1.10: Group Homomorphism

We call a map $\varphi : G_1 \to G_2$ a **group homomorphism** if it preserves the operation; $\varphi(gh) = \varphi(g)\varphi(h)$ for every $g, h \in G_1$.

If the homomorphism is bijective, then it is an **isomorphism**. A homomorphism φ is an isomorphism if and only if $\mathrm{Ker}\varphi = e_1$ and $\mathrm{Im}\varphi = G_2$.

Proposition 2.1.5

Let G and H be groups and let $\varphi : G \to H$ be a homomorphism.

- $\varphi(1_G) = 1_H$
- $\varphi(g^{-1}) = \varphi(g)^{-1}$
- $\varphi(g^n) = \varphi(g)^n$
- $\mathrm{Ker}\varphi \triangleleft G$
- $\mathrm{Im}\varphi \leq H$

In fact, a subgroup $N \triangleleft G$ is normal if and only if it is the kernel of a group homomorphism.

Definition 2.1.11: Quotient Group

We denote by G/N the **quotient group**, whose elements are the cosets of the normal subgroup N, with operations defined by $(aN)(bN) = (abN)$

Theorem 2.1.3: First Isomorphism Theorem

If $\varphi : G_1 \to G_2$ is a homomorphism, then

$$\mathrm{Im}\varphi \cong G_1/\mathrm{Ker}\varphi.$$

This tells us that φ is injective if and only if the kernel is trivial, and we can also see that $|G : \mathrm{Ker}\varphi| = |\varphi(G)|$.

This key theorem allows us to fully connect the notion of normal subgroups partitioning a group.

Definition 2.1.12: Natural Homomorphism

If $N \triangleleft G$, then $\psi : G \to G/N$ defined by $\psi(g) = gN$ is the natural homomorphism with $\mathrm{Ker}\psi = N$ and $\mathrm{Im}\psi = G/N$.

Theorem 2.1.4: Third Isomorphism Theorem

Let G be a group, and let $H, K \triangleleft G$ with $H \leq K$. Then $K/H \triangleleft G/H$ and

$$(G/H)/(K/H) \cong G/K$$

The point of this theorem is that quotients of quotient groups provide little additional information.

Theorem 2.1.5: Fourth Isomorphism Theorem

Let $N \triangleleft G$ be a normal subgroup of G. There is a bijection from the set of subgroups A satisfying $N \leq A \leq G$ onto the set of subgroups $A/N \leq G/N$.

That is, every subgroup of G/N can be viewed as some A/N for some subgroup A containing N. Furthermore, for all $A, B \leq G$ with $N \leq A, B$,

(i). $A \leq B \iff A/N \leq B/N$

(i). $A \leq B \implies |B : A| = |B/N : A/N|$

(i). $\langle A, B\rangle/N = \langle A/N, B/N\rangle$

(i). $A \triangleleft G \iff A/N \triangleleft G/N$

This theorem really just tells us that we can get isomorphisms beween structures via lattices– if two group structures have a certain lattice structure, there is a natural isomorphism between each other.

2.1.3 Direct Product of Groups

Definition 2.1.13: Direct Product

The **direct product** $G_1 \times G_2$ of groups G_1, G_2 is the group of all ordered pairs (g_1, g_2) where $g_i \in G_i$, with the usual definition of multiplication:

$$(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2).$$

It is clearly a group, and the projection subsets $G_1^* = \{(g_1, e_2) \mid g_1 \in G_1\}$ and $G_2^* = \{(e_1, g_2) \mid g_2 \in G_2\}$ are isomorphic to their respective groups. This in turn tells us that $|G_1 \times G_2| = |G_1|\,|G_2|$.

Proposition 2.1.6

$G_1^*, G_2^* \triangleleft G_1 \times G_2$ are normal subgroups, and every $u \in G_1 \times G_2$ can be decomposed as $u = u_1u_2$, $u_i \in G_i^*$.

The converse holds as well; if N, M are normal subgroups of a group G, and every $g \in G$ can be written as $g = nm$, $n \in N, m \in M$, then $G \cong N \times M$.

Of course, $(G_1 \times G_2)/G_1^* \cong G_2$ and vice versa.

We can even take the direct product of more than two groups:

$$g = (g_1, g_2, \ldots, g_n) \in G_1 \times G_2 \times \ldots \times G_n$$
$$(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n) = (g_1h_1, g_2h_2, \ldots, g_nh_n).$$

We will later see that direct products provide us a means of characterizing all finitely generated abelian groups.

2.2 Cyclic Groups

One particular important class of groups are cyclic groups.

Definition 2.2.1: Cyclic Group

A group G is **cyclic** if G can be generated by a single element. That is, there is some element $g \in G$ such that

$$G = \{g^n \mid n \in \mathbb{Z}\}.$$

We write a cyclic group by $G = \langle g \rangle$.

It is not necessarily true that all powers of g are distinct (to see this, observe that in a finite group, if $g^n = 1$, then $g^{n+k} = g^k$). However, it is true that all cyclic groups are abelian (due to the law of exponents).

Proposition 2.2.1

Let $G = \langle g \rangle$. Then $|G| = |g|$. That is, the order of the group is the order of the generator– if the order is infinite, then the group must also be infinite.

Ideas from cyclic groups are useful in the general case for groups as well. For example, if G is any group, and $g^n = g^m = 1$ for some $m, n \in \mathbb{Z}$, then $g^{(m,n)} = 1$. This actually gives us the following theorem:

Theorem 2.2.1

Any two cyclic groups of the same order are isomorphic. In particular, if $\langle g \rangle$ and $\langle h \rangle$ are finite cyclic groups of order n, we have an isomorphism

$$\begin{aligned} \varphi : \langle g \rangle &\to \langle h \rangle \\ x^k &\mapsto h^k \end{aligned}$$

and if $\langle g \rangle$ has infinite order, then

$$\begin{aligned} \varphi : \mathbb{Z} &\to \langle g \rangle \\ k &\mapsto g^k \end{aligned}$$

is an isomorphism.

A finite group G is cyclic if and only if $|G| = o(g)$ for some $g \in G$. Lagrange's theorem implies that $o(g) \mid |G|$ for $|G| < \infty$.

Of course, a generator for a cyclic group is not necessarily unique. For example, if g generates a group with order n, then g^a will also generate the group provided that $(n, a) = 1$. Combining this with previous results allow us to completely classify cyclic groups.

Theorem 2.2.2: Classification of cyclic groups

Let $G = \langle g \rangle$ be a cyclic group.

(i). Every subgroup $H \leq G$ is cyclic. In particular, $H = \{1\}$ or $H = \langle g^d \rangle$, where d is the smallest positive integer such that $g^d \in K$.

