Math 315 - Artin Notes and Fun

Elijah Thompson

December 31, 2020

Contents

1 Matrix Basics

1.1 Determinants

1.2 Permutation Matrices

Definition 1.1 (Permutation)**.** A **permutation** of a set S is a bijective map on S.

Definition 1.2 (Permutation Matrix)**.** A **permutation matrix** P with the following property:

The operation of left multiplication by the matrix P is a permutation of rows.

Example 1.3. Let P be the permuation matrix

$$P = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

and let $\mathbf{X}$ be a three-dimensional column vector. It follows that

$$P\ \mathbf{X} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_2 \\ x_3 \\ x_1 \end{bmatrix}$$

Note that the indices are permuted as $1 \to 2 \to 3 \to 1$, which is the inverse of where the entries are sent. We say the permutation associated with P is the one which describes its action on the entries of a column vector. Then the indices are permuted by the inverse:

$$P\ \mathbf{X} = \begin{bmatrix} x_{p^{-1}(1)} \\ \vdots \\ x_{p^{-1}(n)} \end{bmatrix}$$

Proposition 1.4. *Let P be the permutation matrix associated to the permutation p.*

1. *The jth column of P is the column vector $e_{p(j)}$*
2. *P is the sum of n matrix units:*

$$P = e_{p(1),1} + \ldots + e_{p(n),n} = \sum_{j=1}^{n} e_{p(j),j}$$

Proposition 1.5. *1. Let p and q be permutations with associated permutation matrices P and Q. Then the matrix associated to the permutation pq is PQ*

2. A permutation matrix P is invertible, and its inverse is the transpose matrix (it is orthogonal)

Definition 1.6 (Sign)**.** The **sign** of a permutation p is the determinant of its associated permutation matrix. A permutation is even if its sign is $+1$, and is odd if its sign is -1.

2 Groups

2.1 Intro to Groups

Definition 2.1 (Group)**.** A group is a set G with a **law of composition** $\cdot : G \times G \to G$ defined on G such that

1. $\cdot$ is associative.
2. There exists $e \in G$ so that for all $g \in G$, $e \cdot g = g \cdot e = g$
3. For all $g \in G$ there exists $g^{-1} \in G$ so that $g \cdot g^{-1} = g^{-1} \cdot g = e$

If a group has the added property that for all $g, g' \in G$, $gg' = g'g$, then G is said to be **abelian** or **commutative**

Proposition 2.2. *Suppose we have an associative law of composition on a set S. There is a unique way to define, for every integer n, a product of n elements $a_1, ..., a_n$ of S (denote it by $[a_1...a_n]$ for now) with the following properties:*

1. *The product $[a_1]$ of one element is the element itself*
2. *The product $[a_1a_2]$ of two elements is given by the law of composition*
3. *For any integer i between 1 and n, $[a_1...a_n] = [a_1...a_i][a_{i+1}...a_n]$*

Proof. Suppose $n \in \mathbb{N}$. We argue by induction on n. The product is defined by 1) and 2) for $n \leq 2$, and it satisfies 3) when $n = 2$. Suppose we are able to define the product rule for $r \leq n-1$, and that this product is the unique product satisfying 3). We then define the product of n elements by the rule

$$[a_1 \dots a_n] = [a_1 \dots a_{n-1}][a_n] \tag{2.1}$$

where the terms on the right side are already defined by the induction hypothesis. If a product satisfying 3) exists, then this formula gives the product because it satisfies 3) when $i = n-1$. So, if it exists, the product is unique. We must now check 3) for $i < n-1$:

$$\begin{aligned}
[a_1 \dots a_n] &= [a_1 \dots a_{n-1}][a_n] && \text{(our definition)} \\
&= ([a_1 \dots a_i][a_{i+1} \dots a_{n-1}])[a_n] && \text{(by the induction hypothesis)} \\
&= [a_1 \dots a_i]([a_{i+1} \dots a_{n-1}][a_n) && \text{(by associativity)} \\
&= [a_1 \dots a_i][a_{i+1} \dots a_n] && \text{(by the induction hypothesis)}
\end{aligned}$$

This completes the proof. ■

Proposition 2.3 (Cancellation Law)**.** *Let a, b, c be elements of a group G. If $ab = ac$ then $b = c$. Additionally, if $ba = ca$ then $b = c$ as well.*

Example 2.4 (Examples of Groups)**.** .

1. The **general linear group of order n** over F is the set of all invertible matrices over a field F, with the law of composition being matrix multiplication: $GL_n(F) = \{A \in M_{n\times n}(F) : \det(A) \neq 0\}$.
2. The set $S = Aut(T, T)$ of bijective functions on the set T is a group with the composition law being function composition.
3. The group of **permutations** of the set $\{1, 2, ..., n\}$ is called the **symmetric group on n letters**, and is denoted by

$$S_n := \{f : \{1, 2, ..., n\} \to \{1, 2, ..., n\} : \exists f^{-1}\} \tag{2.2}$$

The order of S_n is $n!$. Moreover, for $n \geq 3$, S_n is non-abelian.

2.2 Subgroups

Definition 2.5 (Subgroup)**.** A subset H of a group G is called a **subgroup** if it has the following properties:

1. Closure: $\forall h, h' \in H, hh' \in H$
2. Identity: $\exists 1 \in H$
3. Inverses: $\forall h \in H, \exists h^{-1} \in H : hh^{-1} = h^{-1}h = 1$

Example 2.6 (Obvious Subgroups)**.** Every group G has the subgroups G and $\{e\}$.

Proposition 2.7 (Subgroups of the Integers)**.** *For any integer b, the subset $b\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$. Moreover, every subgroup $H \subset \mathbb{Z}$ is of the form $H = b\mathbb{Z}$ for some $b \in \mathbb{Z}$.*

Proof. Suppose $b \in \mathbb{Z}$. Then observe that for all $bk, bl \in b\mathbb{Z}$, $bk + bl = b(k + l) \in b\mathbb{Z}$, $0 = b0 \in b\mathbb{Z}$, and $(-k)b \in b\mathbb{Z}$, so $b\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. Now, suppose H is a subgroup of $\mathbb{Z}$. Then, if $H = \{0\}$, $H = 0\mathbb{Z}$. Otherwise, H has at least one positive integer since it is a subgroup, and hence stable under inversion. Now, suppose by the Well-Ordering Principle of the positive integers that b is the smallest positive integer of H. Then, let $c \in H$. By the Quotient Remainder Theorem there exists unique integers $q, r \in \mathbb{Z}$ so that $c = bq + r$ where $0 \leq r < b$. In particular, since H is a subgroup, $r \in H$. Hence, $r = 0$, as otherwise r would be a positive integer in H which is smaller than b, which would be a contradiction. Therefore $b \mid c$, so $H \subset b\mathbb{Z}$, and since $b \in H$ and H is a subgroup, $b\mathbb{Z} \subset H$. Hence, we conclude that $H = b\mathbb{Z}$. ■

Definition 2.8 (Subgroup of the Integers Generated by Two Integers)**.** The set

$$a\mathbb{Z} + b\mathbb{Z} := \{n \in \mathbb{Z} : n = ar + bs, r, s \in \mathbb{Z}\} \tag{2.3}$$

is the subgroup of $\mathbb{Z}$ generated by a and b.

Proposition 2.9 (GCD)**.** *Let $a, b \in \mathbb{Z}$, not both zero, and let d be the positive integer which generates the subgroup $a\mathbb{Z} + b\mathbb{Z}$. Then*

1. *d can be written in the form $d = ar + bs$ for some $r, s \in \mathbb{Z}$*
2. *d divides a and b*
3. *If an integer e divides a and b, then it also divides d*

Proof. Since d generates $a\mathbb{Z} + b\mathbb{Z}$, $d \in a\mathbb{Z} + b\mathbb{Z}$. In particular, there exist $r, s \in \mathbb{Z}$ so that $d = ar + bs$. Next, notice that a and b are in the subgroup $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. Then by definition d divides a and b. Finally, if e is an integer which divides a and b, then a and b are in $e\mathbb{Z}$. This being so, any integer $n = ar + bs$ is also in $e\mathbb{Z}$. In particular, d has this form by assumption so $d \in e\mathbb{Z}$ and e divides d. ■

Definition 2.10 (Cyclic Subgroup)**.** Suppose that G is a group and $x \in G$. Then the **cyclic subgroup generate by** x is the set

$$\langle x \rangle := \{x^n : n \in \mathbb{Z}\} \tag{2.4}$$

In particular, $\langle x \rangle$ is the smallest subgroup of G which contains x. If all the elements in the set are distinct, then the group $\langle x \rangle$ is called infinite cyclic.

Lemma 2.11. *The set S of integers n such that $x^n = 1$ is a subgroup of $(\mathbb{Z}, +)$.*

Proof. Suppose $x^m = 1$ and $x^n = 1$. Then $x^{m+n} = x^m x^n = 1$ too. Hence, if $m, n \in S$, $m + n \in S$. Moreover, $x^0 = 1$, so $0 \in S$. Finally, if $x^n = 1$, then $x^{-n} = x^{-n}x^n = x^0 = 1$, so $-n \in S$. Thus, S is a subgroup of $(\mathbb{Z}, +)$ ■

Definition 2.12 (Order)**.** The **order** of any group is the number of its elements. We say that a cyclic group $\langle x \rangle$ is of order m if m is the smallest positive integer such that $x^m = 1$. Moreover, an element of a group is said to have order m if the order of the cyclic group it generates is of order m.

Remark 2.13. As with elements, if U is a subset of a group G, then the smallest subgroup of G containing U is the subgroup of G generated by U.

Definition 2.14 (Klien Four Group)**.** The **Klien Four Group** K_4 is the simplest group which is not cyclic. One representation of the Klien Four Group is

$$K_4 = \left\{ \begin{bmatrix} \pm 1 & \\ & \pm 1 \end{bmatrix} \right\} \tag{2.5}$$

Definition 2.15 (Quaternion Group)**.** The **Quaternion Group** H is a group which can be represented as a subgroup of $GL_2(\mathbb{C})$, defined as

$$H := \left\{ \pm \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}, \pm \begin{bmatrix} i & \\ & -i \end{bmatrix}, \pm \begin{bmatrix} & 1 \\ -1 & \end{bmatrix}, \pm \begin{bmatrix} & i \\ i & \end{bmatrix} \right\} \tag{2.6}$$

2.3 Group Homomorphisms

2.3.1 Textbook

Definition 2.16 (Isomorphic)**.** Two groups G and G' are said to be **isomorphic** if all properties of the group structure of G hold for G' and vice-versa. We formalize this by saying there exists a bijection map between G and G' which respects the composition law of groups. An isomorphism $\phi : G \to G'$ is a bijective map with the condition that

$$\phi(ab) = \phi(a)\phi(b), \forall a, b \in G \tag{2.7}$$

and we write $G \cong G'$

Definition 2.17 (Automorphisms)**.** An **automorphism** on a group G is a map $\phi : G \to G$ which is an isomorphism. The set $Aut(G)$ of automorphisms on G is a group with the law of composition being function composition.

Definition 2.18 (Inner Automorphisms)**.** An **inner automorphism** ϕ on a group G is an automorphism given by $\phi(g) = xgx^{-1}$ for some $x \in G$. Such a map is also called **conjugation by x**. The element bab^{-1} is called the **conjugate of a by b**. Two elements $a, a' \in G$ are called **conjugate** if there exists $b \in G$ so that $a' = bab^{-1}$.

Definition 2.19 (Homomorphism)**.** Let G and G' be groups. Then a **homomorphism** $\phi : G \to G'$ is any map which respects the group structure, so

$$\phi(ab) = \phi(a)\phi(b), \forall a, b \in G \tag{2.8}$$

Example 2.20. .

1. The determinate function $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$.
2. The sign of a permutation, $sign : S_n \to \langle \pm 1 \rangle$
3. The map $\phi : (\mathbb{Z}, +) \to G$ defined by $\phi(n) = a^n$ where a is fixed in G
4. The inclusion map $i : H \to G$ of a subgroup H into a group G, defined by $i(x) = x$

Proposition 2.21. *A group homomorphism carries the identity to the identity and carries inverses to inverses.*

Definition 2.22 (Image and Kernel)**.** Given a homomorphism $\phi : G \to G'$, the **image** of ϕ is

$$\text{im}(\phi) := \{\phi(g) \in G' : g \in G\} \tag{2.9}$$

and is a subgroup of G'. The **kernel** of ϕ is the set of elements of G which are sent to the identity in G':

$$\ker(\phi) := \{g \in G : \phi(g) = 1\} \tag{2.10}$$

The kernel can also be described as the inverse image of the identity, $\phi^{-1}(1)$, and is a subgroup of G.

Example 2.23. The kernel of the determinant map is known as the **special linear group** and is denoted

$$SL_n(\mathbb{R}) := \{A \in GL_n(\mathbb{R}) : \det(A) = 1\} \tag{2.11}$$

The kernel of the sign homomorphism is the **alternating group on n letters** defined by

$$A_n := \{even\ permutations\} \tag{2.12}$$

Definition 2.24 (Normal Subgroups)**.** A subgroup N of a group G is called a **normal subgroup** of G if it is stable under conjugation. That is for all $a \in N$ and for all $g \in G$, $gng^{-1} \in N$.

Remark 2.25. The kernel of a homomorphism is a normal subgroup.

Definition 2.26 (Center)**.** The **center** of a group G is the set of all elements in G which commute with all elements in G, and is denoted

$$Z(G) := \{z \in G : \forall g \in G, zg = gz\} \tag{2.13}$$

The center of any group is a normal subgroup of the group.

2.3.2 Lecture

Definition 2.27 (Homomorphism)**.** A **group homomorphism** $f : G \to H$ is a homomorphism of sets (a function) between groups such that for all $g, h \in G$

$$f(g \cdot h) = f(g) \cdot f(h) \tag{2.14}$$

Property 2.28 (General Properties)**.** *Let $f : G \to H$ be a* ***homomorphism****.*

1. *$f(e_G) = e_H$ (The identity is stabilized under group homomorphisms)*
2. *$f(g^{-1}) = f(g)^{-1}$ for all $g \in G$.*

Definition 2.29 (Composition)**.** Let $f : G \to H$ and $g : H \to G'$ be homomorphisms. Then $g \circ f : G \to G'$ is a homomorphism.

Definition 2.30 (Image and Kernel)**.** There are two very important sets for any given homomorphism $f : G \to H$:

$$Im(f) := \{g' = f(g) : g \in G\} \leq H \tag{2.15}$$

$$ker(f) := \{g \in G : f(g) = e\} \leq G \tag{2.16}$$

Both of these sets are **subgroups**.

Definition 2.31 (Isomorphism)**.** A group **isomorphism** is a group homomorphism $f : G \to G'$ that is bijective. If $G = G'$, then f is an **automorphism**.

Theorem 2.32 (Isomorphism)**.** *A group homomorphism, $f : G \to G'$, is an isomorphism if and only if $Im(f) = G'$ and $ker(f) = \{e\}$.*

Definition 2.33 (Normal Subgroup)**.** A subgroup H of G is **normal**, denoted $H \trianglelefteq G$, has the property that for all $g \in G$, we have that $gHg^{-1} := \{ghg^{-1} : h \in H\} = H$ - that is normal subgroups are closed under **conjugation** by all elements in the larger group.

Observation 2.34. First, note that in an abelian group, all subgroups are normal. Take the non-abelian group $G = S_3$, and let $H = \langle e, \tau_{12} \rangle$. Let us try conjugate by τ_{23}. Observe that

$$\tau_{23}\tau_{12}\tau_{23}^{-1}(3) = \tau_{23}\tau_{12}\tau_{23}(3) = 1 \neq \tau_{12}(3)$$

Hence, $\tau_{23}\tau_{12}\tau_{23}^{-1} \notin H$. Thus, H is not normal.

Proposition 2.35 (Normal Kernel)**.** *The kernel of any group homomorphism is a normal subgroup of the domain group.*

Remark 2.36. Everything is about homomorphisms fundamentally.

Example 2.37 (1)**.** Take $\det : GL_n(\mathbb{R}) \to R^\times = GL_1(\mathbb{R})$ as the map $\det(A)$, with the property that

$$\det(AB) = \det(A)\det(B) \tag{2.17}$$

Note that $Im(f) = R^\times$ since

$$\det \begin{bmatrix} \lambda & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix} = \lambda$$

and $ker(f) = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\} = SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$ (the **special linear group of dimension n**).

Example 2.38 (2)**.** We take the homomorphism $f : S_n \to GL_n(\mathbb{R})$ which takes a permutation σ to a matrix

$$f(\sigma) = A_\sigma = \text{permutation matrix associated to } \sigma \tag{2.18}$$

with the jth column given by

$$A_{\sigma j} = \ \mathbf{e}_{\sigma(j)} \tag{2.19}$$

Example 2.39 (2.1)**.** Take $G = S_3$ and

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

Then the permutation matrix is given by

$$A_\sigma = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

We must check that $f(pq) = A_p A_q$ for all permutations p and q in S_n. Observe that

$$A_p A_q = \left[\ \mathbf{e}_{p(1)} \cdots \ \mathbf{e}_{p(n)}\right] \left[\ \mathbf{e}_{q(1)} \cdots \ \mathbf{e}_{q(n)}\right] = \left[\ \mathbf{e}_{(p\circ q)(1)} \cdots \ \mathbf{e}_{(p\circ q)(n)}\right] = f(pq)$$

The image of f is the subgroup of all permutation matrices in $GL_n(\mathbb{R})$, while the kernel is only the identity permutation.

Example 2.40 (5 - Sign)**.** Note that the determinant of a permutation matrix is ± 1, so the image of this homomorphism is one in which all elements have determinant ± 1. Moreover, if we compose f and det, then we have the homomorphism

$$\det \circ f : S_n \to GL_n(\mathbb{R}) \to \mathbb{R}^\times \tag{2.20}$$

with $Im = \langle -1 \rangle < \mathbb{R}^\times$ and $A_n = ker = \{\sigma : \det(f(\sigma)) = +1\} \trianglelefteq S_n$ is the **alternating group on n letters**.

Example 2.41 (Even and Odd)**.** In S_n, all transpositions are odd permutations and all cycles are even permutations (so are in A_3)

Proposition 2.42 (Alternating Group Size)**.** *For $n \geq 2$, then we have that $|A_n| = \frac{n!}{2}$.*

Definition 2.43 (Center)**.** For a group G, the normal subgroup denoted $Z(G)$ is called the **center of** G, and is the set of all elements in G which commute with every element in G:

$$Z(G) := \{z \in G : zg = gz \forall g \in G\} \tag{2.21}$$

Observation 2.44. The center of any abelian group is equal to the group. The center of S_n on the other hand is $Z(S_n) = \{e\}$ if $n \geq 3$. For the $GL_n(\mathbb{R})$, the center is $Z(GL_n(\mathbb{R}) = \{\lambda I\}$, $\lambda \in \mathbb{R}^\times$. The center is a **normal subgroup which is abelian**.

Example 2.45 (4)**.** Consider the homomorphism $f : G \to Aut(G)$, where G is a group, and $Aut(G)$ is thr group of all automorphisms on G. For all $g \in G$ we take $h \in G$ to

$$f(g)(h) = ghg^{-1} \tag{2.22}$$

Note that $f(g)$ is a set-theoretic isomorphism, since it has an inverse $f(g^{-1})$, and for all $h, h' \in G$

$$f(g)(hh') = ghh'g^{-1} = ghg^{-1}gh'g^{-1} = f(g)(h)f(g)(h')$$

Thus, $f(g)$ gives an automorphism of G, so $f(g) \in Aut(G)$, as desired. Next, observe that for all $g, g' \in G$, we have that

$$f(gg')(h) = gg'h(gg')^{-1} = gg'hg'^{-1}g^{-1} = f(g)(f(g')(h)) = (f(g) \circ f(g'))(h)$$

so f is a homomorphism. The kernel of f is set of all elements in G which are stable under conjugation (The center of G), so $ker(f) = Z(G)$.

Example 2.46 (4.1)**.** Consider $G =$ the **Klein 4-group**,

$$K_4 = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\} = \{e, \tau_1, \tau_2, \tau_3 : \tau_1^2 = \tau_2^2 = \tau_3^2 = e, \tau_1\tau_2 = \tau_3\}$$

Note that the Klein 4-group is abelain, and of order 4, so the image of f is only the identity automorphism. However, it can be shown that $Aut(K_4) \equiv S_3$. In particular, if $a : G \to G$ is an automorphism, then we can associate to a a permutation of $\{\tau_1, \tau_2, \tau_3\}$. This association gives a homomorphism $Aut(K_4) \to S_3$ with trivial kernel. (Check that all permutations of $\{\tau_1, \tau_2, \tau_3\}$ give automorphisms on K_4) And the image is in fact all of S_3.

From this example we see that the image of f need not be all of $Aut(G)$, and in fact the image of f is called the **inner automorphisms of** G, denoted $Inn(G)$, so $Im(f) = Inn(G) = \{a(h) = aha^{-1} : a \in G\}$.

2.4 Cosets

2.4.1 Textbook

Definition 2.47 (Equivalence Relation on Maps)**.** Given any map $\phi : S \to T$, we can define an equivalence relation on the domain S by declaring for all $a, b \in S$, $a \sim b$ if $\phi(a) = \phi(b)$. Note that for an element $t \in T$, the **fibre** of ϕ above t is the set

$$\phi^{-1}(t) := \{s \in S : \phi(s) = t\} \tag{2.23}$$

Therefore, the non-empty fibres of the map ϕ form a partition of the set S. Moreover, the set $\overline{S}$ of equivalence classes is the set of non-empty fibres of the map in this case. This definition induces a bijective map

$$\overline{\phi} : \overline{S} \to \text{im}(\phi) \tag{2.24}$$

by $\overline{\phi}(\overline{s}) = \phi(s)$.

Proposition 2.48. *Let $\phi : G \to G'$ be a group homomorphism with kernel N, and let $a, b \in G$. Then $\phi(a) = \phi(b)$ if and only if $b = an$ for some $n \in N$, or equivalently, $a^{-1}b \in N$.*

Definition 2.49 (Coset)**.** The set with elements of the form an for $n \in N$ and $a \in G$ fixed is called a (left) **coset** of N in G

$$aN := \{an : n \in N\} \tag{2.25}$$

The cosets of a subgroup N of G partition the group.

Corollary 2.50. *A group homomorphism $\phi : G \to G'$ is injective if and only if its kernel is the trivial subgroup $\{1\}$.*

Definition 2.51 (Index)**.** The number of left cosets of a subgroup H in a group G is called the **index** of H in G, and is denoted by $[G : H]$

Proposition 2.52. *For all $a \in G$, there is a bijection map $H \to aH$ which takes $h \mapsto ah$. Thus, $|H| = |aH|$ for all $a \in G$*

Corollary 2.53 (Counting Formula)**.** *Since the cosets of a subgroup H partition the group G, it follows that $|G| = |H|[G : H]$.*

Corollary 2.54 (Lagrange's Theorem)**.** *Let G be a finite group, and let H be a subgroup of G. Then the order of H divides the order of G. Moreover, this implies that for all $g \in G$, the order of g divides the order of G.*

Corollary 2.55. *Suppose that G is a group of order p which is prime. Then for all $a \in G$, if $a \neq 1$, the $G = \langle a \rangle$, so G is a cyclic group generated by all non-trivial elements in it.*

Corollary 2.56 (Counting Formula for Homomorphisms)**.** *Given a homomorphism $\phi : G \to G'$, the left cosets of $\ker(\phi)$ are fibres of $\operatorname{im}(\phi)$. Moreover, the fibres are in bijective correspondance with the elements in the image, so*

$$[G : \ker(\phi)] = |\operatorname{im}(\phi)| \tag{2.26}$$

This implies that if G and G' are finite groups, then

$$|G| = |\ker(\phi)| \cdot |\operatorname{im}(\phi)| \tag{2.27}$$

Thus $|\ker(\phi)|$ divides the order of G, and $|\operatorname{im}(\phi)|$ divides the order of G and G'

Proposition 2.57. *A subgroup H of a group G is normal if and only if every left coset of H is also a right coset. That is, if H is normal, then $aH = Ha$ for all $a \in G$.*

2.4.2 Lecture

Definition 2.58 (Equivalence Relation)**.** An **equivalence relation** on a set S can be thought of as a partition of S as disjoint subsets which union to form the set. In particular, an equivalence relation $\sim$ on S has the properties

1. $a \sim a$ for all $a \in S$
2. If $a \sim b$ then $b \sim a$
3. If $a \sim b$ and $b \sim c$, then $a \sim c$

We can consider the relation as a subset of $S \times S$, with the first property translating to the subset containing the diagonal, and the second equating to if an element is in the set, its reflection across the diagonal is also in the set.

Remark 2.59. Every partition on a set S generates an equivalence relation on S, and every equivalence relation generates a partition of S with equivalence classes.

Definition 2.60 (Equivalence Classes)**.** Each subset of a partition is an **equivalence class**. In particular, given an equivalence relation $\sim$ on a set S, for $a \in S$, the equivalence class of a is given by

$$[a]_\sim = \{b \in S : a \sim b\} \tag{2.28}$$

We can define the **canonical projection** as the map $S \to \overline{S} = \{\text{equivalence classes in S}\}$.

Remark 2.61. If we have a map $f : S \to T$, this gives an equivalence relation or partition on S

$$a \sim b \iff f(a) = f(b) \text{ in } T \tag{2.29}$$

For any $t \in T$, the **fiber above t** on f is the set $f^{-1}(\{t\}) = \{s \in S : f(s) = t\}$. These fibers are the equivalence classes for our partition. We can then directly associated the set of equivalence classes, $\overline{S}$, with the image, $Im(f)$. For each point in the image you have the fiber above it which can be associated with it, so the image can be identified with the partition on S.

Example 2.62. Consider the map $f : \mathbb{R} \to \mathbb{C}$ given by $f(t) = e^{2\pi i t}$ for all $t \in \mathbb{R}$. Then we have that the fiber above 1 is

$$f^{-1}(\{t\}) = \{n \in \mathbb{R} : n \in \mathbb{Z}\}$$

The unit circle in the complex plane can be identified with the partition generated by this map, with the equivalence classes being the points in $[0, 1]$ (where the endpoints are adjoined). (Note that this is in fact a group homomorphism since $f(a + b) = f(a) \cdot f(b)$, and it is also a **homomorphism of Lie Groups**, and preserves the topological structure of $\mathbb{R}$).

Definition 2.63 (Group Homomorphism Partitions)**.** Suppose $f : G \to G'$ be a group homomorphism, and let $H \trianglelefteq G$ be the kernel of f. We then get an equivalence relation on G, where H is one of the equivalence classes (always!).

Question. Why? Because the $H := f^{-1}(e') = \{a \in G : f(a) = f(e) = e'\}$.

Proposition 2.64 (Equivalence Classes)**.** *Equivalence Classes have the form a* $H = \{ah : h \in H\}$ *for some* $a \in G$.

Proof. Say $f(a) = f(b) \in G'$, so $a \sim b$. Then $f(a^{-1}b) = e'$ since f is a homomorphism. Thus, $a^{-1}b \in H$. In other words $a^{-1}b = h \in H$. It follows immediately that $b = ah$. Thus, for all $b \in G$ such that $b \sim a$, so $b \in a\ H$. Conversely, for all $c \in a\ H$, there exists $h \in H$ so that $c = ah$, and $f(c) = f(ah) = f(a)f(h) = f(a)$, since $h \in H$, so $c \sim a$. ■

Definition 2.65 (Coset)**.** A **left coset** of a subgroup H of a group G is a set of the form

$$k\ H := \{kh \in G : h \in H\} \tag{2.30}$$

for some $k \in G$.

Proposition 2.66. *The map* $h \mapsto ah$ *gives a bijection of sets,*

$$H \xrightarrow{\sim} aH \tag{2.31}$$

Proof. One-to-one: If $ah = ah'$, then $h = h'$ (multiplying by a^{-1}. Onto: For any $ah \in a\ H$, take $h \in H$ so $h \mapsto ah$. ■

Corollary 2.67. *In particular, if* $|H|$ *is finite, then* $|H| = |a\ H|$ *for all* $a \in G$.

Corollary 2.68 (Group Homomorphism Equivalence Classes)**.** *For a group homomorphism, the equivalence classes are of the form a* H, $H = ker(f)$, *and have the same size (cardinality).*

Example 2.69 (Counter-example)**.** Take a set-theoretic fap $f : \{1, 2, 3\} \to \{1, 2\}$ with $f(1) = f(2) = 1$ and $f(3) = 2$, so we get unequally sized cosets.

Corollary 2.70 (Lagrange's Theorem)**.** *Assume that G is finite and $f : G \to G'$ is a homomorphism with kernel H. Then*

$$|G| = |H| \cdot |Im(f)| = |ker(f)| \cdot |Im(f)| \tag{2.32}$$

Since the cosets of H partition G, and are all of equal size, with the number of cosets equivalent to the number of points in the image of f (prove this).

Recall. In linear algebra, we have the Dimension Theorem: If $T : V \to W$ is a linear map, then $\dim(V) = \dim(ker(T)) + \dim(Im(T))$.

Example 2.71. It follows that since $|S_n| = n!$, for $n \geq 2$, $|A_n| = \frac{n!}{2}$.

Proof. Take $f : S_n \to \langle \pm 1 \rangle$, then for $n \geq 2$ the map is surjective, so $|Im(f)| = 2$, and $ker(f) = A_n$, so

$$|A_n| = \frac{|S_n|}{|Im(f)|} = \frac{n!}{2}$$

■

Corollary 2.72 (General Result)**.** *Let $H \leq G$ be any subgroup (not necessarily normal). We define the (left) coset of $a \in G$ by*

$$a\,H := \{ah : h \in H\} \tag{2.33}$$

and these subsets are disjoint and partition G. Furthermore, there are in set-theoretic bijection with H, (so have the same cardinality, or number of elements for finite sets).

Definition 2.73 (Index of a Subgroup)**.** We define the **index of H in G**, which might be infinite, as the number of distinct (left) cosets, (or number of equivalence classes). We denote it by

$$[G : H] \tag{2.34}$$

Corollary 2.74 (Lagrange Formula)**.** *It follows from above that*

$$|G| = |H|[G : H] \tag{2.35}$$

Theorem 2.75 (Lagrange's Theorem)**.** *If $|G|$ is finite, and $g \in G$, then the order of g divides $|G|$.*

Recall. Recall that the order of $g \in G$ is the smallest $m \in \mathbb{N}$ so that $g^m = e$.

Proof. We use Lagrange's Theorem, and take $H = \langle g \rangle = \langle e, g, g^2, ...g^{m-1} \rangle$. So $|H| = m =$ order of g. ■

Corollary 2.76 (Prime Order)**.** *Let G be a finite group with the order of $|G| = p$, where p is prime. Then, G is cyclic, generated by any $g \in G$, with $g \neq e$. Furthermore, the only subgroups of G are $\{e\}$ and G.*

Proof. Let $g \neq e \in G$. The order of g divides p, and is not 1 (since the only element of order 1 is e). Hence, since p is prime, the order of g is equal to p. It follows that the order of $\langle g \rangle \leq G$ is also p, and since $|G| = p$, $\langle g \rangle = G$. Then, for any subgroup $H \leq G$, $|H| = 1$ or $|H| = p$, so H is either $\{e\}$ or G. ■

Question. Can we show this is a strong theorem by exhibiting non-cyclic groups of order p^2 or pq?

Answer. Yes, but all groups of order p^2 are abelian.

Example 2.77. Take the Klein 4-group of order 2^2, which is not cyclic. Moreover, if we take S_n, of order $2 * 3$, it is not cyclic or even abelian.

2.5 Simple Groups

Definition 2.78 (Simple)**.** A group G is **simple** if its only normal subgroups H are $\{e\}$ and G (means you can't break it down into simpler groups).

Example 2.79.
1. Any G of prime order p (These are the only abelian simple groups).
2. A_n is simple for $n \geq 5$.
3. Any finite non-abelian simple group has even order

Theorem 2.80 (Finite Non-Abelian Simple Groups)**.** *Any finite non-abelian simple group has even order.*

Remark 2.81. You can make any group out of finite simple groups, but it is very complicated.

Definition 2.82 (Finite Simple Groups)**.** We start with A_5, and we see that A_n for $n \geq 5$ is simple. Another example of a simple group is $SL_2(\mathbb{Z}/p\mathbb{Z})/\langle \pm I \rangle$ is simple for all primes $p \geq 5$. Recall that the order of $GL_2(\mathbb{Z}/p\mathbb{Z})$ is the number of bases, $(p^2-1)(p^2-p)$, and $\det : GL_2(\mathbb{Z}/p\mathbb{Z}) \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^*$, where $(\mathbb{Z}/p\mathbb{Z})^*$ has order $p-1$. Thus, since $|GL_2(\mathbb{Z}/p\mathbb{Z})/SL_2(\mathbb{Z}/p\mathbb{Z})| = |(\mathbb{Z}/p\mathbb{Z})^*|$, $|SL_2(\mathbb{Z}/p\mathbb{Z})| = \frac{|GL_2(\mathbb{Z}/p\mathbb{Z})|}{|(\mathbb{Z}/p\mathbb{Z})^*|}$, so $|SL_2(\mathbb{Z}/p\mathbb{Z})| = (p^2-1)p$, and finally

$$|SL_2(\mathbb{Z}/p\mathbb{Z})/\langle \pm I \rangle = \frac{p(p^2-1)}{2} \tag{2.36}$$

Claude Chevalley came up with a method to produce finite groups of Lie type (this wasn't complete). What we find is the list of groups Chevalley discovered and 24 sporadic groups gives a complete list.

Recall. If $|G| = p^n$, then $Z(G) \neq \{e\}$.

Proof. Consider the class equation

$$|G| = p^n = 1 + \sum_{\substack{conjugacy \\ classes, g \neq e}} \frac{|G|}{|Z_g|} \tag{2.37}$$

If $Z_g \neq G$ for all $g \neq e$, then $\frac{|G|}{|Z_g|}$ is divisible by p. Then, $p^n = 1 + (div\ by\ p)$, which is a contradiction. Therefore, $Z_g = G$ for some $g \neq e$, and so $g \in Z(G)$. Hence the center is non-trivial. ■

Corollary 2.83. *If $|G| = p$, then G is cyclic, generated by any non-identity element. If $|G| = p^2$, G is abelian.*

Proof. The center of G is not equal to $\{e\}$, so has order p or p^2. If the center has order p^2 then we are done. If not, take $g \in G$ such that $g \notin Z(G)$, and consider Z_g. Since $Z(G) \subset Z_g$, and $g \notin Z(G)$, $|Z_g| > |Z(G)|$. Therefore, it must be that $|Z_g| = p^2$, which implies that $Z_g = G$. However, then by definition $g \in Z(G)$, which contradicts our assumption. Therefore, $Z(G) = G$ and G is abelian, as claimed. ■

Example 2.84 (Non-abelian group of order p^3)**.** Take $G \subset GL_3(\mathbb{Z}/p\mathbb{Z})$ consisting of upper triangular matrices, with ones along the diagonal. The center of G has order p, with the only non-zero upper diagonal element being the top-right corner.

2.6 Restriction of Homomorphisms

Definition 2.85 (Restriction of Subgroups)**.** Let H be a subgroup of a group G. Let K be a second subgroup. The **restriction** of K to H is the intersection $K \cap H$.

Proposition 2.86. *The intersection of two subgroups K and H, $K \cap H$, is a subgroup of H. If K is a normal subgroup of G, then $K \cap H$ is a normal subgroup of H.*

Definition 2.87 (Restriction of a Homomorphism)**.** Suppose that a homomorphism $\phi : G \to G'$ is given, and that H is a subgroup of G. Then we **restrict** ϕ to H, obtaining a homomorphism

$$\phi\Big|_H : H \to G' \tag{2.38}$$

This means we take the same map ϕ but restrict its domain to H. The kernel of $\phi\Big|_H$ is given by

$$\ker \phi\Big|_H = (\ker \phi) \cap H \tag{2.39}$$

Note that $|\phi(H)|$ divides the order of H and G'

Proposition 2.88. *Let $\phi : G \to G'$ be a homomorphism and let H' be a subgroup of G'. Denote the inverse image $\phi^{-1}(H') := \{x \in G : \phi(x) \in H'\}$ by $\widetilde{H}$. Then*

1. *$\widetilde{H}$ is a subgroup of G*
2. *If H' is a normal subgroup of G', then $\widetilde{H}$ is a normal subgroup of G*
3. *$\widetilde{H}$ contains* $\ker(\phi)$
4. *The restriction of ϕ to $\widetilde{H}$ defines a homomorphism $\widetilde{H} \to H'$, whose kernel is* $\ker(\phi)$

2.7 Product of Groups

Definition 2.89 (Product Group)**.** Let G and G' be two groups. The product set $G \times G'$ can be made into a group by component-wise multiplication. That is we define a pair-wise rule

$$(a, a')(b, b') \mapsto (ab, a'b') \tag{2.40}$$

for $a, b \in G$ and $a', b' \in G'$. The order of $G \times G'$ is the product of the orders of G and G' (simple combinatorics)

Remark 2.90. The product group $G \times G'$ is related to the component groups through two inclusion maps into the product, and two projection maps out of the product, defined in the canonical fashion. The inclusion maps are injective and the projection maps are surjective.

Proposition 2.91. *Let H be a group. The homomorphisms $\Phi : H \to G \times G'$ are in bijective correspondence with pairs (ϕ, ϕ') of homomorphism $\phi : H \to G$ and $\phi' : H \to G'$. Moreover, the kernel of Φ is the intersection $(\ker \phi) \cap (\ker \phi')$.*

Proposition 2.92. *Let $r, s \in \mathbb{Z}$ such that $\gcd(r, s) = 1$. Then a cyclic group of order rs is isomorphic to the product of a cyclic group of order r and a cyclic group of order s.*

Definition 2.93 (Product Set)**.** Let A and B be subsets of a group G. Then we denote the set of the products of elements in A and B by

$$AB := \{ab \in G : a \in A, b \in B\} \tag{2.41}$$

Proposition 2.94. *Let H and K be subgroups of G.*

1. *If $H \cap K = \{1\}$, the product map $p : H \times K \to G$ defined by $p(h, k) = hk$ is injective. Its image is HK.*
2. *If either H or K is a normal subgroup of G, then the product sets HK and KH are equal and HK is a subgroup of G*
3. *If H and K are normal, $H \cap K = \{1\}$, and $HK = G$, then G is isomorphic to the product group $H \times K$.*

2.8 Modular Arithmetic

Definition 2.95 (Integers Modulo n)**.** The integers modulo n, where $n \geq 1$, is the quotient set $\mathbb{Z}/n\mathbb{Z}$, or the in other words the set of all cosets of the subgroup $n\mathbb{Z}$. We say that two integers a and b are congruent modulo n, denoted $a \equiv b \mod n$, if and only if $n \mid (a - b)$, or $(a - b) \in n\mathbb{Z}$.

Proposition 2.96 (Equivalence Relation)**.** *The relation defined modulo n is an equivalence relation.*

Proof. Fix $n \geq 1$. For all $a \in \mathbb{Z}$, $a - a = 0 = 0n \in n\mathbb{Z}$, so $a \equiv a \mod n$. Moreover, if $a - b \in n\mathbb{Z}$, then $b - a = -(a - b) \in n\mathbb{Z}$, so $b \equiv a \mod n$ when $a \equiv b \mod n$. If we also have that $b - c \in n\mathbb{Z}$, then $a - c = a - b + b - c \in n\mathbb{Z}$ since $n\mathbb{Z}$ is a subgroup. ■

Question. What do the equivalence classes look like?

Answer. All equivalence classes of $n\mathbb{Z}$ modulo n are of the form $\overline{a} = a + n\mathbb{Z}$. Note that this is the form of a coset, so these equivalence classes are just cosets of the subgroup $n\mathbb{Z}$.

Observation 2.97. We are able to write down all the distinct cosets of $n\mathbb{Z}$ (or equivalence classes modulo n). In fact, these cosets are $n\mathbb{Z}, 1+n\mathbb{Z}, ..., n-1+n\mathbb{Z}$ (shown by the Quotient-Remainder Theorem).

Proof. Suppose $a \in \mathbb{Z}$, and $n \geq 1$. Then by the Quotient Remainder Theorem there exists unique $q, r \in \mathbb{Z}$ so that $a = nq+r$, with $0 \leq r < n$, so $a \equiv r \mod n$ where $r \in \{0, 1, 2, ..., n-1\}$. By the uniqueness of the Quotient Remainder, $a \not\equiv r' \mod n$ for all $r' \in \{0, 1, 2, ..., n-1\}$ for $r' \neq r$. ■

Notation 2.98 (Modulo n Equivalence Classes). For the set of equivalence classes of $n\mathbb{Z}$, we write $\mathbb{Z}/n\mathbb{Z}$.

Definition 2.99 (Modulo n Arithmetic)**.** We define addition on $\mathbb{Z}/n\mathbb{Z}$ by for all $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$, $[a]+[b] = [a+b]$, where a and b are representatives. Moreover, we define multiplication as $[a][b] = [ab]$. (It must we shown that these operations are well-defined).

Proof. Suppose $[a_1] = [a_2]$ and $[b_1] = [b_2]$ are elements of $\mathbb{Z}/n\mathbb{Z}$. Then observe that

$$(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in n\mathbb{Z}$$

Moreover,

$$(a_1 b_1) - (a_2 b_2) = b_1(a_1 - a_2) + a_2(b_1 - b_2) \in n\mathbb{Z}$$

Hence, by definition $[a_1 + b_1] = [a_2 + b_2]$ and $[a_1 b_1] = [a_2 b_2]$, so our operations are well-defined. ■

Observation 2.100 (Group Structure). It follows that $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group, with associativity being inherited from $(\mathbb{Z}, +)$, identity of $[0]$, and inverses for $[a]$ of $[-a]$ or $[n - a]$. In other words, the set of cosets of $n\mathbb{Z}$ form a group (note that $n\mathbb{Z}$ is normal since $\mathbb{Z}$ is abelian).

Observation 2.101 (Cyclic). We observe that $\mathbb{Z}/n\mathbb{Z}$ is also cyclic and of order n, with $\mathbb{Z}/n\mathbb{Z} = \langle [1] \rangle$.

Notation 2.102. When we use + for our group operation, we write $n \cdot g$ for $g + ... + g$ n times (not g^n, which is associated with multiplicative notation).

Observation 2.103 (Distributive Law). Addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ distribute

$$[a]([b] + [c]) = [a][b] + [a][c] \tag{2.42}$$

as inherited from $\mathbb{Z}$.

Example 2.104 (Usefulness)**.** Suppose we want to find the last two digits of 2^{1000}. This is equivalent to finding $2^{1000} \mod 100$. Note that

$$2^{10} \equiv 1024 \equiv 24 \mod 100$$

and

$$2^{20} \equiv (2^{10})^2 \equiv 24^2 \equiv 576 \equiv 76 \mod n$$

THen $76^2 \equiv 76 \mod 100$, and by induction $76^n \equiv 76 \mod 100$. It follows that

$$2^{1000} = (2^{20})^5 0 \equiv 76^{50} \equiv 76 \mod 100$$

Question. Is $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ a group?

Answer. No, but we can create a subset of $\mathbb{Z}/n\mathbb{Z}$ which gives a group under multiplication.

Definition 2.105 (Group of Units)**.** We define the group of units

$$U_n = \{[a] \in \mathbb{Z}/n\mathbb{Z} : \exists [c] \in \mathbb{Z}/n\mathbb{Z},\ s.t.\ [a][c] = [1]\} \tag{2.43}$$

Definition 2.106 (GCD)**.** Suppose m and n are integers, not both zero. Then $\gcd(m, n)$ is the unique positive integer, d, such that $d \mid m, n$ and for all $c \mid m, n$, $c \leq d$.

Lemma 2.107 (Sums of Subgroups of $\mathbb{Z}$)**.** *For any $m, n \in \mathbb{Z}$ (not both zero), $m\mathbb{Z} + n\mathbb{Z} = \gcd(m, n)\mathbb{Z}$.*

Proof. Suppose $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ for some $d \geq 1$. Then since $m, n \in m\mathbb{Z} + n\mathbb{Z}$, d divides m and n. Suppose $e \mid m, n$ where e is a positive integer. Then in particular there exists $r, s \in \mathbb{Z}$ so that $d = mr + ns$, so $e \mid d$. Therefore, $e \leq d$, so $d = \gcd(m, n)$ ■

Proposition 2.108 (Multiplicative Subgroups)**.** $U_n = \{[a] \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$.

Proof. Suppose that $[a] \in \mathbb{Z}/n\mathbb{Z}$. First, suppose $\gcd(a,n) = 1$, so $ar + ns = 1$ for some $r, s \in \mathbb{Z}$. Therefore, $ar - 1 \in n\mathbb{Z}$, so $[ar] = [1]$ and $[a][r] = [1]$, which implies $[a] \in U_n$. Next, suppose $ac - 1 = nb$ for some $c, b \in \mathbb{Z}$. Then $ac + nb = 1$, where $ac + nb \in a\mathbb{Z} + n\mathbb{Z}$, so since $1 \in a\mathbb{Z} + n\mathbb{Z}$, $\gcd(a,n) = 1$. ■

Theorem 2.109 (Order of Prime Multiplicative Subgroups)**.** *In general, for a prime number p and positive integer e, $|U_{p^e}| = p^e - p^{e-1}$ (can be proved combinatorially).*

Definition 2.110 (Reduction Homomorphism)**.** Let $n \geq 1$. Then the **reduction homomorphism** $red : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is given by

$$red(a) = [a]_n \tag{2.44}$$

for all $a \in \mathbb{Z}$. By the fact that addition is well-defined in $\mathbb{Z}/n\mathbb{Z}$ this map is a homomorphism, and since all elements of $\mathbb{Z}/n\mathbb{Z}$ are of the form $[a]_n$ for $a \in \mathbb{Z}$, the map is surjective. Furthermore, suppose $a \in ker(red)$. Then $red(a) = [0]_n$, so $a \in n\mathbb{Z}$. Conversely, if $a' \in n\mathbb{Z}$, then $red(a') = [a']_n = [0]_n$, so $a' \in ker(red)$. Therefore, $n\mathbb{Z} = ker(red)$. Thus all normal subgroups of $\mathbb{Z}$ (which are all subgroups since $\mathbb{Z}$ is abelian) are realized as the kernel of a reduction homomorphism.

2.9 Quotient Groups

Recall (Subgroups of $\mathbb{Z}$). All subgroups of $(\mathbb{Z}, +)$ have the form $n\mathbb{Z}$, $n \geq 0$. We can then associate each $n\mathbb{Z} \leq \mathbb{Z}$ a new group

$$\mathbb{Z}/n\mathbb{Z} \tag{2.45}$$

"$\mathbb{Z}$ mod n" (Gauss). We have $[a] \in \mathbb{Z}/n\mathbb{Z}$, and $[a]$ depends on the remainder of the integer a after division by n. For $a, b \in \mathbb{Z}$, $a \equiv b \mod n$ if and only if n divides $a - b$. Then,

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], ..., [n-1]\} \tag{2.46}$$

Note that $\mathbb{Z}/n\mathbb{Z} = \langle [1] \rangle$. We also have a natural homomorphism, called the canonical projection, $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, given by $a \mapsto [a]$, which is a surjective map with kernel $n\mathbb{Z}$. $\mathbb{Z}/n\mathbb{Z}$ is called the **quotient group** of $\mathbb{Z}$ modulo $n\mathbb{Z}$. Where $[a]$ represents the distinct coset $a + n\mathbb{Z}$ for $n\mathbb{Z}$.

Remark 2.111. $(\mathbb{Z}, +, \cdot)$ has the structure of a ring. Additionally, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ also has the structure of a ring.

Remark 2.112. Disquisitiones Arithmeticae is highly focused on the finite rings $\mathbb{Z}/n\mathbb{Z}$.

Definition 2.113 (Units of a Ring)**.** For a ring R, equipped with $(+, 0)$ (which has a group structure) and $(\times, \cdot)$, then we define the multiplicative group of units for R, we write

$$R^\times = \{r \in R : \text{r has a multiplicative inverse}\} \tag{2.47}$$

2.9.1 Textbook

Definition 2.114 (Product of Subsets of a Group)**.** Given two subsets A and B of a group G, we define the product of A and B as

$$AB := \{ab \in G : a \in A, b \in B\} \tag{2.48}$$

Lemma 2.115. *Let N be a normal subgroup of a group G. Then the product of the cosets aN and bN is again a coset, and is in fact*

$$(aN)(bN) = (ab)N \tag{2.49}$$

Notation 2.116. We notate the set of left cosets of $N \trianglelefteq G$ by G/N or $\overline{G}$ with elements aN or $\overline{a}$.

Theorem 2.117. *With the law of composition given above, $\overline{G} = G/N$ is a group, and the canonical projection $\pi : G \to \overline{G}$ sending $a \mapsto \overline{a}$ is a homomorphism with kernel N.*

Definition 2.118 (Index)**.** The order of G/N is the **index** $[G : N]$ of N in G.

Corollary 2.119. *Every normal subgroup of a group G arises as the kernel of a homomorphism.*

Lemma 2.120. *Let G be a group, and let S be any set with a law of composition. Let $\phi : G \to S$ be a surjective map which has the property $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$. Then S is a group.*

2.9.2 Lecture

Question. When can we put a group structure on the set of all cosets $\{aH\}$ for a subgroup $H \leq G$?

Answer. Cases:

1. Case 1: Suppose $H = ker(f)$, $f : G \to G'$. Then the set of cosets of H are the fibers of the map G, so they can be identified bijectively with the points $\overline{a}$ in the $Im(f) \leq G'$. Recall that the $Im(f)$ is a subgroup of G'. Therefore, since the set of cosets are in bijection with the set of the image, and we have a group structure on the image set, that gives us a group structure for the set of cosets. We transport the structure of the image onto the set, G/H, of cosets. To find how to multiply aH by bH, we find how to multiply $\overline{a}$ and $\overline{b}$. Then

$$\overline{a}\overline{b} = f(a)f(b) = f(ab) = \overline{ab} \tag{2.50}$$

   the group structure we derive for the set of cosets (which are the fibers of the map) is then

$$aH \cdot bH = abH \tag{2.51}$$

   This makes the map $F : G \to G/H$, $a \mapsto aH$, a surjective group homomorphism. We then have that the identity is $eH = H$ and inverses are of the form $(aH)^{-1} = a^{-1}H$.

2. Case 2: Let $H \leq G$ be any subgroup. Let G/H =set of all cosets aH. Try to define a group structure on G/H by setting

$$aH \cdot bH = abH \tag{2.52}$$

   But, is this well-defined? If $aH = a'H$ and $bH = b'H$, is $abH = a'b'H$? Not in general.

Suppose $aHa^{-1} \neq H$, i.e. $aH \neq Ha$, for some $a \in G$. Then observe that

$$(aH)(a^{-1}H) = eH = H$$

and since there exists $h \in H$ so that $aha^{-1} \notin H$. Then take $ah \in aH$ and $a^{-1}e \in a^{-1}H$, so $aha^{-1} \notin H$, so the product is not well-defined.

Question. Why did it work in case 1 and not in case 2?

Answer. The kernel of a homomorphism is normal subgroup.

Case 3: Assume $H \trianglelefteq G$ (normal subgroup), so $aHa^{-1} = H$ for all $a \in G$, so $aH = Ha$ and there exists $h, h' \in H$ so that $ah = h'a$. In this case the naive multiplication law on cosets ($aH \cdot bH = abH$) is well defined and defines a group structure on G/H.

Check: Let $a, b \in G$. Then $aH \cdot bH = \{ahbh' \in G : h, h' \in H\}$. We substitute Ha for aH. Then

$$\begin{aligned}
(aH)(bH) &= (Ha)(bH) && \text{(By normality)} \\
&= H(ab)H && \text{(By associativity)} \\
&= (ab) \cdot H \cdot H && \text{(By normality again)} \\
&= (ab) \cdot H && \text{(Since H is a subgroup)}
\end{aligned}$$

Thus, the product is well-defined, and now can be shown to create a group structure on G/H

Corollary 2.121 (Quotient Group)**.** *If H is a subgroup of G, then one can create a group structure on the set G/H wich aligns with the group structure on G if and only if H is a normal subgroup.*

Corollary 2.122 (Quotient Homomorphism)**.** *If $H \trianglelefteq G$, we get a group structure on G/H and a surjective group homomorphism $f : G \to G/H$ given by $a \mapsto aH$ since*

$$f(a)f(b) = aH \cdot bH = (ab)H = f(ab) \tag{2.53}$$

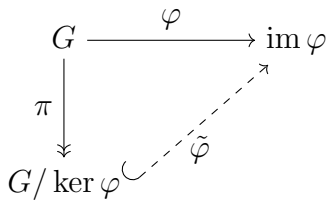
Moreover, we have kernel $f^{-1}(eH) = H$.

Corollary 2.123 (Normal Subgroups)**.** *Every normal subgroup $H \trianglelefteq G$ is the kernel of a group homomorphism.*

Theorem 2.124 (First Group Isomorphism Theorem)**.** *If $f : G \to G'$ is a surjective group homomorphism, with kernel H, then f induces an isomorphism of groups*

$$\overline{f} : G/H \xrightarrow{\sim} G' \tag{2.54}$$

Moreover, $\overline{f}(aH) = f(a)$ (check this is well-defined). Note that the kernel of f is collapsed down to the identity of G/H for the kernel of $\overline{f}$, so it is trivial, and hence $\overline{f}$ is injective. Equivalently, any homomorphism factors through the quotient's canonical homomorphism by the kernel of f.



2.10 Short Exact Sequences of Groups

Definition 2.125 (Short Exact Sequence of Groups)**.** A **short exact sequence of groups** is a diagram of five groups

$$1 \to H \xrightarrow{g} G \xrightarrow{f} G' \to 1 \tag{2.55}$$

where f and f are group homomorphisms, with g being injective, f being surjective, and $g(H) =$ kernel of f. Thus, H is identified with the kernel of f, G' is identified with the image of f, and by the First Isomorphism Theorem, $G' \cong G/H$. (Where $1 = \{e\}$) Note that going left to right, the image of the current map is the kernel of the next.

Note. WARNING: The inputs H and G' do *not* determine the group G.

Example 2.126. Take

$$1 \to A_3 \xrightarrow{inclusion} S_3 \xrightarrow{sign} \langle \pm 1 \rangle \to 1 \tag{2.56}$$

and

$$1 \to \mathbb{Z}/3\mathbb{Z} \cong 2\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} \xrightarrow{a \mapsto a \mod 2} \mathbb{Z}/2\mathbb{Z} \to 1 \tag{2.57}$$

Then, since all groups of prime order are cyclic, $A_3 \cong \mathbb{Z}/3\mathbb{Z}$, and $\langle \pm 1 \rangle \cong \mathbb{Z}/2\mathbb{Z}$. However, S_3 is non-abelian while $\mathbb{Z}/6\mathbb{Z}$ is an abelian group of order six.

Observation 2.127. Suppose $H \trianglelefteq G$, and G/H is the quotient group (set of cosets of H), which comes with a surjective canonical homomorphism $f : G \twoheadrightarrow G/H$ by $a \mapsto aH$, with kernel H.

1. Further suppose $H \trianglelefteq K \leq G$. Then first, H is normal in K since H is normal in G. Therefore, we may construct the quotient group $K/H \subset G/H$. Moreover, it is a subgroup of G/H. In other words, for all $aH, bH \in K/H$, $abH \in K/H$, since if $a, b \in K$, $ab \in K$. Therefore, the quotient group K/H is stable under multiplication because K is stable under multiplication.

2. Conversely, any subgroup of G containing H corresponds to a subgroup of G/H in this manner. In other words, for all subgroups $A = \{aH\}$ of G/H, $K = \bigcup_{aH \in A} aH = f^{-1}(A)$ is a subgroup of G containing H.

3. In other words, there is a bijection between the collection of subgroups of G containing H and the subgroups of G/H.

Example 2.128. Take $G = \mathbb{Z}$, and let p be a prime number. Consider $H = p\mathbb{Z}$. Claim: If $\mathbb{Z} \geq K \geq p\mathbb{Z}$ is a subgroup, then either $K = \mathbb{Z}$ or $K = p\mathbb{Z}$.

Proof. Such a K gives a subgroup of the cyclic quotient group $\mathbb{Z}/p\mathbb{Z}$. So, this gives either $[0]$ or $\mathbb{Z}/p\mathbb{Z}$. If it gives $[0]$, then $K = \bigcup[0] = p\mathbb{Z}$. Otherwise, if it gives $\mathbb{Z}/p\mathbb{Z}$, then the union of the cosets is all of $\mathbb{Z}$, so $K = \mathbb{Z}$. ■

Therefore, H is a **maximal** subgroup of G.

2.11 Actions of a Group on Itself

2.11.1 Textbook

Definition 2.129 (Permutation Representation)**.** Note that by definition the symmetric group on n letters, S_n, acts on the set $\{1, 2, ..., n\}$. A **permutation representation** of a group G is a homomorphism

$$\phi : G \to S_n \tag{2.58}$$

Given such a representation we obtain an action of G on $S = \{1, ..., n\}$ by letting $m_g = \phi(g)$ for all $g \in G$. In fact, actions of a group G on $\{1, ..., n\}$ correspond bijectively with permutation representations.

Proposition 2.130. *Suppose G is a group and S is a set. Then let $Perm(S)$ be the set of permutations on S. Then there is a bijective correspondance*

$$\Psi : \begin{bmatrix} Operations \\ of\ G\ on\ S \end{bmatrix} \longleftrightarrow \begin{bmatrix} homomorphisms \\ G \to Perm(S) \end{bmatrix} \tag{2.59}$$

defined in this way: Given a group action, we define $\phi : G \to Perm(S)$ by the rule $\phi(g) = m_g$, where m_g is the action of g on elements of S via left multiplication.

Proof. First, we shall provd that every element of G acts on S bijectively. Suppose $g \in G$, and consider te action $m_g : S \to S$. Note that by the associativity of group actions, $m_g \circ m_{g^{-1}}(s) = (gg^{-1})(s) = s$ and $m_{g^{-1}} \circ m_g(s) = (g^{-1}g)(s) = s$. Thus, m_g is a bijective map on S, so it is a permutation of S. Therefore, since this is valid for all group actions, all maps $\phi : G \to Perm(S)$ is well-defined. Moreover, given a fixed group action and associated map ϕ, we see that for all $g, g' \in G$ and for all $s \in S$,

$$\phi(gg')(s) = m_{gg'}(s) = (gg').s = g.(g'.s) = m_g(m_{g'}(s)) = \phi(g)(\phi(g')(s))$$

Thus, $\phi(gg') = \phi(g)\phi(g')$, and ϕ is a homomorphism as claimed. Therefore, the map described above is well defined. Now, suppose $\phi : G \to Perm(S)$ is a homomorphism. Define a group action of G on S by declaring $g.s = \phi(g)(s)$. Since ϕ is a homomorphism, $\phi(e)$ is the identity map. Thus, for all $s \in S$, $e.s = \phi(e)(s) = s$. Furthermore, for all $g, g' \in G$ and $s \in S$, $(gg').s = \phi(gg')(s) = \phi(g) \circ \phi(g')(s) = g.(g'.s)$. Therefore, it is a well defined group action, and $\Psi(\text{group action}) = \phi$. Thus, Ψ is surjective. Next, suppose G_1, G_2 are group actions such that $\Psi(G_1) = \Psi(G_2)$. Then $\phi_1 = \phi_2$, so for all $g \in G$, $\phi_1(g) = \phi_2(g)$. Finally, this implies that for all $g \in G$ and $s \in S$, $g._1 s = g._2 s$. Therefore, every element of G acts in the same way on S when using the G_1 and G_2 group action structures. Consequently, $G_1 = G_2$ and Ψ is a bijective map, as claimed. ■

Definition 2.131 (Faithful)**.** If the homomorphism $\phi : G \to Perm(S)$ is injective, then the corresponding group action is said to be **faithful**. Hence, to be faithful, the action must have the property that $m_g \neq$ identity unless $g = 1$, or

$$\forall s \in S, gs = s \implies g = 1 \tag{2.60}$$

Definition 2.132 (Group Action on Itself)**.** A group action of a group G on itself is equivalent to the group action on a set, where now the set is the group. Thus, it is a map

$$G \times G \to G \tag{2.61}$$

such that for all $g, g', g'' \in G$, $e(g) = g$, and $(g'g'')(g) = g'(g''(g))$.

Example 2.133. Suppose G is a group. A common group action of G on itself is Left multiplication: $g.g' \mapsto gg'$. Note that this is evidently a transitive operation on G since $O_e = G$. Additionally, for any $g \in G$, $G_g = \{e\}$. Thus, the action is faithful and the homomorphism

$$G \to Perm(S) \tag{2.62}$$

given by $g \mapsto m_g =$ left multiplication by g.

Theorem 2.134 (Cayley's Theorem)**.** *Every finite group G is isomorphic to a subgroup of the permutation group. If G is of order n, then it is isomorphic to a subgroup of the symmetry group S_n.*

Proof. Since the operation by left multiplication is faithful, G is isomorphic to its image $Perm(G)$. If G is of order n, then $Perm(G)$ is isomorphic to S_n. (??) ■

Example 2.135 (Conjugation)**.** Suppose G is a group. Another common group action of G on itself is **conjugation**, so the map $G \times G \to G$ is defined by

$$(g, x) \mapsto gxg^{-1} \tag{2.63}$$

Obviously any element conjugated by the identity is itself. Moreover, a map defined by conjugation is a homomorphism so the action is associative.

Definition 2.136 (Centralizer)**.** The stabilizer of an element $x \in G$ under the action of conjugation is called the **centralizer** of x, and is denoted by $Z(x)$:

$$Z(x) := \{g \in G : gxg^{-1} = x\} \tag{2.64}$$

Thus, the centralizer of x is the set of all elements which commute with x. Note that $x \in Z(x)$ since x commutes with itself.

Definition 2.137 (Class Equation)**.** The orbit of x for the action of conjugation is called the **conjugacy class** of x. It consists of all conjugate elements gxg^{-1}. We often denote the conjugacy class by

$$C_x = \{x' \in G : \exists g \in G, x' = gxg^{-1}\} \tag{2.65}$$

By the counting formula we have that

$$|G| = |C_x||Z(x)| \tag{2.66}$$

Definition 2.138 (Class Equation)**.** Note that since conjugacy classes are orbits for a group action, G is partitioned by the conjugacy classes. Then for a finite group G we have the **Class Equation**

$$|G| = \sum_{\substack{conjugacy \\ classes\ C}} |C| \tag{2.67}$$

Observation 2.139. Note that on the right of the class equation we have orders of conjugacy classes, or orbits, which divide the group. Additionally, the conjugacy class of the identity is simply $\{e\}$, so at least one element on the right side is 1.

Recall. Recall that the center of a group G is the set Z of elements in G which commute with every element in G. Thus, the conjugacy class of any element in the center is a set consisting of only that element.

Proposition 2.140. *An element x is in the center of the group G if and only if its centralizer $Z(x)$ is the entire group.*

Proposition 2.141. *Suppose G is a* ***p-group****, so $|G| = p^k$, where p is prime, and $k \in \mathbb{N}$. Then the center of G has order > 1.*

Proof. Suppose G is a p-group, so $|G| = p^n$ for some $n \in \mathbb{N}$. Then every conjugacy class has order which divides p^n, so they are all powers of p. Note that $|C_1| = 1$. For the sake of contradiction suppose that no other conjugacy class of order 1 exists. Then

$$p^n = 1 + \sum (powers\ of\ p) \tag{2.68}$$

However, this is impossibly unless $n = 0$. Therefore, the center of G has order > 1, as desired. ■

Proposition 2.142. *Let G be a p-group, and let S be a finite set on which G acts. Assume that the order of S is not divisible by p. Then there is a fixed point for the action G on S, that is, an element $s \in S$ is stabilized by every element of G, so $Z_s = G$.*

Proposition 2.143. *Every group of order p^2 is abelian.*

Proof. Let G be a group of order p^2. We shall show that for all $x \in G$, the centralizer $Z(x)$ is the whole group. Let $x \in G$. If x is in the center Z, then $Z(x) = G$ as claimed. If $x \notin Z$, then $Z(x)$ is strictly larger than Z since it contains Z and x. Now, the orders of Z and $Z(x)$ divide $|G| = p^2$, and from a previous proposition we know that $|Z|$ is at least p. The only possibility is then $|Z(x)| = p^2$. Hence, $Z(x) = G$, and x is in the center, which is a contradiction. Therefore, $x \in Z$ for all $x \in G$, so $Z = G$ and G is correspondingly abelian. ■

Corollary 2.144. *Every group of order p^2 is one of the following types:*

1. *a cyclic group of order p^2*
2. *a product of two cyclic groups of order p*

Proof. Since the order of an element divides p^2, there are two cases two consider

Case 1: G contains an element of order p^2, then G is cyclic.

