

MATH600: Abstract Algebra I

Notes by Yuval Amit

Instructor: Harry Tamvakis

Fall 2025

Contents

Vector Spaces	4
1 Intro To Vector Spaces	4
2 Subspaces	4
3 Bases	5
3.1 Finite Dimensional	5
3.2 Infinite Dimensional	6
4 Linear Maps	7
5 Direct Sums and Products	8
5.1 Infinite Direct Sums and Products	10
6 Quotient Spaces	10
7 Universal Properties	11
8 $\text{Hom}(V, W)$	13
9 Coordinate Systems	14
10 Eigenvectors and Eigenvalues	15
11 Diagonalizable Operators	16
12 Inner Products	18
13 Orthogonal and Unitary Transformations	20
 Groups	 22
14 Basics of Groups	22
15 Subgroups	23
16 Cosets and Lagrange's Theorem	24

17	Products of Groups	28
18	Inner Automorphisms of a Group	29
19	Symmetry	30
20	Finite Subgroups of $\mathcal{O}(2)$	31
21	Group Actions	33
22	Conjugacy Classes in G ; The Class Equation	35
23	Conjugacy Action of G on Subgroups	37
24	The Sylow Theorems	38
25	The Symmetric Group	40
26	Conjugacy in S_n	41
27	Finite Simple Groups	42
28	Semidirect Products	45
29	External Semi Direct Products	45
30	Groups of Order pq	46
31	The Free Group	47
32	Reflection Groups and Coxeter Groups	49
	Rings	52
33	Intro to Rings	52
34	Ring Homomorphisms	54
35	Ideals and Quotients	54
36	The Field of Fractions of an Integral Domain	57
37	Euclidean Domains	58
38	Adjunction of Elements	59
39	Principal Ideal Domains	60
40	Chinese Remainder Theorem	61
41	Unique Factorization Domains	62
42	Irreducibility in Polynomial Rings	67
43	Noetherian Rings	68

Algebraic Geometry	71
44 Introduction to Algebraic Geometry	71
45 The Ideal of a Set of Points	72
46 Algebraic Subsets of the Line and Plane	74
47 Hilbert's Nullstellensatz (Theorem of the Zeroes)	75
 Modules	 78
48 Modules	78
49 Algebras	79
50 Free Modules	80
51 Exact Sequences	81
52 Tensor Products of Modules	81
53 Graded Rings and Algebras	89
54 The Tensor Algebra	89
55 Symmetric Powers and Symmetric Algebras	91
56 Motivation for the Symmetric Algebra	92

Vector Spaces

1. Intro To Vector Spaces

Definition

1.1

A **vector space** over a field F is a set V with two operations:

$+$: $V \times V \rightarrow V$, denoted with $(x, y) \mapsto x + y$

$\cdot$: $F \times V \rightarrow V$, denoted with $(\lambda, x) \mapsto \lambda \cdot x = \lambda x$

satisfying (for all $x, y, z \in V, \lambda, \mu \in F$)

1. $x + y = y + x$
2. $(x + y) + z = x + (y + z)$
3. $\exists 0 \in V, x + 0 = x$
4. $\forall x, \exists x'$ such that $x + x' = 0$.
5. $1 \cdot x = x$
6. $\lambda(\mu x) = (\lambda\mu)x$
7. $(\lambda + \mu)x = \lambda x + \mu x$
8. $\lambda(x + y) = \lambda x + \lambda y$

Proposition

1.2

$0_F \cdot x_V = 0_V$, and $x' = (-1) \cdot x$

2. Subspaces

Definition

2.1

A subset $H \subset V$ is a **subspace** if it's closed under the operations, i.e. H is a vector space. This is often denoted as $H \leq V$

Definition

2.2

Given any subset $S \subset V$, the **span** of S , denoted $\text{Span } S$ or $\langle S \rangle$, is

$$\{\lambda_1 x_1 + \cdots + \lambda_n x_n \mid \lambda_i \in F, x_i \in S, n \in \mathbb{N}\}$$

Remark 2.3.

$$\langle S \rangle = \bigcap_{S \subset H \leq V} H$$

Definition

2.4

A subset $S \subset V$ is **linearly independent** if $\lambda_1 x_1 + \cdots + \lambda_m x_m$ with $\lambda_j \in F, x_j \in S$ implies $\lambda_1 = \cdots = \lambda_m = 0$. Otherwise, S is **linearly dependent**.

Lemma

2.5

- (a) A single vector $v \in V$ is linearly independent if and only if $v \neq 0$
- (b) $\{x, y\}$ is linearly dependent if and only if one is a scalar multiple of the other.

3. Bases

Definition

3.1

A **basis** of a vector space V is a linearly independent subset B that spans V

Definition

3.2

We say V is **finite dimensional** if there exists a finite set S such that $\text{Span}(S) = V$

Remark 3.3. A set B is a basis of a vector space V if and only if every $v \in V$ has a unique representation as a linear combination $v = \sum_{i=1}^n \lambda_i x_i$, for $x_i \in B$. Hence, bases provide coordinate systems on vector spaces.

Our goal is to show that every vector space has a basis

3.1. Finite Dimensional

Linear Dependence Lemma

3.4

Let $v_1, \dots, v_n$ be a list of linearly dependent vectors in V . Then, there exists some $r \in \{1, \dots, n\}$ such that v_r is a linear combination of $v_1, \dots, v_{r-1}$. Furthermore, $\langle v_1, \dots, v_n \rangle = \langle v_1, \dots, \widehat{v_r}, \dots, v_n \rangle$

Proof. Let $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$, and by linear dependence we may assume that not all $\lambda_i = 0$. Let r be the largest index such that $\lambda_r \neq 0$. Then, $\lambda_{r+1} = \cdots = \lambda_n = 0$, and it follows that

$$\lambda_1 v_1 + \cdots + \lambda_r v_r = 0 \implies v_r = -\frac{\lambda_1}{\lambda_r} v_1 + \cdots + \left(-\frac{\lambda_{r-1}}{\lambda_r}\right) v_{r-1}$$

□

Theorem

3.5

Every finite dimensional vector space has a basis.

Proof. Let $v_1, \dots, v_n$ be a spanning set of V . If they are linearly independent, we're done. Otherwise, by the linear dependence lemma we may remove one element, while maintaining the same span. Inductively, we can repeat this process until the list is linearly independent, and still spans V . □

Proposition

3.6

Let V be finite dimensional and $u_1, \dots, u_m$ be a linearly independent list in V . Then, there exists $u_{m+1}, \dots, u_n$ such that $u_1, \dots, u_n$ is a basis of V . In other words, we can always “complete” a linearly independent list to a basis.

Proof. Let $v_1, \dots, v_r$ be a basis of V . Then, $u_1, \dots, u_m, v_1, \dots, v_r$ spans V . By using the linear dependence lemma, it can be reduced to a basis, and note that we won’t remove any of the elements $u_1, \dots, u_m$ because none are in the span of the previous. $\square$

Proposition

3.7

If $v_1, \dots, v_n$ span V and $w_1, \dots, w_m$ are linearly independent, then $m \leq n$.

Corollary

3.8

Any two bases of a finite dimensional vector space V have the same number of elements.

Definition

3.9

The number of element in a basis is the **dimension** of V , denoted $\dim V$ or $\dim_F V$.

Corollary

3.10

If V is finite dimensional and $W \leq V$, then W is finite dimensional with $\dim W \leq \dim V$, with equality if and only if $W = V$.

3.2. Infinite Dimensional

Let $\{A_i\}_{i \in I}$ be a family of nonempty sets.

Definition

3.11

A **choice function** is a $f : I \rightarrow \cup A_i$ such that $f(i) \in A_i$, for all $i \in I$. The set of all such choice functions is called the **Cartesian product** of $\{A_i\}$.

The Axiom of Choice

The cartesian product of any family of non-empty sets is non-empty

Definition

3.12

A **partial order** on a set A is a relation $\leq$ which is reflexive, antisymmetric ($x \leq y$ and $y \leq x \implies x = y$), and transitive.

Definition

3.13

A subset B of A is a **chain** if B is totally ordered, i.e. $x \leq y$ or $y \leq x$ for all $x, y \in B$.

Definition

3.14

A subset $B \subset A$ has an **upper-bound** $M \in A$ if $b \leq M$ for all $b \in B$. An element $a \in A$ is **maximal** if $a \leq x \implies a = x$.

Zorn's Lemma

3.15

Suppose $P \neq \emptyset$ is a partially ordered set such that every chain in P has an upper bound. Then, P has a maximal element.

Theorem

3.16

Every non-zero vector space has a basis.

Proof. Let $P = \{\text{all linearly independent subsets of } V\}$. Since V is non-zero, there exists $v \neq 0 \in V$, so $\{v\} \in P$, hence $P \neq \emptyset$.

Let C be a chain in P , with the partial ordering of set inclusion. Let $X = \cup c$ for all $c \in C$. Pick $v_1, \dots, v_n \in X$, so there exist $c_1, \dots, c_n \in C$ with $v_i \in c_i$. Since C is a chain, there must be some c_j containing all the other c_i . That is, $v_1, \dots, v_n \in c_j$, so as we know $c_j \in P$, it follows that $v_1, \dots, v_n$ is linearly independent. It therefore follows that X is linearly independent, and therefore an upper-bound of C . Thus, by Zorn's Lemma, P contains a maximal element B which is a maximal linearly independent subset of V . By this maximality, we must have $\langle B \rangle = V$, hence B is a basis. $\square$

Note that this argument can also be used to show any linearly independent set $S \subset V$ can be extended to a basis.

4. Linear Maps

Definition

4.1

Given two vector spaces V, W over the same field F , a **linear map** $T : V \rightarrow W$ is a function with $T(x + y) = T(x) + T(y)$ and $T(\lambda x) = \lambda T(x)$.

Proposition

4.2

$T(0) = 0$.

Theorem

4.3

If $T : F^n \rightarrow F^m$ is linear, there exists a matrix $A \in M_{m,n}(F)$ such that $T(x) = Ax$ for all $x \in F^n$. In particular, $A = \begin{pmatrix} Te_1 & \cdots & Te_n \end{pmatrix}$, where $e_1, \dots, e_n$ are the standard basis vectors.

Example 4.4. The matrix $A = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ corresponds to rotation in $\mathbb{R}^2$ by an angle θ .

Remark 4.5. Composition of linear maps corresponds to matrix multiplication.

Remark 4.6. Let V have basis $B = \{b_i\}_{i \in I}$. Then, a linear map $T : V \rightarrow W$ is completely determined by

the values $T(b_i)$, for $i \in I$. Conversely, for any family of vectors $\{w_i\}_{i \in I}$ in W , there exists a unique linear map $T : V \rightarrow W$ with $T(v_i) = w_i$.

Definition

4.7

Given a linear map $T : V \rightarrow W$, we define the **kernel** and **image** of T to be

$$\ker T = \{v \in V \mid T(v) = 0\}$$

$$\text{Img}(T) = \{T(v) \mid v \in V\}$$

Note that $\ker T \leq V$ and $\text{Img } T \leq W$.

Proposition

4.8

T is injective if and only if $\ker T = \{0\}$.

Definition

4.9

Let $T : F^n \rightarrow F^m$ be represented by matrix A . Then, we call $\ker T$ the **null space** and $\text{Img } T$ the **column space** of A . Moreover, $\dim \ker$ is the **nullity**, and $\dim \text{Img}$ is the **rank**.

Definition

4.10

A linear map $T : V \rightarrow W$ is an isomorphism if there exists a linear inverse map $S : W \rightarrow V$, where $T \circ S = \text{id}_W$, $S \circ T = \text{id}_V$.

Proposition

4.11

Suppose V and W are finite dimensional, with $\dim V = \dim W$. TFAE:

- (i) $T : V \rightarrow W$ is an isomorphism.
- (ii) $T : V \rightarrow W$ is injective.
- (iii) $T : V \rightarrow W$ is surjective.

Theorem

4.12

If $\dim V = n$, then $V \cong F^n$.

5. Direct Sums and Products

Let V and W be vector spaces over the same field F .

Definition

5.1

The **external direct sum** $V \oplus W$ is the vector space $V \times W = \{(v, w) \mid v \in V, w \in W\}$ with the expected operations.

Theorem

5.2

If $\dim V, \dim W < \infty$, then $\dim V \oplus W = \dim V + \dim W$.

Definition

5.3

Let V be a vector space. Then, given any two subsets $A, B \subset V$, we define the **internal direct sum** to be $A + B = \{a + b \mid a \in A, b \in B\}$.

If A and B are subspaces, then $A + B$ is a subspace as well.

Definition

5.4

Given U_1, U_2 subspaces of V , we say that V is the **direct sum** of U_1 and U_2 if every $v \in V$ has a unique expression as $v = u_1 + u_2$.

In this case, we get an isomorphism $V \rightarrow U_1 \oplus U_2$ by $(u_1 + u_2) \mapsto (u_1, u_2)$. Conversely, an external direct sum $V \oplus W$ can be viewed as an internal direct sum, with $U_1 = V \oplus 0, U_2 = 0 \oplus W$, subspaces of $V \oplus W$.

In practice, the 2 notions of direct sums are the same.

Proposition

5.5

Suppose U_1, U_2 are subspaces of V . Then, TFAE:

1. $V = U_1 \oplus U_2$
2. $U_1 \cap U_2 = \{0\}$ and $V = U_1 + U_2$.

Proof.

($\Leftarrow$) For an arbitrary $v \in V$, suppose $v = u_1 + u_2 = u'_1 + u'_2$. Then, $u_1 - u'_1 = u_2 - u'_2$, and it follows that $u_1 - u'_1, u_2 - u'_2 \in U_1 \cap U_2$. Thus, $u_1 = u'_1$ and $u_2 = u'_2$, proving the representation of v is unique. Hence, $V = U_1 \oplus U_2$

($\Rightarrow$) If $V = U_1 \oplus U_2$, then clearly $V = U_1 + U_2$. Moreover, for any $v \in U_1 \cap U_2$, we know $v = v + 0 = 0 + v$. As both $0, v \in U_1 \cap U_2$, it follows by uniqueness of representation that $v = 0$. $\square$

Definition

5.6

Given U a subspace of V , another subspace U' of V is called the **complement** of U if $V = U \oplus U'$

Proposition

5.7

If V is a vector space and $U \leq V$, then there exists $U' \leq V$ such that $U \oplus U' = V$

Proof. Let $\{u_i\}_{i \in I}$ be a basis of U . Then, we may extend this linearly independent list to a basis of $V : \{b_i\}_{i \in I} \cup \{b'_j\}_{j \in J}$. It follows that $U' = \langle \{b'_j\}_{j \in J} \rangle$ is the complement of U . $\square$

5.1. Infinite Direct Sums and Products

Let $\{U_i\}_{i \in I}$ be a family of vector spaces over the same field F .

Definition

5.8

The **direct product** $\prod_{i \in I} U_i$ is identified with the Cartesian product of the U_i with pointwise operations as expected.

Definition

5.9

The **direct sum** $\bigoplus_{i \in I} U_i$ is the subspace of $\prod U_i$ consisting of all elements $\prod a_i$ such that only finitely many a_i are non-zero.

Proposition

5.10

$V = \bigoplus_{i \in I} U_i$ if and only if every $v \in V$ has a unique representation as a finite sum $v = \sum_{i \in I} a_i$

6. Quotient Spaces

Definition

6.1

For a subspace U of V , we may define an equivalence relation $\sim$ on V by $a \sim b \iff a - b \in U$. The equivalence class of some $v \in V$ is

$$\{y \in V \mid y \sim v\} = \{y \in V \mid y - v = u \in U\} = \{v + u \mid u \in U\}$$

We define this to be the **U -coset** of v , denoted $v + U$.

The **quotient space** of $V \bmod U$ is the set $V/U = \{v + U \mid v \in V\}$, with operations

$$(v + U) + (v' + U) = (v + v') + U$$

$$\lambda(v + U) = \lambda v + U$$

These operations are well defined.

Proposition

6.2

If U' is a complement of U , the map $U' \rightarrow V/U$ by $x \mapsto x + U$ is an isomorphism. That is, $U' \cong V/U$

Corollary

6.3

If V is finite dimensional, then $\dim(V/U) = \dim(V) - \dim(U)$

First Isomorphism Theorem

6.4

Let $T : V \rightarrow W$ be linear. Then, $\tilde{T} : V/\ker T \rightarrow \text{Img } T$ mapping $v + \ker T \mapsto T(v)$ is an isomorphism. That is, $V/\ker T \cong \text{Img } T$.

Proof. Let $v, v' \in V$. Then,

$$v + \ker T = v' + \ker T \iff T(v - v') = 0 \iff Tv = Tv' \iff \tilde{T}(v + \ker T) = \tilde{T}(v' + \ker T)$$

showing T is well defined and injective. Surjectivity is trivial. $\square$

Corollary (Rank-Nullity)

6.5

If $T : V \rightarrow W$ is linear, $\dim V < \infty$, then $\dim \operatorname{Im} T < \infty$, and

$$\dim V = \dim \ker T + \dim \operatorname{Im} T$$

Second Isomorphism Theorem

6.6

Let $U, W \leq V$. Then, $(W + U)/U \cong W/(W \cap U)$

Proof. Let $\varphi : W \rightarrow (W + U)/U$ be defined by $\varphi(w) = w + U$. An arbitrary element of $(W + U)/U$ is of the form $(w + u) + U$, but note that $(w + u) + U = w + U$. Thus, φ is surjective. Moreover,

$$w \in \ker \varphi \iff \varphi(w) = U \iff w + U = U \iff w \in U$$

It therefore follows that $\ker \varphi = W \cap U$. Thus, by the first isomorphism theorem,

$$W/(W \cap U) = W/\ker \varphi \cong \operatorname{Im} \varphi = (W + U)/U,$$

as desired. $\square$

Corollary

6.7

If $\dim U, \dim W < \infty$, then

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W).$$

In particular, $\dim(U + W) < \infty$

7. Universal Properties

Definition

7.1

Let $U \leq V$ be a subspace. Then, there exists a **canonical projection map** $\pi : V \rightarrow V/U$ defined naturally as $\pi(v) = v + U$.

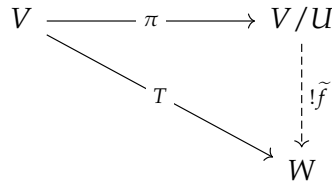
The Universal Property of Quotient Spaces

7.2

For $U \leq V$, the pair $(V/U, \pi)$ satisfy

- (i) $U \subset \ker \pi$
- (ii) For any vector space W and map $T : V \rightarrow W$ such that $U \subset \ker T$, there exist a unique linear map $\tilde{f} : V/U \rightarrow W$ such that $\tilde{f} \circ \pi = T$.

That is, the diagram below commutes.



Proof. (i) is trivial. Let $T : V \rightarrow W$ be such that $U \subset \ker T$. Let $\tilde{f} : V/U \rightarrow W$ be defined by $\tilde{f}(v + U) = T(v)$. If $v + U = v' + U$, then let $v = v' + u$, and it follows that

$$\tilde{f}(v + U) = T(v) = T(v' + u) = T(v') = \tilde{f}(v' + U)$$

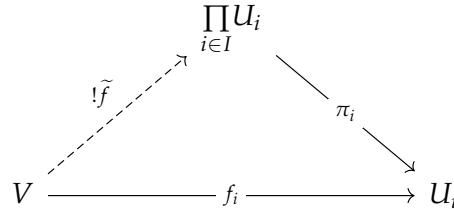
hence $\tilde{f}$ is well defined. Moreover, it's clear by the definition of $\tilde{f}$ that $\tilde{f} \circ \pi = T$. Uniqueness follows from the fact that the desired property of $\tilde{f}$ is essentially how we defined it. This proves (ii). $\square$

Universal Property of Direct Products

7.3

Let $\{U_i\}_{i \in I}$ be a family of vector spaces. Then, for any $j \in I$ we have the projection morphism $\pi_j : \prod U_i \rightarrow U_j$ defined naturally by $\pi_j((u_i)_{i \in I}) = u_j$

Now, for any vector space V and family of morphisms $f_i : V \rightarrow U_i$, there exists a unique map $\tilde{f} : V \rightarrow \prod U_i$ such that $\pi_i \circ \tilde{f} = f_i$ for all $i \in I$. That is, the diagram below commutes.



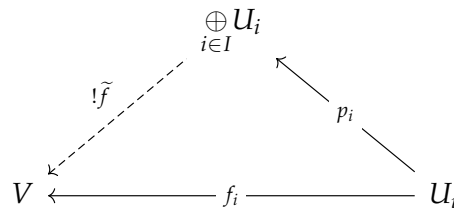
Proof. Let $\tilde{f} : V \rightarrow \prod U_i$ be defined by $\tilde{f}(v) = (f_i(v))_{i \in I}$. Then, it's easy to see how $\pi_j(\tilde{f}(v)) = \pi_j((f_i(v))_{i \in I}) = f_j(v)$. $\square$

Universal Property of Direct Sums

7.4

For each $i \in I$, we have a natural inclusion $p_i : U_i \rightarrow \bigoplus_{i \in I} U_i$ given by $u_i \mapsto u_i$.

So, for any V and maps $f_i : U_i \rightarrow V$, there exists a unique $\tilde{f} : \bigoplus U_i \rightarrow V$ defined by $\tilde{f} \circ p_i = f_i$. That is, the diagram below commutes.



Proof. Similar $\square$

8. Hom(V, W)**Definition**

8.1

Given vector spaces V, W , we define

$$\text{Hom}(V, W) := \{T : V \rightarrow W \mid T \text{ linear}\}$$

with the expected addition and scalar multiplication.

Proposition

8.2

If $\dim V = n$ and $\dim W = m$, then $\dim \text{Hom}(V, W) = mn$.

Proof. Recall that $V \cong F^n, W \cong F^m$. In particular we may identify $\text{Hom}(V, W)$ with $\text{Hom}(F^n, F^m)$ by associating the map $T : V \rightarrow W$ to its matrix representation $A \in M_{m \times n}(F)$. That is, $\text{Hom}(V, W) \cong \text{Hom}(F^n, F^m)$, and the claim follows. $\square$

Definition

8.3

Define $V^* := \text{Hom}(V, F)$, which we call the **dual space** of V .

Theorem

8.4

Let $\dim V = n$, with basis $v_1, \dots, v_n$. Then, there exists a **dual basis** $v_1^*, \dots, v_n^*$ of V^* satisfying

$$v_i^*(v_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

Proof. Since $v_1, \dots, v_n$, these definitions of $v_1^*, \dots, v_n^*$ are uniquely defining. Now, suppose $\lambda_1 v_1^* + \dots + \lambda_n v_n^* = 0$. Then, for an arbitrary v_j , we have

$$0 = (\lambda_1 v_1^* + \dots + \lambda_n v_n^*)(v_j) = \lambda_j v_j^*(v_j) = \lambda_j$$

proving linear independence. Moreover, let $\varphi \in V^*$ be arbitrary, and φ is defined by $\varphi(v_1), \dots, \varphi(v_n)$. Then, for any $v = a_1 v_1 + \dots + a_n v_n \in V$, we have

$$\varphi(v) = a_1 \varphi(v_1) + \dots + a_n \varphi(v_n) = (\varphi(v_1) v_1^* + \dots + \varphi(v_n) v_n^*)(v),$$

i.e. $\varphi = \varphi(v_1) v_1^* + \dots + \varphi(v_n) v_n^*$. Thus, $v_1^*, \dots, v_n^*$ span V^* , and we have proved it's a basis. $\square$

Corollary

8.5

If $\dim V = n$, then $\dim V = \dim V^*$, and furthermore $V \cong V^*$ with the isomorphism $v_i \mapsto v_i^*$. Note that this isomorphism is not "canonical", as it requires the choice of a basis.

Theorem

8.6

Let $\dim V = n$. Then, there exists a natural isomorphism $\Lambda : V \rightarrow V^{**}$

Proof. For any $v \in V$, we may consider $\hat{v} \in V^{**}$ defined by $\hat{v}(f) = f(v)$. One can verify that the operation $v \mapsto \hat{v}$ is an isomorphism. Now that in this instance, we did not have to select a basis

of V . □

9. Coordinate Systems

Definition

9.1

Given a vector space V and an ordered basis $B = \{b_1, \dots, b_n\}$, we obtain an induced coordinate isomorphism $V \rightarrow F^n$ defined by $(\lambda_1 b_1 + \dots + \lambda_n b_n) \mapsto (\lambda_1, \dots, \lambda_n)$. In particular, for $v = \lambda_1 b_1 + \dots + \lambda_n b_n$, we write

$$(v)_B = (\lambda_1, \dots, \lambda_n)$$

Definition

9.2

Let V have two bases $B = \{b_1, \dots, b_n\}$ and $B' = \{b'_1, \dots, b'_n\}$. Every element in V has a coordinate representation in each of these bases, so we can consider the map from F^n to itself defined by this **change of basis**.

Precisely, we define the **change of basis matrix** $(\text{id})_{B,B'} : F^n \rightarrow F^n$ by

$$(\text{id})_{B,B'} = \begin{pmatrix} (b_1)_{B'} & \cdots & (b_n)_{B'} \end{pmatrix}.$$

Then, we have $(\text{id})_{B,B'}(v)_B = (v)_{B'}$. This is also called the **transition matrix**.

Example 9.3. We may consider the change from the standard basis $E = \{e_1, \dots, e_n\}$ in F^n to an arbitrary basis $B = \{b_1, \dots, b_n\}$. Observe $(\text{id})_{E,B} = (\text{id})_{B,E}^{-1} = \begin{pmatrix} b_1 & \cdots & b_n \end{pmatrix}^{-1}$

When we're changing basis, we're simply altering how we represent the vectors in one basis to another. However, we can consider changing the basis while also applying a linear map to the vectors. That is, we have a vector in one basis, and we're transforming it into the image of that vector in another basis. This is useful for linear maps whose domain and co-domain are not the same space.

Definition

9.4

Let $T : V \rightarrow W$ be a linear map, $B = \{b_1, \dots, b_n\}$ be a basis of V , and $C = \{c_1, \dots, c_m\}$ be a basis of W . Furthermore, define $(T)_{B,C} : F^n \rightarrow F^m$ to be

$$(T)_{B,C} = \begin{pmatrix} (Tb_1)_C & \cdots & (Tb_n)_C \end{pmatrix}$$

Then, $(T)_{B,C}$ is the unique matrix satisfying $(T)_{B,C}(v)_B = (Tv)_C$.

Theorem

9.5

Let E be the standard basis of F^n , and E' the standard basis of F^m . Then,

$$(T)_{B,C} = (\text{id})_{E',C}(T)_{E,E'}(\text{id})_{B,E}$$

Proof. $(T)_{B,C}$ with the unique map sending $(v)_B$ to $(Tv)_C$. Well, observe

$$(\text{id})_{E',C}(T)_{E,E'}(\text{id})_{B,E}(v)_B = (\text{id})_{E',C}(T)_{E,E'}(v)_E = (\text{id})_{E',C}(Tv)_{E'} = (Tv)_C$$

so the equality follows from uniqueness. $\square$

Special Case

Let $T : V \rightarrow V$, and let B be a basis for V . We use the shorthand notation $(T)_{B,B} = (T)_B$. Let A be the matrix equivalent to T . Then,

$$(T)_B = (\text{id})_{E,B}(T)_{E,E}(\text{id})_{B,E} = P^{-1}AP$$

where $P = \begin{pmatrix} b_1 & \cdots & b_n \end{pmatrix}$.

$(T)_B$ represents something very natural: given an operator on any (finite dimensional) vector space, we create a matrix representing the linear map on a fixed basis. This is helpful for linear operators on vector spaces other than F^n , and extends the theory of matrices to all operators on finite dimensional spaces.

Definition

9.6

Two matrices A, B are similar if there exists $P \in GL_n(F)$ such that $A = PBP^{-1}$.

As discussed in the special case previously, similar matrices represent the same map with respect to different coordinate systems.

Theorem

9.7

Let $T : V \rightarrow W$ be linear. Then, there exists bases B of V and C of W such that $(T)_{B,C} = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$, where $r = \text{rank } T$

Remark 9.8. Let V have dimension n . Then, $\text{Hom}(V, V) \cong M_n(F)$, but this isomorphism depends on a choice of ordered basis for V . But, if $f : M_n(F) \rightarrow F$ is a function satisfying $f(PAP^{-1}) = f(A)$, then f doesn't depend on the choice of basis of V , so we can view f as a well defined map on $\text{Hom}(V, V) \rightarrow F$. Namely, set $f(T) = f((T)_B)$, and the basis B does not matter.

Example 9.9. $\det : M_n(F) \rightarrow F$ satisfies $\det(PAP^{-1}) = \det(A)$. Therefore, there is a well defined notion of determinant of a linear map. Similar case for trace.

10. Eigenvectors and Eigenvalues

Definition

10.1

A subspace $W \leq V$ is **T -invariant** if $T(W) \subset W$.

Definition

10.2

A non-zero vector $v \in V$ is an **eigenvector** with **eigenvalue** λ given $T(v) = \lambda v$.

Remark 10.3. The span of an eigenvector is a 1 dimensional T -invariant subspace.

Proposition**10.4**

λ is an eigenvalue of $T \iff \ker(T - \lambda I) \neq \{0\} \iff \det(T - \lambda I) = 0$.

Note in particular that $\ker(T - \lambda I)$ is the set of all λ -eigenvectors of T (and 0). We call this the λ -**eigenspace**.

Definition**10.5**

For a variable x , the polynomial $p_T(x) = \det(T - xI)$ is called the **characteristic polynomial** of A

Remark 10.6. The characteristic polynomial of similar matrices is invariant. Moreover, $p_T(x) = x^n - (\text{Tr } T)x^{n-1} + \dots + (-1)^n \det T$

Proof. $\det(PAP^{-1} - xI) = \det(P(A - xI)P^{-1}) = \det(A - xI)$ □

Remark 10.7. The roots of $\det(T - xI)$ are values for x which make the determinant of $T - xI$ equal to 0. These are precisely the eigenvalues of T . In particular, the characteristic polynomial of T is the unique monic polynomial of degree n whose roots are all the eigenvalues of T , with multiplicity.

