Notes on Fundamental Concepts in Various Branches of Mathematics

Henry Fender

Contents

1 Set Theory

1.1 Set Axioms

1.1.1 Undefined notions

Set: $A, B, C, \ldots$

1.1.2 Axioms

1. *Extension:* $\forall A \forall B[\forall C(C \in A \Leftrightarrow C \in B) \Rightarrow A = B]$
2. *Regularity:* $\forall A[\exists C(C \in A) \Rightarrow \exists B(B \in A \wedge \neg\exists D(D \in B \wedge D \in A))]$
(Every nonempty set contains a set that is disjoint from it. Also know as "Axiom of Foundation.")
3. *Schema of Specification:* $\forall B \forall X_1 \forall X_2 \ldots \forall X_n \exists A \forall C[C \in A \Leftrightarrow (C \in B \wedge \phi)]$
4. *Pairing:* $\forall X_1 \forall X_2 \exists A(X_1 \in A \wedge X_2 \in A)$
5. *Union:* $\forall \mathcal{F}_A \exists U \forall A \forall X[(X \in A \wedge A \in \mathcal{F}_A) \Rightarrow X \in U]$
6. *Schema of Replacement:* $\forall A \forall X_1 \forall X_2 \ldots \forall X_n[\forall B(B \in A \Rightarrow \exists! D\phi) \Rightarrow \exists B \forall C(C \in A \Rightarrow \exists D(D \in B \wedge \phi))]$
7. *Infinity:* $\exists \omega[\emptyset \in \omega \wedge \forall X(X \in \omega \Rightarrow X \cup X\} \in \omega)]$
8. *Power Set:* $\forall X \exists \mathcal{P}(X) \forall S[S \subseteq X \Rightarrow S \in \mathcal{P}(X)]$
9. *Empty Set:* $\exists A \forall X(X \notin A)$
10. *Choice:* $\forall X[\emptyset \notin X \Rightarrow \exists(f : X \to \bigcup X)\forall A \in X(f(A) \in A)]$

Proposition 1.1.1. *The empty set axiom is implied by the other nine axioms.*

Proof. Just choose any formula that is always false such as $\phi(X) = X \in B \wedge X \notin B$ and apply the axiom schema of specification. This will give the empty set. The axiom of extension proves uniqueness vacuously. $\square$

1.1.3 Universe

A set U is defined with the following properties...

1. $x \in u \in U \Rightarrow x \in U$
2. $u \in U \wedge v \in U \Rightarrow \{u, v\}, \langle u, v\rangle, u \times v \in U$
3. $X \in U \Rightarrow \mathcal{P}(X) \in U \wedge \bigcup X \in U$
4. $\omega \in U$ is the set of finite ordinals
5. if $f : A \to B$ is a surjective function with $A \in U \wedge B \subset U$, then $B \in U$

(See: Set Constructions.)

In category theory, *small sets* are members of U.

1.2 Set Constructions

1.2.1 Union

- $A \cup B := \{x | x \in A \vee x \in B\}$
- $\bigcup \mathcal{F} := \{x | x \in X \text{ for some } X \in \mathcal{F}\}$

Proposition 1.2.1. *For sets A, B, C, the following hold...*

- Identity: $A \cup \emptyset = A$
- Idempotence: $A \cup A = A$
- Absorption: $A \subseteq B \Leftrightarrow A \cup B = B$
- Commutative: $A \cup B = B \cup A$
- Associative: $A \cup (B \cup C) = (A \cup B) \cup C$

1.2.2 Intersection

- $A \cap B := \{x \in A | x \in B\} = \{x \in B | x \in A\}$
- $\bigcap \mathcal{F} := \{x | x \in X \text{ for all } X \in \mathcal{F}\}$

Proposition 1.2.2. *For sets A, B, C, the following hold...*

- Zero: $A \cap \emptyset = \emptyset$
- Idempotence: $A \cap A = A$
- Absorption: $A \subseteq B \Leftrightarrow A \cap B = A$
- Commutative: $A \cap B = B \cap A$
- Associative: $A \cap (B \cap C) = (A \cap B) \cap C$

1.2.3 Complement

- *Relative Complement:* $A \setminus B := \{x \in A | x \notin B\}$
- *Absolute Complement:* For some universe U and $A \subseteq U$, $A^c := U \setminus A$