(ii). If $|G| = \infty$, then $\langle g^a \rangle \neq \langle g^b \rangle$ for distinct nonnegative integers a, b. Equality only holds if $|a| = |b|$. This implies that subgroups of infinite cyclic groups are in bijection with $\mathbb{Z}_+$.

(iii). If $|G| = n < \infty$, then for each $a \mid n$ with $a > 0$, there is a unique subgroup $H \leq G$ with $|H| = a$. This subgroups is exactly the cyclic group

$$H = \langle x^{n/a} \rangle.$$

In general, for every integer m,

$$\langle x^m \rangle = \langle x^{(n,m)} \rangle.$$

2.3 Groups of Symmetries

While the abstract definition of groups seems very natural, the construction of groups actually originated as a way to capture certain notions of physical systems. One important natural group arises from symmetries of geometric objects.

Let $n \in \mathbb{Z}_+$ be a positive integer with $n \geq 3$, and denote by D_{2n} the set of symmetries of a regular n-gon (the **dihedral group**). We consider a symmetry to be any rigid motion that maintains the same locations of nodes of the n-gon (but the ordering of the nodes might differ).

We can uniquely describe a symmetry s by defining the permutation σ on $\{1, 2, \ldots, n\}$ that permutes the nodes. Notice, however, that not every permutation is allowed– rotations do not change the relative ordering of the nodes, and reflections merely reverse the ordering of the nodes. In short, instead of the $n!$ possible permutations, we are actually restricting ourselves to $2n$ permutations– the n permutations obtained by cycling the list, and the n permutations obtained by reversing each of those permutations.

We can make D_{2n} into a group by defining the oberation st for $s, t \in D_{2n}$, which is the symmetry obtained by first applying the transformations of t, and then the transformations of s. This is associative because it is the composition of functions; the identity is given by the identity permutation (fixing all vertices in place), and the inverse symmetry is the transformations that undoes the symmetries.

In fact, for any n-gon, all symmetries can be described as an element of D_{2n}, and hence we will show some properties of D_{2n} that will allow us to utilize it better as group. We denote by r the transformation given by the rotation clockwise about the origin by $2\pi/n$ radians, and s to be the reflection about the line of symmetry from the first index through the origin. Then D_{2n} has the following properties:

- $1, r, r^2, \ldots, r^{n-1}$ are all distinct, $r^n = 1$ and so $|r| = n$
- $|s| = 2$
- $s \neq r^i$ for any i
- $sr^i \neq sr^j$ for all $i \neq j$, $i, j < n$

These properties allow us to explicitly view the symmetry group by

$$D_{2n} = \left\{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\right\}$$

Furthermore, we have that $rs = sr^{-1}$, and $r^i s = sr^{-i}$. These properties allow us to combine elements and simplify quickly, and hence are good to be familiar with.

Example 2.3.1

Consider $n = 12$, and hence D_{24}. To compose the symmetries given by (sr^9) and (sr^6), we get

$$(sr^9)(sr^6) = s(r^9s)r^6 = s(sr^{-9})r^6 = s^2(r^{-3}) = r^{-3} = r^9$$

2.4 Groups of Permutations

When considering the construction of the dihedral group, one might be curious what occurs if one allows all permutations of nodes within the set. This in fact results in a group as well– the permutaton group.

Definition 2.4.1: Permutation Group

Let Ω be a nonempty set and let S_Ω denote the set of all bijections from Ω to itself. S_Ω is a group under the operation of composition, and is referred to as the **symmetric group on the set** Ω.

If $\Omega = \{1, 2, 3, \ldots, n\}$, the **symmetric group of degree *n*** is denoted S_n.

One learns in combinatorics that the number of permutations of a set of size n is $n!$, and so $|S_n| = n!$.

Now we will describe a clever notation that can be used to write elements σ of S_n referred to as cycle decomposition.

Definition 2.4.2: Cycle Decomposition

A **cycle** is a string of integers representing the elements of S_n which cyclically permutes these integers (and fixes all other integers). For example, the cycle $(a_1a_2 \ldots a_m)$ sends a_1 to a_2, a_2 to a_3, and so on, finally sending a_m to a_1. Every element $\sigma \in S_n$ can be described by following the rearrangement of integers until a cycle forms– and then looking for the cycles in the remaining numbers. Thus, we can write a permutation in the form

$$(a_1a_2 \ldots a_{m_1})(a_{m_1+1}a_{m_1+2} \ldots a_{m_2}) \ldots (a_{m_{k-1}+1}a_{m_{k-1}+2} \ldots a_{m_k})$$

which represents k different cycles that σ partitions Ω into.

This allows us to quickly see how σ acts on elements in S_n. To calculate $\sigma(x)$, find x in the list, and if there is an integer to the right of it, then $\sigma(x)$ equals that integer. Otherwise, it is the end of the cycle and hence $\sigma(x)$ is the first element in the list.

The product of all the cycles is called the **cycle decomposition** of σ.

The **length** of a given cycle is the number of integers that appears in it. A cycle of length t is called a t-cycle. Finally, two cycles are called **disjoint** if they have no numbers in common (in a symmetric group, all cycles are disjoint).

This also makes it simple to find inverses, as the cycle decomposition of σ^{-1} is obtained by reversing the order of elements within each cycle. To compute compositions, first follow the cycle given in the first permutation, then the cycle in the second permutation.

As one works with more examples, they will quickly see that S_n is non-abelian for all $n \geq 3$. But of course, disjoint cycles commute, and so one can rearrange the cycles in any product of disjoint cycles without changing the permutation.

Exercise caution– one will see that a permutation can be written via many different decompositions of cycles. However, there is only one unique decomposition into *disjoint* cycles.

Corollary 2.4.1

With the combinatorial construction of a permutation, we say a permutation is even or odd based on the number of inversions. With this definition, we say that a permutation is even if and only if the permutation is the product of an even number of transpositions.

Thus we can check if a permutation is even or odd by counting the number of even cycles. An odd cycle does not change parity, but an even cycle will. Thus, if a permutation has an even number of even cycles, it is even (parity of one). If instead the number of even cycles is odd, then it is an odd permutation (parity of negative one).

Definition 2.4.3: Permutation Groups

Permutation groups are subgroups of S_n.

For example, the dihedral group is merely one of many permutation groups.

Let A_n denote the set of even permutations. This is clearly a subgroup of S_n.

Proposition 2.4.1

$$|S_n : A_n| = 2.$$

Proof 2.4.1

Observe that there is a bijection from the even permutations to the odd permutations by simply transposing the first two elements.

We will discuss the alternating group A_n momentarily.

Exercise 2.4.1

The order of an element $g \in S_n$ is the LCM of the lengths of disjoint cycles.

2.5 Group Actions

By this point, the reader should have a solid foundation in the basic ideas of group theory. There are richer details to follow, but some of them rely on more advanced ideas in algebra. In particular, group actions are fundamentally connected to permutation groups and group presentations. More details on these topics can be found elsewhere, but one can also get a basic understanding of group actions without this prerequisite knowledge.