11. Diagonalizable Operators

Definition**11.1**

$T : V \rightarrow V$ is **diagonalizable** if V has a basis of eigenvectors for T . Equivalently, T can be represented by a diagonal matrix.

Proposition**11.2**

Let $Tv_1 = \lambda_1 v_1, \dots, Tv_k = \lambda_k v_k$. If $\lambda_1, \dots, \lambda_k$ are distinct, then $v_1, \dots, v_k$ are linearly independent. That is, eigenvectors with distinct eigenvalues are linearly independent.

Theorem**11.3**

Let $T : V \rightarrow V$ be linear, $\dim V = n$. Let $\lambda_1, \dots, \lambda_k$ be distinct eigenvalues of T , and let $W_i = \ker(T - \lambda_i I)$. Then, TFAE:

1. T is diagonalizable
2. $p_T(x) = (x - \lambda_1)^{d_1} \dots (x - \lambda_k)^{d_k}$, with $d_i = \dim(W_i)$
3. $V = W_1 \oplus \dots \oplus W_k$

Remark 11.4. Let λ be an eigenvalue of T , and m be the dimension of the corresponding eigenspace. Then, $m \leq d$, where d is the multiplicity of λ .

Corollary**11.5**

If T has n distinct eigenvalues, then T is diagonalizable.

Example 11.6. Consider the matrix $C = \begin{pmatrix} 0 & 1 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \\ a_0 & a_1 & \cdots & \cdots & a_{n-1} \end{pmatrix}$. Observe that an eigenvector

$(v_1, \dots, v_n)$ must satisfy $v_2 = \lambda v_1, v_3 = \lambda v_2, \dots, v_n = \lambda v_{n-1}$, as well as $\lambda v_n = a_1 v_1 + \cdots + a_n v_n$. In particular, eigenvectors of C must be of the form $(\alpha, \lambda\alpha, \dots, \lambda^{n-1}\alpha)$, where $\lambda^n = a_0 + a_1\lambda + \cdots + a_{n-1}\lambda^{n-1}$. Let $f(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_1x - a_0$. Then, the eigenvalues of C are roots of f . So, as f is monic of degree n , we have $f = p_C(x)$. We call C the **companion** matrix of $f(x)$. This proves that any monic polynomial in $F[x]$ of degree n is the characteristic polynomial of some $A \in M_n(F)$.

Example 11.7. Consider the Fibonacci sequence $F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$ for $n \geq 0$. We can then write

$$\begin{pmatrix} F_n \\ F_{n+1} \end{pmatrix} = \begin{pmatrix} F_n \\ F_n + F_{n-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} F_{n-1} \\ F_n \end{pmatrix}.$$

Thus, if we let $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, we have

$$\begin{pmatrix} F_n \\ F_{n+1} \end{pmatrix} = A \begin{pmatrix} F_{n-1} \\ F_n \end{pmatrix} = A^2 \begin{pmatrix} F_{n-2} \\ F_{n-1} \end{pmatrix} = \cdots = A^n \begin{pmatrix} F_0 \\ F_1 \end{pmatrix} = A^n \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Once can compute the characteristic polynomial of A , $p_A(x) = x^2 - x - 1$, which has roots $\varphi_1 = \frac{1+\sqrt{5}}{2}$ and $\varphi_2 = \frac{1-\sqrt{5}}{2}$, and corresponding eigenvectors $\begin{pmatrix} 1 \\ \varphi_1 \end{pmatrix}, \begin{pmatrix} 1 \\ \varphi_2 \end{pmatrix}$. Therefore, we know by change of basis with these eigenvectors as a basis that

$$\begin{aligned} A &= \begin{pmatrix} 1 & 1 \\ \varphi_1 & \varphi_2 \end{pmatrix} \begin{pmatrix} \varphi_1 & 0 \\ 0 & \varphi_2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \varphi_1 & \varphi_2 \end{pmatrix}^{-1} \\ A^n &= \begin{pmatrix} 1 & 1 \\ \varphi_1 & \varphi_2 \end{pmatrix} \begin{pmatrix} \varphi_1^n & 0 \\ 0 & \varphi_2^n \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \varphi_1 & \varphi_2 \end{pmatrix}^{-1} = \frac{1}{\varphi_2 - \varphi_1} \begin{pmatrix} \varphi_1^n & \varphi_2^n \\ \varphi_1^{n+1} & \varphi_2^{n+1} \end{pmatrix} \begin{pmatrix} \varphi_2 & -1 \\ -\varphi_1 & 1 \end{pmatrix} \\ &= \frac{1}{\varphi_2 - \varphi_1} \begin{pmatrix} \varphi_1^n \varphi_2 - \varphi_2^n \varphi_1 & \varphi_2^n - \varphi_1^n \\ \varphi_1^{n+1} \varphi_2 - \varphi_2^{n+1} \varphi_1 & \varphi_2^{n+1} - \varphi_1^{n+1} \end{pmatrix} \end{aligned}$$

Thus, we may multiply this matrix by $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, and the first component will be exactly F_n . Thus,

$$F_n = \frac{1}{\varphi_2 - \varphi_1} (\varphi_2^n - \varphi_1^n) = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$$

Theorem

11.8

Let V be a complex vector space, $T \in \text{Hom}(V, V)$. Then, there exists a basis B of V such that $(T)_B$ is upper triangular.

12. Inner Products

In this section, we only consider vector spaces over $\mathbb{R}$ or $\mathbb{C}$.

Definition

12.1

Let V be an $\mathbb{R}$ -vector space. An **inner product** on V is a function $\langle, \rangle : V \times V \rightarrow \mathbb{R}$ satisfying

- (i) Linearity in the first variable
- (ii) Symmetry (hence linearity in the second variable as well)
- (iii) $\langle x, x \rangle > 0$ for all $x \neq 0$.

Definition

12.2

Let V be a $\mathbb{C}$ -vector space. A **hermitian inner product** $\langle, \rangle : V \times V \rightarrow \mathbb{C}$ satisfies

- (i) Linearity in the first variable
- (ii) $\langle x, y \rangle = \overline{\langle y, x \rangle}$ (hence conjugate linearity in the second variable)
- (iii) $\langle x, x \rangle > 0$ for all $x \neq 0$.

Definition

12.3

The **norm** or **length** of a vector x is $\|x\| = \sqrt{\langle x, x \rangle}$

Proposition

12.4

- (i) $\|\lambda x\| = |\lambda| \cdot \|x\|$
- (ii) $\|x\| > 0$ if $x \neq 0$
- (iii) **(Cauchy-Schwartz Inequality):** $|\langle x, y \rangle| \leq \|x\| \cdot \|y\|$
- (iv) **(Triangle Inequality):** $\|x + y\| \leq \|x\| + \|y\|$

Proof.

(iii) For $x \neq 0$, $\|x\|^2 \cdot \|y\|^2 - |\langle x, y \rangle|^2 = \frac{1}{\|x\|^2} \|(|y\|)^2 x - \langle x, y \rangle y\|^2 \geq 0$. The rest is left as an exercise.

(iv) $\|x + y\|^2 = \langle x + y, x + y \rangle = \|x\|^2 + \langle x, y \rangle + \langle y, x \rangle + \|y\|^2 = \|x\|^2 + 2\operatorname{Re} \langle x, y \rangle + \|y\|^2 \leq \|x\|^2 + 2\|x\| \cdot \|y\| + \|y\|^2 = (\|x\| + \|y\|)^2$.

□

Definition

12.5

The angle θ between vectors x and y in an $\mathbb{R}$ -vector space is given by $\cos \theta = \frac{\langle x, y \rangle}{\|x\| \cdot \|y\|}$

Definition

12.6

Two vectors x, y are **orthogonal** if $\langle x, y \rangle = 0$. A set S of vectors is **orthogonal** if any two members are orthogonal. S is **orthonormal** if it's orthogonal and consists of unit vectors (vectors

with norm 1).

Proposition

12.7

An orthogonal set is linearly independent. Furthermore, if $x = a_1u_1 + \cdots + a_nu_n$, then for all $k \in \{1, \dots, n\}$, $\langle x, u_k \rangle = a_k \langle u_k, u_k \rangle$, hence $a_k = \frac{\langle x, u_k \rangle}{\langle u_k, u_k \rangle}$. Linear independence follows, since $x = 0$ immediately implies $a_k = 0$ from this formula, for all $k \in \{1, \dots, n\}$.

In general, if $x \in \text{Span}(u_1, \dots, u_n)$, then

$$x = \sum_{i=1}^n \frac{\langle x, u_i \rangle}{\|u_i\|^2} u_i$$

Gram-Schmidt Orthogonalization

12.8

Let $u_1, \dots, u_n$ be a basis of an F -vector space V . Then, there exists an orthogonal basis $v_1, \dots, v_n$ such that $v_k \in \text{Span}(u_1, \dots, u_k)$ for all $k \in \{1, \dots, n\}$.

Proof. We induct on $n = \dim V$. The base case is clear, so suppose $u_1, \dots, u_{n+1}$ is a basis of the $n+1$ dimensional vector space V . Let $W = \text{Span}(u_1, \dots, u_n)$. By the inductive hypothesis, we have an orthogonal basis $v_1, \dots, v_n$ of W such that $v_k \in \text{Span}(u_1, \dots, u_k)$ for all $k \in \{1, \dots, n\}$.

Now, consider our desired $v_{n+1} = u_{n+1} + \lambda_1v_1 + \cdots + \lambda_nv_n$, noting that $v_{n+1} \neq 0$ by the assumption that $u_{n+1} \notin \text{Span}(u_1, \dots, u_n)$. Then, the desired condition $\langle v_{n+1}, v_k \rangle = 0$ means

$$\langle u_{n+1}, v_k \rangle + \lambda_k \langle v_k, v_k \rangle = 0 \iff \lambda_k = -\frac{\langle u_{n+1}, v_k \rangle}{\|v_k\|^2}.$$

Taking such $\lambda_1, \dots, \lambda_n$, we get an orthogonal basis. That is, in general,

$$v_{k+1} = u_{k+1} - \frac{\langle u_{k+1}, v_1 \rangle}{\|v_1\|^2} v_1 - \cdots - \frac{\langle u_{k+1}, v_k \rangle}{\|v_k\|^2} v_k$$

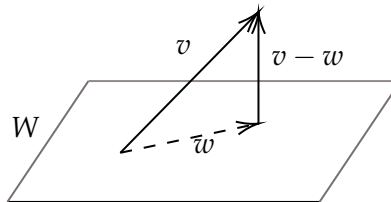
□

Remark 12.9. From an orthogonal basis, we may obtain an orthonormal basis by dividing each vector by its norm, i.e. "normalizing" all the vectors.

Definition

12.10

For some $v \in V$, a vector $w \in W \leq V$ is called the **orthogonal projection** of $v \in V$ onto W if $v - w \perp W$.



Proposition

12.11

For any $v \in V$, there exists a unique orthogonal projection of v onto W , denoted $\text{proj}_W(v)$

Proof. Let $e_1, \dots, e_k$ be an orthonormal basis of W , and we're looking for a specific $w = \lambda_1 e_1 + \dots + \lambda_k e_k$. In particular, we require $(w - v) \perp e_i$ for all i , hence

$$0 = \langle \lambda_1 e_1 + \dots + \lambda_k e_k - v, e_i \rangle = \lambda_i - \langle v, e_i \rangle \iff \lambda_i = \langle v, e_i \rangle.$$

This gives us uniquely determined coefficients, namely

$$\text{proj}_W(v) = \sum_{i=1}^k \langle v, e_i \rangle e_i$$

□

Definition**12.12**

The **orthogonal compliment** of a subspace W is

$$W^\perp = \{v \in V \mid \langle v, w \rangle = 0, w \in W\}$$

Proposition**12.13**

$$V = W \oplus W^\perp$$

13. Orthogonal and Unitary Transformations

Definition**13.1**

Let $F = \mathbb{R}$ (resp. $\mathbb{C}$), and equip F^n with the standard (resp. hermitian) inner product. We say $A \in M_n(F)$ is **orthogonal** (resp. **unitary**) if its columns form an orthonormal basis of F^n

Definition**13.2**

The **adjoint** of a matrix A is defined to be $A^* := \overline{A}^t$.

Theorem**13.3**

Let $A \in M_n(F)$. Then, TFAE

- (i) A is orthogonal/unitary
- (ii) $AA^* = A^*A = I$
- (iii) A preserves the inner product, i.e. $\langle Ax, Ay \rangle = \langle x, y \rangle$.
- (iv) A is a **linear isometry**, meaning it preserves distance, i.e. $d(Ax, Ay) = d(x, y)$.

Proof. Exercise. □

As usual, we can extend the notion of unitary and orthogonal matrices to linear maps.

Definition**13.4**

If V is a standard (resp. hermitian) inner product space, we say $T \in \text{Hom}(V, V)$ is orthogonal (resp. unitary) if $\langle Tx, Ty \rangle = \langle x, y \rangle$ for all $x, y \in V$. This is equivalent to $(T)_B$ being orthogonal (resp. unitary) with respect to any orthonormal basis B .

Example 13.5. Let $A \in M_n(\mathbb{R})$ be orthogonal, so $AA^t = I$. It's known that $\det(A) = \det(A^t)$, hence $\det(A)^2 = \det(I) = 1$, therefore $\det(A) = \pm 1$. We say A is **orientation preserving** if $\det(A) = 1$, and A is **orientation reversing** if $\det(A) = -1$.

Now, consider the case when $A \in M_2(\mathbb{R})$, letting $A = \begin{pmatrix} Ae_1 & Ae_2 \end{pmatrix}$. As the columns are assumed to be orthonormal, we know that if the first column is (x, y) , then $x^2 + y^2 = 1$. It follows that $x = \cos \theta$ and $y = \sin \theta$ for some $\theta \in \mathbb{R}$. It then follows by the necessary orthonormality of the columns that either

- (a) $Ae_2 = \begin{pmatrix} -\sin \theta \\ \cos \theta \end{pmatrix}$, so A is the orientation preserving rotation by θ
- (b) $Ae_2 = \begin{pmatrix} \sin \theta \\ -\cos \theta \end{pmatrix}$, so A is the orientation reversing reflection about some line.

Recall the definition of an isometry from earlier:

Definition

13.6

An **isometry** or **rigid motion** $m : \mathbb{R}^n \rightarrow \mathbb{R}^n$ is a function that preserves distances. That is, $d(m(a), m(b)) = d(a, b)$ for all $a, b \in \mathbb{R}^n$.

Theorem

13.7

- (a) An isometry $m : \mathbb{R}^n \rightarrow \mathbb{R}^n$ with $m(0) = 0$ is linear. Hence, it is left multiplication by some orthogonal matrix.
- (b) Furthermore, every isometry of $\mathbb{R}^n$ is the composition of an orthogonal map and a translation τ_v for some $v \in \mathbb{R}^n$ (so $\tau_v(x) = x + v$)

Groups

14. Basics of Groups

Definition

14.1

A set G is a **group** if it's equipped with a binary operation $\cdot : G \times G \rightarrow G$ satisfying

1. $(ab)c = a(bc)$
2. There exists an identity element $e \in G$ such that $ae = ea = a$ for all $a \in G$.
3. For every $a \in G$ there exists $a^{-1} \in G$ satisfying $aa^{-1} = a^{-1}a = e$.

Definition

14.2

A group is **abelian** if multiplication is commutative, i.e. $ab = ba$ for all $a, b \in G$. Abelian groups are often denoted additively, and the identity is denoted by 0.

Example 14.3. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}^\times, \cdot)$, $(\mathbb{C}^\times, \cdot)$ are all abelian groups.

Example 14.4. Given a set A , we can define $S(A) = \{f : A \rightarrow A \mid f \text{ is bijective}\}$, i.e. the set of all permutations of the elements of A . Then, $(S(A), \circ)$ is a group under composition.

Definition

14.5

For $A = \{1, \dots, n\}$, $(S(A), \circ)$ is the **symmetric group** S_n

Note that S_3 is non-abelian, and in fact is the smallest non-abelian group

Example 14.6. Let F be a field. Then, we have various **matrix groups**. These include

1. $GL_n(F) = \{A \in M_n(F) \mid A \text{ is invertible}\}$. This is called the **general linear group**.
2. $SL_n(F) = \{A \in GL_n(F) \mid \det A = 1\}$. This is the **special linear group**.
3. Given any finite dimensional F -vector space V , we have the group of linear automorphisms $\text{Aut}(V) = \{T \in \text{Hom}(V, V) \mid T \text{ is invertible}\}$. By choosing a basis $\mathcal{B}$ of V , we can identify $\text{Aut}(V) \cong GL_n(F)$.
4. When $F = \mathbb{R}$, we have the **orthogonal group** $O(n) = \{A \in GL_n(\mathbb{R}) \mid AA^t = I\}$. Moreover, we have the **special orthogonal group** $SO(n) = O(n) \cap SL_n(\mathbb{R})$.
5. When $F = \mathbb{C}$, we have the **unitary group** $U(n) = \{A \in GL_n(\mathbb{C}) \mid AA^* = I\}$. Moreover, we have the **special unitary group** $SU(n) = U(n) \cap SL_n(\mathbb{C})$.

Proposition

14.7

If G is a group, then

- (i) The identity element of G is unique
- (ii) Each $a \in G$ has a unique inverse $a^{-1} \in G$
- (iii) $(a^{-1})^{-1} = a$ for all $a \in G$
- (iv) $(ab)^{-1} = b^{-1}a^{-1}$ for all $a, b \in G$

Proof. (ii): Given a with inverses a', a'' , we have $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$ $\square$

Cancellation Laws

14.8

- (i) $ax = ax' \implies x = x'$
- (ii) $xa = x'a \implies x = x'$

15. Subgroups**Definition**

15.1

A non-empty subset H of a group G is a **subgroup** if it's closed under the group operations multiplication and inversion.

Note that this definition implies $e = aa^{-1} \in H$

Lemma

15.2

Let H be a nonempty subset of a group G which is finite and closed under multiplication. Then, H is a subgroup of G .

Proof. Given $a \in H$, we must show that $a^{-1} \in H$. We have $a, a^2, \dots$ are all in H , and since H is finite, there exists r, s with $r < s$ such that $a^r = a^s$. Then, $a^{s-r} = e$, so $a(a^{s-r-1}) = (a^{s-r-1})a = e$. $\square$

Example 15.3. 1. Every group has the trivial subgroups $\{e\}$ and G

2. Subgroups of $\mathbb{Z}$: Suppose H is a non-zero subgroup of $\mathbb{Z}$. Then, let n be the smallest positive number in H . We claim that $H = n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$.

Proof. Since $n \in H$ and H is closed under the group operations, the entire subgroup $n\mathbb{Z} \subset H$. Conversely, if $a \in H$, we may divide a by n : $a = kn + r$ with $0 \leq r < n$. Then, $r = a - kn \in H$, so by minimality of n , we must have $r = 0$. Hence, every $a \in H$ is a multiple of n . $\square$

Application: Given $a, b \in \mathbb{Z}$ both positive, let $a\mathbb{Z} + b\mathbb{Z}$ be the subgroup of $\mathbb{Z}$ generated by $\{a, b\}$. That is, $a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$. Since this is a nonzero subgroup, we must have that $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ for some $d \in \mathbb{Z}^+$. We claim that $d = \gcd(a, b)$.

Proof. Indeed, $d \mid a$ since $a = a \cdot 1 + b \cdot 0 \in d\mathbb{Z}$, hence $a = dk$ for some $k \in \mathbb{Z}$. Similarly, $d \mid b$.

Now, if $c \mid a, c \mid d$, then we must have $c \mid d$, since $d \in a\mathbb{Z} + b\mathbb{Z}$, so $d = ax + by$. $\square$

Definition

15.4

If G is any group and $a \in G$, we can consider the subgroup **generated** by a . Let $\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$. If there exists some $a \in G$ such that $G = \langle a \rangle$, we say that G is **cyclic**.

Example 15.5. For cyclic groups, there are two cases:

1. If all powers $a^i, i \in \mathbb{Z}$ are distinct, then G is an infinite cyclic group
2. If $a^r = a^s$ with $r < s$, then $a^{s-r} = 1$. Hence $a^n = 1$ for some smallest positive integer n , and so $\langle a \rangle = \{1, a, a^2, \dots, a^{n-1}\}$. We in some cases call this group C_n . Note that C_n is realized by the group of n 'th roots of unity in $\mathbb{C}$, which we denote $\mu_n = \{z \in \mathbb{C} : z^n = 1\} = \{e^{2\pi i k/n} \mid k = 0, 1, \dots, n-1\}$

Definition

15.6

The **order** of a finite group G , denoted $|G|$ or $o(G)$, is the number of elements in G . The order $o(a)$ of an element $a \in G$ is the order of the cyclic subgroup $\langle a \rangle$. So, $o(a) = \min\{k \geq 1 \mid a^k = e\}$.

Definition

15.7

Let G be a group, $W \subset G$ be a subset. Then, the **subgroup generated by the subset W** , denoted $\langle W \rangle$, is the smallest subgroup of G containing W . Concretely, it consists of all products of elements of W and their inverses.

Definition

15.8

The **Klein group** V is the smallest non-cyclic group. It is realized as a subgroup of $GL_2(\mathbb{R})$ by $V = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\}$. Note that any 2 non-identity element in V generate V .

Definition

15.9

The group $GL_n(F)$ has the **Borel subgroup** B consisting of all upper triangular matrices.

16. Cosets and Lagrange's Theorem

Fun fact: Lagrange invented his theorem before groups were invented

Definition

16.1

Given $H \leq G$ (" H is a subgroup of G "), we define an equivalence relation $x \sim y \iff x^{-1}y \in H$. We say that x **congruent** to y modulo H , and write $x \equiv y \pmod{H}$

The equivalence class of x is the (left) **coset** of x , i.e. the set $[x] = \{y \in G : x \sim y\} = \{y \mid x^{-1}y = h \in H\} = \{xh \mid h \in H\} = xH$.

Note

We could have used $xy^{-1} \in H$ in the above definition, and this leads to the right cosets Hx

Proposition

16.2

The inversion map $x \mapsto x^{-1}$ gives a 1 – 1 correspondence between left and right H -cosets, since $H^{-1} = \{h^{-1} \mid h \in H\} = H$, hence $(xH)^{-1} = Hx^{-1}$. We'll use left H -cosets. The two notions coincide for abelian groups

Example 16.3. If $G = (\mathbb{Z}, +)$, $H = n\mathbb{Z}$, then $x \equiv y \pmod{H} \iff x \equiv y \pmod{n}$. The cosets are $n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}$.

Proposition

16.4

There is a 1 – 1 correspondence between any two (left) H -cosets. Furthermore, the cosets form a partition of G .

Proof. The cosets partition G because they are equivalence classes. Given any two cosets aH and bH , the map $f : aH \rightarrow bH$ sending $ah \mapsto bh$ is 1 – 1 and onto by the cancellation law. $\square$

Lagrange's Theorem

16.5

Let G be a finite group, and $H \leq G$. Then, $|H|$ divides $|G|$

Proof. If k is the number of left H -cosets, then G is partitioned into k subsets, each with $|H|$ elements. Hence, $|G| = |H| \cdot k$ $\square$

Definition

16.6

The number of left (or right) H -cosets is the **index** of the subgroup H in G , denoted $|G : H|$. Hence, $|G| = |H| \cdot |G : H|$

Corollary

16.7

- (a) If G is a finite group and $a \in G$, then $o(a) \mid o(G)$.
- (b) If $|G| < \infty$ and $a \in G$, then $a^{|G|} = e$.
- (c) If G is a finite group with prime order, then G is cyclic.

Definition (The Quotient Set)

16.8

Given any two subsets A, B of a group G , we define $AB = \{ab \mid a \in A, b \in B\}$. Let G/H denote the set of all left H -cosets of G . We want to make this set into a group, with multiplication of cosets.

Suppose this were the case. Then, for any $g \in G$, $A := gHg^{-1}H$ must equal another H -coset. Clearly, $e \in A$, so as the H -cosets partition the group G , we must have $A = H$. That is, $gHg^{-1}H = H \implies ghg^{-1} \in H$ for all $g \in G, h \in H$.

Definition (Normal Subgroups)

16.9

A subgroup $N \leq G$ is a **normal subgroup** if for each $n \in N$ and $g \in G$, $gng^{-1} \in N$. Equivalently, $gNg^{-1} \subset N$

Proposition

16.10

The following are equivalent, for $N \leq G$

1. N is a normal subgroup of G , denoted $N \trianglelefteq G$
2. $gNg^{-1} = N$ for all $g \in G$
3. Every left coset of N is also a right coset of N in G .

Proof. (i) $\implies$ (ii): Assume $gNg^{-1} \subset N$. Then, $N = g(g^{-1}Ng)g^{-1} \subset gNg^{-1}$.

(ii) $\implies$ (iii): $gNg^{-1} = N \iff gN = Ng$.

(iii) $\implies$ (i): Given any $g \in G$, we have $gN = Nx$ for some $x \in G$. We must therefore have $Nx = Ng$ since $g \in gN = Nx$ and $g \in Ng$. Hence, we get (i) $\square$

We can therefore define a group structure on G/N when N is normal in G , setting $(aN)(bN) = a(Nb)N = a(bN)N = abN$.

Definition

16.11

The above defines the **quotient group** G/N

Example 16.12. If G is abelian, then every subgroup of G is normal, so we always get a quotient group.

Example 16.13 (Modular arithmetic). Let $G = \mathbb{Z}$, $H = n\mathbb{Z}$. So, $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \overline{n-1}\}$, where $\bar{x} := x \pmod{n}$.

Definition

16.14

$(\mathbb{Z}/n\mathbb{Z})^\times$ consists of the multiplicatively invertible elements in $\mathbb{Z}/n\mathbb{Z} \setminus \{0\}$, which are exactly the equivalence classes coprime to n . This makes $(\mathbb{Z}/n\mathbb{Z})^\times$ a multiplicative group with order $\varphi(n)$.

Fact

Normal subgroups are exactly the kernels of group homomorphisms.

Definition (Homomorphisms and Isomorphisms)

16.15

A map $\varphi : G \rightarrow G'$ between two groups is a **homomorphism** of groups if it preserves the group operations: $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$. Furthermore, if φ is bijective, we say it is an **isomorphism**.

Definition ($\text{Hom}(G, G')$ and $\text{Aut}(G)$)

16.16

We write $\text{Hom}(G, G') :=$ the set of all homomorphisms $G \rightarrow G'$. An isomorphism $G \rightarrow G$ is called an **automorphism** of G , and these form a group $\text{Aut}(G)$

Example 16.17. For any homomorphism $\varphi : G \rightarrow G'$, $\varphi(e) = e'$ and $\varphi(x)^{-1} = \varphi(x^{-1})$.

Definition

16.18

The **kernel** of φ is the set of $g \in G$ such that $\varphi(g) = e'$, and the image is $\text{Img } \varphi = \varphi(G)$

Check

$\ker \varphi$ is always a normal subgroup of G .

First Isomorphism Theorem

16.19

For any homomorphism $\varphi : G \rightarrow G'$ of groups, $G / \ker \varphi \cong \text{Img } \varphi$, with the map $g \ker \varphi \mapsto \varphi(g)$.

Proof. Same as for vector spaces. □

Example 16.20. 1. For any field F , $SL_n(F) = \ker(\det : GL_n(F) \rightarrow F^*)$, so we have a normal subgroup of $GL_n(F)$. Furthermore, $GL_n(F)/SL_n(F) \cong (F^*, \cdot)$

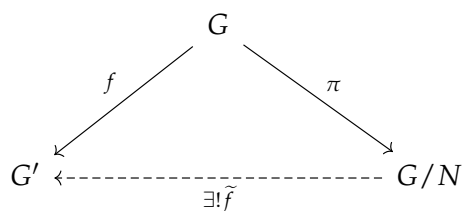
2. If $N \trianglelefteq G$, then we have a projection map $\pi : G \rightarrow G/N$ by $g \mapsto gN$, and $N = \ker \pi$. This helps show how normal subgroups are equivalent to the kernels of homomorphisms

3. Consider $S^1 = \{z \in \mathbb{C} : |z| = 1\} \leq \mathbb{C}^\times$, both of which are groups under multiplication. We have $\mathbb{C}^\times \rightarrow \mathbb{R}_{>0}$ by $z \mapsto |z|$, and $\ker \varphi = S^1$. So, $\mathbb{C}^\times / S^1 \cong \mathbb{R}_{>0}$

Universal Property of Quotient Construction

16.21

Given any group hom $f : G \rightarrow G'$ such that $N \subset \ker f$, there exists a unique map $\tilde{f} : G/N \rightarrow G'$ s.t. $\tilde{f} \circ \pi = f$. That is, the following diagram commutes.



17. Products of Groups

Definition (External Direct Products)

17.1

Given two groups G_1, G_2 , we define $G_1 \times G_2$ as a cartesian product of the sets, with the group operation defined component-wise.

Note

$\overline{G}_1 := G_1 \times \{e_2\}$, and $\overline{G}_2 := \{e_1\} \times G_2$ are normal subgroups of $G_1 \times G_2$.

Question

Given two subgroups H and K of a group G , when is HK a subgroup?

Proposition

17.2

HK is a subgroup of $G \iff HK = KH$

Proof. If $HK \leq G$, then $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$. Now, suppose $HK = KH$. Observe

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(h_3k_3)k_2 = h_4k_4$$

$$(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} = h'k'.$$

So, HK is a group □

Corollary

17.3

If $H, K \leq G$ and H or K is normal in G , then $HK \leq G$

Proof. Say $H \triangleleft G$. Then, $HK = \cup Hk = \cup kH = KH$. So, HK is a subgroup by the above proposition □

Definition (Internal Direct Products)

17.4

Let H, K be subgroups of G . Then, we say G is the internal direct product of H and K if

(i) H and K are both normal

(ii) $G = HK$

(iii) Given any $g \in G$, we can write $g = hk$ for $h \in H$ and $k \in K$ in a unique way

This definition generalizes to more than 2 subgroups.

Lemma

17.5

Suppose $G = N_1 \cdots N_k$ is an internal direct product of its subgroups $N_i \triangleleft G$. Then, for each $i \neq j$, we have $N_i \cap N_j = \{e\}$, and for $a \in N_i, b \in N_j, ab = ba$.