Proposition 1.2.3. *For a universe U and sets $A, B \subseteq U$...*

- $(A^c)^c = A$
- $\emptyset^c = U$
- $U^c = \emptyset$
- $A \cap A^c = \emptyset$

- $A \cup A^c = U$
- $A \subseteq B \Leftrightarrow B^c \subseteq A^c$

Proposition 1.2.4 (DeMorgan's Laws)**.** *For a universe U and sets $A, B \subseteq U \ldots$*

- $(A \cup B)^c = A^c \cap B^c$
- $(A \cap B)^c = A^c \cup B^c$

Proposition 1.2.5. *For sets $A, B \ldots$*

- $A \setminus B = A \cap B^c$
- $A \subseteq B \Leftrightarrow A \setminus B = \emptyset$
- $A \setminus (A \setminus B) = A \cap B$
- $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$
- $A \cap B \subseteq (A \cap C) \cup (B \cap C^c)$
- $(A \cup C) \cap (B \cup C^c) \subseteq A \cup B$

Proposition 1.2.6. *For a family $\mathcal{F} \ldots$*

- $\forall X \in \mathcal{F}$, $\bigcup_{k \in K} X_k = \bigcup_{j \in J} (\bigcup_{i \in I_j} X_i)$
- $\forall X \in \mathcal{F}$, $\bigcap_{k \in K} X_k = \bigcap_{j \in J} (\bigcap_{i \in I_j} X_i)$
- $\forall X \in \mathcal{F}$, $\bigcup_{i \in I} X_i = \bigcup_{j \in J} X_j$
- $\forall X \in \mathcal{F}$, $\bigcap_{i \in I} X_i = \bigcap_{j \in J} X_j$
- $(\bigcup_{i \in I} A_i) \cap (\bigcup_{j \in J} B_j) = \bigcup_{i,j} (A_i \cap B_j)$
- $(\bigcap_{i \in I} A_i) \cup (\bigcap_{j \in J} B_j) = \bigcap_{i,j} (A_i \cup B_j)$

Proposition 1.2.7 (Generalized DeMorgan's Laws)**.** *For a universe U and a family $\mathcal{F} \ldots$*

- $(\bigcup_{X \in \mathcal{F}} X)^c = \bigcap_{X \in \mathcal{F}} X^c$
- $(\bigcap_{X \in \mathcal{F}} X)^c = \bigcup_{X \in \mathcal{F}} X^c$

1.2.4 Symmetric Difference

$A \triangle B := (A \setminus B) \cup (B \setminus A))$

1.2.5 Power Set

$\mathcal{P}(X) := \{S | S \subseteq X\}$

Proposition 1.2.8. *For sets A, B and a family $\mathcal{F}$...*

- $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$
- $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$
- $\bigcap_{X \in \mathcal{F}} \mathcal{P}(X) = \mathcal{P}(\bigcap_{X \in \mathcal{F}} X)$
- $\bigcup_{X \in \mathcal{F}} \mathcal{P}(X) \subseteq \mathcal{P}(\bigcup_{X \in \mathcal{F}} X)$

1.2.5.1 Characteristic Function of a subset

For $A \subseteq X$, $\chi_A : X \to 2$ where...

$$\chi_A(x) := \begin{cases} 0 & x \in X \setminus A \\ 1 & x \in A \end{cases}$$

1.2.6 n-Tuple

- *Ordered pair:* $\langle a, b \rangle := \{\{a\}, \{a, b\}\}$
- $\langle a_1, a_2, a_3, \ldots a_n \rangle := \langle \langle \langle \langle a_1, a_2 \rangle, a_3 \rangle \ldots \rangle, a_n \rangle$

1.2.7 Cartesian Product

- $A \times B := \{\langle a, b \rangle |$ for some $a \in A$ and for some $b \in B\}$
- $\bigtimes \mathcal{F} := \{\langle a_1, a_2, \ldots a_n \rangle |$ for $a_1 \in A_1$, $a_2 \in A_2, \ldots$ $a_n \in A_n$ where $A_1, A_2, \ldots, A_n \in \mathcal{F}\}$

Proposition 1.2.9. *For sets A, B...*

- $(A \cup B) \times X = (A \times X) \cup (B \times X)$
- $(A \cap B) \times (X \cap Y) = (A \times X) \cap (B \times X)$
- $(A \setminus B) \times X = (A \times X) \setminus (B \times X)$