Case 2: Every element $x \in G$ except the identity is of order p. Let $x, y \in G$, $x, y \neq 1$, and let H_1 and H_2 be cyclic subgroups generated by x and y respectively. We may choose y so that it is not a power of x. Then since $y \notin H_1$, $H_1 \cap H_2$ is smaller than H_2, which is of order p. Thus, $H_1 \cap H_2 = \{1\}$. Also, since G is abelian, the subgroups are normal. Since $y \notin H_1$, the group H_1H_2 is strictly larger than H_2, and its order divides p^2. Thus, $H_1H_2 = G$. By a previous result, it follows that $G \cong H_1 \times H_2$

■

Recall. Recall that the order of the icosahedral group is 60. Each of the twenty vertices have a stabilizer of order 3, with opposite vertices sharing the same stabilizer, giving 10 subgroups of order 3, and all of these subgroups only have the identity in common. The twelve faces each have stabilizers of order 5, and since a stabilizer is shared between opposite pairs of faces, we have 6 subgroups of order 5. Finally, there are 15 stabilizers of edges, with elements of order 2. Then, the 1 identity element of order 1, giving the class equation

$$60 = 1 + 15 + 20 + 24 \tag{2.69}$$

Moreover, this equation is split up by conjugacy classes as

$$60 = 1 + 15 + 20 + 12 + 12 \tag{2.70}$$

Recall. Recall that is a group G acts on a set S, and for $s, s' \in S$, $s' \in O_s$, and $s' = gs$ for $g \in G$, the stabilizers of s and s' are conjugate, and in particular $G_{s'} = gG_sg^{-1}$.

Theorem 2.145. *The icosahedral group I has no proper normal subgroups.*

Proof. A proper normal subgroup of I has order which is a proper divisor of 60. Moreover, the order of the subgroup is the sum of some of the terms $1, 15, 20, 12, 12$, including 1. No such integer exists, so no proper normal subgroup of I exists. Therefore, I is simple. ■

Lemma 2.146. .

1. *If a normal subgroup N of a group G contains an element x, then it contains the conjugacy class C_x of x in G. In other words, a normal subgroup is a union of conjugacy classes.*

2. *The order of a normal subgroup N of G is the sum of the orders of the conjugacy classes of which it contains.*

Proof. Suppose that G is a group, and N is a normal subgroup of G. Let $x \in N$. Then given an element $y \in C_x$, y is of the form $y = gxg^{-1}$ for some $g \in G$. Then, since N is normal, $y = gxg^{-1} \in N$, which implies that $C_x \subset N$. Then, since conjugacy is an equivalence relation, the distinct conjugacy classes of elements in N partition the group, so

$$|N| = \sum_{\substack{conjugacy \\ classes\ C}} |C| \tag{2.71}$$

■

Theorem 2.147. *The icosahedral group is isomorphic to the alternating group A_5. (we have I operate on inscribed cubes of the dodecahedron)*

2.11.2 Lecture

Recall (Class equation Results). Any G of order p^2 is abelian. (from before, any G of order p is cyclic ($\cong \mathbb{Z}/p\mathbb{Z}$)).

Question. What about G of order pq (ex: S_3 of order 6), or p^3?

Proposition 2.148. *If G is a group of order p^2, then there are only two such G up to isomorphism:*

1. *There is an element of G of order p^2. Then $G \cong \mathbb{Z}/p^2\mathbb{Z}$ with the map*

$$g \mapsto 1(\mod p^2), g^a \mapsto a(\mod p^2) \tag{2.72}$$

2. *There is no element of G of order p^2. Thus, every $g \neq e$ has order p. Then, the field $\mathbb{Z}/p\mathbb{Z}$ acts on the group G by*

$$a \cdot g = g^a = g + g + ... + g\ (a\ times) \tag{2.73}$$

where $a \in \mathbb{Z}/p\mathbb{Z}$, and $0 \cdot g = e = 0$ in the additive group. In this case, G is a vector space over $\mathbb{Z}/p\mathbb{Z}$, it has order p^2, so it has dimension 2, and it is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$ by a choice of a basis. In sum, if every element has order p, then you obtain an action of the field $\mathbb{Z}/p\mathbb{Z}$ on the group, which turns it into 2-dimensional a vector space.

Definition 2.149 (Elementary Abelian P-group)**.** For $n \geq 1$, we have the group $G = (\mathbb{Z}/p\mathbb{Z})^n$, an n-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$, with order p^n, and every element $g \neq e$ of order p. This is called an **elementary abelian p-grop**.

2.12 Operations on Subsets

2.12.1 Textbook

Definition 2.150 (Action on Subsets)**.** Suppose G is a group that acts on a set S. Let $U \subset S$ be a subset of S. Then

$$gU = \{g.u : u \in U\} \tag{2.74}$$

is another subset of S. Then G operates on the set of subsets of S. If we wish we can consider the action on subsets of a given order, since multiplication by $g \in G$ permutes S, so the subsets U and gU will be of the same order.

Example 2.151. Let O be the octahedral group of 24 rotations of a cube, and let S be the set of vertices of the cube. Consider the operation O on subsets of order 2 of S. There are 28 such subsets, and they form three orbits for the group

1. {pairs of vertices on an edge}
2. {pairs which are opposite on a face of the cube}
3. {pairs which are opposite on the cube}

These orbits have orders of 12, 12 and 4 respectively.

Definition 2.152 (Stabilizer of a Subset)**.** The stabilizer of a subset U is the set of group elements $g \in G$ such that $gU = U$. However, note that the equality does not mean that g leaves the points of U fixed, but rather that g permutes the elements within U, that is $g.u \in U$ whenever $u \in U$.

Proposition 2.153. *Let H be a group which operates on a set S, and let U be a subset of S. Then H stabilizes U if and only if U is the union of $H-$orbits.*

Proof. If H stabilizes U, then the $H-orbit$ of every element in U must be contained in U. Thus, U is the union of the $H-orbits$ of its elements. Conversely, if U is the union of $H-orbits$, then for each $u \in U$, $O_u \in U$, so H stabilizes U by definition. ■

Proposition 2.154. *Let U be a subset of a group G. The order of the stabilizer $Stab(U)$ of U for the operation of left-multiplication divides the order of U.*

Proof. Let H denote the stabilizer of U. The previous proposition tells us that U is a union of $H-orbits$ for action of H on G. These orbits are right cosets of the form Hg for all $g \in G$. Thus, U is the union of right cosets. Hence, the order of U is a multiple of $|H|$. ■

Remark 2.155. Since the stabilizer is a subgroup of G, $|Stab(U)|$ divides $|G|$ and $|U|$, so if $|G|$ and $|U|$ are relatively prime, then $|Stab(U)|$ is the trivial subgroup, $\{e\}$.

Definition 2.156 (Conjugate Subgroup)**.** For a subgroup $H \subset G$ of a group G, the orbit under conjugation of H is the set of **conjugate subgroups**

$$\{gHg^{-1} : g \in G\} \tag{2.75}$$

Consequently, the subgroup H is normal if and only if its orbit under conjugation consists of H alone, that is, $gHg^{-1} = H$ for all $g \in G$.

Definition 2.157 (Normalizer)**.** The stabilizer of a subgroup H under the action of conjugation is known as the **normalizer** of H, and is denoted by

$$N(H) := \{g \in G : gHg^{-1} = H\} \tag{2.76}$$

Theorem 2.158 (Counting Formula)**.** *The* ***counting formula*** *for conjugation on subgroups is*

$$|G| = |N(H)| \cdot |\{conjugate\ subgroups\}| \tag{2.77}$$

Thus, the number of conjugate subgroups is equal to the index $[G : N(H)]$.

Remark 2.159. Note that the normalizer always contains the subgroup

$$H \subset N(H) \tag{2.78}$$

because $hHh^{-1} = H$ when $h \in H$. Thus, by Lagrange's Theorem, $|H|$ divides $|N(H)|$, and $|N(H)|$ divides $|G|$.

Remark 2.160. The definition of a normalizer $N(H)$ implies that $H \trianglelefteq N(H)$, and in fact, $N(H)$ is the largest subgroup of G containing H as a normal subgroup. In particular, $N(H) = G$ if and only if H is a normal subgroup of G.

2.13 The Sylow Theorems

2.13.1 Textbook

In this section we consider a group G of order n. Let p be a prime which divides n, and write

$$n = p^e m \tag{2.79}$$

where $e \geq 1$, and $\gcd(p, m) = 1$ for some integer m.

Theorem 2.161 (First Sylow Theorem)**.** *There is a subgroup of G whose order is p^e, which we call a* ***Sylow p-subgroup****.*

Corollary 2.162. *If a prime p divides the order of a finite group G, then G contains an element of order p.*

Proof. Let H be a supgroup of order p^e, and let x be an element of H different from 1. The order of x divides p^e, so it is p^r with $0 < r \leq e$. Then $x^{p^{r-1}}$ has order p. ■

Corollary 2.163. *There are exactly two isomorphism classes of groups of order* 6*. They are classes of the cyclic group C_6 and of the dihedral group D_6*

Proof. Let x be an element of order 3 and y an element of order 2 in G. It can be seen that the six products $x^i y^j$, $0 \leq i \leq 3, 0 \leq j \leq 2$ are distinct elements of G. For, we can write $x^i y^j = x^r y^s$ in the form $x^{i-r} = y^{s-j}$. Every power of x except the identity has order 3, and every power of y except the identity has order 2. Thus, $x^{i-r} = y^{s-j} = 1$, which shows that $r = i$ and $j = s$. Since G has order 6, the six elements we have shown are distinct run through the whole group. Moreover, yx must be one of these products, and in particular, $yx = xy$ or $yx = x^2 y$ holds in G. Either of these relations along with $x^3 = 1$ and $y^2 = 1$ provides a valid multiplication table for the group. Therefore, there are at most two isomorphism classes for the group. C_6 and D_6 are the only such groups. ■

Definition 2.164 (Sylow p-subgroups)**.** Let G be a group of order $n = p^e m$, where p is a prime, $\gcd(m, p) = 1$, and $e \geq 1$. The subgroups H an G of order p^e are called **Sylow p-subgroups** of G, or often just **Sylow subgroups**.

Theorem 2.165 (Second Sylow Theorem)**.** *Let K be a subgroup of G whose order is divisible by p, and let H be a Sylow p-subgroup of G. There is a conjugate subgroup $H' = gHg^{-1}$ such that $K \cap H'$ is a Sylow subgroup of K.*

Corollary 2.166. .

1. *If K is any subgroup of G which is a p-group, then K is contained in a Sylow p-subgroup of G*
2. *The Sylow p-subgroups are all conjugate.*

Proof. First, note that conjugation is an automorphism of subgroups, so the conjugate of a Sylow p-subgroup is another Sylow p-subgroup. First, note that the Sylow subgroup of the p-group K is K itself. Thus, if H is a Sylow subgroup and K is a p-group, there is a conjugate H' such that $K \cap H' = K$, which is to say that H' contains K (by the Second Sylow Theorem). For the second part, let K and H be Sylow subgroups. Then there is a conjugate H' of H such that $H' \cap K$ is a Sylow subgroup of K. Then since K is a Sylow subgroup, $H' \cap K = K$, and hence $K \subset H'$. Moreover, since $|K| = |H'|$ as they are both Sylow subgroups, $K = H'$. Thus, K and H are conjugate. ■

Theorem 2.167 (Third Sylow Theorem)**.** *Let $|G| = n$, and $n = p^e m$ as initially stated. Let s be the number of Sylow p-subgroups. Then s divides m and is congruent to 1 modulo p: $s \mid m$, and $s = ap + 1$ for some $a \geq 0$.*

Proposition 2.168. .

1. *Every group of order 15 is cyclic.*
2. *There are two isomorphism classes of groups of order 21: the class of the cyclic group C_{21}, and the class of the group G having two generators x, y which satisfy the relation $x^7 = y^3 = 1$, $yx = x^2y$.*

Proof.

1. Let G be a group of order 15. By the Third Sylow Theorem, the number Sylow 3-subgroups of G divides 5 and is congruent to 1 modulo 3. The only such integer is 1. Therefore, there is only one Sylow 3-subgroup H, and thus the conjugacy class of H must be of order 1, so H is normal. Similarly, there is one Sylow 5-subgroup of G, which we shall denote by K. K must also be a normal subgroup of G. Then, since $K \cap H$ is a subgroup of H and K, its order divides 5 and 3 so $K \cap H = \{e\}$. Also, KH is a subgroup of order > 5, so $KH = G$. By a previous result, G is isomorphic to the product group $H \times K$. Thus, every group of order 15 is isomorphic to the direct product of two cyclic groups of orders 3 and 5. In particular, since C_{15} is of order 15, it is also isomorphic to the product, so every group of order 15 is cyclic.

2. Let G be a group of order 21. Then, the Third Sylow Theorem shows that the single Sylow 7-subgroup K must be normal. But, we have the possibility there are 7 Sylow 3-subgroups of G. Let x denote a generator for K, and y a generator for one of the Sylow 3-subgroups H. Then $x^7 = y^3 = 1$, and since K is normal, $yxy^{-1} = x^i$ for some $i < 7$. Using the fact that $y^3 = 1$, we see that

$$x = y^3xy^{-3} = x^{i^3} \tag{2.80}$$

Therefore, i^3 is congruent to 1 modulo 7. This implies that i is either 1, 2, or 4.

Case 1: $yxy^{-1} = x$. Then the group is abelian and by a previous result it is congruent to a direct product of cyclic groups of orders 3 and 7. Such a group is cyclic.

Case 2: $yxy^{-1} = x^2$. The multiplication of G can be carries out using the rules $x^7 = y^3 = 1$, $yx = x^2y$, to reduce every product of elements x and y to one of the form $x^i y^j$, $0 \leq i < 7, 0 \leq j < 3$. (prove existence)

Case 3: $yxy^{-1} = x^4$. In this case we replace y by y^2, which is also a generator for H, to reduce to the previous case: $y^2xy^{-2} = x^2$. Thus, there are two isomorphism classes of the group of order 21 as claimed.

■

Remark 2.169 (Proofs of the Sylow Theorems). We shall now prove the Sylow Theorems.

First Sylow Theorem. We let $\mathcal{J}$ be the set of all subsets of G of order p^e. We shall show that one of these subgroups has a stabilizer of order p^e. The stabilizer will be the required subgroup.

Lemma 2.170. *The number of subsets of order p^e in a set of $n = p^e m$ elements, with $\gcd(p, m) = 1$, is the binomial coefficient*

$$N = \binom{n}{p^e} = \frac{n(n-1)...(n-k)...(n-p^e+1)}{p^e(p^e-1)...(p^e-k)...1} \tag{2.81}$$

Moreover, $\gcd(N, p) = 1$.

Proof of Lemma. Is is a standard fact that the number of subsets of a set of order p^e is this binomial coefficient. To see that N is not divisible by p, note that every time p divides a term $(n-k)$ in the numerator of N, it also divides the term (p^e-k) in the denominator exactly the same number of times: If we write k in the form $k = p^i l$, where $\gcd(p, l) = 1$, then $i < e$. Therefore, $(n-k)$ and (p^e-k) are both divisible by p^i but not divisible by p^{i+1}, satisfying the claim. ■

We decompose $\mathcal{J}$ into orbits for the action of left multiplication, obtaining the formula

$$N = |\mathcal{J}| = \sum_{orbits\ O} |O| \tag{2.82}$$

Since p does not divide N, some orbit has an order not divisible by p, say the orbit of the subset U. Then, G acts transitively on the orbit O_U, so by the Counting Formula

$$|Stab(U)| \cdot |O_U| = |G| = p^e m \tag{2.83}$$

Since $|O_U|$ is not divisible by p, we have that p^e divides $|Stab(U)|$, so $p^e \leq |Stab(U)|$. Moreover, if $g \in Stab(U)$, then $gU = U$. This implies that U is the union of right cosets of $Stab(U)$. In particular, $|Stab(U)| \leq |U| = p^e$, so we conclude that $|Stab(U)| = p^e$, completing the proof. ■

Second Sylow Theorem. We are given a subgroup K of order divisible by p, and a Sylow subgroup H of G, and we are to show that for some conjugate H' of H, the intersection $K \cap H'$ is a Sylow subgroup of K.

Let S denote the set of left cosets G/H. Note that G operates transitively on S, so the set forms a single orbit, and that H is the stabilizer of the element $s = eH$ of S. Thus, the stabilizer of as is the conjugate subgroup aHa^{-1}.

We restrict the group action of G to K, and decompose S into $K - orbits$. Since H is a Sylow subgroup, the order of S is prime to p. Thus, there must exist some $K - orbit\ O$ whose order is prime to p. Say that O is the $K - orbit$ of the element as. Let H' denote the stabilizer aHa^{-1} of as for the operation of G. Then, the stabilizer of as for the restricted action of K is $H' \cap K$, and the index $[K : H' \cap K]$ is $|O|$, which is prime to p. Also, since it is a conjugate of H, H' is a p-group. Therefore, $H' \cap K$ is a p-group. Thus, $H' \cap K$ is a p-group of the largest order in K, so $H' \cap K$ is a Sylow subgroup of K. ■

Third Sylow Theorem. By a corollary of the Second Sylow Theorem above, we have that the Sylow subgroups of G are all conjugate to one another. In particular, they are all conjugate to a given one, say H. Thus, the orbit of H by conjugation by G is the conjugacy class of all Sylow subgroups, and $s = [G : N(H)]$ is the number of Sylow subgroups, where $N(H)$ is the normalizer of H in G under conjugation. Since $H \subset N(H)$, H is a subgroup of $N(H)$ and p^e divides $|N(H)|$ Moreover, note that $[G : H] = m$, and $[G : N(H)] = \frac{[G:H]}{k}$ for some $k > 0$, so in particular, $s = [G : N(H)]$ divides m. To show $s \equiv 1(\mod p)$, we decompose the set $\{H_1, H_2, ..., H_s\}$ of Sylow subgroups into orbits for the operation of conjugation by $H = H_1$. An orbit consists of a single group H_i if and only if H is contained in the normalizer $N(H_i)$ of H_i. If so, then H and H_i are both Sylow subgroups of $N(H_i)$, and H_i is normal in $N(H_i)$. Then, by a previous corollary to the Second Sylow Theorem, H and H_i are conjugate in $N(H_i)$, but H_i is only conjugate with itself in $N(H_i)$. Therefore, $H = H_i$. Thus, H is the only Sylow subgroup with $H - orbit$ of order 1. The other orbits have orders divisible by p since their orbits divide $|H|$, by the Counting Formula. Thus, $s \equiv 1(\mod p)$, completing the proof. ■

2.13.2 Lecture

Definition 2.171 (Operation of a Group on itself by Conjugation)**.** G acts on $G = S$ by conjugation

$$g(s) \mapsto gsg^{-1} \tag{2.84}$$

The orbit O_s is called the **conjugacy class** of the element s, and the stabilizer G_s is called the **centralizer** of s, written usually as $Z_s := \{g \in G : gsg^{-1} = s\}$

Definition 2.172 (Action on Subgroups)**.** G also acts on the set $\mathcal{H}$ of all subgroups of G, by conjugation. In particular, for all $g \in G$ and $H \in \mathcal{H}$, $g(H) = gHg^{-1} = \{ghg^{-1} : h \in H$

another element of $\mathcal{H}$. The orbit of H, O_H = the set of subgroups conjugate to H, and the stabilizer of H is the subgroup $G_H = \{g \in G : gHg^{-1}\} = N(H) \subset G$, which we call the **normalizer** of H. Note that $N(H)$ is a subgroup such that $H \trianglelefteq N(H) \subset G$. Moreover, $N(H)$ is the largest subgroup of G containing H in which H is normal.

Remark 2.173. For a group G we have so far had the notion of G acting on sets, G acting on the set of its own elements, and now G acting on the set of subgroups of G.

Example 2.174 (Examples of Normalizers)**.** Consider S_3 and the normal subgroup $A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$, so $N(A_3) = S_3$. On the other hand $\{e, (1\ 2)\} \subset S_3$ since (1 2) is the only element of order two, not only must a normalizer normalize (1 2) (keep it in the subgroup) it must also centralize it (not change it - i.e. commute with it). However, there is no such element except for the elements already in $\{e, (1\ 2)\}$, so $N(\{e, (1\ 2)\}) = \{e, (1\ 2)\}$.

Let us consider the subgroup

$$H = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \right\} \subset G = GL_2(F) \tag{2.85}$$

Then the normalizer of H is

$$N(H) = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \right\} \tag{2.86}$$

Remark 2.175 (Stabilizers). Recall that if we have G acting transitively on a set S, and G_s is the stabilizer of some element $s \in S$, then G_s is conjugate to the stabilizer $G_{s'}$ for all $s' \in S$. Thus, the stabilizers generate a conjugacy class of subgroups.

Remark 2.176 (Normalizer WARNING). A normalizer does not necessarily centralize the elements of the set it normalizes (i.e. fixes them). All it guarantees is that for any element g in the normalizer G_H of a subgroup H, $ghg^{-1} \in H$ for all $h \in H$.

Remark 2.177 (FACT). If $N = p^m n$, where p is prime, then

$$\binom{N}{p^m} = \frac{N!}{p^m(N-p^m)!} = \frac{(p^m n)!}{p^m(p^m(n-1))!} = \frac{N(N-1)...(N-p^m+1)}{p^m(p^m-1)...1} \tag{2.87}$$

is prime to p. Since the power of p dividing the numemrator = the power of p dividing the denominator (Order of p). In general, the power of of p dividing $(N-k)$ is equal to the power of p dividing $(p^m - k)$, with $k < p^m$ (i.e. $ord_p(N-k) = ord_p(p^m-k)$). This follows from the fact that the same power of p divides N and p^m, so all we need to look at is the k which is the same for both.

Theorem 2.178 (Sylow Theorem)**.** *Assume G is a finite group of order $N = p^m \cdot n$, where p is prime, and $\gcd(n,p) = 1$, so p^m is the highest power of p which divides the group. Then,*

1. *There is a subgroup H of G of order p^m (**Sylow p-subgroups**)*
2. *If K is a subgroup (p-group) of order p^a ($a \leq m$), then K is contained in a conjugate of H. In particular, any two p-Sylow subgroups H and H' are conjugate (the case when $a = m$). $\implies$ thus the Sylow p-subgroups form a conjugacy class of subgroups.*
3. *The number l of Sylow p-subgroups of G (in this single conjugacy class) divides n, and satisfies*

$$l \equiv 1(\mod p) \tag{2.88}$$

Part 1. Let G act on the set S of all subsets of G which have order p^m by translation ($J \subset G$ goes to $gJ \subset G$ by left translation). Moreover, $|S| = \binom{N}{p^m}$, which from above is prime to p. We will realize H as a stabilizer G_s for this action. We break S into $G - orbits$, so

$$|S| = |O_{s_1}| + ... + |O_{s_r}| = \frac{|G|}{|G_{s_1}|} + ... + \frac{|G|}{|G_{s_n}|} \tag{2.89}$$

where G acts transitively on each orbit. Since $|S|$ is prime to p, there is at least one orbit of order prime to p. Say $|O_s|$ is prime to p, $s \in \{s_1, ..., s_n\}$. Since $|O_s| = \frac{p^m n}{|G_s|}$ is prime to p, we must have that p^m divides $|G_s|$. I claim that $|G_s| \leq p^m$. s corresponds to a subset $J \subset G$, and we have an element of the stabilizer of that subset. If $g \in G_s$, then $gJ = J$. This implies that J is a union of left cosets of G_s. In particular ,$|G_s| \leq |J| = p^m$. In fact, J has stabilizer of order p^m if and only if $J = H$ is a Sylow p-subgroup, in which case $J = G_s = H$. ■

Part 2. Suppose H is the Sylow p-subgroup found in part 1. Suppose G acts transitively on $S = G/H$, which has order n prime to p. The stabilizers of any point $s = sH$ in S, G_s, are the conjugates of H. Let K be another p-subgroup, and have K act by the restriction of the G action on S. Since the order of S is of order prime to p, there must be an orbit sH of order prime to p. It follows that $|K|/|stabilizer|$ is prime to p. Note that the order of K is a power of p, so the only option is that the order of the stabilizer is equal to the order of K. Thus, there must be an orbit fixed by K. Recall that $Stab_{sH} = K \cap G_s = K \cap sHs^{-1}$, and since the orders are equal it follows that $K \subset sHs^{-1}$. This shows that our p-group must be contained in some conjugate of our Sylow p subgroup. ■

Part 3. We claim the number of Sylow subgroups, l, is $|G|/|N(H)|$, where H is a Sylow p-subgroup, because G acts transitively on the set of Sylow p-subgroups by conjugation (by part 2), and the stabilizer of H is what we call $N(H)$. Moreover, since $H \subset N(H)$, so $|N(H)|$ is divisible by p^m, so l divides what's left, which is $n = N/p^m$. Now, restrict the action of conjugation on the l Sylows to the subgroup H. The orbit of H has 1-element, and all other orbits have p^a elements, with $a \geq 1$. Since $|H| = p^m$, the size of any orbit must divide this. For the sake of contradiction, suppose H' is another Sylow p in an orbit of size 1, then H normalizes H'. Thus H and H' are both subgroups of $N(H')$. Therefore, since we also have that $N(H') \subset G$, $|N(H')| = p^m n'$, where n' divides n. Moreover, H and H' are Sylow p-subgroups of $N(H')$. Then, by part 2, they are conjugate in $N(H')$. But, in $N(H')$ the only thing conjugate to H' is H'. Thus, we conclude that $H' = H$. ■

Remark 2.179. If d divides the order N of G, there need *not* be a subgroup of order d. For example, if $G = A_4$, it has order 12, but no subgroup of order 6.

Theorem 2.180 (Sylow Theorems Restated)**.** *If G is finite of order $N = p^n m$ with* $\gcd(p, m) = 1$*, the*

1. *There exists Sylow p-subgroups of order p^n*
2. *Any two such subgroups are conjugate*
3. *The number l of such subgroups satisfies $l \mid m$ and $l \equiv 1(\mod p)$ (possible that $l = 1$, i.e¿ that the Sylow subgroup is a normal subgroup, giving a unique Sylow p-subgroup). If $l = 1$, then $gHg^{-1} = H$ for all g, so $H \trianglelefteq G$. Conversely, if H is normal, then $l = 1$.*

Proof Revisited Via Groups Acting on Set. (1) First, G acts by translation on set $\mathcal{J}$ of subsets $J \subset G$, with $|J| = p^n$. The number of such subsets is equal to $\binom{N}{p^n}$, which we have shown is prime to p. So some orbit O_J has size prime to p. Thus, G_J has order divisible by p^n, since $|O_J| = |G|/|G_J|$. But, J is equivalent to the set of right cosets of G_J, so $|G_J| \leq |J| = p^n$. Therefore, $|G_J| = p^n$, and G_J is a Sylow p-subgroup.

(2) Now let H be a Sylow p-subgroup, and let G act by translation transitively on the coset space G/H, with $|G/H| = m$. Then, the Stabilizer of the coset gH is the Sylow p-subgroup gHg^{-1}. Let H' be a Sylow p-subgroup, and restrict G action on G/H to H'. Then the orbits have size p^a, $0 \leq a \leq n$. Some orbit has size 1, not divisble by p, since the order of G/H is prime to p. Then it fixes a point gH, and hence it is contained in the stabilizer $H' \subset gHg^{-1}$. But, $|H'| = p^n$ and $|gHg^{-1}| = p^n$, which implies that $H' = gHg^{-1}$.

(3) Since all Sylow's are conjugate, we have the transitive action of G, by conjugation, on the set $\mathcal{H}$ of all Sylow p-subgroups. The stabilizer of H for this action $G_H = N(H)$. Thus, the set $\mathcal{H}$ is identified with $G/N(H)$. Moreover, since $H \subset N(H) \subset G$, we have that $|\mathcal{H}|$ divides m. Consider the action of H by conjugation on $\mathcal{H}$. This fixes the point H, and I claim this is the unique fixed point, so all other orbits have size divisible by p. Suppose for the sake of contradiction there is another fixed point H'. Then both H and H' are contained in $N(H')$. But, both H and H' are Sylow subgroups of $N(H')$. However, then H and H' must be conjugate, but the normalizer of H' fixes H', so $H = H'$. Thus, the $|\mathcal{H}| \equiv 1(\mod p)$. ■

2.14 Applications of the Sylow Theorems

2.14.1 Lecture

Recall (Classification Theorems). Let G be a group. If $|G| = p$, then G is cyclic $\cong \mathbb{Z}/p\mathbb{Z}$. If $|G| = p^2$, then G is abelian, and either $|cong(\mathbb{Z}/p\mathbb{Z})^2$ is all $g \neq e$ have $|g| = p$, or $\cong \mathbb{Z}/p^2\mathbb{Z}$ is all $g \neq e$ have $|g| = p^2$. Now, let us consider the case $|G| = p \cdot q$, $p < q$ are primes: First,

there exist Sylow subgroups $H_p = \langle \tau \rangle$ and $H_q = \langle \sigma \rangle$, which are both cyclic $\cong \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/q\mathbb{Z}$. Secondly, as a set, $G = H_p H_q = \{\tau^a \sigma^b : 0 \leq a < p, 0 \leq b < q\}$. This is equivalent to saying

$$G = \bigcup_{0 \leq a < p} \tau^a H_q \tag{2.90}$$

the cosets are dictinct for dicting τ τ' in H_p since if $\tau H_q = \tau' H_q$ implies $\tau(\tau')^{-1} \in H_q$, so $\tau(\tau)^{-1} \in H_p \cap H_q = \{e\}$, so $\tau = \tau'$. Now we must just figure out how multiplication must work.

Observation 2.181. Observe that $H_q \trianglelefteq G$ (the bigger prime). The reason is the number of Sylow q-subgroups l divides p and is congruent to $1(\mod p)$. The only such possibility since $p < q$ is $l = 1$. Then $\tau\sigma\tau^{-1} = \sigma^a$ for some a, an element of H_q, so $\tau\sigma = \sigma^a\tau$. In general, $a^p \equiv 1(\mod q)$.

Example 2.182 (Groups of Order Six)**.** $p.q = 6$, so $H_q = \langle 1, \sigma, \sigma^2 \rangle$ and $H_p = \langle 1, \tau \rangle$. Then

$$\tau\sigma\tau^{-1} = \begin{cases} \sigma & \text{so } \tau\sigma = \sigma\tau, G \text{ is abelian, } \cong \mathbb{Z}/6\mathbb{Z} \text{ (generated by } \sigma\tau) \\ \sigma^2 = \sigma^{-1} & \text{so } G \cong D_3 = S_3 \end{cases} \tag{2.91}$$

Example 2.183 (Groups of order $2p$)**.** $H_q = \langle 1, \sigma, \sigma^2, ..., \sigma^{q-1} \rangle$ and $H_p = \langle 1, \tau \rangle$. I claim $a \equiv \pm 1(\mod p)$. Then

$$\sigma = \tau^2\sigma\tau^{-2} = \tau\sigma^a\tau^{-1} = \tau\sigma\tau^{-1}\tau\sigma\tau^{-1}...\tau\sigma\tau^{-1} = \sigma^a\sigma^a...\sigma^a = \sigma^{a^2} \tag{2.92}$$

Thus, $a^2 \equiv 1(\mod q)$, so since q is prime, $a \equiv \pm 1(\mod q)$. Thus, in this case we have the possibilities of σ and σ^{-1}. If it is σ, then $G \cong \mathbb{Z}/2q\mathbb{Z}$ generated by $\tau\sigma$. Otherwise if it is σ^{-1}, then $G \cong D_{2q}$.

Example 2.184 (Groups of Order Fifteen)**.** $|G| = 15 = 3 * 5$. Then we have $\langle \sigma \rangle = H_5 \trianglelefteq G$. In this case $H_3 = \langle 1, \tau, \tau^2 \rangle$ is normal in G as the number l of Sylow 3's divides 5 and is $\equiv 1(\mod 3)$, so $l = 1$. If $\tau\sigma\tau^{-1} = \sigma^a$ with $a^3 \equiv 1(\mod 5)$, which implies that $a \equiv 1(\mod 5)$. This implies that $\tau\sigma = \sigma\tau$, and $G \cong \mathbb{Z}/15\mathbb{Z}$.

Example 2.185 (Groups of Order Twenty-One)**.** $|G| = 21 = 3 * 7$. Then H_7 is normal, but H_3 may not be normal, as there might be 7 Sylow 3s. Then, if we look at $a^3 \equiv 1(\mod 7)$, then $a \equiv 1, 2, 4(\mod 7)$, so we have $\tau\sigma\tau^{-1} = \sigma$, $\tau\sigma\tau^{-1} = \sigma^2$, or $\tau\sigma\tau^{-1} = \sigma^4$. Howeover, the last two give isomorphic non-abelian groups of order 21 with 7 3 Sylows.

Remark 2.186. $a \equiv 1(\mod q)$ gives $G \cong \mathbb{Z}/pq\mathbb{Z}$.

Example 2.187 (Groups of Order $12 = 2^2 * 3$)**.** There are 5 distinct groups, of which, 2 are abelian (one being $\mathbb{Z}/12\mathbb{Z}$, and one being $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$). One is A_4 (Sylow 2 is normal), one is D_{12} (Sylow 3 is normal) and one is new. From the Sylow Theorems we have a subgroup H_4 in G of order 4, and a subgroup H_3 of order 3 in G. But, we don't know if H_4 is $\mathbb{Z}/4\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^2$. The number l of Sylow 2s is equal to 1 or 4. The number of Sylow 3s is 1 or 4. I claim that one or the other must be normal. Imagine we have 4 Sylow 3s, which gives 8 elements of order 3 and 1 of order 1. Then there are only three elements left. Then, the identity and the three remaining elements must be a H_4, so there are no other possibilities for H_4 and it is normal.

2.15 Symmetric Group

2.15.1 Textbook

Remark 2.188. For permutations we will operate left to right. That is, $p \circ q$ will mean first apply p then apply q. Notationally, if we permute an index i by a permutation p we write

$$(i)p \tag{2.93}$$

(but we will usually drop the parenthesis.

Remark 2.189 (Permutation Matrices). For permutation matrices, defined previously, we now take the transpose of the permutation matrix and multiply a row vector on the right by it to permute the row vector.

Notation 2.190 (Tables). Other notations for permutations is a table with two rows. For example, the permutation

$$p = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 8 & 3 & 5 & 2 & 1 & 7 \end{bmatrix} \tag{2.94}$$

takes $1p = 4$, $2p = 6$, etc. We can then multiply two such tables by reading them left to right, and seeing where each element is taken.

Notation 2.191 (Cycle Notation). Cycle notation describes a permutation of n elements in at most n symbols, and is based on the partition of the indices into orbits for the action of the permutation. Let p be a permutation and let $H = \{1, p, p^2, ...\}$ be the cyclic subgroup generated by p. We decompose the set $\{1, 2, ..., n\}$ into $H - orbits$ and refer to these orbits as p-orbits. The p-orbits form a partition of the set of indices, called the **cycle decomposition** associated to the permutation p.

If an index i is in the orbit of k elements, then the elements of the orbit will be

$$O = \{i, ip, ip^2, ..., ip^{k-1}\} \tag{2.95}$$

Let us denote ip^r by i_r, so that $O = \{i_0, ..., i_{k-1}\}$. Then p permutes this orbit, and we write this **cyclic permutation** (where a cyclic permutation only has one associated orbit) as

$$(i_0\ i_1\ ...\ i_{k-1}) \tag{2.96}$$

The order of the cyclic permutation is the number of elements in its associated orbit. A cyclic permutation of order 2 is called a **transposition**.

Proposition 2.192. *Let σ and τ be permutations which operate on disjoint sets of indices. Then $\sigma\tau = \tau\sigma$.*

Proof. If neither σ nor τ operate on an index i, then $i\sigma\tau = i = i\tau\sigma$. If σ sends i to $j \neq i$, and τ fixes both j and i, then $i\sigma\tau = j\tau = j = i\sigma = i\tau\sigma$. The case that τ operates on i is identical. ■

Proposition 2.193. *Every permutation p not the identity is a product of cyclic permutations which operate on disjoint sets of indices: $p = \sigma_1\sigma_2...\sigma_k$, and these cyclic permutations σ_r are uniquely determined by p.*

Proof. We know that p operates as a cyclic permutation when restricted to a single orbit. For each p-orbit, we may define a cyclic permutation σ_r which permutes that orbit in the same way as p, and fixes the other indices. Clearly p is the product of these cyclic permutations. Conversely, let p be written as the product $\sigma_1...\sigma_k$ of cyclic permutations acting on distinct subsets $O_1, ..., O_k$ of indices. According to the previous proposition, the order of these permutations does not matter. Moreover, note that $\sigma_2, ..., \sigma_k$ fix the elements of O_1; hence, p and σ_1 act in the same way on O_1. Therefore, O_1 is a p-orbit. The same holds for the other cyclic permutations. Thus, $O_1, ..., O_k$ are the p-orbits which contain more than one element, and the permutations σ_i are those constructed at the start of the proof. ■

Proposition 2.194. *We now investigate the conjugate of a permutation p, namely $q^{-1}pq$*

1. *Let σ denote the cyclic permutation $(i_1\ i_2\ ...\ i_k)$, and let q be any permutation. Denote the index i_rq by j_r. Then the conjugate permutation $q^{-1}\sigma q$ is the cyclic permutation $(j_1\ j_2\ ...\ j_k)$*
2. *If an arbitrary permutation p is written as the product of disjoint cycles σ, then $q^{-1}pq$ is the product of the disjoint cycles $q^{-1}\sigma q$.*
3. *Two permutation p and p' are conjugate elements of the symmetric group if and only if their cycle decompositions have the same orders.*

Proof. The proof of the first point is the following computation:

$$j_r q^{-1}\sigma q = i_r \sigma q = i_{r+1} q = j_{r+1} \tag{2.97}$$

in which the indices are read modulo k. Suppose $p = \sigma_1\sigma_2...\sigma_k$, then it follows that

$$q^{-1}pq = q^{-1}\sigma_1 q q^{-1}\sigma_2 ... q q^{-1}\sigma_k q \tag{2.98}$$

Then note that if $iq^{-1}\sigma q = iq^{-1}\sigma' q$ for some index i, then since all of these operations are permutations, $j\sigma = j\sigma'$. However, $\sigma_1, ..., \sigma_k$ are disjoint, so it follows that $q^{-1}\sigma_1 q, ..., q^{-1}\sigma_k q$ are disjoint cycles. In particular, if σ fixes an element i, then $q^{-1}\sigma q$ fixes the element iq. Moreover, if j is moved by σ, then jq is moved by $q^{-1}\sigma q$. Thus, the order of a cycle and its conjugate are equivalent. Therefore, conjugate permutations have cycle decompositions with the same orders. Conversely, suppose p and p' are permutations with cycle decompositions with the same orders. Say $p = (i_1 \ ... \ i_r)(i'_1 \ ... \ i'_s)...$ and $q = (j_1 \ ... \ j_r)(j'_1 \ ... \ j'_s)....$ Define q to be the permutation sending $i_v \mapsto j_v$, $i'_v \mapsto j'_v$, and so on. Then $p' = q^{-1}pq$. ■

Example 2.195. Consider the subgroups G of the symmetric group S_p whose order is divisible by p, and whose Sylow p-subgroup is normal. We assume that p is a prime integer. Since p divides $p!$ only once, it also divides $|G|$ only once, and so the Sylow p-subgroups of G is a cyclic group.

To describe such subgroups, we can consider the finite field $\mathbb{Z}/p\mathbb{Z}$ acting on its set of elements as indices, where addition and multiplication by $c \neq 0$ give permutations. All such operators are of the form

$$x \mapsto xc + a \tag{2.99}$$

And this set gives a subgroup G of order $p(p-1)$ of the symmetric group. This group can also be represented by the set of invertible 2×2 matrices over the field $\mathbb{Z}/p\mathbb{Z}$ of the form

$$\left\{ \begin{bmatrix} 1 & a \\ & c \end{bmatrix} \right\} \tag{2.100}$$

with these matrices operating by right multiplication on the vector $[1 \ x] \mapsto [1 \ cx + a]$.

Theorem 2.196. *Let p be a prime, and let H be a subgroup of the symmetric group S_p whose order is divisible by p. If the Sylow p-subgroup of H is normal, then, with suitable labeling of the indices, H is contained in the group of operators of the above form.*

Proof. The only elements of order p of S_p are the p-cycles. So, H contains a p-cycle, say σ. We may relabel indices so that σ becomes the p-cycle $(0 \ 1 \ ... \ (p-1))$. Then, this permutation generates the Sylow p-subgroup of H.

Let τ_1 be another element of H. We have to show that τ_1 corresponds to an operator of the form above. Say that τ_1 sends the index 0 to the index i. Since σ^i also sends 0 to i, the product $\tau = \sigma^{-i}\tau_1$ fixes 0. It suffices to show that τ has the above form, so we will show

τ is one of the operators (multiply by c). By hypothesis $K = \{1, \sigma, ..., \sigma^{p-1}\}$ is a normal subgroup of H. Therefore

$$\tau^{-1}\sigma\tau = \sigma^k \tag{2.101}$$

for some $1 \leq k \leq p-1$. By a previous proposition, the left side is the p-cycle $\tau^{-1}\sigma\tau = (0\tau\ 1\tau\ ...(p-1)\tau)$ while direct computation of the right side gives $\sigma^k = (0\ k\ 2k\ ...\ (p-1)k)$. Since cycle notation is not unique, we must be careful in our analysis of the equality of these cycles. Since we normalized τ so that $0\tau = 0$, we may conclude that

$$1\tau = k,\ 2\tau = 2k\ ... \tag{2.102}$$

This is the operator (multiply by k), as claimed. ■

2.15.2 Lecture

Recall (Symmetric Group). The symmetric group on n letters, S_n, which is the set of bijections from $\{1, ..., n\}$ to itself. These permutations will act on the right (that is $(i)p$ for an index i and permutation p).

Notation 2.197 (Notations). The first notation is to give a table with the first row begin the elements $\{1, ..., n\}$ in order, and below each element is the element it's sent to: For example

$$p = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 4 & 1 & 2 \end{bmatrix} \quad q = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 5 & 6 & 3 \end{bmatrix} \tag{2.103}$$

Moreover, the product will be

$$pq = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 4 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 5 & 6 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 5 & 2 & 1 \end{bmatrix} \tag{2.104}$$

The other primary notation is cycle notation. For example, p and q in cycle notation would be

$$p = (1\ 3\ 5)(2\ 6),\ q = (1\ 2)(3\ 4\ 5\ 6) \tag{2.105}$$

Then the product would be

$$pq = (1\ 4\ 5\ 2\ 3\ 6) \tag{2.106}$$

Proposition 2.198. *Any permutation can be written uniquely as a product of disjoint cycles up to reorderings of the cycles and cyclical permutations of the index in a given cycle.*

Example 2.199 (Conjugates)**.** We wish to calculate $q^{-1}pq$ (as defined above)

$$q^{-1}pq = \begin{bmatrix}1&2&3&4&5&6\\2&1&4&5&6&3\end{bmatrix}^{-1}(1\ 3\ 5)(2\ 6)(4)\begin{bmatrix}1&2&3&4&5&6\\2&1&4&5&6&3\end{bmatrix} = (2\ 4\ 6)(1\ 3)(5) \quad (2.107)$$

Note that the "cycle shape" is the same, with the same number of disjoint cycles of the same size. Moreover, the elements in new cycle are the q images of the elements in p's original cycles. Thus, $q^{-1}(1\ 3\ 5)(2\ 6)(4)q = (1q\ 3q\ 5q)(2q\ 6q)(4q)$

Remark 2.200 (Conjugation). Suppose $ip = j$. Then observe that $(iq)(q^{-1}pq) = (ip)q = jq$, so if $p = (i_1\ i_2\ ...\ i_r)(i'_1\ ...\ i'_s)...$, then

$$q^{-1}pq = ((i_1q)\ (i_2q)\ ...\ (i_rq))((i'_1q)\ ...\ (i'_sq))... \quad (2.108)$$

Proposition 2.201. *Two permutations which are conjugate in S_n have the same* ***cycle shape****, where the same cycle shape means when expressed as a product of disjoint cycles, they have the same number of cycles of every length. Conversely, if two permutations have the same cycle shape, then they are conjugate.*

Example 2.202. Consider the permutation $(1\ 3\ 5)(2\ 6)(4)$ and the permutation $(6\ 5\ 4)(3\ 2)(1)$. By the proposition these are conjugate. Take $q = (1\ 6\ 2\ 3\ 5\ 4)$. Then it follows that

$$(1\ 6\ 2\ 3\ 5\ 4)^{-1}(1\ 3\ 5)(2\ 6)(4)(1\ 6\ 2\ 3\ 5\ 4) = (6\ 5\ 4)(3\ 2)(1) \quad (2.109)$$

As desired.

Example 2.203. Suppose $p = (1\ 2)(3\ 4)(5\ 6)(7\ 8\ 9)(10\ 11\ 12)$, then what is the number of $q \in S_{12}$ such that $q^{-1}pq = p$.

Remark 2.204. If p has a_1 1-cycles, a_2 2-cycles, etc, then how many q satisfy $q^{-1}pq = p$? It would be

$$\prod_{i=1}^{n} a_i! * i^{a_i} \quad (2.110)$$

where n is the disjoint cycle in p's decomposition.

Example 2.205. Consider S_5, noting that $|S_5| = 5! = 120$, then representatives of the conjugacy classes are $(1\ 2\ 3\ 4\ 5)$, $(1\ 2\ 3\ 4)(5)$, $(1\ 2\ 3)(4)(5)$, $(1\ 2)(3)(4)(5)$, $(1)(2)(3)(4)(5)$, $(1\ 2\ 3)(4\ 5)$, $(1\ 2)(3\ 4)(5)$.

Remark 2.206. The order of the conjugacy class of p in S_n is

$$\frac{n!}{\prod_{i=1}^{m}(a_i!i^{a_i})} \tag{2.111}$$

Remark 2.207. If p is prime, then $|S_p| = p! = pm$, where $\gcd(p, m) = 1$. Thus, we have a Sylow p-subgroup of order p, which implies that the subgroup generated by any p-cycle is a Sylow p-subgroup.

Question. The normalizer in S_p for a Sylow p-subgroup is what?

Answer. Suppose P is a Sylow p-subgroup with generator (after relabeling if needed) (1 2 ... p). Then, suppose $\sigma \in S_p$. Then $\sigma^{-1}(1\ 2\ ..\ p)\sigma = (1\sigma\ 2\sigma\ ...\ p\sigma)$. For $\sigma \in N(P)$, 1σ can be any element, so it has p choices, 2σ can be any other element, so it has $p-1$ choices, but after these choices are made 3σ onwards is decided, so $|N(P)| = p(p-1)$.

2.16 Little Review

Recall (Sylow Theorem). Let G be a group of order $N = p^n m$, where $\gcd(p, m) = 1$ and p is prime. Then:

1. The number of Sylow p-subgroups, $n_p(G)$, is congruent to 1 mod p, and $n_p(G)$ divides m.
2. Every two Sylow p-subgroups are conjugate. Some Consequences: Let $H \subset G$ be a Sylow p-subgroup
   (a) H is normal $\iff n_p(G) = 1$
   (b) $[G : N_G(H)] = [G : (\textit{stabilizer of } H \textit{ where } G \textit{ acts on the Sylow } p\textit{−subgroups by cpnjugation}]$ $|O_H|(\textit{by counting formula}) = n_p(G)$
   (c) If $|G| = pm$, $\gcd(p, m) = 1$, then the number of elements of order p in G is $n_p(G)(p-1)$

2.16.1 Applications of the Sylow Theorems

Remark 2.208. Groups of order $|G| = pq$ ($p < q$ being primes): By the Sylow Theorems we know that there exist Sylow p-subgroups and Sylow q-subgroups. In particular, $n_q(G) = 1$, so there exists a unique Sylow q-subgroup of G, and it is normal. If $p \nmid q - 1$, then there is a unique Sylow p-subgroup, and it is also normal, so $n_p(G) = 1$. Moreover, $G \cong \mathbb{Z}/pq\mathbb{Z}$. On the other hand, if $p \mid q - 1$, then there exists a unique non-abelian group of order pq.

Remark 2.209 (Order 12 Groups). If $|G| = 12$, then either G has a normal Sylow 3-subgroup, or $G \cong A_4$, which has a normal Sylow 2-subgroup.

Remark 2.210 (Groups of Order p^2q). If $p > q$, then by the Sylow theorems we must have a normal Sylow p-subgroup. Otherwise, if $p < q$, it can be shown that either G has normal Sylow q-subgroup or $p^2q = 12$, and $G \cong A_4$.

Remark 2.211 (Finding the Structure of a Group). Semi-direct products allow us to break down groups using their normal subgroups.

Remark 2.212 (Conjugacy in S_n). We have disjoint cycle decomposition. Given $\tau \in S_n$, if $\sigma = (a_{11}\ ...\ a_{1l_1})...(a_{k1}\ ...\ a_{kl_k})$, then $\tau\sigma\tau^{-1} = (\tau(a_{11})\ ...\ \tau(a_{1l_1}))...(\tau(a_{k1})\ ...\ \tau(a_{kl_k}))$, so elements are conjugate if and only if they have the same cycle shape.

2.16.2 Notes on A_5

Proposition 2.213. *A_5 is simple.*

Proposition 2.214. *If G is a simple group of order 60, then $G = A_5$.*

Proof. First, note that $|G| = 2^2 * 15$. Then $n_2(G) \equiv 1 \mod 2$, and $n_2(G) \mid 15$. Then $n_2(G)$ is either 1, 3, 5, or 15. It suffices to show G has no proper subgroups of index < 5, since if P is a Sylow 2-subgroup, $[G : N_G(P)] = n_2(G)$. Suppose for the sake of contradiction that $[G : H] = 2, 3$ or 4. Then we have an action of G on G/H by left multiplication, which is transitive. Moreover, for every $g \in G$, g induces a permutation of the coset space G/H, so the action is faithful. Thus, this action induces a homomorphism $\phi : G \to Sym(G/H)$, with $g \mapsto$ permutation induced by g. Then, by general principles, $\ker(\phi) \subset H$, which is a proper subgroup of G. Moreover, we know that G is simple, so $\ker(\phi) = \{e\}$. Thus, ϕ must be injective, so G is isomorphic to some subgroup of $Sym(G/H)$. However, $|G| \leq |Sym(G/H)| \leq 4! = 24$, and $|G| = 60$, which is a contradiction. Our second claim is that if $n_2(G) = 5$, then $G \cong A_5$. Let P be a Sylow 2-subgroup, and let $N = N_G(P)$. Then $[G : N] = n_2(G) = 5$, and we again take the group action of translation by G on G/N. Moreover, we again have a homomorphism $\phi : G \to Sym(G/N) \cong S_5$, and again G acts transitively on G/N, and N is proper, so since G is simple, $\ker(\phi) = \{e\}$. Thus, ϕ is injective, and G is isomorphic to a subgroup of S_5. For the sake of contradiction suppose the image of ϕ is not contained in A_5. Then, we know that $GA_5 = S_5$, and $[G : A_5 \cap G] = [S_5 : A_5] = 2$. This implies that $A_5 \cap G \trianglelefteq G$. But, since G is simple, and $A_5 \cap G$ is a non-trivial normal subgroup, this is a contradiction. Therefore, $G \subset A_5$, and in particular, since $|G| = 60 = |A_5|$, we conclude that $G = A_5$. Claim 3, in $n_2(G) \neq 15$ (prove by contradiction) ■

2.16.3 Notes on A_n

Theorem 2.215 (Simple A_n)**.** *A_n is simple for $n \geq 5$.*

Proof. (By induction) Suppose $n \in \mathbb{N}$, $n \geq 5$. We proceed by induction on n. Base Case: From a previous result, A_5 is simple, so the base case holds. Induction Hypothesis: Suppose for some $n-1 \geq 5$, A_{n-1} is simple. We now aim to show that $G = A_n$ is simple. Suppose for the sake of contradiction that there exists $H \trianglelefteq G$, which is proper and non-trivial. Let G act on the set $\{1, ..., n\}$ through natural permutations, and let G_i be the stabilizer of i. Then $G_i \cong A_{n-1}$ after reindexing. Then, by the induction hypothesis we have that A_{n-1} is simple, so for each $i \in \{1, ..., n\}$, G_i is simple. First, we claim that there exists no $\tau \in H$, $\tau \neq e$, such that $\tau(i) = i$ for some i. If there was a non-identity element $\tau \in H$ such that $\tau(i) = i$ for some i, then $\tau \in G_i$, and $G_i \cap H$ would be a non-trivial subgroup of G_i. In particular, $G_i \cap H$ would be a non-trivial normal subgroup of G_i, but G_i is simple so this is a contradiction. It follows that if $\tau_1(i) = \tau_2(i)$ for some i, with $\tau_1, \tau_2 \in H$, $\tau_2^{-1}\tau_1(i) = i$, so $\tau_2^{-1}\tau_2 = e$, and $\tau_1 = \tau_2$. Secondly, we would claim that given $\tau \in H$, only 2 cycles can appear in its disjoint cycle decomposition. Finally, we claim that given $\tau \in H$, τ doesn't just have 2 cycles in its decomposition. ■

3 Vector Spaces

Definition 3.1 (Vector Space over the Reals)**.** A vector space V over $\mathbb{R}$ consists of

1. An abelian group, with operation $+$, identity $\mathbf{0}_V$, and inverses $-\mathbf{v}$.
2. A scalar multiplication by $c \in \mathbb{R}$ given by $\mathbf{v} \mapsto c\ \mathbf{v}$ following certain properties, such as $0 \cdot \mathbf{v} = \mathbf{0}$, $1 \cdot \mathbf{v} = \mathbf{v}$, $(ab)\ \mathbf{v} = a(b\ \mathbf{v}) = b(a\ \mathbf{v})$ for all $a, b \in \mathbb{R}$.

Example 3.2. 1. $\{0\} = V$

2. $V = \mathbb{R}$
3. $V = \mathbb{R}^n$, $\mathbf{v} \in V$, $\mathbf{v} = (a_1, ..., a_n)$, $a_i \in \mathbb{R}$, $a\ \mathbf{v} = (aa_1, ..., aa_n)$, and $\mathbf{v} + \mathbf{w} = (a_1 + b_1, ..., a_n + b_n)$. $\mathbb{R}^n$ we also have additional structure with the euclidean inner product $\mathbf{v} \cdot \mathbf{w} = \sum a_i b_i$ and norm $||\ \mathbf{v}|| = \sqrt{\mathbf{v} \cdot \mathbf{v}}$.

3.1 Field Definitions

Definition 3.3 (Field)**.** A field F is a set with the following properties/structure:

1. It is an abelian group under $+$, with identity 0, and inverses $-a$.
2. $F/\{0\} = F^*$ forms an abelian group under $\times$ with identity 1, and inverses $a^{-1} = \frac{1}{a}$. In particular, every non-zero element has a multiplicative inverse.
3. There is a distributive law which satisfies $a(b + c) = ab + ac$ for all $a, b, c \in F$.

Definition 3.4 (Subfield)**.** A subset F' of a field F is a subfield of F if it is closed under $+$ and $\times$, and is closed under inversion.

Remark 3.5 (Simplest field). For all fields F, $\{0, 1\} \subset F$. The simplest field is $F = \{0, 1\}$. Note that $0 + 1 = 1$. Then We define $1 + 1 = 0$. Moreover, $0 * 1 = 0$, and $1 * 1 = 1$.

Definition 3.6 (Prime Fields)**.** If p is a prime number, then $\mathbb{Z}/p\mathbb{Z}$ with the multiplication inherited from $\mathbb{Z}$ is a field.

Note. Warning: $\mathbb{Z}/n\mathbb{Z}$ is not a field if n is composite.

Proof. To prove this we must show that if $a \not\equiv 0 \mod p$, then there exists b: $ab \equiv 1 \mod p$, so $b \equiv a^{-1} \mod p$. Recall that $p\mathbb{Z} \subset \mathbb{Z}$ is a maximal subgroup. If $a \not\equiv 0 \mod p$, then $a \notin p\mathbb{Z}$. Hence, $p\mathbb{Z} + a\mathbb{Z} = \mathbb{Z}$, as this is a subgroup of $\mathbb{Z}$ containing $p\mathbb{Z}$, but not equal to $p\mathbb{Z}$. Then there exists $m, n \in \mathbb{Z}$ so that $1 = mp + na$ since $1 \in \mathbb{Z}$. Thus $1 \equiv na \mod p$. ■

Observation 3.7 (Properties of the Finite Prime Fields). $\mathbb{Z}/p\mathbb{Z}$ is not a subfield of $\mathbb{C}$! Note, that $1 \in F$ for any field F. Moreover, $1+1+...+1 \in F$ for any number of 1's. In $\mathbb{C}$, for all $n > m \geq 1$, the sum of 1 n times is greater than the sum of 1 m times. However, the sum of 1 p times in $\mathbb{Z}/p\mathbb{Z}$ is the identity.

Question (Galois). What are the finite field beyond $\mathbb{Z}/p\mathbb{Z}$?

Answer. For a finite field, what is the order of $|F|$? It is p^n for a prime p, $n \geq 1$. Additionally, for each p and n there is a unique such F up to isomorphism.

Definition 3.8 (Characteristic of a Field)**.** A field F is said to have **characteristic** p if p is the smallest positive integer such that the multiplicative identity 1 added p times is the additive identity 0. In other words, the characteristic of F is the order of 1 as an element of the additive group $(F, +)$, provided that the order is finite. If no such p exists, then F is said to have characteristic 0.

3.2 Vector Spaces over Arbitrary Fields

Definition 3.9 (Vector Space over Arbitrary Fields)**.** A **vector space over a field** F is a set of vectors V, with the following properties/structure:

1. V is an abelian group under + with identity $\mathbf{0}_V$
2. There is an operation called the scalar product

$$V \times F \to V \tag{3.1}$$

$$(\mathbf{v}, c) \mapsto c \cdot \mathbf{v} \tag{3.2}$$

With the properties $0 \cdot \mathbf{v} = \mathbf{0}_V$, $1 \cdot \mathbf{v} = \mathbf{v}$, $(ab)\ \mathbf{v} = a(b\ \mathbf{v})$, $a(\mathbf{v} + \mathbf{w}) = a \cdot \mathbf{v} + a \cdot \mathbf{w}$, and $(a+b)\ \mathbf{v} = a\ \mathbf{v} + b\ \mathbf{v}$.

Example 3.10. Of V over F

1. $\{\mathbf{0}_V\}$
2. $V = F$.
3. $V = F^n$, all n-tuples $(a_1, ..., a_n)$, $a_i \in F$.
4. $V = F[x] :=$ {all polynomials $p(x)$ with coefficients in F}

Definition 3.11 (Subspace)**.** For a vector space V over F, $W \subset V$ is a **vector subspace** if it is a subgroup under $+$ (contains 0), and is stable under scalar multiplication by F (i.e. closed).

Definition 3.12 (Linear Homomorphism)**.** A map $T : V \to W$ is a homomorphism (linear transformation) if it is a group homomorphism,

$$T(\mathbf{v} + \mathbf{w}) = T(\mathbf{v}) + T(\mathbf{w}) \tag{3.3}$$

and it commutes with scalar multiplication

$$T(c\ \mathbf{v}) = cT(\mathbf{v}) \tag{3.4}$$

Moreover, a bijective homomorphism is an isomorphism. Furthermore, $ker(T) = \{\mathbf{v} : T(\mathbf{v}) = \mathbf{0}_W\}$ is a subspace of V, and $Im(T) := \{T(\mathbf{v}) \in W : \mathbf{v} \in V\}$ is a subspace of W.

Definition 3.13 (Quotient Space)**.** For a subspace $W \subset V$, we define the **quotient space** V/W (Set of cosets of W in V), which is an abelian group, and is closed under a defined scalar multiplication. I.E. It has the structure of a vector space over F, and the canonical projection (homomorphism) $f : V \to V/W$ is a linear transformation with kernel W.

Remark 3.14. Once a field is picked, it is fixed - you can't do a linear transformation between vector spaces over different fields.

3.3 Bases and Dimension

3.3.1 Textbook

Definition 3.15 (Linear Combination)**.** Let V be a vector space over a field F, and let $(\mathbf{v}_1, ..., \mathbf{v}_n)$ be an ordered set of elements of V. A **linear combination** of the vectors in this ordered set is any vector of the form

$$\mathbf{w} = c_1\ \mathbf{v}_1 + ... + c_n\ \mathbf{v}_n, c_i \in F \tag{3.5}$$

Definition 3.16 (Span)**.** The set of all vectors $\mathbf{w}$ which are a linear combination of vectors in the ordered set $(\mathbf{v}_1, ..., \mathbf{v}_n)$ forms a subspace W of V, called the subspace **spanned** by the set, and is denoted $W := \text{span}(\mathbf{v}_1, ..., \mathbf{v}_n)$. In particular, the space spanned by a set S is often denoted span(S), and span(S) is the smallest subspace of V which contains S. We could also call it the subspace generated by S.

Proposition 3.17. *Let S be a set of vectors of V, and let W be a subspace of V. If $S \subset W$, then* $\text{span}(S) \subset W$.

Proof. Since W is stable under vector addition and scalar multiplication and $S \subset W$, any linear combination of elements in S is in W, so $\text{span}(S) \subset W$. ■

Definition 3.18 (Linear Independence)**.** A **linear relation** among vectors $\mathbf{v}_1, ..., \mathbf{v}_n$ is any relation of the form

$$c_1 \mathbf{v}_1 + ... + c_n \mathbf{v}_n = \mathbf{0}_V \tag{3.6}$$

where the coefficients c_i are in F. An ordered set $(\mathbf{v}_1, ..., \mathbf{v}_n)$ is called **linearly independent** if there is no linear relation among the vectors in the set except the trivial relation with each $c_i = 0$. In other words, the set is linearly independent if and only if the equation $c_1 \mathbf{v}_1 + ... + c_n \mathbf{v}_n = \mathbf{0}_V$ implies that $c_i = 0$ for all $i = 1, 2, ..., n$. Otherwise, if a non-trivial linear relation exists among the vectors, then the set is said to be **linearly dependent**.

Proposition 3.19 (Facts about Independence)**.** .

1. *Any reordering of a linearly independent set is linearly independent.*
2. *If $\boldsymbol{v}_1 \in V$ is a nonzero vector, then the set $(\boldsymbol{v}_1)$ is linearly independent.*
3. *A set $(\boldsymbol{v}_1, \boldsymbol{v}_2)$ is linearly dependent if and only if one vector is a scalar multiple of the other.*

Definition 3.20 (Basis)**.** A set of vectors $(\mathbf{v}_1, ..., \mathbf{v}_n)$ which is linearly independent and also spans V is called a **basis** for V.