Proof. Suppose $x \in N_i \cap N_j$. Then, $x = e \cdots e \cdot x_i \cdot e \cdots e = e \cdots e \cdot x_j \cdot e \cdots e$, we by uniqueness of representation, $x = e$. If $a \in N_i, b \in N_j$, consider the commutator $[a, b] := aba^{-1}b^{-1}$. We then have $[a, b] = (aba^{-1})b^{-1} = a(ba^{-1}b^{-1})$. Observe $aba^{-1} \in N_j$ and $ba^{-1}b^{-1} \in N_i$ by normality. So,

the commutator lies in $N_i \cap N_j = \{e\}$. Thus, $ab = ba$. $\square$

Remark 17.6. If $N_1, \dots, N_k$ are normal subgroups of G , we need a stronger condition than $N_i \cap N_j = \{e\}$ for $i \neq j$ to ensure that the product is a direct product. Namely, we need $N_i \cap (N_1 \cdots N_{i-1} N_{i+1} \cdots N_k) = \{e\}$.

Theorem

17.7

Suppose G is the internal direct product $G = N_1 \cdots N_k$. Then, G is isomorphic to the external direct product $N_1 \times \cdots \times N_k$.

Proof. The map $\varphi : G \rightarrow N_1 \times \cdots \times N_k$ sending $x_1 \cdots x_k \mapsto (x_1, x_2, \dots, x_k)$ is well defined by uniqueness. Furthermore, φ is clearly bijective. Moreover, $\varphi((x_1 \cdots x_k)(y_1 \cdots y_k)) = \varphi(x_1 y_1 \cdots x_k y_k)$ by the previous lemma. This maps to

$$(x_1 y_1, \dots, x_k y_k) = (x_1, \dots, x_k)(y_1, \dots, y_k) = \varphi(x_1 \cdots x_k) \varphi(y_1 \cdots y_k)$$

 $\square$

Because of this theorem we do not distinguish between internal and external direct products.

Example 17.8 (On Homework). If C_n is cyclic of order n , show that if $\gcd(m, n) = 1$, then $C_m \times C_n \cong C_{mn}$.

Second Isomorphism Theorem

17.9

If M and N are subgroups of G with $N \triangleleft G$, then there is a natural isomorphism $MN/N \cong M/M \cap N$.

Proof. Let $\varphi : M \rightarrow MN/N$ map $m \mapsto mN$. Then, φ is clearly surjective, and

$$\ker \varphi = \{m \in M \mid m \in N\} = M \cap N.$$

Thus, the first isomorphism theorem gives $M/M \cap N \cong MN/N$. $\square$

Corollary

17.10

If M and N are as above and are both finite subgroups, then $|MN| = \frac{|M||N|}{|M \cap N|}$.

18. Inner Automorphisms of a Group

Let $G = GL_n(F)$. Then, for a fixed $P \in G$, we have the map $A \mapsto PAP^{-1}$, an automorphism. We want to generalize this.

Definition

18.1

Let G be a group, and $g \in G$. We define $T_g : G \rightarrow G$ by $T_g(x) = gxg^{-1}$. Then, $T_g \in \text{Aut } G$, i.e. it's an isomorphism from G to itself. We call T_g the **inner automorphism given by g** .

Note

$T_g \circ T_h(x) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = T_{gh}(x)$. So, $T_g \circ T_h = T_{gh}$.

Definition

18.2

Let $\mathcal{I}(G)$ be the group of all inner automorphisms of G , under composition. We then have a morphism $\psi : G \rightarrow \mathcal{I}(G)$ sending $g \mapsto T_g$.

What is the kernel of ψ ?

$\ker \psi = \{g \in G \mid T_g(x) = x\} = \{g \in G \mid gx = xg, x \in G\} = Z(G)$, the **center** of G . Thus,

Proposition

18.3

As $\text{Im} \psi = \mathcal{I}(G)$, we have $\mathcal{I}(G) \cong G/Z(G)$.

Example 18.4. For $G = GL_n(F)$, we showed in HW 1 that the center of $Z(G) = \{\lambda I_n : \lambda \in F^\times\} \cong F^\times$. So, $\mathcal{I}(GL_n(F)) \cong GL_n(F)/F^\times =: PGL_n(F)$. We can think of $GL_n(F)$ as linear automorphisms on F^n , and by analogy $PGL_n(F)$ are algebraic automorphisms of $P(F^n) = \mathbb{P}_F^{n-1}$, which is $n - 1$ dimensional projective space.

19. Symmetry

Let M_n be the group of all isometries or rigid motions $\mathbb{R}^n \rightarrow \mathbb{R}^n$.

Recall

Any $m \in M_n$ has representation as $m = \tau_v \circ \rho$, where $\tau_v(x) = x + v$ is a translation by v , and $\rho \in O(n)$.

Definition

19.1

Let $F \subset \mathbb{R}^n$ be a subset. A **symmetry** of F is a rigid motion m with $m(F) = F$. The set of all symmetries of F form a subgroup of M_n , which is the group of symmetries of F .

Goal

Find all possible finite groups of symmetry of plane figures.

Theorem

19.2

Let G be a finite subgroup of M_n . Then, there exists $x \in \mathbb{R}^n$ fixed by all $g \in G$, i.e. $g(x) = x$ for all $g \in G$.

Proof. Given any point $s \in \mathbb{R}^n$, consider the orbit $\mathcal{O}_s$ under the action of G . That is, $\mathcal{O}_s := \{g(s) \mid g \in G\}$. Any $g \in G$ permutes the set $\mathcal{O}_s$, since $\mathcal{O}_s$ is a finite set and g is injective on $\mathbb{R}^n$, hence is injective on $\mathcal{O}_s$.

Lemma**19.3**

Let $S := \{s_1, \dots, s_n\}$ be a finite set in $\mathbb{R}^m$. Let $p := \frac{1}{n}(s_1 + \dots + s_n)$ be the **center of gravity** of S . Then, if $s'_i = g(s_i)$ for $g \in M_n$, and $g(p) = p'$, then $p' = \frac{1}{n}(s'_1 + \dots + s'_n)$. That is, rigid motions send centers of gravity to centers of gravity.

Proof. Since $g = \tau_v \circ \rho$, it suffices to consider the 2 cases:

- (i) $g = \rho$ is linear. Then, $g(p) = g(\frac{1}{n} \sum s_i) = \frac{1}{n} \sum s'_i = p'$.
- (ii) $g = \tau_v$. Then, $\tau_v(s_i) = s_i + v$, so $\tau_v(p) = p + v = p'$.

□

Now, to prove the theorem, notice that the lemma implies any $g \in G$ fixes the center of gravity of $\mathcal{O}_s$.

□

20. Finite Subgroups of $\mathcal{O}(2)$

By the theorem, any finite subgroup of M_2 has a fixed point o . By choosing coordinates so that o is the origin, we reduce to $G \leq \mathcal{O}(2)$.

Theorem**20.1**

If G is a subgroup of $\mathcal{O}(2)$, and $|G| < \infty$, then

- (i) $G = C_n$, the cyclic group of order n generated by the rotation ρ_θ , where $\theta = 2\pi/n$
- (ii) $G = D_n$, the dihedral group of order $2n$, generated by a rotation ρ_θ for $\theta = 2\pi/n$, and a reflection r about the line through the origin 0 . We can choose coordinates so that r is a reflection $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ about the x -axis.

Corollary**20.2**

If G is a finite subgroup of M_2 , then for a suitable choice of coordinates, G becomes one of the groups C_n or D_n , where C_n is generated by $\rho_{2\pi/n}$, and D_n by $\rho_{2\pi/n}$ and r . When $n \geq 3$, D_n is the group of symmetries of an n sided regular polygon.

Example 20.3. 1. $C_1 = \{1\}$, $D_1 = \{1, r\}$, $C_2 = \{1, \rho_\pi\}$, $D_2 = \{1, \rho_\pi, r, \rho_\pi \circ r\} \cong V_4$

Proposition**20.4**

D_n is generated by two elements x and y satisfying the relations $x^n = 1$, $y^2 = 1$, and $yx = x^{-1}y$. The elements of D_n are exactly $\{1, x, x^2, \dots, x^{n-1}, xy, x^2y, \dots, x^{n-1}y\}$, so $|D_n| = 2n$.

Proof. We let $x = \rho_{2\pi/n}$ and $y = r$. Clearly, x, y satisfy the given relations...

□

Exercise

If $x = \begin{cases} 1 \rightarrow 3 \\ 2 \rightarrow 1 \\ 3 \rightarrow 2 \end{cases}$ and $y = \begin{cases} 1 \rightarrow 2 \\ 2 \rightarrow 1 \\ 3 \rightarrow 3 \end{cases}$ are in S_3 , check that $x^3 = 1$, $y^2 = 1$, and $yx = x^{-1}y$, hence $D_3 \cong S_3$

Proof. Proof of [Theorem 20.1](#). Let $G \leq O(2)$, $|G| < \infty$.

Case 1: $G \leq SO(2)$, i.e. all elements in G are rotations. If $G = \{1\}$, we're ok, so assume G is non-trivial. Let $\theta = \min\{\alpha > 0 \mid \rho_\alpha \in G\}$, which exists as G is finite. Then, $G = \langle \rho_\theta \rangle$. [Indeed, if $\rho_\alpha \in G$, then $\alpha = n\theta + \beta$, where $0 \leq \beta < \theta$. So, $\rho_\beta = \rho_\alpha(\rho_\theta)^{-n} \in G \implies \beta = 0$ by definition of θ .] Thus, G is a finite cyclic group C_n .

Case 2: G contains an element of the form $\rho_\theta \circ r$. Since $\rho_\theta \circ r = \begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix}$ has a square of 1, it must be a reflection as it is orthogonal. In fact, check that $\rho_\theta \circ r \begin{pmatrix} \cos(\theta/2) \\ \sin(\theta/2) \end{pmatrix} = \begin{pmatrix} \cos(\theta/2) \\ \sin(\theta/2) \end{pmatrix}$, so $\rho_\theta r$ is a reflection about the line $\langle \begin{pmatrix} \cos(\theta/2) \\ \sin(\theta/2) \end{pmatrix} \rangle$. Adjusting coordinates if necessary, we may assume $r \in G$. Let $H := G \cap SO(2)$, the subgroup of rotations in G . By case 1, we get that H is cyclic, generated by ρ_θ where $\theta = 2\pi/n$. Hence G contains all products $\rho_\theta^i r^j$ for $0 \leq i < n$, $0 \leq j < 2$, so $D_n \subset G$. Now, if x is an arbitrary orientation reversing element of G , then $xr \in SO(2) \cap G = H$, so $x \in H_r \subset D_n$. Thus, $G = D_n$. $\square$

Theorem**20.5**

Every finite subgroup of $SO(3)$ is one of the following:

1. The cyclic group C_n of rotations by multiples of $2\pi/n$ about a line through the origin.
2. The dihedral group D_n
3. The tetrahedral group of 12 rotations carrying a regular tetrahedron to itself. (A_4)
4. The octahedral group of 24 rotations of a cube or regular octahedron (S_4)
5. The icosahedral group of 60 rotations of a regular dodecahedron or icosahedron. (A_5)

In every dimension, the tetrahedron generalizes to the simplex, the cube generalizes to the hypercube, and the regular octahedron generalizes to the convex hull $\langle \pm e_1, \dots, \pm e_n \rangle$.

Remark 20.6. *The tetrahedron, cube, and octahedron have analogous forms in all dimensions. The only other regular polytopes are*

1. *Dimension 3: case (5)*
2. *Dimension 4: (Schläfli, 1842) The 24-cell, 120-cell, 600-cell, bounded by 24 octahedra, 120 dodecahedra, and 600 tetrahedra respectively.*
3. *That's it lol*

21. Group Actions

Definition (Group Actions)

21.1

Let G be a group and X be a set. We say that G **acts on** X (on the left) if there exists a map $G \times X \rightarrow X$, given by $(g, x) \mapsto g \cdot x$, satisfying

- (i) $e \cdot x = x$ for all $x \in X$
- (ii) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ for all $g_1, g_2 \in G, x \in X$.

We also say that X is a G -set.

Example 21.2. 1. The group M_2 of rigid motions of the plane $\mathbb{R}^2$ acts on the set of points, the set of lines, the set of triangles, etc.

2. Any group G acts on itself by

- Left multiplication
- Conjugation (inner automorphisms)

3. If H is a subgroup of G , then G acts naturally on G/H by $g \cdot (xH) = gxH$.

4. For any set X , $S(X)$ acts on X .

5. The group G of rotational symmetries of the cube acts on the set of (1) faces of the cube; (2) edges of the cube; (3) vertices of the cube.

6. Suppose X is a connected manifold with universal covering space $p : \tilde{X} \rightarrow X$. Fix a base point $x \in X$. Then the fundamental group $\pi_1(x)$ acts on $p^{-1}(x)$. For example, $p : \mathbb{R} \rightarrow S^1, \theta \mapsto e^{2\pi i \theta} \dots$

7. Suppose K is a finite field extension of $\mathbb{Q}$. We have a ring of "integers" $\mathcal{O}_K$ in K such that $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. Any prime ideal $\mathcal{P}$ of $\mathcal{O}_K$ lies above a rational prime $p \in \mathbb{Z}$ if $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$. For any $p \in \mathbb{Z}$, there exist finitely many prime ideals $\mathcal{P}_1, \dots, \mathcal{P}_r$ above p . If $K/\mathbb{Q}$ is a Galois extension, then the Galois group G acts transitively on the set of these r prime ideals. For example, $K = \mathbb{Q}(\zeta_n)$, and then $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$, and the Galois group is $G = (\mathbb{Z}/n\mathbb{Z})^\times$.

Permutation Representations

21.3

Let G be a group and X be a set. There is a 1 – 1 correspondence between actions of G on X and group homomorphisms $G \rightarrow S(X)$. Such homomorphisms are called **permutation representations** of G

Proof. If G acts on X , then for any $g \in G$, define $\eta_g \in S(X)$ by $\eta_g(x) := g \cdot x$. Check that η_g is a bijection and the map $g \mapsto \eta_g$ is a group homomorphism $G \rightarrow S(X)$. Conversely, given a group homomorphism $\varphi : G \rightarrow S(X)$, we define an action of G on X by $g \cdot x = \varphi(g)(x)$. Check that these two processes are inverse to each other. $\square$

Definition

21.4

A G -action is **faithful** if the corresponding map $G \rightarrow S(X)$ is injective. This means that $g \cdot x = x \ \forall x \in X \implies g = e$.

Cayley's Theorem

21.5

Every group G is isomorphic to a subgroup of $S(G)$. In particular, if $|G| = n$, then $G \leq S_n$

Proof. Note that the action of G on itself by left multiplication is faithful, so we get an injection $G \hookrightarrow S(G)$. $\square$

Definition

21.6

Let X be a G -set. Then, for any $x \in X$, the **orbit** of x , denoted $\mathcal{O}_x$, is the set $\mathcal{O}_x = \{gx \mid g \in G\}$. $\mathcal{O}_x$ is itself a G -set. Furthermore, the orbits for a G -action are equivalence classes for the equivalence relation $x \sim y \iff x = gy$ for some $g \in G$.

Proposition

21.7

The orbits of X partition the set X . Every $x \in X$ lies in exactly one orbit, namely $\mathcal{O}_x$.

Definition

21.8

If X consists of just one orbit, we say that G acts transitively on X . So, this occurs if and only if $\forall x, y \in X, \exists g \in G$ such that $y = g \cdot x$.

Definition

21.9

If $x, y \in X$ lie in the same G -orbit, we often say they are **conjugates** under the G -action.

Definition

21.10

For $x \in X$, the **stabilizer** G_x of x is the subgroup $G_x := \{g \in G \mid g \cdot x = x\}$

Theorem

21.11

- (a) If X is a transitive G -set and $x \in X$, then there is a natural bijection $\varphi : G/G_x \rightarrow X$ which maps $gG_x \mapsto g \cdot x$, which is compatible with the G -action, that is $\varphi(gC) = g \cdot \varphi(C)$ for every coset C . Thus, G/G_x and X are isomorphic as G -sets. In particular for an arbitrary G -action, we have $G/G_x \cong \mathcal{O}_x$ for any $x \in X$.
- (b) If X is any G -set, then $G_{gx} = gG_xg^{-1}$ for all $g \in G, x \in X$. So, the stabilizer subgroups of points belonging to the same G -orbit are conjugate.

Proof.

(a)

$gG_x = g'G_x \iff g^{-1}g' \in G_x \iff g^{-1}g'(x) = x \iff g \cdot x = g' \cdot x$. This shows φ is well defined and injective. If $y \in X$, there exists $g \in G$ such that $y = g \cdot x$ by transitivity, so $y = \varphi(g \cdot G_x)$, thus φ is surjective. Finally, it's easy to check that φ respects the G -action.

(b)

$$G_{gx} = \{u \in G \mid ugx = gx\} = \{u \in G \mid (g^{-1}ug)x = x\} = \{u \in G \mid g^{-1}ug \in G_x\} = gG_xg^{-1} \quad \square$$

Example 21.12. 1. Let M be the group of rigid motions of $\mathbb{R}^2$. If $p \in \mathbb{R}^2$ is any point, then $M_p =$

$$M_{\tau_p(0)} = \tau_p M_0 \tau_p^{-1} = \tau_p O(2) \tau_p^{-1}, \text{ by part (b)}$$

2. **(Exercise)** Let $h = \{z \in \mathbb{C} \mid \operatorname{Im}(z) > 0\}$ be the upper half plane in $\mathbb{C}$, and $G = SL_2(\mathbb{R})$.

For $g \in \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, we let $g \cdot z = \frac{az+b}{cz+d}$. Check that this defines a transitive G -action on h .

The stabilizer subgroup of $i = \sqrt{-1}$ is $K := G_i := \left\{ \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \mid \theta \in \mathbb{R} \right\}$. Therefore,

$$h \cong SL_2(\mathbb{R})/K$$

Corollary

21.13

For any G -action on a finite set X , we have the counting formulas:

$$|X| = \sum_{\text{orbits}} |\mathcal{O}_x| = \sum |G : G_x|,$$

where the sum is over distinct orbits, and

$$|\mathcal{O}_x| = |G|/|G_x| \iff |G| = |\mathcal{O}_x| \cdot |G_x|, \forall x \in X$$

Example 21.14. 1. A group is **simple** if its only normal subgroups are $\{e\}$ and itself. If H is any proper subgroup of a simple group G , we get an injection $G \hookrightarrow S_k$, where $k = |G : H|$ (Just consider the G -action on the coset space $G/H \iff$ a map $G \rightarrow S(G/H)$)

2. **Check:** If H and K are subgroups of G , then the G -sets G/H and G/K are isomorphic if and only if H and K are conjugate subgroups of G .

3. Suppose G is a finite group and H and K are two subgroups of G . We compute $|HK|$. Consider $X := G/K$ and consider the action of H on X by left multiplication. Then, the orbit of K in G/K under the H -action is HK . Therefore, $|HK| = |K| \cdot (\# \text{ of } H\text{-cosets that lie in this orbit})$. The stabilizer H_K of the coset K is $H \cap K$, hence the orbit in question includes $|H : H \cap K|$ cosets of K . Thus, $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$

22. Conjugacy Classes in G ; The Class Equation

Recall the conjugation action of a group G on itself is defined by $g \cdot x = gxg^{-1}$.

Definition

22.1

The stabilizer of an element $x \in G$ under the action of conjugation is called the **centralizer** of x , denoted $Z(x)$. That is, $Z(x) = \{g \in G \mid gx = xg\}$.

Definition

22.2

The orbit $\mathcal{O}_x$ of x under the G -action is the **conjugacy class** $C_x = \{y \in G \mid y = gxg^{-1} \text{ for some } g \in G\}$

The Class Equation

22.3

By the counting formula, $|G| = |Z(x)| \cdot |C_x|$, so $|C_x| = |G : Z(x)|$

We also have the **class equation**: let $x_1, \dots, x_n$ be all the representatives of distinct conjugacy classes, then

$$|G| = \sum_{i=1}^n |C_{x_i}| = \sum_{i=1}^n |G : Z(x_i)|.$$

Furthermore, any element in the center of G only has itself in the orbit. Therefore, we can let $g_1, \dots, g_m$ be all representatives of non-central conjugacy classes, and then

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

Note by assumption that $|G : Z(g_i)| \geq 2$.

Remark 22.4. All the integers on the right hand side of the class equation divide $|G|$, and $|Z(G)| \geq 1$.

Example 22.5. $G = D_3$ has conjugacy classes $\{1\}, \{r, r^2\}, \{s, sr, sr^2\}$. The class equation is $6 = 1 + 2 + 3$.

Example 22.6. If X is the set of nilpotent matrices in $M_n(F)$ and $G = GL_n(F)$ acting on X by conjugation, then the G -orbits are given by Jordan canonical form. We'll prove this later.

Definition

22.7

A group G is a **p -group** if $|G| = p^k$, p prime.

Proposition

22.8

The center $Z(G)$ of any p -group G is non-trivial.

Proof. If $Z(G) = \{1\}$, then the class equation for G reads $p^k = |G| = 1 + \sum |G : Z(g_i)|$, but $|G : Z(g_i)| = p^{k_i}$ for some $k_i > 1$, which is a contradiction. $\square$

Corollary

22.9

Every group of order p^2 for a prime p is abelian.

Proof. Suppose $|G| = p^2$. If $Z(G) = G$, then G is abelian. Otherwise, we have $|Z(G)| = p$. Let $x \in G$, and we'll show $Z(x) = G$. If $x \in Z(G)$, we're ok, and otherwise we have $1 \subsetneq Z(G) \subsetneq Z(x)$, which implies $Z(x) = G$. $\square$

Corollary

22.10

If $|G| = p^2$, then

- (i) $G = C_{p^2}$ is cyclic, or
- (ii) $G = C_p \times C_p$

Proof. We know that G is abelian. If G contains an element of order p^2 , then G is cyclic. Otherwise,

the order of any non-identity element x of G is p , so pick $x \neq 1$, set $H_1 = \langle x \rangle$. Pick $y \in G \setminus H_1$, and $H_2 = \langle y \rangle$. Then, $H_1 \trianglelefteq G$ and $H_2 \trianglelefteq G$ by G being abelian. Furthermore, $H_1 \cap H_2 = \{1\}$, and since $H_1 \subsetneq H_1 H_2$, we have $H_1 H_2 = G$. So, $G \cong H_1 \times H_2 = C_p \times C_p$. $\square$

Remark 22.11. Groups of order p^3 are more complicated

There is $C_{p^3}, C_{p^2} \times C_p, C_p \times C_p \times C_p$, which are distinct. However, there are also some non-abelian groups. In fact, for any prime p , there are exactly two non-isomorphic non-abelian groups of order p^3 .

Example 22.12 ($p = 2$). When $p = 2$, there are 2 non-abelian groups of order 8. They are the dihedral group D_4 , and the **quaternion group** $Q = \{\pm 1, \pm i, \pm j, \pm k \mid (-1)x = -x, i^2 = j^2 = k^2 = ijk = -1\}$. Q has only one element of order 2, so $Q \not\cong D_4$.

Here is a presentation of Q using matrices: Let $a = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then, $a^4 = 1, a^2 = b^2$, and $ba = a^3b$. We get that $Q = \langle a, b \rangle$. Prove this classification as an **exercise**.

If p is odd, then the non-abelian groups of order p^3 are

$$\text{Heis}(\mathbb{Z}/p\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}$$

$$G_p = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{Z}/p^2\mathbb{Z}, a \equiv 1 \pmod{p} \right\}$$

Note that when $p = 2$, the Heisenberg group and G_2 are both isomorphic to D_4 .

23. Conjugacy Action of G on Subgroups

G acts on the set $X = \{\text{subgroups of } G\}$ by conjugation: $g \cdot H := gHg^{-1}$.

Definition

23.1

The stabilizer of a subgroup H under this action is $G_H = \{g \in G \mid gHg^{-1} = H\}$, which we call the **normalizer** $N_G(H)$.

Remark 23.2. Clearly, $H \triangleleft N(H)$, and one can check that $N(H)$ is the largest subgroup of G which contains H as a normal subgroup.

Corollary

23.3

The number of conjugate subgroups of H equals the index of the normalizer $N_G(H)$ in G .

Notation

If G acts on a set X , then let X^G denote the set of fixed points $\{x \in X \mid gx = x\}$. Then, $|X| = |X^G| + \sum_{|\mathcal{O}_i| > 1} |\mathcal{O}_i| = |X^G| + \sum_{G_{x_i} \neq G} |G : G_{x_i}|$

24. The Sylow Theorems

The Sylow theorems give a partial converse to Lagrange's theorem.

Definition

24.1

Suppose $|G| = p^r m$, where $\gcd(p, m) = 1$. A **p -Sylow subgroup** of G is a subgroup of order p^r . A subgroup of G is called a **Sylow subgroup** if it is a p -Sylow subgroup for some p dividing $|G|$.

First Sylow Theorem

24.2

For every prime p dividing $|G|$, G has a p -Sylow subgroup.

Proof. Let $|G| = p^r m$, $r \geq 1$ and $p \nmid m$. Let X be the collection of all subsets of G of cardinality p^r . That is, $X := \{A \subset G : |A| = p^r\}$. G acts on X by left multiplication $A \mapsto g \cdot A$.

Lemma

24.3

The cardinality $|X| = \binom{p^r m}{p^r} \not\equiv 0 \pmod{p}$.

Proof.

$$\binom{p^r m}{p^r} = \frac{p^r m (p^r m - 1) \cdots (p^r m - p^r + 1)}{p^r \cdot (p^r - 1) \cdots 1}$$

Note that for each integer k with $0 \leq k < p^r$, $p^i \mid (p^r m - k) \iff p^i \mid (p^r - k)$. (Indeed, if we write $k = p^j l$, $j < r$, $p \nmid l$, then $p^r m - k = p^r m - p^j l = p^j (p^{r-j} m - l)$). This implies that all powers of p in the numerator are exactly canceled by the powers of p in the denominator. $\square$

Now, write X as a union of G -orbits $\mathcal{O}$. Then, $|X| = \sum |\mathcal{O}|$. Since $p \nmid |X|$, there exists some orbit $\mathcal{O}$ with $|\mathcal{O}| \not\equiv 0 \pmod{p}$. Let $A \in \mathcal{O}$ be a subset of $\mathcal{O}$ with $1 \in A$. (Such an A lies in every orbit). Consider G_A . We have $G_A \subset G_A \cdot A = A \implies |G_A| \leq |A| = p^r$. On the other hand, $|G| = |\mathcal{O}| \cdot |G_A|$. So, as $p \nmid |\mathcal{O}|$, we must have $p^r \mid |G_A|$, showing $|G_A| \geq p^r$. Hence, $|G_A| = p^r$, so G_A is a p -Sylow subgroup. $\square$

Remark 24.4. A variant of this argument shows that G has a subgroup of order p^i for each $i \in \{1, \dots, r\}$.

Corollary (Cauchy's Theorem)

24.5

If p divides $|G|$, then G contains an element of order p .

Proof. Let H be a p -Sylow subgroup of G , and $x \in H$, $x \neq 1$. Then, $|x| = p^k$ for some $k \geq 1$. Hence, $(x^{p^{k-1}})^p = x^{p^k} = 1$, and by minimality of order $x^{p^{k-1}} \neq 1$, showing $|x^{p^{k-1}}| = p$. $\square$

Second Sylow Theorem

24.6

Any two p -Sylow subgroups of G are conjugate.

Proof. We'll show something stronger: Let $H \leq G$ be any p -subgroup of G and P be a p -Sylow subgroup. We claim that there exists $x \in G$ such that $H \subset xPx^{-1}$.

Consider G/P , the set of all P cosets xP in G , and the left H -action on G/P by $h \cdot xP = hxP$ for all $xP \in G/P$. By the counting formula, recalling $|G| = m \cdot p^r = m|P|$, we get that

$$m = |G/P| = |(G/P)^H| + \sum_{H_i \neq H} |H : H_i|.$$

Since H is a p -group all $|H : H_i|$ are non trivial powers of p . So, modulo p , this implies $0 \not\equiv m \equiv |(G/P)^H| \pmod{p}$. We deduce in particular that $(G/P)^H$, the set of H -fixed points, is not empty. So, there exists xP fixed by all $h \in H$. That is,

$$hxP = xP \implies x^{-1}hx \in P \implies h \in xPx^{-1} \implies H \subset xPx^{-1}$$

□

Corollary**24.7**

- (i) All Sylow p -subgroups of G are isomorphic
- (ii) Let P be a p -Sylow subgroup. Then, $P \triangleleft G \iff P$ is the unique p -Sylow subgroup.
- (iii) The number of p -Sylow subgroups is $|G : N_G(P)|$, where P is a p -Sylow subgroup, and note that $|G : N_G(P)|$ divides $|G|$.
- (iv) Any p -group in G is contained in a p -Sylow subgroup.

Corollary**24.8**

Let p be a prime, and let $|G|_p$ denote the highest power of p that divides $|G|$. Then, the number of p -Sylow subgroups of G divides $|G|/|G|_p$.

Proof. We know that the number of p -Sylow subgroups of G is $|G : N_G(P)|$, where P is any one of them. Moreover, $|G : N_G(P)| \cdot |N_G(P) : P| = |G : P| = |G|/|P| = |G|/|G|_p$. Thus, $|G : N_G(P)|$ divides $|G|/|G|_p$ as desired. □

Corollary**24.9**

Any element of order p in G is contained in some p -Sylow subgroup.

Third Sylow Theorem**24.10**

The number of p -Sylow subgroups is $\equiv 1 \pmod{p}$.

Proof. Let X be the set of all p -Sylow subgroups, and let P be one of them. Then, P acts on X by conjugation, and for this action, we have $|X| \equiv |X^P| \pmod{p}$ by the counting formula (recall that all the other terms are divisible by p). We claim that $|X^P| = 1$, in other words $X^P = \{P\}$.

Indeed, suppose $Q \in X^P$, so $xQx^{-1} = Q$ for all $x \in P$. That is, $P \subset N_G(Q)$. Now, Q is a p -Sylow subgroup of $N_G(Q)$, and $Q \trianglelefteq N_G(Q)$. Hence, $P = Q$. □

Note that the number of p -Sylow subgroups must be $1 \pmod{p}$ and must divide the order of $|G|$, which is a fairly strong condition.