Proposition 1.2.10. *For families $\{A_i\}_{i \in I}, \{B_j\}_{j \in J}, \{X_i\}_{i \in I}$...*

- $(\bigcup_{i \in I} A_i) \times (\bigcup_{j \in J} B_j) = \bigcup_{i,j} (A_i \times B_j)$
- $(\bigcap_{i \in I} A_i) \times (\bigcap_{j \in J} B_j) = \bigcap_{i,j} (A_i \times B_j)$
- $\bigcap_i X_i \subseteq X_j \subseteq \bigcup_i X_i$

1.2.8 Quotient by Equivalence Relation

$X/\sim := \{[a]_\sim | a \in X\}$ (See: equivalence relations)

1.2.9 Family

Given a set X and an index set I, a family is a function $\mathcal{F} : I \to X$. A cleaner way of denoting the concept is...

$\mathcal{F}(i) := S_i,\ \{S_i\}_{i \in I}$

1.3 Relations

$\mathcal{R} :\subseteq A \times B$ for some $A \times B$

1.3.1 Equivalence Relations

Relations $\sim \subseteq A \times A$ such that $\forall a, b, c \in A$...

- *Reflexive:* $a \sim a$
- *Symmetric:* $a \sim b \Rightarrow b \sim a$
- *Transitive:* $a \sim b \wedge b \sim c \Rightarrow a \sim c$

1.3.1.1 Equivalence Class

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

1.3.1.2 Set of Equivalence Classes

$[A] = \{[a]_\sim | a \in A\}$

1.3.1.3 Set Partition

A set $P :\subseteq \mathcal{P}(X)$ such that...

- $\bigcup P = X$
- $\forall S_1, S_2 \in P(S_1 \cap S_2 \neq \emptyset \Rightarrow S_1 = S_2)$

Proposition 1.3.1. *Let A is a set and $\sim$ an equivalence relation on A. Then $[A]$ is a partition of A.*

Proposition 1.3.2. *Let A be a set and P be a partition of A. Define a relation $x \sim y$ if and only if $x, y \in C \in P$. Then $\sim$ is an equivalence relation.*

1.3.1.4 Congruence Relation

A congruence $\sim$ of a set A with a binary operation $\mu : A \times A \to A$ is an equivalence relation such that...

$$\overline{\mu}([a], [b]) = [\mu(a, b)]$$

induces a well-defined binary operation on $[A]$.

Proposition 1.3.3. *An equivalence relation $\sim$ on A with $\mu : A \times A \to A$ is a congruence relation if for any $a, a', b, b' \in A$, whenever $[a] = [a']$ and [b] = [b'], we have $[\mu(a, b)] = [\mu(a', b')]$.*

1.3.2 Functions

A relation $f : A \to B$ satisfying $\forall a \in A\ \exists! b \in B$ such that afb, denoted $f(a) = b$.

1.3.2.1 Injection

A function $f : A \hookrightarrow B$ such that $\forall\, x, y \in A$ if $x \neq y$, then $f(x) \neq f(y)$. (See: monomorphism. Injections have right inverses.)

1.3.2.2 Surjection

A function $f : A \twoheadrightarrow B$ such that $\forall\, b \in B\ \exists\, a \in A$ such that $f(a) = b$. (See: epimorphism, Stirling numbers of the second kind. Surjections have left inverses, called *sections*.)

1.3.2.3 Bijection

A function $f : A \xrightarrow{\sim} B$ which is an injection and a surjection. (See: isomorphism)

1.3.2.4 Restriction

For $C \subseteq A$ and $f : A \to B$, $f\restriction_C : C \to B$ where $\forall c \in C\ f\restriction_C(c) := f(c)$

1.3.2.5 Image

$f(A) := \{f(a) | a \in A\}$

Proposition 1.3.4. *For a function $f : A \to B$ and a family $\{X_i\}_{i \in I}$ where $\forall i \in I\ X_i \subseteq A\ldots$*

- $f(\bigcup_i X_i) = \bigcup_i f(X_i)$
- *In general,* $f(\bigcap_i X_i) \neq \bigcap_i f(X_i)$
- *In general,* $f(X)^c \neq f(X^c)$

1.3.2.6 Preimage

$f^{-1}(A) := \{a \in A | f(a) \in B\}$

Proposition 1.3.5. *Given a function $f : X \to Y$, f is surjective if and only if $\forall A \subseteq Y$, where $A \neq \emptyset$, $f^{-1}(A) \neq \emptyset$.*