Proposition 3.21 (Basis Representation)**.** *The set $B = (\boldsymbol{v}_1, ..., \boldsymbol{v}_n)$ is a basis if and only if every vector $\boldsymbol{w} \in V$ can be written in a **unique** way as a linear combination of the vectors in B.*

Proof. Suppose that B is a basis of a vector space V, and $\mathbf{w} \in V$. Then $\mathbf{w}$ can be represented as a linear combination of the vectors in B. Suppose with can be done two ways, so

$$c_1 \mathbf{v}_1 + ... + c_n \mathbf{v}_n = \mathbf{w} = c_1' \mathbf{v}_1 + ... + c_n' \mathbf{v}_n$$

Then we have the linear relation $(c_1 - c_1') \mathbf{v}_1 + ... + (c_n - c_n') \mathbf{v}_n = \mathbf{0}_V$, so since B is a basis, it follows that $c_i - c_i' = 0$, or $c_i = c_i'$ for all $i = 1, 2, ..., n$. On the other hand, suppose that every vector in V can be expressed in a unique way via a linear combination of the vectors in B. Then $\text{span}(B) = V$, and the zero vector can be represented in a unique way

$$c_1 \mathbf{v}_1 + ... + c_n \mathbf{v}_n = \mathbf{0}_V$$

but since the trivial representation always exists, it follows that $c_i = 0$ for all $i = 1, 2, ..., n$. Therefore, B is a basis of V by definition. ■

Proposition 3.22. *Let L be a linearly independent ordered set in V, and let $\boldsymbol{v} \in V$ be any vector. Then the ordered set $L' = (L, \ \boldsymbol{v})$ is linearly independent if and only if $\boldsymbol{v} \notin \text{span}(L)$.*

Proof. Suppose $L = (\ \mathbf{v}_1, ..., \ \mathbf{v}_r)$ is an ordered linearly independent set in V, and let $\mathbf{v} \in V$. If $\mathbf{v} \in \text{span}(L)$, then $c_1\ \mathbf{v}_1 + ... + c_r\ \mathbf{v}_r = \ \mathbf{v}$ for some scalars c_i, so

$$c_1\ \mathbf{v}_1 + ... + c_r\ \mathbf{v}_r + (-1)\ \mathbf{v} = \ \mathbf{0}_V$$

is a linear relation among the vectors of L' that is non-trivial, so L' is linearly dependent. Conversely, suppose L' is linearly independent, so there exists a non-trivial linear relation

$$c_1\ \mathbf{v}_1 + ... + c_r\ \mathbf{v}_r + b\ \mathbf{v} = \ \mathbf{0}_V$$

where certainly $b \neq 0$, as otherwise we obtain a linear relation of L, which must be trivial. Therefore,

$$\mathbf{v} = -\frac{c_1}{b}\ \mathbf{v}_1 - ... - \frac{c_r}{b}\ \mathbf{v}_r$$

so $\mathbf{v} \in \text{span}(L)$. ■

Proposition 3.23. *Let S be an ordered set of vectors, let $\boldsymbol{v} \in V$ be any vector, and let $S' = (S, \ \boldsymbol{v})$. Then $\text{span}(S) = \text{span}(S')$ if and only if $\boldsymbol{v} \in S$.*

Proof. By definition $\mathbf{v} \in S'$. Thus, if $\mathbf{v} \notin \text{span}(S)$, then $\text{span}(S) \neq \text{span}(S')$. Conversely, if $\mathbf{v} \in \text{span}(S)$, then $S' \subset \text{span}(S)$, so $\text{span}(S') \subset \text{span}(S)$. Furthremore, by definition $S \subset S'$ so $S \subset \text{span}(S')$, and hence $\text{span}(S) \subset \text{span}(S')$. Therefore $\text{span}(S) = \text{span}(S')$. ■

Definition 3.24 (Finite Dimensional)**.** A vector space V is called **finite-dimensional** if there exists some finite subset S of V which spans V.

Proposition 3.25 (Existence of Bases)**.** *Any finite set S which spans V contains a basis. In particular, any finite-dimensional vector space has a basis. Note that the empty set is linearly independent (trivially), and its span is the zero vector.*

Proof. Suppose $S = (\ \mathbf{v}_1, ..., \ \mathbf{v}_n)$ is a spanning set of V. If S is linearly independent we're done, so suppose S is linearly dependent. Then there exists a linear relation

$$c_1\ \mathbf{v}_1 + ... + c_n\ \mathbf{v}_n = \ \mathbf{0}_V$$

where some c_i is non-zero. Without loss of generality let $c_n \neq 0$. Then

$$\mathbf{v}_n = -\frac{c_1}{c_n}\ \mathbf{v}_1 - ... - \frac{c_{n-1}}{c_n}\ \mathbf{v}_{n-1}$$

This shows that $\mathbf{v}_n \in \text{span}(\ \mathbf{v}_1, ..., \ \mathbf{v}_{n-1})$, so $\text{span}(\ \mathbf{v}_1, ..., \ \mathbf{v}_{n-1}) = \text{span}(\ \mathbf{v}_1, ..., \ \mathbf{v}_n) = V$. Thus, we may eliminate $\mathbf{v}_n$ from S, Continuing this way we eventually obtain a family which is linearly independent and spans V (a basis). ■

Proposition 3.26 (Extending to a Basis)**.** *Let V be a finite-dimensional vector space. Any linearly independent set L can be extended by adding elements to get a basis.*

Proof. Let S be a finite set which spans V. If all elements of S are in span(L) then L spans V. Otherwise, there exists $\mathbf{v} \in S$ which is not in span(L). Therefore, $(L, \mathbf{v})$ is linearly independent. We continue in this fashion until we obtain a linearly independent spanning set. ■

Proposition 3.27. *Let S and L be finite subsets of a vector space V, with S being a spanning set and L being linearly independent. Then $|L| \leq |S|$.*

Proposition 3.28. *Two bases B_1, B_2 of a vector space V have the same number of elements.*

Definition 3.29 (Dimension)**.** The **dimension** of a finite-dimensional vector space V is the number of vectors in a basis, and is denoted $\dim(V)$.

Proposition 3.30. .

1. *If S spans V, then $|S| \geq \dim(V)$, and equality holds if S is a basis.*
2. *If L is linearly independent, then $|L| \leq \dim(V)$, and equality holds if L is a basis.*

Proposition 3.31. *If $W \subset V$ is a subspace of a finite-dimensional vector space, then W is finite dimensional, and $\dim(W) \leq \dim(V)$. Moreover, $\dim(W) = \dim(V)$ if and only if $W = V$.*

Definition 3.32 (Space of Formal Linear Combinations)**.** Suppose that S is a set of n distinct elements. Then we define the **space of formal linear combinations of S** as the set $V(S)$ of a field F that contains all linear combinations

$$a_1 \ \mathbf{s}_1 + ... + a_n \ \mathbf{s}_n, a_i \in F \tag{3.7}$$

where addition and scalar multiplication are defined coefficient wise.

3.3.2 Lecture

Let V be a vector space over a field F. Let $S = (\ \mathbf{v}_1, ...,\ \mathbf{v}_n)$ be an ordered set of vectors in $\mathbf{V}$.

Definition 3.33 (Linear Combination)**.** A linear combination of the vectors in our ordered set is a vector of the form

$$\mathbf{w} = a_1\ \mathbf{v}_1 + ... + a_n\ \mathbf{v}_n$$

with $a_i \in F$. The set of all such $\mathbf{w}$ is the span of the set S (this is a subspace of V). If $S = \emptyset$, then by convention $\text{span}(S) = \{0\}$.

Definition 3.34. V is finite=dimensional if there is a finite set S of vector in V with $\text{span}(S) = V$.

Example 3.35. $V = F^n$ is finite dimensional with basis $S = \{(1, 0, ..., 0), (0, 1, ..., 0), ..., (0, ..., 0, 1)\}$.

Example 3.36 (Non-example)**.** $V = F[x]$ is not finite-dimensional (argument: use the degree of a polynomial in $F[x]$).

Definition 3.37 (Linear Independence)**.** A set of vectors $\{\ \mathbf{v}_1, ...,\ \mathbf{v}_n\}$ is linearly independent if the relation

$$a_1\ \mathbf{v}_1 + ... + a_n\ \mathbf{v}_n = \ \mathbf{0}_V$$

only holds when $a_1 = a_2 = ... = a_n = 0$.

Example 3.38. Take $V = \mathbb{R}^3$ and $v_1 = (1, 0, 0)$, $v_2 = (1, 2, 0)$, and $v_3 = (1, 2, 3)$. Then we claim that $\text{span}\{v_1, v_2\} = \{v = (a, b, 0)\}$, with $(a, b, 0) = b/2v_2 + (a - b/2)v_1$. Moreover, the set $\{v_1, v_2, v_3\}$ is linearly independent.

Definition 3.39 (Basis)**.** The ordered set $(v_1, ..., v_n)$ is a **basis** of V if it spans V and is linearly independent.

Observation 3.40. This means that every vector $\mathbf{w} \in V$ is uniquely expressed as a linear combination $\mathbf{w} = a_1v_1 + ... + a_nv_n$.

Observation 3.41 (Interpretation of a Basis). A basis gives rise to an isomorphism of vector spaces

$$V \xrightarrow{f} F^n \tag{3.8}$$

with

$$\mathbf{w} \mapsto (a_1, a_2, ..., a_n) \tag{3.9}$$

In particular, note $f(\ \mathbf{w} +\ \mathbf{w}') = (a_1 + b_1, ..., a_n + b_n) = (a_1, ..., a_n) + (b_1, ..., b_n) = f(\ \mathbf{w}) + f(\ \mathbf{w}')$ and $f(c\ \mathbf{w}) = (ca_1, ..., ca_n) = c(a_1, ..., a_n) = cf(\ \mathbf{w})$ so it is a homomorphism of vector spaces. Note that f is surjective since all linear combinations of our basis is in V, and since the basis is linearly independent, the kernel of f is trivial, so f is injective.

Theorem 3.42. *If $S = \{v_1, ..., v_n\}$ is a finite set which spans V, then a subset of S gives a basis for V.*

Proof. If the elements of S are linearly independent, we're done. If not, we have a relation

$$a_1 v_1 + ... + a_n v_n = \mathbf{0}_V$$

with some $a_i \neq 0$. We can reorder S so that $a_n \neq 0$. Then we can write v_n as

$$a_n v_n = -(a_1 v_1 + ... + a_{n-1} v_{n-1})$$

Then a_n^{-1} since F is a field, so

$$v_n = -\frac{1}{a_n}(a_1 v_1 + ... + a_{n-1} v_{n-1})$$

Hence, $V = \text{span}(S) = \text{span}\{v_1, ..., v_{n-1}\}$. If $\{v_1, ..., v_{n-1}\}$ is linearly independent, we're done. If not, we can repeat the procedure until we obtain a linearly independent set (possibly the empty set). ■

Theorem 3.43. *If $L = \{w_1, ..., w_r\}$ is a linearly independent set of vectors, it can be extended to form a basis of V.*

Proof. If L spans V, then we're done. If not, let S be a finite set spanning V. Moreover, let $\mathbf{v} \in S$ with $\mathbf{v} \notin \text{span}(L)$. Then, we claim that $L \cup \{\mathbf{v}\} = L'$ is linearly independent. Suppose we have a linear relation

$$\sum a_i w_i + b\ \mathbf{v} = \mathbf{0}_V$$

Note that $b = 0$, or else $\mathbf{v} = -\frac{1}{b}(\sum a_i w_i) \in \text{span}(L)$, which is a contradiction. Hence, $\sum a_i w_i = 0$, which implies that all $a_i = 0$ as L is a linearly independent set. If L' spans, we are done. If not, there is a vector $\mathbf{v}' \in S$ such that $\mathbf{v}' \notin \text{span}(L')$. Then, since S is finite this process will terminate, and when it terminates the final linearly independent set $\overline{L}$ will contain S in its span, so $V = \text{span}(S) = \text{span}(\overline{L})$, and hence we have constructed a basis. ■

Theorem 3.44 (Main Theorem)**.** *If $S = \{v_1, ..., v_n\}$ spans V and $L = \{w_1, ..., w_m\}$ is linearly independent, then $n \geq m$.*

Proof. Since S spans V, we may write every element

$$w_j = \sum_{i=1}^{n} a_{ij} v_i$$

Next, try to make a non-trivial linear relation on the w_j.

$$\mathbf{0}_V = \sum_{j=1}^{m} c_j w_j = \sum_{j=1}^{m} c_j \left(\sum_{i=1}^{n} a_{ij} v_i \right) = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} a_{ij} c_j \right) v_i$$

If we can arrange that

$$\sum_{j=1}^{m} a_{ij} c_j = 0$$

for all i with some $c_j \neq 0$, then the w_j could not be linearly independent. This is n linear equations (the i's) with m unknowns (the j's). If $m > n$ (more unknowns, c_j, then the $i-$equations) we can find a non-trivial solutions. Hence, if $m > n$, we arrive at a contradiction, so $n \geq m$, as desired. ■

Proposition 3.45 (Linear Equations Unknowns and Equations)**.** *Suppose we have a system of n equations and m unknowns. Then if $m > n$, we can reduce the system by Gaussian Elimination to a system with at most n pivots. ...*

Corollary 3.46. *All bases of V have the same number of elements, and that number of elements is by definition* $\dim(V)$*. Furthermore, all spanning sets S have $|S| \geq \dim(V)$, and if L is a linearly independent set then $|L| \leq \dim(V)$. Note that* $\dim(\{\ \boldsymbol{0}\}) = 0$.

Proof. Let B and B' be two bases of V. Since B spans and B' is linearly independent, $|B| \geq |B'|$, and since B' spans and B is linearly independent, $|B'| \geq |B|$. Therefore, $|B| = |B'|$. ■

Theorem 3.47. *Suppose W is a subspace of V (finite-dimensional), and $\{w_1, ..., w_m\}$ is a basis for W. Then, we may extend to a basis for V: $\{w_1, ..., w_m, v_{m+1}, ..., v_n\}$.*

Proof. W's basis is linearly independent in V, so it can be extended to a basis of V. ■

Observation 3.48. Since a subspace $W \subset V$ gives a homomorphism

$$f : V \to V/W \tag{3.10}$$

to the quotient space. In fact, $(f(v_{m+1}), ..., f(v_n))$ gives a basis for V/W. Consequently, $\dim(V) = \dim(W) + \dim(V/W)$. If we let $W' = \text{span}(v_{m+1}, ..., v_n)$, then W' is a subspace of V mapping isomorphically to V/W (Note, this can not be done for groups - in general?).

Proof. Suppose that W is a subspace of V with basis $(w_1, ..., w_m)$. We can then extend the basis of W to a basis of V as $(w_1, ..., w_m, v_{m+1}, ..., v_n)$. Let $W' = \text{span}(v_{m+1}, ..., v_n)$. Consider the canonical homomorphism $\pi : V \to V/W$. Suppose $\overline{v} \in V/W$. Then there exists $v \in V$ such that $\pi(v) = \overline{v}$. Furthermore, v can be represented uniquely as $v = a_1w_1 + ... + a_mw_m + a_{m+1}v_{m+1} + ... + a_nv_n$. It follows that

$$\begin{aligned}\overline{v} &= \pi(v) \\ &= \pi(a_1w_1 + ... + a_mw_m + a_{m+1}v_{m+1} + ... + a_nv_n) \\ &= a_1\pi(w_1) + ... + a_m\pi(w_m) + a_{m+1}\pi(v_{m+1}) + ... + a_n\pi(v_n) \\ &= a_{m+1}\pi(v_{m+1}) + ... + a_n\pi(v_n)\end{aligned}$$

Therefore, $\pi(W') = V/W$. Now, suppose we have a relation $b_{m+1}\pi(v_{m+1}) + ... + b_n\pi(v_n) = \overline{\mathbf{0}}$. Then it follows that $b_{m+1}v_{m+1} + ... + b_nv_n \in ker(\pi) = W$, so there exists c_i such that $b_{m+1}v_{m+1} + ... + b_nv_n = c_1w_1 + ...c_mw_m$. Moreover, we find that

$$b_{m+1}v_{m+1} + ... + b_nv_n - c_1w_1 - ... - c_mw_m$$

but since $(w_1, ..., w_m, v_{m+1}, ..., v_n)$ is a basis of V, $c_1 = ... = c_m = b_{m+1} = ... = b_n = 0$. Therefore, $(\pi(v_{m+1}), ..., \pi(v_n))$ gives a basis for V/W, and $\dim(V) = \dim(W) + \dim(V/W)$. Furthermore, since $W' \cap ker(\phi) = \emptyset$, we find that

$$\pi\Big|_{W'} : W' \to V/W \tag{3.11}$$

is a surjective homomorphism with a trivial kernel, so it is an isomorphism. ■

Example 3.49 (Counter-example for groups)**.** Take $\mathbb{Z}/2\mathbb{Z} \cong 2\mathbb{Z}/4\mathbb{Z} \subset \mathbb{Z}/4\mathbb{Z}$. The quotient group $(\mathbb{Z}/4\mathbb{Z})/(2\mathbb{Z}/4\mathbb{Z})$ is a cyclic group of order 2, but there does not exist an H in $\mathbb{Z}/4\mathbb{Z}$ mapping isomorphically to $2\mathbb{Z}/4\mathbb{Z}$ with the canonical projection.

3.4 Bases and Computation

3.4.1 Textbook

Let V be a finite-dimensional vector space over a field F, with a basis $S = (v_1, ..., v_n)$

Definition 3.50 (Coordinates)**.** For any vector $\mathbf{v} \in V$, we can express it uniquely as a linear combination

$$\mathbf{v} = \sum_{i=1}^{n} x_iv_i \tag{3.12}$$

with each $x_i \in F$. The scalars x_i are called the **coordinates** of $\mathbf{v}$ in the basis S. Then the column vector

$$[\ \mathbf{v}]_S = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \tag{3.13}$$

is called the **coordinate vector** of $\mathbf{v}$ with respect to the basis S.

Definition 3.51. If $V = F^n$, then S is a set of column vectors (in the standard basis), and we can convert any coordinate vector $[\ \mathbf{v}]_S$ to its representation in the standard basis by

$$[S][\ \mathbf{v}]_S = \begin{bmatrix} | & & | \\ v_1 & \dots & v_n \\ | & & | \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = x_1 v_1 + ...x_n v_n \tag{3.14}$$

Moreover, if a vector γ is given in the standard basis, we can find its coordinate vector with respect to S by solving the linear equation $[S][\gamma]_S = \gamma$.

Proposition 3.52. *Let S be a basis of F^n, and let $\gamma \in F^n$ be any vector. The coordinate vector of γ with respect to the basis S*

$$[\gamma]_S = [S]^{-1}\gamma \tag{3.15}$$

Proposition 3.53. *Let A be an $n \times n$ matrix with entries in a field F. The columns of A form a basis of F^n if and only if A is invertible.*

Proof. Denote the ith column vector of A by v_i. Then for any column vector $X = [x_1, ..., x_n]^T$, the matrix product $AX = x_1 v_1 + ...x_n v_n$ is a linear combination of the columns of A. Then, note that $AX = \mathbf{0}$ has only the trivial solution if and only if A is invertible. This implies that the columns of A are linearly independent if and only if A is invertible. Then, since A has n columns and $\dim(F^n) = n$, the columns of A are a basis of F^n if and only if they are invertible. ■

Definition 3.54 (Hyper Vector)**.** For an abstract vector space V we define the ordered set $(v_1, ..., v_n)$ as a hypervector. Then we define multiplication by an $n \times m$ matrix of scalars as

$$(v_1, ..., v_n)A = (w_1, ..., w_m) \tag{3.16}$$

where $w_j = a_{1j}v_1 + ... + a_{nj}v_n$.

Proposition 3.55. *Let $S = (v_1, ..., v_m)$ and $U = (u_1, ..., u_n)$ be ordered sets of elements in a vector space V. $U \subset \text{span}(S)$ if and only if there is an $m \times n$ matrix A such that $(v_1, ..., v_m)A = (u_1, ..., u_n)$.*

Observation 3.56. Given a basis $B = (v_1, ..., v_n)$ we can define an isomorphism of vector spaces

$$\Psi : F^n \to V, X \mapsto BX \tag{3.17}$$

This map is bijective due to each vector in V being able to be represented as a unique linear combination of the vectors in B. Moreover, this isomorphism allows us to introduce coordinates into our vector space V, where the coordinate vector of a vector $\mathbf{v}$ is $X = \Psi^{-1}(\mathbf{v})$ (Note that B^{-1} is not well-defined in this case, but the inverse isomorphism does indeed exist)

Corollary 3.57. *Every vector space V of dimension n is isomorphic to the column space F^n.*

Definition 3.58 (Change of Basis)**.** Suppose we have two bases $B = (v_1, ..., v_n)$ and $B' = (w_1, ..., w_n)$ of a vector space V. Note that every vector in B can be represented uniquely by a linear combination of the vectors in B'. Let P be an $n \times n$ coordinate matrix over F such that

$$(w_1, ..., w_n)P = (v_1, ..., v_n) \tag{3.18}$$

Where $v_j = v_{1j}w_1 + ... + v_{nj}w_n$. In other words, the jth column of P is the coordinate vector of the jth basis vector of B (v_j) with respect to the basis B'. Note that if we interchange the roles we can find a matrix P' so that

$$(v_1, ..., v_n)P' = (w_1, ..., w_n) \tag{3.19}$$

so $BP' = B'$. Then $B = B'P = BP'P$, so P is invertible with inverse P'. Let $P' = P_{B'}^{B}$ and $P = P_{B}^{B'}$. Then, let $[v]_B$ be the coordinate vector of v with respect to B, so $v = B[v]_B$. Then it follows that $v = B'P_B^{B'}[v]_B$, so $[v]_{B'} = P_B^{B'}[v]_B$

Corollary 3.59. *Let B be a basis of a vector space V.The other bases are the sets of the form $B' = BP^{-1}$, where $P \in GL_n(F)$ is an invertible matrix.*

Corollary 3.60. *The general linear group $GL_2(\mathbb{Z}/p\mathbb{Z})$ has order $p(p+1)(p-1)^2$.*

Proof. The previous corollary establishes a bijective correspondence between bases of F^n and elements in $GL_n(F)$. ■

3.4.2 Lecture

Recall (Important). We know that if we start with a finite dimensional vector space V, and a linearly independent subset $S = \{v_1, ..., v_n\}$, then S can be extended to a basis $\{v_1, ..., v_n, v_{n+1}, ..., v_m\}$ of V.

Remark 3.61 (Consequences). .

1. Let W be the subspace of V spanned by $\{v_1, ..., v_n\}$, and let W' be the subspace spanned by $\{v_{n+1}, ..., v_m\}$. Then $W \cap W' = \{0\}$, and for $W \times W' := \{(w, w'), w \in W, w' \in W'\}$ we have a linear isomorphism $\iota : W \times W' \to V$ given by $(w, w') \mapsto w + w'$. The fact that $W \cap W' = \{0\}$ follows immediately from the linear independence of the combined bases of W and W'. The fact that ι is a homomorphism follows from the vector space structure for a product space. Then, since the union of the bases of W and W' is a basis, every vector can be written as a unique linear combination of the unioned basis vectors, so surjectivity follows from spanning and injectivity follows from spanning.

2. If $W \subset V$ is some subspace of V, then there is another subspace $W' \subset V$, such that the composite map
$$W' \xhookrightarrow{w' \mapsto w'} V \xrightarrow{w' \mapsto w' + W} V/W \tag{3.20}$$
is an isomorphsim (where the second one is the canonical projection map). Why does this work? We take a basis $\{v_1, ..., v_n\}$ of W, extend to a basis $\{v_1, ..., v_m\}$ of V, and let $W' = \text{span}\{v_{n+1}, ..., v_m\}$. Surjectivity comes from definition of cosets and spanning, and injectivity comes from injectivity and the definition of V/W and W'.

3. Suppose $W \subset V$ is a subspace, then if we put results 1) and 2) together, we obtain an isomorphism
$$V \xrightarrow{\sim} W \times V/W \tag{3.21}$$
(Why do 1) and 2) come together to give this). Therefore, we can understand to be "complements" in a way. Note that this implies $\dim(V) = \dim(W) + \dim(V/W)$.

4. If $f : V \to U$ is a linear transformation, then $V \xrightarrow{\sim} \ker(f) \times \text{im}(f)$, and $\dim(V) = \dim(\ker(f)) + \dim(\text{im}(f))$. Why? The First Isomorphism Theorem for Groups implies that given a linear homomorphism $f : V \to W$, the map $\overline{f} : V/\ker(f) \xrightarrow{\sim} \text{im}(f)$, $v + \ker(f) \mapsto f(v)$, is a well-defined linear isomorphism.

Remark 3.62 (Problem for Groups). Given $f : G \to G'$, find $\ker(\phi)$ and $\text{im}(\phi)$ - in general this is very difficult! But in the case of vector spaces, we can solve this using bases, matrices, and matrix algorithms.

Remark 3.63 (Correspondences). .

1. We know that if V is an n dimensional vector space over a field F, then ordered bases correspond one-to-one to isomorphisms between F^n and V. Suppose $B = (v_1, ..., v_n)$. Then we define an isomorphism $V \xrightarrow{\sim} F^n$ by

$$(v_1, ..., v_n) \mapsto \left[\begin{array}{c} \rho_B : F^n \to V \\ \begin{bmatrix} a_1 \\ \dots \\ a_n \end{bmatrix} \mapsto a_1 v_1 + ...a_n v_n \end{array} \right] \tag{3.22}$$

   Conversely, we have

$$\rho : F^n \to V \mapsto \left(\rho \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, ..., \rho \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix} \right) \tag{3.23}$$

   This works since ρ is an isomorphism.

2. Linear transformation $F^n \to F^m$ correspond in a one-to-one relationship with matrices in $M_{m \times n}(F)$. For a linear transformation $f : F^n \to F^m$ we take

$$f : F^n \to F^m \mapsto [f] = \begin{bmatrix} f \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} & \dots & f \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix} \end{bmatrix} \tag{3.24}$$

   Then, to go in the other direction we have

$$A \mapsto f : F^n \xrightarrow{v \mapsto Av} F^m \tag{3.25}$$

   We then note that $[c_1 f_1 + c_2 f_2] = c_1[f_1] + c_2[f_2]$ and $[f_1 \circ f_2] = [f_1][f_2]$,

3. Putting together 1) and 2): Given a linear transformation $f : V \to V'$, with $\dim(V) = n$, $\dim(V') = m$, and B being a basis of V and B' a basis of V'. We then define the matrix of f with respect to B and B':

$$[f]_B^{B'} = [\rho_{B'}^{-1} \circ f \circ \rho_B] \tag{3.26}$$

   Explicitly, if $B = (v_1, ..., v_n)$ and $B' = (w_1, ..., w_m)$, then for any j

$$f(v_j) = \sum_{i=1}^{m} a_{ij} w_i \tag{3.27}$$

   so $[f]_B^{B'} = (a_{ij})$. In summary, $Hom(V, V') = \{\text{set of linear transformations } V \to V'\} \xrightarrow{\sim} M_{m \times n}(F)$. Put explicitly, $[c_1 f_1 + c_2 f_2]_B^{B'} = c_1[f_1]_B^{B'} + c_2[f_2]_B^{B'}$ and for $f : V \to V'$ and $g : V' \to V''$ (with bases B, B', and B''), we have that

$$[g \circ f]_B^{B''} = [g]_{B'}^{B''}[f]_B^{B'} \tag{3.28}$$

Definition 3.64 (Change of Basis)**.** Suppose V is a vector space with bases B_1 and B_2, and a vector space V' with bases B_1' and B_2'. Then take $f : V \to V'$ as a linear homomorphism. Then

$$\begin{aligned}[f]_{B_2}^{B_2'} &= [\rho_{B_2'}^{-1} \circ f \circ \rho_{B_2}] \\ &= [\rho_{B_2'}^{-1} \circ \rho_{B_1'} \circ \rho_{B_1'}^{-1} \circ f \circ \rho_{B_1} \circ \rho_{B_1}^{-1} \circ \rho_{B_2}] \\ &= [\rho_{B_2'}^{-1} \circ \rho_{B_1'}][\rho_{B_1'}^{-1} \circ f \circ \rho_{B_1}][\rho_{B_1}^{-1} \circ \rho_{B_2}] \\ &= [\rho_{B_2'}^{-1} \circ \rho_{B_1'}][f]_{B_1}^{B_1'}[\rho_{B_1}^{-1} \circ \rho_{B_2}]\end{aligned}$$

We call something of the forom $[\rho_{B_1}^{-1}\rho_{B_2}]$ a change of basis matrix. If $V = V'$, then

$$[f]_{B_2}^{B_2} = [\rho_{B_1}^{-1}\rho_{B_2}]^{-1}[f]_{B_1}^{B_1}[\rho_{B_1}^{-1}\rho_{B_2}] \tag{3.29}$$

Note, if $B_1 = (v_1, ..., v_n)$ and $B_2 = (w_1, ..., w_n)$, then

$$[\rho_{B_1}^{-1}\rho_{B_2}] = (c_{ij}) \tag{3.30}$$

where

Definition 3.65 (Group of Linear Isomorphisms)**.** Let V be a vector space. Then we define $GL(V) := \{\text{linear isomorphisms } V \to V\}$. In other words, they are the invertible linear transformations $V \to V$, or $Hom(V, V)^\times$. Therefore, given a basis B of V, we have seen that we can rewrite this isomorphically as the set of invertible matrices in $M_{n\times n}(F) = GL_n(F)$, where $\dim(V) = n$.

Question. What is the image of a linear transformation in term of matrices? It is the column space of a matrix. Similarly, the null space of a matrix is the kernel of our linear transformation.

3.5 The Dimension Formula

3.5.1 Textbook

Definition 3.66 (Linear Homomorphisms)**.** A homomorphism of vector spaces of a field F is a map $T : V \to W$ between vector spaces over F which is compatible with addition and multiplication:

$$T(c_1v_1 + c_2v_2) = c_1T(v_1) + c_2T(v_2), \forall c_1, c_2 \in F, \forall v_1, v_2 \in V \tag{3.31}$$

This type of map is called a **linear transformation**, and in general, it can be shown by induction that the image of the linear combination is the linear combination of the images:

$$T\left(\sum_i c_iv_i\right) = \sum_i c_iT(v_i) \tag{3.32}$$

Example 3.67. .

1. Left multiplication by an $m \times n$ matrix A induces a linear transformation $T_A : F^n \xrightarrow{v \mapsto Av} F^m$.
2. Let P_n be a vector space of real polynomials of degree $\leq n$ of the form $a_n x^n + ... + a_1 x + a_0$. Then the derivative is a linear transformation from P_n to P_{n-1}.

Remark 3.68. The image and kernel of a linear transformation $T : V \to W$ induce two subspaces, with $\ker(T) \subset V$ and $\text{im}(T) \subset W$.

Theorem 3.69 (Dimension Formula)**.** *Let $T : V \to W$ be a linear transformation, and assume that V is finite-dimensional. Then*

$$\dim(V) = \dim(\ker(T)) + \dim(\text{im}(T)) \tag{3.33}$$

Where we often denote $\dim(\ker(T)) = \text{nullity}(T)$ *and* $\dim(\text{im}(T)) = \text{rank}(T)$.

Proof. Suppose V is a vector space with $\dim(V) = n$. Let $(u_1, ..., u_k)$ be a basis for $\ker(T)$, and extend it to a basis of V

$$(u_1, ..., u_k; v_1, ..., v_{n-k}) \tag{3.34}$$

Let $w_i = T(v_i)$ for $i = 1, ..., n-k$. If we prove that $(w_1, ..., w_{n-k}) = S$ is a basis for $\text{im}(T)$, then it will follow that $\text{rank}(T) = n - k$. Let $w \in \text{im}(T)$ be arbitrary. Then there exists $v \in V$ such that $w = T(v)$. We then write v in terms of the basis

$$v = a_1 u_1 + ... + a_k u_k + b_1 v_1 + ... + b_{n-k} v_{n-k} \tag{3.35}$$

and apply T, which gives

$$w = 0 + ... + 0 + b_1 T(v_1) + ... + b_{n-k} T(v_{n-k}) \tag{3.36}$$

Thus, w is in the span of S, so S spans $\text{im}(T)$. Next, suppose we have a linear relation

$$c_1 w_1 + ... + c_{n-k} w_{n-k} = 0 \tag{3.37}$$

and we consider the linear combination $v = c_1 v_1 + ... + c_{n-k} v_{n-k}$, where v_i are basis vectors. Applying T to v gives $T(v) = 0$, so $v \in \ker(T)$. Thus, v can be expressed as $v = a_1 u_1 + ... + a_k u_k$, which gives the linear relation

$$-a_1 u_1 - ... - a_k u_k + c_1 v_1 + ... + c_{n-k} v_{n-k} = 0 \tag{3.38}$$

But since these vectors form a basis, this relation must be trivial, so $a_1 = ... = a_k = c_1 = ... = c_{n-k} = 0$. Therefore, our above relation is trivial so S is linearly independent, and hence forms a basis for $\text{im}(T)$. ■

Proposition 3.70. *Suppose that A is an $m \times n$ matrix and B is a vector in the image space of left multiplication by A such that for the equation $AX = B$, there exists at least one solution $X = X_0$. Let K denote the space of solutions of the homogeneous equation $AX = 0$. Then the set of solutions to the equation $AX = B$ is the coset $X_0 + K$.*

3.6 Matrix of a Linear Transformation

3.6.1 Textbook

Definition 3.71 (Matrix Representation for Canonical Vector Spaces)**.** Given a linear transformation $T : F^n \to F^m$, we construct a matrix representation A over the standard bases of F^n and F^m by taking

$$T(X) = \sum_{j=1} T(e_j)x_j = \begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix} x_1 + ... + \begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix} x_n = AX \tag{3.39}$$

Definition 3.72 (Matrix Representation for Arbitrary Vector Spaces)**.** Let $T : V \to W$ be a linear transformation. Let $B = (v_1, ..., v_n)$ and $C = (w_1, .., w_m)$ be bases of V and of W. Let us use the shorthand $T(B)$ for the hypervector $T(B) = (T(v_1), T(v_2), ..., T(v_n))$. Since this hypervector is in W and C is a basis of W, we have an $m \times n$ matrix A such that

$$(w_1, ..., w_m)A = (T(v_1), ..., T(v_n)) \tag{3.40}$$

or in short hand, $CA = T(B)$. Recall this means for each $j = 1, ..., n$

$$T(v_j) = \sum_{i=1}^{m} w_i a_{ij} \tag{3.41}$$

This matrix A is the matrix of T with respect to the bases B and C. We can find the then find the coordinate vector of $T(v)$ by

$$T(v) = T(v_1)x_1 + \ldots + T(v_n)x_n = T(B)X = CAX \tag{3.42}$$

So the coordinate vector of $T(v)$ is $Y = AX$.

Remark 3.73 (Isomorphism Perspective). The relationship between a linear transformation $T : V \to W$ and its matrix representation A can be explained by isomorphisms $\psi : F^n \to V$ and $\psi' : F^m \to W$ determined by the choice of bases for V and W ($(\phi(e_1), ..., \phi(e_n))$ and $(\phi'(e_1), ..., \phi'(e_m))$ correspond to our choices of bases).

$$\begin{array}{ccc} V & \xrightarrow{T} & W \\ {\scriptstyle\psi}\uparrow & & \uparrow{\scriptstyle\psi'} \\ F^n & \xrightarrow{\text{mult by A}} & F^m \end{array} \quad , \quad \begin{array}{ccc} \mathbf{B}X & \to & \mathbf{C}AX \\ \uparrow & & \uparrow \\ X & \longrightarrow & AX \end{array} \tag{3.43}$$

Remark 3.74. We say that these diagrams commute, so $T \circ \phi = \phi' \circ A$.

Definition 3.75 (Changing Bases)**.** Let $B' = (v'_1, ..., v'_n)$ and $C' = (w'_1, ..., w'_m)$ be new bases of V and W. We can relate the new bases to the old one's using a matrices $P \in GL_n(F)$ and $Q \in GL_m(F)$ by $PX = X'$ and $QY = Y'$, where the non-primed letters are coordinate vectors in the old bases. Let A' be the matrix of T with respect to these new bases. $A'X' = Y'$, and $QAP^{-1}X' = QAX = QY = Y'$, so $A' = QAP^{-1}$.

Proposition 3.76. *Let A be a matrix of a linear transformation T with respect to some given bases B and C. The matrices A' which represents T with respect to other bases are of the form*

$$A' = QAP^{-1} \tag{3.44}$$

where $Q \in GL_m(F)$ and $P \in GL_n(F)$ are arbitrary invertible matrices. Given any $m \times n$ matrix A, there exist matrices $Q \in GL_m(F)$ and $P \in GL_n(F)$ so that QAP^{-1} has the form

$$\left[\begin{array}{c|c} I_r & \boldsymbol{0} \\ \hline \boldsymbol{0} & \boldsymbol{0} \end{array}\right] \tag{3.45}$$

3.7 Bases and Linear Operators

3.7.1 Textbook

Definition 3.77 (Linear Operator)**.** A linear transformation $T : V \to V$ is called a linear operator on V.

Remark 3.78. For linear operators we want to find a matrix when we pick only one basis $B = (v_1, ..., v_n)$ fo V. We then write

$$T(B) = BA \tag{3.46}$$

or

$$T(v_j) = \sum_{i=1}^{n} v_i a_{ij} \tag{3.47}$$

This defines the matrix $A = (a_{ij})$. In other words, A is a square matrix whose jth column is the coordinate vector of $T(v_j)$ with respect to the basis B. If X and Y denote the coordinate vectors of v and $T(v)$ respectively, then $Y = AX$.

Proposition 3.79 (Changing Bases)**.** *Suppose we have a new basis $B' = (v'_1, ..., v'_n)$. Then if A is the matrix of the linear operator T with respect to the basis B, and A' is the matrix which represents T in the new basis B', then*

$$A' = PAP^{-1} \tag{3.48}$$

for some $P \in GL_n(F)$.

Definition 3.80 (Invariant Subspace)**.** Let $T : V \to V$ be a linear operator on a vector space. A subspace W of V is called an **invariant subspace** or a **T-invariant subspace** if it is carried to itself by the operator:

$$TW \subset W \tag{3.49}$$

In other words, W is T-invariant if $T(w) \in W$ for all $w \in W$. When this is so, T defines a linear operator on W called the **restriction** of T to W.

Corollary 3.81. *Let $T : V \to V$ be a linear operator and let W be an invariant subspace. Then, let $(w_1, ..., w_k)$ be a basis for W. We extend it to a basis $B = (w_1, ..., w_k, v_1, ..., v_{n-k})$ of V. Then, the fact that W is invariant can be read off from the matrix M representing T with respect to the basis B by the fact that the columns of the matrix are the coordinate vectors of the images of the basis vectors, and since $T(w_j)$ is in W, it's a linear combination of $(w_1, ..., w_k)$. It follows that M as a block matrix is*

$$M = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix} \tag{3.50}$$

where A is a $k \times k$ matrix. Moreover, A is the matrix of the restriction of T to W with respect to the basis $(w_1, ..., w_k)$.

Proposition 3.82. *Suppose that $V = W_1 \oplus W_2$ is the direct sum of two T-invariant subspaces, and B_i is a basis of W_i. Then we can make a basis B of V by adjoining the bases B_1 and B_2. In this case, the matrix of T with respect to B will be in block diagonal form*

$$M = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix} \tag{3.51}$$

Where A_i is the matrix of T restricted to W_i.

Definition 3.83 (Eigenvectors)**.** An **eigenvector** v for a linear operator T is a nonzero vector such that

$$T(v) = cv \tag{3.52}$$

for some scalar $c \in F$. Here c is called the **eigenvalue** associated to the eigenvector v.

Corollary 3.84. *Let v be an eigenvector for a linear operator T. Then the subspace W spanned by v is T-invariant, because $T(av) = acv \in W$ for all $a \in F$. Conversely, if this subspace is invariant, then v is an eigenvector. Thus, an eigenvector is a basis of a T-invariant one-dimensional subspace.*

Corollary 3.85. *Similar or conjugate matrices have the same eigenvalues.*

Proposition 3.86. *The basis vector v_j is an eigenvector of T, with eigenvalue c, if and only if the jth column of A has the form ce_j, for the matrix A is defined by the property $T(v_j) = v_1a_{1j} + ... + v_na_{nj}$, so if $T(v_j) = cv_j$ then $a_{jj} = c$ and $a_{ij} = 0$ for $i \neq j$.*

Corollary 3.87. *With the above notation, the matrix A of a linear operator T with respect to a basis B is diagonal if and only if B is a basis of eigenvectors of T.*

Corollary 3.88. *The matrix A of a linear transformation is similar or conjugate to a diagonal matrix if and only if there is a basis $B' = (v'_1, ..., v'_n)$ of V made up of eigenvectors.*

Lemma 3.89. *The following conditions on a linear operator $T : V \to V$ on a finite dimensional vector are equivalent:*

1. $\text{nullity}(T) > 0$
2. $\text{rank}(T) < \dim(V)$
3. *If A is the matrix of the operator with respect to an arbitrary basis, then* $\det(A) = 0$
4. *0 is an eigenvalue of T*

Definition 3.90 (Singular and Non-Singular)**.** A linear operator T on a finite-dimensional vector space V is called **singular** if it satisfies any of the equivalent conditions in the above lemma. Otherwise, T is **nonsingular**

Proposition 3.91. *The operator T has an eigenvalue c if and only if the operator $T - cI$ has a non-zero kernel.*

Corollary 3.92. *The eigenvalues of a linear operator T are scalars $c \in F$ such that $T - cI$ is singular.*

Definition 3.93 (Characteristic Polynomial)**.** The **characteristic polynomial** of a linear operator T is the polynomial

$$p(t) = \det(tI - A) \tag{3.53}$$

where A is the matrix of T with respect to some basis. Then, $c \in F$ is an eigenvalue if and only if $p(c) = 0$.

Corollary 3.94. *The eigenvalues of a linear operator are the roots of its characteristic polynomial.*

Corollary 3.95. *The eigenvalues of an upper or lower triangular matrix are its diagonal entries.*

Proposition 3.96. *The characteristic polynomial of an operator T does not depend on the choice of basis.*

Proposition 3.97. *The characteristic polynomial $p(t)$ has the form*

$$p(t) = t^n - (\operatorname{tr} A)t^{n-1} + (\textit{intermediate terms}) + (-1)^n(\det A) \tag{3.54}$$

Proposition 3.98. *Let T be a linear operator on a finite-dimensional vector space V.*

1. *If V has dimension n, then T has at most n eigenvalues.*
2. *If F is a field of complex numbers and $V \neq \{0\}$, then T has at least one eigenvalue, and hence it has an eigenvector.*

3.7.2 Lecture

Let V and W be finite dimensional vector spaces over the field F. Let $T : V \to W$ is a linear transformation.

Example 3.99. Let $V = F[x]_{deg \leq n}$ and $W = F[x]_{deg \leq n-1}$, then $T : \frac{d}{dx} : V \to W$ is a linear operator. Moreover, the **total derivative of a function** $f : \mathbb{R}^n \to \mathbb{R}^m$ is a linear map. What is $\ker\left(\frac{d}{dx}\right)$ when $F = \mathbb{Z}/p\mathbb{Z}$? Well, $F \subset \ker(T)$. But, if $n \geq p$, we also have x^p in the kernel, since

$$\frac{d}{dx}(x^p) = px^{p-1} = 0 \tag{3.55}$$

Definition 3.100 (Kernel and Image)**.** We define

$$\ker(T) := \{v \in V : T(v) = 0\} \subset V \tag{3.56}$$

and

$$\text{im}(T) := \{w \in W : w = T(v)\} \subset W \tag{3.57}$$

Theorem 3.101 (Dimension Formula)**.**

$$\dim(V) = \dim(\ker(T)) + \dim(\text{im}(T)) \tag{3.58}$$

Proof. Let $\{v_1, ..., v_k\}$ be a basis of $\ker(T)$. Then since it is linearly independent, we can extend it to a basis $\{v_1, ..., v_k, v_{k+1}, ..., v_n\}$ of V. Then, let $w_i = T(v_{k+i})$ for all $i = 1, ..., n-k$. Note that the set $\{w_1, ..., w_{n-k}\}$ spans $\text{im}(T)$ since

$$w = T(v) = T\left(\sum_{i=1}^{k} a_i v_i + \sum_{k+1}^{n} b_i v_i\right) = \sum_{i=1}^{k} a_i T(v_i) + \sum_{k+1}^{n} b_i T(v_i) = \sum_{k+1}^{n} b_i w_i \tag{3.59}$$

for any $w \in \text{im}(T)$. Now, suppose we have a linear relation $\sum b_i w_i = 0_W$. Consider the vector $v_0 = \sum_{i=1}^{n-k} b_i v_{i+k}$ in V. Then by our linear relation, $T(v_0) = 0_W$. Therefore, by definition $v_0 \in \ker(T)$, so we can express it as $v_0 = \sum_{i=1}^{k} a_i v_i = \sum_{i=1}^{n-k} b_i v_{i+k}$. This give the linear relation

$$\sum_{i=1}^{k} a_i v_i - \sum_{i=1}^{n-k} b_i v_{i+k} = 0_V \tag{3.60}$$

This is a linear relation on a basis of V, so all $a_i = 0$ and $b_i = 0$. Therefore, the set $\{w_1, ..., w_{n-k}\}$ is linearly independent. Thus $\{w_1, ..., w_{n-k}\}$ is a basis, and the proof is complete. ■

Corollary 3.102. *If V is finite-dimensional and $W \subset V$ is a subspace, then* $\dim(W) + \dim(V/W) = \dim(V)$

Proof. There exists a canonical homomorphism $T : V \to V/W$, $v \mapsto v + W$, which is surjective with kernel W. ■

Notation 3.103. The dimension of the image is also known as the **rank** of T, and the dimension of the kernel is known as the **nullity** of T.

Definition 3.104 (Linear Operators and Bases)**.** Let $\{v_1, ..., v_n\}$ be a basis of V and $\{w_1, ..., w_m\}$ be a basis of W. Then the basis of V corresponds to a lienar isomorphism $V \to F^n$ which takes any $v = \sum_{i=1}^{n} a_i v_i \mapsto [a_1 ... a_n]^T$. (A choice of a basis gives you an isomorphism between any abstract space to the canonical vector space of the same dimension). A similarly isomorphism arises for the basis of W.

Question. What does $T : V \to W$ look like once these isomorphisms have been chosen?

$$\begin{array}{ccc} V & \xrightarrow{\sim} & F^n \\ {\scriptstyle T}\downarrow & & \vdots \\ W & \xrightarrow[\sim]{} & F^m \end{array}$$

Answer. Each $T(v_j) = \sum_{i=1}^{m} a_{ij} w_i$ for $j = 1, 2, ..., n$, where $a_{ij} \in F$ are determined by T and the choice of bases (By the fact that the w_i form a basis of W). Conversely, the scalars $\{a_{ij}\}_{i=1,j=1}^{i=m,j=n}$ determine T uniquely. Why? Because we write $v = \sum_{j=1}^{n} x_j v_j$, so

$$T(v) = \sum_{j=1}^{n} x_j \left(\sum_{i=1}^{m} a_{ij} w_i \right) \tag{3.61}$$

If we define A to be the $m \times n$ matrix (a_{ij}), which means we put the coordinate of the image of v_j in the jth column

$$A = \begin{bmatrix} & & | & & \\ \dots & \dots & [T(v_j)]_W & \dots & \dots \\ & & | & & \end{bmatrix} \tag{3.62}$$

Then, if we write $T(v) = \sum_{i=1}^{m} y_i w_i$, with $y_i = \sum_{j=1}^{n} a_{ij} x_j$ really is the formula

$$\begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix} = Y = AX = A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \tag{3.63}$$

Therefore, associated to a linear transformation and the choices of bases for the domain and codomain is a set of mn scalars which we put in a matrix, and the linear transformation is given by left multiplying the vector by A.

$$\begin{array}{ccc} V & \xrightarrow{\sim} & F^n \\ {\scriptstyle T}\downarrow & & \vdots \text{ left multiplication by } A \\ W & \xrightarrow[\sim]{} & F^m \end{array}$$

Example 3.105. Take $T : V \to W$ with V with a basis $\{v_1, v_2\}$ and W has a basis $\{w_1, w_2\}$, and $T(v_1) = 2w_1$ and $T(v_2) = 3w_1 + 4w_2$. Then the matrix is

$$A = \begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix} \tag{3.64}$$

Let $v = 7v_1 + 8v_2$. Then

$$[T(v)] = A[7\ 8]^T = [38\ 32]^T \tag{3.65}$$

Which implies that $T(v) = 38w_1 + 32w_2$.

Remark 3.106 (Special Case). If we have a linear transformation $T : V \to V$ (an **endomorphism** - a homomorphism from a vector space to itself) and consider one basis $B = \{v_1, ..., v_n\}$, then we get a square matrix $A = [T]_B$. Moreover, if we have another endomorphism $S : V \to V$, and S has matrix B (n by n), then the matrix for $S \circ T : V \to V$ is $B \cdot A$ given by matrix multiplication (this is how matrix multiplication is derived as the composition of linear operators).

Proposition 3.107. *For a transformation $T : V \to V$, the following are equivalent:*

1. *T is an automorphism of vector spaces*
2. $\ker(T) = \{0_V\}$
3. $\text{im}(T) = V$
4. *If the matrix A of T, with respect to $\{v_1, ..., v_n\}$ is A, then A is invertible*
5. $\det(A) \neq 0$ *in F.*

Definition 3.108. The set of all $T : V \to V$ which are isomorphisms forms a group $GL(V)$, and is isomorphic to $GL_n(F)$, where $\dim(V) = n$. So really, $GL_n(F)$ can be thought of as invertible linear transformations of an n-dimensional vector space over the field F.

Example 3.109. Let $F = \mathbb{Z}/2$. What is the group $GL_2(F)$. Note we have 16 choices of 2×2 matrices over F, but only six of them are invertible. Moreover, $GL_2(F) \cong S_3$.

Definition 3.110 (Change of Basis)**.** If A is the matrix of a transformation $T : V \to V$ with respect to the basis $B = \{v_1, ..., v_n\}$, what is the matrix with respect to the basis $B' = \{v_1', ..., v_n'\}$ A'? Then $A' = PAP^{-1}$, where P is the invertable $n \times n$ matrix giving the change of basis. A' is also called the conjugate matrix.

Remark 3.111. The advantage of the (V, T) point of view over the (F^n, A) point of view is by choosing a convenient basis, we can get a simpler form for our operator.

Example 3.112 (Two Bases)**.** From our first proposition: $T : V \to W$.
There exists a basis of V and a basis of W so that the matrix of T is

$$\begin{bmatrix} \begin{bmatrix} 1_1 & & & 0 \\ & 1_2 & & \\ & & \ddots & \\ 0 & & & 1_r \end{bmatrix} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \tag{3.66}$$

where $r = rank(T)$. We take basis $\{v_{k+1}, ..., v_n, v_1, ..., v_k\}$ where the first part maps to the basis of the image, the second part maps to the kernel, and for W we take $\{T(v_{k+1}), ..., T(v_n), ...\}$.

Example 3.113 (One Basis)**.** A more interesting case is for $T : V \to V$.
We seek to find a basis of **eigenvectors** so that $T(v) = cv$. If we found a basis of such, then we find the matrix

$$A = \begin{bmatrix} c_1 & & & 0 \\ & c_2 & & \\ & & \ddots & \\ 0 & & & c_n \end{bmatrix} \tag{3.67}$$

Question. Let $T : V \to V$ be a linear operator. Can we fina good basis so that the matrix A of T is in simple form?

Definition 3.114 (T-Invariant)**.** An **invariant subspace** $W \subset V$ is a subspace such that $T(W) \subset W$. If you make a matrix A of T with respect to a basis extended from a basis of W, then

$$A = \left[\begin{array}{c|c} a & b \\ \hline 0 & d \end{array}\right] \tag{3.68}$$

so the first basis vectors are in W, and so are the $T(w_i)$.

Definition 3.115 (Invariant Complement)**.** Suppose W is a T-invariant subspace of V, and it has an **invariant complement** W', which implies each element of V can be denoted uniquely by the sum of a vector in W and a vector in W', and we denote it by the **direct sum** $V = W \oplus W'$. Then, the matrix A of the transformation with respect to a basis of V obtained from adjoining a basis of W to a basis of W' has the form

$$A = \left[\begin{array}{c|c} a & 0 \\ \hline 0 & d \end{array}\right] \tag{3.69}$$

Remark 3.116. An extreme case of this is if W is one dimensional, $W = Fw := \{cw : c \in F\}$, and is invariant, then $Tw = cw$. We then say that w is an eigenvector of T with associated eigenvector c. If there is a basis $\{v_1, ..., v_n\}$ of V consisting of eigenvectors with eigenvalues $c_1, .., c_n$, then the associated matrix for T is

$$A = \begin{bmatrix} c_1 & & & 0 \\ & c_2 & & \\ & & \ddots & \\ 0 & & & c_n \end{bmatrix} \tag{3.70}$$

The eigenbasis gives a decomposition of the space into lines (one-dimensional vector spaces), each stable under T, such that V is the direct sum of those lines, and the matrix of T can be represented very simply.

Example 3.117 (Counter-Example)**.** .

1. Consider the rotation of $\mathbb{R}^2$ by an angle θ. In the standard basis, the matrix representation of the rotation is
$$A = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \tag{3.71}$$

2. Here, the transformation has no eigenvectors. Consider the linear operator $T : F^2 \to F^2$ so that $T(e_1) = e_1$ and $T(e_2) = e_1 + e_2$, so it has a matrix over the standard basis of the form
$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \tag{3.72}$$
There is no basis of eigenvectors (There is no complement W' which is T-invariant where $W = Fe_1$).

Question. Given T, what are the possible eigenvalues?

Answer. If $Tw = cw$, and you consider the new operator $(T - cI)$, then $(T - cI)w = 0$. In other words, w is in the kernel of the linear operator $T - cI$. So, $T - cI$ is not invertible since it has a non-trivial kernel. Conversely, if $T - cI$ has a kernel (or just is not invertible) then c is an eigenvalue for T.

Remark 3.118. The set of eigenvalues is equal to the set of $c \in F$ such that $T - cI$ is not invertible. This is equivalent to $\det(A - cI) = 0$, where A is the matrix of T with respect to some basis.

Definition 3.119 (Characteristic Polynomial)**.** Consider the determinant $\det(tI - A)$, where

$$tI - A = \begin{bmatrix} t - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & t - a_{22} & & \vdots \\ \vdots & & \ddots & \\ -a_{n1} & \dots & & t - a_{nn} \end{bmatrix} \tag{3.73}$$

Then $\det(tI - A) = t^n - (a_{11} + a_{22} + ... + a_{nn})t^{n-1} + ... + (-1)^n \det A = p(t)$ is a polynomial in t of degree n with coefficients in the field F. This is the **characteristic polynomial of T**, where its roots c are the eigenvalues of T.

Observation 3.120. Tbe characteristic polynomial $p(t)$ depends only on T, not on the basis of V used to obtain the matrix A to calculate it. If we used a different basis, then we get $A' = PAP^{-1}$. Observe that

$$\det(tI - A') = \det\big(tI - PAP^{-1}\big) = \det\big(P(tI - A)P^{-1}\big) = \det(P)p(t)\det\big(P^{-1}\big) = p(t) \tag{3.74}$$

Lemma 3.121. *If $p(t)$ has degree n over a field F, then it has at most n distinct roots c in F.*

Proof. By the Euclidean Algorithm for polynomials, $f(t) = (t - c)g(t) + d$ with $\deg g(t) = n - 1$, $d \in F$. If $f(c) = 0$, then $d = 0$, so $f(t) = (t - c)g(t)$. If c' is another root with $c' \neq c$, then $g(c') = 0$. Then, we use induction on the degree of g. ■

Corollary 3.122. *The roots of the characteristic polynomial are eigenvalues, so we have at most n distinct eigenvalues, where $n = \dim(V)$.*

Example 3.123. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then $p(t) = t^2 - (a + d)t + (ad - bc)$.

Example 3.124. Let $A = \begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix}$, then $p(t) = t^2 - 7t + 10$, so it has eigenvalues 2 and 5. Then if $2 \neq 5$ in F, then we obtain a basis of eigenvectors.

Corollary 3.125. *If your characteristic polynomial factors as $p(t) = (t-c_1)(t-c_2)...(t-c_n)$ with $c_i \neq c_j$, $i \neq j$, then you have a basis of eigenvectors for your linear operator.*

Remark 3.126. Take a linear operator $T : V \to V$ on a finite-dimensional vector space, then it gives a vector in $Hom(V, V)$ (a vector space of all linear maps over V, where if $\dim(V) = n$, then $\dim(Hom(V, V)) = n^2$). Consider $\{I, T, T^2, ..., T^{n^2}\}$. Since there are $n^2 + 1$ of them, they must be linearly dependent. Thus, there must be a linear relation

$$a_0 I + a_1 T + a_2 T^2 + ... + a_{n^2} T^{n^2} = 0 \tag{3.75}$$

in $Hom(V, V)$, where 0 is the zero operator. In other words T satisfies a polynomial of degree $\leq n^2$ with coefficients in F. If we let $F(t) = a_0 + a_1 t + ... + a_{n^2} t^{n^2}$, then $F(T) = 0$.

Theorem 3.127 (Caley-Hamilton Theorem)**.** *T always satisfies its own characteristic polynomial (a polynomial of degree n).*

Proof. When $f(t) = (t - c_1)(t - c_2)...(t - c_n)$, where all c_i are distint. Then we can find a matrix representation of T with the eigenvalues along the diagonal, and all other entries zero. Then, $f(A) = (A - c_1 I)(A - c_2 I)...(A - c_n I) = 0$ since each matrix binomial will have its ith row will be zero, where i corresponds to the c_i of the binomial. ■

Example 3.128. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then $p(t) = t^2 - (a + d)t + (ad - bc)$. Then $A^2 = \begin{bmatrix} a^2 + bc & ab + bd \\ ac + dc & bc + d^2 \end{bmatrix}$. Plugging A^2 into the characteristic polynomial we obtain

$$p(A) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \tag{3.76}$$

3.8 Orthogonal Matrices and Groups

3.8.1 Textbook

Remark 3.129. In $\mathbb{R}^3$, a rotation about the origin can be described by a pair (v, θ) consisting of a unit vector v, which lies in the axis of rotation, and a nonzero angle θ.

Definition 3.130 (Orthogonal Matrix)**.** A real $n \times n$ matrix A is said to be orthogonal if $A^T = A^{-1}$, or equivalently if $A^T A = I$. The orthogonal $n \times n$ matrices form a subgroup of $GL_n(\mathbb{R})$ denoted by O_n and called the orthogonal group:

$$O_n := \{A \in GL_n(\mathbb{R}) : A^T A = I\} \tag{3.77}$$

The determinant of an orthogonal matrix is ± 1 since $A^T A = I$ implies that

$$(\det(A))^2 = \det(A) \det\left(A^T\right) = 1 \tag{3.78}$$

Remark 3.131. The orthogonal matrices having determinant +1 form a subgroup called the **special linear orthogonal group**, and denoted

$$SO_n := \{A \in GL_n(\mathbb{R}) : A^T A = I, \det(A) = 1\} \tag{3.79}$$

This subgroup has one coset in addition to SO_n, which is the set of elements with determinant -1. Thus, $[O_n : SO_n] = 2$.

Theorem 3.132. *The rotations of $\mathbb{R}^2$ and $\mathbb{R}^3$ about the origin are the linear operators whose matrices with respect to the standard basis are orthogonal and have determinant 1. In other words, a matrix A represents a rotation of $\mathbb{R}^2$ (or $\mathbb{R}^3$) if and only if $A \in SO_2(\mathbb{R})$ (or $SO_3(\mathbb{R})$).*

Corollary 3.133. *The composition of two rotations about the origin in $\mathbb{R}^3$ is also a rotation.*

Definition 3.134 (Dot Product)**.** The dot product of real column vectors X and Y is $(X \cdot Y) = x_1y_1 + ... + x_ny_n = X^TY$. Over the reals, the dot product is the square of the norm of a vector, $x \cdot x = ||x||^2$, and $(X \cdot Y) = ||X||||Y|| \cos(\theta)$, where θ is the angle between the vectors X and Y (consequence of the law of cosines).

Definition 3.135 (Orthogonality)**.** Two vectors X and Y are orthogonal if and only if $(X \cdot Y) = 0$.

Proposition 3.136. *The following conditions on a real $n \times n$ matrix A are equivalent:*

1. *A is orthogonal*
2. *Multiplication by A preserves the dot product, that is, $(AX \cdot AY) = (X \cdot Y)$ for all column vectors X and Y.*
3. *The columns of A are mutually orthogonal unit vectors. That is, they form an orthonormal basis for $\mathbb{R}^n$*

Proof. If A is orthogonal, then $(AX \cdot AY) = (AX)^T AY = X^T A^T AY = X^T Y = (X \cdot Y)$. Conversely, suppose $X^TY = X^T A^T AY$ for all X and Y. Let $B = I - A^T A$, so $X^T BY = 0$. Note that for any B, $e_i^T Be_j = b_{ij}$, so if $X^T BY = 0$ for all X and Y, then $b_{ij} = 0$ for all $i = 1, ..., n$ and $j = 1, ..., n$. Thus, $B = 0$ and $I = A^T A$. Let A_j denote the jth column vector of A. The (i, j) entry of the product matrix $A^T A$ is $(A_i \cdot A_j)$. Thus, $A^T A = I$ if and only if $(A_i \cdot A_i) = 1$ for all i, and $(A_i \cdot A_j) = 0$ for all $j \neq i$. Thus the columns of A have length 1 and are orthogonal, proving the equivalence of (1) and (3). ■

Definition 3.137 (Rigid Motion or Isometry)**.** A **rigid motion** or **isometry** of $\mathbb{R}^n$ is a map $m : \mathbb{R}^n \to \mathbb{R}^n$ which preserves distances; that is, if X and Y are in $\mathbb{R}^n$, then the distance from X to Y is equal to the distance from $m(X)$ to $m(Y)$

$$|m(X) - m(Y)| = |X - Y| \tag{3.80}$$

Such motions preserve angles and shapes in general. Moreover, the rigid motions of $\mathbb{R}^n$ form a group M_n, with composition of operations as its law of composition, and it is often called **the group of motions**.

Proposition 3.138. *For a map $m : \mathbb{R}^n \to \mathbb{R}^n$, the following conditions are equivalent:*

1. *m is a rigid motion which fixes the origin*
2. *m preserves the dot product: that is, for all $X, Y \in \mathbb{R}^n$, $(m(X) \cdot m(Y)) = (X \cdot Y)$*
3. *m is left multiplication by an orthogonal matrix*

Proof. Suppose m is a rigid motion which fixes 0. The fact that m preserves distances means

$$(m(X) - m(Y) \cdot m(X) - m(Y)) = (X - Y \cdot X - Y) \tag{3.81}$$

for all vectors X and Y. Setting $Y = 0$ shows that $(m(X) \cdot m(X)) = (X \cdot X)$. Expanding both sides and cancelling terms gives $(m(X) \cdot m(Y)) = (X \cdot Y)$. This shows that m preserves the dot product, so (1) implies (2).

Next, suppose m preserves the dot product. First, note that if m fixed the basis vectors e_i then it is the identity as

$$x_j = (X \cdot e_j) = (m(X) \cdot m(e_j)) = (m(X) \cdot e_j) = m(x)_j$$

for all j. Hence, $X = m(X)$, and m is the identity.

Now, since m preserves the dot product, the images $m(e_1), ..., m(e_n)$ of the standard basis vectors are orthogonal: $(m(e_i) \cdot m(e_i)) = (e_i \cdot e_i) = 1$ and $(m(e_i) \cdot m(e_j)) = (e_i \cdot e_j) = 0$, for $i \neq j$. Let $B' = (m(e_1), ..., m(e_n))$ and $A = [B']$. Then the columns of A form an orthonormal basis of $\mathbb{R}^n$ by definition, so A is orthogonal. Note that $A^{-1} = A^T$ is also orthogonal, so multiplication by A^{-1} preserves the dot-product. Moreover, the composed motion $A^{-1}m$ preserves the dot product and fixes the basis vectors e_i. Thus, $A^{-1}m$ is the identity map. This shows m is left multiplication by A as required.

Finally, if m is a linear operator whose matrix, A, is orthogonal, then $m(X) - m(Y) = m(X - Y)$ because m is linear, and $||m(X) - m(Y)|| = ||m(X - Y)|| = ||X - Y||$ by the fact that orthogonal matrices preserve dot products. Thus, m is a rigid motion. Since a linear operator always fixes 0, we see that (3) implies (1). ■

Corollary 3.139. *A rigid motion witch fixes the origin is a linear operator.*

Definition 3.140 (Translation)**.** A **translation** is a rigid motion t_b of the form

$$t_b(X) = X + b = \begin{bmatrix} x_1 + b_1 \\ \vdots \\ x_n + b_n \end{bmatrix} \tag{3.82}$$

where b is some fixed vector in $\mathbb{R}^n$.