Example 24.11. Every group of order 15 is cyclic:

Proof. The number of 3-Sylow subgroups divides $15/3 = 5$ and is $\equiv 1 \pmod{3}$, so there exists a unique 3-Sylow subgroup H . Similarly, the number of 5-Sylow subgroups divides $15/5 = 3$ and is $\equiv 1 \pmod{5}$, so there's a unique 5-Sylow subgroup K . The uniqueness implies $H, K \trianglelefteq G$, and clearly $H \cap K = 1, HK = G$, so $G \cong H \times K \cong C_3 \times C_5 \cong C_{15}$. $\square$

This generalizes to groups of order pq with $q \not\equiv 1 \pmod{p}$.

Example 24.12. Any finite abelian group is the direct product of its Sylow subgroups.

Proof. If $P_1, \dots, P_k$ are the distinct Sylow subgroups of an abelian group A , then $P_1, \dots, P_k \trianglelefteq A$ by A being abelian. Moreover, $P_i \cap (P_1 \cdots \widehat{P_i} \cdots P_k) = 1$ by order considerations, for all $i = 1, \dots, k$. Furthermore, $P_1 P_2 \cdots P_k = A$, also by cardinality considerations. So, $G = P_1 \times \cdots \times P_k$. $\square$

Later: we'll classify all finite abelian groups.

25. The Symmetric Group

Recall that $S_n = S(\{1, \dots, n\})$, with order $n!$.

Definition

25.1

A permutation $\sigma \in S_n$ is a **cycle of length r** , or an **r -cycle** if there exists distinct integers $a_1, \dots, a_r \in [1, n]$ such that $\sigma(a_i) = a_{i+1}$ for $i < r$, and $\sigma(a_r) = a_1$, while $\sigma(x) = x$ for all $x \notin \{a_1, \dots, a_r\}$. We write $\sigma = (a_1 \cdots a_r)$, and we note that any r -cycle can be written like this in r different ways. We say that two cycles are **disjoint** if no number is moved by both of them.

Proposition

25.2

Any two disjoint cycles commute. Moreover, any $\sigma \in S_n$ has a (unique) decomposition as a product of disjoint cycles.

Proof. (Sketch): Given any $w \in S_n$, we consider the subgroup $\langle w \rangle$ generated by w . The cycles in the decomposition of w correspond to the orbits of the $\langle w \rangle$ -action on the set $\{1, 2, \dots, n\}$. $\square$

Example 25.3. $\sigma = 46835217 \in S_8$ has cycle decomposition $(14387)(26)$.

Definition

25.4

A **transposition** in S_n is any 2-cycle (ij) .

Proposition

25.5

Every $w \in S_n$ is a product of (not necessarily disjoint) transpositions (in a non-unique way)

Proof. Any r -cycle $(a_1 \cdots a_r)$ satisfies $(a_1 \cdots a_r) = (a_1 a_r)(a_1 a_{r-1}) \cdots (a_1 a_2)$. $\square$

Definition

25.6

A permutation is **even** if it can be written as a product of an even number of transpositions. Otherwise, it is **odd**.

We'll prove that this notion is well defined.

26. Conjugacy in S_n **Proposition**

26.1

Let $\sigma, \tau \in S_n$, and suppose that σ has cycle decomposition

$$\sigma = (a_1 a_2 \cdots a_{k_1})(b_1 b_2 \cdots b_{k_2}) \cdots$$

Then, $\tau\sigma\tau^{-1} = (\tau(a_1) \cdots \tau(a_{k_1}))(\tau(b_1) \cdots \tau(b_{k_2}))$, hence two elements of S_n are conjugate if and only if their cycle decompositions have the same orders (i.e. σ and τ have the same cycle type). The number of conjugacy classes in S_n equals the number of integer partitions of n .

Proof. It suffices to check that $\tau(ij)\tau^{-1} = (\tau(i)\tau(j))$ for any transposition (ij) (easy). Alternatively, observe that if $\sigma(a) = b$, then $\tau\sigma\tau^{-1}(\tau(a)) = \tau(b)$. Hence, if the pair "ab" appears in the cycle decomposition of σ , then the pair $\tau(a)\tau(b)$ appears in the cycle decomposition of $\tau\sigma\tau^{-1}$. $\square$

Corollary

26.2

If $n \geq 3$, then $Z(S_n)$ is trivial.

Example 26.3 (Class Equation for S_4). The conjugacy classes are 1, the 6 transpositions, the 3 transposition products, the 8 three cycles, and the 6 four cycles. So, $|S_4| = 24 = 1 + 3 + 6 + 6 + 8$

Back to the proof that "even" and "odd" are well defined.

Proof. We consider the Vandermonde product $\Delta(x) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$, where $x_1, \dots, x_n$ are variables. If $f(x_1, \dots, x_n)$ is any polynomial in $x_1, \dots, x_n$, the symmetric group S_n acts on f by permuting the variables. That is, $\sigma \cdot f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$. So, observe

$$\sigma\Delta = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}) = \pm\Delta. \text{ Now, define } \varphi : S_n \rightarrow \{\pm 1\} \text{ by } \varphi(\sigma) = \begin{cases} +1 & \sigma\Delta = +\Delta \\ -1 & \sigma\Delta = -\Delta \end{cases}.$$

We claim φ is a group homomorphism. Indeed, $(\sigma\tau)(\Delta(x)) = \prod_{1 \leq i < j \leq n} (x_{\sigma\tau(i)} - x_{\sigma\tau(j)}) = \sigma \left(\prod_{1 \leq i < j \leq n} (x_{\tau(i)} - x_{\tau(j)}) \right)$. It follows that $\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau)$.

Next, we claim that for any transposition $\tau = (ab)$, $\tau(\Delta) = -\Delta$. This is obvious when $\tau = (12)$, and in general, if $\tau = (ab)$, let $w \in S_n$ be any element such that $w(1) = a, w(2) = b$. Then, $w(12)w^{-1} = (ab)$. Since φ is a homomorphism, it follows that

$$\varphi(ab) = \varphi(w)\varphi(12)\varphi(w)^{-1} = \varphi(12) = -1$$

Finally, if $\sigma \in S_n$ is any permutation, and $\sigma = \tau_1 \cdots \tau_k$, where each τ_i is a transposition, then $\varphi(\sigma) = \varphi(\tau_1) \cdots \varphi(\tau_k) = (-1)^k$, hence the parity of k depends only on σ . $\square$

Definition

26.4

The **alternating group** $A_n = \ker \varphi$, i.e. the group of all even permutations in S_n .

Proposition

26.5

$|S_n : A_n| = 2$, and $A_n \trianglelefteq S_n$.

Simplicity of A_5 (Galois)

26.6

A_5 is a simple group.

Proof. We have $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$. The number of Sylow 5-subgroups of A_5 is a divisor of $60/5 = 12$ and is $\equiv 1 \pmod{5}$. Since any 5-cycle in A_5 generates a Sylow 5-subgroup, we see that the number of Sylow 5-subgroups is 6. Hence, the number of elements of order 5 in A_5 is $6 \cdot (5 - 1) = 24$. These are the 5-cycles $(1xyzw)$ where $xyzw$ is a permutation of 2345.

Similarly, A_5 could have 1, 4, or 10 Sylow 3-subgroups, and by inspection we see the number is 10. These 10 subgroups give $10 \cdot (3 - 1) = 20$ elements of order 3 in A_5 .

Choose $i \in \{1, \dots, 5\}$, let $\{a, b, c, d\} = \{1, 2, 3, 4, 5\} \setminus \{i\}$, and define

$$V_i := \{1, (ab)(cd), (ac)(bd), (ad)(bc)\} \leq A_5.$$

Each V_i is a Sylow 2-subgroup of A_5 , and $V_i \cap V_j = \{1\}$ for $i \neq j$, and by inspection $\sigma V_i \sigma^{-1} = V_{\sigma(i)}$ for all $\sigma \in A_5$. Therefore, $V_1, \dots, V_5$ are the only Sylow 2-subgroups of A_5 . It also follows that A_5 has $5 \cdot (4 - 1) = 15$ elements of order 2. One checks (exercise) that any 2 such elements of A_5 are conjugate to each other.

Now, let $N \trianglelefteq A_5$ be nontrivial. If N contains an element x of order 5, then it contains the Sylow 5-subgroup generated by x , hence (since N is normal) all of the Sylow 5-subgroups of A_5 are in N . That is, N either contains all 24 elements of order 5 or none of them. Similarly, N contains all 20 elements of order 3 or none of them, and N contains all 15 elements of order 2 or none of them. But then the cardinality is $1 + |X|$, where X is a nonempty subset of $\{15, 20, 24\}$. Also, $|N|$ divides 60, so we deduce that $|N| = 60$, thus $N = A_5$. $\square$

27. Finite Simple Groups

Lemma

27.1

A_5 is the only nontrivial proper normal subgroup of S_5 .

Proof. Suppose $H \trianglelefteq S_5, \{1\} \neq H \neq S_5$. If $H \neq A_5$, then $H \not\subseteq A_5$ because A_5 is simple, so $HA_5 = S_5$. The second isomorphism theorem gives $HA_5/H \cong A_5/(H \cap A_5)$. Therefore, $H \cap A_5$ is a proper normal subgroup of A_5 , hence $H \cap A_5 = \{1\}$. It follows that $|HA_5|/|H| = |A_5|$, hence $|H| = 2$. But, no subgroup of order 2 in S_5 can be normal. $\square$

Theorem

27.2

Any simple group of order 60 is isomorphic to A_5 .

Proof. Let G be a simple group of order 60. If G has a subgroup H with index $|G : H| = n$, then the left action of G on G/H gives a homomorphism from G to $S(G/H) \cong S_n$. Since G is simple, $\ker \varphi = 1$ or G , but clearly $\ker \varphi$ can't be G . So, φ is injective. Thus, if $n \leq 4$, then $|S_n| \leq 24 < 60$, so G couldn't be a subgroup of S_n . We deduce that $H = G$ or $|G : H| \geq 5$.

We now claim that G has a subgroup of index 5, and hence G is isomorphic to a subgroup of S_5 . This claim will prove the theorem, since G would have index 2 in S_5 , hence $G \trianglelefteq S_5$, and we use the lemma.

Suppose G does not have a subgroup of index 5. The number of Sylow 2-subgroups of G divides $60/4 = 15$. Since this number equals $|G : N(P)|$ for any Sylow 2-subgroup P , by our hypothesis, and the previous analysis, we deduce that the number is exactly 15. Let H_1 and H_2 be distinct 2-Sylow subgroups of G , and suppose there exists $1 \neq t \in H_1 \cap H_2$. Then, $|Z(t)| > 4$, because H_1 and H_2 are distinct and abelian, both contained in $Z(t)$. Also 4 divides $|Z(t)|$ since $H_1 \subset Z(t)$. It follows that $|G : Z(t)| \leq 5$. Previous analysis and our assumption shows that $Z(t) = G$, but then $t \in Z(G)$, so G has a nontrivial center, contradicting the fact that G is simple. Therefore, no two of the 15 2-Sylow subgroups of G have a non-trivial element in common. Hence, G has $15 \cdot (4 - 1) = 45$ elements of order 2 or 4. But, G is simple, so G must have more than 1 5-Sylow subgroup, this G has 6 5-Sylow subgroups, and hence 24 elements of order 5. Bad! $\square$

Remark 27.3. *It is a relatively easy (and tedious) exercise to show that the only simple groups of order < 60 are the cyclic groups of prime order. Hence, A_5 is the smallest non-abelian simple group. The non-abelian finite simple group of next smallest order is $PSL_2(\mathbb{F}_7)$, which has order 168. (Note: $A_5 \cong PSL_2(\mathbb{F}_5) \cong PSL_2(\mathbb{F}_4)$)*

Classification of Finite Simple Groups, 1984, 15000 pages

27.4

1. $(\mathbb{Z}/p\mathbb{Z}, +)$, p prime
2. A_n , $n \geq 5$
3. Finite groups of Lie type, such as $PSL_2(\mathbb{Z}/p\mathbb{Z})$, $p \geq 5$ prime.
4. 26 others, known as **sporadic groups**. The smallest is the Mathieu group M_{11} of order 7920, and the largest is the monster group of order $\sim 10^{53}$

Definition

27.5

A **composition series** for a group G is a normal series $1 = G_s \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$ such that each G_{i+1} is a maximal proper normal subgroup of G_i , i.e. G_i/G_{i+1} is a nontrivial simple group for all $i \geq 1$. These quotient groups are the **composition factors** of the series.

Remark 27.6. *Clearly, finite groups have a composition series.*

Jordan-Hölder Theorem

27.7

Let G be a finite group and $1 = G_s \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$ and $1 = H_t \triangleleft \cdots \triangleleft H_1 \triangleleft H_0 = G$ be two composition series for G . Then, $s = t$, and there exists a permutation $i \rightarrow j$ of $[1, s]$ such that $G_i/G_{i+1} \cong H_j/H_{j+1}$ for all $1 \leq i \leq s$. Thus, the composition factors G are determined up to isomorphism.

Proof. We prove this by induction on $|G|$. This is trivial for groups of small order. We have to cases:

1. $G_1 = H_1$: The claim is clear by induction
2. $G_1 \neq H_1$:

Since $G_1, H_1 \triangleleft G$, we have $G_1 H_1 \triangleleft G$. As $G_1 \subsetneq G_1 H_1$, we have $G_1 H_1 = G$ by maximality of G_1 as a normal subgroup. So, by the 2nd isomorphism theorem, we get $G/G_1 \cong H_1/(G_1 \cap H_1)$ and similarly $G/H_1 \cong G_1/(G_1 \cap H_1)$. Let $K_2 := G_1 \cap H_1$. Then, K_2 is a maximal normal subgroup of both G_1 and H_1 . Let $1 = K_u \triangleleft \cdots \triangleleft K_3 \triangleleft K_2$ be a composition series for K_2 . We then have the following 4 composition series:

- (i) $G_s \triangleleft \cdots \triangleleft G_2 \triangleleft G_1 \triangleleft G_0 = G$
- (ii) $K_u \triangleleft \cdots \triangleleft K_2 \triangleleft G_1 \triangleleft G_0 = G$
- (iii) $K_u \triangleleft \cdots \triangleleft K_2 \triangleleft H_1 \triangleleft H_0 = G$
- (iv) $H_t \triangleleft \cdots \triangleleft H_2 \triangleleft H_1 \triangleleft H_0 = G$

By our first case above, we compare (i) and (ii), and (iii) and (iv) to see that $s = u = t$. Moreover, we have the same composition factors with each pair. But the latter is also true between (ii) and (iii), since the first 2 composition factors $G/G_1, G_1/K_2$ or (ii), $H_0/H_1, H_1/K_2$ for (iii), which are isomorphic to each other. $\square$

Definition

27.8

A finite group G is **solvable** if the simple factors in any composition series of G are cyclic groups of prime order.

Example 27.9. 1. Any abelian group is solvable

2. S_4 is solvable, which has a composition series $1 \triangleleft C_2 \triangleleft V \triangleleft A_4 \triangleleft S_4$.
3. S_n is not solvable for $n \geq 5$, having composition series $1 \triangleleft A_n \triangleleft S_n$

Feit-Thompson, 1963, 255 pages

27.10

If $|G|$ is odd, then G is solvable. In particular, any non-abelian simple group must have even order.

Question

If N_1 and N_2 are simple groups, how many groups G have $N_1 \leq G$ and $G/N_1 \cong N_2$?

This is too hard.

28. Semidirect Products

Definition (Semi-direct products)

28.1

Suppose a group G has a subgroup H and a normal subgroup N , such that $G = NH$ and $N \cap H = \{1\}$. Recall that if H were also normal, then G would be the direct product of N and H . Without this assumption, we say that G is the **(internal) semi-direct product** $G = N \rtimes H$.

Remark 28.2. 1. As $H \cap N = \{1\}$,

$$H = H/H \cap N \cong HN/N = G/N,$$

so if G is finite, we have $|G| = |H| \cdot |N|$.

2. Every $g \in G$ has a unique expression as $g = nh$ for $n \in N$ and $h \in H$.
3. For $x, y \in G$, write $x = n_1 h_1$ and $y = n_2 h_2$, $n_i \in N, h_i \in H$. Then, $xy = n_1 h_1 n_2 h_2 = n_1 (h_1 n_2 h_1^{-1}) (h_1 h_2) = n_1 n'_2 (h_1 h_2) = nh$.
4. For $h \in H$, we use conjugation by h to define a map $\varphi_h : N \rightarrow N$ by $\varphi_h(n) := h n h^{-1}, n \in N$. Then, $\varphi_h \in \text{Aut}(N)$ and $\varphi_{h_1} \circ \varphi_{h_2} = \varphi_{h_1 h_2}$, so we get a homomorphism $\varphi : H \rightarrow \text{Aut}(N)$, $h \mapsto \varphi_h$. This φ is called the **conjugation homomorphism** of the semi-direct product. We see that $(n_1 h_1)(n_2 h_2) = n_1 \varphi(h_1)(n_2) \cdot h_1 h_2$. So, the group operation on G can be expressed in terms of the group operations on N and H , and the homomorphism $\varphi : H \rightarrow \text{Aut}(N)$.
5. If the conjugation homomorphism φ is trivial, then

$$n h n^{-1} = (n h n^{-1})(h^{-1} h) = n \varphi_h(n^{-1}) h = n \varphi(h)(n^{-1}) h = n n^{-1} h = h,$$

so H is normal in G , and $G = N \times H$. Conversely, if $G = N \times H$, then φ is trivial. If φ is non-trivial, then G is non-abelian.

29. External Semi Direct Products

Definition

29.1

Let N and H be groups, and $\varphi : H \rightarrow \text{Aut}(N)$ any group homomorphism. Define a binary operation on $N \times H$ by $(n_1 h_1) \cdot (n_2 h_2) := (n_1 \varphi(h_1)(n_2), h_1 h_2)$. This turns $N \times H$ into a group with identity $(1, 1)$; the inverse of (n, h) is $(\varphi(h^{-1})(n^{-1}), h^{-1})$. This group is called the **external semi-direct product of N by H , corresponding to φ** , denoted $G = N \rtimes_{\varphi} H$.

Now, G has subgroups $\mathbb{N} := N \times 1$ and $\mathbb{H} = 1 \times H$, which are isomorphic to N and H , respectively. For $(x, 1) \in \mathbb{N}$ and $(n, h) \in G$, we have

$$(n, h)(x, 1)(n, h)^{-1} = (n \varphi(h)(x), h)(\varphi(h^{-1})(n^{-1}), h^{-1}) = (n \varphi(h)(x) n^{-1}, 1) \in \mathbb{N},$$

hence $\mathbb{N} \trianglelefteq G$. Moreover, we see $(n, h) = (n \varphi(1)(1), h) = (n, 1) \cdot (1, h)$, so $G = \mathbb{N} \cdot \mathbb{H}$. Finally, as $\mathbb{N} \cap \mathbb{H} = \{(1, 1)\}$, we see that G is the internal semi-direct product $G = \mathbb{N} \rtimes \mathbb{H}$.

Finally, given $(n, 1) \in \mathbb{N}$ and $(1, h) \in \mathbb{H}$, we have $(1, h)(n, 1)(1, h)^{-1} = (\varphi(h)(n), 1)$, hence the

conjugation homomorphism $\mathbb{H} \rightarrow \text{Aut}(\mathbb{N})$ of $\mathbb{N} \rtimes \mathbb{H}$ corresponds to the original homomorphism $\varphi : H \rightarrow \text{Aut}(N)$. In this way, we can identify internal and external semi-direct products.

Remark 29.2. If $\varphi, \psi : H \rightarrow \text{Aut}(N)$ are distinct homomorphisms, the groups $N \rtimes_{\varphi} H$ and $N \rtimes_{\psi} H$ are not necessarily isomorphic.

Lemma**29.3**

Let H be a cyclic group, and N be any group. Suppose that $\varphi, \psi : H \rightarrow \text{Aut}(N)$ are monomorphisms (1-1 homomorphisms) such that $\varphi(H) = \psi(H)$. Then, we have $N \rtimes_{\varphi} H \cong N \rtimes_{\psi} H$.

Proof. Let $H = \langle x \rangle$. Since $\varphi(H)$ and $\psi(H)$ coincide, we see that $\varphi(x)$ and $\psi(x)$ generate the same cyclic subgroup of $\text{Aut}(N)$. Hence, there exists $a, b \in \mathbb{Z}$ such that $\varphi(x)^a = \psi(x)$, and $\psi(x)^b = \varphi(x)$. Since H is cyclic generated by x , we get in general that $\varphi(h)^a = \psi(h)$, $\psi(h)^b = \varphi(h)$ for all $h \in H$. Moreover, $\varphi(x) = \psi(x)^b = \varphi(x)^{ab} = \varphi(x^{ab})$, and φ is 1-1, so $x^{ab} = x \iff h^{ab} = h$ for all $h \in H$. Now, define $\tau : N \rtimes_{\psi} H \rightarrow N \rtimes_{\varphi} H$ by $\tau(nh) := nh^a$.

Then,

$$\tau((n_1h_1)(n_2h_2)) = \tau(n, \psi(h_1)(n_2)h_1h_2) = \cdots = (n_1h_1^a)(n_2h_2^a) = \tau(n_1h_1)\tau(n_2h_2)$$

Similarly, we show that $\tau' : N \rtimes_{\varphi} H \rightarrow N \rtimes_{\psi} H$ sending nh to nh^b is a homomorphism. Since $h^{ab} = h$, it follows that τ and τ' are mutually inverse, hence they are isomorphisms. $\square$

Proposition**29.4**

If $G = C_n$ is a cyclic group of order n , then $\text{Aut } G \cong (\mathbb{Z}/n\mathbb{Z})^{\times}$, an abelian group of order $\varphi(n)$.

Proof. Let g be a generator of $G = C_n$. If $\varphi \in \text{Aut } G$, then $\varphi(g) = g^a$ uniquely determines φ ; we denote this by φ_a . Since $o(g^a) = o(g) = n$, we must have $(a, n) = 1$, and conversely for any such a coprime to n , the map $\varphi(x) = x^a$ gives an automorphism of C_n . We thus have a surjective map $f : \text{Aut}(C_n) \rightarrow (\mathbb{Z}/n\mathbb{Z})^{\times}$ mapping $\varphi_a \mapsto a + n\mathbb{Z}$, and f is a group homomorphism. Hence, it is an isomorphism. We'll see later that if $n = p$ is prime, then $\text{Aut}(C_p) \cong C_{p-1}$. More generally, this remains true for $\text{Aut}(C_{p^k}) \cong C_{p^{k-1}(p-1)}$ where $p \geq 3$. However, for all $k \geq 3$, $\text{Aut}(C_{2^k}) \cong C_2 \times C_{2^{k-2}}$. $\square$

30. Groups of Order pq

Let p, q be distinct primes, $p > q$.

Theorem**30.1**

If $p \not\equiv 1 \pmod{q}$, then any group of order pq is isomorphic to C_{pq} . Otherwise, if $p \equiv 1 \pmod{q}$, then any abelian group of order pq is isomorphic to C_{pq} , and there's exactly one non-abelian group of order pq , up to isomorphism.

Proof. Let $|G| = pq$, and let P and Q be a p -Sylow and q -Sylow subgroup of G , respectively. Since $|P| = p$, $|Q| = q$, we have $P \cong C_p$, $Q \cong C_q$, and $P \cap Q = \{1\}$. Now, the number of conjugates of P

in G divides $|G : P| = q$, and is congruent to 1 modulo p . But, $q \not\equiv 1 \pmod{p}$ as $q < p$, so P has only one conjugate in G , hence $P \triangleleft G$.

Now, Q has either 1 or p conjugates in G , and if the latter happens, we must have $p \equiv 1 \pmod{q}$. If $Q \trianglelefteq G$, then $G = C_p \times C_q \cong C_{pq}$. So, we are reduced to the case when $p \equiv 1 \pmod{q}$ and G is non-abelian. In this instance, $G = P \rtimes Q$. Let $\varphi : Q \rightarrow \text{Aut}(P)$ be the conjugation homomorphism. Now, φ is non-trivial, and Q is a simple group, so φ is 1-1. We're reduced to studying monomorphisms $C_q \rightarrow \text{Aut}(C_p) = C_{p-1}$. Since $q \mid p-1$, $\text{Aut}(C_p)$ has a unique subgroup K of order q . Define $\varphi : C_q \rightarrow \text{Aut}(C_p)$ by letting $\varphi(x)$ be a generator of the cyclic group $K \leq \text{Aut}(C_p)$, where x is a generator of C_q . This shows that a nontrivial φ exists, so a non-abelian group of order pq .

Now, if $\psi : C_q \rightarrow \text{Aut}(C_p)$ is another monomorphism, then by uniqueness of K , we must have $\psi(C_q) = K = \varphi(C_q)$. Hence, [Lemma 29.3](#) shows that $C_p \rtimes_{\varphi} C_q \cong C_p \rtimes_{\psi} C_q$, this is non-abelian group is unique. $\square$

Example 30.2 (Examples of Semi-Direct Products). 1. M_n is the group of rigid motions of $\mathbb{R}^n$.

Then, $M_n = O(n) \ltimes \mathbb{R}^n$.

2. The dihedral group $D_n = C_n \rtimes C_2$

3. The symmetric group $S_n = A_n \rtimes C_2$.

31. The Free Group

Motivation

Make precise presentations of groups like

$$C_n = \langle x \mid x^n = 1 \rangle \quad \text{or} \quad D_n = \langle x, y \mid x^2 = y^n = 1, xy = y^{-1}x \rangle.$$

Definition (Words)

31.1

Let S be a (possibly infinite) set of symbols (e.g. $\{a, b, \dots\}$), and define $S' = S \cup S^{-1} = \{a, a^{-1}, b, b^{-1}, \dots\}$. A **word** is a finite string of symbols of S' . Words are multiplied by concatenation:

$$(aa)(ba) = aaba$$

1 denotes the **empty word** with no letters, and let W be the set of all words.

If a word contains xx^{-1} or $x^{-1}x$ for some $x \in S$, we agree to **cancel** x, x^{-1} , and reduce the length of the word. The word is **reduced** if no such cancellation can occur. Starting with any $w \in W$, we can perform a sequence of cancellations until we reach a reduced word w_0 . This is called a **reduced form** of w .

Proposition

31.2

There is only one reduced form for any given $w \in W$

Proof. We may induct on the length of w . If w is already reduced, then there's nothing to prove. Otherwise, there exists a pair xx^{-1} in W which can be canceled (here, $x \in S'$, and by convention if $x = a^{-1}$, then $x^{-1} = a$). It suffices, using induction, to prove that we can obtain each reduced form of w by canceling xx^{-1} first.

Let w_0 be a reduced form of w , i.e. w_0 is obtained from w by a sequence of cancellations. If xx^{-1} is canceled at some point during the process, we can rearrange to cancel it first. The only other possibility is that x or x^{-1} in " xx^{-1} " was canceled at some point. If, say, x was canceled, then it happened like $x^{-1}xx^{-1} \rightarrow x^{-1}$. But, notice that canceling the original pair has the same effect. (similar if x^{-1} was canceled first) So, we're back in the previous case. $\square$

Definition**31.3**

$w, w' \in W$ are **equivalent** if they have the same reduced form.

Proposition**31.4**

The product of equivalent words are equivalent. We can therefore multiply equivalence classes of words.

Proof. If $w \sim w', v \sim v'$, let w_0, v_0 be the reduced form for w, w' , and v, v' respectively. It follows that $wv \sim w_0v_0 \sim w'v'$. $\square$

Remark 31.5. We have inverses, as, for example $[abc \cdots z]^{-1} = [z^{-1} \cdots c^{-1}b^{-1}a^{-1}]$

Definition (The Free Group)**31.6**

The group $F(S) = \langle S \rangle$ of equivalence classes of words on S' is the **free group** on S .

We can now introduce power notation:

$$aaabb = a^3b^2.$$

Definition**31.7**

The elements of S are the **generators** of $F(S)$

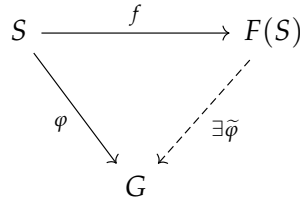
Example 31.8. 1. If $S = \{x\}$, then $F(S) = \{x^k \mid k \in \mathbb{Z}\}$ is the infinite cyclic group generated by x .

2. If $S = \{a, b\}$, $F(a, b) = \{1, a, a^{-1}, b, b^{-1}, ab, ba, a^{-1}b, \dots\}$

Universal Property of the Free Groups**31.9**

Notice that the free group $F(S)$ comes with a map of sets $f : S \rightarrow F(S)$ with $a \mapsto a$. The pair $(S, F(S))$ has the following universal property:

For any group G and map of sets $\varphi : S \rightarrow G$, there exists a unique homomorphism $\tilde{\varphi} : F(S) \rightarrow G$ such that $\tilde{\varphi} \circ f = \varphi$. That is, the below diagram commutes.



Proof. Not the whole proof, but observe that the obvious definition of $\tilde{\varphi}$ on words in W passes to equivalence classes. $\square$

Remark 31.10. If G is a group and $S \subset G$ is any subset, from the universal property we get a unique map $\varphi : F(S) \rightarrow G$. φ is surjective if and only if G is generated by S . When φ is onto, we get $G \cong F(S) / \ker \varphi$, hence the elements in $\ker \varphi$ are relations among the generators in the set S .

Definition (Relations)

31.11

A set of words $R = \{r_1, r_2, \dots\}$ is a set of **defining relations** if $R \subset \ker \varphi$ from the above remark, and $\ker \varphi$ is the smallest normal subgroup containing R (so, $\ker \varphi$ is generated by all words in R with their conjugates).

We use the notation $G = \langle x_1, x_2, \dots \mid r_1, r_2, \dots \rangle$, where $S = \{x_1, x_2, \dots\}$.

Example 31.12. 1. $G = \mathbb{Z}/n\mathbb{Z}$, $\varphi : \langle x \rangle \rightarrow G$, $x \mapsto 1$. $\ker \varphi$ is generated by x^n , so $G = \langle x \mid x^n = 1 \rangle$
 2. $G = \langle x, y \mid xyx^{-1}y^{-1} = 1 \rangle = \{x^i y^j \mid i, j \in \mathbb{Z}\} \cong \mathbb{Z} \oplus \mathbb{Z}$, the **free abelian group** on x and y .