Definition 2.5.1: (Left) Action

A (left) **action** of a group G on a set Ω is a function $\mu : G \times \Omega \to \Omega$ with the following two properties:

- $\mu(g_1, \mu(g_2, x)) = \mu(g_1 g_2, x)$ for all $x \in \Omega$, $g_1, g_2 \in G$.
- $\mu(e, x) = x$ for all $x \in \Omega$.

It immediately follows that $\mu(g^{-1}, \mu(g, x)) = \mu(g, \mu(g^{-1}, x)) = x$ for all $x \in \Omega, g \in G$.

While $\mu(e, x) = x$, it doesn't have to be the only element which does so. The **kernel** of the action is the set of elements of G that act trivially on Ω:

$$\mathrm{Ker}\mu = \{g \in G \mid g \cdot x = x \quad \forall x \in \Omega\}$$

If this set is trivial, then we say the action is **faithful**. Regardless, the kernel forms a normal subgroup, as we will see later.

Proposition 2.5.1

- For any $g \in G$, the map $\sigma_g : \Omega \to \Omega$ defined by $\sigma_g x = \mu(g, x)$ is a permutation.
- The map $\theta : G \to S_n$ defined by $\theta(g) = \sigma_g$ is a homomorphism (where S_n is the set of permutations of Ω, so $n = |\Omega|$)
- Conversely, given a homomorphism $\theta : G \to S_n$, there is an action μ of G on Ω given by $\mu(g, x) = \theta(g)x$.

Viewing group actions via permutations is a good way to get a grasp of group actions. One can view group actions of G on Ω as each element $g \in G$ permuting the set Ω. We call the homomorphism $G \to S_\Omega$ given by $\theta(g) = \sigma_g$ to be the **permutation representation** associated to the given action.

Example 2.5.1

- Let H be a subgroup of G. Let Ω be the set of all left cosets of H in G (written as gH for some $g \in G$). Define an action by $\mu(g, g'H) = (gg')H$. This is the action of **left multiplication**.
- Define an action of G on itself ($\Omega = G$) by the rule $\mu(g, x) = gxg^{-1}$. This is the action of **conjugation**.
- Let Ω be the set of all subgroups of G. Then G acts on Ω by **conjugation**: $\mu(g, H) = gHg^{-1}$.

An equivalence relation on Ω is formed by a group action via the rule that $x \sim y$ if there exists $g \in G$ with $\mu(g, x) = y$. The equivalence classes are called **orbits**. The set Ω decomposes into a disjoint union of orbits.

Definition 2.5.2: Transitivity

We say that an action is **transitive** if there is just one orbit, and **intransitive** otherwise.

Left multiplication is transitive, but conjugation is in general not. The orbits for conjugation of G onto itself are the **conjugacy classes** of G.

Definition 2.5.3: Stabilizer

The **stabilizer** of an element $x \in \Omega$ is the set

$$\{g \in G \mid \mu(g, x) = x\}$$

of elements of G for which the corresponding permutation fixes x. It is denoted G_x.

Notice that the union of all stabilizers on Ω is exactly the kernel of the action.

Example 2.5.2

Let A be a subset of G. Consider the action of G on A by conjugation, i.e. $\mu(g, a) = gag^{-1}$. Then the stabilizer of an element $a \in A$ is called the **centralizer of *a*** denoted by $C_G(a)$. Considering the entire subset A, we define

$$C_G(A) = \left\{g \in G \mid gag^{-1} = a \forall a\right\}$$

to be the **centralizer of *A***.

It turns out that $C_G(A) \leq G$ is a subgroup.

One will find that abelian groups prove not to be good examples for centralizers, as one will quickly see that in an abelian group G, $C_G(A) = G$ for all subsets A. However, one can check that

$$C_{Q_8}(i) = \{\pm 1, \pm i\}.$$

There are some similar subgroups that will be of interest soon.

Recall the center subgroup of G denoted by

$$Z(G) = \{g \in G \mid gx = xg \; x \in G\}.$$

The center plays an important role with these new ideas, as one can see that $Z(G) = C_G(G)$ (and hence we already know that $Z(G)$ is a subgroup).

One might recall that we also defined conjugation by subgroups earlier. This also corresponds to a variation of a centralizer.

Definition 2.5.4: Normalizer

Let A be a subset of G, and consider the action of G on A by coset conjugation, i.e. $\mu(g, A) = gAg^{-1} = \left\{gag^{-1} \mid a \in A\right\}$. Then the set of elements which fix A is called the **normalizer** of A in G, denoted by

$$N_G(A) = \left\{g \in G \mid gAg^{-1} = A\right\}.$$

This is actually a larger subgroup containing the centralizer– if $g \in C_G(A)$, then $gag^{-1} = a \in A$, and so $C_G(A) \leq N_G(A)$. One can show that $N_G(A)$ is a subgroup as well.

Proposition 2.5.2

Let $N \leq G$ be a subgroup of G. Then $N \triangleleft G$ is a normal subgroup of G if and only if $N_G(N) = G$.

There are some other nice properties of subgroups that come about from the normalizer.

Proposition 2.5.3

If $H, K \leq G$ are subgroups of G, and $H \leq N_G(K)$, then $HK \leq G$.

Thus, if $K \triangleleft G$ then $HK \leq G$ for any $H \leq G$.

Definition 2.5.5

If A is any subset of $N_G(K)$, we say A **normalizes** K.

Example 2.5.3

Consider $G = S_4$ and $H = D_8$. Let $K = \langle(123)\rangle$. We can view D_8 as a subgroup of S_4 by identifying each symmetry by its permutation on the four vertices. Lagrange's Theorem tells us that $H \cap K = 1$ (as their orders are relatively prime), and hence $|HK| = 24$ and hence $HK = S_4$.

Furthermore, H nor K normalizes the other.

It is worthwhile to notice that if we take $S = \mathcal{P}(G)$, then the action of G on S by coset conjugation admits a stabilizer on its elements A by $N_G(A)$.

Finally, we can also let $N_G(A)$ act on A by conjugation $a \mapsto gag^{-1}$. Then the centralizer $C_G(A)$ is precisely the kernel of this action, and so we have now conceptualized these main definitions via group actions.

Now we will state some theorems that formalize these ideas.

Theorem 2.5.1: Second Isomorphism Theorem

Let G be a group with $A, B \leq G$. Assume $A \leq N_G(B)$. Then

- $AB \leq G$
- $B \triangleleft AB$
- $A \cap B \triangleleft A$
- $AB/B \cong A/(A \cap B)$

Note that AB/A is not necessarily a group, i.e. A is not necessarily normal in AB.