Proposition 3.141. *Every rigid motion m is the composition of an orthogonal linear operator and a translation. In other words, it has the form $m(X) = AX + b$ for some orthogonal matrix A and fixed vector b.*

Proof. Let $b = m(0)$. Then $t_{-b}(b) = 0$, so the composed operation $t_{-b}m$ is a rigid motion which fixes the origin. Then, $t_{-b}m$ is realized by left multiplication by a orthogonal matrix A, so $t_{-b}m(X) = AX$. Applying t_b we see that $m(X) = AX + b$. Note that both the vector b and matrix A are uniquely determined by m, because $b = m(0)$ and A is the operator $t_{-b}(m)$. ■

Definition 3.142. An orthogonal operator is called **orientation preserving** if its determinant is $+1$, and **orientation reversing** if it is -1. Similarly, a rigid motion m is **orientation preserving** if $\det A = 1$ and **orientation reversing** if $\det A = -1$.

Corollary 3.143. *The rotations of $\mathbb{R}^2$ and $\mathbb{R}^3$ are the orientation preserving rigid motions which fix the origin.*

Lemma 3.144. *Every element $A \in SO_3$ has the eigenvalue 1.*

3.8.2 Lecture

Definition 3.145 (Orthogonal Groups)**.** Suppose that F is a field. Then $GL_n(F)$ is the **general linear group** over F composed of $n \times n$ invertible matrices with coefficients in F. Then $O_n(F) \subset GL_n(F)$ is a subgroup called the **orthogonal linear group** composed of orthogonal $n \times n$ matrices with coefficients in F. Finally, $SO_n(F) \trianglelefteq O_n(F)$ is the **special orthogonal linear group** composed of orthogonal $n \times n$ matrices with coefficients in F and determinant 1.

Definition 3.146 (Orthogonal Groups)**.** Take the vector space $V = F^n$, then $GL_n(F)$ is the group of linear maps on V which are isomorphisms. We put additional structure on V, which is an **inner product** $\langle , \rangle : F^n \times F^n \to F$ (more generally **bilinear forms**) which has the properties

1. For $v = (a_1, ..., a_n)$ and $w = (b_1, ..., b_n)$, then $\langle v, w\rangle = \sum_{i=1}^{n} a_i b_i$

We define

$$O_n(F) := \{A \in GL_n(F) : \langle Av, Aw\rangle \langle v, w\rangle\} \tag{3.83}$$

Certainly, $I \in O_n(F)$. Moreover, for $A, B \in O_n(F)$,

$$\langle ABv, ABw\rangle = \langle A(Bv), A(Bw)\rangle = \langle Bv, Bw\rangle = \langle v, w\rangle$$

so $AB \in O_n(F)$. Finally, for $A \in O_n(F)$,

$$\langle A^{-1}v, A^{-1}w\rangle = \langle A(A^{-1}v), A(A^{-1}w)\rangle = \langle v, w\rangle \tag{3.84}$$

Thus, $O_n(F)$ is a subgroup of $GL_n(F)$.

Remark 3.147 (Shape of Orthogonal Matrices)*.* Note that for the standard basis of $V = F^n$, $\langle e_i, e_i\rangle = 1$ for all i, and $\langle e_i, e_j\rangle = 0$ for $i \neq j$. Furthermore, note that the jth column of a matrix $A \in O_n(F)$ is given by $A(e_j)$. Then since A preserves the inner product, the inner product of the jth column with itself must be 1. Moreover, the inner product of the jth column with the ith column must be zero for $i \neq j$. This implies that

$$\langle Ae_i, Ae_j\rangle = \begin{cases} 1 & if\ i = j \\ 0 & if\ i \neq j \end{cases} \tag{3.85}$$

Then it follows that

$$A^T A = I \tag{3.86}$$

since the ij-th entry of $A^T A$ is the inner product of the i-th and j-th columns of A, which gives 1's along the diagonal, and zeroes everywhere else. This is equivalent to saying that

$$A^T = A^{-1} \tag{3.87}$$

Proposition 3.148. *Conversely, if $A \in GL_n(F)$ has $A^T = A^{-1}$, then it preserves the inner product we have defined on the vector space $V = F^n$, and hence $A \in O_n(F)$.*

Proof. First, note that if v and w are column vectors, $\langle v, w\rangle = v^T \cdot w$, where $\cdot$ is the matrix product. Then observe that $\langle Av, Aw\rangle = (Av)^T \cdot Aw = v^T A^T Aw = v^T w = \langle v, w\rangle$. Therefore, $A \in O_n(F)$, as A preserves the inner product. ■

Corollary 3.149. *Then,* $O_n(F) = \{A \in GL_n(F) : A^T = A^{-1}$.

Proposition 3.150. *For all* $A \in O_n(F)$, $\det(A) = \pm 1$.

Definition 3.151 (Special Orthogonal Group)**.** If we take the homomorphism $\det : O_n(F) \twoheadrightarrow F$, then the kernel of the homomorphism is the **special linear orthogonal group** $SO_n(F) := \{A \in O_n(F) : \det(A) = 1\}$, and $[O_n(F) : SO_n(F)] = 2$ (if $1 \neq -1$ in F)

Proposition 3.152. *The permutation matrices are in* $O_n(F)$*, which gives an injective homomorphism* $f : S_n \hookrightarrow O_n(F)$*, and* $A_n \trianglelefteq S_n$*, then the restriction* $f \Big|_{A_n} A_n \hookrightarrow SO_n(F)$*. Thus, we can consider* S_n *as a finite subgroup of the orthogonal group over ANY field.*

Remark 3.153 (WARNING). If $1 = -1$ in F, then the determinant homomorphism for $O_n(F)$ has only a trivial image, and $SO_n(F) = O_n(F)$.

Remark 3.154. Let $F = \mathbb{R}$. Then the inner product is $\langle v, v\rangle = \sum_{i=1}^{n} a_i^2 \geq 0$ and $\langle v, v\rangle = 0$ only when $v = \mathbf{0}$. Then we define the norm of v as $|v| = \sqrt{\langle v, v\rangle}$. Moreover, we have the Cauchy-Schwarz inequality

$$-1 \leq \frac{\langle v, w}{|v| \cdot |w|} \leq +1, \implies \frac{\langle v, w}{|v| \cdot |w|} \leq |\cos(\theta)| \tag{3.88}$$

where $0 \leq \theta \leq \pi$ is the angle between the two vectors (comes from the law of cosines in the 2-dimensional case), and this is well defined since the map $\cos : [0, \pi] \to [-1, 1]$ is a bijection. Moreover, the group $O_n(\mathbb{R})$ acts linearly on $\mathbb{R}^n$, and it preserves the length and angle. In other words, it preserves the notions of Euclidean geometry.

4 Symmetry

4.1 Groups of Motions

4.1.1 Textbook

Definition 4.1 (Types of Symmetry)**.** Below are a few types of symmetry:

1. **Bilateral symmetry**
2. **Rotational symmetry**
3. **Translational symmetry**
4. **Glide symmetry**

Figures can have any number of symmetries.

Definition 4.2 (Isometry)**.** An **isometry** is a mad $m : P \to P$ from a space P two itself if it preserves the sense of distance for the space. The set of all rigid motions M form a group with the law of composition being composition of functions. If a rigid motion m carries a subset F of a plane to itself, we call it a **symmetry** of F. The set of all symmetries of F is a subgroup of M, called the **group of symmetries of the figure**.

Definition 4.3 (Basic Partition of M)**.** The coarsest classification of motions is into **orientation preserving** and **orientation reversing** motions. This partition can be used to define a map

$$M \to \{\pm 1\} \tag{4.1}$$

by sending orientation preserving motions to 1 and orientation reversing motions to -1.

Definition 4.4 (Classification of Motions)**.** Rigid motions can be classified as follows

1. Orientation preserving:
   (a) Translation: parallel motion of the plane by a vector a:$p \mapsto p + a$
   (b) Rotation: rotates the plane by an angle $\theta \neq 0$ about some point
2. Orientation reversing:
   (a) Reflection about the line l
   (b) Glide reflection: obtained by reflecting about the line l, and then translating by a nonzero vector a parallel to l

The above list is complete.

Theorem 4.5. *The above list is complete, as every rigid motion is a translation, a rotation, a reflection, a glide reflection, or the identity.*

Proof. Let m be a rigid motion which preserves orientation but is not a translation. We want to prove that m is a rotation about some point. It is clear that an orientation preserving map which fixes a point p in the plane must be a rotation about p. We write $m = t_a\rho_\theta$. By assumption $\theta \neq 0$. To find the fixed point we must solve the equation $x = t_a\rho_\theta(x) = \rho_\theta(x)+a$. In other words, we need to solve the equation

$$\begin{bmatrix} 1-\cos(\theta) & \sin(\theta) \\ -\sin(\theta) & 1-\cos(\theta) \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \tag{4.2}$$

Note that $\det(1-\rho_\theta) = 2-2\cos(\theta)$, so for $\theta \neq 0$, we have a unique solution which is our fixed point, so the motion is a rotation about our derived unique point. (The corollary below shows that we obtain a rotation about its fixed point)

Next, we will show that any orientation-reversing motion $m = t_a\rho_\theta r$ is a glide reflection or a reflection. We do this by finding a line l which is sent to itself by m, and so that the motion of m on l is a translation. It is clear geometrically that an orientation reversing which acts in this way on a line is a glide reflection.

We shall reduce the problem in two steps. First, the motion $\rho_\theta r = r'$ is a reflection about a line. The line is the one which intersects the x_1-axis at an angle of $\frac{1}{2}\theta$ at the origin. So, our motion m is the product of the translation t_a and the reflection r'. We may rotate coordinates so that the x_1-axis becomes the line of reflection of r'. Then r' becomes the standard reflection r, and the translation t_a remains a translation, though the coordinates of the vector a will have changed. In this new coordinate system $m = t_a r$, and we find that it acts

$$m \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 + a_1 \\ -x_2 + a_2 \end{bmatrix} \tag{4.3}$$

This motion send the line $x_2 = \frac{1}{2}a_2$ to the itself, by the translation $(x_1, \frac{1}{2}a_2)^T \mapsto (x_1 + a_1, \frac{1}{2}a_2)^T$, and so m is a glide reflection for this line. ■

Corollary 4.6. *The composition of rotations about two different points is a rotation about a third, unless it is a translation, since the composition of orientation preserving motions preserves orientation.*

Corollary 4.7. *The composition of reflections about two nonparallel lines l_1 and l_2 is a rotation through their intersection point, $p = l_1 \cap l_2$. The composition of two reflections about parallel lines is a translation by a vector orthogonal to the lines.*

Definition 4.8. Take the plane to be $\mathbb{R}^2$ by a choice of coordinates. We then choose generators for translations, rotations, and reflections:

1. Translation t_a by a vector a: $t_a(x) = x + a = \begin{bmatrix} x_1 + a_1 \\ x_2 + a_2 \end{bmatrix}$
2. Rotation ρ_θ by an angle θ about the origin:
$$\rho_\theta(x) = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$
3. Reflection r about the $x_1 - axis$: $r(x) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ -x_2 \end{bmatrix}$

Since the fix the origin, ρ_θ and r are orthogonal operators on $\mathbb{R}^2$. Every element of M is a product of these motions. Note that every rigid motion is the composition of an orthogonal operator and a translation. The expression of a motion as a product, $t_a\rho_\theta r^i$, of these generators is unique.

Corollary 4.9. *Any rigid motion m is the product of the above generators, since every rigid motion is the product of an orthogonal linear operator and a translation. Moreover, if the determinant of the operator is one, then it is a rotation, and if the determinant is negative one, then, then the determinant of the operator composed with a reflection r is 1, so the operator is the product of a rotation and the standard reflection, r, (which gives a reflection) so*
$$m = t_a\rho_\theta \text{ or else } m = t_a\rho_\theta r \tag{4.4}$$
for some vector a and angle θ. This expression is also unique.

Uniqueness. If $m = t_a\rho_\theta r^i = t_b\rho_\nu r^j$, then m is either orientation preserving, $j = i = 0$, or orientation reversing, $j = i = 1$. Thus, we can cancel r from both sides and obtain $t_a\rho_\theta = t_b\rho_\nu$. Then, we find that $t_{a-b} = \rho_{\theta-\nu}$. But, any non-zero translation fixes nothing, while all rotations fix at least one point. Therefore, both sides must be the identity operator, and $a = b$ and $\theta = \nu$. ■

Definition 4.10 (Composition Rules)**.** Using the definitions of the above generators, we can define rulse for composition in M:

1. $t_at_b = t_{a+b}$, $\rho_\theta\rho_\nu = \rho_{\theta+\nu}$, and $rr = 1$
2. $\rho_\theta t_a = t_{a'}\rho_\theta$ where $a' = \rho_\theta(a)$
3. $rt_a = t_{a'}r$ where $a' = r(a)$
4. $r\rho_\theta = \rho_{-\theta}r$

Corollary 4.11. *The motion $m = t_a\rho_\theta$ is the rotation through the angle θ about its fixed point.*

Proof. The fixed point is one which satisfies the relation $p = \rho_\theta(p) + a$. Then, for any x,

$$m(p+x) = t_a\rho_\theta(p+x) = \rho_\theta(p+x) + a = \rho_\theta(p) + \rho_\theta(x) + a = p + \rho_\theta(x) \tag{4.5}$$

Thus m sends $p+x$ to $p+\rho_\theta(x)$. Therefore, m is a rotation through an angle θ about the fixed point p. ■

Definition 4.12 (Subgroups of M)**.** Two important subgroups of the group of motions M is the group of translations T and the group of orthogonal operators O.Note that with a choice of coordinates, we obtain a bijective correspondance

$$\mathbb{R}^2 \xrightarrow{a\mapsto t_a} T \tag{4.6}$$

In fact, this is an isomorphism of the additive group $(\mathbb{R}^2, +)$ with the subgroup T. Using our choice of coordinates we can also define an isomorphism

$$O_2(\mathbb{R}) \xrightarrow{\sim} O \tag{4.7}$$

Proposition 4.13. .

1. *Let p be a point of the plane. Let ρ'_θ denote the rotation through the angle θ about p, and let r' denote the reflection about the line through p and parallel to the x-axis. Then $\rho'_\theta = t_p\rho_\theta t_p^{-1}$ and $r' = t_p r t_p^{-1}$*
2. *The subgroup of M of motions fixing the point p is the conjugate subgroup*

$$O' = t_p O t_p^{-1} \tag{4.8}$$

Proof. We can obtain the rotation ρ'_θ in this way: First translate p to the origin, next rotate the plane about the origin and through the angle θ, and finally translate the origin back to p:

$$\rho'_\theta = t_p\rho_\theta t_{-p} = t_p\rho_\theta t_p^{-1} \tag{4.9}$$

The reflection r' can be obtained in the same way:

$$r' = t_p r t_{-p} = t_p r t_p^{-1} \tag{4.10}$$

Since every motion fixing p has the form ρ'_θ or $\rho'_\theta r'$, the proof is complete. ■

Remark 4.14. We have an important homomorphism $\phi : M \to O$ whose kernel is T, which is obtained by $t_a\rho_\theta r^i \mapsto \rho_\theta r^i$.

Proposition 4.15. *Let p be any point of the plane, and let ρ'_θ denote the rotation through the angle θ about p. Then $\phi(\rho'_\theta) = \rho_\theta$. Similarly, if r' is the reflection about the line through p and parallel to the x-axis, then $\phi(r') = r$.*

Remark 4.16. The homomorphism ϕ does not depend on the choice of origin.

4.1.2 Lecture

Recall. We have that the orthogonal group $O_n(F)$ is a subgroup group of $GL_n(F)$, which is the group of automorphisms of the space F^n, and that $O_n(F)$ preserves the structure of the inner product $\langle v, w\rangle = \sum_{i=1}^{n} v_i w_i$. Moreover, for all $A \in O_n(F)$, $A^{-1} = A^T$. We also saw from this that $\det(A)^2 = \det(I) = +1$, then since the determinant of A satisfies the polynomial $x^2 - 1 = 0$, we find that $\det(A) = \pm 1$ (where 1 may equal -1 depending on the field). Moreover, if $1 \neq -1$ in F, then we may define $SO_n(F) \trianglelefteq O_n(F)$, where $SO_n(F) := \{A \in GL_n(F) : A^T = A^{-1}, \det(A) = +1\}$

Remark 4.17. If $F = \mathbb{R}$, then if A preserves the inner product $\langle v, w\rangle$, it also preserves the Euclidean distance

$$|v| = \sqrt{\langle v, v\rangle} = \sqrt{\sum_{i=1}^{n} v_i^2} \geq 0 \tag{4.11}$$

It also approves the Euclidean angle which is defined by the Cauchy-Schwarz inequality

$$\cos(\theta) = \frac{\langle v, w\rangle}{|v||w|} \tag{4.12}$$

Observation 4.18. If v is an eigenvector for $A \in O_n(F)$, with eigenvalue λ, $Av = \lambda v$, and $\langle v, v\rangle \neq 0$, then $\lambda^2 = 1$ (in other words $\lambda = \pm 1$).

Question. What do transformations A in $SO_2(\mathbb{R})$ look like?

Answer. We consider the standard basis vectors $e_1 = (1, 0)^T$ and $e_2 = (0, 1)^T$. Then, since A is an orthogonal transformation, it preserves the norm of a vector, so $|Ae_1| = |Ae_2| = 1$ and $\langle Ae_1, Ae_2\rangle = 0$. Then $Ae_1 = (\cos(\theta), \sin(\theta))$ for some θ. Then, since $A \in SO_2(\mathbb{R})$, $\det(A) = +1$, and $Ae_2 = (-\sin(\theta), \cos(\theta)$. Thus,

$$A = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} = rot(\theta) \tag{4.13}$$

Using the laws of sines and cosines we find that $rot(\theta) \circ rot(\phi) = rot(\theta + \phi)$. We then get an isomorphism of (abelian) groups

$$SO_2(\mathbb{R}) \xrightarrow{f} \{z \in \mathbb{C}^* : |z| = 1\} \tag{4.14}$$

with $A = rot(\theta) \mapsto z = e^{i\theta} = f(e_1)$. Note that only $rot(0)$ and $rot(\pi)$ have eigenvectors.

Question. What are the transformations $A \in O_2(\mathbb{R}) \backslash SO_2(\mathbb{R})$?

Answer. Each such A has two orthogonal eigenvectors v_1, v_2, with the property that

$$Av_1 = v_1, Av_2 = -v_2 \tag{4.15}$$

Proof. The characteristic polynomial of A looks like $x^2 - Tr(A)x - 1 = 0$, since $\det(A) = -1$. If the roots are not real, then they would be complex conjugates (use the quadratic formula). Then, $\det(A) = z\overline{z} \geq 0$, but $\det(A) = -1$, which is a contradiction. Therefore, the two roots λ_1 and λ_2 are real, and $\lambda_1\lambda_2 = -1$. But, the eigenvalues of A must be ± 1, so $\lambda_1 = \pm 1$ and $\lambda_2 = \mp 1$. Then, the resulting eigenvectors v_1 and v_2 and orthogonal. Take $Av_1 = v_1$ and $Av_2 = -v_2$, so $\langle v_1, v_2 \rangle =$ ■

Answer. So A has an orthonormal basis of eigenvectors. Moreover, the transformation reflects over the line that it fixed by the transformation. Moreover, $A^2 = I$, and so every element in the non-trivial coset $O_2(\mathbb{R})\backslash SO_2(\mathbb{R})$ is of order 2. However, the elements don't commute with eachother since $refl(v_1) \circ refl(v_2) = rot(\theta)$ (because the composition will have determinant $+1$).

Theorem 4.19 (Euler's Theorem)**.** *Any $A \in SO_3(\mathbb{R})$ has an eigenvalue of $+1$. So, there is a $v \in \mathbb{R}^3$ such that $Av = v$. In other words, any motion preserving the sphere $S^2 \in \mathbb{R}^3$ with orientation preserving motion (determinant 1) has an axis of rotation.*

Proof. The characteristic polynomial $p(t)$ has degree 3, se we factor it in $\mathbb{C}$. Possibilities: $\{\lambda_1, \lambda_2, \lambda_3\}$ all real or $\{\lambda, z, \overline{z}\}$ (always must be at least one real root for a real polynomial of odd degree by the Intermediate Value Theorem). Note that $z\overline{z} > 0$, and $\det(A) = 1 = \lambda z\overline{z}$. Moreover, any real eigenvalue must be ± 1, so in the first case at least one must be $+1$, and in the second case we must have that $\lambda = +1$. Therefore, we have an eigenvector, or axis, that is fixed. ■

Remark 4.20. In three-space, for all $A \in SO_3(\mathbb{R})$, A preserves the sphere centered at the origin. Moreover, from Euler's theorem it preserves an axis through the origin. Furthermore, it preserves the plane orthogonal to the fixed axis. This follows from the fact that if $\langle v, w \rangle = 0$, then $\langle v, Aw \rangle = \langle Av, Aw \rangle = \langle v, w \rangle = 0$. Then, if we choose a basis with the first basis vector being the fixed unit vector v, and extend it to a basis of $\mathbb{R}^3$ with orthonormal vectors in the plane orthogonal to v, we get a matrix of the form

$$A = \left[\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & & \\ 0 & & \end{array}\right] \tag{4.16}$$

Where since A is orthogonal, the 2×2 submatrix must be orthogonal, and since $A \in SO_3(\mathbb{R})$, its determinant must be 1 so the 2×2 submatrix is in $SO_2(\mathbb{R})$. Therefore, in the orthogonal plane to v, we are rotating through some angle θ. Then since anything in $SO_3(\mathbb{R})$ is a rotation about an axis, we find that the composition of rotations about two axes must be a rotation about a third.

Definition 4.21 (Rigid Motions)**.** All motions from $\mathbb{R}^n \to \mathbb{R}^n$ which preserve the distance $d(v, w)$ between two points (where $d(v, w) = |v - w|$) is called the group M of rigid motions. All set-theoretic maps which preserve the distance between two points.

Proposition 4.22. *If m is a rigid motion, and $m(0) = 0$, then $m = A$ is a linear transformation in $O_n(\mathbb{R})$.*

Proof. Sketch: For distances, we know that $|v - w|^2 = \langle v - w, v - w\rangle = |v|^2 + |w|^2 - 2\langle v, w\rangle$. Then, since m preserves distances and preserves the origin, it must preserve $|v - w|^2$, $|v|^2$, and $|w|^2$, which implies that it preserves $\langle v, w\rangle$. ■

Proposition 4.23. *Subgroups of M:*

1. *$O_n(\mathbb{R}) \subset M$ preserving the origin.*
2. *Translations with a fixed vector b, $t_b(v) = v+b$. Moreover, the subgroup T is isomorphic to $(\mathbb{R}^n, +)$*

Then, $M = O_n(\mathbb{R}).\mathbb{R}^n$, with $\mathbb{R}^n$ as a normal subgroup.

Proof. Let m be a rigid motion. Then $m(0) = b$ for some $b \in \mathbb{R}^n$. Then $t_{-b} \circ m(0) = 0$, so $t_{-b} \circ m(0)$ is an orthogonal transformation. ■

Remark 4.24. We have the subgroup of translations of the group of rigid motions, which is isomorphic to the additive group $(\mathbb{R}^n, +)$.

Proposition 4.25. *Every element in M can be written uniquely as $M = \mathbb{R}^n \cdot M_0$, where M_0 is the set of rigid motions which fix the origin.*

Proof. Suppose $m(0) = b$, where m is a rigid motion. Then $t_{-b} \circ m(0) = 0$, where $t_{-b} \circ m$ is a rigid motion which fixes the origin, so it is in M_0. Thus, $m = t_b \circ (t_{-b} \circ m)$. Moreover, the intersection of the subgroup of translations and the subgroup of rigid motions which fixes the origin is the identity. ■

Proposition 4.26. *We claim that $M_0 \cong O_n(\mathbb{R})$ is the group of orthogonal transformations.*

Proof. Take $m \in M_0$. Then note that $\langle m(v), m(w)\rangle = \langle v, w\rangle$, and let $e_1, ..., e_n$ be the standard basis of $\mathbb{R}^n$. Note that $\langle e_i, e_i\rangle = 1$ and $\langle e_i, e_j\rangle = 0$ for $i \neq j$. Then $m(e_1), m(e_2), ..., m(e_n)$ is another orthonormal basis. Let $A \in O_n(\mathbb{R})$ with column vectors

$$A = \begin{bmatrix} | & & | \\ m(e_1) & \dots & m(e_n) \\ | & & | \end{bmatrix} \tag{4.17}$$

We claim that $m = A$ as a transformation of $\mathbb{R}^n$. Consider the motion $m \circ A^{-1} = m'$. It is a motion of space which preserves distance and fixes the origin since m and A are rigid motions which fix the origin. It follows that $m'(e_i) = e_i$ for all $i = 1, 2, ..., n$. Then, let $v \in \mathbb{R}^n$, and consider $m'(v)$. Then the ith coordinate of $m'(v)$ is

$$\langle m'(v), e_i \rangle = \langle m'(v), m'(e_i) \rangle = \langle v, e_i \rangle = v_i \tag{4.18}$$

so the ith coordinate of $m'(v)$ is the same as the ith coordinate of v, so m' fixes v. Therefore, m' fixes every vector in $\mathbb{R}^n$, so $m \circ A^{-1} = m' = I$, or in other words $m = A$ as desired. ■

Remark 4.27. Then we have that $M = \mathbb{R}^n \cdot O_n(\mathbb{R})$, so for any $m \in M$, we have a pair (b, A) such that

$$m(v) = A(v) + b \tag{4.19}$$

Suppose that $(b', A') \in M$. Then obserse that

$$(b, A) \cdot (b', A')(v) = (b, A)(A'v + b') = A(A'v + b') + b = AA'v + (Ab' + b) \tag{4.20}$$

Then $(b, a) \cdot (b', A') = (b + A(b'), AA')$ (note that this is not quite a product group, since if it was, $(b, A)(b', A') = (bb', AA')$) Nonetheless, note that we get the homomorphism $\phi : M \to O_n(\mathbb{R})$ which takes $(b, A) \mapsto A$ is a surjective homomorphism with kernel $\mathbb{R}^n = \{(b, I)\}$ ($(b, I)(v) = v + b = t_b(v)$), so $\mathbb{R}^n$ is a normal subgroup, and $O_n(\mathbb{R}) \cong M/\mathbb{R}^n$.

4.2 Finite Groups of Motion

4.2.1 Textbook

Theorem 4.28 (Fixed Point Theorem)**.** *Let G be a finite subgroup of the group of motions M. There is a point p in the plane which is left fixed by every element of G, that is, there is a point p such that $g(p) = p$ for all $g \in G$.*

Geometric. Let s be any point in the plane, and let S be the set of points which are the images of s under the various motions in G. So each element $s' \in S$ has the form $g(s) = s'$ for some $g \in G$. This set is called the **orbit** of s under the action of G. The element s is in the orbit because the identity element 1 is in G, and $s = 1(s)$. Any element of the group G will permute the orbit S. In other words, if $s' \in S$ and $x \in G$, then $x(s') \in S$. For, say that $s' = g(s)$, with $g \in G$. Since G is a group, $xg \in G$. Therefore, by definition, $xg(s) \in S$. Since $xg(s) = x(s')$, this shows that $x(s') \in S$.

Note that because G is finite, S is finite. We list the elements of S arbitrarily, writing $S = \{s_1, ..., s_n\}$. The fixed point we are looking for is the **center of gravity** of the orbit, defined as

$$p = \frac{1}{n}(s_1 + ... + s_n) \tag{4.21}$$

where the right side is computed via vector addition, using an arbitrary coordinate system in the plane. The centre of gravity should be considered an average of the points $s_1, ..., s_n$.

From the below lemma, the center of gravity for our S is a fixed point for the action of G. This follows from the fact that any $g_i \in G$ permutes the orbit S, so the lemma shows it sends the center of gravity to itself. ■

Lemma 4.29. *Let $S = \{s_1, ..., s_n\}$ be a finite set of points of the plane, and let p be its center of gravity. Let m be a rigid motion, and let $m(s_i) = s_i'$) and $m(p) = p'$. Then $p' = \frac{1}{n}(s_1' + ... + s_n')$. In other words, rigid motions carry centers of gravity to centers of gravity.*

Proof. We create separately the cases $m = t_a$, $m = \rho_\theta$, and $m = r$, since every rigid motion is created from a composition of these.

Case 1: $m = t_a$. Then $p' = p + a$ and $s_i' = s_i + a$, so we see that

$$p' = p + a = \frac{1}{n}((s_1 + a) + ... + (s_n + a)) = \frac{1}{n}(s_1' + ... + s_n') \tag{4.22}$$

Case 2: $m = \rho_{theta}$ or r. Then m is a linear operator. Therefore,

$$p' = m(\frac{1}{n}(s_1 + ... + s_n)) = \frac{1}{n}(m(s_1) + ... + m(s_n)) = \frac{1}{n}(s_1' + ... + s_n') \tag{4.23}$$

■

Corollary 4.30. *Any subgroup of M which contains rotations about two different points is infinite.*

Remark 4.31. Let G be a finite subgroup of M. Then G fixes a point in the plane, and we may choose our coordinates so the origin is that fixed point. Then, G will be a subgroup of O. Thus, to describe the finite subgroups G of M, we need only describe the finite subgroups of O.

Theorem 4.32. *Let G be a finite subgroup of the group O of rigid motions that fix the origin. Then G is one of the following groups:*

1. *$G = C_n$: the **cyclic group** of order n, generated by the rotation ρ_θ, where $\theta = \frac{2\pi}{n}$*
2. *$G = D_n$: the **dihedral group** of order $2n$, generated by two elements - the rotation ρ_θ, with $\theta = \frac{2\pi}{n}$, and the reflection r' about a line through the origin.*

Proof. Let G be a finite subgroup of O. Recall that elements of O are rotations, ρ_θ, and reflections, $\rho_\theta r$.

Case 1: All elements of G are rotations. We must prove that G is cyclic in this case. If $G = \{1\}$, then $G = C_1$. Otherwise, G contains a nontrivial rotation ρ_θ. Let θ be the smallest positive angle of rotation among the elements of G. Let $\rho_\alpha \in G$, where the angle α is represented as a real number. Let $n\theta$ be the greatest integer multiple of θ which is less than α. Then $\alpha = n\theta + \beta$, where $0 \leq \beta < \theta$. Since G is a group and since ρ_α and ρ_θ are in G, the product $\rho_\beta = \rho_\alpha \rho_{-n\theta}$ is also in G. But, by assumption θ is the smallest positive angle of rotation in G. Therefore, $\beta = 0$ and $\alpha = n\theta$. This shows that G is cyclic. Let $n\theta$ be the smallest multiple of θ such that $2\pi \leq n\theta < 2\pi + \theta$. Since θ is the smallest positive angle of rotation in G, $n\theta = 2\pi$. Thus, $\theta = \frac{2\pi}{n}$ for some integer n.

Case 2: G contains a reflection. Adjusting our coordinates as necessary, we may assume our standard reflection r is in G. Let H denote the subgroup of rotations in G. From case 1 we see that $H = C_n$ for some $n \in \mathbb{N}$. Moreover, the $2n$ products $\rho_\theta^i, r\rho_\theta^i$, $0 \leq i \leq n-1$, are in G, and so G contains the dihedral group D_n. If an element g of G is a rotation, then $g \in H$ by definition of H; hence, $g \in D_n$. If g is a reflection, we can write it in the form $\rho_\alpha r$ for some rotation ρ_α. Since $r \in G$, so is the product $\rho_\alpha rr = \rho_\alpha$. Therefore, $\rho_\alpha \in H$, and g is in D_n too. Thus, $G = D_n$, completing the proof.

■

Remark 4.33. The group D_n depends on the line of reflection, but we may choose coordinates so that it is the x-axis, and then r' is our standard rotation r. If G were given as a finite subgroup of M, we would first need to shift the origin so that it is the fixed point.

Corollary 4.34. *Let G be a finite subgroup of the group of motions M. If coordinates are introduced suitably, then G becomes one of C_n or D_n, where C_n is generated by ρ_θ, $\theta = \frac{2\pi}{n}$, and D_n is generated by ρ_θ and r.*

Observation 4.35. When $n \geq 3$, the dihedral group D_n is the group of symmetries of the regular n-sided polygon.

Remark 4.36. The dihedral group D_2 is isomorphic to the Klien four group.

Proposition 4.37 (Defining Relations for the Dihedral Group)**.** *The dihedral group D_n is generated by two elements ρ and r satisfying*

$$\rho^n = 1, \quad r^2 = 1 \quad \rho r = r\rho^{-1} \tag{4.24}$$

The elements of D_n are

$$\{1, \rho, ..., \rho^{n-1}; r, r\rho, ..., r\rho^{n-1}\} = \{r^j \rho^i : 0 \leq i < n, 0 \leq j < 2\} \tag{4.25}$$

Proof. The elements $\rho = \rho_\theta$ and r generate D_n by definition of the group. The relations $r^2 = 1$ and $r\rho = \rho^{-1}r$ follow from the defining relations of rotations and reflections for the group of rigid motions M. The relation $\rho^n = 1$ follows from the fact that $\theta = \frac{2\pi}{n}$, which also shows that $1, \rho, ..., \rho^{n-1}$ are distinct. It follows that the elements $r, r\rho, ..., r\rho^{n-1}$ are also distinct and, since they are reflections while the powers of ρ are rotations, that there is no repitition in the list of elements. Finally, the relations can be used to reduce any product $r, \rho, r^{-1}, \rho^{-1}$ to the form $r^j\rho^i$ $(0 \leq j < 2, 0 \leq i < n)$. Therefore, the list of elements of the group generated by r and ρ which generate D_n are complete. ■

Remark 4.38. The third relation can be written equivalently as

$$r\rho = \rho^{n-1}r, \;\; r\rho r\rho = 1 \tag{4.26}$$

Corollary 4.39. *The dihedral group D_3 and the symmetric group S_3 are isomorphic.*

4.2.2 Lecture

Definition 4.40 (n=2)**.** We consider $M = \mathbb{R}^2.O_2(\mathbb{R})$. Note that $M_0 = O_2(\mathbb{R}) = SO_2(\mathbb{R}) \cup SO_2(\mathbb{R})_{r_l}$, where $SO_2(\mathbb{R})_{r_l}$ is the reflections through the line l in the plane, and $SO_2(\mathbb{R})$ are the rotations through the origin. Note that $SO_2(\mathbb{R})$ is an abelian group.

Question. What is $r_l \circ rot(\theta) \circ r_l^{-1}$?

Answer. First, note that $r_l^{-1} = r_l$. Then $r_l \circ rot(\theta) \circ r_l = rot(\theta')$ since the linear operator has determinant 1. Consider a point p on l. Then $r_l(p) = p$, then $rot(\theta)(p)$ has an angle θ from l. Moreover, $r_l(rot(\theta)(p))$ gives a rotation by $-\theta$. Thus, $r_1 \circ rot(\theta) \circ r_l = rot(-\theta) = rot(\theta)^{-1}$.

Observation 4.41. It follows that for $M_0 = SO_2(\mathbb{R}) \cup SO_2(\mathbb{R})_{r_l}$, $SO_2(\mathbb{R})$ is a commutative group, and is in fact a normal subgroup, and for any $r \in SO_2(\mathbb{R})_{r_l}$ and for any $h \in SO_2(\mathbb{R})$, $rhr^{-1} = h^{-1}$.

Theorem 4.42 (Types of Motions in $\mathbb{R}^2$)**.** *For any $g \in M$, it is one of these 4 types (recall that we have a surjective homomorphism* $\det : M \twoheadrightarrow O_n(\mathbb{R}) \twoheadrightarrow \langle \pm 1 \rangle$*):*

1. *If* $\det(g) = +1$*, then we say that g is* ***orientation preserving*** *(of the form $t_b \circ rot(\theta)$)*
   (a) *Translation: t_b, which fix no points (or all points if $b = 0$)*
   (b) *Rotations: $t_b \circ rot(\theta)$, which fix a single points p, and denotes a rotation around p.*

2. *If* $\det(g) = -1$*, then we say that* g *is* ***orientation reversing*** *(of the form* $t_b \circ rot(\theta) \circ refl(l)$*)*

   (a) *Reflection:* $refl(l')$*, where* $b = 0$*, and is a reflection through the line* l' *(fixes everything on the line* l' *- point wise)*

   (b) *Glide Reflection:* $refl(l) + b$ *where* b *is parallel to* l*, so you reflect through a line, than translate along a vector parallel to the line. (doesn't fix everything on the line* l*, but fixes the line - not point wise)*

First bit. If $\theta \neq 0$, and if $b = 0$, then we fix $p = 0$, and $m \in M_0 = SO_2(\mathbb{R})$. Otherwise, assume $b \neq 0$. Then, there is a unique line l orthogonal to b. We then take a sector centered around the orthogonal line, with angle theta, orientated so that it is rotated away from b. By continuity the sector is getting larger, and eventually will have a vector going from one edge to the other which is of the same length as, and parallel to, b. Then, the point p at the tip of the new vector b on one of the edges of the sector is the fixed point. Then, since it preserves distances, and m is not the identity transformation, it follows that all other points must not be fixed. Furthermore, if we have an orthogonal basis with p as the origin, since it preserves distances and angles, and the $\det(m) = +1$, the orthogonal basis vectors will be rotated about the angle θ. ■

Definition 4.43 (Finite Subgroups)**.** Finite subgroups of $M = \mathbb{R}^2.O_2(\mathbb{R})$, Γ. Note that finite subgroups contain no translations, as they will march out forever.

Theorem 4.44 (Fixed Point Theorem)**.** *Any finite* Γ *fixes a point* $p \in \mathbb{R}^2$*. That is,* $\gamma(p) = p$ *for all* $\gamma \in \Gamma$*. If* $p = 0$*, then* $\gamma \subset O_2(\mathbb{R})$*. Moreover, in general,* $\Gamma \subset M_p \subset M$*, where* $M_p := \{g(p) = p\} = t_p M_0 t_p^{-1}$*, a conjugate of* M_9*. Recall that conjugation is an automorphism of* M*, so conjugating* Γ *will not change its structure, so* $t_p^{-1}\Gamma t_p = \Gamma^* \subset M_0 = O_2(\mathbb{R})$*, where* Γ^* *is a finite subgroup isomorphic to* Γ*.*

Proposition 4.45 (Abstract recipe for fixed point p)**.** *Let* $s \in \mathbb{R}^2$ *be any vector. Consider the vectors* $S = \{\gamma(s) : \gamma \in \Gamma\}$*. Since* Γ *is finite,* S *is a finite set. Then, we let* p *be the center of mass of the set, where* $n = |\Gamma|$*,*

$$p = \frac{1}{n} \sum_{\gamma \in \Gamma} \gamma(s) \tag{4.27}$$

We claim that p *is a fixed point. We note that for all* $m \in M$*,* $m(p) = \frac{1}{n} \sum_{\gamma \in \Gamma} g(\gamma(s))$ *since translations fix the center of mass and linear transformations fix the center of mass, so their composition fixes the center of mass. Then for all* $\gamma' \in \Gamma$*,*

$$\gamma'(p) = \frac{1}{n} \sum_{\gamma \in \Gamma} \gamma'(\gamma(s)) \tag{4.28}$$

Then, since γ' is a rigid motion, it is a bijection, so it merely permutes S, and hence $\sum_{\gamma\in\Gamma}\gamma'(\gamma(s)) = \sum_{\gamma\in\Gamma}\gamma(s)$ since vector addition is commutative. Therefore, $\gamma'(p) = p$, so p is a fixed point.

Theorem 4.46 (Classification)**.** *The finite subgroups $\Gamma \subset O_2(\mathbb{R})$*

1. *$\Gamma \subset SO_2(\mathbb{R})$ ($\det(\Gamma) = +1$)*

   Proof. Every $\gamma = rot(\theta)$, $0 \le \theta < 2\pi$. Let θ be the smallest angle of rotation for $\gamma \in \Gamma$, $\theta > 0$. We claim that Γ is then a cyclic group generated by this element. Moreover, if $|\Gamma| = n$, then $\theta = \frac{2\pi}{n}$. Suppose that $rot(\alpha) \in \Gamma$. Then for some $n \in \mathbb{Z}$, $n\theta \le \alpha < \theta(n+1)$, so $0 \le \alpha - n\theta < \theta$, so $\alpha - n\theta = 0$, so Γ is cyclic. Moreover, if $|\Gamma| = n$, then $|rot(\theta)| = n$, so $n\theta = 2\pi$, and $\theta = \frac{2\pi}{n}$. In particular, every subgroup here is cyclic, and all orders occur. ■

2. *$\Gamma \cap SO_2(\mathbb{R}) = \Gamma_+$ has index 2 in Γ (normal subgroup) ($\det(\Gamma) = \pm 1$) so $\det : \Gamma \to \langle \pm 1\rangle$*

   Proof. Note that Γ_+ is cyclic of some order n. Moreover, since it has index 2 in Γ, $|\Gamma| = 2n$, and it contains in it C_n. Suppose $refl(l) = r \in \Gamma$, where $r \notin C_n$, with $r^2 = 1$, and for all $h \in C_n$, $rhr = h^{n-1}$. Therefore, $\Gamma = \langle rot(\frac{2\pi}{n}, r\rangle$. Such a group is called a dihedral group D_n (or D_{2n}) of order $2n$. Moreover, for $n \ge 3$, D_n is non-abelian. ■

4.3 Discrete Groups

4.3.1 Textbook

Definition 4.47 (Discrete)**.** A subgroup G of the group of motions M is called **discrete** if it does not contain arbitrarily small translations or rotations. More precisely, G is discrete if there is some real number $\varepsilon > 0$ so that

1. if t_a is a translation in G by a nonzero vector a, then the length of a is at least ε: $|a| \ge \varepsilon$
2. if ρ is a rotation in G about some point through a nonzero angle θ, then the angle θ is at least ε: $\theta \ge \varepsilon$.

Note that these are conditions on orientation preserving motions.

Proposition 4.48. *Every discrete group of motions is the group of symmetries of a plane figure.*

Rationale. Let R be a figure in the plane. We require that R does not have any symmetries except the identity. Thus, every element g of our group G will move R to a different position, gR. The required figure F is the union of all plane figures gR. An element $x \in G$ send gR to xgR, which is also a part of F, and hence it sends F to itself. If R is sufficiently random, G will be its group of symmetries. ■

Definition 4.49 (Translation Groups)**.** Let G be a discrete group. Then the **translation group** of G is the set of vectors a such that $t_a \in G$. Since $t_a t_b = t_{a+b}$ and $t_{-a} = t_a^{-1}$, this is a subgroup of the additive group of vectors, which we will denote by L_G. Using a choice of coordinates we identify the vectors with $\mathbb{R}^2$. Then

$$L_G \cong \{a \in \mathbb{R}^2 : t_a \in G\} \tag{4.29}$$

This group is isomorphic to the subgroup $T \cap G$ of translations in G, by the isomorphism $a \mapsto t_a$. Since it is a subgroup of G, $T \cap G$ is also discrete. Thus, in L_G we find no vectors of length $< \varepsilon$, except for the zero vector. A subgroup L of $(\mathbb{R}^n, +)$ which satisfies the statement for some $\varepsilon > 0$ is called a discrete subgroup of $\mathbb{R}^n$ (the adjective dicrete means the elements of L are separated by a fixed distance in this case). The distance between any vectors $a, b \in L$ is at least ε, if $a \neq b$, since $a - b \in L$ because L is a subgroup.

Proposition 4.50. *Every discrete subgroup L of $\mathbb{R}^2$ has one of these forms:*

1. $L = \{0\}$
2. *L is generated as an additive group by one nonzero vector a:*

$$L = \langle ma : m \in \mathbb{Z} \rangle \tag{4.30}$$

3. *L is generated by two linearly independent vectors a and b:*

$$L = \langle ma + nb : m, n \in \mathbb{Z} \rangle \tag{4.31}$$

Groups of the third type are called ***plane lattices****, and the generating set (a, b) is called a* ***lattice basis****.*

Proof. Let L be a discrete subgroup of $\mathbb{R}^2$. The possibility that $L = \{0\}$ is included in the list. If $L \neq \{0\}$, there is a nonzero vector $a \in L$, and we have two possibilities:

> Case 1: All vectors in L lie on one line l through the origin. We choose a vector $a \in L$ of minimal length. We claim that L is generated by a. Let $v \in L$. Then it is a real multiple $v = ra$ of a, since $L \subset l$. Take out the integer part of r, writing $r = n + r_0$, where n is an integer and $0 \leq r_0 < 1$. Then $v - na = r_0 a$ has length less than a, and since L is a group, this element is in L. Therefore, $r_0 = 0$. This shows that v is an integer multiple of a, and hence it is in the subgroup generated by a, as required.

Case 2: The elements of L do not lie on a line. Then L contains two linearly independent vectors a', b'. We start with an arbitrary pair of linearly independent vectors, and we try to replace them with vectors that will generate L. To begin, we replace a' with the shortest vector a on the line l which a' spans. The discussion of case 1 shows that $l \cap L$ is generated by a. Next, consider the parallelogram P' whose vertices are $0, a, b', a+b'$. Since P' is bounded it only contains finitely many points of L. We search through this set to find a point b whose distance to the line l is as small as possible, but positive. We replace b' with b. Let P be the parallelogram with vertices $0, a, b, a+b$. We note that P contains no points of L except for its vertices. First, notice that any lattice point c in P which is not a vertex must lie on one of the line segments $[b, a+b]$ or $[0, a]$. Otherwise, the two points c and $c-a$ would be closer to l than b, and one of these points would lie in P'. Next, the line segment $[0, a]$ is ruled out since a is the shortest vector on that line l. Finally, if there were a point c on $[b, a+b]$ then $c-b$ would lie in L and on the line segment L. The proof is completed by the second lemma below.

■

Definition 4.51 (Points Groups)**.** Recall that we have a homomorphism $\phi : M \to O$ with kernel T. If we restrict this homomorphism to G, we obtain a homomorphism

$$\phi\Big|_G : G \to O \tag{4.32}$$

where its kernel is $T \cap G$, (which is the subgroup isomorphic to the translation group L_G). The **point group** $\overline{G}$ is the image of G in O. Thus, $\overline{G}$ is a subgroup of O. By definition, a rotation $\rho_\theta \in \overline{G}$ if $t_a\rho_\theta \in G$ for some t_a. The inverse image of an element $\rho_\theta \in \overline{G}$ consists of all elements of G which are rotations through the angle θ about some point. Similarly, let l denote the line of reflection of $\rho_\theta r$. Its angle with the x-axis is $\frac{1}{2}\theta$. The point group $\overline{G}$ contains $\rho_\theta r$ if there is some element $t_a\rho_\theta r \in G$, and $t_a\rho_\theta r$ is a reflection or glide reflection on lines parallel to l. Note that since G is discrete, so is $\overline{G}$, so it is a discrete subgroup of O.

Proposition 4.52. *A discrete subgroup of O is a finite group.*

Proof. Suppose that G is a discrete subgroup of O. We then proceed in two cases

Case 1: Suppose all elements of G are rotations. If $G = \{1\}$, then G is finite. Otherwise, G contains a rotation ρ_θ for some nonzero angle θ. Then, since G is discrete, there exists $\varepsilon > 0$ so that $|\theta| \geq \varepsilon$ for all rotations ρ_θ. Let θ be the smallest positive, so $\theta \geq \varepsilon$. Now, suppose $\rho_\alpha \in G$. Then, let $k \in \mathbb{Z}$ so that $k\theta \leq \alpha < \theta(k+1)$. It follows that $0 \leq \alpha - k\theta < \theta$, so since G is a subgroup, $\rho_{\alpha - k\theta} \in G$, which implies that $\alpha = k\theta$, so ρ_θ is a generator for G. Now, suppose $n \in \mathbb{N}$ so that $2\pi \leq n\theta < 2\pi + \theta$, so $0 \leq n\theta - 2\pi < \theta$. It follows by the same argument as above that $\theta = \frac{2\pi}{n}$ for some $n \in \mathbb{N}$. In particular, $\rho_\theta^n = \rho_{n\theta} = 1$, so ρ_θ has order n. Then, since G is generated by ρ_θ, $|G| = n$, and hence, G is finite.

Case 2: Suppose that G contains a reflection. Then, via an intelligent choice of coordinate systems, we can suppose without loss of generality that $r \in G$. Let H denote the subgroup of rotations in G. Then from case 1 $H = C_n$ for some $n \in \mathbb{N}$, so in particular, H is finite. Moreover, the $2n$ products ρ_θ^i, $\rho_\theta^i r$, for $0 \leq i \leq n-1$ are in G, so G contains D_n. Suppose $g \in G$. If g is a rotation then $g \in H$ by definition. Otherwise, if g is a reflection, g can be written as $\rho_\alpha r$ for some ρ_α. Then, since $r \in G$, $\rho_\alpha = \rho_\alpha r r \in G$. Thus, $\rho_\alpha \in H$, so $g \in D_n$. Thus, $G = D_n$, and G is finite.

■

Corollary 4.53. *The point group $\overline{G}$ of a discrete group G is either cyclic or dihedral.*

Proposition 4.54 (Relation of Point and Translation Groups)**.** *Let G be a discrete group of M, with translation group $L = L_G$ and point group $\overline{G}$. The elements of $\overline{G}$ carry the group L to itself. In other words, if $\overline{g} \in \overline{G}$, and $a \in L$, then $\overline{g}(a) \in L$*

Proof. To say that $a \in L$ means that $t_a \in G$. So, we have to show that if $t_a \in G$ and $\overline{g} \in \overline{G}$, then $t_{\overline{g}(a)} \in G$. Now by definition of the point group, $\overline{g}$ is the image of some element $g \in G$: $\phi(g) = \overline{g}$. We write $g = t_b\rho$ or $t_b\rho r$, where $\rho = \rho_\theta$. Then $\overline{g} = \rho$ or ρr, according to the case. In the first case

$$g t_a g^{-1} = t_b \rho t_a \rho^{-1} t_b^{-1} = t_b t_{\rho(a)} \rho\rho^{-1} t_{-b} = t_{b+\rho(a)-b} = t_{\rho(a)} \tag{4.33}$$

as required. In the other case

$$g t_a g^{-1} = t_b \rho r t_a r \rho^{-1} t_{-b} = t_b t_{\rho(r(a))} t_{-b} = t_{\rho(r(a))} \tag{4.34}$$

Thus, in both cases $t_{g(a)} \in G$, so the statement holds. ■

Proposition 4.55 (Crystallographic Restriction)**.** *Let $H \subset O$ be a finite subgroup of the group of symmetries of a lattice L. Then*

1. *Every rotation in H has order $1, 2, 3, 4,$ or 6.*
2. *H is one of the groups C_n, D_n, where $n = 1, 2, 3, 4,$ or 6*

Proof. First, note that the second proposition follows from the first by a previous proposition. To prove the first proposition, let θ be the smallest nonzero angle of rotation in H, and let a be a nonzero vector in L of minimal length. Then, since H operates on L, $\rho_\theta(a)$ is also in L; hence $b = \rho_\theta(a) - a \in L$. Since a has minimal length, $|b| \geq |a|$. It follows that $\theta \geq \frac{2\pi}{6}$. Thus, ρ_θ has order ≤ 6. The case that $\theta = \frac{2\pi}{5}$ is ruled out as then the element $b' = \rho_\theta^2(a) + a$ is shorter than a. This completes the proof. ■

Lemma 4.56. *Let L be a discrete subgroup of $\mathbb{R}^2$.*

1. *A bounded subset S of $\mathbb{R}^2$ contains only finitely many elements of L*
2. *If $L = \{0\}$, then L contains a nonzero vector of minimal length*

Proof. 1. Recall that a subset S of $\mathbb{R}^2$ is bounded if it is contained in some larger box, or if the points of S do not have arbitrarily large coordinates. Certainly, if S is bounded so is $S \cap L$. Now, a bounded set which is infinite must contain sum points that are arbitrarily close to each other - so the elements can not be separated by a fixed positive distance ε. This is not the case for L, by definition, so $L \cap S$ is finite.

2. When we say a nonzero vector a has minimal length, we mean that every nonzero vector $v \in L$ has length at least $|a|$. Assume that $L \neq \{0\}$. To prove that a vector of minimal length exists, we let $b \in L$ be a nonzero vector, and let S be the disc or radius $|b|$ about the origin. This disc is a bounded set so it contains finitely many elements of L, including b. Thus, there exists a nonzero vector of minimal length in L in S, as desired.

■

Lemma 4.57. *Let a, b be linearly independent vectors which are elements of a subgroup L of $\mathbb{R}^2$. Suppose that the parallelogram P which they span contains no elements of L other than the vertices $0, a, b, b + a$. Then L is generated by a and b, that is*

$$L = \langle na + mb : n, m \in \mathbb{Z} \rangle \tag{4.35}$$

Proof. Let v be an arbitrary vector of L. Then since (a, b) is a basis of $\mathbb{R}^2$, v is a linear combination, say $v = ra + sb$, where r, s are real. Let $r = m + r_0$ and $s = n + s_0$ where m and n are integers and $0 \leq r_0, s_0 < 1$. Let $v_0 = r_0 a + s_0 b = v - am - bn$. Then v_0 lies in the parallelogram P, and $v_o \in L$. Henc, v_0 is one of the vertices, and since $r_0, s_0 < 1$, it must be the origin. Thus, $v = ma + nb$. This completes the proof of the Lemma and the Proposition above. ■

Definition 4.58 (Primitive)**.** Let L be a lattice in $\mathbb{R}^2$. An element $v \in L$ is called primitive if it is not an integer multiple of another vector in L.

Corollary 4.59. *Let L be a lattice, and let v be a primitive element of L. There is an element $w \in L$ so that the set (v, w) is a lattice basis.*

Observation 4.60 (Classification of the Discrete Group of Motions). Let G be the discrete group of motions. If L_G is trivial, then the homomorphism from G to its point group is an isomorphism, and G is finite. The discrete groups G such that L_G is infinite cyclic (along a line) are the symmetry groups of **frieze patterns**. If L_G is a lattice, then G is a **two-dimensional crystallographic group**, or a **lattice group**. These groups are the groups of symmetries of wallpaper patterns and of two-dimensional crystals.

Proposition 4.61. *Let G be a lattice group whose point group contains a rotation ρ through the angle $\frac{\pi}{2}$. Choose coordinates such that the origin is the point of rotation by $\frac{\pi}{2}$ in G. Let a be a shortest vector in $L = L_G$, let $b = \rho(a)$, and let $c = \frac{1}{2}(a+b)$. Denote by r the reflection about the line spanned by a. Then G is generated by one of the following sets: $\{t_a, \rho\}, \{t_a, \rho, r\}, \{t_a, \rho, t_c r\}$. Thus, there are three such groups.*

Proof. We first note that L is a square lattice generated by a and b. For, a is in L by hypothesis, and a previous proposition asserts that $b = \rho(a)$ is also in L. These vectors generate a square sublatice L' of L. If $L' \neq L$, then by a previous lemma, there exists $w \in L$ such that w is in the square with vertices $0, a, b, a+b$, and is not one of the vertices. But, any such vector should be at a distance less that $|a|$ from at least one of the vertices of v, and the difference $w - v$ would be in L but shorter than a, contrary to the choice of a. Thus, $L = L'$, as claimed.

Now, the elements t_a and ρ are in G, and $\rho t_a \rho^{-1} = t_b$. So, the subgroup H of G generated by $\{t_a, \rho\}$ contains t_a and t_b. Hence, it contains t_w for every $w \in L$. The elements of this group are the products $t_w \rho^i$

$$H = \{t_w \rho^i : w \in L, 0 \leq i \leq 3\} \tag{4.36}$$

This is one of our groups. We now consider the possible additional elements G may contain.

Case 1: Every element of G preserves rotation. In this case, the point group is C_4. Every element of G has the form $m = t_u \rho_\theta$, and if such an element is in G, then ρ_θ is in the point group. So $\rho_\theta = \rho^i$ for some $0 \leq i \leq 3$, and $m\rho^{-i} = t_u \in G$ too. Therefore, $u \in L$, and $m \in H$. Thus, $G = H$ in this case.

Case 2: G contains an orientation-reversing motion. In this case the point group is D_4, and it contains the reflection about the line spanned by a. We choose coordinates so that this reflection becomes our standard reflection r. Then r will be represented in G by an element of the form $m = t_u r$.

Case 2a: The element u is in L; that is, $t_u \in G$. Then $r \in G$ too, so G contains its point group $\overline{G} = D_4$. If $m' = t_w \rho_\theta$ or $t_w \rho_\theta r$ is an element of G, then $\rho_\theta r$ is in G too; hence $t_w \in G$, and $w \in L$. Therefore, G is the group generated by the set $\{t_a, \rho, r\}$.

Case 2b: The element u is not in L. This is the hard case.

Lemma 4.62. *Let U be the set of vectors u such that $t_u r \in G$. Then*

(a) $L + U = U$

(b) $\rho U = U$

(c) $U + rU \subset L$

Proof. If $v \in L$ and $u \in U$, then t_v and $t_u r$ are in G; hence, $t_v t_u r = t_{v+u} r \in G$. This shows that $v + u \in U$, and proves the first point. Next, suppose $u \in U$. Then $\rho t_u r \rho = t_{\rho(u)} \rho r \rho = t_{\rho(u)} r \in G$. This shows that $\rho(u) \in U$ and proves the second point. Finally, if $u, v \in U$, then $t_u r t_v r = t_{u+r(v)} \in G$; hence, $u + r(v) \in L$, which proves the third point. ■

Part 1 of the lemma allows us to choose $u \in U$ lying in the square whose vertices are $0, a, b, a+b$ and which is not on the line segments $[a, a+b]$ and $[b, a+b]$. We write u in terms of the basis (a, b), say $u = xa+yb$, where $0 \leq x, y < 1$. Then $u+ru = 2xa$. Since $u + ru \in L$, x is either 0 or $1/2$. Next, $\rho(u) + a = (1 - y)a + xb$ lies in the square too, and the same reasoning shows that y is 0 or $1/2$. Thus, the three possibilities for u are $1/2a$, $1/2b$, or $1/2(a + b) = c$. But, of $u = 1/2a$, then $\rho(u) = 1/2b$ and $ru = u = 1/2a$, which would imply that $c = 1/2(a + b) \in L$. This is impossibly as c is shorter than a. Similarly, the case for $u = 1/2b$ is impossible. Thus, $u = C$, which means that G is generated by $\{t_a, \rho, t_c r\}$.

■

4.3.2 Lecture

Recall. Recall that $M = \mathbb{R}^n.O_n(\mathbb{R})$ is the group of motions of $\mathbb{R}^n$ preserving $d(v, w)$

Recall. If $\Gamma \subset M$ is finite, then Γ fixes a point p in $\mathbb{R}^n$, so it is conjugate to a subgroup

$$\Gamma \subset O_n(\mathbb{R}) = M_0 \tag{4.37}$$

fixing the origin.

Recall (n=2). For the finite subgroups $\Gamma \subset O_2(\mathbb{R})$, with $\Gamma_+ := \{\gamma \in \Gamma : \det(\gamma) = +1\}$, we have that

1. $\Gamma = \Gamma_+$ is a cyclic group of order $n \geq 1$, generated by $rot(\theta)$, where θ is the smallest possible nonnegative rotation.
2. $\Gamma_+ \trianglelefteq \Gamma$ (of index 2) are the dihedral groups of order $2n$, $n \geq 1$, and that $rrot(\theta)r^{-1} = rot(\theta)^{-1}$, $r \in \Gamma - \Gamma_+$

Observation 4.63. If we consider the regular hexagon, then the cyclic group of order six permutes the vertices of the hexagon (so an orbit of the group is the regular hexagon). Additionally, if we consider reflections through midpoints of edges and vertices, then the dihedral group of order 12 also act on the regular hexagon. Note, that the 6 reflections in D_{12} is grouped in 3s, with 3 going through the edges, and 3 going through the vertices. On the other hand, for the triangle, the reflections of D_3 go through a vertex and midpoint each.

Remark 4.64. For D_{2n}, when n is odd, the elements in $\Gamma - \Gamma_+$ are all conjugate in Γ, while if n is even, then the elements in $\Gamma - \Gamma_+$ form two conjugacy classes with Γ.

Remark 4.65 (Klien Four Group). Note that D_4 =Klien 4 group.

Remark 4.66. For $n \geq 3$, D_{2n} is non-abelian. In general, we can consider D_{2n} as a subgroup of S_n, so $D_{2n} \hookrightarrow S_n$.

Definition 4.67 (Discrete Groups)**.** We want to classify the **discrete** subgroups $\Gamma \subset M$. Take $M = \mathbb{R}^2.O_2(\mathbb{R})$. A subgroup Γ is discrete if it does not contain arbitrarily small rotations or translation. i.e. there is an $\varepsilon > 0$ so that if $t_b \in \Gamma$, then $|b| \geq \varepsilon$, and if $rot(\theta) \in \Gamma$, then $|\theta| \geq \varepsilon$. In general, if $t_b \in \Gamma$, then $|b| \geq \varepsilon$, and if $A \in \Gamma$, $A \in O_n(\mathbb{R})$, A is not arbitrarily close to I_n in the sense that the entries of A are not all within ε of the identity elements. That is, for all $a_{ij} \in A$, $|a_{ij} - I_{ij}| \geq \varepsilon$.

Example 4.68 (Infinite Discrete Subgroup of M)**.** Let $b \neq 0$ in $\mathbb{R}^n$. Take $\Gamma =$ the cyclic group generated by t_b. Then, since the order of t_b is infinite, so is Γ, and no translation has distance less than b, so the subgroup is discrete.

Proposition 4.69 (Classification)**.** *Let Γ be a discrete subgroup of $M = \mathbb{R}^2.O_2(\mathbb{R})$. Consider*

1. *$L = \Gamma \cap \mathbb{R}^2 = \{t_b$ in $\Gamma\}$, which is the additive subgroup of Γ.*
2. *The image $\overline{\Gamma}$ of M in $O_2(\mathbb{R}) \cong M/\mathbb{R}^2$, which is isomorphic to the quotient group Γ/L. (point stabilizer or image of the discrete group in $O_2(\mathbb{R})$)*

Question. What are the possibilities for L?

Answer. The only possibilites are:

1. $L = \{0\}$, so Γ is finite and isomorphic to $\overline{\Gamma}$
2. $L = \mathbb{Z}b$, where $b \neq 0$ is in $\mathbb{R}^2$

3. $L = \mathbb{Z}a + \mathbb{Z}b$ where a and b are linearly independent (over $\mathbb{R}$) in $\mathbb{R}^2$ (the **lattice group**)

Proof. Case 1 is clear, as that is covered in the classification of the finite groups. Then, assume $L \neq \{0\}$:

> Case 2: All vectors in L lie on a line $l \subset \mathbb{R}^2$. Let b be a vector in L, closest to 0 (not necessarily unique). Then, $L = \mathbb{Z}b$. Why? Suppose $b' \in L$. Then $b' = nb + r_0 b$, where $0 \leq r_0 < 1$, and $n \in \mathbb{Z}$. If $r_0 \neq 0$, then $r_0 b \in L$, and $|r_0 b| < |b|$, which is a contradiction. Thus, $r_0 = 0$, and all elements in L are integer multiples of b, so $L = \mathbb{Z}b$.
>
> Case 3: Suppose not all $b \in L$ lie on a line. In other words, L contains a basis of $\mathbb{R}^2$. Take the basis (a, b) in L, with b being the shortest vector in L on $\mathbb{R}b$, and a being the shortest vector in L on $\mathbb{R}a$. (look at below Lemma then come back) Consider the parallelogram P spanned by a and b. Note that by the lemma below, there are finitely many points in L that are in P. Replace b with a point $c \in L \cap P$, such that c is the closest point in P to the line spanned a, but not on it. Then we take a new parallelogram P' spanned by c and a. Note that there can exist no points in $L \cap P'$ on the line $[a, a + c]$, as then subtracting by a would give a point on $[0, c]$ closer to the line spanned by a. Similarly, if any point was on $[c, a + c]$, then subtractin c would give a point closer to the origin than a on the line spanned by a, which would be a contradiction. We claim now, that $L = \mathbb{Z}a + \mathbb{Z}c$. First, note that any $v \in \mathbb{R}^2$ is given uniquely by $v = ra + sc$, $r, s \in \mathbb{R}$, which we may write as $v = (na + r_0 a) + (mc + s_0 c)$, where m and n are integers, and $0 \leq r_0, s_0 < 1$. Then, if $v \in L$, then $r_0 a + s_0 c \in L$, and in particular, $r_0 a + s_0 c \in P'$. But then, $r_0 a + s_0 c$ would be in P' and closer to a then c, which is a contradiction. Thus, $r_0 a + s_0 c = 0$. Therefore, $v = na + mc$, and $L = \mathbb{Z}a + \mathbb{Z}c$. Additionally, $P' \cap L = \{0, a, c, a + c\}$.