This is where the material for the midterm ends.

32. Reflection Groups and Coxeter Groups

Definition (Reflections)

32.1

Let $V = \mathbb{R}^n$. For any $\alpha \neq 0$ in V , let $H_\alpha = \langle \alpha \rangle^\perp = \{x \in V \mid \langle x, \alpha \rangle = 0\}$. Then, the **reflection** $s_\alpha : V \rightarrow V$ is the map in $O(V) \cong O(n)$ such that $s_\alpha(x) = x$ for all $x \in H_\alpha$, and $s_\alpha(\alpha) = -\alpha$.

Proposition

32.2

$$s_\alpha(x) = x - \frac{2\langle x, \alpha \rangle}{\langle \alpha, \alpha \rangle} \alpha$$

Definition (The Reflection Group)

32.3

The reflection group is a finite subgroup W of $O(V)$ generated as a group of reflections.

Example 32.4. 1. $D_n = \langle x, y \mid x^2 = 1, y^n = 1, (xy^2) = 1 \rangle$. So, set $s_1 = x, s_2 = xy$, and $D_n = \langle s_1, s_2 \mid s_1^2 = s_2^2 = 1, (s_1 s_2)^n = 1 \rangle$
 2. The symmetric group $S_n \leq O(n)$, where $w \in S_n$ permutes $e_1, \dots, e_n$ (w is a permutation matrix). The transposition (ij) acts as the reflections $s_{e_i - e_j}$ about $H_{e_i - e_j} = \{x \in \mathbb{R}^n \mid x_i = x_j\}$. In fact, S_n

is the symmetry group of the $(n-1)$ -simplex $\Delta_{n-1} := \{\sum_{i=1}^n \lambda_i e_i \mid \lambda_i \geq 0, \lambda_1 + \cdots + \lambda_n = 1\}$.

$$S_n = \{s_1, \dots, s_{n-1} \mid (s_i s_j)^2 = 1, |i-j| \geq 2, (s_i s_{i+1})^3 = 1\}$$

3. Let $V = \mathbb{R}^n$, and let S_n act as before. Now, add the n reflections about the coordinate hyperplanes H_{e_i} , $1 \leq i \leq n$. These n reflections generate a group N of order 2^n isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$. Note that $N \cap S_n = 1$, and N and S_n generate a group $W = N \rtimes S_n$, called the **hyperoctahedral group** (the permutation action of S_n on $(\mathbb{Z}/2\mathbb{Z})^n$ is the conjugation homomorphism $S_n \rightarrow \text{Aut}(N)$). W is the symmetry group of the n -cube $[-1, 1]^n = \{\sum \lambda_i e_i \mid -1 \leq \lambda_i \leq 1\}$. The elements of W_n are **signed permutation matrices** (like permutation matrices but they can have ± 1 instead of just 1). In one line notation, $w \in W$ is a **signed permutation** $w = (w_1, w_2, \dots, w_n)$, where $w_i = w(i)$, and $\{|w_1|, \dots, |w_n|\} = \{1, \dots, n\}$. W_n is generated by the simple reflections $s_1, \dots, s_{n-1} \in S_n$ and the **sign change** $s_0 := (-1, 2, \dots, n)$. The presentation is $W_n = \{s_0, \dots, s_{n-1} \mid s_i^2 = 1, (s_i s_j)^2 = 1, |i-j| \geq 2, (s_i s_{i+1})^3 = 1, i \geq 1, (s_0 s_1)^4 = 1\}$

Lemma

32.5

Given $\alpha, \beta \in \mathbb{R}^2 \setminus \{0\}$, $s_\beta \circ s_\alpha$ is a rotation through twice the angle between α and β . There's a version of this in $\mathbb{R}^n$ as well.

Proof. Exercise □

Definition (Coxeter Groups)

32.6

A group W is a **Coxeter Group** if there exists $S \subset W$ such that W is a quotient of the free group $F(S)$ modulo the relations:

- (i) $s^2 = 1$ for all $s \in S$,
- (ii) $(ss')^{m_{s,s'}} = 1$ for all $s, s' \in S$ with $s \neq s'$, and for some minimal integers $m_{s,s'} = m_{s',s} \geq 2$.

We represent W by a labeled graph Γ_W called the **Coxeter graph** with one vertex for each $s \in S$, and an edge connecting s, s' if $m_{s,s'} \geq 3$ labeled by $m_{s,s'}$. In practice, if $m_{s,s'} = 3$, the label 3 is omitted.

W is **irreducible** if Γ_W is **connected** (if not, we can write $W = W_1 \times \cdots \times W_r$ depending on the connected components of Γ_W).

Example 32.7. 1. $D_m = I_2(m)$

2. $S_n \equiv A_{n-1}$

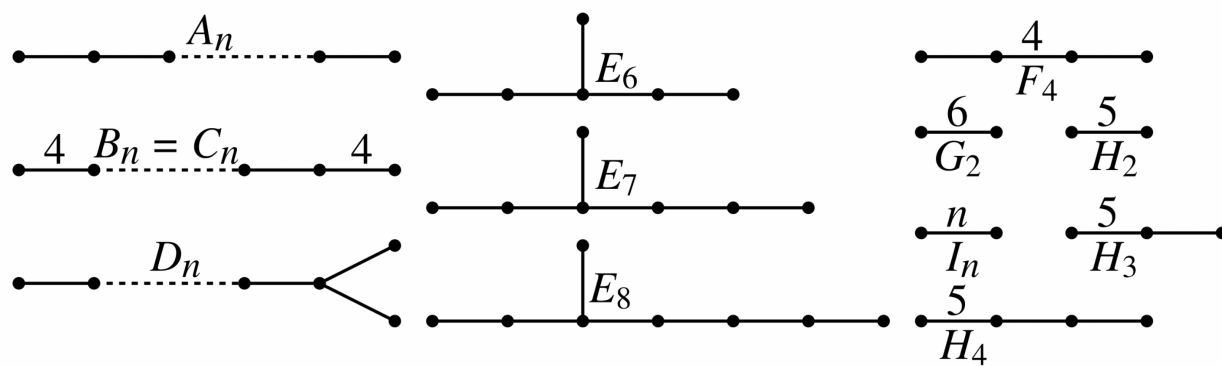
3. $W_n \equiv BC_n$

Theorem

32.8

Let (W, S) be a Coxeter group, where S is a finite set of Coxeter generators, with connected Coxeter diagram Γ_W . Then, TFAE

- 1. W is a finite group
- 2. Γ is one of the following Coxeter diagrams: A_n with $n \geq 1$ vertices, BC_n with $n \geq 2$ vertices, D_n with $n \geq 4$ vertices, $E_6, E_7, E_8, F_4, G_2, H_3, H_4, I_2(m)$. See below.

Figure 1: Source: Rgugliel on [Wikipedia](#)

Rings

33. Intro to Rings

Definition (Rings)

33.1

A **ring** R is a set together with two binary operations $+, \cdot : R \times R \rightarrow R$ satisfying

- (i) $(R, +)$ is an additive abelian group
- (ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$
- (iii) There exists $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$
- (iv) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$

Remark 33.2. (ii) and (iii) say that $(R, \cdot)$ is an **associative monoid**.

Definition

33.3

A ring R is **commutative** if multiplication is commutative, i.e. $a \cdot b = b \cdot a$ for all $a, b \in R$. We say R is a **division ring** if $1 \neq 0$, and every $a \in R \setminus \{0\}$ has a multiplicative inverse. A commutative division ring is called a **field**.

Example 33.4. 1. There is a unique ring with $1 = 0$, which is the 0 ring $\{0\}$.

- 2. Any field is a ring
- 3. $(\mathbb{Z}, +, \cdot)$ is a ring
- 4. For any $n \in \mathbb{N}$, the coset space $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a ring, which is a field if and only if n is prime.
- 5. Let A be any set, and R be a ring. Then, the set $F(A) = \{f : A \rightarrow R\}$ is a ring under pointwise operations.
- 6. Let i, j, k be symbols obeying the relations $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j = -ik$ (the quaternions). Then, the **ring of quaternions** $\mathbb{H}$ is the 4 dimensional real vector space

$$\mathbb{H} := \{x + yi + zj + wk \mid x, y, z, w \in \mathbb{R}\}$$

with multiplication defined multilinearly. Every quaternion has a norm $\|q\|^2 = x^2 + y^2 + z^2 + w^2$.

If $q \neq 0$, one checks that $q^{-1} = \frac{\bar{q}}{\|q\|^2}$

- 7. If R is any ring, we get a **matrix ring** $M_n(R)$ for each $n \geq 1$, consisting of $n \times n$ matrices in R , with operations defined as usual.
- 8. Let R be a ring. The **ring of polynomials** $R[x]$ in the variable x with coefficients in R is the set of all formal sums

$$a_0 + a_1x + \cdots + a_nx^n$$

with only finitely many $a_i \neq 0$. The operations are defined as usual. That is,

$$\left(\sum_i a_i x^i\right)\left(\sum_j b_j x^j\right) = \sum_k c_k x^k \quad c_k := \sum_{i+j=k} a_i b_j$$

9. For R a ring, there is also the ring of polynomials in several variables, $R[x_1, x_2, \dots, x_n]$. We assume the x_i 's commute. Observe that $R[x, y] \equiv (R[x])[y]$

Definition

33.5

Let R' be a ring. Then, a **subring** R of R' is a ring sharing the same operations and identity $1_R = 1_{R'}$.

Example 33.6. R is a subring of $R[x]$. Moreover, $R[x]$ is commutative if and only if R is commutative.

Proposition

33.7

Let R be a ring, and $a, b \in R$ be arbitrary. Then,

1. $0a = a0 = 0$.
2. $(-a)b = -ab = a(-b)$, and $(-a)(-b) = ab$.
3. The identity 1 is unique, and $-a = (-1)a$.

Remark 33.8. In a general ring, it is possible that $xy = 0$ while x and y are both nonzero. For example, $(2 + 6\mathbb{Z})(3 + 6\mathbb{Z}) = 6\mathbb{Z} = 0$.

Definition (Zero Divisors and Units)

33.9

Let R be a ring. A non-zero element $x \in R$ is a **zero-divisor** in R if there exists $y \in R$ non-zero such that $xy = 0$ or $yx = 0$. An element $u \in R$ is a **unit** in R if there exists $v \in R$ such that $uv = vu = 1$. The set of all units in R is denoted $R^\times$, and forms a group under multiplication, called the **group of units** in R .

Example 33.10. 1. $\mathbb{Z}^\times = \{\pm 1\}$

2. Every non-zero element of $\mathbb{Z}/n\mathbb{Z}$ is either a zero divisor or a unit. $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$.

Definition (Integral Domains)

33.11

A commutative ring R with identity $1 \neq 0$ is called an **integral domain** if it has no zero-divisors. That is, $xy = 0 \implies x = 0$ or $y = 0$.

Proposition

33.12

If R is a domain, then R has the **cancellation property** $ax = ay \implies x = y$ or $a = 0$.

Corollary

33.13

Every finite integral domain is a field.

Proof. Let R be a finite integral domain, and let $a \in R \setminus 0$. Then, define $i : R \rightarrow R$ defined by

$x \mapsto ax$ is injective, by the cancellation property. Hence, as R is finite, i must also be surjective, so there exists $b \in R$ such that $i(b) = 1$. That is, $ab = 1$, hence a is a unit. $\square$

34. Ring Homomorphisms

Definition (Ring Homomorphisms)

34.1

If R, R' are rings, a map $\varphi : R \rightarrow R'$ is a **ring homomorphism** if

- (i) $\varphi(x + y) = \varphi(x) + \varphi(y)$
- (ii) $\varphi(xy) = \varphi(x)\varphi(y)$
- (iii) $\varphi(1_R) = 1_{R'}$

A bijective ring homomorphism is an **isomorphism**. The kernel of φ is

$$\ker \varphi = \{x \in R \mid \varphi(x) = 0\}$$

Proposition

34.2

φ is injective if and only if $\ker \varphi = \{0\}$, and φ is surjective if and only if $\text{Img } \varphi = R'$.

Example 34.3. 1. There is a unique homomorphism $i : \mathbb{Z} \rightarrow R$ for any ring R . Namely, $i(1) = 1$, and $i(n) = 1_R + \cdots + 1_R$ for $n \geq 1$, and $i(-n) = -i(n)$. The kernel of i is a subgroup of $\mathbb{Z}$, so it must be $n\mathbb{Z}$ for some $n \geq 0$. This n is called the **characteristic** of R . For example, if R is an integral domain, then the characteristic of R is prime or 0.

2. (**Substitution Principle**) Let $\varphi : R \rightarrow R'$ be a morphism of commutative rings (actually, only R' needs to be commutative). Then, for any element $\alpha \in R'$, there exists a unique ring homomorphism $\tilde{\varphi} : R[x] \rightarrow R'$ which agrees with φ on constant polynomials, i.e. R , and has $\tilde{\varphi}(x) := \alpha$. In fact, we must have $\tilde{\varphi}(\sum a_i x^i) = \sum \varphi(a_i) \alpha^i$. This extends to polynomial rings in more than one variable as well.

35. Ideals and Quotients

We want to define, for certain subgroups $I \subset R$, a quotient ring R/I . These additive subgroups should be exactly the kernels of ring homomorphisms $\varphi : R \rightarrow R'$.

Note

$\ker \varphi$ is not a subring of R unless $1 \in \ker \varphi$, which is equivalent to saying that $\ker \varphi = R$. But, $\ker \varphi$ has all the other properties of a subring, including the special property that if $r \in R, a \in \ker \varphi$, then $a \cdot r = r \cdot a \in \ker \varphi$

Definition (Ideals)

35.1

A subset $\emptyset \neq I \subset R$ is called a

- (i) **left ideal** if I is a subgroup of $(R, +)$ and $ra \in I$ for all $r \in R, a \in I$, i.e. $rI \subset I$ for all $r \in R$.
- (ii) **right ideal** if I is a subgroup of $(R, +)$ and $ar \in I$ for all $r \in R, a \in I$, i.e. $Ir \subset I$ for all $r \in R$.
- (iii) **two-sided ideal** if its both a left and right ideal.

An **ideal** will always mean a two-sided ideal. The notion of left and right ideals are the same in commutative rings.

Example 35.2. All kernels of homomorphisms $\varphi : R \rightarrow R'$ are two sided ideals.

Definition (Quotient Rings)

35.3

Given $I \subset R$ a two sided ideal, we have a quotient group $(R/I, +)$. Moreover, the multiplication $(a + I)(b + I) = ab + I$ then defines a ring structure on R/I . We call R/I a **quotient ring**.

Proof. If $a + I = a' + I$ and $b + I = b' + I$, then $a' = a + u_1, b' = b + u_2$ with $u_1, u_2 \in I$. It follows that $a'b' = ab + au_2 + bu_1 + u_1u_2 = ab + u$, for $u \in I$. Hence, $ab + I = a'b' + I$. $\square$

Remark 35.4. The identity in R/I is $1 + I$, and we have a canonical **projection map** $\pi : R \rightarrow R/I$; the ring structure on R/I is that which makes π a ring homomorphism.

Theorem

35.5

$(R/I, \pi)$ also satisfies the universal property as in the case of vector spaces and groups.

First Ring Isomorphism Theorem

35.6

Let $\varphi : R \rightarrow R'$ be homomorphism of rings. Then, $\text{Img } \varphi$ is a subring of R' , $\ker \varphi$ is an ideal of R , and the induced map $\tilde{\varphi} : R/\ker \varphi \rightarrow \text{Img } \varphi$ which maps $r + \ker \varphi \mapsto \varphi(r)$ is an isomorphism. That is, $R/\ker \varphi \cong \text{Img } \varphi$.

Second Ring Isomorphism Theorem

35.7

Suppose R is a ring, and A, B are subsets of R such that A is a subring and B is an ideal. Then, $(A + B)/B \cong A/A \cap B$

Definition

35.8

Given a subset $A \subset R$, we denote by (A) the **left ideal generated by A** , i.e. the smallest left ideal of R containing A . We have that

$$(A) = \bigcap_{A \subset I \text{ left ideal}} I = R \cdot A := \{r_1 a_1 + \cdots + r_k a_k \mid r_i \in R, a_i \in A, k \in \mathbb{N}\}$$

A left ideal I is **finitely generated** if $I = (A)$ for some finite set $A \subset R$. We say that I is **principal** if $I = (a) = Ra$ for some $a \in R$. We can work similarly with right or 2-sided ideals.

Example 35.9. 1. $(0), R$ are two sided ideals in any ring R .

2. An ideal of $\mathbb{Z}$ is a subgroup, so it must be principal $n\mathbb{Z}$. Similarly, if F is a field, all ideals in $F[x]$ are principle. This fails in $\mathbb{Z}[x]$ or $\mathbb{C}[x, y]$.

Exercise: Check that the ideal (x, y) in $\mathbb{C}[x, y]$ is not principal.

Hard exercise: Show that all ideals in $\mathbb{C}[x, y]$ are finitely generated.

Example 35.10 (Examples of Quotient Rings). 1. If R is any ring, we have an *evaluation map* at 0, which is $\varphi : R[x] \rightarrow R, f(x) \mapsto f(0)$. Note that $\text{Im } \varphi = R, \ker \varphi = (x)$, so $R[x]/(x) \cong R$.

2. Consider the evaluation at $i = \sqrt{-1}$ in $\varphi : \mathbb{R}[x] \rightarrow \mathbb{C}, f(x) \mapsto f(i)$. Since $\varphi(ax + b) = ai + b$ for all $a, b \in \mathbb{R}$, we know φ is surjective. We claim $\ker \varphi = (x^2 + 1)$. Indeed, if $f(x) = (x^2 + 1)g(x)$, then $f(i) = 0$. Conversely, if $f(i) = 0$, then since f has real coefficients, $f(-i) = 0$ as well by conjugation. So, $f(x)$ is divisible by $(x - i)(x + i) = x^2 + 1$. Therefore, $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

3. Consider the ring $\mathbb{C}[x, y]/(y^2 - x^2 - x^3)$. This is unlike any ring we've seen before. Let's prove some results to help.

Proposition

35.11

Let $I \subset R$ be a left ideal.

1. $I = R \iff I$ contains a unit
2. Suppose R is commutative. Then, R is a field if and only if the only ideals of R are (0) and R .

Corollary

35.12

If F is a field and $\varphi : F \rightarrow R$ is any ring homomorphism, φ must be either injective or trivial.

Definition

35.13

A left ideal m in R is **maximal** if it's maximal among all proper ideals of R .

Theorem

35.14

Any proper (left) ideal of a ring R is contained in a maximal ideal.

Proof. An ideal I of R is proper if and only if $1 \notin I$. So, we can use Zorn's lemma: if $\mathcal{I}$ is the set of all proper left ideals of R , ordered by inclusion, then any chain $(I_j)_{j \in J}$ of ideals in $\mathcal{I}$ has an upper bound. Namely, take $\cup I_j$, and since we're working with a chain, this is still a proper ideal, as $1 \notin \cup I_j$. Thus, by Zorn's lemma, $\mathcal{I}$ has a maximal element m . $\square$

Example 35.15. 1. The ideals of $(\mathbb{Z}, +, \cdot)$ are the subgroups $n\mathbb{Z}$ for $n \geq 1$. The maximal ideals are $p\mathbb{Z}$, where p is prime.

2. (Deeper) If F is any field, the maximal ideals of $F[x]$ are of the form $(f(x))$ where $f(x)$ can't be

factored (it's a principal ideal domain). In other words, f is irreducible over F .

3. (Even deeper) Consider $\mathbb{C}[x, y]$. Recall that the maximal ideals in $\mathbb{C}$ are $x - a$ for $a \in \mathbb{C}$. Similarly, the maximal ideals in $\mathbb{C}[x, y]$ are $(x - a, y - b)$ for $a, b \in \mathbb{C}$ (not entirely easy to prove).

Remark 35.16. Let R be a ring, $I \subset R$ a left ideal. Then, there is a 1-1 correspondence between left ideals in R/I and left ideals $J \subset R$ which contain I .

Proof. Exercise. □

Theorem

35.17

Let R be a commutative ring. An ideal $M \subset R$ is maximal if and only if R/M is a field.

Proof. If R/M is a field, its only ideals are $(0) = M$ and R/M , so by the above remark, this implies that there are no ideals J of R with $M \subsetneq J \subsetneq R$, hence M is maximal. (Note that this direction does not require the ring to be commutative)

Conversely, if M is maximal, the only ideals of R/M are (0) and M . Hence, since R is commutative, R/M is a field. □

Definition

35.18

And ideal $P \subset R$ is **prime** if whenever $ab \in P$, we have $a \in P$ or $b \in P$.

Proposition

35.19

An ideal P of R is prime if and only if R/P is an integral domain.

Proof. The defining condition for a prime ideal, in the quotient, translates to $(a + P)(b + P) = P$, then $a + P = P$ or $b + P = P$, exactly the condition for an integral domain. □

Corollary

35.20

Let R be a commutative ring. Then, all maximal ideals in R are prime. The converse is not necessarily true.

Example 35.21. In $R = \mathbb{C}[x, y]$, the ideal $I := (x) = x\mathbb{C}[x, y]$ satisfies $R/I \cong \mathbb{C}[y]$. This is a domain, but not a field.

36. The Field of Fractions of an Integral Domain

This generalizes the standard construction of the rational numbers from the integers.

Definition

36.1

Let R be a domain and $S := R \setminus \{0\}$. We define an equivalence relation on $R \times S$ by $(a, b) \sim (c, d) \iff ad = bc$. We denote by $\frac{a}{b}$ the equivalence class of (a, b) . We may define addition

and multiplication of these classes in the usual way:

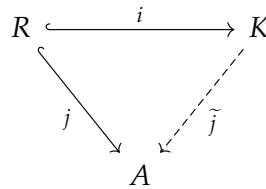
$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

The set K of all equivalence classes becomes a ring with identities $\frac{0}{1}$ and $\frac{1}{1}$. Moreover, K is a field, since $(\frac{a}{b})^{-1} = (\frac{b}{a})$ if $\frac{a}{b} \neq \frac{0}{1}$. There is an embedding $i : R \hookrightarrow K$ by $a \mapsto \frac{a}{1}$. K is called the **field of fractions** or **quotient field** of R , often denoted $Q(R)$.

Proposition

36.2

The pair (R, K) with the embedding $i : R \rightarrow K$ is characterized by a universal property: for any field A and monomorphism $j : R \hookrightarrow A$, there exists a unique homomorphism $\tilde{j} : K \rightarrow A$ such that $j = \tilde{j} \circ i$. That is, the diagram below commute.



Example 36.3. 1. $\mathbb{Q}$ is the quotient field of $\mathbb{Z}$

2. If R is an integral domain, we claim $R[x]$ is an integral domain. Indeed if $f(x) = a_n x^n + \cdots + a_1 x + a_0$, and $g(x) = b_m x^m + \cdots + b_1 x + b_0$, with $a_n, b_m \neq 0$, then $a_n b_m \neq 0$, hence $f(x) \cdot g(x) = a_n b_m x^{n+m} + \cdots \neq 0$. The quotient field of $R[x]$ is the field $R(x)$ of rational functions in x over R .

$$R(x) = \left\{ \frac{p(x)}{q(x)} \mid p, q \in R[x], q \neq 0 \right\}$$

37. Euclidean Domains

Let's study nice rings.

Definition

37.1

A ring R is a **Euclidean Domain** if

- (i) R is an integral domain
- (ii) There is a **norm map** $d : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ such that the division algorithm holds: given $a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ such that $a = bq + r$, and either $r = 0$ or $d(r) < d(b)$.

Example 37.2. 1. The ring of integers $\mathbb{Z}$, with $d(k) = |k|$.

2. $\mathbb{Z}[i] := \{x + iy \mid x, y \in \mathbb{Z}\} = \mathbb{Z}[x]/(x^2 + 1)$ is the ring of **Gaussian integers**. It is Euclidean: Let $d : \mathbb{Z}[i] \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ by $d(x + iy) = x^2 + y^2$. Take $a, b \in \mathbb{Z}[i]$ with $b \neq 0$. We want to divide a by b .

Case 1: Suppose $b = n \in \mathbb{N}$. Write $a = x + iy$, and let $x = w_1 n + x', y = w_2 n + y'$ such that $|x'|, |y'| \leq \frac{n}{2}$. Then, $a = n(w_1 + w_2) + x' + iy'$, and $d(x' + iy') = (x')^2 + (y')^2 \leq \frac{n^2}{2} < n^2 =$

$d(b)$.

Case 2: We use case 1 to divide $a\bar{b}$ by $b\bar{b}$, yielding $a\bar{b} = qb\bar{b} + r'$, with $d(r') < d(b\bar{b}) = d(b)^2$.

Now,

$$d(a - qb)d(b) = d((a - qb)\bar{b}) = d(r') < d(b)^2 \implies d(a - qb) < d(b)$$

so taking $r := a - qb$ works.

3. **Polynomial division algorithm:** Here, R is assumed to be commutative. We define the **degree** $\deg(f)$ of a non-zero $f(x) \in R[x]$ as usual, and set $\deg(0) := -\infty$. Suppose $g \in R[x]$ is a **monic**, that is $g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. Then, for any $f \in R[x]$, there exists $q, r \in R[x]$ such that $f = qg + r$, and $\deg r < \deg g$. Furthermore, $q(x)$ and $r(x)$ are unique.

Proof. Suppose $\deg f(x) = m$. We use induction on m to prove the existence of q and r . If $m < n$, we're ok, since $f = 0 \cdot g + f$. Otherwise, if $m \geq n$, then write $f(x) = c_mx^m + \cdots + c_1x + c_0$ with $c_m \neq 0$, and note that

$$\deg(f(x) - c_mx^{n-m}g(x)) < m.$$

By induction, $f - c_mx^{n-m}g = q'g + r'$, so $f = (c_mx^{n-m} + q')g + r'$, and $\deg r' < n$.

For uniqueness, suppose $f = qg + r = q'g + r'$, then subtracting yields $(q - q')g = r' - r$. But, $\deg(r - r') < \deg(g)$, and if $q - q' \neq 0$, then the degree of the LHS is $\geq \deg g$ (since g is monic!). Therefore, we must have $q = q'$, and hence $r = r'$. $\square$

Remark 37.3. The division algorithm above also works if we replace "g monic" by "g unitary", meaning that the leading coefficient of g is a unit.

Corollary

37.4

If F is a field, then $F[x]$ is a Euclidean domain, with $d(f) = \deg f$.

38. Adjunction of Elements

Given a commutative ring R , we want to create a new ring R' which contains R and α , where α is some element satisfying some polynomial relations $f_i(\alpha) = 0, i \in I$.

Definition

38.1

Let R be a commutative ring, and let α be some value satisfying a set of polynomial relations $f_i(x) \in R[x], i \in I$. We then define $R' := R[\alpha] = R[x] / \langle f_i(x) \mid i \in I \rangle$. This is called **adjoining** α to R .

Special Case

Suppose α satisfies a single monic polynomial relation $f(\alpha) = 0$, where $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 \in R[x]$. Then, $R[\alpha]$ is in bijective correspondence with the elements of R^n .

Proof. $(r_0, \dots, r_{n-1})$ corresponds to $r_0 + r_1\alpha + \dots + r_{n-1}\alpha^{n-1}$. Indeed, since f is monic, any $g(x) \in R[x]/(f)$ can be written as a polynomial in x of degree $\leq n-1$, and this polynomial is unique. $\square$

Example 38.2. 1. For any field F , we can define $F[x, x^{-1}] = F[x][x^{-1}] := F[x, y]/\langle xy - 1 \rangle$, and we get the ring of Laurent polynomials in x .

2. $\mathbb{Z}[1/5] := \mathbb{Z}[x]/\langle 5x - 1 \rangle$

39. Principal Ideal Domains

Definition

39.1

We say an integral domain R is a **principal ideal domain** (or PID) if every ideal in R is principal.

Proposition

39.2

Any Euclidean domain is principal.

Proof. If R is Euclidean, with norm d , and I is a non-zero ideal of R , let a be the element of I with $d(a)$ minimal. Then, we claim $I = (a)$. Indeed, if $b \in I$, divide b by a to get $b = qa + r$, and $d(r) < d(a)$, but $r = b - qa \in I$, so we must have $d(r) = 0$ by minimality. $\square$

Corollary

39.3

If F is a field, then $F[x]$ is a principal ideal domain.

Example 39.4. $\mathbb{Z}$ and $\mathbb{Z}[i]$ are both PIDs.

Definition

39.5

Let R be a commutative ring, and take $a, b \in R$ with $b \neq 0$. We say

- (i) a is a **multiple** of b , and b **divides** a , written $b \mid a$, if there exists $x \in R$ with $a = xb$. This is equivalent to $Ra \subset Rb$.
- (ii) A **greatest common divisor** d of a and b is a non-zero element d such that $d \mid a$, $d \mid b$, and if $c \mid a$, $c \mid b$, then $c \mid d$. We denote the gcd as (a, b) or $\gcd(a, b)$.

Proposition

39.6

Let R be an integral domain. If two elements a, b of R generate the same principal ideal, i.e. $Ra = Rb$, then $a = ub$ for some unit $u \in R$. In particular, if d and d' are greatest common divisors of a, b , then $d' = ud$ for some unit $u \in R$.

Proof. Suppose $Ra = Rb$. Then, $a = xb = xya$ for some $x, y \in R$. It follows that $a(1 - xy) = 0$, so $a = 0$ or $xy = 1$. If d and d' are greatest common divisors of a and b , then $d \mid d'$ and $d' \mid d$, hence $Rd = Rd'$, thus $d' = ud$. $\square$

Definition

39.7

We say that a and b are **associates** if $a = ub$ for some unit u of R .

Theorem

39.8

Let R be a PID, $a, b \in R \setminus \{0\}$. Then, a and b have a greatest common divisor in R . Furthermore, let $d = \gcd(a, b)$, then there exists $x, y \in R$ with $d = xa + yb$. If R is Euclidean, there is an algorithm for computing d .

Proof. Consider the ideal $Ra + Rb$, which must be Rd for some $d \in R$. It's easy to see that $d = \gcd(a, b)$. We then see that $d = xa + yb$ for some $x, y \in R$.