Theorem 2.5.2: Orbit-Stabilizer Theorem

Given an action of G onto Ω, and $x \in \Omega$, the stabilizers G_x form a subgroup of G. Furthermore, there is a bijection between the orbit of x and the set of left cosets of G_x in G given by

$$\mu^i x \mapsto \mu^i G_x.$$

If G is finite, the size of the orbit of x is equal to $|G : G_x| = |G| / |G_x|$.

Corollary 2.5.1

Every transitive action is isomorphic to an action by left multiplication on the left cosets of a subgroup. Furthermore, the actions on the left cosets of two subgroups H, K are isomorphic if and only if H, K are conjugate.

Note: Let $\mathrm{fix}(g)$ denote the number of elements in Ω that are mapped to themselves when g is applied to them as an action.

Theorem 2.5.3: Orbit-Counting Lemma

The number of orbits of G on Ω is given by

$$\frac{1}{|G|} \sum_{g \in G} \mathrm{fix}(g).$$

Lemma 2.5.1: Burnside's Lemma

The number of orbits is equal to the average number of fixed points. We can write this by

$$|G| \cdot (\text{number of orbits}) = \sum_{g \in G} |S^g|$$

We can get some interesting results by considering the action of G on itself, or subsets of itself. This corresponds to the notion of permutations of a group.

Theorem 2.5.4

Let $H \leq G$ be a subgroup and let G act by left multiplication on the set A of left cosets of H in G. We denote this action by σ_H, the associated permutation representation. Then

- G acts transitively on A
- The stabilizer in G of $eH \in A$ is the subgroup H
- The kernel of σ_H is $\bigcap_{x \in G} xHx^{-1}$, and $\mathrm{Ker}\sigma_H$ is the largest normal subgroup of G contained in H

Corollary 2.5.2: Jordan's Theorem

- Let G act transitively on the finite set Ω, where $|\Omega| > 1$. Then there is an element of G which fixes no point of Ω.
- Let H be a proper subgroup of a finite group G. Then

$$\bigcup_{g \in G} g^{-1} H g \neq G.$$

Theorem 2.5.5: Cayley's Theorem

Every group of size n is isomorphic to a subgroup of S_n.

Proof 2.5.1

Let S_n be all permutations of the group $G = \{e, g_2, \ldots, g_n\}$ and define $\varphi : G \to S_n$ by $\binom{g \mapsto g_i}{g g_i}$. In other words, we assign to $g \in G$ the permutation of G onto itself; we multiply every g_i by the given g from the left. One can check that φ is an injective homomorphism, and so $G \cong \text{Image}(\varphi) \leq S_n$.

Cayley's theorem can also be seen as a consequence of the above theorem, as one can simply take H to be trivial to get the result.

Proposition 2.5.4

If G is a finite group with $|G| = n$, and p is the smallest prime that satisfies $p \mid n$, then any subgroup of index p is normal.

This can be proven via Cayley's Theorem.

2.5.1 Conjugacy Classes

Earlier, we obtained interesting results such as Cayley's theorem by having G act on itself via left multiplication. We can also get some interesting results by letting G act on itself by conjugation:

$$g \cdot a = gag^{-1} \quad \forall g, a \in G.$$

Definition 2.5.6: Conjugates

Two elements $a, b \in G$ are said to be **conjugate in G** if there is some $g \in G$ such that $b = gag^{-1}$. The orbits of G acting on itself by conjugation are called the **conjugacy classes of G**.

One can clearly see that a, b are conjugate in G if they are contained in the same orbit.

Example 2.5.4

Observe that if G is abelian, then the action of G on itself by conjugation is trivial, and hence not interesting.

If G is non-trivial, then G will never act transitively on itself by conjugation. This is because the identity will always have its own orbit.

As an example, the conjugacy classes of S_3 are

$$\{1\}, \{(12), (13), (23)\}, \{(123), (132)\}$$

G can act on subsets of itself by conjugation, as well. We define this for $S \subset G$ by:

$$gSg^{-1} = \left\{ gsg^{-1} \mid s \in S \right\}.$$

We can even use this to define a group action on a higher level– that is, we can define an action of G on $\mathcal{P}(G)$ by $g \cdot S$.

Definition 2.5.7: Set Conjugates

Two subsets $S, T \subset G$ are said to be **conjugate in G** if there is some $g \in G$ such that $T = gSg^{-1}$, i.e. they are in the same orbit of G acting on its subsets by conjugation.

Our previous propositions give us the index of these conjugates within the group:

Proposition 2.5.5

The number of conjugates of $S \subset G$ is the index of the normalizer of S

$$|G : N_G(S)|.$$

The number of conjugates of an element s of G is hence

$$|G : C_G(s)|.$$

Theorem 2.5.6

Let G be a finite group and let $g_1, \ldots, g_n$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G) \leq G$. Then

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

This essentially partitions the order of G into its abelian and non-abelian parts.

This has a lot of useful consequences naturally. For example, we can use this to help classify groups of prime power order.

Corollary 2.5.3

Let G be a group with $|G| = p^\alpha$ for some p prime, $\alpha \geq 1$. Then G has a nontrivial center.

Proof 2.5.2

The class equation tells us that

$$|G| = |Z(G)| + \sum_{i=1}^{n} |G : C_G(g_i)|$$

Because $C_G(g_i)$ are non-central conjugacy classes they cannot be the full group G. Thus, $p \mid |G : C_G(g_i)|$, and hence divides the sum. Thus $p \mid |Z(G)|$, proving the result desired.

Corollary 2.5.4

If $|G| = p^2$ for some prime p, then G is abelian and isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Now we will look at the specific case of S_n.

Proposition 2.5.6

Let σ, τ be elements of the symmetric group S_n and suppose σ has cycle decomposition

$$(a_1 a_2 \dots a_{k_1})(b_1 b_2 \dots b_{k_2}) \dots$$

Then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$(\tau(a_1)\tau(a_2)\dots\tau(a_{k_1}))\dots(\tau(b_1)\tau(b_2)\dots\tau(b_{k_2})).$$

This provides an easy means of computing conjugation in S_n of course, but moreover it tells us that conjugation doesn't change the general structure of cycles.

Definition 2.5.8: Cycle lengths and partitions

If $\sigma \in S_n$ is the product of disjoint cycles of length $n_1, n_2, \dots, n_r$ with

$$n_1 \leq n_2 \leq \dots \leq n_r,$$

then the integers $\{n_i\}_{i=1}^r$ are called the **cycle type of σ**.

If $n \in \mathbb{Z}_+$, a **partition of n** is any nondecreasing sequence of positive integers whose sum is n.

The previous proposition tells us that the cycle type of a permutation is unique.

Proposition 2.5.7

Two elements of S_n are conjugate in S_n if and only if they have the same cycle type.

The number of conjugacy classes of S_n is the number of partitions of n.