Proposition 1.3.6. *Given a function $f : X \to Y$, f is injective if and only if $\forall A \subseteq$ ran f, where A is a singleton, $f^{-1}(A)$ is a singleton.*

Proposition 1.3.7. *Given a function $f : X \to Y \dots$*

- *If $B \subseteq Y$, then $f(f^{-1}(B)) \subseteq B$.*
- *If f is surjective, then $f(f^{-1}(B)) = B$.*
- *If $A \subseteq X$, then $A \subseteq f^{-1}(f(A))$.*
- *If f is injective, then $A = f(f^{-1}(A))$.*
- *If $\{B_i\}$ is a family of subset of Y, then $f^{-1}(\bigcup_i B_i) = \bigcup_i f^{-1}(B_i)$ and $f^{-1}(\bigcap_i B_i) = \bigcap_i f^{-1}(B_i)$.*

1.3.2.7 Function Composition

$f : X \to Y$ and $g : Y \to Z \Rightarrow g \circ f : X \to Z$ where $\forall\, x \in X$, $g \circ f(x) := g(f(x))$

1.4 Natural Numbers

1.4.1 Successor

For a set n, its *successor* n^+ is defined by...

$$n^+ = n \cup \{n\}$$

1.4.2 Inductive

A set N is *inductive* if and only if $\emptyset \in N$ and $(\forall n \in N)\, n^+ \in N$.

The Axiom of Infinity may be restated in terms of "inductiveness," i.e....

There exists an inductive set ω.

1.4.3 Natural Number

A *natural number* is a set that belongs to every inductive set, i.e. the intersection of them all.

The following theorem is a consequence of the definition...

Theorem 1.4.1 (Induction on ω)**.** *Any inductive subset of ω coincides with ω.*

Proposition 1.4.1. *Every natural number except* 0 *is the successor of some natural number.*

Proof. Let $T = \{n \in \omega | n = 0 \vee (\exists p \in \omega) n = p^+\}$ and use induction. $\square$

1.4.4 Peano's Postulates

1.4.4.1 Peano System

An ordered triple $\langle N, S, e\rangle$ consiting of a set N, a function $S : N \to N$, and a member $e \in N$ such that the following three conditions are met:

1. $e \notin \text{ran}S$.
2. S is injective.
3. Any subset $A \subseteq N$ that contains e and is closed under S equals N itself.

Proposition 1.4.2. *Let $\sigma = \{\langle n, n^+\rangle | n \in \omega\}$. Then $\langle \omega, \sigma, 0\rangle$ is a Peano system.*

1.4.4.2 Transitive Set

A set A is said to be a *transitive set* if and only if $x \in a \in A \Rightarrow x \in A$.

Proposition 1.4.3. *For a transitive set a,*

$$\bigcup(a^+) = a.$$

Proposition 1.4.4. *Every natural number is a transitive set and ω is a transitive set.*

Proof. Use induction. □

1.4.5 Recursion

Theorem 1.4.2 (Recursion Theorem on ω)**.** *Let A be a set, $a \in A$, and $F : A \to A$. Then there exists an unique function $h : \omega \to A$ such that...*

$$h(0) = a,$$

and for every $n \in \omega$,

$$h(n^+) = F(h(n)).$$

Proof. The idea is to lef h be the union of many approximating functions. For the purposes of this proof, call a function v *acceptable* if and only if dom $v \subseteq \omega$, ran $v \subseteq A$, and the following conditions hold:

1. If $0 \in$ dom v, then $v(0) = a$.
2. If $n^+ \in$ dom v (where $n \in \omega$), then also $n \in$ dom v and $v(n^+) = F(v(n))$.

Let $\mathcal{H}$ be the collection of all acceptable functions, and let $h = \bigcup \mathcal{H}$. Thus...

$$(\star) \quad \langle n, y\rangle \in h \Leftrightarrow \langle n, y\rangle \text{ is a member of some acceptable } v$$
$$\Leftrightarrow v(n) = y \text{ for some acceptabe } v.$$

We claim that this h meets the demands of the theorem. This claim can be broken down into four parts. The four parts involve showing that (I) h is a function, (II) h is acceptable, (III) dom h is all of ω, and (IV) h is unique.