If R is Euclidean, then we have the Euclidean algorithm for computing d :

$$a = q_0b + r_0, d(r_0) < d(b)$$

$$b = q_1r_0 + r_1, d(r_1) < d(r_0)$$

$$\vdots$$

Since $d(b) > d(r_0) > d(r_1) < \dots$, this process terminates with $r_{n-1} = q_{n+1}r_n + 0$. We claim $d = r_n = \gcd(a, b)$. Indeed,

$$r_n \mid r_{n-1} \implies r_n \mid r_{n-2} \implies \dots \implies r_n \mid b, r_n \mid a.$$

Moreover, if $c \mid a$ and $c \mid b$, then $c \mid r_0, c \mid r_1, \dots, c \mid r_n$. □

40. Chinese Remainder Theorem

Definition

40.1

If $\{R_i\}_{i \in I}$ is a family of rings, their **direct product** $\prod_{i \in I} R_i$ is defined as the direct product of the abelian groups, $(R_i, +)$, along with products defined component-wise.

Example 40.2. $R_1 \times R_2$ has $(x, y) + (x', y') = (x + x', y + y')$, and $(x, y)(x', y') = (xx', yy')$.

For the rest of this section, we assume all rings are commutative

Definition

40.3

Given two ideals I, J of a commutative ring R , we say that I and J are **comaximal** if $I + J = R$.

Example 40.4. $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z} \iff (m, n) = 1$.

Definition

40.5

The **product ideal** IJ is the ideal generated by all products xy , with $x \in I, y \in J$. That is,

$$IJ = \left\{ \sum_{i=1}^n x_i y_i \mid x_i \in I, y_i \in J, n \geq 1 \right\}$$

Chinese Remainder Theorem

40.6

If $I + J = R$, then $IJ = I \cap J$, and the map $\varphi : R \rightarrow R/I \times R/J$ given by $r \mapsto (r + I, r + J)$ is surjective, and induces a ring isomorphism

$$R/IJ = R/I \cap J \cong R/I \times R/J$$

Proof. It's clear that φ is a ring homomorphism and has kernel $I \cap J$. Since $I + J = R$, in particular there are elements $x \in I, y \in J$ such that $x + y = 1$. Given $(r + I, s + J) \in R/I \times R/J$, we claim $\varphi(xs + yr) = (r + I, s + J)$. Indeed,

$$\varphi(x) = (x + I, x + J) = (I, 1 - y + J) = (I, 1 + J) \equiv (0, 1).$$

Similarly, $\varphi(y) = (1, 0)$. Thus, $\varphi(xs + yr) = (0, s + J) + (r + I, 0) = (r + I, s + J)$ as desired. This proves φ is surjective.

Finally, we claim $I \cap J = IJ$. Note that $IJ \subset I \cap J$ always. If I and J are comaximal, with $x + y = 1$ as before, and $z \in I \cap J$, then $z = z \cdot 1 = z(x + y) = zx + zy \in IJ$. Hence $I \cap J \subset IJ$. $\square$

Example 40.7. 1. If $I_1, \dots, I_k$ are ideals of R such that $I_i + I_j = R$ for all pairs $i \neq j$, using induction we can show

$$R/I_1 \cdots I_k = R/(I_1 \cap \cdots \cap I_k) \cong R/I_1 \times \cdots \times R/I_k$$

2. The theorem gets its name from the special case $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ if $\gcd(m, n) = 1$. This comes from the ancient problem of finding a solution x to a system $x \equiv a \pmod{m}, x \equiv b \pmod{n}$. The result implies there is a unique solution x modulo mn .

41. Unique Factorization Domains

Motivation

Our favorite ring is $\mathbb{Z}$. How do we generalize the notion of a prime number in $\mathbb{Z}$? There are two properties we think about:

1. If $p = xy$, then $x = 1$ or $y = 1$
2. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

In $\mathbb{Z}$, these properties are equivalent, but in an arbitrary ring they may not be.

Definition

41.1

Let A be an integral domain. An element $a \in A \setminus (A^\times \cup \{0\})$ is **irreducible** if $a = bc \implies b \in A^\times$ or $c \in A^\times$. An element $p \in A \setminus \{0\}$ is **prime** if $Ap = (p)$ is a prime ideal (which is equivalent to $A/(p)$ being a domain).

Proposition

41.2

Suppose A is an integral domain. Then, any prime element is irreducible.

Proof. Let p be a prime element and suppose $p = bc$. Set $\bar{A} := A/Ap$. Then, $\bar{b} \cdot \bar{c} = 0$, and therefore $\bar{b} = 0$ or $\bar{c} = 0$, by the domain assumption. Assume $\bar{c} = 0$. Then,

$$c = pa \implies p = bc = bpa \implies p(ba - 1) = 0 \implies ab = 1,$$

thus b is a unit. Therefore, p is irreducible. $\square$

Corollary

41.3

Let A be a PID, $p \in A$. TFAE:

1. p is irreducible
2. p is prime
3. Ap is a maximal ideal.

Proof. Clearly (3) $\implies$ (2), and we showed (2) $\implies$ (1). Let's prove (1) $\implies$ (3).

Suppose p is irreducible, and contrarily suppose Ap is not maximal, so we have $Ap \subsetneq Ar \subsetneq A$ for some $r \in R$. Then, $p = rx$ for some x . Since $Ar \neq A$, r is not a unit, so x must be. Then, $r = x^{-1}p \in Ap$, hence $Ar \subset Ap$, a contradiction. $\square$

Corollary

41.4

We deduce that in a PID, all prime ideals are maximal.

Example 41.5. In $\mathbb{Z}$, the prime ideal $p\mathbb{Z}$ is maximal, so $\mathbb{Z}/p\mathbb{Z}$ is a field.

Definition

41.6

A **unique factorization domain** is an integral domain R in which every element $r \in R \setminus (R^\times \cup \{0\})$ satisfies

- (i) r is a product of irreducible elements.
- (ii) The decomposition in (i) is unique up to associates. Namely, if $r = p_1 \cdots p_n = q_1 \cdots q_m$, then $n = m$ and $\exists \sigma \in S_n$ such that $p_i = \varepsilon_i q_{\sigma(i)}$, with ε_i a unit.

By convention, we say 1 is equal to the empty product $\prod_{\emptyset} p_i$.

Example 41.7. 1. We'll soon show that PIDs are UFDs. So, $\mathbb{Z}, F[x]$ for F a field, and $\mathbb{Z}[i]$ are all UFDs. For example, any Gaussian integer has a unique factorization into Gaussian primes, up to units in $\mathbb{Z}[i]$, which are $\pm 1, \pm i$.

2. Consider $\mathbb{Z}[2i] = \{a + 2bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{Z}[i]$. The units in $\mathbb{Z}[2i]$ are just ± 1 . Observe that $2, 2i$ are irreducible in $\mathbb{Z}[2i]$ but are not associates. We thus have 2 distinct factorization of $4 = 2 \cdot 2 = (2i)(-2i)$. Therefore, $\mathbb{Z}[2i]$ is not a UFD. Moreover, $\mathbb{Z}[2i]/(2i) \cong \mathbb{Z}/4\mathbb{Z}$ which is not a domain, hence $2i$ is not prime. It follows that $\mathbb{Z}[2i]$ is not even a PID.

Proposition**41.8**

Let R be an integral domain. Then, TFAE:

- (i) R is a UFD
- (ii) (a) Any $x \in R \setminus \{0\}$ is a product of irreducible elements and (b) Irreducible elements are prime.
- (iii) (a) If $(r_1) \subset (r_2) \subset \cdots$ is an ascending chain of principal ideals, then there exists N such that $(r_i) = (r_{i+1})$ for all $i \geq N$, and (b) Irreducible elements are prime.

Proof.

(i) $\implies$ (ii): (a) holds by definition. For (b), suppose x is irreducible, and suppose $x \mid ab$. Then, x must appear in the unique factorization of a or b into irreducibles. Hence, $x \mid a$ or $x \mid b$. Thus, x is prime.

(ii) $\implies$ (i): Suppose $x = p_1 \cdots p_n = q_1 \cdots q_s$ with p_i, q_j primes (same as irreducibles). We use induction on n : Since p_1 divides $q_1 \cdots q_s$ and p_1 is prime, we have p_1 divides some q_i , so $q_i = p_1 \varepsilon_i$ with $\varepsilon_i \in R^\times$. Now, we set $\sigma(1) = i$, and cancel to get $p_2 \cdots p_n = q_1 \cdots \widehat{q_i} \cdots q_s$ up to a unit. By induction, we have $n - 1 = s - 1$, and σ can be extended to a permutation in S_n .

(ii) $\implies$ (iii): Given $(r_1) \subset (r_2) \subset \cdots$, suppose r_k is such that it has the least number of elements in its factorization into irreducibles (which are the same as primes). Suppose there exists $(r_j) \supsetneq (r_k)$. Then, $r_k = r_j x$ with x not a unit. It follows that r_j has less elements in its factorization than r_k , a contradiction. Thus, $(r_k) = (r_j)$ for all $j \geq k$.

(iii) $\implies$ (ii): It suffices to show that each $x \in R \setminus \{0\}$ is a product of irreducible elements. If x is irreducible or a unit, we're done. Otherwise, x has a factorization $x = r_1 r_2$ with r_1, r_2 not units. If both r_1 and r_2 are irreducible, we're done. Otherwise, one of them factors further, etc. The continued factorization leads to an ascending sequence of principal ideals, which must terminate by assumption. This termination corresponds to irreducibility of factors. $\square$

Theorem**41.9**

R is a PID $\implies R$ is a UFD.

Proof. We check that R satisfies (iii). We've already shown that if x is irreducible, then x is prime. Given an ascending chain $(r_1) \subset (r_2) \subset \cdots$, we form the ideal $I = \bigcup (r_i)$. Since R is a PID, $I = (r)$ for some r . Then, there must exist some r_k such that $r \in (r_k)$. Thus, $(r_k) \subset (r) \subset (r_k)$, so the chain stabilizes. $\square$

Remark 41.10. Greatest common divisors and least common multiples exist in UFDs. In fact, if R is a UFD and $x, y \in R$, we work as follows: For each principal prime ideal I , fix a generator p so $I = Rp$, and let $\mathcal{P}$ be the set of all chosen primes. Then,

$$x = \varepsilon \prod_{p \in \mathcal{P}} p^{v_p(x)}, y = \varepsilon' \prod_{p \in \mathcal{P}} p^{v_p(y)}$$

and then

$$\gcd(x, y) = \prod_{p \in \mathcal{P}} p^{\min\{v_p(x), v_p(y)\}}, \text{lcm}(x, y) = \prod_{p \in \mathcal{P}} p^{\max\{v_p(x), v_p(y)\}}$$

However, we don't necessarily have a Euclidean algorithm for finding them.

Diagram of Containment

Fields $\subsetneq$ Euclidean Domains $\subsetneq$ PIDs $\subsetneq$ UFDs $\subsetneq$ Integral Domains. The last containment is huge.

Between UFDs and integral domains we have Dedekind domains. In **Dedekind domains**, unique factorization of elements fails, but one has unique factorization of ideals into prime ideals.

Motivating Questions

1. If F is a field, we know $F[x]$ is a PID, hence a UFD. What about $F[x, y]$? We'll show that if A is a UFD, then $A[x]$ is a UFD. Then, $F[x, y] = (F[x])[y]$ is a UFD.
2. Suppose $f \in \mathbb{Z}[x]$ is irreducible. Is f still irreducible in $\mathbb{Q}[x]$?

Definition

41.11

For a UFD A , if $f \in A[x] \setminus \{0\}$ with $f(x) = \sum_{i=0}^n a_i x^i$, the **content** of f , denoted $c(f)$, is the gcd of all non-zero coefficients of f . We say that f is **primitive** if $c(f) = 1$. If $c(f) = d$, then $a_i = a'_i d$, so $f = c(f) \cdot f'$, where $f' = \sum a'_i x^i$ is primitive.

If $0 \neq f = df'$ for some $d \in A$, then $c(f) = d \iff c(f') = 1$.

Gauss's Lemma

41.12

If A is a UFD, and $f, g \in A[x] \setminus \{0\}$, then $c(fg) = c(f)c(g)$.

Proof. Write $f = c(f)f_1$ and $g = c(g)g_1$ with f_1, g_1 primitive. Then, $f \cdot g = c(f)c(g)f_1g_1$, so it suffices to show that the product of two primitive polynomials is primitive.

Sub-lemma

$p \in A$ is prime $\iff p$ is prime in $A[x]$.

Proof. For any ideal I of A , let $I[x]$ be the ideal of $A[x]$ generated by I . We have

$$I[x] = \left\{ \sum_{i=0}^n a_i x^i \mid a_i \in I, n \geq 0 \right\}$$

The canonical map $\pi : A \rightarrow A/I$ induces a map $\tilde{\pi} : A[x] \rightarrow (A/I)[x]$ called a **reduction of coefficients mod I** . We have $\ker \tilde{\pi} = I[x]$, and therefore we obtain an isomorphism $A[x]/I[x] \cong (A/I)[x]$. Now, I is a prime ideal in $A \iff A/I$ is a domain $\iff (A/I)[x]$ is a domain $\iff I[x]$ is a prime ideal in $A[x]$. Applying this to $I = (p)$, we obtain the sub-lemma. $\square$

Now, suppose f, g are both primitive in $A[x]$ and $c(fg) = d$. Let $p \in A$ be a prime dividing d . Then, $p \mid fg$ in $A[x]$. Since p remains prime in $A[x]$, we get that $p \mid f$ or $p \mid g$, contradicting the

fact that f and g are primitive. □

Corollary**41.13**

Suppose A is a UFD, and K is the quotient field of A . Then,

1. If $f \in A[x] \setminus \{0\}$ is irreducible, with $\deg f > 0$, then f is irreducible in $K[x]$.
2. Suppose $f \in A[x]$ is primitive. Then, the ideal $K[x] \cdot f$ in $K[x]$ satisfies $K[x]f \cap A[x] = A[x]f$.

Proof.

1. If f is irreducible, then f must be primitive, for $f = c(f)f_1$, with f_1 primitive, and $c(f_1)$ must be a unit. Suppose f is reducible in $K[x]$, so let $f = g \cdot h$, where $g, h \in K[x]$, and $\deg f > \deg g, \deg h > 0$. Write $g = g_1/a$ and $h = h_1/b$, with $a, b \in A \setminus \{0\}$ and $g_1, h_1 \in A[x]$. Then, $abf = g_1h_1$ and $ab = c(abf) = c(g_1)c(h_1)$, hence $abf = c(g_1)c(h_1)g_2h_2$, where $g_2, h_2 \in A[x]$ are primitive. Thus, $f = g_2h_2$, which is a contradiction as g_2, h_2 are not units.
2. Suppose f is primitive, and $g \in K[x]f \cap A[x]$. Then, $g = hf$ for some $h \in K[x]$. Now, there exists $a \in A \setminus \{0\}$ so that $ag = h_1f$ with $h_1 \in A[x]$. Also, $ac(g) = c(h_1) \implies h_1 = ac(g)h_2f \implies g = c(g)h_2f$, and since $c(g)h_2 \in A[x]$, we're done. □

Gauss's Theorem**41.14**

A is a UFD $\implies A[x]$ is a UFD.

Proof. We start with the following lemma

Lemma**41.15**

$f \in A[x] \setminus \{0\}$ irreducible $\implies f$ is prime.

Proof. If $\deg f = 0$ is irreducible in A , a UFD, hence f is prime in A , and also in $A[x]$. If $\deg f > 0$, then f is primitive, hence $K[x]f \cap A[x] = A[x]f$. Consider the map

$$\eta : A[x] \xrightarrow{i} K[x] \xrightarrow{\pi} K[x]/K[x]f.$$

Clearly, $\ker \eta = K[x]f \cap A[x] = A[x]f$. Hence we get an inclusion $A[x]/A[x]f \hookrightarrow K[x]/K[x]f$. Now, f is irreducible in $A[x]$, so f is irreducible in $K[x]$ by the corollary. Therefore, since K is a field, $K[x]$ is a PID, so f is prime in $K[x]$, hence $K[x]/K[x]f$ is a domain. It follows that $A[x]/A[x]f$ is a domain, hence f is prime in $A[x]$. □

Our second claim is:

Lemma**41.16**

Any $f \in A[x] \setminus \{0\}$ is a product of irreducible elements.

Proof. We will prove this by induction on $n = \deg f$. If $n = 0$, then $f \in A$, so $f = \prod p_i$, with p_i primes in A , which remain irreducible in $A[x]$. If $n > 0$, we can factor $f = c(f) \cdot f_1$, where $f_1 \in A[x]$ is primitive. It suffices to show that f_1 is a product of irreducibles. If f_1 is not irreducible,

we have a factorization $f_1 = gh$, with $0 < \deg g, \deg h < \deg f = n$. By induction, g and h are products of irreducibles, and we're done. $\square$

Gauss's Theorem now follows from [Proposition 41.8](#). $\square$

Corollary

41.17

If A is a UFD, then $A[x_1, \dots, x_n]$ is a UFD. Hence $\mathbb{Z}[x_1, \dots, x_n], F[x_1, \dots, x_n]$ are UFDs (F is a field).

It's worth noting that they are not PIDs, as $(x_1, \dots, x_n)$ is not principal for $n \geq 2$.

42. Irreducibility in Polynomial Rings

We want to obtain irreducibility tests in $A[x]$, when A is a UFD. By Gauss's Lemma, it suffices to consider factorizations in $K[x]$, where $K = Q(A)$.

Proposition

42.1

A polynomial $p \in F[x]$ has a linear factor $\iff p(x)$ has a root in F . Hence, a polynomial of degree 2 or 3 is irreducible in $F[x] \iff$ it has no roots in $F[x]$.

Example 42.2. $p(x) = x^2 + x + 1$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$, since $0^2 + 0^2 + 1 = 1^2 + 1 + 1 = 0 \neq 1 \pmod{2}$. It follows that $\mathbb{F}_4 := (\mathbb{Z}/2\mathbb{Z})[x]/(x^2 + x + 1)$ is a field with 4 elements, the classes of $0, 1, x, x + 1$.

Checking for rational roots of a polynomial in $\mathbb{Q}[x]$ is easy using:

Rational Root Theorem

42.3

Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$, with $a_n \neq 0$. If $\frac{r}{s} \in \mathbb{Q}$ with $(r, s) = 1$ is a root of $p(x)$, then $r \mid a_0, s \mid a_n$.

Proof. $p(\frac{r}{s}) = 0 \implies a_n r^n + a_{n-1} s r^{n-1} + \dots + a_1 s^{n-1} r + a_0 s^n = 0$, hence $s \mid a_n r^n \implies s \mid a_n$. Similarly, $r \mid a_0$. $\square$

Note

There is an analogous property for any UFD in place of $\mathbb{Z}$.

Reducing Modulo an Ideal

42.4

Let R be an integral domain and I be a proper ideal of R . Let $p \in R[x]$ be a non-constant monic polynomial. If the image of $p(x)$ in $(R/I)[x]$, under the reduction mod I map, cannot be factored in $(R/I)[x]$ into two polynomials of strictly smaller degree, then p is irreducible in $R[x]$.

Proof. If $p(x) = f(x)g(x)$, then the leading coefficients of f and g are units in R . WLOG, we may assume f and g are monic. But then reducing mod I gives a non-trivial factorization in $(R/I)[x]$,

contradicting the assumption. $\square$

Example 42.5. 1. $x^2 + x + 1 \in \mathbb{Z}[x]$ is irreducible, since it's irreducible in $(\mathbb{Z}/2\mathbb{Z})[x]$. Note that it does reduce modulo 3: $x^2 + x + 1 \equiv (x - 1)^2 \pmod{3}$, so the inverse of the previous proposition does not hold.

2. $x^4 + 1 \in \mathbb{Z}[x]$ is irreducible, but it is reducible modulo every prime $p \in \mathbb{Z}$.

We have a special case:

Eisenstein's Criterion

42.6

Let P be a prime ideal of an integral domain R , and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a monic polynomial with coefficients in R , $n \geq 1$. Suppose $a_{n-1}, \dots, a_1, a_0 \in P$, but $a_0 \notin P^2$. Then, $f(x)$ is irreducible in $R[x]$.

Proof. If we can reduce $f(x) = g(x)h(x) \in R[x]$, then reducing mod P gives

$$\bar{f}(x) = \bar{g}(x)\bar{h}(x) = \bar{x}^n \in (R/P)[x],$$

since all the coefficients vanish. Since R/P is a domain, $\bar{g}$ and $\bar{h}$ must both have a zero constant term, which implies the constant terms of g and h are both in P . But then $a_0 \in P^2$, a contradiction. $\square$

Corollary

42.7

If $f(x) \in \mathbb{Z}[x]$, then $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, and p is a prime such that $p \mid a_{n-1}, \dots, a_0$, but $p^2 \nmid a_0$, then f is irreducible in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

Example 42.8. 1. $x^4 + 10x + 5$ is irreducible in $\mathbb{Z}[x]$.

2. Let $p \in \mathbb{Z}$ be prime, and consider the cyclotomic polynomial $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$. Then, $\Phi_p(x)$ is irreducible $\iff \Phi_p(x + 1)$ is irreducible, and

$$\Phi_p(x + 1) = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-1}x + p.$$

Since $p \mid \binom{p}{k}$ for all $k \in [1, p-1]$, Eisenstein's Criterion applies, proving $\Phi_p(x)$ is irreducible.

3. Let t be a variable and consider $f(x) = x^n - t \in R[x]$, where $R = \mathbb{Q}[t]$. Now, $P := (t)$ is prime (in fact maximal) in R , since $\mathbb{Q}[t]/(t) \cong \mathbb{Q}$. Eisenstein's criterion shows that f is irreducible in $R[x]$.

4. The irreducible polynomials in $\mathbb{R}[x]$ are linear or quadratic: By FTA, any polynomial $f \in \mathbb{C}[x]$ reduces to linear factors: $f(x) = \prod_{i=1}^n (x - p_i)$, $p_i \in \mathbb{C}$. If $f \in \mathbb{R}[x]$ and $\deg f > 2$, then if f has a root $\rho \in \mathbb{R}$, it's divisible by $(x - \rho) \in \mathbb{C}[x]$, hence also in $\mathbb{R}[x]$. Otherwise, it has a pair of complex conjugate roots z and $\bar{z}$, so f is divisible by $(x - z)(x - \bar{z}) \in \mathbb{R}[x]$, hence is reducible in $\mathbb{R}[x]$.

43. Noetherian Rings

(Emmy Noether $\sim$ 1880 – 1930)

Rings need some notion of "finiteness", analogous to "finite dimensional" for vector spaces. For many applications, the most fruitful way to define this is the Noetherian condition.

Definition

43.1

A (not necessarily commutative) ring A is (left) **Noetherian** if every (left) ideal in A is finitely generated.

Proposition

43.2

Let A be a ring. TFAE:

- (i) A is Noetherian
- (ii) If $I_1 \subset I_2 \subset \cdots$ is an **ascending chain** of ideals, then there exists m such that $I_k = I_m$ for all $k \geq m$. (This was Noether's original definition)
- (iii) The ideals of A satisfy a "**maximum condition**": If $\mathcal{F}$ is any non-empty collection of ideals in A , then $\mathcal{F}$ contains a maximal element.

Proof. (ii) $\iff$ (iii) is immediate.

(i) $\implies$ (ii): If $I_1 \subset I_2 \subset \cdots$ is a chain of ideals, then $I := \bigcup_{j=1}^{\infty} I_j$ is also an ideal, which by (i) is finitely generated: $I = (x_1, \dots, x_n)$ for some $x_i \in A$. Thus, there exists $m \geq 1$ such that $x_i \in I_m$ for all $i \in [1, n]$. So, $I = I_m$, and the chain stabilizes at m .

(iii) $\implies$ (i): Let I be an ideal of A . Let $\mathcal{F} := \{J \subset I \mid J \text{ is finitely generated ideal}\}$. Let J_0 be a maximal element of $\mathcal{F}$. If $J_0 \subsetneq I$, choose $x_0 \in I \setminus J_0$, and form $J'_0 = J_0 + Ax_0$. Then, J'_0 is finitely generated, and $J_0 \subsetneq J'_0$, a contradiction. $\square$

Hilbert Basis Theorem

43.3

If A is a commutative Noetherian ring, then $A[x]$ is Noetherian.

Proof. Given a polynomial $f(x) = a_n x^n + \cdots + a_0$, with $a_n \neq 0$, we call a_n the **leading coefficient** of f . Given an ideal $I \subset A[x]$, we define a sequence $f_1, f_2, \dots \in I$ as follows: f_1 is a non-zero element of least degree in I . For each $n \geq 1$, if $(f_1, \dots, f_n) \neq I$, choose f_{n+1} to be an element of least degree in $I \setminus (f_1, \dots, f_n)$. Otherwise, stop (we want to prove I is finitely generated). Let a_j be the leading coefficient of f_j . Since A is Noetherian, $J := (a_1, a_2, \dots)$ is finitely generated. We may choose a set of generators among the a_j , so say $J = (a_1, a_2, \dots, a_m)$. We claim $I = (f_1, \dots, f_m)$. If not, our process chose $f_{m+1} \in I \setminus (f_1, \dots, f_m)$, so write $a_{m+1} = \sum_{j=1}^m u_j a_j$ for some $u_j \in A$. Since the degree of f_{m+1} by construction is $\geq$ the degree of f_i for $1 \leq i \leq m$, we can define $g := \sum_{j=1}^m u_j f_j x^{\deg f_{m+1} - \deg f_j} \in (f_1, \dots, f_m)$. Now, $f_{m+1} - g$ is in $I \setminus (f_1, \dots, f_m)$, and has degree $< \deg f_{m+1}$, a contradiction by construction. $\square$

We're basically going to assume every ring is commutative from now on.

Corollary

43.4

If A is Noetherian, then $A[x_1, \dots, x_n]$ is Noetherian. So, $\mathbb{Z}[x_1, \dots, x_n], F[x_1, \dots, x_n]$ are Noetherian.

Example 43.5. $\mathbb{Z}[x_1, x_2, \dots]$ is a UFD, but not Noetherian.

Proposition**43.6**

If A is commutative and Noetherian, and $I \subset A$ is an ideal, then A/I is Noetherian. If $f : A \rightarrow B$ is a surjective homomorphism, then B is Noetherian.

Proof. We know that any ideal of A/I is of the form J/I , where J is an ideal of A containing I . So, if $x_1, \dots, x_r$ are generators of J , then $x_1 + I, \dots, x_r + I$ are generators of J/I . If $f : A \rightarrow B$ is onto, then $B \cong A / \ker f$. $\square$

Algebraic Geometry

44. Introduction to Algebraic Geometry

We study the solutions of systems of polynomials, working over $\mathbb{C}$, although most everything we say can also be done over arbitrary fields.

Definition

44.1

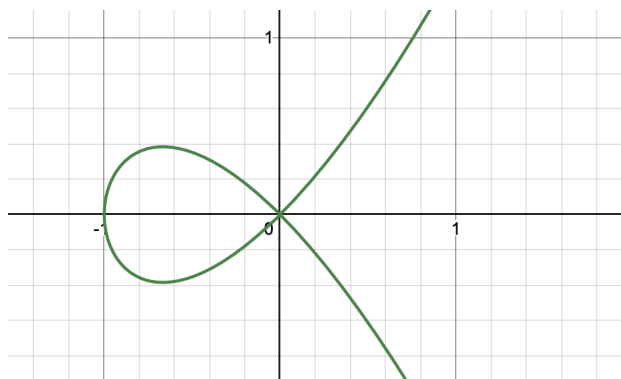
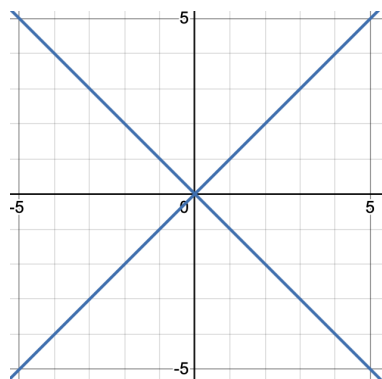
Affine n -space $\mathbb{A}^n := \mathbb{A}^n(\mathbb{C})$ is just $\mathbb{C}^n$; its elements are points. $\mathbb{A}^1$ is the affine line, $\mathbb{A}^2$ is the affine plane.

Normally, the letter $\mathbb{A}$ is used to denote an arbitrary field, but we're only looking at $\mathbb{C}$, so we may just think of it as $\mathbb{C}^n$.

Given $f \in \mathbb{C}[x_1, \dots, x_n]$, a point $a = (a_1, \dots, a_n) \in \mathbb{A}^n$ is a **zero** of f if $f(a) = 0$. If f is not constant, the set of zeroes of f is the **hypersurface** defined by f , denoted $V(f)$. If f has degree 1, then $V(f)$ is a **hyperplane** in $\mathbb{A}^n$.

Example 44.2. The following are pictured below

1. $V(x^2 - y^2) \subset \mathbb{A}^2$
2. $V(y^2 - x^2(x + 1)) \subset \mathbb{A}^2$



Definition

44.3

More generally, if S is any set of polynomials in $\mathbb{C}[x_1, \dots, x_n]$, we let

$$V(S) = \{P \in \mathbb{A}^n \mid f(P) = 0, \forall f \in S\} = \bigcap_{f \in S} V(f)$$

If $S = \{f_1, \dots, f_r\}$, we write $V(f_1, \dots, f_r)$ instead of $V(\{f_1, \dots, f_r\})$. A subset $X \subset \mathbb{A}^n$ is an **affine algebraic set** if $X = V(S)$ for some S .

Proposition

44.4

1. If $I = (S)$ is the ideal of $\mathbb{C}[x_1, \dots, x_n]$ generated by S , then $V(S) = V(I)$. So, every algebraic set is equal to $V(I)$ for some ideal I
2. If $\{I_\alpha\}$ is any collection of ideals, then

$$V\left(\bigcup_{\alpha} I_{\alpha}\right) = \bigcap_{\alpha} V(I_{\alpha}).$$

So, the intersection of algebraic sets is an algebraic set.