We can use these results to prove important ideas– for example, one can give a combinatorial proof that A_5 is a simple group.

2.6 Characterization of Finitely Generated Groups

(Note: One can read this section without having seen Sylow's theorem and simply ignore any statement about Sylow p-groups. However, the content here should be revisited once the reader encounters Sylow's theorem elsewhere)

We have already begun classifying groups via Sylow's theorem, but once we utilize the tools of direct products, we can more generally classify groups. Hence the theorems in this section are an extension of the tools given via Sylow's theorem.

A group G is **finitely generated** if there is a finite subset $A \subset G$ such that $G = \langle A \rangle$.

Definition 2.6.1: Free Abelian Group

Let $r \in \mathbb{N}$ be given. We define the **free abelian group of rank r** to be the group

$$\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \dots^r \times \mathbb{Z}.$$

If $r = 0$, then $\mathbb{Z}^0 = 1$.

Theorem 2.6.1: Fundamental Theorem of Finitely Generated Abelian Groups

Let G be a finitely generated abelian group. Then

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_s}$$

for some integers $r, n_1, n_2, \ldots, n_s$ such that $r \geq 0$, $n_i \geq 2$, and $n_{i+1} \mid n_i$. Furthermore, this factorization of G is unique.

We call r the **free rank** or **Betti number** of G, and the integers $n_1, n_2, \ldots, n_s$ the **invariant factors of G**. The factorization above is hence referred to as the **invariant factor decomposition of G.**

A finitely generated abelian group is a finite group if and only if its free rank is zero. Furthermore, if G is a finite abelian group, then its order is the product of its invariant factors, and we say that G is of **type** $(n_1, \ldots, n_s)$.

Observe that because n_1 is the largest invariant factor, and each $n_i \mid n$, if p is a prime divisor of $|G| = n$, then $p \mid n_1$.

Corollary 2.6.1

If n is the product of distinct primes, then up to isomorphism the only abelian group of order n is $\mathbb{Z}_n$.

The fact that $n_{i+1} \mid n_i$ really puts a strong restriction on the structure of finite abelian groups. When n is finite, we will see that the types of abelian groups of order n correspond to the factorization of n.

Theorem 2.6.2: Primary Decomposition Theorem for Finite Abelian Groups

Let G be an abelian group with $|G| = n > 1$, and let the unique factorization of n into distinct prime powers be given by

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}.$$

Then

$$G \cong A_1 \times A_2 \times \ldots \times A_k$$

where $|A_i| = p_i^{\alpha_i}$, and

$$A_i \cong \mathbb{Z}_{p_i^{\beta_1}} \times \mathbb{Z}_{p_i^{\beta_2}} \times \ldots \times \mathbb{Z}_{p_i^{\beta_t}}$$

where

$$\beta_1 + \beta_2 + \ldots + \beta_t = \alpha_i$$
$$\beta_1 \geq \beta_2 \geq \ldots \geq \beta_t \geq 1.$$

Furthermore, this decomposition is unique.

We call the integers $p_i^{\beta_j}$ the **elementary divisors of G**. Thhis decomposition is called the **elementary divisor decomposition of G**.

The subgroups A_i are the Sylow p_i-subgroups of G, and hence the theorem essentially states that G is isomorphic to the direct product of its Sylow subgroups (which are normal and hence unique, because G is abelian).

Notice that the decomposition in A is the invariant factor decomposition of A with the divisibility condition in the fundamental theorem of finitely generated abelian groups, and hence the elementary divisors of G are the invariant factors of the Sylow p_i-subgroups.

The advantage of this representation is that it lets us easier determine all possible abelian groups of a certain order. Because the β_i are all uniquely determined and satisfy the above properties, it forms a partition of α, and hence we simply look at all combinations of partitions of α_i.

Example 2.6.1: Abelian groups of order p^5

Consider an abelian group G with $|G| = p^5$ for some p prime. Then this technique allows us to distinguish all unique groups like so:

Invariant Factors	Abelian Groups
5	$\mathbb{Z}_{p^5}$
4, 1	$\mathbb{Z}_{p^4} \times \mathbb{Z}_p$
3, 2	$\mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2}$
3, 1, 1	$\mathbb{Z}_{p^3} \times \mathbb{Z}_p \times \mathbb{Z}_p$
2, 2, 1	$\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_p$
2, 1, 1, 1	$\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$
1, 1, 1, 1, 1	$\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$

Hence, there are exactly 7 distinct (up to isomorphism) groups of order p^5.

Of course, it would be more helpful if we had a nice way to pass between the two representations of a factorization of a finite abelian group...

Proposition 2.6.1

Let $m, n \in \mathbb{Z}_+$. Then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if and only if $(m, n) = 1$.

If $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1}^{\alpha_1} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \dots \times \mathbb{Z}_{p_k^{\alpha_k}}.$$

Then we can go back and forth between the two representations by: factoring out our n_i's into their prime decomposition, in which case collecting each p_j factor gives you each of the Sylow p_j subgroups.

For the reverse direction, we group the elementary divisors by their p_i value, then take the product across different p_i in decreasing order. For example, if the elementary divisors of G are $2, 3, 2, 25, 3, 2$, then $|G| = 2^3 \cdot 3^2 \cdot 5^2$, so the invariant factors of G are $(2_1^1 \cdot 3_1^1 \cdot 5_1^2)$, $(2_2^1 \cdot 3_2^1 \cdot 5_2^0)$, and $(2_3^1 \cdot 3_3^0 \cdot 5_3^0)$, so that

$$G \cong \mathbb{Z}_{150} \times \mathbb{Z}_6 \times \mathbb{Z}_2.$$

This makes it very easy to compare groups of the same order, because if their elementary divisors differ, they cannot be isomorphic.

Definition 2.6.2: Rank

If G is a finite abelian group of type $(n_1, \dots, n_t)$, the integer t is called the **rank** of G.

Proposition 2.6.2

- If $|G| = p$, then $G \cong Z_p$
- If $|G| = p^2$, then G is Abelian and $G \cong Z_{p^2}$ OR $Z_p \times Z_p$
- Let $p > 2$, if $|G| = 2p$, then $G \cong Z_{2p}$ OR D_p.

The first two we have already seen from automorphisms. We will see the latter one after developing more group theory.

Chapter 3

Rings

Definition 3.0.1: Rings

A ring is a non-empty set with two operations, $+$ and $\cdot$. The $+$ operation is commutative, associative, has an identity, and inverses for all elements. The $\cdot$ operation is associative. Both operations have two distributive rules, namely, for all a, b, c,

$$(a+b)c = ac + bc$$
$$a(b+c) = ab + ac$$

If multiplication is commutative, then it is a commutative ring. If in addition, multiplication has an identity, and an inverse for all except the additive inverse, then it is a field.

Unless specified otherwise, we will assume our rings have a multiplicative identity.