■

Observation 4.70. If $b, b' \in L$, then $b - b' \in L$ (where $b - b'$ is the vector of translation of $t_b t_{b'}^{-1} = t_{b-b'}$), so $|b - b'| \geq \varepsilon$ for some fixed ε.

Lemma 4.71. *If S is a bounded subset of $\mathbb{R}^2$, then $S \cap L$ is finite.*

Proof. Suppose for the sake of contradiction that $S \cap L$ is infinite. Then since $S \cap L$ is a bounded infinite subset of $\mathbb{R}^2$, it has a convergent subsequence by Bolzano-Wieirstrass. But then that convergent subsequence is Cauchy, so there exist elements in $S \cap L$ which are arbitrarily close. Therefore, L is not discrete, which is a contradiction. Thus, $S \cap L$ is finite. ■

Observation 4.72. Note that for $\gamma \in \Gamma$, $b \in L$, and $v \in \mathbb{R}^2$, $\gamma(v) = Av$, $t_b(v) = v + b$, and $\gamma^{-1}(v) = A^{-1}v$. Then $\gamma t_b \gamma^{-1}(v) = \gamma t_b(A^{-1}v) = \gamma(A^{-1}v + b) = v + Ab$, where $\gamma(b) = Ab$, so $\gamma t_b \gamma^{-1} = t_{\gamma(b)}$

Lemma 4.73. *$\overline{\Gamma}$ preserves the subgroup $L \subset \Gamma$.*

Proof. Suppose $b \in L$, so $t_b \in \Gamma$. Say $\overline{\gamma} \in \overline{\Gamma}$, and lift it to an element $\gamma \in \Gamma$. Consider $\gamma t_b \gamma^{-1} \in \Gamma$, and note that $\gamma t_b \gamma^{-1} \in L$ since L is a normal subgroup. In particular, $\gamma t_b \gamma^{-1} = \overline{\gamma}(b) = t_{\overline{\gamma}(b)}$, so $\overline{\gamma}(b) \in L$. ■

Proposition 4.74. *We now consider the image $\overline{\Gamma}$ of Γ in $O_2(\mathbb{R})$. Note that if $L = \{0\}$, then $\overline{\Gamma} = C_n, D_{2n}$ for some $n \geq 1$. But, if $L = \mathbb{Z}a + \mathbb{Z}b$, where a, b are independent. Then $\overline{\Gamma} = C_n, D_{2n}$ with $n = 1, 2, 3, 4,$ or 6. In particular, it has order less than or equal to 12.*

Proof 1. Suppose $A \in \overline{\Gamma}$ is a rotation. We wish to show that the order of $A = 1, 2, 3, 4,$ or 6. Consider the characteristic polynomial of A: $x^2 - Tr(A)x + 1 = x^2 - tx + 1$. Then the discriminant $t^2 - 4 \leq 0$. On the other hand, because A stabilizes $L = \mathbb{Z}a + \mathbb{Z}b$, I claim $t = Tr(A)$ is an integer, because the matrix of A with respect to the basis (a, b) has integer entries since it preserves the lattice. Then $t = \pm 2, \pm 1, 0$. Moreover, the trace of a matrix is equal to the sum of its eigenvalues, and for a rotation by an angle θ, its eigenvalues are $e^{i\theta}$ and $e^{-i\theta}$. Thus, $t = 2\cos(\theta)$, so if $t = \pm 2$, we have $\theta = \frac{2\pi}{1}$ and $\theta = \frac{2\pi}{2}$, if $t = \pm 1$ we have $\theta = \frac{2\pi}{3}$ or $\theta = \frac{2\pi}{6}$, and finally if $t = 0$, then $\theta = \frac{2\pi}{4}$. Thus, the possible subgroups of the rotations in Γ are $C_1, C_2, C_3, C_4,$ or C_6 (which also restricts $\overline{\Gamma}$ to C_n, D_{2n}, with $n = 1, 2, 3, 4,$ or 6). ■

Proposition 4.75. *If $L = \mathbb{Z}a$, then $\overline{\Gamma} = C_1, C_2, D_2, D_4 =$ Klien Four Group.*

Proof. Take the line generated by $a \in \mathbb{R}^2$. If $\gamma \in \overline{\Gamma}$, then $\gamma(a) \in L$, so $\gamma(a) = na$. In particular, since γ is in the orthogonal group it preserves distances, so $|\gamma(a)| = |a|$, so $\gamma(a) = \pm a$. Then, if $\gamma \in SO_2(\mathbb{R})$, then $\gamma = I$, or $-I$. Thus, the group $\overline{\Gamma}$ can be $C_1, C_2, D_2,$ or D_4. ■

Question. What is the classification of lattices $L = \mathbb{Z}a + \mathbb{Z}b$ in $\mathbb{R}^2$? (To determine what $\overline{\Gamma}$ can be)

Answer. Changing L to γL with $\gamma \in O_2(\mathbb{R})$ just conjugates $\overline{\Gamma} = Aut(L)$ by γ. Also, changing L to cL, where $c \in \mathbb{R}^\times$, doesn't change $\overline{\Gamma}$.

Remark 4.76. L up to action of $O_2(\mathbb{R})$ and $\mathbb{R}^\times$ on $\mathbb{R}^2$. Scale so the shortest vector in L has length 1 (using $\mathbb{R}^\times_+$). Then, use $SO_2(\mathbb{R})$ so that the shortest a is $a = 1$. Where is the second vector b? First, $|b| \geq 1$. Note that its y-coordinate is non-zero since b and a are linearly independent. Replace b by $-b$, to make the y-coordinate positive. Note that we still get the same subgroup $\mathbb{Z}a + \mathbb{Z}b$. Replace b by $b + ma$ so that its x-coordinate is between $1/2$ and $-1/2$. Then, up to the actions of the orthogonal group and scaling, the b's in one half of the upper cylinder above the circle of radius 1 classify the lattice. Thus, $L \cong L_b$, for b in the described region, and $L_b = \mathbb{Z} + \mathbb{Z}b$. The points on the unit circle, and at the edges

of the region are very important. In particular, if you have b on the outer point, then you will obtain the **hexagonal lattice** (if at the origin and at the tip of each lattic point you put a sphere of a radius a half, you obtain the best packing of two-dimensional space by spheres). The lattice with the basis on the inner portion of the region give the **rectangular lattice**. For the general lattice, if b is *inside* (not on the boundary) the region, then the only possibility of $\overline{\Gamma} = 1, C_2$. If b is orthogonal to a, then $\overline{\Gamma} = 1, C_2, D_2$, or D_4. The only lattices with extra rotations is the rectangular lattice, with $\overline{\Gamma} = 1, C_2, C_4, D_4, D_8$, and the hexagonal lattice, with $\overline{\Gamma} = 1, C_2, C_3, C_6, D_6, D_{12}$.

Remark 4.77. We wish to have a classification of all the lattices in $L = \mathbb{Z}a_1 + ... + \mathbb{Z}a_n \in \mathbb{R}^n$ up to scaling and orthagonal operations, $\mathbb{R}^\times.O_n(\mathbb{R})$ (so far we only have $n \leq 8$)

4.4 Abstract Symmetry: Group Operations

4.4.1 Textbook

Example 4.78 (Abstract Notions of Symmetry)**.** Conjugation in $\mathbb{C}$ can be thought of as a symmetry, with $a + bi \mapsto a - bi$. Then since for any $\alpha, \beta \in \mathbb{C}$, $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$ and $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$, conjugation is compatible with addition and multiplication. Thus, it is an **automorphism** on the field $\mathbb{C}$. Indeed, this is just the bilateral symmetry of the complex plane about the real line, but the statement that it is an automorphism relates to its algebraic structure.

Example 4.79. The cyclic group H of order 3 can also be thought to have bilateral symmetry, with there existing an automorphism on H which interchanges the two non-identity elements.

Definition 4.80. The set of automorphisms of a group H (or any mathematical structure H) forms a group $\operatorname{Aut} H$, with the law of composition being the law of composition of set-theoretic maps. Each automorphism should be thought of as a **symmetry** of H (since it is a permutation of the elements of H which is compatible with the structure of H).

Remark 4.81. From the above definition, we see that the words **symmetry** and **automorphism** can be thought of as being synonymous, except that automorphism describes a permutation of a set which preserves some type of structure, while symmetry often refers to a permutation which preserves a geometric structure.

Definition 4.82 (Operation)**.** Suppose that G is a group and S is a set. An **operation** of G on S is a rule of elements $g \in G$ and $s \in S$ to get an element gs of S. In other words, it is a law of composition, a map $G \times S \to S$, which generally write as

$$g.s \to gs \tag{4.38}$$

In order to be an **operation**, this rule must satisfy the following conditions:

1. $1.s = 1s = s$ for all s (1 is the identity of G)
2. Associative Law: $(gg').s = g.(g'.s)$ for all $g, g' \in G$, and $s \in S$.

Definition 4.83 (G-set)**.** A set S with an operation of G is called a $G - set$. Note that the above definition is really a left-operation of G on S, since elements of G multiply on the left.

Example 4.84. Let $G = M$ be the group of rigid motions of the plane. Then M operates on the set of points of the plane, on the set of lines in the plane, on the set of triangles in the plane, and so on. Let G be the cyclic group $\{1, r\}$ of order 2. Then G operates on the set S of complex numbers, by the rule $r\alpha = \overline{\alpha}$.

Remark 4.85. We call such a law of composition an **operation** since if we fix $g \in G$, but let $s \in S$ vary, then left multiplication by g defines a map from S to itself; let m_g denote the map. Thus

$$m_g : S \to S, \text{ defined by } m_g(s) = gs \tag{4.39}$$

This map describes the way the element g operates on S. Note that m_g is a permutation of S; that is, it is bijective. This follows from the associative axiom of group operations, since m_g has the two-sided inverse

$$m_{g^{-1}} : s \mapsto g^{-1}s \tag{4.40}$$

Definition 4.86 (Orbit)**.** Let S be a set operated on by a group G. Let s be an element of S. Then the **orbit** of s in S is the set

$$O_s := \{s' \in S : \exists g \in G, s' = gs\} \tag{4.41}$$

also sometimes denoted by Gs.

Remark 4.87. If we think of the elements of G as operating on S by permutations, then O_s is the set of images of s under the various permutations m_g.

Example 4.88. If $G = M$ is the group of motions, and S is the set of triangles in the plane, the orbit O_Δ of a given triangle Δ is the set of all triangles congruent to Δ.

Definition 4.89. The orbits of a **group action** are equivalence classes for the relation

$$s \sim s' \iff \exists g \in G : s' = gs \tag{4.42}$$

Being equivalence classes, the orbits partition the set S: S is a union of disjoint orbits.

Remark 4.90. The group G operates on S by operating independently on each orbit. In other words, an element $g \in G$ permutes the elements of each orbit and does not carry elements between orbits.

Definition 4.91. If S consists of just one orbit, we say that G operates **transitively** on S; that is, every element of S is carried to every other one by some element of the group G.

Example 4.92. The set of rigid motions M acts transitively on the set of points in the plane and the set of lines in the plane, but not on the set of triangles in the plane.

Definition 4.93 (Stabilizer)**.** The **stabilizer** of an element $s \in S$ is the subgroup G_s of G of elements leaving s fixed:

$$G_s := \{g \in G : g.s = s\} \tag{4.43}$$

We can describe when two elements $x, y \in G$ act in the same way on an element $s \in S$ in terms of the stabilizer G_s:

$$x.s = y.s \iff x^{-1}y \in G_s \tag{4.44}$$

Example 4.94. Consider the action of the group M of rigid motions on the set of points of the plane. The stabilizer of the origin is the subgroup O of orthogonal operators. Additionally, if S is the set of triangles in the plane and Δ is a particular triangle which happens to be equilateral, then the stabilizer of Δ is the group of its symmetries, a subgroup of M isomorphic to D_3. Note that when we are considering a motion m stabilizing Δ, the motion carries Δ to itself but does not necessarily carry every point on Δ to itself.

Definition 4.95. Let H be a subgroup of a group G (not necessarily normal). Then we shall denote the set of left cosets of H, called the **coset space** of H, by G/H. Note that the coset space is not a group unless H is a normal subgroup of G. We observe that G operates on the coset space G/H in a natural way: let $g \in G$, and let $C \in G/H$ be a coset. Then the group action $g.C$ is defined to be the coset

$$g.C := gC = \{gc : c \in C\} \tag{4.45}$$

Thus, if $C = aH$, then $g.C = gaH$. By the definition of a group, the axioms of group actions are satisfied.

Observation 4.96. Note that the group G acts transitively over the coset space G/H since G/H is the orbit of the coset $1H = H$. Moreover, the stabilizer of the coset $1H$ is the subgroup $H \in G$.

Example 4.97. Let G be the group D_3 of symmetries of an equilateral triangle. Note that $D_3 = \langle r, f : r^3 = f^2 = 1, rf = fr^2 \rangle$. Let $H = \{1, f\}$. This is a subgroup of order 2 with cosets:

$$C_1 = H = \{1, f\}, C_2 = \{r, rf\}, C_3 = \{r^2, r^2 f\} \tag{4.46}$$

and G operates on $G/H = \{C_1, C_2, C_3\}$. Note that every element $g \in G$ determines a permutation m_g on G/H. The elements of G act on G/H as:

$$m_1 : \begin{cases} C_1 \to C_1 \\ C_2 \to C_2 \\ C_3 \to C_3 \end{cases} \quad m_r : \begin{cases} C_1 \to C_2 \\ C_2 \to C_3 \\ C_3 \to C_1 \end{cases} \quad m_{r^2} : \begin{cases} C_1 \to C_3 \\ C_2 \to C_1 \\ C_3 \to C_2 \end{cases} \tag{4.47}$$

and

$$m_f : \begin{cases} C_1 \to C_1 \\ C_2 \to C_3 \\ C_3 \to C_2 \end{cases} \quad m_{rf} : \begin{cases} C_1 \to C_2 \\ C_2 \to C_1 \\ C_3 \to C_3 \end{cases} \quad m_{r^2 f} : \begin{cases} C_1 \to C_3 \\ C_2 \to C_2 \\ C_3 \to C_1 \end{cases} \tag{4.48}$$

We see that all six elements of G yield all six permutations of 3 elements, so

$$G \xrightarrow{\sim} S_3 \cong Perm(G/H) \tag{4.49}$$

Proposition 4.98. *Let S be a $G-$set, and let s be an element of S. Let G_s be the stabilizer of s, and let O_s be the orbit of s. There is a natural bijective map*

$$G/G_s \xrightarrow{\phi} O_s \tag{4.50}$$

defined by

$$aG_s \mapsto as \tag{4.51}$$

Moreover, this map is compatible with the group structure of G in the fact that $\phi(gC) = g\phi(C)$ for every coset C and every element $g \in G$.

Proof. Let S be a set acted upon by a group G, and let $s \in S$. Then the subgroup $G_s \subset G$ is the stabilizer of s in G. That is, for all $g \in G_s$, $g.s = s$. Then, consider the coset space G/G_s, and define a map $\phi : G/G_s \to O_s$ by $aG_s \mapsto as$. Suppose that $aG_s = bG_s$, where $a, b \in G$. Then by definition of coset equivalency, $a^{-1}b \in 1G_s$. It follows that $(a^{-1}b).s = s$, which implies by associativity that $b.s = a.s$. Therefore, by definition $\phi(aG_s) = \phi(bG_s)$. Moreover, for any $g \in G$ and $aG_s \in G/G_s$, $\phi(gaG_s) = (ga).s = g.(a.s) = g.\phi(aG_s)$, so ϕ respects the group structure. Suppose $s' \in O_s$. Then by definition there exists $g \in G$ such that $g.s = s'$. Therefore, $\phi(gG_s) = g.s = s'$, so ϕ is surjective. Moreover, suppose $\phi(aG_s) = \phi(bG_s)$ for some $a, b \in G$. Then by definition $a.s = b.s$, so $s = b^{-1}.(a.s) = (b^{-1}a).s$. Hence, $b^{-1}a \in 1G_s$, so $aG_s = bG_s$, and ϕ is injective. Therefore, ϕ is a bijection of sets. ■

Proposition 4.99. *Let S be a $G-$set, and let $s \in S$. Let s' be an element in the orbit of s, say $s' = a.s$. Then,*

1. *The set of elements g of G such that $g.s = s'$ is the left coset*

$$aG_s := \{g \in G : \exists h \in G_s, g = ah\} \tag{4.52}$$

2. *The stabilizer of s' is a* ***conjugate subgroup*** *of the stabilizer of s:*

$$G_{s'} = aG_sa^{-1} := \{g \in G : \exists h \in G_s, g = aha^{-1}\} \tag{4.53}$$

Proof. Suppose $g \in G$ such that $g.s = s'$. Then observe that $g.s = a.s$, so by associativity and existence of inverses, $(a^{-1}g).s = s$, which implies that $a^{-1}g = h$ for some $h \in G_s$. Then, $g = ah$, which by definition implies $g \in aG_s$. Moreover, if $g' \in aG_s$, then $g' = ah'$ for some $h' \in G_s$. Thefore, $g'.s = (ah').s = a.(h'.s) = a.s = s'$. Next, suppose $g \in G_{s'}$. Note that since $a.s = s'$, $a^{-1}.s' = s$. Then, it follows that

$$(a^{-1}ga).s = (a^{-1}g).s' = a^{-1}.s' = s$$

so $a^{-1}ga \in G_s$. Thus, there exists $h \in G_s$ so that $a^{-1}ga = h$, and hence, $g = aha^{-1} \in aG_sa^{-1}$. Consequently, $G_{s'} \subset aG_sa^{-1}$. Now, suppose $g' \in aG_sa^{-1}$. Then there exists $h' \in G_s$ so that $g' = ah'a^{-1}$. Observe that $g'.s' = (ah'a^{-1}).s' = (ah').s = a.s = s'$, so $g' \in G_{s'}$. Thus, $G_{s'} = aG_sa^{-1}$, completing the proof. ■

Example 4.100. Consider the stabilizer of a point p in the plane, for the operation of group motions. Then we have that $t_p(0) = p$, and the stabilizer of the origin is the orthogonal group O. Thus, by the preceeding proposition,

$$G_p = t_pOt_p^{-1} = t_pOt_{-p} = \{m \in M : m = t_p\rho_\theta t_{-p},\ or\ m = t_p\rho_\theta r t_{-p}\} \tag{4.54}$$

Definition 4.101 (Homomorphism of $G-sets$)**.** A map $S \to S'$ of $G-sets$ is called a **homomorphism of** $G-sets$ if $\phi(gs) = g\phi(s)$ for all $s \in S$ and $g \in G$.

4.4.2 Lecture

Remark 4.102. We have studied the actions of the group $G = \mathbb{R}^2.O_2(\mathbb{R})$ on $\mathbb{R}^2$: we shall now generalize this.

Definition 4.103 (Group Action)**.** Group G actions on a general set S are mappings

$$\begin{array}{ccc} G \times S & \to & S \\ (g, s) & \to & g(s) \end{array} \tag{4.55}$$

with the properties that

$$e(s) = s, \forall s \in S \tag{4.56}$$

and for all $g, g' \in G$,

$$g(g'(s)) = (gg')(s), \forall s \in S \tag{4.57}$$

Example 4.104. When we look at the group of motions $G = \mathbb{R}^2.O_2(\mathbb{R})$ acting on the set $S = \mathbb{R}^2$, for all $(b, A) \in G$ and $s \in S$,

$$(b, A)(s) \mapsto As + b \tag{4.58}$$

We could also take the action of G on the set of lines in $\mathbb{R}^2$. Or, we could take the action of G on the set of triangles in $\mathbb{R}^2$.

Definition 4.105 (Orbit and Stabilizers)**.** For a set S acted upon by a group G, if $s \in S$, then the subset $O_s := \{s' = g(s) : g \in G\} \subset S$ is the **orbit** of s in S, and the subgroup $G_s := \{g \in G : g(s) = s\} \subset G$ is the **stabilizer** of s by G.

Remark 4.106. If we take the actions of $G = \mathbb{R}^2.O_2(\mathbb{R})$ on $\mathbb{R}^2$, then $O_{(0,0)} = \mathbb{R}^2$, since using translation we can take any element to $(0, 0)$, and $G_{(0,0)} = O_2(\mathbb{R})$. Now, consider the line l, equal to the x-axis. Then the orbit of that line under the group of rigid motions is every line, $O_l = S$. If we consider the set of triangles in the plane, the orbit of any given triangle is all triangles which are congruent to it.

Definition 4.107 (Transitive Actions)**.** A group action on a set S is **transitive** if the orbit of some element is all of S. In other words, if there exists $s \in S$ such that $O_s = S$, then we say G acts **transitively** on S.

Example 4.108. The group of motions on $\mathbb{R}^2$ is transitive. However, if we only considered $O_2(\mathbb{R})$, it would not be transitive.

Definition 4.109 (Model Case of the Transitive Action)**.** Let G be a group and let H be any subgroup of G. Let $S = G/H = \{aH : a \in H\}$. Then the G action is by left translation on S, $g(aH) = gaH$. This action is transitve since for the coset H, to take it to any other coset aH, we have the translation $a(H) = aH$. Thus, $O_H = S$. Moreover, $G_H = \{g : gH = H\} = H$. Then, if we want to make a transitive action internally from the group, we take any subgroup of our group, and let the set we will be acting on be the set of (left) cosets, and we take the action to be left translation. Then, the resulting action is transitive, with the orbit of the subgroup being the entire set, and its stabilizer being itself.

Question. What is the stabilizer of another coset?

Answer. It is the set $G_{aH} = \{g : gaH = aH\} = aHa^{-1}$. For instance, observe that $(aHa^{-1})(aH) = aHH = aH$. Thus, it is a conjugate of the original subgroup.

Proposition 4.110 (Transitive Actions)**.** *If G is a transitive action on a set S, and for $s, s' \in S$, $g(s) = s'$ (where $O_s = S$), $G_{s'} = gG_sg^{-1} \subset Gm$ si the stabilizers are conjugate. In fact, this is really no more general than the previous case; because, if G acts transitively in S, and $s \in S$ has stabilizer G_s, then there is a bijection of* ***G-sets*** *(sets with a G action) between S and the cosets of G:*

$$\begin{array}{ccc} G/G_s & \xrightarrow{\sim} & S \\ g & \mapsto & g(s) \end{array} \tag{4.59}$$

which is well defined, because it only depends on the coset, its a surjective map since the action is transitive and its also injective since the inverse image of each point is exactly a coset. Thus, we can identify all transitive actions with the transitive action of a group on the set of the cosets of one of its subgroups. ***A transitive action is exactly the same as a conjugacy class of subgroups of $G_s \subset G$.***

Observation 4.111. Suppose that we have a G action on a set S. Then G partitions S into orbits, and on each orbit we have a transitive action. In particular, on each orbit we have a conjugacy class of subgroups of G, such that the orbit is identified on the action on cosets of those subgroups.

Remark 4.112 (Counting Formula). If G and S are finite, then since $G/G_s \xrightarrow{\sim} S$, $[G : G_s] = |G/G_s| = |S|$, and $|G| = |G_s|[G : G_s] = |G_s||S|$.

Definition 4.113. G acts on $S = G$ by conjugation

$$s \mapsto gsg^{-1} \tag{4.60}$$

and orbits = conjugacy classes, and $G_s =$ **centralizer of s** $= g \in G : gs = sg\}$.

4.5 Counting Formula

4.5.1 Textbook

Recall. Let H be a subgroup of a group G. All cosets of H in G are in bijective correspondance, and hence have the same number of elements: $|H| = |aH|$ for all $a \in G$. Since G is the union of non-overlapping cosets, and the number of cosets of H is its index in G, which we write as $[G : H]$, we have the fundamental formula

$$|G| = |H|[G : H] \tag{4.61}$$

Proposition 4.114. *Let S be a $G-$ set, and let $s \in S$. Then*

$$|G| = |G_s||O_s| \tag{4.62}$$

Equivalently, the order of the orbit is equal to the index of the stabilizer in G:

$$|O_s| = [G : G_s] \tag{4.63}$$

Observation 4.115. We may partition S into orbits to count its elements

$$|S| = |O_{s_1}| + |O_{s_2}| + ... + |O_{s_k}| \tag{4.64}$$

Definition 4.116 (Restriction)**.** Suppose G acts on a set S, and let H be a subgroup of G. We may restrict the operation to get an action of H on S. Note that the **H-orbit** of an element will be contained in its G-orbit. We may take a single G-orbit and decompose it into H-orbits.

Proposition 4.117. *Let H and K be subgroups of a group G. Then the index of $H \cap K$ in H is at most equal to the index of K in G:*

$$[H : H \cap K] \leq [G : K] \tag{4.65}$$

Proof. Let us denote $G/K = S$, and $1K$ by s. Thus, $|S| = [G : K]$. First, note that the stabilizer of s is the subgroup K. We now restrict the action of G to the subgroup H, and decompose S into H-orbits. The stabilizer of s for this restricted operation is $H \cap K$. Moreover, the H orbit, O, of s is of course a subset of S. Then, by the previous proposition, $|O| = [H : H \cap K]$. Therefore, $[H : H \cap K] = |O| \leq |S| = [G : K]$. ■

4.5.2 Lecture

Recall. A group action of a group G on a set S is a map:

$$G \times S \to S \tag{4.66}$$

$$(g, s) \mapsto gs \tag{4.67}$$

We also have for every $s \in S$, its orbit $O_s \subset S$, and its stabilizer $G_s \subset G$, and we can identify the orbit as a set with the set of cosets of the stabilizer

$$G/G_s \xrightarrow{\sim} O_s \tag{4.68}$$

Moreover, if you took $s' = g(s)$, then its stabilizer is the conjugate subgroup $G_{s'} = gG_sg^{-1}$. Thus, a transitive action can always be identified with the transitive actions on coset spaces of stabilizer subgroups, G/G_s. Therefore, all transitive actions of a group can be built up internally from its subgroups.

Proposition 4.118 (Counting Formula)**.** *Suppose G acts on S, with orbits $O_{s_1}, O_{s_2}, ..., O_{s_n}$, and $|G|$ and $|S|$ are finite. Then, $|S| = |O_{s_1}| + ... + |O_{s_n}|$ since S is partitioned by the orbits of G. Moreover, since every orbit is identified with a coset space G/G_{s_i}, and $|G/G_{s_i}| = \frac{|G|}{|G_{s_i}|}$, we find that*

$$|S| = |G/G_{s_1}| + ... + |G/G_{s_n}| = |G| \sum_{i=1}^{n} \frac{1}{|G_{s_i}|} \tag{4.69}$$

Proposition 4.119. *Suppose G is a finite group with subgroups H and K, and their intersection $H \cap K$. Then$[G : K] \geq [H : H \cap K]$.*

Proof. Let $S = G/K$, so $|S| = [G : K]$. Note that G acts transitively on S. We can restrict of G on S to the subgroup H, to get an H action. This action is a union of H orbits. Consider the orbit of the coset $s = eK$ under the action of H. Then, $O_s \cong H/H_s$, where $H_s = \{h \in H : hK = K\} = H \cap K$. Since $|O_s| \leq |S|$ by the counting formula, we have that $[H : H \cap K] = |H/H \cap K| \leq |S| = [G : K]$. ■

Definition 4.120 (Class Equation)**.** G acts transitively on $S = G$ by left multiplication

$$g(s) = gs \tag{4.70}$$

$$O_e = G \tag{4.71}$$

But, there is a more interesting action of G on itself, by conjugation

$$g(s) = gsg^{-1} \tag{4.72}$$

However, unless the group is the trivial group, this action is not transitive since $O_e = \{e\}$, and $G_e = G$. Thus, you cannot conjugate a non-identity element into the identity. The orbits of this action are called **conjugacy classes of S** by definition. Moreover, from before we have the **class equation**

$$|G| = \sum_{conj\ classes} |O_s| = \sum_{conj\ classes\ of\ G} \frac{|G|}{|Z_s|} \tag{4.73}$$

Where

$$Z_s := \{g \in G : gs = sg\} \tag{4.74}$$

is the **centralizer** of s in G.

Remark 4.121. Suppose G is abelian, so the centralizer of every element in G is G. Consequently, in an abelian group every orbit has one element in it, so each element is the only element in its own conjugacy class.

Example 4.122. Take $G = S_3$. Then one conjugacy class is $\{e\}$. Another is the elements of order 2 (transpositions). Finally, the two elements of order 3 also form a conjugacy class (cycles). Then the class equation is

$$6 = 1 + 3 + 2 \tag{4.75}$$

Where $|Z_e| = 6$, $|Z_\tau| = 2$ (the identity and itself), $|Z_\sigma| = 3$ ($Z_\sigma = \{e, \sigma, \sigma^2\}$).

Remark 4.123. Although $|S_n| = n!$, the number of conjugacy classes $= p(n) =$ the number of partitions of n (look up partition function).

Remark 4.124 (Monster Group). The monster group G has order $G \sim 10^{47}$, but it has less than 200 conjugacy classes.

Question. For conjugation action, when is $|O_s| = 1$?

Answer. Well since $|O_s| = \frac{|G|}{|G_s|}$, this question is equivalent to asking when $|G_s| = |G|$, i.e. when $G = G_s$. Well G_s is the set of elements that commute with s. Thus, every element must commute with s, which implies that s is in the center of the group G, $s \in Z(G)$ (canonical normal subgroup).

Remark 4.125. The number of elements for which their orbit under the conjugacy action is 1 is the order of the center.

Theorem 4.126 (Non-trivial Center)**.** *If the order of G is $|G| = p^n$, with p a prime, then $Z(G) \neq \{e\}$.*

Proof. For all elements s, $|G|/|Z_s| = p^b$ with $0 \leq b \leq n$. Thus, all orbits must be divisible by p, except when $b = 0$, and $|O_s| = 1$ (so the centralizer is the full group). Therefore, all the terms except the central conjugacy classes are divisble by p, and the order of G is divisible by p, so by the class equation

$$|G| = \sum_{conj\ classes} \frac{|G|}{|Z_s|} \tag{4.76}$$

the number of ones on the right hand side must by divisible by p, and since there is always at least one (with the identity),there are non-trivial elements with full centralizer, which implies they are in the center of G. Thus, the center is non-trivial. ■

Observation 4.127. If G is of prime power order, and $Z(G)$ is the center of G, then the quotient group $G/Z(G) = G_1$ also has prime power order, being less than G, and therefore it also has a non-trivial center $Z_1 = Z(G/Z(G))$, so its quotient group G_1/Z_2 has prime power order less than G_1, and we can continue down until we arrive at the trivial group. We can then build our group up from these non-trivial centers.

Proposition 4.128. *Thus, G is not simple, unless $|G| = p$.*

Theorem 4.129 (Burnside)**.** *If the order of G is $|G| = p^n q^m$, where p and q are prime, then G is* not *simple.*

Example 4.130. For the alternating group A_5, with order $|A_5| = 60 = 2^2 * 3 * 5$, A_5 is in fact simple.

Remark 4.131 (Counting Formula Part 2). Consider finite subgroups $G \subset SO_3(\mathbb{R})$, preserving the regular solids in $\mathbb{R}^3$. Note that elements of $SO_3(\mathbb{R})$ act on three space and preserve the points on the sphere of radius 1 centered at the origin. Let us call such a sphere $S^2 \in \mathbb{R}^3$. Note that from before, every $g \in G$ is a rotation about an axis. Thus, there exists a basis such that

$$A = \left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & rot(\theta) \end{array}\right] \tag{4.77}$$

where rotations are done in the plane perpendicular to the axis.

1. First, let us consider the tetrahedron inscribed in the sphere, which has three triangles around a vertex; the 4 vertices touch the sphere, with the tetrahedron having 6 edges and 4 faces, with every face being an equilateral triangle. Question: What is the

subgroup of $SO_3(\mathbb{R})$ which preserves the tetrahedron? Since there are four vertices, the G preserving tetrehedron is a subgroup of S_4 = the permutation of the vertices. Take the axis that goes through the vertex and the barycenter of the triangle - there are three rotations around this axis which preserves the tetrahedron. In particular,this group acts transitively on the set S of vertices, since can switch the vertex by which we are rotating. Therefore, $|O_s| = 4 = |G|/|G_{stabi}|$, and $|G_{stabi}| = 3$, so $|G| = 12$, which implies that $G \cong A_4$, as it is the only subgroup of S_4 of order 12.

2. Now, let us consider the regular solid, the octahedron, which has four triangles around a vertex. If we consider an axis through two opposite vertices. We then have a rotation of order 4. Moreover, the action on the octahedron is transitive, and the stabilizer of any vertex is of order 4, so the group G is of order $|G| = 4 * 6 = 24$. This happens to be the symmetric group on four letters, with the four objects being permuted being lines intersecting the mid-points of opposite parallel edges.

3. Our final case is an icosahedron, which has five triangles around a vertex, twelve vertices, twenty faces, and thirty edges. Since it permutes the vertices transitively, and each vertex has five points faces coming out of it, which gives it five rotations that fix that vertex. Thus, the order of the group is $|G| = 12 * 5 = 60$, and $G \cong A_5$ (the first simple group).

Remark 4.132. If G is a group action on $G/H = S$. Suppose $H \trianglelefteq G$. Then $G_s = H$ for all s (since a normal subgroup doesn't move under conjugation).

4.6 Regular Solids

Recall. Finite groups associated to the regular solids in $\mathbb{R}^3$, and let $\Gamma \subset SO_3(\mathbb{R})$ be the rotations preserving the regular solid of interest, S.

Definition 4.133 (Classification)**.** The regular solids are

1. S = the tetrahedron, and Γ is of order 12, and isomorphic to A_4 (permuting the vertices)

2. S = the octahedron, and cube, with Γ of order 24, isomorphic to S_4, permuting the diagonals of the cube

3. S = icosahedron, and dodecahedron, with Γ of order 60, which is isomorphic to A_5, permuting inscribed squares in the dodecahedron. (moreover, we shall show A_5 is simple, and in fact its the smallest simple group of non-prime order)

Recall (Abelian Simple Groups). The only abelian simple groups are the cyclic groups of prime order $\cong \mathbb{Z}/p\mathbb{Z}$.

Remark 4.134 (Tetrahedron). We have the identity rotation, e, of order 1. Each vertex has two non-trivial rotations, each of order three, giving a total of 8 rotations of order 3 preserving the tetrahedron. There are also 3 rotations of order 2, which switch pairs of vertices and rotates about the line going through the midpoint of opposite perpendicular edges. Let us enumerate the vertices by

$$\begin{array}{ccc} 1 & & 2 \\ & 4 & \\ & 3 & \end{array}$$

Then the identity permutation is (1)(2)(3)(4) (or simply (1)), and we have rotations such as (1 2 3)(4), (1 3 2)(4), (1)(2 3 4), (1)(2 4 3), (2)(1 3 4), (2)(1 4 3), (3)(1 2 4), (3)(1 4 2), which are our rotations of order 3.

Notation 4.135 (Notating Permutations). The cycle notation of permutations writes permutations in brackets, with elements permuting left to right. For example, if we consider the set $\{1, 2, 3, 4\}$, the permutation (1 2) takes 1 to 2, 2 to 1, and fixes 3 and 4. Additionally, the permutation (1 4)(2 3) takes 1 to 4, 4 to 1, 2 to 3, and 3 to 2. Another permutation is (1 2 3)(4) (where (4) is optional), where 1 goes to 2, 2 goes to 3, 3 goes to 1, and 4 is fixed. Let us consider a permutation on $\{1, 2, 3, 4, 5\}$. The permutation (1 2)(3 5 4) so 1 goes to 2, 2 to 1, 3 to 5, 5 to 4, and 4 to 3.

Remark 4.136 (Cube). The cube has 8 vertices, 6 faces, and 12 edges. The stabilizer of a face, Γ_f, is of order 4, and since the action is transitive (any face can be taken to any other face), the order of Γ is 24. Since there are 8 vertices, there are 4 diagonals in the cube which are permutted by Γ. Thus, Γ is a subgroup of S_4, and since it is of the same order, it is isomorphic to S_4.

Remark 4.137 (Dodecahedron). The dodecahedron has 12 faces (which are pentagons), 20 vertices, and 30 edges. Consider the stabilizer of a face, Γ_f. The order of the stabilizer is 5 (and it's cyclic). Therefore, the order of Γ is 60.

Remark 4.138 (Conjugacy Classes in Γ). The 12 faces give 6 different subgroups isomorphic to $\mathbb{Z}/5\mathbb{Z}$, since the for pairs of opposite faces we have the same rotations. Then, since the intersection of two subgroups is also a subgroup of $\mathbb{Z}/5\mathbb{Z}$, and 5 is prime, their intersection must be the trivial subgroup $\{e\}$. Additionally, in each subgroup we have 4 distinct elements of order 5. Hence, we have 24 elements of order 5. If consider rotations about an axis through opposite edges, we have only the identity and the 180° rotation, which is an element of order 2. Therefore, since we have 30 edges, by pairing we have 15 different subgroups isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Thus, we have 15 elements of order 2. Finally, if we rotate about an axis through opposite vertices, we have two rotations of order 3 (and the identity). Therefore, we have 10 different subgroups isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Hence, we have 20 elements of order 3. Then, note that

$$60 = 1_{order\ 1} + 15_{order\ 2} + 20_{order\ 3} + 24_{order\ 5} \tag{4.78}$$

Note that conjugate elements have the same order. Moreover, the order of a conjugacy class of $g = \frac{|G|}{|Z_g|}$, so it divides the order of $|G|$. Thus, the elements of order 5 are not all conjugate since 24 does not divide 60. In fact, it breaks up into two conjugacy classes - both of order 12. The 15 elements of order 2 are conjugate, as we can permute the edges transitively. Say $g^2 = e$, fixing a pair of oppositive edges (12), and let $g'^2 = e$ fix (34). Let $h \in G$ take edge 1 to edge 3, then since it preserves the dodecahedron, 2 goes to 4. Then $g' = hgh^{-1}$, since $hgh^{-1}(3) = 3$, and $hgh^{-1}(4) = 4$ and has order 2. Note that by the same argument the six subgroups stabilizing pairs of faces are conjugate in Γ, and likewise for the 10 subgroups that fix pairs of vertices. **However, we do not necessarily have that the all of the elements of the subgroups are conjugate**. This does hold for the 10 subgroups of order 3, but not for the six of order four. The case for vertices can be shown as the elements in any of the subgroups are conjugate, as you can switch the vertices and change rotations into other ones. However, for the elements of order five, such an action takes a rotation to its inverse, so not all elements of the subgroup are conjugate with one-another. This breaks up the 24 elements of order 5 into two conugacy classes of order 12 (one by $\pm\frac{2\pi}{5}$, and one by $\pm\frac{4\pi}{5}$. Finally we have five conjugacy classes of size 1, 15, 20, 12, and 12.

Proposition 4.139 (A_5 is Simple)**.** $\Gamma \cong A_5$ *is a simple group.*

Proof. Let $H \trianglelefteq \Gamma$, with $H \neq \{e\}$. Then since $gHg^{-1} = H$ for all $g \in G$, H is a union of conjugacy classes. So $H = 1+$ some of the terms (15,20,12, and 12). However, no combination of these terms, except all terms, divides $|\Gamma|$. Thus, the only normal subgroup that is not the identity is the full group, so Γ is simple. ■

Remark 4.140. In our notation for permutations, $g = (1\ 2\ 3\ 4\ 5)$ and $g' = g^2 = (1\ 3\ 5\ 2\ 4)$ are conjugate in S_5, but *not* in A_5.

5 Rings

5.1 Basic Definitions for Rings

5.1.1 Textbook

Example 5.1 (Motivating Example)**.** We consider **subrings** of the field $\mathbb{C}$, which is a subset closed under addition, subtraction, multiplication, and contains 1, but is not necessarily closed under division. A specific example is the **Gaussian Integers**, which are complex numbers $a + bi$, where a and b are integers. The ring is denoted by

$$\mathbb{Z}[i] := \{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\} \tag{5.1}$$

The Gaussian Integers are the points of a square lattice in the complex plane.

Example 5.2 (Generalization of Gaussian Integers)**.** For any $\alpha \in \mathbb{C}$, the subring $\mathbb{Z}[\alpha]$ is defined to be the smallest subring of $\mathbb{C}$ containing α, and we call it the **subring generated by** α. In particular, $\mathbb{Z}[\alpha]$ contains all complex numbers β of the form

$$\beta = a_n\alpha^n + \ldots + a_1\alpha + a_0, a_i \in \mathbb{Z} \tag{5.2}$$

Definition 5.3 (Algebraic)**.** A complex number α is **algebraic** if it is a root of a polynomial integer coefficients, that is, if some expression of the form above is zero.

Definition 5.4 (Transcendental Numbers)**.** If there is no polynomial with integer coefficients having α as a root, then α is called a **transcendental** number. The numbers e and π are examples of transcendental numbers.

Corollary 5.5. *If α is transcendental, then two distinct polynomial expressions over α must represent different complex numbers. In this case the elements of the ring $\mathbb{Z}[\alpha]$ correspond bijectively to polynomials $p(x)$ with integer coefficients, by the rule $p(x) \leftrightarrow p(\alpha)$.*

Definition 5.6 (Ring)**.** A **ring** R is a set with two laws of composition $+$ and $\times$, called addition and multiplication, which satisfy these axioms:

1. With the law of composition $+$, R is an abelian group, with identity denoted by 0. This abelian group is denoted by $R^+ = (R, +)$
2. Multiplication is associative and has an identity element 1 (not always required)

3. Distributive Laws: For all $a, b, c \in R$

$$(a+b)c = ac + bc, \text{ and } a(b+c) = ab + ac \tag{5.3}$$

Definition 5.7 (Subring)**.** A **subring** of a ring R is a subset which is closed under operations of addition, subtraction, and multiplication, and which contains 1 (not always)

Remark 5.8. From here on out, unless otherwise stated, a ring refers to a **commutative ring with identity**.

Example 5.9. The ring $\mathbb{R}^{n\times n}$ is an example of a non-commutative ring with identity.

Definition 5.10 (Polynomial Ring)**.** Given a ring R, a polynomial in indeterminate x with coefficients in R is an expression of the form

$$a_n x^n + \ldots + a_1 x + a_0 \tag{5.4}$$

with $a_i \in R$. The set of these polynomials form a ring which is denoted by $R[x]$.

Proposition 5.11. *Let R be the ring in which $1 = 0$. Then R is the zero ring, i.e. $R = \{e\}$.*

Proof. We first note that $0a = 0$ for any element $a \in R$, since $0a = (0+0)a = 0a + 0a$, and then since R has additive inverses, it has the cancellation law and we find that $0a = 0$. Assume that $0 = 1$ in R, and let a be any element of R. Then $a = 1a = 0a = 0$. Thus, every element of R is 0, which means that R is the zero ring. ■

Definition 5.12 (Units)**.** An element a in a ring R is said to be a **unit** if a has a multiplicative inverse in R. The identity element 1 in any ring R is always a unit.

5.1.2 Lecture

Example 5.13 (Motivating Examples)**.** Examples of rings: $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{C}$, F-field

Definition 5.14 (Ring)**.** A **ring**, R, is a set which is an abelian group an addition operation $+$, with an identity element denoted 0, as well as a multiplication operator $\times$ which is associative and with identity denoted 1. Moreover, there exist distributive laws for the ring:

$$a(b+c) = ab + ac \text{ and } (a+b)c = ac + bc \tag{5.5}$$

for all $a, b, c \in R$.

Definition 5.15 (Subring)**.** A subring $R' \subset R$ is a subset which contains 0 and 1, is a subgroup under $+$, and is closed under multiplication.

Example 5.16 (Subrings of $\mathbb{C}$)**.** Consider subrings of $R = \mathbb{C}$. We have $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, and the Gaussian Integers

$$\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i = \{a + bi : a, b \in \mathbb{Z}\} \tag{5.6}$$

Example 5.17 (Polynomials over $\mathbb{C}$)**.** Let $R =$ all polynomials in 1 variable x over $\mathbb{C} = \{a_n x^n + \ldots + a_1 x + a_0 : a_i \in \mathbb{C}\} = \mathbb{C}[x]$. More generally, if R is a commutative ring, so is $R[x]$. For example, if we take $\mathbb{Z}/2\mathbb{Z} = R$, then an expression $(x+1)(x+1) = x^2 + 2x + 1 = x^2 + 1$, where $2 = 0$ in R. We can also take polynomials over a ring of polynomials. Say $\mathbb{C}[x][y] = \mathbb{C}[x, y]$ is a polynomial in two variables (the order of x and y doesn't matter).

Question. How small can a ring be?

Answer. The smallest ring is the zero ring, $R = \{0\}$, so $1 = 0$.

Lemma 5.18. *If $R \neq \{0\}$ then $1 \neq 0$ in R.*

Proof. Let $a \in R$, and suppose $1 = 0$. Then $a = 1.a = 0.a$, but $0.a = (0+0).a = 0.a + 0.a$, which implies that $0.a = 0$. Thus, if $1 = 0$, then for all $a \in R$, $a = 0$ and $R = \{0\}$. ■

Remark 5.19 (Constructing Any Ring). The best way to get rings (which are called **endomorphism rings**) is to sart with an abelian group $(A, +, 0)$. Let $R = End(A) := \{f : A \to A\}$ homomorphisms. We now define the structure of R:

$$(f+g)(x) = f(x) + g(x) \tag{5.7}$$

Since the addition in the group A is commutative, the addition in R is also commutative. Moreover, we have the zero element

$$0(x) = 0_A \tag{5.8}$$

so $0 + f = f$. Additive inverses are defined such that $(-f)(a) = -(f(a))$. We define the multiplication law as

$$(f \times g)(a) = f(g(a)) \tag{5.9}$$

Then this operation is naturally associative, and the multiplicative identity is

$$1(a) = a \tag{5.10}$$

Note that from these definitions, we see that multiplication is not necessarily commutative, and does not necessarily have an inverse, as f has an inverse $\iff$ it is an isomorphism of groups.

Example 5.20 (Constructing Rings from Endomorphisms on Cyclic Groups)**.** The ring $\mathbb{Z} = End(\mathbb{Z}, +, 0)$. Suppose we have a map $f : \mathbb{Z} \to \mathbb{Z}$ (a group homomorphism). Then $f(a) = n \in \mathbb{Z}$ determines everything, since $f(k) = f(1+1+...+1) = f(1)+...+f(1) = kf(1)$. We take f, and associate to it the integer $f(1)$, which then gives a multiplication on $\mathbb{Z}$. For example: Suppose $f(1) = n$, and $g(1) = m$, then $f \times g(k) = f(g(k)) = f(k \cdot m) = n(k \cdot m)$, which gives multiplication on $\mathbb{Z}$. Now, suppose f is associated to a negative integer, so $f(1) = n < 0$, then it switches the halfs of the real line. Then, $f \times f(1) = f(f(1)) = f(n) = f(-1 - 1 - ... - 1) = -f(1) - f(1) - ... - f(1) = -n - n - ... - n > 0$. Likewise, $\mathbb{Z}/n\mathbb{Z} = End(\mathbb{Z}/n\mathbb{Z}, +, 0)$, where we identity f by $f(1)$. This works to give a ring structure on cyclic groups.

Example 5.21 (Constructing Rings from Endomorphisms of other Abelian group)**.** Take $A = (\mathbb{Z}/p\mathbb{Z})^2 = \{(a_1, a_2) : a_i \in \mathbb{Z}/p\mathbb{Z}$. Then $End(A) = M_2(\mathbb{Z}/p\mathbb{Z})$. If we have a matrix

$$B = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \tag{5.11}$$

This is an example of a non-commutative ring. In general, if $A = (\mathbb{Z}/p\mathbb{Z})^n$, then $End(A) = M_n(\mathbb{Z}/p\mathbb{Z})$.

5.2 Construction of Polynomials and the Integers

5.2.1 Textbook

Definition 5.22 (Construction and Axioms of $\mathbb{N}$)**.** We define the set $\mathbb{N}$, called the set of natural numbers, to be the set of positive integers. It is characterized by these properties, called **Peano's axioms**:

1. The set $\mathbb{N}$ contains a particular number 1
2. **Successor function**: There is a map $\sigma : \mathbb{N} \to \mathbb{N}$ that sends every integer $n \in \mathbb{N}$ to another integer, called the next integer or successor. This map is injective, and for every $n \in \mathbb{N}$, $\sigma(n) \neq 1$.

3. **Induction Axiom**: Suppose that a subset S of $\mathbb{N}$ has these properties

   (a) $1 \in S$

   (b) if $n \in S$ then $\sigma(n) \in S$.

   Then S contains every natural number: $S = \mathbb{N}$

Definition 5.23 (Recursive Definitions)**.** Peano's axioms allow us to make **recursive definitions**. Such definitions refer to the definition of a sequence of objects O_n indexed by the natural numbers in which each object is defined in terms of the preceding. The important notes are that

1. O_1 is defined
2. a rule is given to define $O_{\sigma(n)}$ in terms of O_n.

Definition 5.24 (Addition and Multiplication)**.** Using $\mathbb{N}$ and the ability to make recursive definitions, we define addition and multiplication as

$$m + 1 = \sigma(m) \text{ and } m + \sigma(n) = \sigma(m + n) \tag{5.12}$$

and

$$m \cdot 1 = m \text{ and } m \cdot n' = m \cdot n + m \tag{5.13}$$

Definition 5.25 (Polynomial)**.** A **polynomial** with coefficients in any ring R is to mean a linear combination of powers of the indeterminate variable

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \tag{5.14}$$

where $a_i \in R$. Such expressions are often called **formal polynomials**. We consider the monomials x^i as independent.

The **degree** of a nonzero polynomial is the largest integer k such that the coefficient a_k of x^k is non-zero. The coefficient of the highest degree term of a polynomial which is not zero is called its **leading coefficient**, and a **monic** polynomial is one in which its leading coefficient is 1.

In standard form we write a polynomial as

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots \tag{5.15}$$

where $a_i \in R$, and only finitely many coefficients are nonzero. Formally, the polynomial is determined by a sequence of coefficients a_i

$$\mathbf{a} = (a_0, a_1, a_2, ...) \tag{5.16}$$

where $a_i \in R$ and only a finite number of a_i are not zero. The sequence with 1 in the ith position and zero everywhere else corresponds to the indeterminate monomial x^i, and the monomials form a basis of the space of polynomials.

Addition and multiplication of polynomials $f(x) = a_0 + a_1 x + \ldots$ and $g(x) = b_0 + b_1 x + \ldots$ is given by

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots = \sum_{i=0} (a_i + b_i)x^i \tag{5.17}$$

Multiplication is done by collectin monials of equal power, giving

$$f(x)g(x) = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + \ldots = \sum_{i=0} \left(\sum_{k=0}^{i} a_{i-k} b_k \right) x^i \tag{5.18}$$

Proposition 5.26. *There is a unique commutative ring structure on the set of polynomials $R[x]$ having these properties:*

1. *Addition of polynomials is done coefficient wise for equal degree monomials (like vector addition)*
2. *Multiplication of monomials is given by the rule above*
3. *The ring R is a subring of $R[x]$, when the elements of R are identified with the constant polynomials*

Definition 5.27 (Polynomials in Multiple Variables)**.** Let $x_1, ..., x_n$ be variables (indeterminates). A **monomial** is a formal product of these variables of the form

$$x_1^{i_1} x_2^{i_2} ... x_n^{i_n} \tag{5.19}$$

where the exponents i_v are nonnegative numbers. The n-tuple $(i_1, ..., i_n)$ of exponents determines the monomial. Such an n-tuple is called a **multi-index**, and vector notation $\mathbf{i} = (i_1, ..., i_n)$ for multi-indices is convenient. Using it, we may write the monomial symbolically as

$$x^{\mathbf{i}} = x_1^{i_1} x_2^{i_2} ... x_n^{i_n} \tag{5.20}$$

The monomial $x^{\mathbf{0}}$ is denoted by 1.

A polynomial with coefficients in a ring R is a finite linear combination of monomials with coefficients in R. Using the shorthand, any polynomial $f(x) = f(x_1, ..., x_n)$ can be written uniquely in the form

$$f(x) = \sum_i a_i x^{\mathbf{i}} \tag{5.21}$$

And only finitely many of the coefficients $a_i \in R$ are different from zero.

A polynomial which is the product of a nonzero element $r \in R$ with a monomial is also called a monomial

$$m = r x^{\mathbf{i}} \tag{5.22}$$

Using multi-index notation, the addition and multiplication for polynomials in multiple variables is analoguous to the case for one variable using the formulas defined above, and the above proposition also holds analoguously for polynomials in multiple variables.

A ring of polynomials in severable variables with coefficients in the ring R is denoted by

$$R[x_1, ..., x_n] \text{ or } R[x],\ x = (x_1, ..., x_n) \tag{5.23}$$

5.3 Ring Homomorphisms and Ideals

5.3.1 Textbook

Definition 5.28 (Ring Homomorphism)**.** A **ring homomorphism** $\phi : R \to R'$ is a map compatible with the laws of composition, and which carries 1 to 1, that is for all $a, b \in R$,

$$\phi(a + b) = \phi(a) + \phi(b),\ \phi(ab) = \phi(a)(\phi(b),\ \phi(1) = 1 \tag{5.24}$$

Definition 5.29 (Ring Isomorphism)**.** An isomorphism of rings is a ring homomorphism which is bijective. To rings which have a ring isomorphism between them are said to be isomorphic as rings.

Example 5.30 (Evaluation Homomorphisms)**.** The evaluation map of a ring of polynomials is a ring homomorphisms. For example, if we consider the real polynomials and $a \in \mathbb{R}$, then the evaluation map

$$\mathbb{R}[x] \to \mathbb{R}, p(x) \mapsto p(a) \tag{5.25}$$

is a ring homomorphism. We can also evaluate $\mathbb{R}[x]$ at complex numbers such as i

$$\mathbb{R}[x] \to \mathbb{C}, p(x) \mapsto p(i) \tag{5.26}$$

Proposition 5.31 (Substitution Principle)**.** *Let $\phi : R \to R'$ be a ring homomorphism.*

1. *Given an element $\alpha \in R'$, there is a unique homomorphism $\Phi : R[x] \to R'$ which agrees with the map ϕ on constant polynomials, and which sends $x \mapsto \alpha$*
2. *More generally, given $\alpha_1, ..., \alpha_n \in R'$, there is a unique homomorphism $\Phi : R[x_1, ..., x_n] \to R'$ from the polynomial ring in n variables to R', which agrees with ϕ on constant polynomials and which sends $x_i \mapsto \alpha_i$, for $i = 1, 2, ..., n$*

Proof. With vector notation for indices, the proof of (2) is identical to that of (1). Let us denote the image of an element $r \in R$ in R' by r'. Using the fact that Φ is a homomorphism

which restricts to ϕ on R, and sends $x_v \mapsto \alpha_v$, we find that it acts on a polynomial $f(x) = \sum r_i x^i$ by sending

$$\sum r_i x^i \mapsto \sum \phi(r_i)\alpha^i = \sum r_i' \alpha^i \tag{5.27}$$

In other words, Φ acts on the coefficients of a polynomial as ϕ, and it substitutes α for x. Since this formula describes Φ completely for us, we have proved the uniqueness of the substitution homomorphism. To prove its existence, we take this formula as the definition of Φ, and we show that the map is a ring homomorphism $R[x] \to R'$. Since ϕ is a ring homomorphism, Ψ sends 1 to 1, and by the above formula, it is compatible with addition of polynomials. Using the formula we also find that it is compatible with multiplication as

$$\begin{aligned}
\Psi(fg) &= \Psi\left(\sum a_i b_j x^{i+j}\right) \\
&= \sum \Psi(a_i b_j x^{i+j}) \\
&= \sum_{i,j} a_i' b_j' \alpha^{i+j} \\
&= \left(\sum_i a_i' \alpha^i\right)\left(\sum_j b_j' \alpha^j\right) \\
&= \Psi(f)\Psi(g)
\end{aligned}$$

■

Example 5.32. We consider the case of a homomorphism $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. This map extends to a homomorphism

$$\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x], f(x) = a_n x^n + \ldots + a_0 \mapsto \overline{a_n} x^n + \ldots + \overline{a_0} = \overline{f}(x) \tag{5.28}$$

where $\overline{a_i}$ denotes the **residue class** of a_i modulo p. We call the polynomial $\overline{f}(x)$ the **residue of** $f(x)$ **modulo** p.

Corollary 5.33. *Let $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_m)$ denote set of variables. There is a unique isomorphism $R[x, y] \xrightarrow{\sim} R[x][y]$ which is the identity on R and which sends the variables to themselves.*

Proof. Note that R is a subring of $R[x]$, and that $R[x]$ is a subring of $R[x][y]$. So R is also a subring of $R[x][y]$. Consider the inclusion map $\phi : R \hookrightarrow R[x][y]$. The Substitution Principle tells us that there is a unique homomorphism $\Phi : R[x, y] \to R[x][y]$ which extends the map and sends variables x_μ, y_ν wherever we wish. Thus, we can send the variables to themselves. The map Φ constructed is thus the desired isomorphism. Using the Substitution Principle once more, we note that $R[x]$ is a subring of $R[x, y]$, so we can extend the inclusion map $\psi : R[x] \to R[x, y]$ to a map $\Psi : R[x][y] \to R[x, y]$ by sending y_j to itself. The composed homomorphism $\Psi\Phi : R[x, y] \to R[x, y]$ is the identity on R and on $\{x_\mu, y_\nu\}$. By uniqueness of the Substitution Principle, $\Psi\Phi$ is the identity map. Similarly, $\Phi\Psi$ is the identity on $R[x][y]$. Thus, Φ is a bijective homomorphism, so it is an isomorphism. ■

Proposition 5.34. *Let $\mathcal{R}$ denote the ring of continuous real-valued functions on $\mathbb{R}^n$. The map $\phi : \mathbb{R}[x_1, ..., x_n] \to \mathcal{R}$ sending a polynomial to its associated polynomial function is an injective homomorphism.*

Proof. The existence of this homomorphism follows from the Substitution Principle. To prove injectivity, it is enough to show that if the function associated to a polynomial $f(x)$ is the zero function, then $f(x)$ is the zero polynomial. Let the associated function be $\widetilde{f}(x)$. If $\widetilde{f}(x)$ is identically zero, then all its derivatives are zero too. On the other hand we can differentiate a formal polynomial by using the power rule and the linearity of the derivative. If some coefficients of $f(x)$ are nonzero, then the constant term of a suitable derivative will be nonzero too. Hence, that derivative will not vanish at the origin. Therefore, $\widetilde{f}(x)$ can't be the zero function. ■

Proposition 5.35. *There is exactly one ring homomorphism*

$$\phi : \mathbb{Z} \to R \tag{5.29}$$

from the ring of integers to an arbitrary ring R. It is the map defined by $\phi(n) = 1_R + ... + 1_R$ n-times if $n > 0$, and $\phi(-n) = -\phi(n)$.

Remark 5.36. This allows us to identify the images of the integers in an arbitrary ring R. We can hence interpret the symbol 3 as $1 + 1 + 1$ in R.

Definition 5.37 (Kernel)**.** For an arbitrary ring homomorphism $\phi : R \to R'$, its kernel is the subset of R

$$\ker(\phi) := \{r \in R : \phi(r) = 0_{R'}\} \tag{5.30}$$

The kernel of a ring homomorphism is closed under the ring operations of addition and multiplication, and for all $r \in R$ and $k \in \ker(\phi)$, $rk \in \ker(\phi)$. Note that the kernel does not contain the unit element $1 \in R$ (unless R' is the zero ring), so in general $\ker(\phi)$ is not a subring, unless it is the whole ring R.

Definition 5.38 (Ideal)**.** An **ideal** I of a ring R is a subset of R with the following properties:

1. I is a subgroup of $(R, +, 0)$;
2. If $a \in I$ and $r \in R$, then $ra \in I$.

Equivalently, we have that I is non-empty, and a linear combination $r_1a_1 + \ldots + r_na_n$ of elements $a_i \in I$ with coefficients $r_i \in R$ is in I.

Definition 5.39 (Principal Ideal)**.** In any ring R, the set of multiples of an element $a \in R$, denoted (a), forms an ideal called the **principal ideal** generated by a:

$$(a) := aR = Ra = \{ra : r \in R\} \tag{5.31}$$

(recall we are assuming a commutative ring). We may also consider the ideal I generated by a set of elements $a_1, ..., a_n$ of R, which is defined to be the smallest ideal containing the elements. It can be described as the set of all linear combinations

$$r_1a_1 + \ldots r_na_n, \textit{ denoted } (a_1, ..., a_n) := \{r_1a_1 + ... + r_na_n : r_i \in R\} \tag{5.32}$$

Definition 5.40 (Special Ideals)**.** In any ring R, the set containing just 0 is a principal ideal called the **zero ideal**, and R is an ideal generated by 1, and called the **unit ideal**. An ideal is said to be **proper** if it is not (0) or (1).

Remark 5.41. Fields can be characterized by the fact that they have no proper ideals.

Proposition 5.42. .

1. *Let F be a field. The only ideals of F are the zero ideal and the unit ideal.*
2. *Conversely, if a ring R has exactly two ideals, then R is a field.*

Proof. The first proposition follows from that fact that non-zero elements of a field have multiplicative inverses, so if I is an ideal in F, either $I = (0)$, or I contains some non-zero element $a \in R$, so $(a) \subset I$, and $1 = a^{-1}a \in (a)$, so $R = (1) \subset (a) \subset I$, which implies that $I = R$. Next, assume that a ring R has exactly two ideals. The properties that distinguish fields from commutative rings with 1 is that $1 \neq 0$, and every nonzero element $a \in R$ is a unit. As we know, $1 = 0$ only in the zero ring, which has one element, and hence only one ideal. Since our ring has two ideals $1 \neq 0$. Since the ideals (1) and (0) are different, they are the only ideals in R.

Let $a \in R$ be a non-zero element, and consider the principal ideal (a). Since $a \in (a)$ and $a \notin (0)$, it must be that $(a) = (1)$. Thus, there must exist $b \in R$ so that $ba = 1$. Thus, by definition a has a multiplicative inverse. ■

Corollary 5.43. *Let F be a field and let R' be a nonzero ring. Every homomorphism $\phi : F \to R'$ is injective.*

Proof. Note that F has only two ideals, (0) and (1), and that since ϕ is a ring homomorphism, $\ker(\phi)$ is an ideal. If $\ker(\phi) = (1)$, then ϕ is the zero map so R' is the zero ring, which is a contradiction to the assumption. Otherwise, $\ker(\phi) = (0)$ so ϕ is injective as desired. ■

Proposition 5.44. *Every ideal in the ring $\mathbb{Z}$ of integers is a principal ideal.*

Proof. Note that every ideal of $\mathbb{Z}$ is a subgroup of the additive group $(\mathbb{Z}, +)$. Thus, each ideal must be in the form $I = d\mathbb{Z}$ for some $d \in \mathbb{Z}$. Hence, $I = (d)$ as desired. ■

Definition 5.45 (Characteristic)**.** The **characteristic** of a ring is the nonnegative integer n which generates the kernel of the homomorphism $\phi : \mathbb{Z} \to R$. Hence, n is the smallest positive integer such that "n times 1_R" $= 0_R$, or, if kernel is (0), the characteristic is zero.

Proposition 5.46. *Let R be a ring and let f, g be polynomials in $R[x]$. Assume that the leading coefficient of $f(x)$ is a unit in R. Then there are polynomials $q, r \in R[x]$ such that*

$$g(x) = f(x)q(x) + r(x) \tag{5.33}$$

and such that the degree of r is less than the degree of f, or else $r = 0$.