3. If $I \subset J$, then $V(J) \subset V(I)$.
4. $V(fg) = V(f) \cup V(g)$ for all $f, g \in \mathbb{C}[x_1, \dots, x_n]$. More generally, $V(IJ) = V(I) \cup V(J)$.
So, any finite union of algebraic sets is an algebraic set.

$$5. V((0)) = \mathbb{A}^n, V((1)) = \emptyset$$

$$(5') V(X_1 - a_1, X_2 - a_2, \dots, X - a_n) = \{(a_1, \dots, a_n)\}$$

Properties (2), (4), and (5) say that the algebraic sets are the closed sets of a topology on $\mathbb{A}^n$. This is the **Zariski topology**. (5') show that finite subsets of $\mathbb{A}^n$ are algebraic.

Exercise

Check that $V(IJ) = V(I \cap J)$, even though $IJ \subsetneq I \cap J$ in general.

Example 44.5. In $\mathbb{A}^2$, coordinates x and y , let $I := (x)$, $J := (y)$, $IJ = (xy)$, $\langle I \cup J \rangle = \langle x, y \rangle$. $V(x)$ is the y -axis, $V(y)$ is the x -axis, $V(xy)$ is the x and y axes, and $V(x, y)$ is the origin.

45. The Ideal of a Set of Points**Definition**

45.1

For any subset $X \subset \mathbb{A}^n$, let

$$I(X) := \{f \in \mathbb{C}[x_1, \dots, x_n] \mid f(x) = 0, \forall x \in X\}.$$

Then, $I(X)$ is an ideal of $\mathbb{C}[x_1, \dots, x_n]$ called the ideal of X .

Proposition

45.2

1. If $X \subset Y$, then $I(Y) \subset I(X)$
2. $S \subset I(V(S))$ for any set S of polynomials. Similarly, $X \subset V(I(X))$ for any set X of points.
3. $V(I(V(S))) = V(S)$ for any set S of polynomials, and $I(V(I(X))) = I(X)$ for any set X of points.

So, if V is an algebraic set, then $V = V(I(V))$, and if I is the ideal of an algebraic set, then $I = I(V(I))$.

Example 45.3. Not all ideals are ideals of algebraic sets. For example, $J := (x^2) \subset \mathbb{C}[x]$ has $V(J) = \{0\}$, but $I(\{0\}) = (x) \neq J$. If $I = I(X)$ and $f^n \in I$ for some $n > 0$, then $f \in I$. This says exactly that

$I = \text{rad}(I)$, so I is a radical ideal.

Proposition

45.4

$I(X)$ is a radical ideal for any set $X \subset \mathbb{A}^n$. (Later, we'll show that radical ideals are exactly the ideals of algebraic sets.)

Hilbert Basis Theorem For $\mathbb{C}[x_1, \dots, x_n]$, Rephrased

45.5

Every algebraic set is the intersection of a finite number of hypersurfaces.

Note

Notice how the algebraic set comprised x and y axes together is "reducible", into the irreducible algebraic sets the x -axis and y -axis.

Definition

45.6

We say an algebraic set V is **reducible** if $V = V_1 \cup V_2$, where V_1 and V_2 are algebraic sets in $\mathbb{A}^n$, $V_i \subsetneq V$, $i = 1, 2$. Otherwise, we say V is irreducible.

Proposition

45.7

An algebraic set V is irreducible $\iff I(V)$ is a prime ideal.

Proof. If $I(V)$ is not prime, then there exist F_1, F_2 with $F_1 F_2 \in I(V)$, but neither F_1 nor F_2 are in $I(V)$. Then, $V = (V \cap V(F_1)) \cup (V \cap V(F_2))$. Then, $V \cap V(F_1) \neq V$ and $V \cap V(F_2) \neq V$, so V is reducible.

Conversely, suppose $V = V_1 \cup V_2$, $V_i \subsetneq V$. Then, $I(V_i) \supsetneq I(V)$ [If $I(V_i) = I(V)$, then $V_i = V(I(V_i)) = V(I(V)) = V$, a contradiction.] Let $F_i \in I(V_i)$, $F_i \notin I(V)$. Then $F_1 F_2 \in I(V)$, so $I(V)$ is not prime. $\square$

Theorem

45.8

If I is a prime ideal, then $V(I)$ is irreducible.

This is much harder to show.

Theorem

45.9

Let $V \subset \mathbb{A}^n$ be an algebraic set. Then, there are unique irreducible algebraic sets $V_1, \dots, V_m$ such that $V = V_1 \cup V_2 \cup \dots \cup V_m$, and $V_i \not\subset V_j$ for all $i \neq j$. The V_i are the **irreducible components** of V .

Proof. Recall that since $\mathbb{C}[x_1, \dots, x_n]$ is Noetherian, any collection of ideals has a maximal element. Rephrased, this implies that any collection of algebraic sets has a minimal element. Let $\mathcal{S} := \{\text{Algebraic sets } V \subset \mathbb{A}^n \mid V \text{ is not the union of finitely many irreducible algebraic sets}\}$. We want to show $\mathcal{S} = \emptyset$. Otherwise, $\mathcal{S}$ has a minimal member V . Since $V \in \mathcal{S}$, it's not irreducible. So, $V = V_1 \cup V_2$ with $\emptyset \neq V_i \subset V$, V_i algebraic. Now, $V_1, V_2 \notin \mathcal{S}$, so $V_i = \cup V_{i_k}$ for $i = 1, 2$ and V_{i_k}

irreducibles. Then, $V = \cup_{i,k} V_{i,k}$, a contradiction.

Hence, any algebraic set $V = V_1 \cup \cdots \cup V_m$ for V_i irreducible. To achieve the second condition, if $V_i \subset V_j$ for some $i \neq j$, then throw away V_i . This proves existence. Now, suppose $V = V_1 \cup \cdots \cup V_m = W_1 \cup \cdots \cup W_s$. Then,

$$V_i = V_i \cap \left(\bigcup_{j=1}^s W_j \right) = \bigcup_{j=1}^s (V_i \cap W_j)$$

and V_i is irreducible, so $V_i \subset W_{j(i)}$ for some $j(i)$. Similarly, $W_{j(i)} \subset V_k$ for some k . Then, $V_i \subset W_{j(i)} \subset V_k \implies k = i$, so $V_i = W_{j(i)}$. Likewise, each W_j is equal to some $V_{i(j)}$. $\square$

Definition

45.10

Let R be a commutative ring. We define the **Krull Dimension** of R to be the maximum m such that there exists a chain of prime ideals $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_m \subset R$.

Thought Exercise

What does the previous theorem say in terms of ideals in $\mathbb{C}[x_1, \dots, x_n]$? More generally, for any commutative Noetherian ring?

Answer (Lasker-Noether)

Primary decomposition theorem for ideals in Noetherian Rings, which generalizes the fundamental theorem of arithmetic.

46. Algebraic Subsets of the Line and Plane

For the affine line $\mathbb{A}^1(\mathbb{C}) = \mathbb{C}$, if $V = V(I)$ is an algebraic subset, then $I = (f(x))$, so V is $\emptyset$, $\mathbb{A}^1$, or a finite number of points, which the roots corresponding to the roots of f . If $f(x) = \prod_{i=1}^n (x - a_i)^{k_i}$, then $\text{rad}(I) = (\prod_{i=1}^n (x - a_i))$. The irreducible algebraic sets are $\emptyset$, $\mathbb{A}^1$, and single points.

Proposition

46.1

Let f, g be polynomials in $\mathbb{C}[x, y]$ with no common factors. Then, $V(f, g) = V(f) \cap V(g)$ is a finite number of points.

Proof. f and g are coprime in $\mathbb{C}[x][y]$. By Gauss's lemma, f and g are coprime in $\mathbb{C}(x)[y]$, which is a PID because $\mathbb{C}(x)$ is a field. Hence, $(f, g) = (1)$ in $\mathbb{C}(x)[y]$, so there exists $r, s \in \mathbb{C}(x)[y]$ with $rf + sg = 1$. Now, there is a polynomial $d(x) \in \mathbb{C}[x]$ so that $dr = a, ds = b$ both lie in $\mathbb{C}[x, y]$ (eliminating denominators), hence $af + bg = d \in \mathbb{C}[x, y]$. If $(a_0, b_0) \in V(f, g)$, then $d(a_0) = 0$. But, d only has a finite number of zeroes, hence there is a finite number of x -coordinates which appear in $V(f, g)$. The same reasoning can be applied to the y -coordinates, proving that $V(f, g)$ is finite. $\square$

Lemma**46.2**

If $F \in \mathbb{C}[x, y]$ is any non-constant polynomial, then $V(F)$ is infinite.

Proof. On homework □

Corollary**46.3**

If $f \in \mathbb{C}[x, y]$ is irreducible, then $I(V(f)) = (f)$ and $V(f)$ is irreducible.

Proof. If $g \in I(V(f))$, then $V(f, g) \supset V(f)$, which is infinite by the lemma. The previous proposition therefore implies that f and g are not coprime, so as f is irreducible, we have $f \mid g$. That is, $g \in (f)$. The opposite inclusion is immediate, therefore $I(V(f)) = (f)$. Finally, since (f) is prime, a previous proposition implies $V(f)$ is irreducible. □

Corollary**46.4**

The irreducible algebraic subsets of $\mathbb{A}^2$ are $\emptyset$, $\mathbb{A}^2$, points, and irreducible plane curves $V(f)$, where $f \in \mathbb{C}[x, y]$ is irreducible.

Proof. Suppose V is any irreducible algebraic set. If V is finite, or $I(V) = (0)$, then V is of the required type. Otherwise, let $f \in I(V)$ be non-constant, and since $I(V)$ is prime, some irreducible factor of f lies in $I(V)$, so we can assume f is irreducible. Then, we claim $I(V) = (f)$: if $g \in I(V)$, $g \notin (f)$, then $V \subset V(f, g)$ is finite, because f, g are coprime, a contradiction. □

Corollary**46.5**

Let $f \in \mathbb{C}[x, y]$ and $f = \prod_{i=1}^r f_i^{n_i}$ be the decomposition of f into irreducible factors. Then, $V(f) = V(f_1) \cup \cdots \cup V(f_r)$, so this is the decomposition of $V(f)$ into irreducible components, and $I(V(f)) = (f_1 \cdots f_r)$.

Proof. No f_i divides f_j for $i \neq j$, so there are no inclusion issues among the $V(f_i)$. Moreover,

$$I\left(\bigcup_i V(f_i)\right) = \bigcap_i I(V(f_i)) = \bigcap_i (f_i) = (f_1 \cdots f_r)$$

□

47. Hilbert's Nullstellensatz (Theorem of the Zeroes)

This gives the relationship between ideals of $\mathbb{C}[x_1, \dots, x_n]$ and algebraic sets.

Question

Given some ideal $I \subset \mathbb{C}[x_1, \dots, x_n]$, when is $V(I) \neq \emptyset$.

If $1 \in I$, then clearly $V(I)$ is empty. What about the converse?

Let $I \subsetneq \mathbb{C}[x_1, \dots, x_n]$ be a proper ideal, and let M be a maximal ideal containing I . Then, $V(I) \supset V(M)$. What can we prove about M ?

Weak Nullstellensatz

47.1

The maximal ideals in $\mathbb{C}[x_1, \dots, x_n]$ are in bijective correspondence with the points of $\mathbb{A}^n = \mathbb{C}^n$. So, each point $(a_1, \dots, a_n)$ corresponds to the ideal

$$M_a := (x_1 - a_1, \dots, x_n - a_n).$$

Proof. We first check that M_a is indeed maximal. We have an evaluation map at $a = (a_1, \dots, a_n)$: $ev : \mathbb{C}[x_1, \dots, x_n] \rightarrow \mathbb{C}, f \mapsto f(a)$. We claim that $\ker(ev) = M_a$. Clearly, $M_a \subset \ker(ev)$. Conversely, assume $f(a) = 0$, and expand f into a Taylor expansion around a :

$$f(x) = f(a) + \sum_i c_i(x_i - a_i) + \sum_{i,j} c_{i,j}(x_i - a_i)(x_j - a_j) + \dots$$

Since $f(a) = 0$, we see that $f \in M_a$. Thus, $\mathbb{C}[x_1, \dots, x_n]/M_a \cong \mathbb{C}$ is a field, hence M_a is maximal. Now, let M be a maximal ideal of $\mathbb{C}[x_1, \dots, x_n]$. Consider the map

$$\pi_1 : \mathbb{C}[x_1] \hookrightarrow \mathbb{C}[x_1, \dots, x_n] \rightarrow \mathbb{C}[x_1, \dots, x_n]/M = K,$$

where K is a field. Then, $\ker \pi_1$ is either 0 or a maximal ideal of $\mathbb{C}[x_1]$, which we see because $\mathbb{C}[x_1]/\ker \pi_1 \hookrightarrow K$, so it's a domain, and $\mathbb{C}$ is a PID (prime ideals are maximal).

Now, we claim $\ker \pi_1 \neq 0$. Suppose not: then, $\pi_1 : \mathbb{C}[x] \hookrightarrow K$. By the universal property of the quotient field $\mathbb{C}(x_1)$, π_1 extends to an injection $\mathbb{C}(x_1) \hookrightarrow K$. Thus, K contains a field isomorphic to $\mathbb{C}(x)$. As a vector space over $\mathbb{C}$, $\mathbb{C}[x_1, \dots, x_n]$ has a countable basis, namely $\{x_1^{a_1}, \dots, x_n^{a_n}\}_{a_i \geq 0}$. Therefore $K = \mathbb{C}[x_1, \dots, x_n]/M$ must also have a countable basis $\{v_1, v_2, \dots\}$. Now, if $S \subset K$ is any linearly independent set, then S is also countable, since $S = \bigcup_{n \geq 1} (S \cap \langle v_1, \dots, v_n \rangle)$ is a countable union of finite sets. On the other hand, $\mathbb{C}(x)$ contains the elements $\frac{1}{x-a}$, where $a \in \mathbb{C}$, and these form an uncountable linearly independent set, a contradiction. (If $\sum \frac{\lambda_i}{x-a_i} = 0$, and $\lambda_i \neq 0$, then the limit as $x \rightarrow a_i$ of the LHS is ∞). We've therefore shown that $\ker \pi_1 \neq 0$, hence it's a maximal ideal of $\mathbb{C}[x_1]$, which we know must be $(x_1 - a_1)$ for some $a_1 \in \mathbb{C}$. It follows that $(x_1 - a_1) \in M$, and the same argument can be applied for all x_i . So $x_i - a_i \in M$ for $1 \leq i \leq n$, and $a_i \in \mathbb{C}$, but then $M_a \subset M$, so $M = M_a$. $\square$

Corollary

47.2

If $I \subset \mathbb{C}[x_1, \dots, x_n]$ is a proper ideal, then $V(I) \neq \emptyset$.

Proof. I must be contained in some maximal ideal M , and $V(I) \supset V(M) \neq \emptyset$ $\square$

Corollary

47.3

If $n = 1$, we get the fundamental theorem of algebra.

Strong Nullstellensatz

47.4

Let I be an ideal in $\mathbb{C}[x_1, \dots, x_n]$. Then, $I(V(I)) = \text{rad}(I)$. Concretely, this says: Let $I = (f_1, \dots, f_r)$. If g is such that g vanishes wherever $f_1, \dots, f_r$ all vanish, then there is an equation $g^N = a_1 f_1 + \dots + a_r f_r$ for some $N \in \mathbb{N}$, $a_1, \dots, a_r \in \mathbb{C}[x_1, \dots, x_n]$.

Proof. Note that $\text{rad}(I) \subset I(V(I))$ is easy (exercise). Suppose $g \in I(V(f_1, \dots, f_r))$, with $f_i \in \mathbb{C}[x_1, \dots, x_n]$. Consider the ideal

$$J = (f_1, \dots, f_r, x_{n+1}g - 1) \subset \mathbb{C}[x_1, \dots, x_n, x_{n+1}].$$

Then, notice that $V(J) = \emptyset$, because when $f_1, \dots, f_r$ all vanish, g does as well, and then the last component is non-zero. We deduce from weak Nullstellensatz that $1 \in J$, so there exists $a_1, \dots, a_r, b \in \mathbb{C}[x_1, \dots, x_{n+1}]$ with

$$1 = \sum_i a_i(x_1, \dots, x_{n+1})f_i + b(x_1, \dots, x_{n+1})(x_{n+1}g - 1)$$

Now, set $x_{n+1} := \frac{1}{g}$. This gives

$$1 = \sum_i a_i(x_1, \dots, x_n, \frac{1}{g})f_i,$$

and multiplying by a large enough g^N to clear the denominators gives

$$g^N = \sum_i c_i(x_1, \dots, x_n)f_i, \quad c_1, \dots, c_r \in \mathbb{C}[x_1, \dots, x_n]$$

□

Corollary (Ideal-Variety Correspondence)

47.5

We'll work in $F[x_1, \dots, x_n]$, where F is any field.

1. The maps $\{\text{algebraic sets}\} \leftrightarrow \{\text{ideals}\}$ and $\{\text{ideals}\} \rightarrow \{\text{algebraic sets}\}$ are inclusion reversing. (i.e. $I_1 \subset I_2 \implies V(I_2) \subset V(I_1)$, etc). Furthermore, for any algebraic set V , $V(I(V)) = V$, so I is always injective.
2. If $F = \mathbb{C}$ (or generally F is algebraically closed), then we have inclusion reversing bijections $\{\text{algebraic sets}\} \longleftrightarrow \{\text{radical ideals}\}$, containing $\{\text{irreducible algebraic sets}\} \longleftrightarrow \{\text{prime ideals}\}$, containing $\{\text{points}\} \longleftrightarrow \{\text{maximal ideals}\}$. This is why this is called algebraic geometry, as we have a dictionary between geometric structures and algebraic structures.

Modules

48. Modules

Definition

48.1

Let A be a ring. A (left) **A -module** is a set $(M, +, \cdot)$ endowed with two operations:

$$+ : M \times M \rightarrow M \quad (x, y) \mapsto x + y$$

$$\cdot : A \times M \rightarrow M \quad (a, m) \mapsto a \cdot m$$

such that for all $a, b \in A, x, y \in M$,

(i) $(M, +)$ is an additive abelian group

(ii) a) $a(x + y) = ax + ay$, b) $(a + b)x = ax + bx$, c) $1 \cdot x = x$, d) $(ab) \cdot x = a(bx)$

Remark 48.2. Modules are to rings as vector spaces are to fields. Their significance is that modules “linearize” rings, and represent them. One can show that if A is commutative, then the category $A\text{-MOD}$ of all A modules determines A .

Morita’s Theorem

48.3

The category of A modules is equivalent to the category of $M_n(A)$ modules, for all fixed $n \geq 1$.

Example 48.4. 1. A is an A -module, in an obvious way. More generally, if $f : A \rightarrow B$ is any ring homomorphism, then B becomes an A -module with product $a \cdot b := f(a) \cdot b$ for $a \in A, b \in B$. In fact, we can replace B by any B -module N , then N becomes an A -module via the map f .

2. If $A = F$ for F a field, then an A -module is just an F -vector space.

3. If $A = \mathbb{Z}$, then a $\mathbb{Z}$ -module M is the same as an abelian group, with $n \cdot x = (1 + \cdots + 1)x = x + \cdots + x$, $n \geq 1$.

4. An example we’ll study carefully later: Let $A = F[x]$, for F a field, and V be an $F[x]$ -module. Then, V is also an F -module, so V is an F -vector space. The element x induces an F -linear map $T : V \rightarrow V$ mapping $v \mapsto x \cdot v$. Now, any power x^k acts on V by $v \mapsto T^k(v)$. So, an $F[x]$ -module is an F -vector space, together with a linear map $T : V \rightarrow V$. Conversely, given any F -vector space V , and any F -linear map $T : V \rightarrow V$, we can turn V into an $F[x]$ module by setting $f(x) \cdot v = f(T)(v)$, for any $f \in F[x]$. Classifying the $F[x]$ modules up to isomorphism leads to the canonical forms of matrices.

From here on, we assume A is commutative

Definition**48.5**

1. A subgroup $N \subset M$ is a **submodule** of M if N is an A -module with the induced operations from M .
2. A map $\varphi : M \rightarrow N$ is a **homomorphism** of A -modules, or an A -linear map, if $\varphi(x + y) = \varphi(x) + \varphi(y)$, $\varphi(ax) = a\varphi(x)$, for all $x, y \in M, a \in A$.
3. We define, for $\varphi : M \rightarrow N$ an A -linear map, $\ker \varphi$ and $\text{Img } \varphi$ as for vector spaces. The first and second isomorphism theorems hold for modules.
4. Given $N \subset M$ any submodule, we can always form the quotient module M/N with the projection map $\pi : M \rightarrow M/N$. Submodules of M/N correspond to submodules M' of M with $M' \subset N$.
5. Given any two A -modules M and N , we have an A -module $\text{Hom}_A(M, N)$ consisting of all A -linear maps $M \rightarrow N$. Taking $N = A$ defines the **dual module**.
6. We can form sums and intersections of submodules of an A -module M . If $S \subset M$ is any subset, we have the submodule $\langle S \rangle$ generated by S :

$$\langle S \rangle := \bigcap_{S \subset N \text{ submodule}} N = \{a_1 s_1 + \cdots + a_r s_r \mid a_i \in A, s_i \in S, r \geq 1\}.$$

M is **finitely generated** if there is a finite set S with $M = \langle S \rangle$.

7. We can form direct sums $\bigoplus_{i \in I} M_i$ and **direct products** $\prod_{i \in I} M_i$ of a family $\{M_i\}_{i \in I}$ of A -modules.

Example 48.6. The A -submodules of A are the left ideals in A . In examples (2) and (3) from before, we get linear subspaces and subgroups, respectively.

Exercise

let $f : A \rightarrow B$ be a ring homomorphism and N a B -module. If N is finitely generated as B -module, and B is finitely generated as an A -module, then N is finitely generated as an A module.

49. Algebras**Definition****49.1**

Let $f : A \rightarrow B$ be a ring homomorphism, and assume A, B are commutative. If $a \in A$ and $b \in B$, we define a product $a \cdot b := f(a) \cdot b$. We've seen this turns B into an A -module. But, B is also a ring, and the two structures are compatible with each other in an obvious sense. The ring B equipped with this A -module structure is said to be an A -algebra. So, an **A -algebra** is a ring B together with a ring homomorphism $f : A \rightarrow B$.

- Remark 49.2.**
1. If $A = F$ is a field and $B \neq 0$, then f is injective, so F can be identified with its image in B . So, an F -algebra, for F a field, is a ring B which contains F as a subring.
 2. Any ring A is automatically a $\mathbb{Z}$ -algebra, through the unique map $\mathbb{Z} \rightarrow A$.

50. Free Modules

Definition

50.1

Given a ring A , one can form the A -modules $A^k = A \oplus \cdots \oplus A$ or $\bigoplus_{i \in I} Ae_i$ for a family of elements $\{e_i\}_{i \in I}$. When A is a field, this exhausts the list of all A -modules up to isomorphism.

Definition

50.2

Given an A -module M , we define **linearly independent** subsets of M in the same way as for vector spaces. A set $S \subset M$ is a **basis** of M if S is linearly independent, and $M = \langle S \rangle$.

Example 50.3. The *standard basis* $e_1, \dots, e_n$ is a basis of A^n .

Definition

50.4

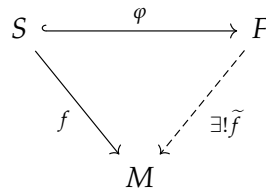
An A -module M is **free** if it has a basis S . In this case, we say M is **free on S** , and there exists an isomorphism $M \cong \bigoplus_{s \in S} As$, which is $\cong A^{|S|}$ when S is finite.

Equivalently, each element $m \in M$ has a unique expression $m = \sum a_i s_i$ as a finite sum, for $a_i \in A, s_i \in S$.

Theorem

50.5

We have a universal property of the pair (M, S) for S a basis: Given F free on S , a map $\varphi : S \rightarrow F$, there exists a unique module homomorphism $\tilde{f}$ such that $f = \tilde{f} \circ \varphi$.



Example 50.6. 1. Any vector space V over a field F is a free F -module.

2. $\mathbb{Z}^n$ is a free $\mathbb{Z}$ -module, but $\mathbb{Z}/n\mathbb{Z}$ is not.

3. There exists an example of a non-commutative ring A with $A^n \cong A^m$ as A -modules, but $n \neq m$. We'll see that this never happens when A is commutative.

4. $(\mathbb{Q}, +)$ is not a free $\mathbb{Z}$ -module. [Indeed, given $y \in \mathbb{Q}$, the equation $2x = y$ always has a solution in x . But, this property fails for any free $\mathbb{Z}$ -module $\bigoplus_{i \in I} \mathbb{Z}e_i$]

Proposition

50.7

Let R be a non-zero commutative ring. If M is a free R -module, with a basis of n elements, then any other basis of M has n elements. So, we can define $\dim_R(M) := n$.

Proof. If I is an ideal of R , we get a submodule IM of M , generated by all products am , $a \in I, m \in M$. If $e_1, \dots, e_n$ is a basis of M , then $IM \equiv \{(a_1 e_1, \dots, a_n e_n) \mid a_i \in I\}$. Also, M/IM is an R/I -module via the product $(r + I)(m + IM) := rm + IM$. Now, let $\mathfrak{m}$ be any maximal ideal of

R . Then, M/mM is a k -vector space, where $k := R/m$. Moreover, if $\bar{e}_i = e_i + mM, 1 \leq i \leq n$, then $\bar{e}_1, \dots, \bar{e}_n$ is a basis of M/mM over k (for linear independence, note that if $\sum r_i \bar{e}_i \in mM$, then $r_i \in m \forall i$). The result then follows from the vector space case. $\square$

51. Exact Sequences

Definition

51.1

Suppose M is a module, $N \subset M$ a submodule. We then have a sequence $N \xhookrightarrow{i} M \xrightarrow{\pi} M/N$ such that $\ker \pi = \text{Im } i \equiv N$. More generally, a sequence of A -modules $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ and homomorphisms is **exact at** M if $\text{Im } \alpha = \ker \beta$. Note that $0 \rightarrow M' \xrightarrow{\alpha} M$ is exact $\iff \alpha$ is injective, and $M \xrightarrow{\beta} M'' \rightarrow 0$ is exact $\iff \beta$ is surjective. A diagram

$$M_1 \xrightarrow{a_1} M_2 \xrightarrow{a_2} M_3 \rightarrow \dots \rightarrow \xrightarrow{a_{n-1}} M_n$$

is **exact** if each consecutive triplet is exact. A **short exact sequence** is an exact sequence of the form

$$0 \rightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \rightarrow 0,$$

in which case α is injective, β is surjective, and $M'' \cong M/M'$.

Example 51.2. Given a finitely generated A -module M , with generators $s_1, \dots, s_r$, we have a morphism $F := A^r = \bigoplus_{i=1}^r A s_i \xrightarrow{\varphi} M \rightarrow 0$. If $K = \ker \varphi$, we get the short exact sequence $0 \rightarrow K \rightarrow F \rightarrow M \rightarrow 0$. $K \subset F$ is the submodule of **relations** among the generators s_i . The short exact sequence gives a **presentation** of M

52. Tensor Products of Modules

Let A be a commutative ring, and M, N be A -modules. We want to study **bilinear** maps $\varphi : M \times N \rightarrow G$, where G is another A -module, i.e. maps φ which are linear in each variable, when the other is fixed. The idea is to form a new module $M \otimes N$ such that the A -linear maps $M \otimes N \rightarrow G$ correspond to the bilinear maps φ .

Example 52.1 (First Motivation for Tensor Products). Suppose V and W are finite dimensional F -vector spaces. We want to study the vector space $M = \text{Bil}(V \times W, F)$ of all bilinear maps $V \times W \rightarrow F$. Given $f \in V^*, g \in W^*$, we can form $f \otimes g \in M$ by $(f \otimes g)(x, y) := f(x)g(y)$. Note that $f \otimes g + f' \otimes g' \neq f'' \otimes g''$ in general. So the set of all maps $f \otimes g$ does not exhaust M . However, we'll show

$$M = \left\{ \sum_{i=1}^n f_i \otimes g_i \mid f_i \in V^*, g_i \in W^* \right\} =: V^* \otimes W^*$$

Example 52.2 (Second Motivation for Tensor Products). Suppose V is a finite dimensional real vector space, and $T : V \rightarrow V$ a linear operator such that $T^2 + I = 0$. Then, T has no real eigenvalues. We may want to enlarge V to get a vector space $V_{\mathbb{C}}$ over $\mathbb{C}$, with an extended map $T_{\mathbb{C}} : V_{\mathbb{C}} \rightarrow V_{\mathbb{C}}$ to rectify this. We do this by extension of scalars, via the inclusion $\mathbb{R} \hookrightarrow \mathbb{C}$. V and $\mathbb{C}$ are both $\mathbb{R}$ -modules, so

we can form $V_{\mathbb{C}} := \mathbb{C} \otimes_{\mathbb{R}} V$, and R -module. But, $V_{\mathbb{C}}$ is also naturally a $\mathbb{C}$ module, via the operation $\lambda(z \otimes v) = (\lambda z) \otimes v$, for $\lambda, z \in \mathbb{C}, v \in V$. Moreover, T extends to $T_{\mathbb{C}} := 1 \otimes T : V_{\mathbb{C}} \rightarrow V_{\mathbb{C}}$, which is $\mathbb{C}$ -linear.

Let R be a commutative ring, $R \neq 0$. Given M, N two R -modules, the **tensor product** $M \otimes_R N$ is an R -module, together with a bilinear map $\varphi : M \times N \rightarrow M \otimes_R N$. That is,

$$\varphi(\lambda m + m', n) = \lambda \varphi(m, n) + \varphi(m', n) \quad \varphi(m, \lambda n + n') = \lambda \varphi(m, n) + \varphi(m, n').$$

We want φ to be universal in the following sense: for any **bilinear map** $f : M \times N \rightarrow G$ of R -modules, there is a unique R -linear map $\tilde{f} : M \otimes_R N \rightarrow G$ such that $\tilde{f} \circ \varphi = f$. That is, the below diagram commutes.

$$\begin{array}{ccc} & & M \otimes_R N \\ & \nearrow \varphi & \downarrow \exists! \tilde{f} \\ M \times N & & G \\ & \searrow f & \end{array}$$

The definition extends to **multilinear maps** to obtain any finite tensor product $E_1 \otimes E_2 \otimes \cdots \otimes E_n$ of R -modules. We construct the tensor product below.