Definition 3.0.2: Zero Divisors and Units

Let R be a ring. A nonzero element $a \in R$ is called a **zero divisor** if there exists a nonzero element $b \in R$ such that $ab = 0$ or $ba = 0$.

An element $u \in R$ is called a **unit** in R if there is a $v \in R$ such that $uv = vu = 1$– that is, u has a multiplicative inverse. The set of units in R is denoted R^X.

Every element besides 0 is a unit in a field. We can also see that units form a group under multiplication.

Notice that zero divisors and units are distinct concepts– a zero divisor can never be a unit.

Definition 3.0.3: Integral Domain

A commutative ring is called an **integral domain** if it has no zero divisors.

Proposition 3.0.1

Let $a, b, c \in R$ be elements of a ring with a not a zero divisor. Then

$$ab = ac \implies a = 0 \text{ or } b = c$$

In particular, if R is an integral domain this always holds.

Exercise 3.0.1

Prove that any finite integral domain is a field.
(Hint: consider $x \mapsto ax$ for a nonzero)

3.1 Subring, Ideals, Quotient rings, Ring homomorphisms

Definition 3.1.1: Subring

A subring is a subset S of a ring R which is a ring under the restriction of the operations in R. We denote this by $S \leq R$.

Remark 3.1.1

$S \leq R$ nonempty is a subring if and only if $a, b \in S \implies a+b, ab, -a \in S$. This is equivalent to $a, b \in S \implies a-b, ab \in S$.

Definition 3.1.2: Ideal

An ideal is a subring $I \leq R$ which is closed under multiplication with elements of R. Notationally, we say that $I \triangleleft R$.

Remark 3.1.2

I nonempty is an ideal if and only if $a, b \in I \implies a - b \in I$, which is equivalent to $a \in I, r \in R \implies ar, ra \in I$.

Exercise 3.1.1

Show that a field has only trivial ideals.

Definition 3.1.3: Principal Ideal

If R is commutative and has an identity, then the principal ideal generated by c is the ideal $(c) = \{rc \mid r \in R\}$.

This is the smallest ideal containing c.

3.2 Ring Homomorphisms and Quotient Rings

Definition 3.2.1: Ring Homomorphism

Let R, S be rings. A map $\varphi : R \to S$ that preserves operations is a **ring homomorphism**. In other words,

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = \varphi(a)\varphi(b)$$

Note that $\varphi(0) = 0$ and $\varphi(-a) = -\varphi(a)$. Furthermore, the kernel of a ring homomorphism is an ideal

Definition 3.2.2: Isomorphism

Let R, S be rings. A function $\varphi : R \to S$ that is bijective and a ring homomorphism is a **isomorphism**. If there exists a isomorphism between two rings, we say the rings are **isomorphic**.

Proposition 3.2.1: Equivalence of Isomorphism

A ring homomorphism $\varphi : R \to S$ is an isomorphism if and only if $\mathrm{Ker}\varphi = \{0\}$ and $\mathrm{Im}\varphi = S$

This is of course equivalent to φ being bijective.

Definition 3.2.3: Residue Class

The equivalence class of the integer a with the congruence relation, denoted by $\overline{a}_n$, is the set

$$\{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}$$

In other words, the set of integers congruent to $a \pmod{n}$ is the **residue class** of the integer a modulo n.

We can arbitrarily pick an element from a residue class as our representative when working with other residue classes– this greatly simplifies calculations.

Definition 3.2.4: Coset

Let $I \triangleleft R$. A **coset** denoted $r + I$ is the set

$$\{r + i \mid i \in I\}.$$

Proposition 3.2.2

Two cosets are either equal or disjoint.

We define addition and multiplication of cosets by

$$(r + I) + (s + I) = (r + s) + I$$
$$(r + I)(s + I) = rs + I$$

Definition 3.2.5: Sum and Products of Ideals

Let $I, J \triangleleft R$. Then we define:

$$I + J := \{a + b \mid a \in I,\ b \in J\},$$
$$IJ := \{a_1b_1 + a_2b_2 + \ldots + a_nb_n \mid a_i \in I,\ b_i \in J,\ n \in \mathbb{Z}_+\}$$
$$I^n = \left\{ \sum_{j=1}^{m} \{a_1a_2 \ldots a_n \mid a_i \in I\}_j \mid m \in \mathbb{Z}_+ \right\}$$

Equivalently, we can inductively define $I^n = II^{n-1}$.

Definition 3.2.6: Quotient Ring

Let $I \triangleleft R$. We notate by R/I the **quotient ring**, which is the ring with all of the cosets of I as elements, using the coset addition and multiplication defined above.

Theorem 3.2.1: First Isomorphism Theorem

Let $\varphi : R \to S$ be a ring homomorphism. Then $R/\mathrm{Ker}\varphi \cong \mathrm{Im}\varphi$.

Proof 3.2.1

We know that

$$a + \mathrm{Ker}\varphi = b + \mathrm{Ker}\varphi \iff \varphi(a) = \varphi(b).$$

Let $\psi : R/\mathrm{Ker}\varphi \to \mathrm{Im}\varphi$ be the map defined by $a + I \mapsto \varphi(a)$. This map is well-defined and bijective. Now it suffices to show that ψ is a ring homomorphism.

$$\psi\left((a + \mathrm{Ker}\varphi) + (b + \mathrm{Ker}\varphi)\right) = \psi\left((a + b) + \mathrm{Ker}\varphi\right) = \varphi(a + b) = \varphi(a) + \varphi(b)$$

which is equivalent to the sum of elements of ψ, as desired. One can check that multiplication holds the same as well.

This means that the homomorphism is completely determined by R.

Definition 3.2.7: Natural Homomorphism

Let $I \triangleleft R$ be an ideal of R. There exists a **natural homomorphism** $\varphi : R \to R/I$ defined by $\varphi : a \mapsto a + I$.

3.3 Direct Sums of Rings

Definition 3.3.1: Direct Sum

The **direct sum** of two rings $R_1 \oplus R_2$ (or direct product $R_1 \times R_2$) is the ring of all ordered pairs (r_1, r_2), with $r_i \in R_i$, with addition and multiplication defined by adding and multiplying the components:

$$(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2) \quad (r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2).$$

One can check that this indeed satisfies the properties of a ring.

Definition 3.3.2: Projection

The **projection** subsets are defined by

$$R_1^* := \{(r_1, 0) \mid r_1 \in R_1\}$$
$$R_2^* := \{(0, r_2) \mid r_2 \in R_2\}$$

These projection subsets are isomorphic to R_1, R_2 respectively. Furthermore, R_1^*, R_2^* are ideals in $R_1 \oplus R_2$, and every $c \in R_1 \oplus R_2$ has a unique decomposition $c = c_1 + c_2$ with $c_i \in R_i$.