I. We first claim that h is a function. Let...

$$S = \{n \in \omega | \text{ for at most one } y, \langle n, y\rangle \in h\}.$$

We must check that S is inductive. If $\langle 0, y_1\rangle \in h$ and $\langle 0, y_2\rangle \in h$, then by $(\star)$ there exist acceptable v_1 and v_2 such that $v_1(0) = y_1$ and $v_2(0) = y_2$. But by (1) it follows that $y_1 = a = y_2$. Thus $0 \in S$.

Next suppose that $k \in S$. Consider $\langle k^+, y_1\rangle \in h$ and $\langle k^+, y_2\rangle \in h$. As before there must exist acceptabel v_1 and v_2 such that $v_1(k^+) = y_1$ and $v_2(k+) = y_2$. By condition (2) it follows that...

$$y_1 = v_1(k^+) = F(v_1(k)) \quad \text{and} \quad y_2 = v_2(k^+) = F(v_2(k)).$$

But since $k \in S$, we have $v_1(k) = v_2(k)$. Therefore...

$$y_1 = F(v_1(k)) = F(v_2(k)) = y_2.$$

So $k^+ \in S$, proving S is inductive and conincides with ω. Consequently h is a function.

II. Next we claime that h itself is acceptable. We have just seen that h is a function, and it is clear from $(\star)$ that dom $h \subseteq \omega$ and ran $h \subseteq A$.

First examine (1). If $0 \in$ dom h, then there must be some acceptable v with $v(0) = h(0)$. Since $v(0) = a$, we have $h(0) = a$.

Next examine (2). Assume $n^+ \in$ dom h. Again there must be some acceptable v with $v(n^+) = h(n^+)$. Since v is acceptable we have $n \in$ dom v (and $v(n) = h(n)$) and

$$h(n^+) = v(n^+) = F(v(n)) = F(h(n)).$$

Thus h satisfies (2) and so is acceptable.

III. We now claim that dom $h = \omega$ (the function is nonempty). It suffices to show that dom h is inductive. The function $\{\langle 0, a\rangle\}$ is acceptable and hence $0 \in$ dom h. Suppose the $k \in$ dome h. If $k^+ \notin$ dom h, then let...

$$v = h \cup \{\langle k^+, F(h(k))\rangle\}.$$

Then v is a function, dom $v \subseteq \omega$, and ran $v \subseteq A$. We will show that v is acceptable.

Condition (1) holds since $v(0) = h(0) = a$. For condition (2) there are two cases. If $n^+ \in$ dom v where $n^+ \neq k^+$, then $n^+ \in$ dom h and $v(n^+) = h(n^+) = F(h(n)) = F(v(n))$. The other case occurs if $n^+ = k^+$. Since the successor operation is injective, $n = k$. By assumption $k \in$ dom h. Thus...

$$v(k^+) = F(h(k)) = F(v(k))$$

and (2) holds. Hence v is acceptable. But then $v \subseteq h$, so that $k^+ \in \text{dom } h$ after all. So dom h is inductive and therefore coincides with ω.

IV. Finally we claim that h is unique. For let h_1 and h_2 both satisfy the conclusion fo the theorem. Let...

$$S = \{n \in \omega | h_1(n) = h_2(n)\}.$$

S is inductive, showing $h_1 = h_2$. Thus h is unique. □

Example 1.4.2.1. *There is no function $h : \mathbb{Z} \to \mathbb{Z}$ such that for every $a \in \mathbb{Z}$,*

$$h(a+1) = h(a)^2 + 1.$$

Proof. Note $h(a) > h(a-1) > h(a-2) > \cdots > 0$. Recursion on ω reliex on there being a starting point 0. $\mathbb{Z}$ has no analogous starting point. □

Theorem 1.4.3. *Let $\langle N, S, e\rangle$ be a Peano system. Then $\langle \omega, \sigma, 0\rangle$ is isomorphic to $\langle N, S, e\rangle$, i.e. there is a funciton h mapping ω bijectively to N in a way that preserves the successor operation*

$$h(\sigma(n)) = S(h(n))$$

and the zero element

$$h(0) = e.$$

1.4.6 Arithmetic

1.4.6.1 Addition

Addition (+) is the binary operation on ω such that for any m and $n \in \omega$,

$$m + n = A_m(n),$$

where $A_m : \omega \to \omega$ is the unique function given by the recursion theorem for which...