Proof. (By induction on the degree of g) ■

Corollary 5.47. *Let $g(x)$ be a monic polynomial in $R[x]$, and let α be an element of R such that $g(\alpha) = 0$. Then $x - \alpha$ divides g in $R[x]$*

Proposition 5.48. *Let F be a field. Every ideal in the ring $F[x]$ of polynomials in a single variable x is a principal ideal.*

Proof. Let I be an ideal of $F[x]$. Since the zero ideal is a principal ideal, we may assume that $I \neq (0)$. The first step in finding a generator of a nonzero subgroup of $\mathbb{Z}$ is to choose its smallest positive element. Our substitute here is to choose a nonzero polynomial f in I of minimal degree. We claim that I is a principal ideal generated by f. It follows by definition of an ideal that the principal ideal (f) is contained in I. Now suppose $g \in I$. Then by the division algorithm for polynomial rings, there exist $p, r \in F[x]$ such that $g = pf + r$, with the degree of r less than f, or equal to $r = 0$. Then, since $f \in I$, $r = g - pf$ is also an element of the ideal. Therefore, since f has minimal degree among nonzero elements, the only possibility is that $r = 0$. Thus, f divides g, as required. ■

Corollary 5.49. *Let F be a field, and let f, g be polynomials in $F[x]$ which are both not zero. There is a unique monic polynomial $d(x)$ called the* ***greatest common divisor*** *of f and g, with the following properties:*

1. *d generates the ideal (f, g) of $F[x]$ generated by the two polynomials f and g*
2. *d divides f and g*

3. *If h is a divisor of f and g, then h divides d*

4. *There are polynomials $p, q \in F[x]$ such that $d = pf + qg$.*

Proof. Suppose f, g are polynomials in $F[x]$, with not both zero. Then the ideal generated by (f, g) is not the zero ideal, and from the previous proposition, there exists $d \in F[x]$ of minimal order that generates (f, g). By definition of the principal ideal, since $(f, g) = (d)$, there exist $r, s \in F[x]$ such that $f = dr$ and $g = ds$. Thus, d divides f and g. (continue from here) ■

5.3.2 Lecture

We consider only commutative rings here.

Definition 5.50 (Ring Homomorphism)**.** A **ring homomorphism** $f : R \to R'$ is a map of sets which is a group homomorphism for $+$, takes $f(1) = 1'$, and $f(ab) = f(a)f(b)$.

Example 5.51. If $R \subset R'$ is a subring, then the inclusion $f : R \hookrightarrow R'$ is a ring homomorphism.

Definition 5.52 (Kernel)**.** For a ring homomorphism $f : R \to R'$, the **kernel** is defined as

$$\ker(f) := \{a \in R : f(a) = 0_{R'}\} \tag{5.34}$$

Kernels of ring homomorphisms have a few properties:

1. It is a subgroup under $+$
2. If $a, b \in \ker(f)$, then $f(ab) = f(a)f(b) = 0 \times 0 = 0$, so $ab \in \ker(f)$.
3. If $a \in \ker(f)$ and $b \in R$, then $ab \in \ker(f)$ since $f(ab) = f(a)f(b) = 0f(b) = 0$

thus, the kernel of a homomorphism is an ideal.

Definition 5.53 (Ideals)**.** A subset $I \subset R$ which is a subgroup under $+$, and is closed under $\times$ by any $b \in R$ is called an **ideal**. (for non-commutative rings we have notions left ideals, right ideals, and two-sided ideals).

Example 5.54. A few examples of ideals

1. $\ker(f)$ is an ideal, where f is a ring homomorphism
2. $\{0_R\} \subset R$ is an ideal, and is the kernel of the identity map $R \to R$, $a \mapsto a$.

3. R, which is the kernel of $R \to \{0\}$, where $\{0\}$ is the zero ring.
4. If you take $a \in R$, then define $I = \{r.a : r \in R\} = (a)$ is the **principal ideal generated by a**.

Definition 5.55 (Quotient Ring)**.** If $I \subset R$ is an ideal in a ring R, then the quotient ring

$$R/I := \{a + I : a \in R\} \tag{5.35}$$

is the set of cosets under $+$ for I, with addition defined normally for quotient groups, since R is an abelian group under $+$, and multiplication defined by

$$(a + I)(b + I) = ab + I \tag{5.36}$$

Theorem 5.56. *Any ideal I is the kernel of a natural ring homomorphism $R \to R/I$, where R/I is the quotient ring, taking $a \mapsto a + I$.*

Proposition 5.57 (Fact)**.** *The only ideals $I \subset \mathbb{Z}$ have the form $I = (n) = n\mathbb{Z}$, and the quotient ring is $\mathbb{Z}/n\mathbb{Z}$.*

Proof. (Euclidean algorithm) ■

Definition 5.58 (Unit)**.** A **unit** in a ring R is an element $a \in R$ which has a multiplicative inverse. The set of all units of R is denoted by $\mathbb{R}^\times \subset R$, which is not closed under multiplication, but forms a group with identity element 1, called the **unit group** of R.

Example 5.59. For $R = F$ a field, then $R^\times = R\backslash\{0\}$. However, $\mathbb{Z}^* = \langle +1, -1\rangle$, and $(\mathbb{Z}/n\mathbb{Z})^*$ is an abelian group with $\phi(n)$ elements (the **Euler number** of the number of things between 1 and n that are relatively prime to n). $M_n(F)^* = GL_n(F)$.

Remark 5.60. For each ideal, I, of ring R, there is a canonical ring homomorphism $f : R \to R'$ with kernel I. This is done by letting $R' = R/I$, with $r \mapsto r+I$, where R/I is an abelian group under $+$ by the theory of groups, and multiplication is defined by $(s + I)(r + I) = (sr + I)$, which is well-defined since I is an ideal.

Remark 5.61 (Natural Ideals). For any ring R, we have the ideals $I = \{0\}$ and $I = R$. For $I = \{0\}$, $R' = R/I = R$, and f is the identity. For $I = R$, $R' = \{0\}$, so $f(r) = 0_{R'}$. Note that if R is the zero ring, these are the same ideal. Otherwise, these two ideals are distinct.

Proposition 5.62. *If R has only one ideal, $R = \{0\}$. R has only two ideals if and only if R is a field (which are R and $\{0\}$).*

Proof. First, let us assume that R is a field, and that I is a non zero ideal. Take $a \in I$ with $a \neq 0$.Since a has an inverse $r \in R$, $1 = ar \in I$. Since $1 \in I$, for any $r \in R$, $r = r.1 \in I$. Thus, $I = R$. Now, let R be a ring with only two ideals. Suppose $a \in R$, $a \neq 0$, and consider the principal ideal $(a) = \{a.r : r \in R\}$. Since R has only two ideals, and $a \neq 0$, $(a) = R$. Thus, $1 \in (a)$, so there exists $r \in R$ so that $a.r = 1$, so r is the multiplicative inverse of a. Thus, R is a field. ■

Example 5.63. Consider $R = \mathbb{Z}/4\mathbb{Z}$. Then some ideals of R are, $I = (0), (1), (2) = \{0, 2\}$. In general, $R = \mathbb{Z}/n\mathbb{Z}$ we have the ideal (d) for all $d \mid n$. In particular, if $R = \mathbb{Z}/p^k\mathbb{Z}$, then the distinct ideals are $(1) \supset (p) \supset (p^2) \supset ... \supset (p^k) = (0)$.

Remark 5.64. In general the set of ideals form a lattice for the ring.

Remark 5.65. $R = \mathbb{Z}$ has an infinite number of distinct ideals, with every ideal of the form $I_n = (n) = n\mathbb{Z}$ for $n \geq 0$ as these are the full list of subgroups, and all are stable under multiplication from $\mathbb{Z}$. Moreover, $I_n \supset I_{n'} \iff n \mid n'$. The quotient $R/I_n = \mathbb{Z}/n\mathbb{Z}$.

Remark 5.66. Another important ring where we know all ideals: Let F be a field, and let $R = F[x] = \{a_n x^n + \dots x_1 x + a_0 : a_i \in F, n \geq 0\}$. We call a polynomial $p(x) \in R$ **monic** if the leading term is 1 ($a_n = 1$). In general, if $q(x)$ of **degree** n is any polynomial, there exists a unique $c \in F^\times$ such that $cq(x)$ is monic of degree n.

Theorem 5.67 (Analog of the Euclidean Algorithm for the Polynomial Ring)**.** *If f and g are two polynomials with $deg(f) \geq deg(g)$, then*

$$f(x) = g(x)q(x) + r(x) \tag{5.37}$$

where $deg(r) < deg(g)$.

Example 5.68. Take $f(x) = x^3 + 2x^2 + 3x + 7$ and $g(x) = x^2 + x + 1$. Then observe that $xg(x) = x^3 + x^2 + x$, and $f(x) - xg(x) = x^2 + 2x + 7$, then $f(x) - (x + 1)g(x) = x + 6$. Let $r(x) = x + 6$, and we find that

$$f(x) = (x + 1)g(x) + (x + 6)$$

Theorem 5.69. *Every ideal I in the ring $R = F[x]$ is principal, $I = (f)$, generated by the monic polynomial f in I of least degree.*

Proof. Let I be an ideal. If $I \neq (0)$, take $f \in I$ of minimal degree, n. Scale f by $c = a_n^{-1}$ to make f monic. Note that since $c \in F[x]$, $c.f \in I$. Let h be another polynomial in I, and write $h(x) = q(x)f(x) + r(x)$, with the degree of $r(x)$ less than $f(x)$. Note that $q(x) \in F[x]$, so $q(x)f(x) \in I$, and $h(x) - q(x)f(x) \in I$. Thus, $r(x) \in I$. But, $r(x)$ has a smaller degree than f, so $r(x) = 0$. Thus, $h(x) = q(x)f(x)$, so $f(x)$ divides $h(x)$, and $I = (f)$. ■

Remark 5.70. Thus, the set of ideals is in a one-to-one correspondance with the set of monic polynomials, and the ideal associated to f, I_f, contains the ideal generated by the monic polynomial g, that is $I_f \supset I_g$, if and only if f divides the polynomial g. Namely, $g(x) = f(x)q(x)$ for some $q(x) \in F[x]$.

Example 5.71 (Evaluation Homomorphism)**.** Consider the map $h : R = F[x] \to F$, with $f(x) \mapsto f(c)$, where $c \in F$ is some fixed value. This is a ring homomorphism. First, $h(f + g) = (f + g)(c) = f(c) + g(c) = h(f) + h(f)$, so h is a group homomorphism over $+$. Additionally, $h(fg) = (fg)(c) = f(c)g(c) = h(f)h(g)$, and $h(1) = 1$, so h is a ring homomorphism. The kernel of ϕ is a polynomial with c as a root. Moreover, the polynomial $f(x) = x - c$ is monic and of degree 1, with $f(c) = 0$. Thus, every $f \in \ker \phi$ is a multiple of $(x - c)$.

Corollary 5.72. *If $f(c) = 0$, then $f(x) = (x - c)g(x)$. Then, a polynomial over any field has at most n roots.*

Proof. (Proof by induction) ■

Example 5.73 (Non-principal Ideals)**.** Take the ring $R = F[x, y] = \{\sum_{i=1,j=1}^{n,m} a_{ij}x^i y^j : a_{ij} \in F\}$. Consider the map $h : R \to F$ by $f(x, y) \mapsto f(0, 0)$. The kernel of h is not generated by one element (so it's not principal). In fact, $\ker h = (x, y) = \{rx + sy : r, s \in R\}$.

Remark 5.74. For any group G, we have a subgroup $\{e\}$. Namely, there is a homomorphism $\{e\} \to G$. For any ring (commutative) R, there is a natural homomorphism $h : \mathbb{Z} \to R$ taking $0 \mapsto 0_R$, $1 \mapsto 1_R$, and $n \mapsto \underbrace{1_R + \ldots 1_R}_{\text{n-times}}$. *WARNING:* h is not necessarily injective. For example, $I = \ker h = n\mathbb{Z}$ for some $n \geq 0$.

Remark 5.75 (Think about this). If R is a field, and h is the natural homomorphism given above, then $\ker h = \{0_R\}$, or $\ker h = p\mathbb{Z}$, where p is prime.

5.4 Quotient Rings and Relations

5.4.1 Textbook

Theorem 5.76. *Let I be an ideal of a ring R:*

1. *There is a unique ring structure on the set of cosets $\overline{R} = R/I$ such that the canonical map $\pi : R \to \overline{R}$ sending $a \mapsto \overline{a} = a + I$ is a ring homomorphism.*
2. *The kernel of π is I.*

Proof. We define addition on $\overline{R}$ following the definition for abelian quotient groups. Next, we define multiplication for any $\overline{x}, \overline{y} \in \overline{R}$ by

$$\overline{xy} = (x + I)(y + I) = xy + I \tag{5.38}$$

Observe that for all $x + u \in x + I$ and $y + v \in y + I$, $u, v \in I$, we have that

$$(x+u+I)(y+v+I) = (x+u)(y+v)+I = xy+xv+uy+uv+I = xy+I = (x+I)(y+I) \tag{5.39}$$

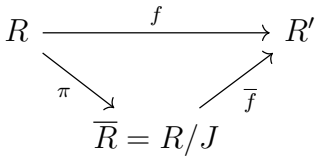
since I is an ideal, so multiplication is well-defined. Next, we have a multiplicative identity $0 + I \in R/I$, and it is easy to see that multiplication is associative. Finally, we must check that the distributive laws hold. For all $a + I, b + I, c + I \in R/I$ we see that

$$[(a+I)+(b+I)](c+I) = [(a+b)+I](c+I) = (a+b)c+I = ac+bc+I = (ac+I)+(bc+I) \tag{5.40}$$

The proof other distributive law is similar. ■

Proposition 5.77 (Mapping Property of Quotient Rings)**.** *Let $f : R \to R'$ be a ring homomorphism with kernel I, and let J be an ideal which is contained in I. Denote the residue ring R/J by $\overline{R}$:*

1. *There is a unique homomorphism $\overline{f} : \overline{R} \to R'$ such that $\overline{f}\pi = f$:*



2. ***First Isomorphism Theorem**: If $J = I$, then $\overline{f}$ maps $\overline{R}$ isomorphically, to the image of f.*

Proposition 5.78 (Correspondance Theorem)**.** *Let $\overline{R} = R/J$, and let π denote the canonical map $\pi : R \to \overline{R}$*

1. *There is a bijective correspondance between the set of ideals of R which contain J and the set of all ideals of $\overline{R}$, given by*

$$I \mapsto \pi(I), \text{ and } \pi^{-1}(\overline{I}) \hookleftarrow \overline{I} \tag{5.41}$$

2. *If $I \subset R$ corresponds to $\overline{I} \subset \overline{R}$, then R/I and $\overline{R}/\overline{I}$ are isomorphic rings. (Third Isomorphism Theorem)*

Proof. To prove (1), we must check the following points:

1. If I is an ideal of R which contains J, then $\pi(I)$ is an ideal of $\overline{R}$
2. If $\overline{I}$ is an ideal of $\overline{R}$, then $\pi^{-1}(\overline{I})$ is an ideal of R.
3. $\pi^{-1}(\pi(I)) = I$ and $\pi(\pi^{-1}(\overline{I})) = \overline{I}$

We know that the image of a subgroup is a subgroup. Thus, to show that $\pi(I)$ is an ideal of $\overline{R}$, we need only prove that it is closed under multiplication by elements of $\overline{R}$. Let $\overline{r} \in \overline{R}$, and let $\overline{x} \in \pi(I)$. We write $\overline{r} = \pi(r)$ for some $r \in R$, and $\overline{x} = \pi(x)$ for some $x \in I$. Then $\overline{rx} = \pi(rx)$ and $rx \in I$. Thus, $\overline{rx} \in \pi(I)$. Note that this proof is valid for all ideals I of R, but the fact that π is surjective is essential.

Next, denote the homomorphism $\overline{R} \to \overline{R}/\overline{I}$ by ϕ, and we consider the composed homomorphism $R \xrightarrow{\pi} \overline{R} \xrightarrow{\phi} \overline{R}/\overline{I}$. Since π and ϕ are surjective, so is $\phi \circ \pi$. Moreover, the kernel of $\phi \circ \pi$ is the set of elements $r \in R$ such that $\pi(r) \in \overline{I} = \ker(\phi)$. By definition, this is $\pi^{-1}(\overline{I})$, Therefore, $\pi^{-1}(\overline{I})$ being the kernel of a ring homomorphism is an ideal of R. Also, the First Isomorphism Theorem applies to the homomorphism $\phi \circ \pi$ and shows that $R/\pi^{-1}(\overline{I})$ is isomorphic to $\overline{R}/\overline{I}$ (This proves the second assertion)

It remains to prove the third subpoint to prove the first proposition. Note that π^{-1} is *not* a map. We note that the inclusions $I \subset \pi^{-1}(\pi(I))$ and $\pi(\pi^{-1}(\overline{I})) \subset \overline{I}$ are properties of general set-theoretic maps. Moreover, the equality $\pi(\pi^{-1}(\overline{I})) = \overline{I}$ follows from the fact that π is surjective. Then, to show the equality of the other sets, let $x \in \pi^{-1}(\pi(I))$. Then $\pi(x) \in \pi(I)$, so there is an element $y \in I$ such that $\pi(y) = \pi(x)$. Since π is a homomorphism, $\pi(x - y) = 0$ and $x - y \in J = \ker(\pi)$. Since $y \in I$ and $J \subset I$, this implies that $x \in I$, as required, so $I = \pi^{-1}(\pi(I))$. ■

Definition 5.79 (Relations)**.** Elements in a ring R are related if after performing a sequence of operations $+$, $\times$, $-$, one can obtain an element a equivalent to zero. What about the case when this can't be done? When a is non-zero? Let a be a nonzero element of R. We wish to impose the relation $a = 0$ on R without losing the operations $+$ or $\times$. Consequently, for any element $b \in R$ we must have that $b + ra = b$ for any $r \in R$. There are in fact no other conditions needed: if we fix b and let r vary, we obtain the coet $b + (a)$, where $(a) = aR$ is the principal ideal generated by a. Setting $b + ra = b$ for all r is the same as equating the elements of this coset. This is precisely what happens when we take the canonical projection of R to $R/(a)$. Thus, it is reasonable to view $R/(a)$ as the ring obtained by introducing the relation $a = 0$ into R.

Example 5.80. Taking the ring of integers, $\mathbb{Z}$, if we add the relation $n = 0$ we obtain the ring $\mathbb{Z}/n\mathbb{Z}$.

Remark 5.81. In general, we can introduce any number of relations $a_1 = ... = a_n = 0$ by taking the ideal I generated by $a_1, a_2, ..., a_n$, which is the set of linear combinations of these elements. Then, the quotient ring R/I can be viewed as the ring obtained by introducing these relations.

Remark 5.82. Two elements $b, b' \in R$ have the same image in R/I under the canonical projection if and only if $b - b' \in I$.

Remark 5.83. Suppose $a, b \in R$, and consider $R/(a)$ as the result of killing a. Introducing the relation $b + (a) = 0$ onto the ring $R/(a)$ leads to the quotient ring $(R/(a))/(b + (a))$, and this ring is isomorphic to the quotient ring $R/(a, b)$ by the Third Isomorphism Theorem since (a, b) and $(b + (a))$ are corresponding ideals.

Proposition 5.84. *The ring $\mathbb{Z}[i]/(1+3i)$ is isomorphic to the ring $\mathbb{Z}/10\mathbb{Z}$ of integers modulo 10.*

Proof. Consider the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}[i]/(1 + 3i)$. By the First Isomorphism Theorem, $\operatorname{im}\phi \cong \mathbb{Z}/(\ker\phi)$. Now every element of $\mathbb{Z}[i]/(1 + 3i)$ is the residue of a Gauss Integer $a + bi$. Since $i = 3$ in $\mathbb{Z}[i]/(1 + 3i)$, the residue of $a + bi$ is the same as that of the integer $a + 3b$. This shows that ϕ is surjective. Let n be any element of $\ker\phi$. Then, it follows that n must be in the ideal $(1+3i)$. That is n is divisible by $(1+3i)$ in the Gaussian integers. So, we may write $n = (a + bi)(1 + 3i) = (a - 3b) + (3a + b)i$ for some integers a, b. Since n is an integer, $3a + b = 0$, $b = -3a$, so $n = a - 3(-3a) = a + 9a = 10a$, and this shows that $\ker\phi \subset 10\mathbb{Z}$. On the other hand, $10 \in \ker\phi$, so $\ker\phi = 10\mathbb{Z}$, as required. ■

Proposition 5.85. *The ring $\mathbb{C}[x, y]/(xy)$ is isomorphic to the subring of the product ring $\mathbb{C}[x] \times \mathbb{C}[y]$ consisting of pairs $(p(x), q(y))$ such that $p(0) = q(0)$*

Proof. First, let us identify the ring $\mathbb{C}[x, y]/(y)$. Because the principal ideal (y) is the kernel of the substitution homomorphism $\phi : \mathbb{C}[x, y] \to \mathbb{C}[x]$, sending $y \mapsto 0$, by the First Isomorphism Theorem, $\mathbb{C}[x, y]/(y) \cong \mathbb{C}[x]$. Similarly, $\mathbb{C}[x, y]/(x) \cong \mathbb{C}[y]$. Now, let us look at the homomorphism of the product ring $\phi : \mathbb{C}[x, y] \to \mathbb{C}[x] \times \mathbb{C}[y]$, which is defined by $f(x, y) \mapsto (f(x, 0), f(0, y))$. The kernel of ϕ is the intersection of the kernels: $\ker\phi = (y) \cap (x)$. To be in this intersection, a polynomial must be divisible by both x and y. This just means that it is divisble by xy. Thus, $\ker\phi = (xy)$. Then, by the First Isomorphism Theorem, $\mathbb{C}[x, y]/(xy)$ is isomorphic to the image of ϕ, which is the subring described in the proposition. ■

5.4.2 Lecture

Remark 5.86 (Canonical Map). If we have a commutative ring R, there is a natural ring homomorphism $f : \mathbb{Z} \to R$ which is completely characterized by $f(1) = 1_R$, so for $n \geq 1$, $f(n) = f(\underbrace{1+1+...+1}_{\text{n-times}}) = \underbrace{1_R + ... + 1_R}_{\text{n-times}}$ and $f(-n) = -f(n)$. This is the canonical ring homomorphism associated to any commutative ring. Moreover, we know that the kernel of f is an ideal of $\mathbb{Z}$, so it is of the form $n\mathbb{Z}$ for some $n \geq 0$. If $R = \{0\}$, then $\ker(f) = \mathbb{Z}$, and if $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, then $\ker(f) = 0\mathbb{Z} = \{0\}$. Moreover, if $R = \mathbb{Z}/n\mathbb{Z}$, then $\ker(f) = n\mathbb{Z}$.

Proposition 5.87. *If R is a field, then $\ker(f) = \{0\}$ or $\ker(f) = p\mathbb{Z}$ for p a prime.*

Proof. For the sake of contradiction suppose $\ker(f) = n\mathbb{Z}$ for $n = ab$ composite, so $1 < a, b < n$. Then $f(n) = 0$ in R. But, $f(n) = f(a)f(b) = a_R b_R = 0_R$, so since R is a field, a_R is zero or b_R is zero. However, this contradicts the fact that the $\ker(f)$ is a multiple of n, and $a, b \notin n\mathbb{Z}$. ■

Definition 5.88 (Characteristic of a Field)**.** The characteristic of a field F is equal to either 0, or the smallest positive integer p such that for the canonical map $f : \mathbb{Z} \to F$, $f(p) = 0$. Note that from the above proposition p must be prime.

Theorem 5.89 (Galois)**.** *Let F be a finite field. Then $|F| = p^f$ for some prime p. Additionally, for any f, there is a finite field with p^f elements, and it is unique up to isomorphism.*

Proof. Consider the canonical homomorphism $\mathbb{Z} \to F$, $n \mapsto n_F$. Since $\mathbb{Z}$ is an infinite ring and F is finite, $\ker(f) \neq \{0\}$. Thus, $\ker(f) = p\mathbb{Z}$ for from prime p, and f induces a homomorphism $\therefore \mathbb{Z}/p\mathbb{Z} \hookrightarrow F$. This gives F the structure of a vector space over the field $\mathbb{Z}/p\mathbb{Z}$, which has finite dimension $= f$. Then $|F| = p^f$. Thus, $F \cong (\mathbb{Z}/p\mathbb{Z})^f$ as a finite dimensional vector space. ■

Theorem 5.90 (First Isomorphism Theorem for Rings)**.** *For a commutative ring R and an ideal $I \subset R$ we have a natural surjective ring homomorphism*

$$R \xrightarrow{f} R/I = \overline{R} \tag{5.42}$$

There is a bijection between

$$\{\text{ideals of } R \text{ containing } I,\ I \subset J \subset R\} \leftrightarrow \{\text{ideals } \overline{J} \text{ of } \overline{R}\} \tag{5.43}$$

In other words, we can obtain all ideals of the quotient ring $\overline{R}$ by taking ideals of R that contain I. We define the bijection for all ideals $J \supset I$ by

$$\begin{array}{ccc} J & \mapsto & f(J) \subset \overline{R} \\ f^{-1}(\overline{J}) & \hookleftarrow & \overline{J} \end{array} \tag{5.44}$$

Moreover, the quotient ring $R/J \cong \overline{R}/\overline{J}$ so we have isomorphisms of quotient rings.

Proof. Suppose R is a commutative ring with ideal I, $\overline{R} = R/I$, and let $J \supset I$ be another ideal of R, and f be the canonical projective ring homomorphism defined previously. First, we shall show that $f(J)$ is an ideal of $\overline{R}$. Assume $f(a), f(b) \in f(J)$, where $a, b \in J$. Then $a + b \in J$, so $f(a) + f(b) = f(a + b) \in f(J)$. Now, suppose $\overline{r} \in \overline{R}$ and $f(a) \in f(J)$. Since f is a surjective ring homomorphism, there exists $r \in R$ so that $f(r) = \overline{r}$. Then $\overline{r}f(a) = f(r)f(a) = f(ra) \in f(J)$ since $ra \in J$ as J is an ideal (note that the image of an ideal may not be an ideal when the homomorphism is not surjective). Now, suppsoe $\overline{J} \subset \overline{R}$ be an ideal. Let $a, b \in f^{-1}(\overline{J})$. Then $f(a), f(b) \in \overline{J}$, so $f(a + b) = f(a) + f(b) \in \overline{J}$, which implies that $a + b \in f^{-1}(\overline{J})$. Now, let $r \in R$ and $a \in f^{-1}(\overline{J}$. Then $f(ra) = f(r)f(a) \in \overline{J}$ since $f(a) \in \overline{J}$ and $\overline{J}$ is an ideal. Hence, $ra \in f^{-1}(\overline{J})$, and $f^{-1}(\overline{J})$ is an ideal as claimed. Now, notice that $I \subset f^{-1}(\overline{J})$ since $I = f^{-1}(0)$ and $0 \in \overline{J}$ since it is an ideal. We now compose the quotient map f with the quotient map $\phi : \overline{R} \to \overline{R}/\overline{J}$, giving the surjective ring homomorphism

$$\phi \circ f : R \to \overline{R}/\overline{J} \tag{5.45}$$

with kernel $\ker \phi \circ f = f^{-1}(\overline{J})$. We claim that $f^{-1}(\overline{J}) = J$. To show this, it is sufficient to prove that $f(f^{-1}(\overline{J})) = \overline{J}$ and $f^{-1}(f(J)) = J$. Firstly, by definition $f(f^{-1}(\overline{J})) \subset \overline{J}$, and since f is surjective, we in fact have that $f(f^{-1}(\overline{J})) = \overline{J}$. Now, also by definition we have that $f^{-1}(f(J)) \supset J$. Now, let $x \in f^{-1}(f(J))$. Then by definition $f(x) \in f(J)$, so there exists $y \in J$ such that $f(x) = f(y)$. Then by the definition of the ring homomorphism, $f(x-y) = \overline{0}$, so $x - y \in I$. Since, $I \subset J$, $x - y \in J$. Finally, since $y \in J$, $x = (x-y)+y \in J$, so $J = f^{-1}(f(J))$. Therefore, we find that $f^{-1}(\overline{J}) = J$, so by the First Isomorphism Theorem of groups, $R/J \cong \overline{R}/\overline{J}$. ■

Remark 5.91 (Warning about image of ideals). If $f : R \to R'$ is a ring homomorphism that is not surjective, and $J \subset R$ is an ideal, then $f(J)$ is not necessarily an ideal as well. For example, $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$ is a ring homomorphism and $\mathbb{Z}$ is an ideal in $\mathbb{Z}$, but $i(\mathbb{Z})$ is not an ideal in $\mathbb{Q}$ since $\mathbb{Q}$ is a field with only trivial ideals.

Question. When is R/I a field?

Answer. R/I is a field if and only if it has only two ideals, $\{0\}$ and R/I, which is equivalent to R having only 2 ideals containing I, which are R and I, which is also equivalent to saying that I is a maximal ideal of R.

Definition 5.92 (Maximal Ideal)**.** An ideal I in a ring R is known as a **maximal ideal** if and only if there exist no proper ideals containing I as a proper ideal.

Definition 5.93 (Ring Relations)**.** Creating Relations in a ring R: Suppose we have an element $a \in R$. If we want a ring $\overline{R}$ which is an image of R, where $\overline{a} = 0$, then the largest such quotient is $\overline{R} = R/(a)$. If we want a ring where we have a number of relations $a_1 = a_2 = ... = a_n = 0$, we can take $(R/(a_1)/(a_2)/.../(a_n)) = \overline{R} = R/(a_1, a_2, ..., a_n)$. This is valid because the ideal $(a_1, ..., a_n)$ contains (a_i) for all i, and then this is successive applications of the Isomorphism Theorem.

Remark 5.94. If R is a ring and $a \in R$, if a is a unit then $R/(a) = \{0\}$ since $(a) = R$. I.e¿ modding out by a unit mods out all elements of the ring.

Note: Moving on we shall talk about $R = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$

Example 5.95. What if we want $2 + i = 0$? Let $I = (2 + i)$ and take $\overline{R} = R/I$. We wish to identify $\overline{R}$. First, let's identify the intersection $I \cap \mathbb{Z}$. First, note that $0 = (2 + i)(2 - i) = 4 + 1 = 5$, so $5 \in I \cap \mathbb{Z}$. In particular, $5\mathbb{Z} \subset I \cap \mathbb{Z}$, where $5\mathbb{Z}$ is a maximal subgroup of $\mathbb{Z}$, so in fact it is a maximal ideal. Therefore, either $I \cap \mathbb{Z} = \mathbb{Z}$ or $I \cap \mathbb{Z} = 5\mathbb{Z}$. Secondly, observe that if $(2 + i)(a + bi) \in \mathbb{Z}$, then $(2a - b) + (2b + a)i \in \mathbb{Z}$. In particular, $2b + a = 0$, so $a = -2b$. It follows that $(2 + i)(a + bi) = 2(-2b) - b = -4b - b = 5(-b) \in 5\mathbb{Z}$. Therefore, $I \cap \mathbb{Z} = 5\mathbb{Z}$. Then, if we take the canonical homomorphism $\mathbb{Z} \to R/I = \overline{R}$, it has kernel $5\mathbb{Z}$, and image $\cong \mathbb{Z}/5\mathbb{Z}$. In fact, $\overline{R} \cong \mathbb{Z}/5\mathbb{Z}$ under this map, or in other words, the map is surjective. Note that since $2 + i \equiv 0 \mod I$, $i \equiv -2 \mod I$, and $a + bi \equiv a - 2b \mod I$ in R/I, but $a - 2b \in \mathbb{Z}$. Thus, the map is surjective, so the image of the integers, $\mathbb{Z}/5\mathbb{Z}$, must be isomorphic to R/I.

Theorem 5.96. *More generally, if p is a prime number with $p \equiv 1 \mod 4$, there is an ideal $I \subset \mathbb{Z}[i] = R$ with $R/I \cong \mathbb{Z}/p\mathbb{Z}$.*

Proof. First, note that for the canonical homomorphism $f : R \to R/I$, if $R/I \cong \mathbb{Z}/p\mathbb{Z}$, then $f(i)$ must have order 4 multiplicatively since $i^4 = 1$ and $i^2 = -1$, so $f(i)^2 \cong -1 \mod p$. If $f(i)$ has order 4 in $(\mathbb{Z}/p\mathbb{Z})^*$, then $p \equiv 1 \mod 4$. Then, recall by Wilson's Theorem that $(p - 1)! \equiv -1 \mod p$. Now, consider the element $\left(\frac{p-1}{2}\right)!$, and complete it $1 * 2 * ... * \frac{p-1}{2} * \frac{p+3}{2} * ... * (p - 2) * (p - 1) \cong -1 \mod p$. But, the terms in the first half are minus the terms in the second, so the product of the first half is equal to that of the second half times the number of minus signs. Note that the number of minus signs is $(-1)^{\frac{p-1}{2}}$, and since $p \equiv 1 \mod 4$, $\frac{p-1}{2}$ is even. Thus, the product of the first half is equal to the product of the second half. Hence, the square of $a \equiv \left(\frac{p-1}{2}\right)!$ is -1, so it is our element of order 4. Then, let I be the ideal generated by p and $i - a$, so $I = (p, i - a)$. First, note that $I \cap \mathbb{Z} \supset p\mathbb{Z}$. Moreover, $(i - a)(b + ci) = (-ab - c) + (-ac + b)i$, where $-ac + b = 0$, so $-ab - c = -a^2c - c = -c(a^2 + 1)$. But, $a^2 \cong -1 \mod p$, so $a^2 + 1 \cong 0 \mod p$. Thus, $-c(a^2 + 1) \in p\mathbb{Z}$. Hence, $\mathbb{Z} \to R/I$ is surjective, as $i \cong a \in R/I$, with kernel $p\mathbb{Z}$, so $R/I \cong \mathbb{Z}/p\mathbb{Z}$. ∎

Theorem 5.97 (Gauss's Theorem)**.** *For $R = \mathbb{Z}[i]$, every ideal $I \in R$ is principal.*

Corollary 5.98. *Since every $I \subset \mathbb{Z}[i]$ is principal, so is $(p, i - a)$, which implies $(p, i - a) = (a + bi)$ for some $a + bi \in \mathbb{Z}[i]$, and from above, $R/(a + bi) \cong \mathbb{Z}/p\mathbb{Z}$. This implies that $a^2 + b^2 = p$.*

Theorem 5.99 (Fermat's Theorem)**.** *For any prime number p such that $p \equiv 1 \mod 4$, $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.*

Remark 5.100. Gauss showed that if you can write all primes $p \equiv 1 \mod 4$ as $p = a^2 + b^2$, then every ideal $(a + bi) \subset \mathbb{Z}[i]$ must be principal.

Remark 5.101. The first step to prove Gauss's theorem is to show that for all prime $p \equiv 1 \mod 4$, there is an ideal $(a + bi)$ so that $R/(a + bi) \cong \mathbb{Z}/p\mathbb{Z}$, then the second step is to show that all ideals are principal, and then the third step is to show that if you have a quotient $R/(a + bi) \cong \mathbb{Z}/p\mathbb{Z}$, $a^2 + b^2 = p$.

Remark 5.102. More generally, the order of the finite ring $R/(a+bi)$ is $a^2+b^2 = (a+bi)(a-bi)$ providing that $(a + bi) \neq (0)$.

5.5 Adjunction of Elements

5.5.1 Textbook

Definition 5.103 (Adjuction)**.** Let R be an arbitrary ring, and consider the problem of building a bigger ring containing the elements of R and a new element, say α. We will most likely want α to satisfy some relations with the elements of R. A ring R' containing R as a subring is called a **ring extension**. If α is already in a known R', then $R[\alpha]$ is the subring generated by R and α. In general, $R[\alpha]$ consists of elements of R' which have polynomial expressions

$$r_n\alpha^n + \ldots + r_1\alpha + r_0 \tag{5.46}$$

with coefficients $r_i \in R$. In general, $R[x]$ is always our solution for adjoining a new element, as indicated by the Substitution Principle: If α is an element of any ring extension R' of R, then there is a unique map $R[x] \to R'$ which is the identity on R and which carries $x \mapsto \alpha$. The image of this map will be the subring $R[\alpha]$

Remark 5.104 (Adding Relations). Note that for the polynomial ring, $R[x]$, x satisfies no relations except $0x = 0$ as indicated by the ring axioms. To add relations to $R[x]$ we follow the same procedure as before, using the **quotient construction** on the polynomial ring.

Example 5.105 (Complex Numbers)**.** We can obtain the complex numbers by introducing the relation $x^2 + 1 = 0$ into the ring of real polynomials $\mathbb{R}[x] = P$. To do so, we form the quotient ring $\overline{P} = P/(x^2 + 1)$, where the residue of x becomes our desired element i. The fact that $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ follows from the First Isomorphism Theorem.

Definition 5.106 (Nilpotent)**.** An element of a ring R is **infinitesimal** or **nilpotent** if some power is zero. We may adjoin infinitesimals to a ring using the relation $x^n = 0$ for the power we want.

Example 5.107. If we wanted an infinitesimal element ϵ such that $\epsilon^2 = 0$, we may adjoin it to the quotient ring $R[x]/(x^2)$, so the residue of x is ϵ.

Definition 5.108 (Adjoining)**.** In general, if we want to adjoin an element α to a ring R satisfying one or more polynomial relations of the form

$$f(\alpha) = c_n\alpha^n + \ldots + c_1\alpha + c_0 = 0 \tag{5.47}$$

the solution is $R' = R[x]/I$, where I is the ideal in $R[x]$ generated by the polynomials $f(x)$. If α denotes the residue $\overline{x}$ of x in R', then

$$0 = \overline{f(x)} = \overline{c_n}\overline{x}^n + \ldots \overline{c_1}\overline{x} + \overline{c_0} = \overline{c_n}\alpha^n + \ldots \overline{c_1}\alpha + \overline{c_0} \tag{5.48}$$

where here $\overline{c_i}$ is the image in R' of the constant polynomial c_i. The ring obtained in this way is denoted by

$$R[\alpha] = \text{ring obtained by adjoining } \alpha \text{ to } R \tag{5.49}$$

Remark 5.109. Several elements $\alpha_1, ..., \alpha_m$ can be adjoined by repeating this procedure, or by introducing the appropriate relations in the polynomial ring $R[x_1, ..., x_m]$ in m variables.

Proposition 5.110. *Let R be a ring, and let $f(x)$ be a monic polynomial of positive degree n, with coefficients in R. Let $R[\alpha]$ denote the ring obtained by adjoining an element satisfying the relation $f(\alpha) = 0$. The elements of $R[\alpha]$ are in bijective correspondance with vectors $(r_0, ..., r_{n-1}) \in R^n$. Such a vector corresponds to the linear combination*

$$r_0 + r_1\alpha + r_2\alpha^2 + \ldots + r_{n-1}\alpha^{n-1},\ r_i \in R \tag{5.50}$$

That is, the powers $1, \alpha, ..., \alpha^{n-1}$ forms a basis for $R[\alpha]$ over R. To multiply tw such linear combinations we multiply them as polynomials, and then divide the product by f, giving the linear combination representing the product.

Proof. Since $R[\alpha]$ is a quotient ring of a polynomial ring $R[x]$, every element of $R[\alpha]$ is the residue of a polynomial. This means that it can be written in the form $g(\alpha)$ for some polynomial $g(x) \in R[x]$. The relation $f(\alpha) = 0$ can be used to replace any polynomial $g(\alpha)$ of degree $\geq n$ by one of lower degree: We perform division with remainder by $f(x)$ on the polynomial $g(x)$, obtaining an expression of the form $g(x) = f(x)q(x)+r(x)$. Since $f(\alpha) = 0$, $g(\alpha) = r(\alpha)$. Thus, every element β of $R[\alpha]$ can be written as a polynomial in α of degree $< n$.

We now show that the principal ideal generated by $f(x)$ contains no elements of degree $< n$, and there fore $g(\alpha) \neq 0$ for every non-zero polynomia $g(x)$ of degree $< n$. This will imply that the expression of degree $< n$ for an element β is unique. The principal ideal generated by $f(x)$ is the set of all multiples hf of f. Suppose $h(x) = b_m x^m + \ldots + b_0$, with $b_m \neq 0$. Then the highest degree term of $h(x)f(x)$ is $b_m x^{m+n}$, and hence hf has degree $m + n \geq n$. This completes the proof of the proposition. ■

Example 5.111 (Adjoining Inverses)**.** Suppose $a \in R$, and suppose we want to adjoin the inverse α of a to R. Then α satisfies the relation $a\alpha - 1 = 0$. The desired ring is then $R' = R[x]/(ax - 1)$. Then, Suppose $\beta = r_0 + r_1\alpha + ... + r_{n-1}\alpha^{n-1}$ is an element of R'. Since $a\alpha = 1$, it follows that $\beta = \alpha^{n-1}(r_0 a^{n-1} + r_1 a^{n-2} + ... + r_{n-1})$.

Example 5.112. Suppose that $R = F[t]$ is a polynomial ring and we want to adjoin an inverse to the variable t. Then $R' = F[t, x]/(xt - 1)$. This identifies naturally with the ring $F[t, t^{-1}]$ of **Laurent polynomials** in t. A Laurent polynomial is a polynomial in t and t^{-1} of the form

$$f(t) = \sum_{-n}^{n} a_i t^i = a_{-n}t^{-n} + \ldots + a_{-1}t^{-1} + a_0 + a_1 t + \ldots a_n t^n \tag{5.51}$$

Question. When we adjoin an element α to a ring R and impose some relations, will our original R be a subring of the ring $R[\alpha]$ which we obtain?

Answer. We know R is contained as a subring in the ring of polynomials $R[x]$, as the subring of constant polynomials. So, the restriction of the canonical map $\pi : R[x] \to R[x]/I = R[\alpha]$ to constant polynomials gives us a homomorphism $\psi : R \to R[\alpha]$, which is the map $r \mapsto \overline{r}$. The kernel of ψ is the set of constant polynomials in I, i.e¿

$$\ker \psi = R \cap I \tag{5.52}$$

Note that the degree of the relation $f(\alpha) = 0$ used to construct $R[\alpha]$ is always greater than or equal to 1, so by the previous proposition, the principal ideal I generated by $f(x)$ will not contain constant polynomials, so the kernel of ψ is $\{0\}$ and ψ is injective when α is required to satisfy *one monic* equation. WARNING: ψ *is not always injective.*

Example 5.113. If we adjoin an inverse of zero to a ring, i.e. $0\alpha = 1$, we conclude that $0 = 1$. The zero element is invertible only in the zero ring, so if we adjoin an inverse of 0, we must obtain the whole ring.

Remark 5.114 (Generally). Let $a, b \in R$, with $ab = 0$. Then a is not invertible unless $b = 0$. For if a^{-1} exists in R, then $b = a^{-1}ab = a^{-1}0 = 0$. It follows that if the product of two elements of a ring R is zero, then the procedure of adjoining an inverse of a to R must kill b.

Definition 5.115 (Zero Divisors)**.** An element a of a ring is called a **zero divisor** if there is a nonzero element b such that $ab = 0$.

5.5.2 Lecture

Recall. If we have elements $a_1, ..., a_n$ in a ring R, and we want to impose the relations $a_1 = a_2 = ... = a_n = 0$, the ring which collapses just enough to satisfy these relations is the ring

$$\overline{R} = R/(a_1, ..., a_n) \tag{5.53}$$

where $(a_1, ..., a_n) = \{r_1a_1 + \ldots + r_na_n : r_i \in R\}$ is an ideal, and we have the natural projective ring homomorphism $f : R \to \overline{R}$

Definition 5.116 (Adjoining)**.** We wish to adjoin elements α to a ring R.

Example 5.117 (When we have a universal ring)**.** If $\mathbb{Z} \subset R \subset \mathbb{C}$, and $\alpha \in \mathbb{C}$, then we can create the ring $R' = R[\alpha] = \{r_0 + r_1\alpha + ... + r_n\alpha^n : n \geq 0, r_i \in R\} \supset R$. In particular, if you try to create a larger ring than R by adjoining an element of $\mathbb{C}$ which is not in R, you must include all linear combinations of multiples of that new element with elements in R. In fact, $R[\alpha]$ is the smallest subring of $\mathbb{C}$ containing R and α.

Remark 5.118. The structure of $R' = R[\alpha]$ depends on α.

Example 5.119. If $\alpha \in R$, then $R' = R[\alpha] = R$, and α satisfies the monic polynomial $x - \alpha = 0$ over R (a linear monic monomial).

Observation 5.120. General Adjoining If α satisfies a monic polynomial of least degree n over R, then

$$R' = \{r_0 + r_1\alpha + \ldots + r_{n-1}\alpha^{n-1} : r_i \in R\} \cong R^n \tag{5.54}$$

with all elements distinct. The reason is that once we reach α^n, it can be expressed polynomial of degree less than or equal to $n - 1$, since α satisfies the polynomial

$$f(\alpha) = \alpha^n + r'_{n-1}\alpha^{n-1} + \ldots + r'_1\alpha + r'_0 = 0 \implies \alpha^n = -(r'_{n-1}\alpha^{n-1} + \ldots + r'_1\alpha + r'_0) \tag{5.55}$$

and all higher powers of α can be expressed as a linear combination of the powers of $\alpha \leq n - 1$. If there was a linear combination in R' that was zero but had non-zero coefficients, then α would satisfy a polynomial of degree less than n, which would be a contradiction.

Remark 5.121. If the polynomial isn't monic, then we may not be able to write α^n in terms of the smaller powers of α for general rings. We would have $r'_n\alpha^n = -(r'_{n-1}\alpha^{n-1} + \ldots + r'_1\alpha + r'_0)$, for some $r'_n \in R$.

Definition 5.122 (Transcendental)**.** Even more generally, α may not satisfy any polynomial with coefficients in R. Then, α is called **transcendental**. If this is the case, then all polynomials of α over R are distinct, as if any two are equal, there difference would produce a non-zero polynomial in terms of α which it satisfies.

Example 5.123. Suppose $R = \mathbb{Z}$ or $\mathbb{Q}$ and take $\alpha = \pi$ or e. Then since π and e are transcendental, they do not satisfy any polynomial with coefficients in R.

Remark 5.124 (Cantor Argument). First, note that $\mathbb{Q}$ is countable. It can be proven that the set of numbers which satisfy an algebraic polynomial over $\mathbb{Q}$ is also countable. However, $\mathbb{R}$ and $\mathbb{C}$ are uncountable, so there must be transcendental numbers.

Remark 5.125 (Open Question). Is $\gamma = \lim_{n\to\infty} \left(\left(1 + \frac{1}{2} + \ldots + \frac{1}{n}\right) - \log(n)\right)$, Euler's constant, transcendental?

Proposition 5.126. *If α is transcendental, then for any ring R, $R[\alpha] \cong R[x]$.*

Proposition 5.127. *If α satisfies a monic polynomial of minimal degree f, then $R[\alpha] \cong R[x]/(f(x))$.*

Remark 5.128 (The Adjunction of Elements). If we want a larger ring than R, containing a new element α satisfying a monic polynomial of minimal degree $f(x)$ over R, we can take the ring $R' = R[x]/(f(x)) = \{r_0 + r_1x + \ldots + r_{n-1}x^{n-1} : n \geq 1, r_i \in R\} \cong R^n$, and the map $r \mapsto r_0$ imbedds R as a subring of R'. Additionally, x satisfies $f(x) = 0$, so we may identify α with the residue of x.

Note that addition is coefficient wise, but multiplication involves taking remainders after division by $f(x)$

Example 5.129. We may now write $\mathbb{Z}[i] = \mathbb{Z}[x]/(x^2 + 1) = \mathbb{Z} + \mathbb{Z}x$, $x^2 = -1$.

Definition 5.130 (Irreducible)**.** A polynomial is called **irreducible** if it is not the product of two nonconstant polynomials. That is, $f(x) \in R[x]$ is irreducible if $f(x) \neq g(x)h(x)$ for all $g(x), h(x) \in R[x]$ with $deg(g), deg(h) \geq 1$ (note that it depends on the ring).

Example 5.131. Take $R = \mathbb{Z}/3\mathbb{Z}$. Note that $0^2 \equiv 0$, $1^2 \equiv 1$, and $2^2 \equiv 1$. Thus, we do not have a square root of 2 in $\mathbb{Z}/3\mathbb{Z}$. In particular, $f(x) = x^2 - 2$ is irreducible in $\mathbb{Z}/3\mathbb{Z}$, as there are no roots. Suppose we want to construct a ring R' with the square root of 2. Then we take $R' = \mathbb{Z}/3\mathbb{Z}[x]/(x^2 - 2) = \mathbb{Z}/3\mathbb{Z} + \mathbb{Z}/3\mathbb{Z}x$, so it has 9 elements in it. Moreover, R' is a field. Take $(a + bx), (a - bx) \in R'$. Then $(a + bx)(a - bx) = a^2 - 2b^2 \neq 0$ in $\mathbb{Z}/3\mathbb{Z}$ if a and b are not both zero in $\mathbb{Z}/3\mathbb{Z}$, and since $\mathbb{Z}/3\mathbb{Z}$ is a field, $a^2 - 2b^2$ is invertible. Thereofore, $(a + bx)\left(\frac{a-bx}{a^2-2b^2}\right) = 1$, so it is invertible. Thus, R' is a field.

Proposition 5.132 (Generally)**.** *More generally, let F be a field, and let $f(x)$ be a monic polynomial with coefficients in F, and of degree n. Consider the ring $R = F[x]/(f(x)) \cong F^n$. R is a field if and only if $f(x)$ is irreducible over the field F.*

Proof. Let F be a field and let $f(x)$ be a monic polynomial of degree n with coefficients in F. Define $R = F[x]/(f(x))$. Recall that R is a field if and only if it has only two ideals, R and (0). Moreover, we know that the ideals of R are the ideals of $F[x]$ containing $(f(x))$. In other words, R is a field if and only if there are exactly two ideals in $F[x]$ containing $(f(x))$. That is, $(f(x))$ is a **maximal ideal** of $F[x]$. But, we know all ideals in $F[x]$ are principal ideals generated by a minimial monic polynomial by the Euclidean Algorithm for polynomials. Moreover, I claim that $(f(x)) \subset (g(x)) \subset F[x]$ if and only if $g(x)$ divides $f(x)$. Therefore, if $f(x)$ is irreducible, then the only polynomials that divide $f(x)$ are $f(x)$ and 1. Thus, the only ideals which contain $(f(x))$ are (1) and $(f(x))$. On the other hand, if R is a field, then the only ideals which contain $(f(x))$ are itself and (1), so if a polynomial $g(x)$ divides $f(x)$, then $g(x) = f(x)$ or $g(x) = 1$. Thus, $f(x)$ is irreducible. Therefore, the proof is complete. ■

Example 5.133. Take $F = \mathbb{Q}$ and note that $f(x) = x^2 + 1$ and $g(x) = x^2 - 2$ are irreducible polynomials. Then $\mathbb{Q}[x]/(f(x)), \mathbb{Q}[x]/(g(x)) \cong \mathbb{Q} + \mathbb{Q}x$ as abelian groups, but not as fields.

Proposition 5.134. *To produce a field F' of order p^2, we need an irreducible quadratic polynomial of the form $x^2 + bx + c$ over $\mathbb{Z}/p\mathbb{Z}$.*

Remark 5.135 ($p = 2$). Take the polynomial $x^2 + x + 1 = f(x)$. Then $f(x)$ is irreducible in $\mathbb{Z}/2\mathbb{Z}$. Then $\mathbb{Z}/2\mathbb{Z}[x]/(x^2 + x + 1) \cong (\mathbb{Z}/2\mathbb{Z})^2$ is a field of 4 elements.

Remark 5.136 ($p > 2$). Consider $f(x) = x^2 - c$. $f(x)$ will be irreducible if c is not a square in $\mathbb{Z}/p\mathbb{Z}$. Note that in fact, there is no c that works for all primes p. Moreover, there are primes p where the first 1000, 10000, 1000000, c are all squares.

Proposition 5.137 (Euler's Argument)**.** *There exists some $c \in \mathbb{Z}/p\mathbb{Z}$ that is not a square.*

Proof. Note that $(\mathbb{Z}/p\mathbb{Z})^*$ is an abelian group of order $p-1$, and we consider the group homomorphism $h : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ given by $h(a) = a^2$, which is a group homomorphismsince $(\mathbb{Z}/p\mathbb{Z})^*$ is abelian. The claim that there is $c \in \mathbb{Z}/p\mathbb{Z}$ which is not a square is equivalent to the claim that h is not surjective. If h is not surjective, there are $c \in (\mathbb{Z}/p\mathbb{Z})^*$ which are not of the form $c = a^2$. Note that the image of homomorphism is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*/\ker(h)$. Then h is surjective if and only if it has no kernel since the domain and codomain are identical. This is equivalent to the statement that $\ker(h) = \{1\}$. But, $\ker(h) = \{a \in (\mathbb{Z}/p\mathbb{Z})^* : a^2 \cong 1 \mod p = \{\pm 1\}\}$, where $1 \neq -1$ since $p > 2$. Thus, the kernel of h is non-trivial, and the image of h is of order $\frac{p-1}{2}$, so half the terms are squares and half are non-squares. ■

‘

5.6 Integral Domains and Fraction Fields

5.6.1 Textbook

Remark 5.138. Note that we have seen that adjoining inverses to zero divisors in a ring will kill certain elements, so a ring with zero divisors cannot be embedded into a field.

Definition 5.139 (Integral Domain)**.** An **integral domain** R is a nonzero ring having no zero divisors. In other words, it has the property that if $ab = 0$, then $a = 0$ or $b = 0$, and also $1 \neq 0$ in R.

Observation 5.140. Any subring of a field is an integral domain.

Remark 5.141 (Cancellation Law)*.* If R is an integral domain and $ab = ac$ for some $a, b, c \in R$ with $a \neq 0$, then $b = c$.

Proposition 5.142. *Let R be an integral domain. Then the polynomial ring $R[x]$ is an integral domain.*

Proof. Suppose R is an integral domain. Then we know that $R[x]$ is a ring. Let $p(x) = a_0 + a_1x + ... + a_nx^n, q(x) = b_0 + b_1x + ... + b_mx^m \in R[x]$ with $a_n, b_m \neq 0$. Then $q(x)p(x)$ has the term $a_nb_mx^{m+n}$. Since $a_n, b_m \neq 0$ and R is an integral domain, $a_nb_m \neq 0$. In particular, $a_nb_mx^{m+n} \neq 0$, so $q(x)p(x) \neq 0$. Thus, $R[x]$ is an integral domain as claimed. ■

Proposition 5.143. *An integral domain with finitely many elements is a field.*

Proof. Suppose that R is an integral domain, and let $|R| = n$ for some $n \in \mathbb{N}$. Then, note that the characteristic of R is n. Furthermore, note that if n is composite, then $n = ab$, $1 < a, b < n$, and $n = 0$, so $ab = 0$. Howeover, R is an integral domain so this is a contradiction. Thus, $n = p$ must be prime. Now take $a \in R$, $a \neq 0$. Then $1 \leq a \leq p - 1$. In particular, a is relatively prime to p. Thus, there exist $x \in \mathbb{N}$ so that $ax = 1$. Hence, a is invertible so R is a field. ■

Theorem 5.144. *Let R be an integral domain. There exists an imbedding of R into a field, meaning an injective ring homomorphism $R \to F$, where F is a field.*

Remark 5.145. Note that we could construct the field F by adjoining inverses for all nonzero elements in R.

Definition 5.146 (Fractions)**.** Let R be an integral domain. A **fraction** will be a symbol a/b where $a, b \in R$ and $b \neq 0$. Two fractions a_1/b_1 and a_2/b_2 are called **equivalent**, $a_1/b_1 \approx a_2/b_2$, if

$$a_1 b_2 = a_2 b_1 \tag{5.56}$$

This relation is an equivalence relation on the set $R \times R \backslash \{0\}$.

Definition 5.147 (Field of Fractions)**.** The **field of fractions** F of an integral domain R is the set of equivalence classes of fractions. We will speak of fractions, a_1/b_1 and a_2/b_2, as equal elements of F if they are equivalent fractions: $a_1 b_2 = a_2 b_1$. Addition and multiplication are defined as in arithmetic

$$(a/b)(c/d) = ab/cd, \; a/b + c/d = \frac{ad + bc}{bd} \tag{5.57}$$

Remark 5.148. Note that in the above construction, R is contained in F provided that we identify $a \in R$ with $a/1$ in F, because $a/1 \approx b/1$ if and only if $a = b$. The map $a \mapsto a/1$ is the injective homomorphism referred to in the theorem.

Definition 5.149 (Field of Rational Functions)**.** Take the polynomial ring $K[x]$, where K is any field. This is an integral domain, and its fraction field is called the **field of rational functions in x**, with coefficients in K. This field is usually denoted by

$$K(x) = \left\{ \begin{array}{c} \text{equivalence classes of fractions } f/g, \text{ where } f, \, g \\ \text{are polynomials and } g \text{ is not the zero polynomial} \end{array} \right\} \tag{5.58}$$

Remark 5.150. If $K = \mathbb{R}$ then the rational function $f(x)/g(x)$ defines an actual function on the real line for $g(x) \neq 0$ via the evaluation ring homomorphism.

Proposition 5.151. *Let R be an integral domain, with field of fractions F, and let $\phi : R \to K$ be an injective homomorphism of R to the field K. Then the rule*

$$\Phi(a/b) = \phi(a)\phi(b)^{-1} \tag{5.59}$$

defines the unique extension of ϕ to a homomorphism $\Phi : F \to K$.

Proof. We must first check that this extension is well defined. First, since the denominator of the fraction is non-zero and ϕ is injective, $\phi(b) \neq 0$ for any fraction a/b. Thus, $\phi(b)$ is invertible in K, and $\phi(a)\phi(b)^{-1}$ is an element of K. Next we check that equivalent fractions have the same image: Suppose $a_1/b_1 \approx a_2/b_2$, so $a_1b_2 = a_2b_1$; hence, $\phi(a_1)\phi(b_2) = \phi(a_2)\phi(b_1)$, so we find that

$$\Phi(a_1/b_1) = \phi(a_1)\phi(b_1)^{-1} = \phi(a_2)\phi(b_2)^{-1} = \Phi(a_2/b_2) \tag{5.60}$$

as required. Then, suppose $a/b, c/d \in F$. Observe that

$$\begin{aligned}
\Phi(a/b + c/d) &= \Phi((ad + bc)/bd) \\
&= \phi(ad + bc)\phi(bd)^{-1} \\
&= \phi(ad)\phi(bd)^{-1} + \phi(bc)\phi(bd)^{-1} \\
&= \phi(a)\phi(b)^{-1} + \phi(c)\phi(d)^{-1} \\
&= \Phi(a/b) + \Phi(c/d)
\end{aligned}$$

The fact that multiplication is preserved under Φ and $\Phi(1/1) = 1$ are clear. Furthermore, by definition of Φ, it is the unique extension of ϕ to a homomorphism of $F \to K$, so the proof is complete. ■

5.6.2 Lecture

Definition 5.152 (Integral Domains)**.** A commutative ring R is an **integral domain** (domain) if it has the following property: Whenever $ab = 0$ in R, then either $a = 0$ or $b = 0$.

Example 5.153. If $R = F$ is a field, then R is an integral domain: If $ab = 0$ and $a \neq 0$, then $b = a^{-1}ab = a^{-1}0 = 0$.

Example 5.154. The integers is an integral domain. Additionally, $R = F[x]$ where F is a field is a domain. In general, if R is a domain, so is $R[x]$, and more generally, $R[x_1, ..., x_n]$.

Example 5.155. $R = \mathbb{Z}/4\mathbb{Z}$ is not a domain.

Proposition 5.156 (Cancellation Property)**.** *If R is a domain and $ab = ac$ where $a \neq 0$, then $b = c$ in R.*

Example 5.157. The gaussian integers $\mathbb{Z}[i]$ is a domain.

Observation 5.158. Suppose $R \hookrightarrow F$ is a subring of a field. Then R is a domain.

Theorem 5.159 (Main Theorem for Domains)**.** *If R is a domain, there is a field F we can construct from R in a natural way (quotient field), and an inclusion of rings $R \hookrightarrow F$.*

Example 5.160. For $R = \mathbb{Z}$ we have $F = \mathbb{Q}$, and for $R = \mathbb{Z}[i]$ we have $F = \mathbb{Q}(i) = \{\alpha + \beta i : \alpha, \beta \in \mathbb{Q}\}$. Additionally, for $R = k[x]$, where k is a field, $F = k(x) = \{rational\ functions\ \frac{f(x)}{g(x)} : g(x) \neq 0\}$.

Remark 5.161. The idea is to construct F from R by adding elements $1/a$ for all $a \neq 0$ in R.

Definition 5.162 (Construction of F from R)**.** Start with the set of all symbols $S = \{a/b : a \in R, b \neq 0\ in\ R\}$. We put the equivalence relation $\sim$ on S be declaring $a/b \sim a'/b' \iff ab' = a'b$ in R. The fact that $\sim$ is reflexive and symmetric follows immediately from the fact that $=$ is an equivalence relation and R is commutative. Now, suppose $ab' = a'b$ and $a'b'' = a''b'$. Then $ab'b'' = ba'b'' = bb'a''$, so subtracting from both sides and factoring out b' using the distributive law we obtain $b'(ab'' - ba'') = 0$ where $b' \neq 0$, so $ab'' - ba'' = 0$, so $ab'' = ba''$. Thus, $a/b \sim a''/b''$, so $\sim$ is transitive. Hence, $\sim$ is an equivalence relation.

We now define $F = S/\sim$. We must now show that F has the structure of a field which contains R. We define addition by

$$a/b + c/d := \frac{ad + bc}{bd} \tag{5.61}$$

and we define multiplication by

$$a/b \times c/d := ac/bd \tag{5.62}$$

Moreover, if $a/b \neq 0/1$, then $a \neq 0$, and $b/a \in F$. Moreover, $a/b * b/a = ab/ab = 1/1$, so all nonzero elements of F are invertible.

We define the inclusion of $R \hookrightarrow F$ by $a \mapsto a/1$.

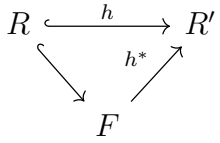
Check of Well-Defined Definitions. Suppose $a/b = a'/b'$ and $c/d = c'/d'$. Then observe that $ac/bd = a'c'/b'd'$ since $acb'd' = a'c'bd$. Moreover, $(ad + bc)/bd = (a'd' + b'c')/b'd'$ since

$$adb'd' + bcb'd' = a'dbd' + bc'b'd$$

■

Remark 5.163. This process is an example of **Localization**.

Definition 5.164 (Universal Property of the Quotient Field)**.** If $f : R \hookrightarrow k$ is any ring inclusion into a field, and $g : R \hookrightarrow F$ is the quotient field of R, then there is a natural homomorphism of fields $h : F \to k$ such that $h \circ g = f$. Additionally, a homomorphism of fields is always injective since the kernel of a field homomorphism is an ideal, and the image of 1 is 1 so the kernel is not the whole field, and hence it must by the trivial ideal (0).



Definition 5.165 (h^*)**.** We define $h^*(a/b) = h(a)h(b)^{-1}$, where $b \neq 0$, so $h(b) \neq 0$ since h is an injective homomorphism, so $h(b)^{-1}$ exists in k.

Observation 5.166. The quotient field is the smallest field which contains the domain which constructs it.

6 Factorization

6.1 Factorization of Integers and Polynomials

6.1.1 Textbook

Theorem 6.1 (Quotient Remainder Theorem)**.** *If $a, b \in \mathbb{Z}$ and $a \neq 0$, then there exist unique $q, r \in \mathbb{Z}$ so tha*

$$b = aq + r \tag{6.1}$$

and $0 \leq r < |a|$.

Corollary 6.2. *Every subgroup of $\mathbb{Z}^+$ is an ideal, and every ideal of $\mathbb{Z}$ is principal, that is, it has the form $d\mathbb{Z}$ for some integer $d \geq 0$.*

Corollary 6.3 (GCD)**.** *For integers a, b (not both zero), there exists a unique positive integer d such that $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, d divides a and b, $ar + bs = d$ for some $r, s \in \mathbb{Z}$, and if c divides a and b then c is less than or equal to d.*

Proposition 6.4. *Let p be a prime integer, and let a, b be integers. If p divides the product ab then p divides a or p divides b.*

Theorem 6.5 (Fundamental Theorem of Arithmetic)**.** *Every integer $a \neq 0$ can be written as a product*

$$a = cp_1...p_k \tag{6.2}$$

where $c = \pm 1$, the p_i are positive prime numbers, and $k \geq 0$. Moreover, this expression is unique up to reordering.

Proof. First, we must prove a prime factorization exists. To prove this it is enough to consider the case of $a > 1$. We proceed by induction on a. If $a = 2$ then a is in its prime factorization so we are done. Now, suppose for all $b < a$, $b \geq 2$ we have a prime factorization of b. Then either a is prime, in which case the product is of one element, or there is a proper divisor $b \neq a$. Then, $a = bb'$ where $b' \neq a$. Both b and b' are smaller than a, and by induction they have prime factorizations. Setting there factors side by side gives the factorization for a.