Proposition 3.3.1: Unique Decompositions

If I, J are ideals in a ring R such that every $r \in R$ can be uniquely written as $r = i + j$, with $i \in I$, $j \in J$, then $R \cong I \oplus J$

Theorem 3.3.1: More Isomorphism Theorems

Let R be a ring.

- *(Second Isomorphism Theorem for Rings)* Let $A \leq R$ and $B \triangleleft R$. Then

$$A + B \leq R$$
$$A \cap B \triangleleft A$$
$$(A + B)/B \cong A/(A \cap B)$$

- *(Third Isomorphism Theorem for Rings* Let $I, J \triangleleft R$ with $I \subset J$. Then

$$J/I \triangleleft R/I$$
$$(R/I)/(J/I) \cong R/J$$

- Let $I \triangleleft R$. Then there is a correspondence between subrings $A < R$ that contain an ideal I and the subrings of R/I by $A \leftrightarrow A/I$. Furthermore, if $A \leq R$ contains I, then $A \triangleleft R$ if and only if $A/I \triangleleft R/I$.

3.4 Rings with Division Structures

For the section, assume that R is an integral domain.

Definition 3.4.1: Units and Associates

Let R be an integral domain. An element that divides every element of R is called a **unit**. The corresponding products are called **associates**; the associate of c is the product of c and the unit.

Definition 3.4.2: Irreducibles and Primes

A non-unit, non-zero $r \in R$ is **irreducible** if it can be factored ONLY trivially:

$$r = ab \implies a \text{ or } b \text{ is a unit}$$

A non-unit, non-zero $p \in R$ is a **prime** if it divides a product ONLY trivially:

$$p \mid ab \implies p \mid a \text{ or } p \mid b$$

Every prime is irreducible, but the converse is false in many rings.

Definition 3.4.3: Greatest Common Divisor

A **greatest common divisor** of a and b is a common divisor which is a multiple of all common divisors.

Any two gcds are associates; not every pair of elements has a gcd. This is closely related to the ideal (a, b).

Definition 3.4.4: UFD

R is a **unique factorization domain** if every non-zero and non-unit element in R is the product of irreducible elements, and the decomposition is unique aside from associates and the order of the factors.

$\mathbb{Z}, F[x], \mathbb{Z}[x]$ are some examples of UFDs.

Definition 3.4.5: PID

R is a **principal ideal domain** if every ideal of a principal ideal. A PID automatically satisfies the conditions for a UFD. However, the converse does not hold.

Definition 3.4.6: ED

R is a **Euclidean domain** if a division algorithm can be performed in R. This means that there is a function $f : R \setminus \{0\} \to \mathbb{N}$ such that, to any $b \neq 0, a \in R$ there exist $c, d \in R$ satisfying

$$a = bc + d \quad \text{and} \quad f(d) < f(b) \text{ or } d = 0$$

Some examples include $\mathbb{Z}$, $F[x]$, and the ring of Gaussian integers. Every ED is a PID, and so also a UFD. However, the converse does not hold.

Theorem 3.4.1: Connection with Ideals

- $c \mid d \iff d \in (c) \iff (d) \subset (c)$
- c and d are associates if and only if $(c) = (d)$
- $(d) = (a, b) \implies d = \gcd\{a, b\}$
- $(d) = (a, b) \iff d = \gcd\{a, b\}$ and $d = au + bv, \quad u, v \in R$

Theorem 3.4.2: UFD

An integral domain R is a UFD if and only if

- a strictly increasing sequence

  $$(a_1) \subset (a_2) \subset \ldots \subset (a_j) \subset \ldots$$

  of principal ideals cannot be infinite; and
- every irreducible element is a prime

3.5 Gaussian Integers and Applications

Definition 3.5.1: Gaussian Integers

The ring G with elements $a + bi \in \mathbb{C}$, with $a, b \in \mathbb{Z}$, is called the ring of **Gaussian Integers**.

[Norm] Let $\alpha \in \mathbb{C}$. Then the norm of α is defined by $\alpha\overline{\alpha}$

Theorem 3.5.1

$x^2 + y^2 = n$ solvable iff number of solutions

Theorem 3.5.2

The Gaussian Integers form a Euclidean Domain.

Proof 3.5.1

We will show that $f(\alpha) = N(\alpha)$ suffices. Observe that

$$\begin{aligned} \alpha = \beta\rho + \theta &\iff \\ \frac{\alpha}{\beta} = \rho + \frac{\theta}{\beta} &\iff \\ \frac{\alpha}{\beta} - \rho = \frac{\theta}{\beta} &\iff \\ \left|\frac{\alpha}{\beta} - \rho\right| < 1 & \end{aligned}$$

Of course, this is the distance between $\frac{\alpha}{\beta}$ and ρ. But there always exists a lattice point within distance 1 of any $\mathbb{C}$, and so therefore the statement holds.

Now we characterize all G-primes.

Proposition 3.5.1

To every Gaussian prime π, there exists exactly one positive prime number p satisfying $\pi \mid p$. Furthermore, every positive prime p is either a Gaussian prime, or the product of two complex conjugate Gaussian primes with norm p.

Theorem 3.5.3

All Gaussian primes take on the form:

- $\varepsilon(1+i)$
- εq, with q a positive prime of the form $4k-1$
- π where $N(\pi)$ is a positive prime of the form $4k+1$

where ε is a unit.

Proposition 3.5.2: Disjoint Partitions of Fields

Let R be a field. Then we can partition R into disjoint sets by taking all sets of the form

$$\left\{a, -a, a^{-1}, (-a)^{-1}\right\}$$

where a is non-zero, and taking the set $\{0\}$.

Theorem 3.5.4: Two Squares Theorem

Consider the equation $x^2+y^2 = n$, and let $n = 2^{\alpha} p_1^{\beta_1} \dots p_r^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s}$ be the Gaussian factorization of n. Then, $x^2+y^2 = n$ is solvable in $\mathbb{Z}$ if and only if all γ_j are even. Furthermore, the number of solutions is

$$4\prod_{j=1}^{r}(\beta_j + 1)$$

Proof 3.5.2

First, we write $n = x^2 + y^2 = (x + yi)(x - yi)$. Using the Gaussian factorization, we rewrite

$$n = 2^\alpha p_1^{\beta_1} \cdot \ldots \cdot q_1^{\gamma_1} \cdot \ldots = (-i)^\alpha (1+i)^{2\alpha} \pi_1^{\beta_1} \overline{\pi_1}^{\beta_1} \cdot \ldots \cdot q_1^{\gamma_1}$$

Now observe that

$$\begin{aligned}(x+yi) \mid n \implies x + yi &= \varepsilon(1+i)^{\alpha'} \pi_1^{\beta_1'} \overline{\pi_1}^{\beta_1''} \cdot \ldots \cdot q_1^{\gamma_1'} \cdot \ldots \\ \implies x - yi &= \overline{\varepsilon}(1-i)^{\alpha'} \overline{\pi_1}^{\beta_1'} \pi_1^{\beta_1'} \cdot \ldots \cdot q_1^{\gamma_1}\end{aligned}$$