In the following construction, we will work with 2 R -modules E and F , and construct $E \otimes_R F$. A similar idea is used to construct any finite tensor product.

Definition

52.3

Let E, F be two R -modules. Let M be the free R -module generated by the set $E \times F$. That is,

$$M := \bigoplus_{e \in E, f \in F} R \cdot (e, f)$$

Let $N \subset M$ be the submodule generated by all elements of the form

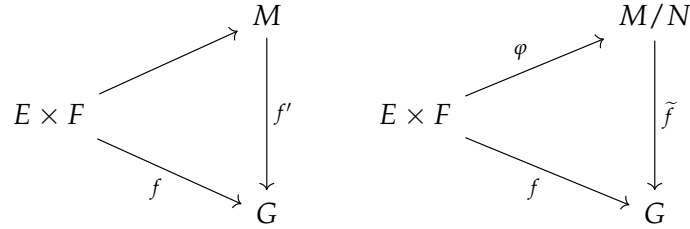
$$(\lambda e + e', f) - \lambda(e, f) - (e', f), \text{ and}$$

$$(e, \lambda f + f') - \lambda(e, f) - (e, f')$$

where $\lambda \in R, e, e' \in E, f, f' \in F$. We have an injection $E \times F \hookrightarrow M$ of sets. Compose this with the canonical map $M \rightarrow M/N$ to get a map $\varphi : E \times F \rightarrow M/N$. That is, $(e, f) \mapsto (e, f) + N$. We claim φ is bilinear and a **tensor product** in the sense we want. So, we can define $E \otimes_R F$ to be M/N .

Proof. Bilinearity of φ is obvious, using the relations in N . Now, let $f : E \times F \rightarrow G$ be any bilinear map. By the universal property of the free module generated by $E \times F$, we have an induced map $f' : M \rightarrow G$ which makes the first diagram below commute. Since f is bilinear, f' is zero on N . Hence, by the universal property of quotient modules, f' can be factored through M/N . This gives a map $\tilde{f} : M/N \rightarrow G$ which makes the second diagram commute. Since M/N is

generated by the image $\text{Img } \varphi$ of φ , it follows that $\tilde{f}$ is uniquely determined. This completes the construction, and we denote M/N by $E \otimes_R F$, or $E \otimes F$. $\square$



Remark 52.4. 1. If $x_i \in E_i$ for $1 \leq i \leq n$, write $x_1 \otimes \cdots \otimes x_n$ for the element $\varphi(x_1, \dots, x_n)$. This is called a **tensor**. We have

$$x_1 \otimes \cdots \otimes (\lambda x_i + x'_i) \otimes \cdots \otimes x_n = \lambda \cdot x_1 \otimes \cdots \otimes x_n + x_1 \otimes \cdots \otimes x'_i \otimes \cdots \otimes x_n$$

2. Every element of $E \otimes F$ is a sum of terms $x \otimes y$ with $x \in E, y \in F$, and $\lambda(x \otimes y) = (\lambda x) \otimes y = x \otimes (\lambda y)$, for any $\lambda \in R$.

Example 52.5. The tensor product of modules can involve a great deal of collapsing. For example, if $m, n \in \mathbb{Z}_{>0}$ with $(m, n) = 1$, then $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} = 0$: If $x \otimes y \in \mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z}$, then $n(x \otimes y) = x \otimes (ny) = x \otimes 0 = 0$, and the same for m . We deduce that $x \otimes y = 0$.

Exercise

Show more generally that

$$\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/(m, n)\mathbb{Z}$$

Theorem

52.6

Let E, F, G be three R -modules. We have canonical isomorphisms

$$\text{Hom}(E \otimes F, G) \cong \text{Bil}(E \times F, G) \cong \text{Hom}(E, \text{Hom}(F, G))$$

Proof. All the isomorphisms involved are very natural. The isomorphism $\text{Bil}(E \times F, G) \xrightarrow{\sim} \text{Hom}(E \otimes F, G)$ which maps $f \mapsto \tilde{f}$ is defined by the universal property of $E \otimes F$. It is injective by uniqueness of $\tilde{f}$, and surjective because composing any linear map $g : E \otimes F \rightarrow G$ with the canonical bilinear map $\varphi : E \times F \rightarrow E \otimes F$ gives a bilinear map $E \times F \rightarrow G$.

For the second isomorphism, construct i and j as follows:

$$i : \text{Bil}(E \times F, G) \rightarrow \text{Hom}(E, \text{Hom}(F, G))$$

Given $f : E \times F \rightarrow G$ and $x \in E$, we obtain a linear map $f_x : F \rightarrow G$ by $f_x(y) := f(x, y)$. Moreover, the map $x \mapsto f_x$ is linear in x , as desired. That is, i maps $f \mapsto (x \mapsto f_x)$.

$$j : \text{Hom}(E, \text{Hom}(F, G)) \rightarrow \text{Bil}(E \times F, G)$$

Let $\alpha : E \rightarrow \text{Hom}(F, G)$ be R -linear. Define a bilinear map $f_\alpha : E \times F \rightarrow G$ by $f_\alpha(x, y) := \alpha(x)(y)$. Then, j is the mapping $\alpha \mapsto f_\alpha$.

One can check that j is the inverse map to i . $\square$

Example 52.7. Let E and F be vector spaces over the field k ($\equiv R$) and set $G := k$. Then, we have isomorphisms

$$(E \otimes F)^* \cong \text{Bil}(E \times F, k) \cong \text{Hom}(E, F^*)$$

Corollary**52.8**

Let E and F be finite dimensional vector spaces over a field k . Then, $E \otimes F$ is finite dimensional, and $\dim_k(E \otimes F) = \dim E \cdot \dim F$. Moreover, if $e_1, \dots, e_m$ is a basis of E , and $f_1, \dots, f_n$ is a basis of F , then $\{e_i \otimes f_j\}_{1 \leq i \leq m, 1 \leq j \leq n}$ is a basis of $E \otimes F$.

Proof. For the last assertion, we claim that $e_i \otimes f_j$ for $1 \leq i \leq m$ and $1 \leq j \leq n$ span $E \otimes F$. Indeed, clearly $\text{Img } \varphi = \{v \otimes w \mid v \in V, w \in W\}$ lies in $\text{Span} \langle e_i \otimes f_j \rangle$, and we know $\text{Img } \varphi$ generated $E \otimes_k F$ $\square$

Exercise

With E and F as in the corollary, we have

$$(E \times F)^* \cong E^* \otimes F^*$$

Hence

$$E \otimes F \cong \text{Hom}(E^*, F).$$

Under the latter isomorphism, the tensor $e \otimes f$ maps to the homomorphism $g \mapsto g(e) \cdot f$, for $g \in E^*$.

Example 52.9. 1. (*Tensor Product of 2 Homomorphisms*) Let $f : M \rightarrow M'$ and $g : N \rightarrow N'$ be R -module homomorphisms. Then, there exists a unique R -linear map $f \otimes g : M \otimes N \rightarrow M' \otimes N'$ such that $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$ for all $x \in M, y \in N$. (First, define the bilinear map $M \times N \rightarrow M' \otimes N'$ sending $(x, y) \mapsto f(x) \otimes g(y)$, and then use the universal property of $M \otimes N$)

2. (*Change of Base*) Let $f : R \rightarrow S$ be any ring homomorphism, with R and S commutative. Recall that S becomes an R -module by setting $r \cdot s := f(r)s$, $r \in R, s \in S$. If M is any R -module, then $S \otimes_R M$ is an S -module via $s \cdot (s' \otimes m) := (ss') \otimes m$. We say that $S \otimes_R M$ is obtained from M by **changing the base** from R to S . A typical case of this is when R is a subring of S , in which case $S \otimes_R M$ is an **extension of scalars** from R to S . For example, if $R \subset S$ is a subring, then $S \otimes_R R[x_1, \dots, x_n] \cong S[x_1, \dots, x_n]$.

Proposition**52.10**

$$E \otimes_R F \cong F \otimes_R E$$

as modules.

Proof. The map $E \times F \rightarrow F \otimes_R E$ which maps $(x, y) \mapsto y \otimes x$ is bilinear, so by the universal property there exists an R -linear map

$$E \otimes_R F \rightarrow F \otimes_R E$$

sending $x \otimes y \mapsto y \otimes x$, which has a clear inverse by symmetry. $\square$

Proposition**52.11**

The (unique) map $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$ induces an isomorphism

$$(E \otimes F) \otimes G \cong E \otimes (F \otimes G)$$

Proof. Since the tensors $(x \otimes y) \otimes z$ generate $(E \otimes F) \otimes G$, the uniqueness is clear. To prove existence, fix a $z \in G$, then the map $\lambda_z : E \otimes F \rightarrow E \otimes (F \otimes G)$ mapping

$$\lambda_z(x, y) := x \otimes (y \otimes z)$$

is bilinear in x and y , so induces a linear map $\tilde{\lambda}_z : E \otimes F \rightarrow E \otimes (F \otimes G)$. Furthermore, consider the map $(E \otimes F) \times G \rightarrow E \otimes (F \otimes G)$ which sends $(\alpha, z) \mapsto \tilde{\lambda}_z(\alpha)$, and note that it's bilinear, hence factors through to get the desired linear isomorphism. $\square$

Example 52.12. 1. Let F be a field and V and W be F -vector spaces with $\dim_F V = n, \dim_F W = m$. Then, if $E := (e_1, \dots, e_n)$ and $E' := (e'_1, \dots, e'_m)$ are ordered bases of V, W respectively, then

$$\{e_i \otimes e'_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$$

forms a basis of $V \otimes W$. Now, suppose $S : V \rightarrow V$ and $T : W \rightarrow W$ are F -linear maps represented by the matrices $A = (S)_E, B = (T)_{E'}$ respectively. We've seen that $S \otimes T : V \otimes W \rightarrow V \otimes W$ is a linear map characterized by

$$(S \otimes T)(v \otimes w) = S(v) \otimes T(w).$$

If the basis $\{e_i \otimes e'_j\}$ is ordered as follows:

$$e_1 \otimes e'_1, \dots, e_1 \otimes e'_m, \dots, e_n \otimes e'_1, \dots, e_n \otimes e'_m,$$

then the matrix representing $S \otimes T$ is denoted by $A \otimes B$, and has the block form

$$\begin{pmatrix} a_{1,1}B & \cdots & a_{1,n}B \\ \vdots & \ddots & \vdots \\ a_{n,1}B & \cdots & a_{n,n}B \end{pmatrix} = \{a_{ij}B\}_{1 \leq i,j \leq n}.$$

This is called the **Kronecker product** or **tensor product** of the matrices A and B .

2. **Tensor product of R -algebras:** Let R be a commutative ring, and A and B be two commutative R -algebras, via the ring homomorphisms $f : R \rightarrow A, g : R \rightarrow B$. Since A and B are R -modules, we can form their tensor product $D := A \otimes_R B$, which is an R -module. We now define a product on D : Consider the map $A \times B \times A \times B \rightarrow D$ mapping $(a, b, a', b') \mapsto aa' \otimes bb'$. This is R -linear in each factor, hence determines an R -module homomorphism

$$A \otimes B \otimes A \otimes B \rightarrow D,$$

and hence an R -module homomorphism $D \otimes D \rightarrow D$. This in turn corresponds to a bilinear mapping $\mu : D \times D \rightarrow D$ such that $\mu(a \otimes b, a' \otimes b') = (aa') \otimes (bb')$. Of course, we could've written this formula directly, but this construction shows μ is well defined. We have thus defined a product on $D = A \otimes_R B$. On elements of the form $a \otimes b$, it looks like $(a \otimes b)(a' \otimes b') = (aa') \otimes (bb')$, and in general

$$\left(\sum_i a_i \otimes b_i \right) \left(\sum_j a'_j \otimes b'_j \right) = \sum_{i,j} a_i a'_j \otimes b_i b'_j.$$

This makes D into a commutative ring with identity $1 \otimes 1$. Also, D is an R -algebra via the map $r \mapsto f(r) \otimes g(r)$ (a ring homomorphism $R \rightarrow D$). These constructions also extend to the non-commutative setting.

Definition (Tensor Products as R -Algebras)
52.13

For R commutative, we say that an **R -algebra** is a (possibly noncommutative) ring A together with a ring homomorphism $f : R \rightarrow A$ such that the subring $\text{Img}(f)$ of A is contained in the center $Z(A)$ of A . Equivalently, A is a ring that is also a left R -module such that $r(ab) = (ra)b = a(rb)$ for all $r \in R, ab \in A$ (In this case, $f : R \rightarrow A$ sends r to $r \cdot 1_A$, and one can check that $f(R)$ is in the center). Now, if A and B are R -algebras, then the product $(a \otimes a')(a' \otimes b') := (aa') \otimes (bb')$ is well defined and makes $A \otimes_R B$ into an R -algebra.

Proposition
52.14

Suppose R is a commutative ring, and I, J are ideals of R . Then,

$$(R/I) \otimes_R (R/J) \cong R/(I+J)$$

as R -algebras.

Proof. Define $f : R/I \times R/J \rightarrow R/(I+J)$ by $f(x+I, y+J) := xy + I+J$. f is R -bilinear. Moreover, for any R -module G and R -bilinear $g : R/I \times R/J \rightarrow G$, define $\tilde{g} : R/(I+J) \rightarrow G$ by $\tilde{g}(x+I+J) = g(x+I, 1+J)$. Then,

1. $\tilde{g}$ is well defined: If $x+I+J = x'+I+J$, then $x' = x+a+b$ for $a \in I, b \in J$, hence $x'+I = x+b+I$, and

$$\begin{aligned} g(x'+I, 1+J) &= g(x+b+I, 1+J) = g(x+I, 1+J) + g(b+I, 1+J) \\ &= g(x+I, 1+J) + g(1+I, b+J) = g(x+I, 1+J) \end{aligned}$$

2. $\tilde{g}$ is R -linear: clear
3. $\tilde{g}$ satisfies the universal property:

$$\tilde{g} \circ f(x+I, y+J) = \tilde{g}(xy+I+J) = g(xy+I, 1+J) = g(x+I, y+J),$$

hence $\tilde{g}$ is uniquely determined, since f maps $R/I \times R/J$ onto $R/I+J$.

Therefore, $R/I+J$ and $R/I \otimes_R R/J$ are isomorphic as R -modules. Moreover, the map $x+I+J \mapsto (x+I) \otimes (1+J)$ is an explicit isomorphism between them, and is an R -algebra isomorphism. $\square$

Corollary
52.15

$$\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/(m,n)\mathbb{Z}$$

Proposition**52.16**

Let $N := \bigoplus_{i=1}^n N_i$ be a direct sum of R -modules. Then, we have an isomorphism

$$M \otimes N \cong \bigoplus_{i=1}^n (M \otimes N_i)$$

as R -modules.

Proof. Consider the map $M \times (\bigoplus_{i=1}^n N_i) \rightarrow \bigoplus_{i=1}^n (M \otimes N_i)$ mapping

$$(m, \sum n_i) \mapsto \sum m \otimes n_i.$$

It is R -bilinear, hence induces a map

$$f : M \otimes \left(\bigoplus_{i=1}^n N_i \right) \rightarrow \bigoplus_{i=1}^n (M \otimes N_i).$$

In the other direction, for each $i \in [1, n]$, we have a map $M \times N_i \rightarrow M \otimes (\bigoplus_{i=1}^n N_i)$ sending $(m, n_i) \rightarrow m \otimes n_i$. These induce maps

$$M \otimes N_i \rightarrow M \otimes \left(\bigoplus_{i=1}^n N_i \right)$$

for each i . By the universal property of the direct sum, we obtain a map

$$g : \bigoplus_{i=1}^n (M \otimes N_i) \rightarrow M \otimes \left(\bigoplus_{i=1}^n N_i \right),$$

and one can check that f and g are inverses of each other. $\square$

Exercise

Show that the previous proposition holds for arbitrary direct sums:

$$M \otimes \left(\bigoplus_{i \in I} N_i \right) \cong \bigoplus_{i \in I} (M \otimes N_i).$$

We say that $\otimes$ **commutes with direct sums**.

The next result shows that E is a free R -module, there is no collapsing in a tensor product $F \otimes_R E$.

Proposition**52.17**

Let E be free over R with basis $\{e_i\}_{i \in I}$. Then, for any R -module F , each element of $F \otimes E$ has a unique expression of the form

$$x = \sum_{i \in I} f_i \otimes e_i,$$

where only finitely many $f_i \in F$ are non-zero.

Proof. Assume first that $\dim_R E = 1$, so $E = Re$ for some $e \in E$. Since $f \otimes (\lambda e) = (\lambda f) \otimes e$, and any sum

$$\sum_{i=1}^n (f_i \otimes e) = \left(\sum_{i=1}^n f_i \right) \otimes e$$

by linearity, we deduce that any element of $F \otimes E$ may be written as $f \otimes e$ for some $f \in F$. The linear map $F \rightarrow F \otimes E$ sending $f \mapsto f \otimes e$ is an isomorphism with inverse $F \otimes E \rightarrow F$ mapping

$f \otimes (\lambda e) \rightarrow \lambda f$, for $f \in F, \lambda \in R$. Since $F \otimes E \cong F$, each element of $F \otimes E$ has a unique expression as $f \otimes e$ for some $f \in F$.

Now, in general, if E is free with basis $\{e_i\}_{i \in I}$, then we have

$$F \otimes E = F \otimes \left(\bigoplus_{i \in I} Re_i \right) = \bigoplus_{i \in I} (F \otimes Re_i),$$

and the result follows from the rank 1 case. $\square$

Corollary

52.18

Let E, F be free R -modules with bases $\{e_i\}_{i \in I}$ and $\{f_j\}_{j \in J}$ respectively. Then, $E \otimes F$ is free with basis $\{e_i \otimes f_j\}_{i \in I, j \in J}$. If E and F are both finite dimensional, then we have

$$\dim_R(E \otimes F) = \dim_R(E) \cdot \dim_R(F)$$

Remark 52.19. When E is free over R , every element of $F \otimes E$ can be viewed as a "formal" linear combination of elements in a basis $\{e_i\}$ of E , with coefficients in F . In particular

$$R \otimes E \cong E \otimes R \cong E$$

via the map $r \otimes e \mapsto re$. (Check: Is E being free here necessary?)

Example 52.20. If V is a vector space over a field F , and $K \supset F$ is a field extension, then $V_K := K \otimes_F V$ is a K -vector space. If $\dim_F(V) = n$, and $\{x_1, \dots, x_n\}$ is an F -basis of V , then observe

$$V_K = K \otimes_F V \cong K \otimes_F (F^n) \cong (K \otimes_F F)^n \cong K^n$$

and $\{1 \otimes x_1, \dots, 1 \otimes x_n\}$ is a K -basis for V_K .

Explicitly, given

$$x = \sum_{j=1}^m a_j \otimes v_j \in V_K,$$

we may write each $v_j = \sum_{i=1}^n \lambda_{i,j} x_i$ for $\lambda_{i,j} \in F$, and therefore

$$x = \sum_{j=1}^m a_j \otimes \left(\sum_{i=1}^n \lambda_{i,j} x_i \right) = \sum_{i=1}^n \left(\sum_{j=1}^m \lambda_{i,j} a_j \right) (1 \otimes x_i).$$

Exercise

Show that if $K \supset F$ is a finite extension, and $[K : F] = \dim_F K$, then

$$\dim_F V_K = [K : F] \dim_F V.$$

Corollary

52.21

Let $f : R \rightarrow S$ be a ring homomorphism. Then,

$$S \otimes_R R^n \cong S^n$$

as S -modules. This is called **extension of scalars for free modules**.

Proof. Use the isomorphism $S \otimes_R R \cong S$. $\square$

53. Graded Rings and Algebras

Definition

53.1

A ring A is **graded** if A is a direct sum

$$A = \bigoplus_{i=0}^{\infty} A_i$$

of additive subgroups A_i such that the ring multiplication maps $A_i \times A_j \hookrightarrow A_{i+j}$ for all $i, j \geq 0$. In particular, we see that A_0 is a subring of A . The elements of A_k are called the **homogeneous elements of degree k** .

A **graded ring homomorphism** $f : A \rightarrow A'$ is a homomorphism of rings that respects the grading, i.e. $f(A_k) \subset A'_k$ for all k .

The definition of **graded R -algebras** is similar - in this case each A_k is an R -submodule of A , where R is the ring. (Usually we have $R \equiv A_0$)

Example 53.2. For R a commutative ring,

$$R[x_1, \dots, x_n] = \bigoplus_{k=0}^{\infty} R[x_1, \dots, x_n]_k,$$

where $R[x_1, \dots, x_n]_k :=$ homogeneous polynomials of degree k .

54. The Tensor Algebra

Definition

54.1

Let R be a commutative ring, and M be an R -module. We then define $T^0 M := R$, $T^1 M := M$, and

$$T^k M := M \otimes_R \cdots \otimes_R M$$

The elements of $T^k M$ are called k -tensors.

Definition

54.2

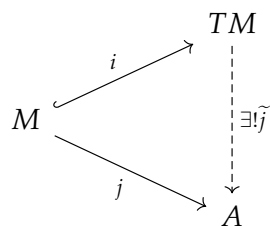
The **tensor algebra** TM is the graded R -algebra

$$TM = \bigoplus_{k=0}^{\infty} T^k M$$

as an R -module. The product in TM is induced by the maps $T^m M \otimes T^n M \rightarrow T^{m+n} M$ sending $(x_1 \otimes \cdots \otimes x_m) \otimes (y_1 \otimes \cdots \otimes y_n)$ to $x_1 \otimes \cdots \otimes x_m \otimes y_1 \otimes \cdots \otimes y_n$ for $m, n \geq 0$, which extend to a map $TM \otimes TM \rightarrow TM$ using the universal properties.

The identification of M with $T^1 M$ gives an inclusion $i : M \hookrightarrow TM$. The pair (TM, i) is characterized by the following universal property:

For any R -algebra A and R -linear map $j : M \rightarrow A$ (of R -modules), there exists a unique map $\tilde{j} : TM \rightarrow A$ of R -algebras such that $\tilde{j} \circ i = j$

**Definition**

54.3

Let P be an algebra over R . We say that P is a **non-commutative polynomial algebra** if there exist elements $x_1, \dots, x_n \in P$ such that the elements $x_I := x_{i_1} \cdots x_{i_s}$, $I = (i_1, \dots, i_s)$, $1 \leq i_k \leq n$ form a basis of P over R . We call these elements x_I **non-commutative monomials** in $x_1, \dots, x_n$. By convention, when $s = 0$, the corresponding monomial is the identity element in P .

We say that $x_1, \dots, x_n$ are independent noncommutative variables over R , and write $P \cong R \langle x_1, \dots, x_n \rangle$, the latter being the non-commutative polynomial ring in these variables.

In other words, a non-commutative polynomial algebra in $x_1, \dots, x_n$ is almost the same as $R[x_1, \dots, x_n]$, except that the variables don't commute.

Proposition

54.4

Let E be a free R -module, $\dim_R E = n$. Then, TE is isomorphic to the non-commutative polynomial algebra on n variables over R . In other words, if $e_1, \dots, e_n$ is a basis of E over R , then the elements

$$e_I := e_{i_1} \otimes \cdots \otimes e_{i_s}, I = (i_1, \dots, i_s), 1 \leq i_k \leq n$$

form a basis of $T^s E$, and each element of TE has a unique expression as a finite sum $\sum_I r_I e_I$ where $r_I \in R$, with all but finitely many r_I equal to 0.

Proof. Recall that for any R -module F , every element of $F \otimes E$ has a unique expression of the form $\sum_{i=1}^n f_i \otimes e_i$, with $f_i \in F$. The proposition follows immediately from this. $\square$

Remark 54.5. The tensor algebra construction is **functorial**, in the sense that a morphism $f : M \rightarrow N$ between R -modules induces a map $Tf : TM \rightarrow TN$ between tensor algebras.

Now, we don't really like non-commutative polynomial rings. We've shown how a free R module can be translated into a non-commutative polynomial algebra. The key problem is that $x \otimes y = y \otimes x$. Let's fix it!

55. Symmetric Powers and Symmetric Algebras

Definition

55.1

Let M be an R -module and $n \geq 0$. The **symmetric power** $S^n M \equiv \text{Sym}^n M$ is an R -module together with an R -multilinear map $\psi : M \times \cdots \times M \rightarrow S^n M$, with $\psi(x_1, \dots, x_n)$ denoted $x_1 \cdot x_2 \cdots x_n$, that is symmetric. This means that $x_{\sigma(1)} \cdots x_{\sigma(n)} = x_1 \cdots x_n$ for all $\sigma \in S_n$. The pair $(S^n M, \psi)$ satisfies the universal property:

For any R -module N , and symmetric multilinear map $f : M \times \cdots \times M \rightarrow N$, there exists a unique map $\tilde{f} : S^n M \rightarrow N$ of R -modules such that $\tilde{f} \circ \psi = f$.

$$\begin{array}{ccc}
 & & S^n M \\
 & \nearrow f & \downarrow \exists! \tilde{f} \\
 M \times \cdots \times M & & N \\
 & \searrow \psi &
 \end{array}$$

Proof. We see that $S^n M := T^n M / J$, where J is the R -submodule of $T^n M$ generated by all $x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(n)} - x_1 \otimes \cdots \otimes x_n$. (Exercise: Verify) $\square$

Convention

$$S^0 M = R, S^1 M = M.$$

We have maps $S^a M \otimes S^b M \rightarrow S^{a+b} M$, $a, b, \geq 0$ sending

$$(x_1 \cdots x_a) \otimes (y_1 \cdots y_b) \mapsto x_1 \cdots x_a y_1 \cdots y_b.$$

These make $S \cdot M = \bigoplus_{n=0}^{\infty} S^n M$ into a graded commutative R -algebra, which is universal for R -module homomorphisms from M to any commutative R -algebra A , in the same way as for the tensor algebra. In fact, one can define $S \cdot M$ as a commutative quotient of $T \cdot M$: $S \cdot M$ is $T \cdot M$ modded out by the ideal generated by all two sided ideals generated by all differences $x \otimes y - y \otimes x \in T^2 M$, for all $x, y \in M$.

Proposition

55.2

$$S^n(M \oplus N) \cong \bigoplus_{a+b=n} S^a M \otimes_R S^b N$$

Proof. There is a map $S^a M \otimes S^b N$ to $S^{a+b}(M \oplus N)$ using the inclusions $M, N \subset M \oplus N$, sending $x_1 \cdots x_a \otimes y_1 \cdots y_b$ to $x_1 \cdots x_a y_1 \cdots y_b$, as before.

In the other direction, consider the symmetric R -linear map

$$f : (M \oplus N) \times \cdots \times (M \oplus N) \rightarrow \bigoplus_{a+b=n} (S^a M \otimes_R S^b N)$$

defined by

$$f((x_1, y_1) \times \cdots \times (x_n, y_n)) := \bigoplus_{a+b=n} \left(\sum_{\{i_1, \dots, i_a\} \amalg \{j_1, \dots, j_b\} = [1, n]} x_{i_1} \cdots x_{i_a} \otimes y_{j_1} \cdots y_{j_b} \right)$$

This induces the inverse map

$$\tilde{f} : S^n(M \oplus N) \rightarrow \bigoplus_{a+b=n} (S^a M \otimes S^b N)$$

□

Example 55.3. 1. Suppose that $M = R$. Then, $S^n R = T^n R \cong R$ for all $n \geq 0$

2. (Corollary) Suppose E is free over R with basis $e_1, \dots, e_k$. Then $S^n E$ is free on $e_{i_1} \cdots e_{i_n}$ for all $1 \leq i_1 \leq \cdots \leq i_n \leq k$, or all monomials $e_1^{a_1} \cdots e_k^{a_k}$, $a_i \geq 0$, $\sum_i a_i = n$. In other words,

$$S^n M \cong R[e_1, \dots, e_k]$$

is a polynomial ring.

Exercise

Show that the isomorphism

$$S^n(M \oplus N) \cong \bigoplus_{a+b=n} S^a M \otimes_R S^b N$$

is nothing but the n -part of a graded isomorphism $S(M \oplus N) \cong S M \otimes_R S N$ of graded R -algebras.

56. Motivation for the Symmetric Algebra

Given a space $X = \mathbb{C}^n$, we have the ring $R := \mathbb{C}[x_1, \dots, x_n]$ of polynomial functions on X . We can recover X from the ring R by looking at $\text{Specm}(R) := \{\text{all maximal ideals in } R\}$, since any maximal ideal in R is of the form $m_a := (x_1 - a_1, \dots, x_n - a_n)$ for $a = (a_1, \dots, a_n) \in \mathbb{C}^n$.

Now, suppose V is a complex n -dimensional vector space. How do we define R_V , the ring of all polynomial functions on V ? One way: Choose a basis $e_1, \dots, e_n$ of V , use this to get an isomorphism $V \cong \mathbb{C}^n$ of vector spaces, and use $R = \mathbb{C}[x_1, \dots, x_n]$ to get a definition for V . This isn't as satisfying, since we had to choose a basis, i.e. it's not an intrinsic definition of R_V .

To get a basis-free definition, note that R is a graded $\mathbb{C}$ -algebra:

$$R = \mathbb{C}[x_1, \dots, x_n] = \bigoplus_{k=0}^{\infty} \mathbb{C}[x_1, \dots, x_n]_k$$

and $\mathbb{C}[x_1, \dots, x_n]_1$ is essentially the set of all linear forms $a_1 x_1 + \cdots + a_n x_n$ for $a_i \in \mathbb{C}$. Therefore, $\mathbb{C}[x_1, \dots, x_n]_1 \cong (\mathbb{C}^n)^*$. But, the latter has a basis free definition for V , namely dual space $V^* := \text{Hom}_{\mathbb{C}}(V, \mathbb{C})$.

Definition**56.1**

For an n -dimensional vector space V ,

$$R_V := \operatorname{Sym}(V^*)$$

from which V can be recovered as $V = \operatorname{Specm}(S^1 V^*)$

This construction is useful when one studies vector bundles on manifolds, (such as the tangent bundle $TX \rightarrow X$ of a manifold X where intrinsically defined objects make sense).