Second, we must prove uniqueness. Suppose that

$$\pm p_1...p_n = a = \pm q_1...q_m \tag{6.3}$$

Firstly, the signs certainly agree, and applying the previous proposition with $p = p_1$, since p_1 divides $q_1...q_m$, it divides some q_i, say q_1. Since q_1 is prime, $p_1 = q_1$. Cancel p_1. Now

suppose this holds for some $m, n \geq k \geq 1$, so we have that $p_k...p_n = q_k...q_m$, and $p_i = q_i$ for $i < k$. By the same argument as for the base case we find that $p_k = q_k$. Moreover, note that since this process may be repeated for all i, after the $n - threpitition$ one would have $q_{n+1}...q_m = 1$, but each q_i is prime so $n = m$. Thus, $q_i = p_i$ for all $1 \leq i \leq n$ after reordering if needed, so the factorization of a is unique. ■

Definition 6.6 (Irreducible)**.** A polynomial $p(x)$ with coefficients in a field F is called **irreducible** if it is not constant and if its only divisors of lower degree in $F[x]$ are constants.

Theorem 6.7. *Let F be a field, and let $F[x]$ denote the polynomial ring in one variable over F.*

1. *If two polynomials f, g have no common nonconstant factor, then there are polynomials $r, s \in F[x]$ such that $rf + sg = 1$*
2. *If an irreducible polynomial $p \in F[x]$ divides a product fg, then p divides one of the factors f or g.*
3. *Every nonzero polynomial $f \in F[x]$ can be written as a product*

$$f = cp_1...p_k \tag{6.4}$$

where c is a nonzero constant, the p_i are monic irreducible polynomials in $F[x]$, and $k \geq 0$. This factorization is unique except for possible reordering.

Example 6.8. Over $\mathbb{C}$ every polynomial $f(x)$ of positive degree has a root α, and hence a divisor $x - \alpha$. Thus, the irreducible polynomials are linear, and the irreducible factorization of f is

$$f(x) = c(x - \alpha_1)(...(x - \alpha_k) \tag{6.5}$$

Example 6.9. When $F = \mathbb{R}$, there irreducible polynomials are either linear polynomials or quadratic polynomials. The factorization of $f(x)$ into irreducible real polynomials is obtained by grouping conjugate pairs in the complex factorization if need be.

Proposition 6.10. *Let F be a field, and let $f(x)$ be a polynomial of degree n with coefficients in F. Then f has at most n roots in F.*

Proof. An element $\alpha \in F$ is a root of f if and only if $x - \alpha$ divides f. If so, we can write $f(x) = (x - \alpha)g(x)$, where $g(x)$ is of degree $n - 1$. If β is another root of f, then $f(\beta) = (\beta - \alpha)g(\beta) = 0$. Since F is a field, the product of non-zero elements is nonzero. Thus, one of the two elements is zero. In the first case $\beta = \alpha$, and in the second case β is a root of $g(x)$. By induction on n, we may assume that $g(x)$ has at most $n - 1$ roots in F. Then there are at most n possibilities for β. ■

6.1.2 Lecture

First, we consider the factorization of $R = \mathbb{Z}$.

Theorem 6.11 (Euclidean Algorithm for $\mathbb{Z}$)**.** *If $a, b \in \mathbb{Z}$, with $|a| < |b|$, then you can write $b = ma + r$ where $0 \leq r < |a|$.*

Corollary 6.12 (Principal Ideals)**.** *Every ideal $I \neq 0$ is principal, $I = (d)$, generated by the smallest positive integer $d \in I$.*

Corollary 6.13 (GCD Existence)**.** *In particular, $I = (a, b) = (d)$ with $d = ma + nb$ for some $m, n \in \mathbb{Z}$. Moreover, d is the greatest common divisor of $a, b \in \mathbb{Z}$.*

Corollary 6.14. *If p is a prime, and $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. If $p \mid a$, then $\gcd(p, a) = 1$, so by the previous corollary, $1 = ma + np$ for some $n, m \in \mathbb{Z}$. It follows that $b = mba + npb = mpk + npb = p(mk + nb)$, where $pk = ab$. Thus, $p \mid b$. ■

Corollary 6.15 (Fundamental Theorem of Arithmetic)**.** *Every integer n, $n \neq 0$, has a unique factorization with primes $n = \pm p_1 p_2 ... p_k$ up to units $\mathbb{Z}^* = \{\pm 1\}$.*

Proof. Existence is done by induction on n, and uniqueness is done by induction on the number of factors using the previous corollary and the cancellation law. ■

We shall now consider factorization of the ring $R = F[x]$

Theorem 6.16 (Euclidean Algorithm for the Polynomial Ring over a Field)**.** *If $g(x), f(x) \in F[x]$, then there exists $q(x), r(x) \in F[x]$ such that $g(x) = f(x)q(x) + r(x)$ and $degr(x) < degf(x)$.*

Corollary 6.17 (Principle Ideals)**.** *Every ideal I is principal generated by $d(x)$ of least degree in I.*

Corollary 6.18. *Any two polynomials f and g have a greatest common divisor $(d(x)) = (f(x), g(x)) = I$, and $d(x) = m(x)f(x) + n(x)g(x)$ for soem $m(x), n(x) \in F[x]$*

Definition 6.19 (Prime or Irreducible)**.** We say a polynomial $p(x)$ is a prime or irreducible polynomial if any factorization $p(x) = p_1(x)p_2(x)$ has $degp_1 = 0$.

Corollary 6.20. *For two polynomials $p(x)$ and $a(x)$ where $p(x)$ is irreducible, $(p(x), a(x)) = \begin{cases} (1) \\ (p(x)) \end{cases}$. In the first case we have that $1 = m(x)p(x) + n(x)a(x)$ for some $m(x), n(x) \in F[x]$.*

Corollary 6.21. *If $p(x)$ is irreducible and $p(x) \mid a(x)b(x)$, then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.*

Corollary 6.22. *For any $f(x) \in F[x]$, $f(x)$ has a unique factorization into "primes"*

$$f(x) = cp_1(x)...p_k(x) \tag{6.6}$$

up to units in the field ($F^*[x] = F^*$ - constant polynomials not equal to zero).

Remark 6.23. Note that the key theorem for any of these results is the existence of a Euclidean algorithm.

6.2 UFD's, PID's, and Euclidean Domains

6.2.1 Textbook

Definition 6.24 (General Factorization Definitions)**.** Suppose R is an integral domain.

1. We say that an element a **divides** an element b, denoted $a \mid b$ if $b = aq$ for some $q \in R$.
2. The element a is a **proper divisor** of b if $b = aq$ for some $q \in R$ and if neither a nor q is a unit.
3. A nonzero element a of R is called **irreducible** if it is not a unit and it has no proper divisor.
4. Two elements a, a' are called **associates** if and only if they differ by a unit factor, that is, if $a' = ua$ for some unit u.

Corollary 6.25. *Suppose R is an integral domain, and $a, a', b, u \in R$.*

1. *u is a unit if and only if $(u) = (1)$*

2. *a and a' are associates if and only if $(a) = (a')$*

3. *a divides b if and only if $(a) \supset (b)$*

4. *a is a proper divisor of b if and only if $(1) > (a) > (b)$.*

Proposition 6.26. *Let R be an integral domain. The following conditions are equivalent:*

1. *For every nonzero element a of R which is not a unit, the process of factoring a terminates after finitely many steps and results in a factorization $a = b_1...b_k$ of a into irreducible elements of R.*

2. *R does not contain an infinite increasing chain of principal ideals*

$$(a_1) < (a_2) < (a_3) < ... \tag{6.7}$$

Proof. Suppose that R contains an infinite increasing sequence $(a_1) < (a_2) < ....$ Then $(a_n) < (1)$ for every n, because $(a_n) < (a_{n+1}) \subset (1)$. Since $(a_{n-1}) < (a_n)$, a_n is a proper divisor of a_{n-1}, say $a_{n-1} = a_n b_n$ where a_n, b_n are not units. This provides a nonterminating sequence of factorizations of a_1: $a_1 = a_2 b_2 = a_3 b_3 b_2 = a_4 b_4 b_3 b_2 = ...$ Conversely, such a sequence of factorizations gives us an increasing chain of ideals. ■

Remark 6.27. We say that **existence of factorization holds** in R if the two equivalent conditions above hold.

Example 6.28 (Factorization Failing)**.** We adjoin all 2^k-th roots of x_1 to the polynomial ring $F[x_1]$: $R = F[x_1, x_2, ...]$ with relations $x_2^2 = x_1$, $x_3^2 = x_2$, $x_4^2 = x_3$,.... Thus, we can factor the element x_1 indefinitely in this ring, corresponding to an infinite chain of increasing ideals $(x_1) < (x_2) < (x_3) < ...$

Remark 6.29 (Uniqueness). In general, units in rings complicate the uniqueness of the Fundamental Theorem of Arithmetic. In the integers where the only units were 1 and -1, we were able to normalize irreducible elements by taking only positive integers. Similarly, in the polynomial ring $F[x]$ we normalized by taking monic polynomials.

Remark 6.30. In general we do not have a reasonable way to normalize elements of an arbitrary integral domain, so instead we will primarily work with ideals instead of elements.

Definition 6.31 (Unique Factorization Domain)**.** An integral domain R is a **Unique Factorization Domain** (**UFD**) if it has the following properties

1. Existence of factorizations is true for R. In other words, the process of factoring a nonzero element a which is not a unit terminates after finitely many steps and yields a factorization $a = p_1...p_m$, where each p_i is irreducible.
2. The irreducible factorization of an element is unique in the following sense: If a is factored in two ways into irreducible elements, say $a = p_1...p_m = q_1...q_n$, then $n = m$, and with suitable ordering of factors, p_i is an associate of q_i for each i.

Definition 6.32 (Abstract Prime)**.** We will call an element p of an integral domain R **prime** if it has these properties:

1. p is not zero and not a unit.
2. If p divides a product of elements of R, it divides on of the factors.

Proposition 6.33. *Let R be an integral domain. Suppose the existence of factorization holds in R. Then R is a unique factorization domain if and only if every irreducible element of R is prime.*

Proof. Suppose that R is an integral domain where the existence of factorization holds. First, suppose that every irreducible element of R is prime. Then let $a \in R$ have factorizations $a = p_1...p_n = q_1...q_m$. Then p_1 divides the product on the right and p_1 is irreducible, and hence prime, we have that p_1 divides q_1 for some i. Via relabeling if necessary take $q_i = q_1$. Since q_1 is irreducible it follows that $p_1 = q_1$. Then, suppose there exists $n, m \leq k \geq 1$ such that for all $1 \leq m \leq k$, $p_m = q_m$. Then, using the cancellation law we have that $p_{k+1}...p_n = q_{k+1}...q_m$. However by the same argument as our base case and suitable relabeling, $p_{k+1} = q_{k+1}$. Then, $p_i = q_i$ for all i so a's factorization is unique (IFFY). ■

Remark 6.34. Note that in UFD's prime and irreducible are synonymous, but in general this is not the case. For example, if we take the ring $R = \mathbb{Z}[\sqrt{-5}]$, the element 2 has no proper factor so it is irreducible, but it is not prime because 2 divides $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, but it does not divide either factor.

Proposition 6.35. *Let R be a UFD, and let $a = p_1...p_r$, $b = q_1...q_s$ be given prime factorizations of two elements of R. Then a divides b in R if and only if $s \geq r$, and with suitable reordering of factors q_i of b, p_i is an associate of q_i for $i = 1, ..., r$.*

Corollary 6.36 (GCD)**.** *Let R be a UFD, and let a, b be elements of R which are not zero. There exists a* ***greatest common divisor*** *d of a and b with the following properties:*

1. *d divides a and b*

2. *if an element c in R divides a and b, then c divides d.*

Remark 6.37. The second condition implies that any two greatest common divisors of a and b are associates. However, the greatest common divisor need not have the form $ar + bs$.

Definition 6.38 (Principal Ideal Domain)**.** An integral domain R is a **principal ideal domain** (**PID**) if every ideal in R is principal.

Proposition 6.39. .

1. *In an integral domain, a prime element is irreducible*
2. *In a PID an irreducible element is prime.*

Proof. Suppose that R is an integral domain, and let $r \in R$ be a prime. Then r is not zero nor a unit, and if r divides a product $ab \in R$, then r divides a or r divides b. For the sake of contradiction suppose that r is not irreducible. Then r has proper factors $x, y \in R$ so that $r = xy$. However, then r must divide x or y. Without loss of generality suppose r divides x. Then there exists $t \in R$ so that $tr = x$. It follows that $r = xy = try$, so $ty = 1$ by the cancellation law. However, y was assumed to be a proper factor of r so it is not invertible, which is a contradiction. Therefore, r must have no proper factors, so it is irreducible.

Suppose R is a PID and that $r \in R$ is an irreducible element. Then there exists no proper divisors for r. In other words, there exists no element $a \in R$ such that $(1) > (a) > (r)$. First, note that since r is irreducible r is not a unit nor zero, since all nonzero elements of R divide zero. Thus, we aim to show that if r divides the product ab, then r divides a or b. If r divides ab, then in particular $(r) \supset (ab)$. Then, note that $(a) \supset (ab)$. If $(r) \supset (a)$ then r divides a and we're done. On the other hand suppose $(a) \supset (r)$. Then, there exists $u \in R$ so that $r = au$. Since r is irreducible, (continue) ■

Theorem 6.40. *A PID is a UFD*

Proof. Suppose that R is a PID. Then every irreducible element of R is prime. Thus, the uniqueness of irreducible factorization is satisfied, so we need only prove that the existence of factorizations holds. This is equivalent to showing that R has no infinite chains of increasing ideals. For the sake of contradiction suppose that R has such a chain, $(a_1) < (a_2) < ....$

Lemma 6.41. *Let R be a ring. The union of an increasing chain of ideals $I_1 \subset I_2 \subset ...$ is an ideal.*

Proof. Let I denote the union of the chain. If $u, v \in I$ then they are in I_n for some n. Then $u + v, ru \in I_n$ for all $r \in R$. Hence I is a ideal. ■

We now apply this lemma to the union I of our chain of principal ideals, and use the hypothesis that R is a PID to conclude that I is principal, say $I = (b)$. Since b is a union of ideals (a_n), it is one of these ideals. But, if $b = (a_n)$ for some n, then $(b) \subset (a_n)$, and on the other hand $(a_n) \subset (a_{n+1}) \subset (b)$. Therefore, $(a_n) = (a_{n+1}) = (b)$. This contradicts the assumption that the chain is infinitely increasing, and this contradiction completes the proof. ■

Proposition 6.42. .

1. *Let p be a nonzero polynomial of a principal ideal domain R. Then $R/(p)$ is a field if and only if p is irreducible.*
2. *The maximal ideals are the principal ideals generated by irreducible elements.*

Proof. Since an ideal M is maximal if and only if R/M is a field, the two parts are equivalent. We shall prove the second part. A principal ideal (a) contains another principal ideal (b) if and only if a divides b. The only divisors of an irreducible element p are the units and associates of p. Therefore, the only principal ideals which contain (p) are (p) and (1). Since every ideal of R is principal, this shows that an irreducible element generates a maximal ideal. Conversely, let b be a polynomial having a proper factorization $b = aq$, where neither a nor q is a unit. Then $(b) < (a) < (1)$, and this shows that (b) is not maximal. ■

Definition 6.43 (Size Function on a Ring)**.** A **size function** on an integral domain R will be any function

$$\sigma : R\backslash\{0\} \to \{0, 1, 2, ...\} \tag{6.8}$$

from the set of nonzero elements of R to the nonnegative integers.

Definition 6.44 (Euclidean Domain)**.** A PID R is a **Euclidean domain** if there is a size function σ on R such that the division algorithm holds: Let $a, b \in R$ and suppose that $a \neq 0$. There are elements $q, r \in R$ so that $b = aq + r$, and either $r = 0$ or $\sigma(r) < \sigma(a)$

Proposition 6.45. *The rings $\mathbb{Z}$, $F[x]$, and $\mathbb{Z}[i]$are Euclidean domains.*

Remark 6.46. Note that $\mathbb{Z}$ has size function absolute value, $F[x]$ has size function degree, and $\mathbb{Z}[i]$ has size function modulus squared.

Proposition 6.47. *A Euclidean domain is a PID, and hence it is a UFD.*

Corollary 6.48. *The rings $\mathbb{Z}$, $\mathbb{Z}[i]$, and $F[x]$ (F is a field) are PIDs and UFDs.*

6.2.2 Lecture

Recall. Recall that an integral domain is a commutative ring R such that if $ab = 0$ in R, then either $a = 0$ or $b = 0$. Examples of this are $\mathbb{Z}$, $F[x]$, and if R is a domain, so is $R[x]$.

Recall. Associated to any integral domain R is a field $R \hookrightarrow F$ called the field of fractions of R, which is constructed on the set of symbols $S = \{a/b : a, b \in S, b \neq 0\}$ by an equivalence relation $\sim$, so

$$F := S/\sim = \{a/b : a, b \in R, b \neq 0, a/b \sim a'/b' \iff ab' = a'b \in R\} \tag{6.9}$$

We define natural senses of addition and multiplication, and we imbed R by taking $R \hookrightarrow F$, $a \mapsto a/1$.

Definition 6.49 (Euclidean Domain)**.** A domain R is **Euclidean** if there is a size function

$$\delta : R\backslash\{0\} \to \{0, 1, 2, 3, ...\} \tag{6.10}$$

such that for any $a, b \neq 0$ in R, we have

$$b = ma + r, \text{ with either } r = 0 \text{ or } \delta(r) < \delta(a) \tag{6.11}$$

Example 6.50. For $\mathbb{Z}$ the size function is the absolute value, $\delta(n) = |n|$. For $F[x]$ we take $\delta(f(x)) = deg f + 1 \geq 1$.

Remark 6.51. The results found for $F[x]$ and $\mathbb{Z}$ then follow for the Euclidean domains.

Example 6.52 (Gaussian Integers)**.** The ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is Euclidean with size function $\delta(a + bi) = |a + bi|^2 = a^2 + b^2$.

Proof. Suppose $A, B \in \mathbb{Z}[i]$, and we can write $B = A \cdot w$ where $w = \alpha + \beta i$, where $\alpha, \beta \in \mathbb{Q}$. This follows from the fact that in $\mathbb{C}$ we can write

$$B/A = B\overline{A}/A\overline{A}$$

where the denominator is a positive integer. Take $\alpha = \alpha_0 + r_0$ and $\beta = \beta_0 + s_0$ where $-1/2 \leq r_0, s_0 < 1/2$ and $\alpha_0, \beta_0 \in \mathbb{Z}$. Then we get $B = A(\alpha_0 + \beta_0 i) + A(r_0 + s_0 i)$, where the first term we shall label by M, and the second we shall label by R. We claim that $R = 0$ or $\delta(R) < \frac{1}{2}\delta(A)$. Then,

$$\delta(R) = \delta(A)(r_0^2 + s_0^2) \leq \delta(A)(\frac{1}{4} + \frac{1}{4}) = \frac{1}{2}\delta(A)$$

Since the size function, modulus squared, is multiplicative ($|zw| = |z||w|$). Thus, $\mathbb{Z}[i]$ is Euclidean, as desired. ■

Corollary 6.53. *Every ideal I is principal, so in particular the ideal constructed a 4-6 lectures ago with $\mathbb{Z}[i]/I \cong \mathbb{Z}/p\mathbb{Z}$ for $p \equiv 1 \mod 4$ is generated by a single element $a+bi$ which implies that $a^2+b^2=p$ (Fermat).*

Example 6.54 (Non-example)**.** Consider $R = \{a+b\sqrt{-5} : a,b \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{-5}]$. Suppose we take $\delta(a+b\sqrt{-5}) = a^2+5b^2$. However, this size function does not give a number less then one multiplied by A when performing the same computation as above, so it fails. In fact, this R is not Euclidean, so you cannot find the Euclidean algorithm in this ring for any size function. This can be seen from the fact that one of the properties which follow from the Euclidean algorithm fails. In particular, we do not have a unique factorization: namely $6 = 2*3$ in this ring and $6 = (1+\sqrt{-5})(1-\sqrt{-5})$ are prime factorizations of 6 in this ring which are not equal. In fact, there are ideals in this ring which are not principal. For example $I = (2, 1+\sqrt{-5})$ is not principal. This is the kernel of the ring homomorphism $R \to \mathbb{Z}/2\mathbb{Z}$, $a+b\sqrt{-5} \mapsto a+b \mod 2$

Figure 1: We have shown for an ideal R

$$\begin{array}{c} RisEuclidean \\ \downarrow \\ Risaprincipalidealdomain \end{array}$$

$$\begin{array}{c} (everyI = (a)) \\ \downarrow \\ Uniquefactorizationintoprimeelements \end{array}$$

Definition 6.55 (Divide, Prime, etc. In terms of Ideals)**.** Suppose R is an integral domain.

1. a divides b in $R \hookrightarrow b = ma$ for some $m \in R \hookrightarrow b \in (a) \hookrightarrow (b) \subset (a)$
2. a divides b **properly** in R if neither a nore m is a unit in R, with $b = ma \hookrightarrow (b) \underbrace{\subsetneq}_{m \text{ is not a unit}} (a) \underbrace{\subsetneq}_{a \text{ is not a unit}} R$
3. p is prime (or irreducible if R is a PID) in R if p is not a unit and p has no proper factor in $R \hookrightarrow (p) \subsetneq R$ and (p) is maximal with respect to principal ideals $\iff R/(p)$ is an integral domain.

Remark 6.56 (Prime and Irreducible). If R is a PID then p is prime $\iff$ the ideal generated by p, (p), is a maximal ideal of R $\iff$ $R/(p)$ is a field (has only two principal ideals).

Example 6.57 (UFD but not a PID)**.** Take $R = \mathbb{Z}[x]$. Take the ideal $I = (x)$ (where x is a prime). Moreover, $R/I \cong \mathbb{Z}$ by the map $f(x) \mapsto f(0)$, and $\mathbb{Z}$ is an integral domain. Thus x is prime in R since its quotient is an integral domain, and also, since $\mathbb{Z}$ is not a field, R is not a PID. Consequently, I is only maximal with respect to principal ideals, and there must be ideals that contain I in R that are not principal. (continue)

Remark 6.58. If we can ever find an ideal such that the quotient under that principal ideal is an integral domain which is not a field, then the original ring is not PID.

Recall. For a domain R, R is Euclidean if we have a size function

$$\delta : R\backslash\{0\} \to \{1, 2, ...\} \tag{6.12}$$

that satisfies the Euclidean Algorithm, so for $b, a \in R$, $a \neq 0$, there exists $m, r \in R$ so that $b = ma + r$ and $\delta(r) < \delta(a)$. Moreover, R being Euclidean implies that every ideal is principal, generated by the element of least size δ in the ideal (so it's a PID), which implies that every element of R has a unique prime factorization (so it is a UFD), so for any $a \in R$, $a = u\underbrace{p_1...p_r}_{primes}$, where u is a unit, and this expression is unique up to units. Additionally, recall $p \in R$ is prime $\iff$ $(p) \subsetneq R$ is maximal with respect to principal ideals $\iff$ $R/(p)$ is an integral domain.

Observation 6.59. If $R/(p)$ is not a field, then there exists an ideal $(p) \subsetneq I \subsetneq R$.

Example 6.60. $R = \mathbb{Z}[x]$, $p = x$, $R/(p) \cong \mathbb{Z}$ is a domain (not a field), and the map $R \to \mathbb{Z}/2\mathbb{Z}$ given $f(x) \mapsto f(0) \mod 2$ gives $R \supset (x, 2) \supset (p)$.

6.3 Gauss's Lemma

6.3.1 Textbook

Remark 6.61. Consider $R = \mathbb{Q}[x]$. From a previous proposition we have that every polynomial $f(x) \in \mathbb{Q}[x]$ can be expressed uniquely in the form $cp_1...p_k$ up to units $c \in \mathbb{Q}$, where p_i are monic polynomials which are irreducible over $\mathbb{Q}$. Suppose $f(x) \in \mathbb{Z}[x]$, and f can be factored in $\mathbb{Q}[x]$. Can it be factored without leaving $\mathbb{Z}[x]$?

Definition 6.62 (Primitive)**.** A polynomial $f(x) = a_0 + ... + a_n x^n$ is called **primitive** if its coefficients $a_0, ..., a_n$ have no common integer factor except for the units ± 1 and if its highest coefficient a_n is positive.

Lemma 6.63. *Every polynomial $f(x) \in \mathbb{Q}[x]$ can be written as the product:*

$$f(x) = cf(x_0) \tag{6.13}$$

where c is a rational number and $f_0(x)$ is a primitive polynomial in $\mathbb{Z}[x]$. Moreover, this expression for f is unique. The polynomial $f(x)$ has integer coefficients if and only if c is an integer. If so, then $|c|$ is the greatest common divisor of the coefficients of f, and the sign of c is the sign of the leading coeffient of f.

Proof. To find f_0, we first multiply f by an integer to clear the denominators in its coefficients. This will give us a polynomial f_1 with integer coefficients. Then, we factor out the greatest common divisor of the coefficients of f_1, and adjust the sign of the leading coefficient. The resulting polynomial f_0 is primitive, and $f = cf_0$ for some rational number c. This proves existence.

Now, suppose $cf_0 = dg_0$, where $c, d \in \mathbb{Q}$ and f_0, g_0 are primitive polynomials. Let $\{a_i\}, \{b_i\}$ be the coefficients of f_0 and g_0 respectively. Then $ca_i = db_i$ for all i. Suppose that c is an integer. Then since the gcd of $\{a_0, ..., a_n\}$ is one, the gcd of $\{ca_0, ..., ca_n\}$ is c. Similarly, d is the gcd of $\{db_0, ..., db_n\} = \{ca_0, ..., ca_n\}$. Hence $c = \pm d$ and $f_0 = \pm g_0$. Since f_0, g_0 have positive leading coefficients $f_0 = g_0$ and $c = d$. If f has integer coefficients the denominators don't need to be cleared out, so c is an integer, and up to sign it is the gcd of the coefficients. ■

Remark 6.64 (Content)*.* The rational number c is the **content** of f. If f has integer coefficients then the content of f divides f in $\mathbb{Z}[x]$. Also, f is primitive if and only if its content is one.

Theorem 6.65 (Gauss's Lemma)**.** *A product of primitive polynomials in $\mathbb{Z}[x]$ is primitive.*

Proof. Let f, g be primitive polynomials, and let $h = fg$. Since the leading coefficients of f and g are positive, so is the leading coefficient of h. To show h is primitive we shall show that no prime number p divides all the coefficients of $h(x)$. This will show that the content of h is one. Consider the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$ taking a polynomial to its residue modulo p. We have to show that $\overline{h} \neq 0$. Since f is primitive, its coefficients are not all divisible by p. So, $\overline{f} \neq 0$. Similarly, $\overline{g} \neq 0$. Since the polynomial ring $\mathbb{Z}/p\mathbb{Z}[x]$ is an integral domain, $\overline{h} = \overline{f}\overline{g} \neq 0$, as required. ■

Proposition 6.66. .

1. *Let f, g be polynomials in $\mathbb{Q}[x]$, and let f_0, g_0 be the associated primitive polynomials in $\mathbb{Z}[x]$. If f divides g in $\mathbb{Q}[x]$, then f_0 divides g_0 in $\mathbb{Z}[x]$.*

2. *Let f be a primitive polynomial of $\mathbb{Z}[x]$, and let g be any polynomial with integer coefficients. Suppose that f divides g in $\mathbb{Q}[x]$, say $g = fq$, with $q \in \mathbb{Q}[x]$. Then $q \in \mathbb{Z}[x]$, and hence f divides g in $\mathbb{Z}[x]$*

3. *Let f, g be polynomials in $\mathbb{Z}[x]$. If they have a common nonconstant factor in $\mathbb{Q}[x]$, then they have a common nonconstant factor in $\mathbb{Z}[x]$ too.*

Proof. To prove the first proposition we may clear denominators so that f, g become primitive. Then (1) becomes a consequence of (2). To prove (2) we apply a previous proposition to right $q = cq_0$, where q_0 is primitive and $c \in \mathbb{Q}$. By Gauss's lemma, fq_0 is primitive, and the equation $g = cfq_0$ shows that it is the primitive polynomial g_0 associated to g. Therefore $g = cg_0$ and c is the content of g. Since $g \in \mathbb{Z}[x]$, it follows that $c \in \mathbb{Z}$, hence that $q \in \mathbb{Z}[x]$. Finally, to prove (3), suppose that f, g have a common factor $h \in \mathbb{Q}[x]$. We may assume that h is primitive, and then by (2) h divides both f and g in $\mathbb{Z}[x]$. ■

Corollary 6.67. *If a nonconstant polynomial f is irreducible in $\mathbb{Z}[x]$, then it is irreducible in $\mathbb{Q}[x]$.*

Proposition 6.68. *Let f be an integer polynomial with positive leading coefficient. Then f is irreducible in $\mathbb{Z}[x]$ if and only if either*

1. *f is a prime integer, or*

2. *f has a primitive polynomial which is irreducible in $\mathbb{Q}[x]$*

Proof. Suppose that f is irreducible. We may write $f = cf_0$ where f_0 is primitive. Since f is irreducible, this cannot be a proper factorization. Hence, either c or f_0 is 1. If $f_0 = 1$, then f is constant, and to be irreducible, a constant polynomial must be a prime integer. If $c = 1$ then f is primitive and is irreducible in $\mathbb{Q}[x]$ by the previous corollary. The converse that integer primes and primitive irreducible polynomials are irreducible in $\mathbb{Z}[x]$ is clear. ■

Proposition 6.69. *Every irreducible element of $\mathbb{Z}[x]$ is a prime element.*

Proof. Let f be irreducible, and suppose f divides gh, where $g, h \in \mathbb{Z}[x]$.

Case 1: $f = p$ is a prime integer. Write $g = cg_0$ and $h = dh_0$. Then g_0h_0 is primitive, and hence some coefficient a of g_0h_0 is not divisible by p. But, since p divides gh, the corresponding coefficient, which is cda, is divisible by p. Hence, p divides c or p divides d, so p divides g or h.

Case 2: f is a primitive polynomial which is irreducible in $\mathbb{Q}[x]$. Since $\mathbb{Q}$ is a field, $\mathbb{Q}[x]$ is a PID and f is a prime element of $\mathbb{Q}[x]$. Hence f divides g or h in $\mathbb{Q}[x]$. In particular, f divides g or h in $\mathbb{Z}[x]$. ■

Theorem 6.70. *The polynomial ring $\mathbb{Z}[x]$ is a UFD. Every nonzero polynomial $f(x) \in \mathbb{Z}[x]$ which is not ± 1 can be written as a product*

$$f(x) = \pm p_1 ... p_m q_1(x) ... q_n(x) \tag{6.14}$$

where the p_i are prime integers and the $q_i(x)$ are irreducible primitive polynomials. This expression is unique up to rearrangement of factors.

Theorem 6.71 (Generalization to Arbitrary UFDs)**.** *Let R be a UFD with field of fractions F:*

1. *Let f, g be polynomials in $F[x]$, and let f_0, g_0 be the associated primitive polynomials in $R[x]$. If f divides g in $F[x]$, then f_0 divides g_0 in $R[x]$.*
2. *Let f be a primitive polynomial in $R[x]$, and let g be any polynomial in $R[x]$. Suppose that f divides g in $F[x]$, say $g = fq$, $q \in F[x]$. Then $q \in R[x]$ and hence f divides g in $R[x]$*
3. *Let f, g be polynomials in $R[x]$. If they have a common nonconstant factor in $F[x]$, then they have a common nonconstant factor in $R[x]$ too.*
4. *If a nonconstant polynomial f is irreducible in $R[x]$, then it is irreducible in $F[x]$.*
5. *$R[x]$ is a UFD.*

Corollary 6.72. *Recall that $R[x_1, ..., x_n] \cong R[x_1, ..., x_{n-1}][x_n]$. The polynomials $\mathbb{Z}[x_1, ...x_n]$ and $F[x_1, ..., x_n]$, where F is a field, are UFDs.*

6.3.2 Lecture

Remark 6.73. Even though $\mathbb{Z}[x]$ is not a principal ideal domain, it has unique factorization.

Theorem 6.74. *If R is a domain with unique factorization into primes, so is $R[x]$.*

Corollary 6.75. *Then, given a UFD R, then $R[x_1, ..., x_n]$ is a UFD.*

Remark 6.76. Take $f(x) \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$. Since $\mathbb{Q}$ is a field, $\mathbb{Q}[x]$ is a Euclidean domain, so it's a PID, and in particular it is a UFD, and we can factor f in $\mathbb{Q}[x]$ as $f(x) = cp_1(x)...p_k(x)$, where p_i are monic irreducible polynomials in $\mathbb{Q}[x]$, and c is a unit in $\mathbb{Q}[x]$. We want to define an analog of monic so that the p_i have integral coefficients.

Definition 6.77 (Analog of Monic Polynomials: Primitive polynomial)**.** A primitive polynomial has the form $f_0 = a_n x^n + ...a_1 x + a_0$, where $a_i \in \mathbb{Z}$, and $\gcd(a_0, a_1, ..., a_n) = 1$, or $(a_0, ..., a_n) = \mathbb{Z}$. Moreover, the highest non-zero coefficient, a_n, is positive ($a_n > 0$).

Proposition 6.78. *Any $f \in \mathbb{Z}[x]$ can be written uniquely as $f = cf_0$, where f_0 is primitive.*

Corollary 6.79. *In fact, if $f(x) \in \mathbb{Q}[x]$, then $f(x) = cf_0(x)$ where f_0 is primitive in $\mathbb{Z}[x]$, and $c \in \mathbb{Q}$, and this expression is unique.*

Proof. Take $f(x) \in \mathbb{Q}[x]$. There exists a nonzero integer n so that $na_i \in \mathbb{Z}$ for all i, so $nf(x) \in \mathbb{Z}[x]$. Then we can write $nf(x) = df_0(x)$, where $f_0(x)$ is primitive, so $f(x) = \frac{d}{n} f_0(x)$. ■

Definition 6.80 (Content)**.** The **content** of of a polynomial $f(x) \in \mathbb{Q}[x]$ is the number $c \in \mathbb{Q}$ such that $f(x) = cf_0(x)$ in the above decomposition.

Corollary 6.81. *In fact, $f(x) \in \mathbb{Z}[x] \iff$ the content $c \in \mathbb{Z}$.*

Remark 6.82. Take $f(x) \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$, with factorization $f = cp_1(x)...p_k(x)$ in $\mathbb{Q}[x]$. Then we can write

$$f(x) = c(c_1 q_1(x))...(c_k q_k(x)) = dq_1(x)...q_k(x) \tag{6.15}$$

where $d = cc_1...c_k \in \mathbb{Q}$ and $q_i \in \mathbb{Z}[x]$ are primitive, and in fact irreducible polynomials in $\mathbb{Q}[x]$ since they are multiples of irreducible polynomials.

Lemma 6.83 (Gauss's Lemma)**.** *If f_0 and g_0 are primitive polynomials in $\mathbb{Z}[x]$, so is $f_0 g_0$.*

Proof. If not, say the prime p divides all the coefficients of $f_0(x)g_0(x)$. Consider the ring homomorphism $\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$ that takes $a \mapsto a \mod p$ and $x \mapsto x$. This implies that the image of $f_0 g_0$ under the homomorphism is 0. Then, since $\mathbb{Z}/p\mathbb{Z}[x]$ is an integral domain and $\overline{f_0(x)g_0(x)} = 0$ implies that either $\overline{f_0} = 0$ or $\overline{g_0 = 0}$. However, this implies that one of factors isn't primitive, which is a contradiction. ■

Remark 6.84. Thus, $q_1...q_k$ in the above decomposition is itself a primitive polynomial. Then, since $f(x) = d(q_1...q_k)$ is the unique decomposition described above, d must be an integer.

Corollary 6.85. *If f is irreducible in $\mathbb{Q}[x]$, then it is irreducible in $\mathbb{Z}[x]$.*

Remark 6.86. Then, in the above factorization with $f(x) = d(q_1...q_k)$, to obtain our unique factorization in $\mathbb{Z}[x]$ we need only factor d into its primes so that $f(x) = \pm p_1 p_2 ... p_l q_1(x)...q_k(x)$ where p_i are integer primes, and $q_i(x)$ are primitive irreducible polynomials in $\mathbb{Z}[x]$, where $p_1...p_l$ is the prime factorization of the content of $f(x)$.

Remark 6.87. It is easier to prove polynomials in $\mathbb{Z}[x]$ are irreducible than to prove polynomials in $\mathbb{Q}[x]$ are irreducible. This can be done using the homomorphism $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}[x]$.

Example 6.88. Take $x^3 + x + 1 = f(x)$. Look at the image in $\mathbb{Z}/2\mathbb{Z}[x]$. Does it have a factor $f(x) = m(x)n(x)$? We know that $m(x)$ must be degree 1 and $n(x)$ must be of degree 2. Then $m(x) = (x + a)$ and $n(x) = (x^2 + bx + c)$, so $f(x)$ would have a root in $\mathbb{Z}/2\mathbb{Z}[x]$. However, $f(0) = 1$ and $f(1) = 1$, so f has no roots in $\mathbb{Z}/2\mathbb{Z}[x]$, and hence is irreducible.

Example 6.89. Take $x^4 + x^3 + 1 = f(x)$. Note that $f(x)$ cannot be the factor of a degree 3 polynomial and a degree 1 polynomial as it has no roots in $\mathbb{Z}/2\mathbb{Z}[x]$. Then suppose $f(x) = (x^2 + ax + b)(x^2 + cx + d)$ where these factors must be irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$ since f has no roots in $\mathbb{Z}/2\mathbb{Z}[x]$. The only such irreducible polynomial of degree 2 is $x^2+x+1 = m(x)$. But, the square of $m(x)$ is not $f(x)$, so f must be irreducible as it can't be written as the product of irreducible polynomials in $\mathbb{Z}/2\mathbb{Z}[x]$.

Remark 6.90 (WARNING). There exist polynomials which are irreducible over the integers, but can be factored in every ring $\mathbb{Z}/p\mathbb{Z}[x]$.

Remark 6.91. For $\mathbb{Z}/2\mathbb{Z}[x]$, there is an irreducible $f(x)$ of every degree.

6.4 Explicit Factorization of Polynomials

6.4.1 Textbook

Proposition 6.92. *Let $f(x) = a_0 + ... + a_n x^n \in \mathbb{Z}[x]$ be an integer polynomial, and let p be a prime integer which does not divide a_n. If the residue $\overline{f}$ of f modulo p is irreducible, then f is irreducible in $\mathbb{Q}[x]$.*

Proof. We may assume that f is primitive. Since p does not divide a_n, the degrees of f and $\overline{f}$ are equal. If f factors in $\mathbb{Q}[x]$ then it also factors in $\mathbb{Z}[x]$. Let $f = gh$ be a proper factorization in $\mathbb{Z}[x]$. Since f is primitive, g and h have positive degree. Since $deg f = deg\overline{f}$ and $\overline{f} = \overline{g}\overline{h}$, it follows that $deg g = deg\overline{g}$ and $deg h = deg\overline{h}$, hence $\overline{f} = \overline{g}\overline{h}$ is a proper factorization, which shows that $\overline{f}$ is reducible (proof by contrapositive). ■

Remark 6.93 (Sieve of Eratosthenes). Suppose we want to find all the prime integers less than n. Then, we make a list of all the integers from 2 to n. after passing 2 we remove all of its multiples from the list. We repeat this for every integer remaining in the list following 2. This process can in fact be done to find the irreducible polynomials of the ring $\mathbb{Z}/p\mathbb{Z}[x]$.

Theorem 6.94 (Eisenstein Criterion)**.** *Let $f(x) = a_n x^n + ... + a_0 \in \mathbb{Z}[x]$ be an integer polynomial, and let p be a prime integer. Suppose that the coefficients of f satisfy the following conditions*

1. *p does not divide a_n;*
2. *p divides the other coefficients $a_{n-1}, ..., a_0$;*
3. *p^2 does not divide a_0.*

Then f is irreducible in $\mathbb{Q}[x]$. If f is primitive, it is irreducible in $\mathbb{Z}[x]$

Proof. Suppose that the conditions are met for f. Let $\overline{f}$ denote the residue modulo p. The hypothesis (1) and (2) imply that $\overline{f} = \overline{a_n} x^n$ and $\overline{a_n} \neq 0$. If f is reducible in $\mathbb{Q}[x]$, then it will factor in $\mathbb{Z}[x]$ into factors of positive degree, $f = gh$. Then $\overline{g}$ and $\overline{h}$ divide $\overline{a_n} x^n$, and hence each of these polynomials is a monomial. Therefore, all coefficients of g and h except for the highest ones are divisible by p. Let the constant coefficients of g, h be b_0, c_0. Then the constant coefficient of f is $a_0 = b_0 c_0$. Since p divides b_0 and c_0, it follows that p^2 divides a_0 which contradicts (3). This shows that f is irreducible. ■

Corollary 6.95. *Let p be a prime. The* ***cyclotomic polynomial*** *$f(x) = x^{p-1} + ... + x + 1$, whose roots are the p-th roots of unity, is irreducible in $\mathbb{Q}[x]$.*

Proof. Note that $(x-1)f(x) = x^p - 1$. Next, we make the substitution $x = y + 1$ into this product, obtaining

$$yf(y+1) = (y+1)^p - 1 = y^p + \binom{p}{1} y^{p-1} + ... + \binom{p}{p-1} y. \tag{6.16}$$

We have $\binom{p}{i} = \frac{p(p-1)...(p-i+1)}{i!}$. If $i < p$, then the prime isn't a factor of $i!$, so $i!$ divides the product $(p-1)...(p-i+1)$. This implies that $\binom{p}{i}$ is divisible by p. Dividing the expansion $yf(y+1)$ by y shows that $f(y+1)$ satisfies the conditions of the Eisenstein Criterion, hence that it is an irreducible polynomial. It follows that $f(x)$ is irreducible too. ■

Proposition 6.96. *Let $f(t, x)$ be a polynomial in $\mathbb{C}[t, x]$, written as a polynomial whose coefficients are in polynomials of t: $f(t, x) = a_n(t)x^n + ... + a_1(t)x + a_0(t)$. Suppose that*

1. *t does not divide $a_n(t)$;*

2. *t divides $a_{n-1}(t), ..., a_0(t)$;*

3. *t^2 does not divide $a_0(t)$.*

Then $f(x,t)$ is irreducible in the ring $\mathbb{C}(t)[x]$. If f is primitive, meaning that it has no factor which is a polynomial in t alone, then f is irreducible in $\mathbb{C}[t][x]$.

6.5 Primes in the Gaussian Integers

6.5.1 Textbook

Theorem 6.97. .

1. *Let p be a prime integer. Then either p is a **Gauss prime**, or else it is the product of two complex conjugate Gauss primes: $p = \pi\overline{\pi}$*

2. *Let π be a Gauss prime. Then either $\pi\overline{\pi}$ is a prime integer, or else it is the square of a prime integer.*

3. *The prime integers which are Gauss primes are thos congruent to 3 modulo 4; that is $3, 7, 11, 19, ...$*

4. *Let p be a prime integer. The following are equivalent:*

   (a) *p is a product of two complex conjugate Gauss primes*

   (b) *p is the sum of two integer squares: $p = a^2 + b^2$, with $a, b \in \mathbb{Z}$*

   (c) *The congruence $x^2 \equiv -1 \mod p$ has an integer solution*

   (d) *$p \equiv 1 \mod 4$, or $p = 2$; that is $p = 2, 5, 13, 17, ...$*

Proof. (In the book - long) ■

Lemma 6.98. *A Gauss integer which is a real number is an ordinary integer. An ordinary integer d divides another integer a in $\mathbb{Z}[i]$ if and only if d divides a in $\mathbb{Z}$. Moreover, d divides a Gauss integer $a + bi$ if and only if d divides both a and b.*

Lemma 6.99. *Let p be a prime integer. Then the following conditions are equivalent:*

1. *p is a Gauss prime*

2. *the ring $R' = \mathbb{Z}[i]/(p)$ is a field*

3. *$x^2 + 1$ is an irreducible polynomial in the ring $\mathbb{Z}/p\mathbb{Z}[x]$.*

Proof. The equivalence of the first two statements follows from the fact that $\mathbb{Z}[i]$ is a Euclidean domain, so in particular it is a principal ideal domain. From the Third Isomorphism Theorem we know that to construct the ring R', the order of the relations introduced into $\mathbb{Z}[x]$ is irrelevant. Thus, let us reverse the order. Then we now by the Substitution Principle that the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$ has kernel $p\mathbb{Z}[x]$, so $\mathbb{Z}[x]/p\mathbb{Z}[x] \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}[x]$. Now, we introduce our other relation $x^2 + 1 = 0$ into the ring. Then we have an isomorphism $\mathbb{Z}/p\mathbb{Z}[x]/(x^2+1) \xrightarrow{\sim} R'$. Then, since $\mathbb{Z}/p\mathbb{Z}[x]$ is a Euclidean domain, it is a PID, and it follows that R' is a field if and only if (x^2+1) is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$. Thus, since R' is a field, (x^2+1) is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$. ■

Lemma 6.100. *Let p be an odd prime, and let $\overline{a}$ denote the residue of an integer a modulo p.*

1. *The integer a solves the congruence relation $x^2 \equiv -1 \mod p$ if and only if its residue $\overline{a}$ is an element of order 4 in the multiplicative group of the field $\mathbb{Z}/p\mathbb{Z}$.*
2. *The multiplicative group $\mathbb{Z}/p\mathbb{Z}^\times$ contains an element of order 4 if and only if $p \equiv 1 \mod 4$.*

Proof. There is exactly one element of order 2 in $\mathbb{Z}/p\mathbb{Z}^\times$ - namely, the residue of -1. If a residue $\overline{a}$ has order 4 in $\mathbb{Z}/p\mathbb{Z}^{times}$, then $\overline{a}^2$ has order 2; hence, $\overline{a}^2 = -1$, which means $a^2 \equiv -1 \mod p$. Conversely, if $a^2 \equiv -1 \mod p$, then $\overline{a}$ has order 4 in $\mathbb{Z}/p\mathbb{Z}^\times$.

Now the order of the group $\mathbb{Z}/p\mathbb{Z}^\times$ is $p-1$. Hence, if this group has an element of order four, $p-1$ is divisible by 4, so $p \equiv 1 \mod 4$. Conversely, suppose $p-1$ is divisible by 4, and let H be a Sylow 2-subgroup of $\mathbb{Z}/p\mathbb{Z}^\times$, whose order is the largest power 2^r of 2 which divides $p-1$. Since 4 divides $p-1$, the order of H is at least 4, so there is an element $\overline{a}$ in H different from ± 1. This element does not have order 2 nor order 1. But, since H is a 2-group, the order of $\overline{a}$ is a power of 2. Thus, some power of $\overline{a}$ has order exactly 4, completing the proof. ■

6.5.2 Lecture

Recall. The ring of Gaussian Integers, $R = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, with the size function $\delta = |\cdot|^2$ is a Euclidean domain, so if you have gaussian integers α, β, $\alpha \neq 0$, we can write $\beta = q\alpha + r$ with $\delta(r) < \delta(\alpha)$. From this we find that every ideal $I \subset \mathbb{Z}[i]$ is principal, so $I = (\alpha)$ with $\delta(\alpha)$ minimal. Also, if $I \neq (0)$, then $\mathbb{Z}[i]/I$ is a finite ring, so I has finite index in R.

Proof. Suppose $\alpha \neq 0$ is in I. Then $\alpha\overline{\alpha} = a^2 + b^2 = n > 0$, so $n \in I$ since $\alpha \in I$ and $\overline{\alpha} \in R$. Therefore, $R \supset I \supset (n)$, and I claim the index of (n) in R is finite, and in particular it is n^2. This follows from the fact that $(n) = \{na + nbi : a, b \in \mathbb{Z}\}$, so $R/(n) = \{a + bi : 0 \leq a < n, 0 \leq b < n\}$. Therefore, there are n^2 cosets, since there are n choices for a and n choices for b. Note that $[R : (n)] = [R : I][I : (n)]$, so the index of I must also be finite. ■

Corollary 6.101. *In fact, if $I = (\alpha)$, then $[R : I] = \delta(\alpha) = a^2 + b^2$.*

Proof. Right $\alpha \in \mathbb{Z}[i]$ as $\alpha = re^{i\theta}$, and note that $\delta(\alpha) = r^2$. Note that $\mathbb{Z}[i]$ forms a square lattice in the complex plane. We wish to know what subset of these points is $\alpha R = \{\alpha a + \alpha bi\}$. Hence, α and αi generate R, and note that they are perpendicular so we will obtain a rectangular lattice rotated by θ and scaled by r. Note that when you scale a lattice by a factor, the sublattice you get has index that factor squared. We can also argue by volumes (2-dimensional volumes) and how these volumes are scaled. Hence, this scaled lattice by r has index r^2. ■

Remark 6.102. We can see this works when $\alpha = n \in \mathbb{Z}$.

Proposition 6.103. *R has unique factorization into primes. That is, an arbitrary gaussian number can be written as a unit and prime gaussian numbers, $\alpha = u \cdot p_1 ... p_k$, where u is a unit, and p_i are gaussian primes. Recall that if p is prime in R, then (p) is maximal with respect to principal ideals, but since in this case R is a PID, (p) is a maximal ideal, or equivalently $R/(p) =$ a field. Moreover, since the quotient is finite $R/(p)$ is a finite field.*

Recall. In the theory for $\mathbb{Z}$, we now that the units were $\mathbb{Z}^* = \{\pm 1\}$, and the primes are $2, 3, 5, 7, 11, 13, 17, ...$, so we have a way for describing them. Additionally, if $R = F[x]$, then the units are $R^* = F^*$ the constant nonzero polynomials, a primes $p(x) =$ the irreducible monic polynomials over F. For $F = \mathbb{C}$, $p(x) = x - \alpha$ with $\alpha \in \mathbb{C}$ (by Fundamental Theorem of Algebra). For $F = \mathbb{R}$, $p(x) = x - c$ or $x^2 - rx + s$, where $c, r, s \in \mathbb{R}$ and $r^2 - 4s < 0$.

We will now describe the primes and unites in $\mathbb{C}$

Observation 6.104. We have $\delta : R \to \mathbb{Z}_{\geq 0}$ which takes $\alpha \mapsto \alpha\overline{\alpha}$. Note that δ is not a ring homomorphism. Nonetheless, we have the nice property $\delta(\alpha\beta) = \delta(\alpha)\delta(\beta)$ and $\delta(1) = 1$.

Proposition 6.105. *α is a unit if and only if $\delta(\alpha) = 1$.*

Proof. If $\delta(\alpha) = 1$, then $\overline{\alpha}$ is a multiplicative inverse of α, so α is a unit. Now, suppose α is a unit so we have $\beta \in R$ so that $\alpha\beta = 1$. Then $\delta(\alpha)\delta(\beta) = \delta(1) = 1$, where $\delta(\alpha)$ and $\delta(\beta)$ are positive integers. Hence, $\delta(\alpha) = \delta(\beta) = 1$. Moreover, this occurs when $a^2 + b^2 = 1$, where $a, b \in \mathbb{Z}$, so $a = \pm 1$ and $b = 0$, or $a = 0$ and $b = \pm 1$. Therefore, α can be $1, -1, i, -i$ only. ■

Remark 6.106. Hence, $R^\times = \langle 1, -1, i, -i \rangle$ is cyclic of order four.

Question. What are the primes π of R?

Remark 6.107. We know that $R/(\pi)$ is a finite field, so $|R/(\pi)| = p^f$ for some prime $p \in \mathbb{Z}$ and $f \geq 1$. This occurs from the fact that the vector space $(\mathbb{Z}/p\mathbb{Z})^f$ is additionally a field (though multiplication can be complicated). We arrived at $\mathbb{Z}/p\mathbb{Z}$ from the canonical map $\mathbb{Z} \to R'$ which determines the characteristic of the ring R', and is defined by $1 \mapsto 1_r$. This map has a kernel (since R' is finite by assumption) which is an ideal $I = (n)$ of $\mathbb{Z}$, and by the first isomorphism theorem $\mathbb{Z}/(n)$ is isomorphic to the image of the map, which is a subring of R'. But, if n is not a prime, then $\mathbb{Z}/(n)$ has zero divisors (i.e. it is not an integral domain), which would imply R' has zero divisors. Thus, if we want R' to be a finite field, since fields are integral domains we must have that n is a prime p. This homomorphism gives R' the structure of a vector space over the field $\mathbb{Z}/p\mathbb{Z}$, with finite dimension f.

Proposition 6.108. *In fact, $R/(\pi)$ has order p or p^2 since p is in the kernel of the canonical map, so multiplication by p is zero. This implies that $p \in (\pi)$, so $p = \alpha\pi$ in R for some $\alpha \in R$. So, $(pR) \subset (\pi R) \subset R$, and we now that $[R : (\pi R)][(\pi R) : (pR)] = [R : (pR)] = p^2 = \delta(p)$, so $[R : (\pi R)]$ must divide p^2 in $\mathbb{Z}$. Moreover, since $(\pi R) \neq R$, $[R : (\pi R)]$ is either p or p^2.*

Remark 6.109. This is analogous to the fact that $|\mathbb{Z}/(p)| = p$.

Proposition 6.110 (Cases)**.** *We have two cases:*

1. *$R/(\pi)$ has order p^2. Then $(\pi) = (p)$, so $\pi = up$, where u is a unit, so they are associates and p is a prime in R, and R/p is a field of order p^2.*
2. *$R/(p)$ is not a field, so there are non-trivial ideals (π) between (p) and R, and these are generated by primes with $R/(\pi) \cong \mathbb{Z}/p\mathbb{Z}$.*

Remark 6.111. To each prime π in $\mathbb{Z}[i]$ we can associate a rational prime p in $\mathbb{Z}$, and every rational prime occurs (might not be one-to-one).

Remark 6.112 (Study the Finite Ring $R/(p)$ for a Rational Prime p). Note that $R/(p) = \mathbb{Z}[i]/(p) = (\mathbb{Z}[x]/(x^2+1)/(p) = \mathbb{Z}[x]/(x^2+1, p) = (\mathbb{Z}[x]/(p))/(x^2+1) = (\mathbb{Z}/p\mathbb{Z}[x])/(x^2+1)$ which is a field precisely when x^2+1 is irreducible over $\mathbb{Z}/p\mathbb{Z}$. Therefore, we are in case 1 precisely when x^2+1 is irreducible, and we are in case 2 precisely when x^2+1 is reducible over $\mathbb{Z}/p\mathbb{Z}$. Since x^2+1 is a polynomial of degree 2, it is irreducible provided that it has no roots in $\mathbb{Z}/p\mathbb{Z}$. That is, we cannot solve $x^2 \cong -1 \mod p$ in $\mathbb{Z}/p\mathbb{Z}$.

> [Case 1] First take $p = 2$. Then $x^2 + 1 \cong (x+1)^2 \mod 2$. Thus, the polynomial is reducible with a unique root $x \cong -1 \cong 1 \mod 2$. In this case $R/(p)$ is not a field, but there is a unique prime $\pi = 1 + i$ with $R \supset (\pi) \supset (2)$ and $[R : (\pi)] = 2$, since $\delta(\pi) = 2 = a^2 + b^2$, so a and b must be ± 1, and hence we have for solutions which are in fact associates, so we obtain one ideal.

[Case 2] If $p \cong 3 \mod 4$ then $|(\mathbb{Z}/p\mathbb{Z})^*| = p-1 = 2*$odd number. Note that the x we are looking for would be invertible mod p and have order 4 in $(\mathbb{Z}/p\mathbb{Z})^*$. But, since the order of $(\mathbb{Z}/p\mathbb{Z})^*$ is two times an odd, the order of the Sylow 2-subgroup is 2, so $(\mathbb{Z}/p\mathbb{Z})^*$ has no elements of order 4. Thus, x^2+1 is irreducible modulo p and $R/(p)$ is a field. Thus, (p) is prime in this case.

[Case 3] If $p \cong 1 \mod 4$ then $x^2+1 \cong (x-a)(x+a)$ where $a^2 \cong -1 \mod p$. Namely, we can find an element of order four. In this case $|(\mathbb{Z}/p\mathbb{Z})^*| = p-1 = 2^k*$odd number, where $k \geq 2$. Consequently, the Sylow 2-subgroup is of order 2^k, $k \geq 2$. But, the only elements of order 2 are $\pm 1 \mod p$, since if $p \mid a^2-1 = (a-1)(a+1)$, a must be $\pm 1 \mod p$. Therefore, the Sylow 2-subgroup has elements of order greater than 2. Moreover, if we have such an element of order greater than 2, we can take a power of it to obtain an element of order 4, so there must exist elements a of order 4 which factors x^2+1. Additionally, $(x-a)$ corresponds to an ideal $\pi = (p, i-a)$ and $(x+a)$ corresponds to an ideal $\pi' = (p, i+a)$, which are both primes in R with $R/(\pi) \cong \mathbb{Z}/p\mathbb{Z}$ and $R/(\pi') \cong \mathbb{Z}/p\mathbb{Z}$.

Observation 6.113. Consider the sum

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \frac{1}{13} - ... = \frac{\pi}{4} \tag{6.17}$$

This is a theorem which says that every ideal in the gaussian numbers is principal.

6.6 Algebraic Integers

6.6.1 Textbook

Example 6.114 (Motivation)**.** Euler proved that the Fermat Equation $x^3+y^3=z^3$ has no integer solutions. To prove this we may take $x^3 = z^3 - x^3$ and factor to obtain

$$x^3 = (z-y)(z-\xi y)(z-\bar{\xi} y) \tag{6.18}$$

where $\xi = e^{2\pi i/3}$, and then we analyze the equation using the arithmetic in the ring $\mathbb{Z}[\xi]$, which is in fact a Euclidean domain. Problems of this type which ask for integer solutions of polynomial equation are called **Diophantine problems**

Definition 6.115 (Algebraic Integers)**.** A complex number α is called **algebraic** if it is the root of a nonzero polynomial $f(x)$ with rational coefficients. Since we can clear denominators in $f(x)$, α is also the root of an integer polynomial. α is called a **algebraic integer** if it is the root of a monic polynomial with integer coefficients, a polynomial of the form

$$f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0, a_i \in \mathbb{Z} \tag{6.19}$$

Remark 6.116. Let α be an algebraic number. Then the set of all polynomials in $\mathbb{Q}[x]$ which have α as a root is the kernel of the substitution $\mathbb{Q}[x] \to \mathbb{C}, f(x) \mapsto f(\alpha)$. Thus, it is a principal ideal generated by an irreducible element $f(x)$ of the polynomial ring which is called the **irreducible polynomial for α over $\mathbb{Q}$**. The degree of $f(x)$ is called the **degree of α over $\mathbb{Q}$**.

Proposition 6.117. *The kernel of the map $\mathbb{Z}[x] \to \mathbb{C}$, $x \mapsto \alpha$, is the principal ideal of $\mathbb{Z}[x]$ generated by the primitive irreducible polynomial for α.*

Proof. Let $f(x)$ be a primitive irreducible polynomial for α. If $g \in \mathbb{Z}[x]$ has α as a root, then f divides g in $\mathbb{Q}[x]$, and hence f divides g in $\mathbb{Z}[x]$ too. Thus, g is in the principal ideal of $\mathbb{Z}[x]$ generated by f. ■

Proposition 6.118. *An algebraic number α is an algebraic integer if and only if the primitive irreducible polynomial for α is monic. Equivalently, α is an algebraic integer if and only if the monic irreducible polynomial for α in $\mathbb{Q}[x]$ has integer coefficients.*

Corollary 6.119. *A rational number r is an algebraic integer if and only if it is an ordinary integer.*

Remark 6.120 (Motivation). We can think of the leading coefficient of the primitive irreducible polynomials $f(x)$ for α as a "denominator." If α is a root of an integer polynomial $f(x) = dx^n + a_{n-1}x^{n-1} + ... + a_0$, then $d\alpha$ is an algebraic integer, because it is a root of the monic integer polynomial

$$x^n + a_{n-1}x^{n-1} + da_{n-2}x^{n-2} + ... + d^{n-2}a_1x + d^{n-1}a_0 \tag{6.20}$$

Proposition 6.121. *The set of algebraic integers form a subring for $\mathbb{C}$.*

Definition 6.122 (Quadratic Number Field)**.** A **quadratic number field** $F = \mathbb{Q}[\sqrt{d}]$ consists of all complex numbers of the form

$$a + b\sqrt{d}, a, b \in \mathbb{Q} \tag{6.21}$$

where d is a fixed integer, which is not a rational square. Since we can pull out square factors of d, it is customary to assume that d is **square free**.

The field F is called a **real quadratic number field** if $d > 0$, or an **imaginary quadratic number field** if $d < 0$.

Corollary 6.123. *$\alpha = a + b\sqrt{d}$ is an algebraic integer if and only if $2a$ and $a^2 - b^2 d$ are integers (proven by considering its "$\sqrt{d}$ conjugate").*

Proposition 6.124. *The algebraic integers in the quadratic field $F = \mathbb{Q}[\sqrt{d}]$ have the form $\alpha = a + b\sqrt{d}$, where*

1. *If $d \equiv 2$ or $3 \mod 4$, then a and b integers.*
2. *If $d \equiv 1 \mod 4$, then either $a, b \in \mathbb{Z}$ or $a, b \in \mathbb{Z} + \frac{1}{2}$*

Proposition 6.125. *Assume that $d \equiv 1 \mod 4$. Then the algebraic integers in $F = \mathbb{Q}[\sqrt{d}]$ are $a + b\nu$, where $a, b \in \mathbb{Z}$ and $\nu = \frac{1}{2}(1 + \sqrt{d})$, where ν is obtained as a root of the quadratic polynomial $x^2 - x + \frac{1}{4}(1 - d)$.*

Remark 6.126. From these propositions it can be seen that the algebraic integers in F form a ring R called the **ring of integers** in F. The **discriminant** of F is defined to be the discriminant of $x^2 - d$ if $R = \mathbb{Z}[\sqrt{d}]$, and the discriminant of $x^2 - x + \frac{1}{4}(1 - d)$ if $R = \mathbb{Z}[\nu]$. This discriminant is denoted by D, so

$$D = \begin{cases} 4d & if\ d \equiv 2, 3 \\ d & if\ d \equiv 1 \end{cases} \mod 4 \tag{6.22}$$

Remark 6.127. In the case of $d < 0$, if $D = 4d$ the ring R forms a lattice in the complex plane which is rectangular, and if $D = d$ then the lattice is in the form of "isosceles triangles."

6.6.2 Lecture

Definition 6.128 (Algebraic Integer)**.** A complex number $\alpha \in \mathbb{C}$ is said to be an **algebraic integer** if α is the root of a monic polynomial $f(x) \in \mathbb{Z}[x]$

$$f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 \tag{6.23}$$

Example 6.129. Every integer $n \in \mathbb{Z}$ is an algebraic integer since it is the root of $f(x) = x - n$. $\sqrt{d}$ for $d \in \mathbb{Z}$ is an algebraic integer since it's the root of the polynomial $f(x) = x^2 - d$. Another example is $\alpha = \frac{-1 \pm \sqrt{-3}}{2}$ which is the root of $f(x) = x^2 + x + 1$.

Question. Suppose α satisfies $f(x)$ with rational coefficients, where $f(x)$ is monic and irreducible. Is α an algebraic integer?

Answer. α is an algebraic integer $\iff$ the monic irreducible $f(x)$ with rational coefficients satisfied by α has integral coefficients.

Proof. Let $f_0(x)$ be the primitive polynomial over $\mathbb{Z}$ with $f(x) = c \cdot f_0(x)$, with c being the content in $\mathbb{Q}$. Then $f_0(\alpha) = 0$. I claim any $g(x) \in \mathbb{Z}[x]$ with $g(\alpha) = 0$ has the form $g(x) = f_0(x)q(x)$, where $q(x) \in \mathbb{Z}[x]$. We know that $g(x) = f_0(x)q(x)$ where $q(x)$ has rational coefficients as $(f) = (f_0)$ is the full ideal of polynomials in $\mathbb{Q}[x]$ vanishing at α. Then, write $q(x) = dq_0(x)$ where q_0 is primitive. Then $g(x) = d(f_0q_0)$, where f_0q_0 is primitive by Gauss's Lemma, so since $g(x) \in \mathbb{Z}[x]$, it must be that $d \in \mathbb{Z}$, which implies that $q(x) \in \mathbb{Z}[x]$. Therefore, every $g(x) \in \mathbb{Z}[x]$ which α satisfies is divided by $f_0(x)$ in $\mathbb{Z}[x]$. Therefore, if $f_0(x) \neq f(x)$, then $f_0(x)$ is not monic, so in particular any integer polynomial multiple of $f_0(x)$ is not monic so $g(x)$ is not monic. Therefore, α would not be an algebraic integer. ■

Example 6.130. $\frac{1}{2}$ is not an algebraic integer since it satisfies $x - \frac{1}{2} = f(x)$ which is a monic irreducible polynomial with rational coefficients. In particular any $\alpha \in \mathbb{Q}$ with $\alpha \notin \mathbb{Z}$ is *not* and algebraic integer. Another non-example is $\alpha = \frac{\sqrt{2}}{3}$ since it satisfies $x^2 - \frac{2}{9} = 0$.