Then because

$$\begin{aligned}n = (x+yi)(x-yi) &\implies \\ 2\alpha = \alpha' + \alpha' &\iff \alpha' = \alpha \\ \beta_1 = \beta_1' + \beta_1'' &\iff \beta_1' = 0, 1, \ldots, \beta_1; \beta_1'' = \beta_1 - \beta_1' \\ \gamma_1 = \gamma_1' + \gamma_1' &\iff \gamma_1 \text{ even}, \gamma_1' = \frac{\gamma_1}{2} \\ (-i)^\alpha = \varepsilon\overline{\varepsilon}(-i)^\alpha &\iff 1 = \varepsilon\overline{\varepsilon} \text{ which always holds}\end{aligned}$$

Thus, the equation is always solvable if all the γ are even. Looking at the above, the number of solutions will be

$$1 \cdot (\beta_j + 1) \cdot 1 \cdot 4 = 4 \prod_{j=1}^{r} (\beta_j + 1)$$

3.5.1 Fermat's Last Theorem

Theorem 3.5.5: Fermat's Last Theorem

Let $n \geq 3$. Does $x^n + y^n = z^n$ have positive integer solutions?

It is clear that if it is true for $n = 4$, $n = p$ prime, then it holds, as of course it will hold for any multiples. We can rewrite this as

$$x^p = z^p - y^p$$

y is a parameter, so the roots are

$$z^p = y^p \implies z = (y^p)^{\frac{1}{p}} = z, z\rho, z\rho^2, \ldots, z\rho^{p-1} \text{ where } \rho = \cos\frac{\pi}{p} + i\sin^2\frac{2\pi}{p}$$

So we can rewrite this as

$$x^p = z^p - y^p = (z-y)(z-\rho y)\ldots(z-\rho y^{p-1})$$

Observe that each prime must be a p-th power as they cannot share factors. Let

$$\begin{aligned}H_p = \left\{a_0 + a_1\rho + \ldots + a_{p-2}\rho^{p-2}\right\}, a_j \in \mathbb{Z} \\ \rho^{p-1} + \rho^{p-2} + \ldots + \rho + 1 = 0\end{aligned}$$

If the factors on the RHS are pairwise coprime, then $z - y = \varepsilon_0\theta_0^p$, $z - y\rho = e_1\theta_1^p$ BUT the units are non-trivial for these types of coefficients, AND we don't have UFT.

Then Kummer did a different direction. Note that "if there is a gcd then it is UFT" (not exactly, but dw about it). Then consider for $a, b \in \mathbb{Z}$

$$\gcd(a,b) = d \implies d = au + bv$$

Consider the set

$$\{ak + bl \mid k, l \in \mathbb{Z}\} = \{dn \mid n \in \mathbb{Z}\}$$

Now consider

$$\{ak + bl \mid k, l \in H_p\}$$

If $\exists \gcd(a, b) \implies$ this set is the set of multiples of gcd. So for "ideal numbers" UFT holds and the proof holds. So for "ideal numbers" UFT holds and the proof holds.

3.6 Finite Fields

Theorem 3.6.1

Let F be a finite field. $|F| = p^k$, p prime. Conversely, for every p^k there exists exactly one F such that $|F| = p^k$

Proof 3.6.1

We will show that the $\dim = k$; namely that there exists a basis $b_1, \ldots, b_k$ that generates all elements in F uniquely by

$$a = \lambda_1 b_1 + \ldots + \lambda_k b_k$$

where $\lambda_1, \ldots, \lambda_k \in \mathbb{Z}_p$, which by our other theorem is a subfield. This is isomorphic to $\mathbb{Z}_p[x]/(g)$ which is F. Observe that $\deg g = k$These are the residues mod g, or

$$a_0 + a_1 x + \ldots + a_{k-1} x^{k-1}$$

Each a_i can be chosen p ways, so then $|F| = p^k$, as desired.

Theorem 3.6.2

For any element $a \in F$ a finite field,

$$a + \ldots + a = 0$$

where a is added exactly p times.

Proof 3.6.2

For all a there exists an n such that

$$a + \ldots + a = 0$$

when a is added n times, because eventually the sequence $a, a+a, a+a+a, \ldots$ must repeat, and then you'll have your n. There are infinite solutions, but finitely many elements in F. This implies that

$$a + \ldots + a = a + \ldots + a$$

where on the LHS, a is added i times, and on the RHS added j times.
Assume that $i < j$. Observe that

$$a + \ldots + a = 0$$

for $j - i$ additions. Now assume that $a \neq 0$. Then multiply both sides by b implies

$$\forall b, b + \ldots + b = 0$$

because we can factor. Thus the assumption holds. Now we want to find the smallest $n > 0$. Assume for the sake of contradiction that $n = kl$, both greater than 1 (not prime). Then we can separate the sum into blocks of k and blocks of l. Then

$$\underbrace{a + \ldots + a}_{k} + \underbrace{\ldots}_{l} + \underbrace{a + \ldots + a}_{k} = 0$$

By assumption $a + \ldots + a$ is non-zero, so it is some $b \in F$. But then $\underbrace{b + \ldots + b}_{l} = 0$, which is a contradiction. So it has to be prime, as desired.

Theorem 3.6.3

Let F be a finite field. Then

$$F = \left\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{|F|-2}\right\}$$

and $\alpha^{|F|-1} = 1$

Theorem 3.6.4: Finite Field Extensions

For all finite fields F,there exists an $H \leq F$ such that $H \cong \mathbb{Z}_p$ for some p. Furthermore, F is a vector space over $\mathbb{Z}^p$.

F is then a field extension of H. Consider

$$H = \left\{0, 1, 1+1, \ldots, \underbrace{1 + \ldots + 1}_{p-1}\right\}$$

Observe that adding and multiplying elements works like traditional addition and subtraction; namely that

$$(t \cdot 1) + (s \cdot 1) = (s + t) \pmod{p} \cdot 1$$

for $0 \leq t \leq p - 1$ and

$$(\underbrace{1 + \ldots + 1}_{t}) \cdot (\underbrace{1 + \ldots + 1}_{s}) = (ts) \pmod{p} \cdot 1$$

and so the isomorphism to $\mathbb{Z}_p$ holds, as all the elements can then be written by multiplication of $0 \leq t \leq p - 1$ and 1.

Theorem 3.6.5

For any finite field F, $F \cong \mathbb{Z}_{p[x]}/(g)$ where g is a polynomial over $\mathbb{Z}_p$, $\deg\, g = k$, g irreducible over $\mathbb{Z}_p$