Example 6.131 (Application)**.** Let's determina all algebraic integers in the field $\mathbb{Q}[x]/(x^2 - d) = \mathbb{Q}(\sqrt{d}) = \mathbb{Q} + \mathbb{Q}\sqrt{d}$, with $d \in \mathbb{Z}$ and d is square free so $d = \pm p_1 ... p_k$, with $p_i \neq p_j$ whenever $i \neq j$. We know that every element of $\mathbb{Z} + \mathbb{Z}\sqrt{d}$ is an algebraic integer. Sometimes we will get more.

Proof. Consider $a + b\sqrt{d} = \alpha$. Then α satisfies the quadratic polynomial $(x - \alpha)(x - \alpha')$, where $\alpha' = a - b\sqrt{d}$. Then, observe that

$$(x - \alpha)(x - \alpha') = x^2 - 2ax + (a^2 - db^2) \tag{6.24}$$

which is a monic quadratic polynomial with rational coefficients, and it is irreducible if $b \neq 0$. Any element $\alpha \in \mathbb{Q}(\sqrt{d})$ satisfies this monic polynomial with rational coefficients. If $\alpha \in \mathbb{Z} + \mathbb{Z}\sqrt{d}$, then it satisfies a polynomial with integer coefficients. Moreover, for $b \neq 0$, α is an algebraic integer $\iff$ $2a$ is an integer and $a^2 - db^2$ is an integer. If $b = 0$, then $\alpha = a$ is an algebraic integer $\iff$ $a \in \mathbb{Z}$. In general, α is an algebraic integer in $\mathbb{Q}(\sqrt{d})$ $\iff$ $2a$ is an integer and $a^2 - db^2$ is an integer. ■

Remark 6.132. We have two cases

1. a is an integer. Since $a^2 - b^2d$ is an integer, then b^2d must be an integer. In particular, since d is square free, b^2 must be an integer, so b is an integer.
2. a is in $\frac{1}{2}\mathbb{Z} - \mathbb{Z}$, i.e $2a$ is an odd integer. Write $2a = m$. Then $a^2 = \frac{1}{4}m^2$, so $4a^2 = m^2$ is an integer, so $4db^2$ is an integer, so $db^2 = \frac{1}{4}n$, with n being odd. This implies that $b = \frac{1}{2}n_0$, with n_0 an odd integer. Then, recall that

$$a^2 - db^2 = \frac{1}{4}m^2 - d\frac{1}{4}n_0^2 = \frac{1}{4}(m^2 - dn_0^2) \tag{6.25}$$

must be an integer, so $m^2 - dn_0^2 \equiv 0 \mod 4$. Moreover, since m and n_0 are odd, $m^2, n_0^2 \equiv 1 \mod 4$, so $d \equiv 1 \mod 4$. Then, $a = \frac{1}{2}m$ and $b = \frac{1}{2}n_0$ works.

Corollary 6.133 (Summary)**.** *d is a square free integer.*

1. *If $d \equiv 2, 3 \mod 4$, then the algebraic integers in $\mathbb{Q}(\sqrt{d})$ form the ring $R = \mathbb{Z} + \mathbb{Z}\sqrt{d}$*
2. *If $d \equiv 1 \mod 4$, then the algebraic integers in $\mathbb{Q}(\sqrt{d})$ form the larger ring $R = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right) \supset \mathbb{Z} + \mathbb{Z}\sqrt{d}$.*

Definition 6.134 (Discriminant)**.** The polynomial satisfied by $\sqrt{d}$ is $x^2 - d$. Its discriminant is $D = 4d$. The polynomial satisfied by $\frac{1+\sqrt{d}}{2}$ is $x^2 - x + \frac{1-d}{4}$, where $\frac{1-d}{4}$ since $d \equiv 1 \mod 4$. Its discriminant is $1 - (1 - d) = d = D$. We shall use the index D to index these rings.

Proposition 6.135. *D has the following property:*

1. *$D \equiv 0, 1 \mod 4$.*
2. *D is as square free as possible, given condition* (1)*.*

Example 6.136. If $D < 0$ we say R is an imaginary quadratic ring, and if $D > 0$ then R is a real quadratic ring. Let us list the possible D's

1. $D < 0$: $-3, -4, -7, -8, -11, -15, -19, -20, -23, ...$ (-4 is the Gaussian integers)
2. $D > 0$: $5, 8, 12, 13, 17, 21, 24, 28, 29, ...$

For every one of these numbers we get a ring.

Question (Question Gauss Asked). Which of these rings have the property that every ideal is principal? (PIDs) For $D < 0$, Gauss said that $-3, -4, -7, -8, -11, -19, -43, -67$, and -163 are the only rings that are PIDs (this has been shown). For $D > 0$ Gauss said that there are an infinite number (this has yet to be proven or disproven).

Remark 6.137. We shall focus on the imaginary quadratic rings. If $D < 0$, the unit group $R^\times$ is finite cyclic group, and if $D = -3$ it has order 6, if $D = -4$ it has order 4, and if $D < -4$, it has order 2, $R^\times = \mathbb{Z}^\times = \{\pm 1\}$. However, in the real quadratic case $R^\times$ is an infinite group always, so it is much more difficult to deal with.

6.7 Factorization in Imaginary Quadratic Fields

Definition 6.138 (Norm)**.** Let R be the ring of integers of an imaginary quadratic field $F = \mathbb{Q}[\delta]$. If $\alpha = a + b\delta$ is in R, so is its complex conjugate $\overline{\alpha} = a - b\delta$. We call the **norm** of α

$$N(\alpha) = \alpha\overline{\alpha} \tag{6.26}$$

It is also equal to $a^2 - b^2 d$, and it is the constant term of the irreducible polynomial for α over $\mathbb{Q}$. Thus $N(\alpha)$ is positive unless $\alpha = 0$. Note that

$$N(\beta\gamma) = N(\beta)N(\gamma) \tag{6.27}$$

Proposition 6.139. .

1. *An element α of R is a unit if and only if $N(\alpha) = 1$*
2. *The units of R are $\{\pm 1\}$ unless $d = -1$ or -3. If $d = -1$, so that R is the ring of Gauss integers, the units are $\{\pm 1, \pm i\}$, and if $d = -3$ they are the powers of the 6th root of unity $\frac{1}{2}(1 + \sqrt{-3})$.*

Proof. If α is a unit, then $N(\alpha)N(\alpha^{-1}) = N(1) = 1$. Since $N(\alpha)$ and $N(\alpha^{-1}$ are positive integers they are both equal to one. Conversely, if $N(\alpha) = \alpha\overline{\alpha} = 1$, then $\overline{\alpha} = \alpha^{-1}$. Thus, $\alpha^{-1} \in R$, and α is a unit. Thus, α is a unit if and only if it lies in the unit circles of the plane. The second assertion follows from the configuration of the lattice R. ■

Proposition 6.140. *Existence of factorization is true in R.*

Proof. If $\alpha = \beta\gamma$ is a proper factorization in R, then β, γ aren't units. Hence, by the previous proposition, $N(\alpha) = N(\beta)N(\gamma)$ is a proper factorization in the ring of integers. The existence of factorization in R follows from the existence of factorization in $\mathbb{Z}$. ■

Remark 6.141. Factorization into irreducible elements will not be unique in most cases.

Proposition 6.142. *The only ring R with $d \equiv 3 \mod 4$ which is a UFD is the ring of Gauss integers.*

Proof. Assume that $d \equiv 3 \mod 4$, but $d \neq -1$. Then

$$1 - d = 2\left(\frac{1-d}{2}\right), \text{ and } 1 - d = (1 + \sqrt{-d})(1 - \sqrt{-d}) \tag{6.28}$$

There are two factorizations of $1 - d$ in R. The element 2 is irreducible because $N(2) = 4$ is the smallest value > 1 taken on by $N(\alpha)$. Thus, if there were a common refinement of the above factorization, 2 would divide either $1 + \delta$ or $1 - \delta$ in R, which is does not: $\frac{1}{2} \pm \frac{1}{2}\delta$ is not in R when $d \equiv 3 \mod 4$. ■

Theorem 6.143. *Let R be the ring of integers in the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$. Then R is a UFD if and only if d is one of the integers $-1, -2, -3, -7, -11, -19, -43, -67, -163$.*

Remark 6.144. Every non-principal ideal of R is a sublattice of R. However, not every sublattice is an ideal.

Proposition 6.145. *If $d \equiv 2$ or $3 \mod 4$, the nonzero ideals of R are sublattices which are closed under multiplication by $\sqrt{d}$. If $d \equiv 1 \mod 4$, they are sublattices which are closed under multiplication by $\frac{1}{2}(1+\sqrt{d})$.*

Proof. To be an ideal, a subset A must be closed under addition and under multiplication by elements of R. Any lattice is closed under addition and under multiplication by integers. Hence, if it is also closed under multiplication by $\sqrt{d}$, then it is also closed under multiplication by an element of the form $a + b\sqrt{d}$, with $a, b \in \mathbb{Z}$. This includes all elements of R if $d \equiv 2$ or $3 \mod 4$. ■

Theorem 6.146. *Let $R = \mathbb{Z}[\sqrt{-5}]$, and let A be a nonzero ideal of R. Let α be a nonzero element of A of minimal absolute value $|\alpha|$. There are two cases:*

1. *A is a principal ideal (α), which has the lattice basis $(\alpha, \alpha\delta)$,*
2. *A has a lattice basis $(\alpha, \frac{1}{2}(\alpha + \alpha\delta))$, and is not a principal ideal.*

Definition 6.147 (Similarity)**.** The similarity classes of ideals are called the **ideal classes**, and their number is called the **class number** of R (classes of ideals with similar lattice structure)

Lemma 6.148. *Let r be the minimum absolute value among nonzero element of a lattice A, and let γ be an element of A. Let D be the disc of radius $\frac{1}{n}r$ about the point $\frac{1}{n}\gamma$. There is no point of A in the interior of D other than its center $\frac{1}{n}\gamma$. The center may or may not lie in A.*

Proof. Let $|beta$ be a point in the interior of D. Then by definition of the disc, $|\beta - \frac{1}{n}\gamma| < \frac{1}{n}r$, or equivalently, $|n\beta - \gamma| < r$. If $\beta \in A$, then $n\beta - \gamma \in A$ too. In this case , $n\beta - \gamma$ is an element of A of absolute value less than r, which implies that $n\beta - \gamma = 0$, hence that $\beta = \frac{1}{n}\gamma$. ■

6.7.1 Lecture

Recall. The primes in $\mathbb{Z}[i]$ associated well with number theory in $\mathbb{Z}$, with the fact that if $p \in \mathbb{Z}$ is prime then

1. if $p \equiv 1 \mod 4$ it gives rise to two primes π and π', $\pi\pi' = p$. This is the statement that if $\pi = a + bi$, then $a^2 + b^2 = p$, proving Fermat's theorem.
2. if $p \equiv 3 \mod 4$, it gives rise to one prime π which is an associate of p.

Remark 6.149. We will now consider rings R analogous to $\mathbb{Z}[i]$. For example, we have $R = \mathbb{Z}[\sqrt{-2}]$, which is also Euclidean, and $R = \mathbb{Z}[\sqrt{-5}]$ which doesn't even have unique factorization $(2 * 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}))$.

Question. What about rings of the form $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\} = \mathbb{Z}[x]/(x^2 - d)$, where $d \neq$ a square if we want $x^2 - d$ to be irreducible in $\mathbb{Z}$?

Answer. This is not quite the right analog we want. For example, consider $f(x) = x^2 + x + 1$. Then its roots are $\alpha = \frac{-1 \pm \sqrt{-3}}{2}$. If we took $R = \mathbb{Z}[x]/(f(x))$, which is a monic irreducible polynomial of degree 2 in $\mathbb{Z}$, and in particular this ring is $R = \mathbb{Z} + \mathbb{Z}\alpha \supset \mathbb{Z} + \mathbb{Z}\sqrt{-3} = R'$ since $2\alpha + 1 = \pm\sqrt{-3}$, and R' has index 2 in R. Moreover, both are integral domains, with field of fractions $\mathbb{Q}(\sqrt{-3})$. Thus, sometimes we can enlarge $\mathbb{Z}[\sqrt{d}]$ in its field of fractions.

Recall. The set of all algebraic integers in the field $\mathbb{Q}(\sqrt{d})$, where d is a square free integer is

$$R = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d} & d \equiv 2, 3 \mod 4 \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right) & d \equiv 1 \mod 4 \end{cases} \tag{6.29}$$

which is a ring. In other words, the things in R are of the form $a + b\sqrt{d}$ where $a, b \in \mathbb{Z}$ or $a, b \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$ when $d \equiv 1 \mod 4$.

Recall. We index R by the discriminant D such that

$$D = \begin{cases} 4d & d \equiv 2, 3 \mod 4 \\ d & d \equiv 1 \mod 4 \end{cases} \tag{6.30}$$

Then, we can write $R_D = \mathbb{Z} + \mathbb{Z}\left(\frac{D+\sqrt{D}}{2}\right)$ as the ring of algebraic integers.

Definition 6.150. When $D < 0$, we have what is called an **imaginary quadratic ring**.

Observation 6.151. We have the map $\delta = N : R \to \mathbb{Z}$, which is called a norm, and which takes $N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$. This map has the nice multiplicative property

$$N(\alpha\beta) = N(\alpha)N(\beta) \tag{6.31}$$

Additionally, for $d < 0$, this norm is nonnegative.

Proposition 6.152. *α is a unit in $R \iff N(\alpha) = \pm 1$ is a unit in $\mathbb{Z}$.*

Proof. If α is a unit, there exists $\beta \in R$ such that $\alpha\beta = 1$. Then $N(\alpha\beta) = N(\alpha)N(\beta)) = N(1) = 1$, where $N(\alpha)$ and $N(\beta)$ are integers, so they must be ± 1. Conversely, if $N(\alpha) = \alpha\alpha' = \pm 1$, then $\pm\alpha'$ is an inverse of α, so α is a unit. ■

Corollary 6.153. *If $D < 0$ then α is a unit if and only if $N(\alpha) = +1$. In fact, if $D = -3$ there are 6 units, if $D = -4$ there are 4 units, and if $D < -4$ there are 2 units $R^\times = \{\pm 1\}$.*

Proof. A unit $\alpha = a + b\sqrt{d}$ is a solution to $a^2 - b^2 d = 1$, where $a, b \in \mathbb{Z}$ or $a, b \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$. If $b = 0$, then $a^2 = 1$ so $a = \pm 1$. If $b \neq 0$, then $-b^2 d \geq -\frac{d}{4}$. If $-d > 4$, then $a^2 - b^2 d > 1$, so it's hopeless. ■

Proposition 6.154. *If $D > 0$, $R^\times$ is infinite.*

Example 6.155. $D = 5$, so $R = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right)$, and let $\alpha = \frac{1+\sqrt{5}}{2}$. Note that $\alpha\alpha' = \frac{1^2-5}{4} = -1$, so α is a unit with inverse $-\alpha'$. Then, $\alpha^2 = \frac{3+\sqrt{5}}{2}$, and since the norm is multiplicative, $N(\alpha^2) = +1$. In particular, all powers of α are distinct units of the ring.

6.8 Ideal Factorization

6.8.1 Textbook

Let R be the ring of algebraic integers in an imaginary quadratic field. We shall denote elements of R by $\alpha, \beta, ...$, and elements of $\mathbb{Z}$ by $a, b, ...$

Notation 6.156. The notation $A = (\alpha, \beta, ..., \gamma)$ denotes the ideal generated by $\alpha, \beta, ...\gamma$. Since an ideal of R is a plane lattice, it has a lattice basis consisting of two elements.

Definition 6.157 (Ideal Multiplication)**.** Dedikend extended the notion of divisibility to ideals with this definition of ideal multiplication. Let A and B be ideals in a ring R. We define the **product ideal** AB as the set of all finite sums of products

$$\sum_i \alpha_i \beta_i, \quad \text{where } \alpha_i \in A, \beta_i \in B \tag{6.32}$$

This set of sums is the smallest ideal of R which contains all products $\alpha\beta$.

Observation 6.158. We observe that ideal multiplication defined in this way is associative and commutive since R is a commutative ring, and R is a unit element.

$$AR = RA = A, AB = BA, A(BC) = (AB)C \tag{6.33}$$

Proposition 6.159. .

1. *The product of principal ideals is principal: If $A = (\alpha)$ and $B = (\beta)$, then $AB = (\alpha\beta)$.*
2. *Assume that $A = (\alpha)$ is principal, but let B be arbitrary. Then*

$$AB = \alpha B = \{\alpha\beta : \beta \in B\} \tag{6.34}$$

3. *Let $\alpha_1, ..., \alpha_m$ and $\beta_1, ..., \beta_n$ be generators for the ideals A and B respectively. Then AB is generated as an ideal by the mn products $\alpha_i\beta_j$*

Proposition 1. Suppose $A = (\alpha)$ and $B = (\beta)$ are principal ideals. First, suppose that $\alpha\beta \in AB$, so $(\alpha\beta) \subset AB$. Now, take $\sum_i \alpha_i\beta_i \in AB$. Since $A = (\alpha)$ and $B = (\beta)$, for each i we have that $\alpha_i = \alpha r_i$ and $\beta_i = \beta r_i'$ where $r_i, r_i' \in R$. Then

$$\sum_i \alpha_i\beta_i = \sum_i \alpha\beta r_i r_i' = \alpha\beta\left(\sum_i r_i r_i'\right) \in (\alpha\beta) \tag{6.35}$$

Therefore, we find that $AB = (\alpha\beta)$

[Proposition 2] If $A = (\alpha)$ and B is an arbitrary ideal, then $AB \supset \{\alpha\beta : \beta \in B\}$ and from a similar argument to that in proposition 1, $AB \subset= \{\alpha\beta : \beta \in B\}$, so we conclude that $AB = \{\alpha\beta : \beta \in B\}$.

[Proposition 3] (Later) ■

Definition 6.160 (Division)**.** We say that an ideal A **divides** another ideal B if there is an ideal C so that $B = AC$.

We will now prove unique factorization of ideals in the rings of algebraic integers in imaginary quadratic number fields

Proposition 6.161. *Let P be an ideal of a ring R which is not the unit ideal. The following conditions are equivalent*

1. *If α, β are elements of R such that $\alpha\beta \in P$, then $\alpha \in P$ or $\beta \in P$*
2. *If A, B are ideals of R such that $AB \subset P$, then $A \subset P$ or $B \subset P$*
3. *The quotient ring R/P is an integral domain.*

An ideal which satisfies one of these conditions is called ***prime****.*

Proof. The condition for $\overline{R} = R/P$ to be an integral domain are that $\overline{R} \neq 0$, and that $\overline{\alpha\beta} = 0$ implies $\overline{\alpha} = 0$ or $\overline{\beta} = 0$. These conditions translate to $P \neq R$ and if $\alpha\beta \in P$ then $\alpha \in P$ or $\beta \in P$. Thus, (1) and (3) are equivalent. The fact that (2) implies (1) is seen by taking $A = (\alpha)$ and $B = (\beta)$. Now we must show the converse, so suppose (1) holds and let A, B be ideals such that $AB \subset P$. If A is not contained in P, there is some element $\alpha \in A$ which is not in P. If β is an element of B, then $\alpha\beta \in AB$; hence $\alpha\beta \in P$ and by part (1) $\beta \in P$. Then, since this is true for all β, $B \subset P$ as required. ■

Corollary 6.162. *Every maximal ideal M is prime because if M is maximal then R/M is a field, which is an integral domain. The zero ideal of a ring R is a prime ideal if and only if R is an integral domain.*

Lemma 6.163. *Let $A \subset B$ be lattices in $\mathbb{R}^2$. There are only finitely many lattices L between A and B, that is, such that $A \subset L \subset B$.*

Proof. Let (α_1, α_2) be a lattice basis for A, and let P be the parallelogram with vertices $0, \alpha_1, \alpha_2, \alpha_1 + \alpha_2$. There are finitely many elements of B contained in P, so if L is a lattice between A and B, there are finitely many possibilities for the set $L \cap P$. Call this set S. We shall show that S and A are sufficient to determine the lattice L. To show this let $\gamma \in L$. Then there is an element $\alpha \in A$ such that $\gamma - \alpha \in P$, hence in S. Symbolically, we have that $L = S + A$. This describes L in terms of S and A, as required. ■

Proposition 6.164. *Let R be a ring of integers in an imaginary quadratic number field.*

1. *Let B be a nonzero ideal of R. There are finitely many ideals between B and R.*
2. *Every proper ideal of R is contained in a maximal ideal.*
3. *The nonzero prime ideals of R are the maximal ideals.*

Proof. 1. This follows from the previous lemma.

2. Let B be a proper ideal. Then B is contained in only finitely many ideals. We can search through them to find a maximal ideal.

3. Recall that we already know that maximal ideals are prime. Conversely, let P be a nonzero prime ideal. Then P has finite index in R. Then, R/P is an integral domain with finite order, so it is a field. Thus, it must be that P is maximal.

■

Theorem 6.165. *Let R be the ring of integers in a imaginary quadratic field F. Every nonzero ideal of R which is not the whole ring is a product of prime ideals. This factorization is unique up to the order of the factors.*

Observation 6.166. This can be extended to other rings of algebraic integers, but it is a very special property of such rings. This is due to the fact that in most rings the inclusion $A \supset B$ does not imply that A divides B.

Lemma 6.167 (Main Lemma)**.** *Let R be the ring of integers of an imaginary quadratic number field. The product of a nonzero ideal and its conjugate is a principal ideal of R generated by an ordinary integer:*

$$A\overline{A} = (n), \text{ for some } n \in \mathbb{Z} \tag{6.36}$$

Corollary 6.168. *Let R be the ring of integers of an imaginary quadratic number field.*

1. *Cancellation law: Let A, B, C be nonzero ideals of R. If $AB \supset AC$ then $B \supset C$. If $AB = AC$ then $B = C$.*

2. *If A and B are nonzero ideals of R, then $A \supset B$ if and only if A divides B, that is, if and only if $B = AC$ for some ideal C*

3. *Let P be a nonzero prime ideal of R. If P divides a product AB of ideals, then P divides one of the factors A or B.*

Proof. 1. Assume that $AB \supset AC$. If $A = (\alpha)$ is principal, then $AB = \alpha B$ and $AC = \alpha C$. Viewing these sets as subsets of $\mathbb{C}$ we can multiply $\alpha B \supset \alpha C$ by α^{-1} to obtain $B \supset C$. In general, if $AB \supset AC$, then multiplying both sides by $\overline{A}$ and applying the main lemma will give $nB = \overline{A}AB \supset \overline{A}AC = nC$. Applying the method used in the first case gives us $B \supset C$. The case for $AB = AC$ is identical.

2. The backward implication is clear, but the forward is not. We shall first check this in the case of $A = (\alpha)$ being principal. In this case, to say that $(\alpha) \supset B$ means that α divides every element β of B. Let $C = \alpha^{-1}B$ be the set of quotients, that is, $\alpha^{-1}\beta$, with $\beta \in B$. It can be shown that C is an ideal, and $\alpha C = B$. Hence, $B = AC$ in this case. Now, letting A be arbitrary, and assuming that $A \supset B$, we have that $(n) = \overline{A}A \supset \overline{A}B$ by the main lemma. By what has already been shown there is an ideal C such that $nC = \overline{A}B$, or $\overline{A}AC = \overline{A}B$. By the cancellation law we conclude that $AC = B$.

3. If P divides a product AB, then by the 2nd proposition $P \supset AB$. Then, since P is a prime ideal $P \subset A$ or $P \supset B$. Moreover, using the 2nd proposition once again, we have that P divides A or P divides B.

■

Unique Factorization Proof

Proof. First we must show that every proper, nonzero ideal A is a product of prime ideals. If A is not itself prime, then it is not maximal, so we can find a proper ideal A_1 strictly larger than A. Then A_1 divides A, so we can write $A = A_1B_1$. It follows that $A \subset B_1$. Moreover, if we had $A = B_1$, the cancellation law would imply that $R = A_1$, contradicting the fact that A_1 is a proper ideal. Thus, $A \subsetneq B_1$ and $A \subsetneq A_1$. Since there are only finitely many ideals between A and R, this process of factoring an ideal terminates. When it does, all factors will be maximal, and hence prime. Thus, every proper ideal A can be factored into primes.

Now, to prove uniqueness, suppose $P_1...P_r = A = Q_1...Q_s$ are prime factorizations of A. Then P_1 divides $Q_1...Q_s$, and hence it divides one of the factors, say Q_1. Since Q_1 is maximal and $P_1 \neq R$, $P_1 = Q_1$. Then, using the cancellation law and preceding by induction on r we conclude that $r = s$ and $P_i = Q_i$ for all i after reordering. ■

Theorem 6.169. *The ring of integers R is a unique factorization domain if and only if it is a principal ideal domain. If so, then the factorizations of elements and of ideals correspond naturally.*

Proof. It is a well known fact that PIDs have unique factorizations. Conversely, suppose R is a unique factorization domain, and let P be any nonzero prime ideal of R. Then P contains an irreducible element say π. For, any nonzero element α of P is a product of irreducible elements, and, by definition of prime ideal, P contains one of its irreducible factors. Then, since R is a UFD and π is irreducible, π is in fact a prime element which implies that (π) is a prime ideal. Then, (π) is maximal, and since $(\pi) \subset P$ it follows that $(\pi) = P$. Hence, P is principal. Then, we know that any nonprincipal ideal A is the product of prime ideals, and since by the definition of the product of ideals we know that the product of principal ideals is principal, we find that A is itself principal. Therefore, R is a principal ideal domain as required. ■

We shall now consider what these prime ideals are in general

Proposition 6.170. *Let P be a nonzero prime ideal of R. There is an integer prime p so that either $P = (p)$ or $P\overline{P} = (p)$. Conversely, let p be a prime integer. There is a prime ideal P of R so that either $P = (p)$ or $P\overline{P} = (p)$.*

Definition 6.171 (Prime Ideal Terminology)**.** If (p) is a prime ideal, then we say that p **remains prime** in R. If $P\overline{P} = (p)$, then we say that p **splits** in R, unless $P = \overline{P}$, in which case we say that P **ramifies** in R.

Remark 6.172. Suppose $d \equiv 2, 3 \mod 4$. In this case $R = \mathbb{Z}[\sqrt{d}]$ is isomorphic to $\mathbb{Z}[x]/(x^2 - d)$. To ask for prime ideals containing (p) is equivalent to asking for prime ideals of the ring $R/(p)$. Note that

$$R/(p) \cong \mathbb{Z}[x]/(x^2 - d, p) \tag{6.37}$$

Interchanging the order of the defining relations $x^2 - d = 0$ and $p = 0$ gives the first part of the proposition below, and the second part is found in the same way using the polynomial $x^2 - x + \frac{1}{4}(1 - d)$.

Proposition 6.173. .

1. *Assume that $d \equiv 2, 3 \mod 4$. An integer prime p remains prime in R if and only if the polynomial $x^2 - d$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$.*
2. *Assume that $d \equiv 1 \mod 4$. Then p remains prime if and only if the polynomial $x^2 - x + \frac{1}{4}(1 - d)$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$.*

6.8.2 Lecture

Ideal Theory of R when $D < 0$

Recall. When $d = -1$, $\mathbb{Z}[i]$ is a Euclidean ring!

Proposition 6.174. *If $d \equiv 3 \mod 4$ and $d < -1$, then $R = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ is not a unique factorization domain.*

Proof. Consider the factorization of $1 - d = (1 + \sqrt{d})(1 - \sqrt{d}) = 2 \cdot \frac{1-d}{2}$. I claim that 2 is an irreducible elment (a prime) in R. Suppose that $2 = \alpha\beta$ with neither α nor β a unit. Then $N(2) = 4 = N(\alpha)N(\beta)$. But, since the norm of α and β is not one, since they aren't units, $N(\alpha) = N(\beta) = 2$. Howeover, this is impossible as $\alpha = a + b\sqrt{d}$, $a, b \in \mathbb{Z}$, $N(\alpha) = a^2 - db^2$,

where $-d \geq 5$, which would imply $b = 0$, so $a^2 = 2$, but this is a contradiction since 2 isn't a square. Therefore, 2 cannot factor this way, so 2 is an irreducible element. Now, 2 divides $1-d$ from above, but 2 does not divide $(1+\sqrt{d})$ or $(1-\sqrt{d})$ as their factorization in the field is not in the ring R! Therefore, factorization is not unique for $d \equiv 3 \mod 4$ and $d < -1$. ■

Corollary 6.175. *In the case of the above proposition, we further have that R has non-principal ideals; that is, it is not a PID.*

Proposition 6.176. *Although not all ideals $I \subset R$ are principal, every I can be generated by two elements, $I = (\alpha, \beta)$.*

Proof. Either $I = (0)$, or I has finite index in R. (R/I is a finite ring). If $\alpha \neq 0$ in I, then $N(\alpha) = \alpha\alpha' = n > 0$ is also in I. So, $(n) \subset I \subset R = \mathbb{Z} + \mathbb{Z}\left(\frac{D+\sqrt{D}}{2}\right)$, and $[R : (n)] = n^2$, and $[R : I][I : (n)] = [R : (n)]$ so $[R : I]$ must also be finite. In particular, $[R : I] \leq n^2$. The points of $R \subset \mathbb{C}$ form a lattice in the complex plane which is stable under addition and multiplication. Moreover, I in R gives a smaller subgroup in $\mathbb{C}$ which is stable under multiplication from R, and in general all you must do is check it's stable under multiplication by $\frac{D+\sqrt{D}}{2}$. ■

Example 6.177. Take $D = d = -3 \equiv 1 \mod 4$. Then $R = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-3}}{2}\right)$. Moreover, R has six units which are distributed evenly on the unit circle. In fact this set, when observed as a subgroup gives the best sphere packing in 2-space, where spheres of radius 1/2 are centred at each point.

Theorem 6.178. *Any subgroup of R of finite index can be generated (as a subgroup) by 2 elements (the lattice basis of the subgroup).*

Remark 6.179 (Clarification of Definitions). Clarification of certain definitions with primes

1. A **prime** element p in a ring R is not a unit, and if $p \mid ab$ then $p \mid a$ or $p \mid b$
2. An **irreducible** element ι is not a unit, and if $\iota = ab$, then either a is a unit or b is a unit.
3. Let R be a domain (no zero divisors), then any non-zero prime p is irreducible.

   Proof. Suppose $p = ab$ with $a, b \in R$, then $p \mid ab$. Without loss of generality suppose $p \mid a$, so $a = pc$ for some $c \in R$, so $p = ab = pcb$, then using the cancellation law for domains, $1 = cb$, which implies that b is a unit. Thus, p is irreducible. ■

4. WARNING, for an arbitrary domain, the converse is false.

   Example 6.180. Take $d \equiv 3 \mod 4$ which is square free and < -1, and consider $R = \mathbb{Z}[\sqrt{d}]$. Then $2\frac{1-d}{2} = (1-\sqrt{d})(1+\sqrt{d})$ in R, and we have shown that 2 is irreducible. However, 2 does not divide $1-\sqrt{d}$ or $1+\sqrt{d}$, so 2 is in fact not prime.

and special rings

1. We have the following containment for certain special rings

$$\left\{ \begin{array}{c} all \\ rings \end{array} \right\} \supset \underbrace{\left\{ \begin{array}{c} integral \\ domains \end{array} \right\}}_{\text{no zero divisors}} \supset \underbrace{\{\ UFD\ \}}_{\text{unique up to associates}} \supset \underbrace{\{\ PID\ \}}_{\text{Ideals are Principal}} \supset \underbrace{\left\{ \begin{array}{c} Euclidean \\ domains \end{array} \right\}}_{\delta \text{ Euclidean norm}} \supset \{\ Fields\ \} \tag{6.38}$$

2. $\mathbb{Z} \times \mathbb{Z}$ is a ring which is not a domain; $\mathbb{Z}[\sqrt{d}]$ where $d \equiv 3 \mod 4$, $d < -1$, and square free, is a domain which is not a UFD; $\mathbb{Z}[x]$ is a UFD but not a PID; $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a PID but not a ED; $\mathbb{Z}$ is an example of an ED which is not a field; $\mathbb{R}$ is an example of a field.

An addendum to the first not on primes:

Proposition 6.181. *If R is a UFD and $r \in R$, $r \neq 0$, then r is prime if and only if r is irreducible.*

Recall. If $M \subsetneq R$ is a proper ideal, the M is maximal if and only if $M \subset I \subset R$ implies that $I = M$ or R.

Proposition 6.182. *M is a maximal ideal $\iff$ R/M is a field.*

Definition 6.183 (Prime Ideal)**.** A proper ideal $P \subsetneq R$ is called a **prime ideal** if $ab \in P$ implies $a \in P$ or $b \in P$.

Corollary 6.184. *$p \in R$ is a prime element if and only if (p) is a prime ideal.*

Proof. $p \mid x \iff x \in (p)$, so $[p \mid ab \implies p \mid a,\ or\ p \mid b] \iff [ab \in (p) \implies a \in (p)\ or\ b \in (p)]$ ■

Remark 6.185 (WARNING). Prime ideals are not necessarily principle. For example, note that $\mathbb{Z}[x,y]/(x,y) \cong \mathbb{Z}$, which implies that (x,y) is a prime ideal, but this is not principle.

Proposition 6.186. *P is a prime ideal if and only if R/P is a domain.*

Proof. Suppose that P is a prime idea. Suppose $xy = 0$ in R/P. Then their preimage $\widetilde{x}\widetilde{y} \in P$. Without loss of generality suppose $\widetilde{x} \in P$. Then by the definition of the quotient ring, $x = 0$, so R/P is a domain. The converse is identical with reversing the argument. ■

Corollary 6.187. *Every maximal ideal M in R is a prime ideal.*

Proof. R/M being a field implies R/M is a domain, so M is prime. ■

Corollary 6.188. *The zero ideal, (0), is a prime ideal if and only if R is a domain.*

6.9 Ideal Classes in Imaginary Quadratic Fields

6.9.1 Textbook

Definition 6.189 (Similarity Relation)**.** We call two ideals A and B **similar** ($A \sim B$) if there are nonzero elements $\sigma, \tau \in R$ so that

$$\sigma B = \tau A \tag{6.39}$$

This is an equivalence relation. The equivalence classes for this relation are called **ideal classes**, and the ideal class of A is denoted by $\langle A \rangle$.

Remark 6.190. We could also take the element $\lambda = \sigma^{-1}\tau$ of the quadratic number field $F = \mathbb{Q}[\sqrt{d}]$ and say that A and B are similar if

$$B = \lambda A, \text{ for some } \lambda \in \mathbb{Q}[\sqrt{d}] \tag{6.40}$$

Observation 6.191 (Geometric Interpretation)*.* Two ideals A and B are similar if the lattices in the complex plane which represent them are similar geometric figures, by a similarity which is **orientation-preserving**. This follows from the fact that multiplication in the complex plane is equivalent to scaling and rotating shapes about the origin.

Corollary 6.192. *An ideal B is similar to the unit ideal R if and only if $B = \lambda R$ for some λ in the field. In this case B is the principal ideal (λ).*

Proposition 6.193. *The ideal class $\langle R \rangle$ consists of principal ideals.*

Proposition 6.194. *The ideal classes form an abelian group $\mathcal{C}$, with law of composition induced by multiplication of ideals*

$$\langle A\rangle\langle B\rangle = \langle AB\rangle \tag{6.41}$$

the class of principal ideals is the identity: $\langle R\rangle = \langle 1\rangle$.

Proof. If $A \sim A'$ and $B \sim B'$, then $A' = \lambda A$ and $B' = \mu B$ for some $\lambda, \mu \in F = \mathbb{Q}[\sqrt{d}]$; hence, $A'B' = \lambda\mu AB$. This shows that $\langle AB\rangle = \langle A'B'\rangle$, so the law of composition is well defined. Next, the law is commutative and associative because the ideal product is associative and commutative. Moreover, we have the identity $\langle R\rangle$. Finally, $A\overline{A} = (n)$ is principal by the Main Lemma previously. Since the class of the principal ideal $\langle (n)\rangle n$ is the identity in $\mathcal{C}$, we have $\langle A\rangle\langle\overline{A}\rangle = \langle R\rangle$, so $\langle\overline{A}\rangle = \langle A\rangle^{-1}$. ■

Corollary 6.195. *Let R be the ring of integers in an imaginary quadratic number field. The following assertions are equivalent:*

1. *R is a principal ideal domain*
2. *R is a unique factorization domain*
3. *the ideal class group $\mathcal{C}$ of R is the trivial group.*

Definition 6.196 (Class Number)**.** The **class number** of the group of ideal classes for a ring R is a measure of the nonuniqueness of factorization of elements in R. More precise information is given by the structure of $\mathcal{C}$ as a group.

Definition 6.197 (Convex and Centrally Symmetric)**.** A bounded subset S of the plane $\mathbb{R}^2$ is called **convex** and **centrally symmetric** if it has these properties

1. **Convexity**: If $p, q \in S$, then the line segment joining p and q is in S
2. **Central Symmetry**: If $p \in S$, then $-p \in S$.

note that these conditions imply that $0 \in S$ unless S is empty.

Lemma 6.198 (Minkowski's Lemma)**.** *Let L be a lattice in $\mathbb{R}^2$, and let S be a convex, centrally symmetric subset of $\mathbb{R}^2$. Let $\Delta(L)$ denote the area of the parallelogram spanned by a lattice basis for L. If*

$$Area(S) > 4\Delta(L) \tag{6.42}$$

then S contains a lattice point other than zero.

Proof. Define U to be the convex set similar to S, but with half the linear dimension. In other words, we put $p \in U$ if $2p \in S$. Then U is also a convex and centrally symmetric subset of $\mathbb{R}^2$, and $Area(U) = \frac{1}{4}Area(S)$. Hence, the above inequality can be translated to $Area(U) > \Delta(L)$.

Lemma 6.199. *There is an element $\alpha \in L$ such that $U \cap (U + \alpha)$ is not empty.*

Proof. Let P be the parallelogram spanned by a lattice basis for L. The translates $P+\alpha$ with $\alpha \in L$ cover the plane without overlapping except along their edges. Since U is a bounded set, it meets finitely many translates $P + \alpha$, say it meets $P + \alpha_1, ..., P + \alpha_k$. Denote U_i by the set $(P + \alpha_i) \cap U$. Then U is cut into pieces $U_1, ..., U_k$ and $Area(U) = \sum Area(U_i)$. We translate U_i back to P by subtracting α_i, setting $V_i = U_i - \alpha_i$, and we note that $V_i P \cap (U - \alpha_i)$. Thus, V_i is a subset of P, and $Area(V_i) = Area(U_i)$. Then, $\sum Area(V_i) = \sum Area(U_i) > \Delta(L) = Area(P)$. This implies that two of the sets V_i must overlap, that is, for some $i \neq j$, $(U - \alpha_i)(U - \alpha_j)$ is nonempty. Adding α_i and setting $\alpha = \alpha_i - \alpha_j$, we find that $U \cap (U + \alpha)$ is nonempty too. ■

Returning to the Minkowski Lemma, choose α as in the above lemma, and let p be a point of $U \cap (U + \alpha)$. From $p \in U + \alpha$, it follows that $p - \alpha \in U$. By central symmetry $q = \alpha - p \in U$ too. The midpoint between p and q is $\frac{1}{2}\alpha$, which is also in U, because U is convex. Therefore $\alpha \in S$, as required. ■

Corollary 6.200. *Any lattice L in $\mathbb{R}^2$ contains a nonzero vector α such that*

$$|\alpha|^2 \leq 4\Delta(L)/\pi \tag{6.43}$$

Definition 6.201 (Size of an Ideal: 1)**.** The first measure for the size of an ideal I in R is its index. Since an ideal A is a sublattice of R, it has finite index

$$[R : A] = \text{number of additive cosets of } A \text{ in } R \tag{6.44}$$

Lemma 6.202. *Let (a_1, a_2) and (b_1, b_2) be lattice bases for lattices $B \supset A$ in $\mathbb{R}^2$, and let $\Delta(A)$ and $\Delta(B)$ be the areas of the parallelograms spanned by these bases. Then $[B : A] = \Delta(A)/\Delta(B)$.*

Corollary 6.203. .

1. *Let A be a plane lattice. The area $\Delta(A)$ is independent of the lattice basis for A*
2. *If $C \supset B \supset A$ are lattices, then $[C : A] = [C : B][B : A]$*

Remark 6.204 (Area of R). We can compute the area $\Delta(R)$ using the ring's description

$$\Delta(R) = \frac{1}{2}\sqrt{|D|} = \begin{cases} \sqrt{|d|} & if \quad d \equiv 2,3 \mod 4 \\ \frac{1}{2}\sqrt{|d|} & if \quad d \equiv 1 \mod 4 \end{cases} \tag{6.45}$$

where D is the discriminant.

Definition 6.205 (Size of an Ideal: 2)**.** For the second measure of the size of an ideal A, we note that $A\overline{A} = (n)$, and take the integer n (choosing such that $n > 0$). This measure is called the **norm** of the ideal since

$$N(A) = n \; if \; A\overline{A} = (n) \tag{6.46}$$

where the norm has the multiplicative proeprty

$$N(AB) = N(A)N(B) \tag{6.47}$$

Note also that if A is the principal ideal (α), then its norm is the norm of α

$$N((\alpha)) = \alpha\overline{\alpha} = N(\alpha) \tag{6.48}$$

Lemma 6.206. *For any nonzero ideal A of R,*

$$[R : A] = N(A) \tag{6.49}$$

Corollary 6.207 (Multiplicative Property of the Index)**.** *Let A and B be nonzero ideals of R. Then*

$$[R : AB] = [R : A][R : B] \tag{6.50}$$

Theorem 6.208. *Let $\mu = 2\sqrt{|D|}/\pi$. Every ideal class contains an ideal A such that $N(A) \leq \mu$.*

Proof. Let A be an ideal. From a previous corollary we have that there exists $\alpha \in A$ so that

$$N(\alpha) = \alpha^2 \leq 4\Delta(A)/\pi \tag{6.51}$$

Then $A \supset (\alpha)$. This implies that A divides (α), that is $AC = (\alpha)$ for some ideal C. By the multiplicative property of norms $N(A)N(C) = N(\alpha) \leq 4\Delta(A)/\pi$. We then write $\Delta(A) = [R : A]\Delta(R) = \frac{1}{2}N(A)\sqrt{|D|}$. Substituting for $\Delta(A)$ and cancelling $N(A)$, we find that $N(C) \leq \mu$.

Now, since CA is a principal ideal, the class $\langle C\rangle$ is the inverse of $\langle A\rangle$, so $\langle C\rangle = \langle\overline{A}\rangle$. Hence, we have shown that $\langle\overline{A}\rangle$ contains an ideal whose norm satisfies the required inequality. Interchanging the roles of A and $\overline{A}$ completes the proof. ■

Theorem 6.209. *The ideal class group $\mathcal{C}$ is finite.*

Proof. Due to the previous results, it is sufficient to show that there are only finitely many ideals with index $[R : A] \leq \mu$. In other words, we must show there are finitely many sublattices $L \subset R$ with $[R : L] \leq \mu$. Choose an integer $n \leq \mu$, and let L be the sublattice such that $[R : L] = n$. Then R/L is an abelian group of order n, so multiplication by n is the zero map of this group. The translation of this fact to R is the statement $nR \subset L$: Sublattices of index n contain nR. A previous lemma implies that there are finitely many such lattices L. Since there are also only finitely many possibilities for n, we are done. ■

Proposition 6.210. *The ideal class group $\mathcal{C}$ is generated by the classes of the prime ideals P which divide integer primes $p \leq [\mu]$, where $[\mu]$ is the floor of μ.*

Proof. We know that every class contains an ideal of norm $N(A) \leq \mu$, and since $N(A)$ is an integer, $N(A) \leq [\mu]$. Suppose that an ideal A with norm $\leq \mu$ is factored into prime ideals: $A = P_1...P_r$. Then $N(A) = N(P_1)...N(P_r)$. Hence, $N(P_i) \leq [\mu]$ for each i. Thus, the classes of prime ideals P of norm $\leq [\mu]$ form a set generating $\mathcal{C}$, as claimed. ■

Lemma 6.211. *Let n be an ordinary integer, and let A be an ideal. Then*

$$[R : nA] = n^2[R : A] \tag{6.52}$$

6.9.2 Lecture

Definition 6.212 (Multiplication of Ideals)**.** Let $I, J \subset R$ be ideals. Then we define there product to be

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J \right\} \tag{6.53}$$

which is also an ideal.

Corollary 6.213. *If (a) and (b) are principal ideals, then there product is $(a)(b) = (ab)$, so it is also a principal ideal.*

Definition 6.214 (Dedekind Domains)**.** Let R be a domain with a field of fractions $K \neq R/$ Then we say that R is a **Dedekind domain** if for every ideal $I \subset R$, there exists an ideal $(0) \neq J \subset R$ such that $IJ = (r)$ is principal with $r \in R$.

Example 6.215. Suppose $K = \mathbb{Q}(\sqrt{d})$ where d is a square free integer. Then $\mathcal{O}_K =$ the ring of all algebraic integers in $K = \left\{ \begin{array}{cc} \mathbb{Z} + \mathbb{Z}\sqrt{d} & if \quad d \equiv 2,3 \mod 4 \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right) & if \quad d \equiv 1 \mod 4 \end{array} \right\}$. Moreover, this is a Dedekind domain (shown in 10.8.10 in the book). If I is an ideal of $\mathcal{O}_K$, then $I' = \{\alpha' = a - b\sqrt{d} : \alpha = a + b\sqrt{d} \in I\}$. This is an ideal satisfying

$$II' = (n), n \in \mathbb{Z} \tag{6.54}$$

Theorem 6.216. *If F is a field which contains $\mathbb{Q}$, and is of finite dimension over $\mathbb{Q}$, then if you consider the set of algebraic integers in F, $\mathcal{O}_F$, not only is it a ring, but it is a Dedekind domain.*

Theorem 6.217 (Structure of Ideals in Dedekind Domains)**.** *Let R be a Dedekind domain, and let $I \subset R$, $I \neq (0)$, be an ideal. Then I can written uniquely up to reordering as $I = P_1...P_k$ where P_i are nonzero prime ideals.*

Remark 6.218. This gives a way of salvaging unique factorization.

Example 6.219. In $\mathbb{Z}[\sqrt{-5}]$, we have $6 = 2 * 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, where this is a non-unique factorization so $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. However, we know that $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain, and we have the unique factorization

$$(6) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) \tag{6.55}$$

into prime ideals.

Theorem 6.220. *R is a PID if and only if R is a UFD and a Dedekind domain.*

Definition 6.221 (Class Groups)**.** This measures how far a Dedekind domain is from being a PID. Let R be a Dedekind domain. We define an equivalence relation $\sim$ on the set of ideals, saying $I \sim J$ if and only if there exists $r, s \in R$ so that $rI = sJ$, $r, s \neq 0$.

Let $\langle I \rangle =$ the equivalence class of $I =$ the ideal class of I. We then define the set $\mathcal{C}(R) =$ the set of ideal classes $= \langle I \rangle : (0) \neq I \underbrace{\subset}_{ideal} R\}$. (where all ideals $\neq (0)$)

Proposition 6.222. *If we define multiplication of ideal classes by*

$$\langle I\rangle\langle J\rangle = \langle IJ\rangle \tag{6.56}$$

and this well defines a group structure on $\mathcal{C}(R)$

Proposition 6.223. *If* R *is a Dedekind domain, then* R *is a PID* $\iff$ $\mathcal{C}(R)$ *is the trivial group* $\{\langle 1\rangle\}$.

Theorem 6.224. *The class group of the ring of algebraic integers in a field is finite,* $\mathcal{C}(\mathcal{O}_K)$.

Example 6.225. $\mathcal{C}(\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}) = \{\langle(1)\rangle, \langle(2, 1+\sqrt{-5})\rangle\} \cong \mathbb{Z}/2\mathbb{Z}$

Remark 6.226. To calculate $\mathcal{C}(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})$

6.10 Special Lecture

Recall. Recall for imaginary quadratic fields of the form $\mathbb{Q}(\sqrt{d})$, where d is a square-free integer, we index the rings of algebraic integers by the discriminant $D = \begin{cases} 4d & if \quad d \equiv 2,3 \mod 4 \\ d & if \quad d \equiv 1 \mod 4 \end{cases}$, and write $R_D = \mathbb{Z} + \mathbb{Z}\left(\frac{D+\sqrt{D}}{2}\right) \subset \mathbb{C}$, and taking $D < 0$, we have that in $\mathbb{C}$ R_D forms a lattice (and all of its ideals form sublattices).

Recall if $(0) \neq I \subset R_D$ is an ideal, with $[R_D : I] = N(I)$, and if $I = \alpha R_D$, then $N(I) = N(\alpha) = \alpha\overline{\alpha} = [R_D : (\alpha)]$.

Question. How far away from a principal ideal domain are we?

Answer. First, note that not all I are principal.

Definition 6.227 (Fractional Ideal)**.** A **fractional ideal** is an $I \subset \mathbb{Q}(\sqrt{D}) =$ quotient field of R_D, which is a lattice in $\mathbb{C}$, stable under multiplication by R_D. Note that a lattice is a discrete subgroup under addition.

Example 6.228. Take $0 \neq \beta \in \mathbb{Q}(\sqrt{D}) - R_D$. Then, consider $I = \beta R_D$. For example, if $R = \mathbb{Z}[i]$, then we may have the lattice $I = \frac{1}{2}R$, which is not contained in R.

Definition 6.229 (Multiplication of Fractional Ideals)**.** Multiplication of ideals generalizes to multiplication of fractional ideals. Take fractional ideals $I, J \subset \mathbb{Q}(\sqrt{D})$, then their product ideal is

$$I \cdot J := \left\{ \sum_{i=1}^{n} \alpha_i \beta_i : \alpha_i \in I, \beta_i \in J \right\} \tag{6.57}$$

Remark 6.230. This multiplication is only really simple when $I = \alpha R$ and $J = \beta R$ are principle, and $I \cdot J = (\alpha\beta)R$.

Proposition 6.231. .

1. *The fractional ideals form an infinite abelian group under multiplication, with identity the ideal $R = (1)$. The content of this proposition is the existence of inverses, such that $I \cdot (I)^{-1} = R$.*
2. *The principal ideals form a subgroup.*
3. *The quotient group C_D is a finite group, which is called the ideal class group. Every class has a ideal of R as a representitive (not just fractional ideals).*

Remark 6.232. Suppose $I \subset \mathbb{Q}(\sqrt{D})$ is a fractional ideal (so it's a lattice), then it has a lattice basis (α, β). Since $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$, there exists $N \geq 1$ so that $N\alpha, N\beta \in R$, which implies that $(NR)I \subset R$, since $(NR)I$ has basis $(N\alpha, N\beta)$.

Definition 6.233. We let h_D be the order of the ideal class group C_D.

Table 1: Orders of Ideal Class Groups for different Discriminants

Discriminant, D	Order of the Class Group, h_D
-3	1
-4	1
-7	1
-8	1
-11	1
-15	2
-19	1
-20	2
-23	3

Remark 6.234. The last time $h_D = 1$ is $D = -163$. In fact, it appeared that h_D was growing as $|D|$ was growing. Gauss guessed that

$$h_D \approx |D|^{1/2} \tag{6.58}$$

More precisely, Gauss conjectured $C'|D|^{1/2}/\log|D| < h_D < C|D|^{1/2}\log|D|$ for constants C and C' independent of D. The right side of the inequality is known, but the left side is still an open problem, which is related to the Riemann hypothesis.

Theorem 6.235 (Zeta Function - Euler)**.** *The* ***Zeta function*** *is given by the sum*

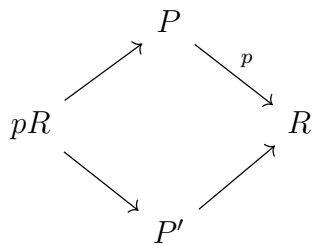
$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p-primes} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p-primes} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \dots\right) \tag{6.59}$$

for $s > 1$ (from prime factorizations).

Corollary 6.236. $\sum_{p-prime} \frac{1}{p}$ *is infinite.*

Theorem 6.237 (Dirichlet (1837))**.** *We have the series*

$$\zeta_R(s) = \sum_{\substack{I \subset R_D \\ I \neq 0}} \frac{1}{(N(I))^s} = \prod_{\substack{P \\ primeideals}} \left(1 - \frac{1}{(N(P))^s}\right)^{-1} \tag{6.60}$$



which converges for $s > 1$. (Recall that $N(I) = [R : I]$). Using the below result, we can also write it as

$$\zeta_R(s) = \prod_{p-primes} \begin{cases} \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 + \frac{1}{p^s}\right)^{-1} \\ \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 - \frac{1}{p^s}\right)^{-1} \\ \left(1 - \frac{1}{p^s}\right)^{-1} \end{cases} \tag{6.61}$$

with the products depending on the way p factors in terms of ideals in the breakdown below. Moreover, each term of $\zeta_R(s)$ is divisible by the corresponding term of $\zeta(s)$. Then, the quotient function is well defined and is

$$L(s) = \frac{\zeta_R(s)}{\zeta(s)} = \prod_{p-rat.\ prime} \left(1 \pm \frac{1}{p^s}\right)^{-1} \tag{6.62}$$

This quotient function converges for $s = 1$, and it is the ***Class Number Formula***

$$L(1) = \frac{2\pi}{\sqrt{|D|}} \cdot \frac{h_D}{|R^*|} \tag{6.63}$$

Recall. Consider a rational prime p in the gaussian integers, $R = \mathbb{Z}[i]$. Then there are three posibilities for p:

1. pR can be a prime ideal, with $N(pR) = p^2$ (it remains prime)
2. There are two prime ideals such that $PP' = pR$ (it splits)
3. There is one prime ideal $pR \subset P \subset_p R$ with $P^2 = pR$.

Remark 6.238. For $\mathbb{Z}[i]$, we have that

$$L(s) = \prod_{p \cong 1 \mod 4} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p \cong 3 \mod 4} \left(1 + \frac{1}{p^s}\right)^{-1} = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} - \frac{1}{11^s} + \ldots = \sum_{n \geq 1,\ odd} \frac{\pm 1}{n^s} \tag{6.64}$$

And in fact, this converges at $s = 1$, $L(s) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} + \ldots = \frac{\pi}{4}$ converges! From above, $L(1) = \frac{2\pi}{\sqrt{4}} \frac{h_4}{4} = \frac{\pi}{4} h_4$, which implies $h_4 = 1$.

Remark 6.239. What we want to show is that $L(1)$ is not too small (as a real number), $L(1) \approx 1$, then $h_D \sim |D|^{1/2}$.

Remark 6.240 (Reimann Conjecture). All zeroes of $\zeta(s)$, with $0 < Re(s) < 1$, have $Re(s) = \frac{1}{2}$. Note that $\left|\frac{1}{n^s}\right| = \frac{1}{n^{Re(s)}}$, so if $Re(s) > 1$, then $\zeta(s)$ converges absolutely. The function $\zeta(s) - \frac{1}{s-1}$ has an analytic continuation for the entire plane, with $s = 1$, and the interesting behaviour occurs in the critical strip between $s = 0$ and $s = 1$.

7 General Review

7.1 Motions

Recall. A rigid motion in $\mathbb{R}^n$ is a group homomorphism which preserves distance.

Remark 7.1 (Canonical Form). Any rigid motion can be written in the form $m = (translation-possibly\ trivial)(rotation-possibly\ trivial)(reflection\ or\ identity)$. Moreover, the translations arise as elements of the additive group of $\mathbb{R}^n$, while rotations and reflections arrise as orthogonal linear operators in $O_n(\mathbb{R})$, which can be expressed as orthogonal matrices once coordinates have been chosen. Mpreover, rotations are in the group $SO_n(\mathbb{R})$ while reflections are of the form $(O_n(\mathbb{R})\backslash SO_n(\mathbb{R})) \cup \{e\}$.

Remark 7.2. The group of translations $T \cong (\mathbb{R}^n, +)$ is a normal subgroup of the group of motions as it is the kernel of the canonical map from the motion group to the group of linear operators $O_n(\mathbb{R})$.

Example 7.3 (Special Case)**.** For $n = 2$, we consider motions in the plane. In particular, we classified the discrete motions in $\mathbb{R}^n$. This was achieved by decomposing the group of discrete motions into a translation subgroup and a subgroup of $O_2(\mathbb{R})$.

Remark 7.4 (Classification of Discrete Motions in $\mathbb{R}^2$). The subgroups of $O_2(\mathbb{R})$ for discrete motions are always of the form C_n, or D_{2n} for some n. For a trivial translation group, n can be anything. Howeover, for a linear translation group n can only be 1 or 2, and for a lattice translation group, $n = 1, 2, 3, 4$ or 6 depending on the lattice.

7.2 Group Actions

Definition 7.5. We say that a group G acts on a set S if we have a map $G \times S \to S$ such that $e.s = s$ for all $s \in S$, and for all $g, g' \in G$, $(gg').s = g.(g'.s)$.

Definition 7.6 (Orbits and Stabilizers)**.** Suppose G acts on a set S and let $s \in S$. Then the orbit of s is $O_s := \{g.s : g \in G\}$. Moreover, the stabilizer of s is the subgroup $G_s := \{g \in G : g.s = s\}$ of G.

Proposition 7.7. *We have a natural group action of G on the coset space G/G_s which is transitive, and in fact, G/G_s is isomorphic as a set to O_s by the map $gG_s \mapsto g.s$.*

Proposition 7.8. *Given that G is finite, $|G| = [G : G_s]|G_s| = |O_s||G_s|$.*

Proposition 7.9. *If we consider the stabilizer $G_{g.s}$, then $G_{g.s} = gG_sg^{-1}$.*

Proposition 7.10 (Classification)**.** *Fix a group G and a set S. There is a one-to-one correspondance between actions of G on S and group homomorphisms $G \to Sym(S)$. In particular we have a bijection $G \circlearrowright S \mapsto [g \mapsto [s \mapsto g.s]]$ and a bijection $[\phi : G \to Sym(S)] \mapsto g.s = \phi(g)(s)$.*

Remark 7.11. If $|S| = n$, then $Sym(S) \cong S_n$, and if we have that $G \circlearrowright S$ gives a homomorphism (of groups) $G \to S_n$.

Remark 7.12. In particular, we can act $G \circlearrowright G$ by left translation, so if $|G| = n$, then we have a group homomorphism $\phi : G \to S_n$, and its kernel (elements sent to the identity map) is trivial, so ϕ is in fact injective and we say that the action $G \circlearrowright G$ is faithful.

Definition 7.13 (Conjugation)**.** We consider the action $G \circlearrowright G$ by conjugation: $g.x \mapsto gxg^{-1}$. From this, we can obtain the class equation

$$|G| = \sum_{conj.//classesC} |C| = \sum_{conj.//classesC} \frac{|G|}{|N(c)|} \tag{7.1}$$

Moreover, if we have a conjugacy class of order 1, then it is in the center of G (and vice-versa).

Example 7.14 (Applications to p-groups)**.** From the class equation we know that p-groups have center of order > 1, and every group of order p^2 is abelian.

Definition 7.15 (Simple Group)**.** If G is a subgroup and $H \trianglelefteq G$, then $H = \{1\}$ or G.

Remark 7.16. These groups are structurally important. For example, if we have a group homomorphism $f : G \to G'$, where G is simple, then f is injective or trivial.

Proposition 7.17. *If H is a normal subgroup of G, then H is a union of conjugacy classes. This is due to the fact that H is stable under conjugation, so for every element x in H, x's conjugacy class must also be in H.*

Example 7.18. If we take the class equation plus the fact that $|H| \mid |G|$, we can sometimes show a group is simple.

7.3 Sylow Theory

Theorem 7.19 (Sylow Theorem)**.** *Given a group G of order $p^n m$, where $\gcd(p, m) = 1$ and $n \geq 1$, we have that*

1. *There exists a Sylow p-subgroup of G (i.e. a subgroup of order p^n)*
2. *For any subgroup K of G with order divisible by p, there exists a Sylow p-subgroup H such that $H \cap K$ is a Sylow p-subgroup of K. In particular, all Sylow p-subgroups are conjugate.*
3. *The number of Sylow p-subgroups, $n_p(G)$, divides m and is congruent to $1 \mod p$.*

Example 7.20 (Applications)**.** Here are a few applications

1. For groups G of order pq ($p < q$), G has a unique normal subgroup which is a Sylow q-subgroup of G.
2. Moreover, if q is not congruent to 1 mod p, then G also has a unique normal Sylow p-subgroup.
3. Groups of order 12

7.4 Conjugacy in S_n

Remark 7.21. Every permutation of S_n has a disjoint cycle decomposition. Moreover, disjoint cycles commute.

Remark 7.22 (Conjugation). Then, given a permuation $p = (i_1, ..., i_r)...(i'_1, ..., i'_s)$ and another permutation τ, if we proceed right to left, then the conjugate $\tau p \tau^{-1} = (\tau(i_1), ..., \tau(i_r))...(\tau(i'_1), ..., \tau(i'_s))$.

7.5 Ring Theory

Definition 7.23 (Rings)**.** Rings are 3-tuples $(R, +, \times)$ where R is a set and an abelian group under $+$, and $\times$ for R is associative with identity 1, and $+$ and $\times$ interact via the distributive laws $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for all $a, b, c \in R$

Definition 7.24 (Homomorphisms)**.** Ring homomorphisms preserve $+$, $\times$, and 1

Definition 7.25 (Ideals)**.** Ideals are subgroups $I \subset R$ under the addition operation, and for all $r \in R$ and $x \in I$, $rx \in I$.

Remark 7.26. Note that the kernel of any ring homomorphism is an ideal, and all ideals arise as the kernel of some ring homomorphism.

Definition 7.27 (Principal Ideal)**.** A principal ideal of a ring R is an ideal $(a) = \{ra : r \in R\}$ generated by $a \in R$.

Proposition 7.28. *If R is a commutative ring, then R is a field if and only if R has exactly two ideals. Namely (0) and $(1) = R$.*

Question. For what rings are ideals always principal?

Answer (Euclidean algorithm). The euclidean algorithm implies that every ideal of $\mathbb{Z}$ is principal. Moreover, if F is a field, we have a euclidean algorithm for the ring $F[x]$, and this implies that every ideal of $F[x]$ is principal.

Theorem 7.29 (Ideals of Quotients)**.** *If R is a ring with an ideal I, then the ideals of R/I are in bijective correspondance with the ideals J of R such that $J \supset I$. This correspondance is realized by the canonical homomorphism $f : R \to R/I = \overline{R}$, and $\overline{J} \mapsto f^{-1}(\overline{J})$ and $J \mapsto f(J)$.*

Remark 7.30. By the first isomorphism theorem we find that $R/J \cong \overline{R}/\overline{J}$ by the map $R \to \overline{R} \to \overline{R}/\overline{J}$ which is surjective with kernel J.

7.5.1 Relations

Proposition 7.31. *If F is a field and we consider $F[x]$ and make the relation $x = 0$, we obtain $F[x]/(x) \cong F$.*

Proof. Take the ring homomorphism $\phi : F[x] \to F$ by $p(x) \mapsto p(0)$. Note that ϕ is surjective. Moreover, $(x) \subset \ker \phi$. Then if $p(x) \in \phi$, $p(0) = 0$, so p's constant term is zero. In particular, $p(x) = xq(x)$ since $x = 0$ is a root of $p(x)$, where $q(x)$ is of degree less than p. Then $p(x) \in (x)$ so $\ker \phi = (x)$. Therefore, by the first isomorphism theorem, we have a unique canonical map $\overline{\phi} : F[x]/(x) \xrightarrow{F}$. ■