- $A_m(0) = m$
- $A_m(n^+) = A_m(n)^+ \ \forall n \in \omega.$

Proposition 1.4.5. *For natural numbers m and n,*

- $m + 0 = m,$
- $m + n^+ = (m+n)^+$

1.4.6.2 Multiplication

Multiplication $(\cdot)$ is the binary operation on ω such that for any m and $n \in \omega$,

$$m \cdot n = M_m(n),$$

where $M_m : \omega \to \omega$ is the unique function given by the recursion theorem for which...

- $M_m(0) = 0$
- $M_m(n^+) = M_m(n) + m.$

Proposition 1.4.6. *For natural numbers m and n,*

- $m \cdot 0 = 0,$
- $m \cdot n^+ = m \cdot n + m$

1.4.6.3 Exponentiation

Exponentiation is the binary operation on ω such that for any m and $n \in \omega$,

$$m^n = E_m(n),$$

where $E_m : \omega \to \omega$ is the unique function given by the recursion theorem for which...

- $E_m(0) = 1$
- $M_m(n^+) = E_m(n) \cdot m.$

Proposition 1.4.7. *For natural numbers m and n,*

- $m^0 = 1,$
- $m^{(n^+)} = m^n \cdot m.$

1.4.7 Ordering on the natural numbers

Define $m < n$ if and only if $m \in n$.

Lemma 1.4.1. *For any natural numbers m and n...*

- $m \in n \Leftrightarrow m^+ \in n^+.$
- $n \notin n$

Theorem 1.4.4 (Trichotomy Law for ω)**.** *For any natural numbers m and n, exactly one of the three conditions...*

- $m \in n$
- $m = n$

- $n \in m$

holds.

Corollary 1.4.1. *For any natural numbers m and n,*

- $m \in n \Leftrightarrow m \subset n$
- $(m \in n) \vee (m = n) \Leftrightarrow m \subseteq n$

Proposition 1.4.8. *For any natural numbers m, n and p,...*

- $m \in n \Leftrightarrow m + p \in n + p$.
- *If, in addition, $p \neq 0$, then $m \in n \Leftrightarrow m \cdot p \in n \cdot p$.*

Corollary 1.4.2. *The following canncellation laws hold for $m, n, p \in \omega$...*

- $m + p \in n + p \Rightarrow m = n$
- *If, in addition, $p \neq 0$, then $m \cdot p \in n \cdot p \Rightarrow m = n$*

Theorem 1.4.5 (Well Ordering of ω)**.** *Let A be a nonempty set of ω. Then there is some $m \in A$ such that $(m \in n) \vee (m = n)$ for all $n \in A$.*

Proof. Assume that A is a subset of ω without a least element; we will show that $A = \emptyset$. We could attempt to do this by showing that the complement $\omega \setminus A$ is inductive. But in order to show that $k^+ \in \omega - A$, it is not enough to know merely that $k \in \omega \setminus A$, we must know that all numbers smaller than k are in $\omega \setminus A$ as well. Given this additional information, we can argue that $k^+ \in \omega \setminus A$ lest it be a least element of A.

To write down what is approximately this argument, let...

$$B = \{m \in \omega | \text{ no number less than } m \text{ belongs to } A\}.$$

We claim that B is inductive. $0 \in B$ vacuously. Suppose that $k \in B$. Then if n is less that k^+, either n is less than k (in which case $n \notin A$ since $k \in B$) or $n = k$ (in which case $n \notin A$ lest, by trichotomy, it be least in A). In either case, n is outside of A. Hence $k^+ \in B$ and B is inductive. It clearly follows that $A = \emptyset$. □

Corollary 1.4.3. *There is no function $f : \omega \to \omega$ such that $f(n^+) \in f(n)$ for every natural number n.*

Theorem 1.4.6 (Strong Induction Principle for ω)**.** *Let A be a subset of ω, and assume the for every $n \in \omega$, if every number less than n is in A, then $n \in A$. Then $A = \omega$.*

1.5 Constructing Number Systems

For the purposes of this subsection let $\mathbb{N} := \omega$.

1.5.1 The Integers

Let $\sim_{\mathbb{Z}}$ be the equivalence relation on $\mathbb{N} \times \mathbb{N}$ for which...

$$\langle m, n\rangle \Leftrightarrow m + q = p + n.$$

Then the set of *Integers*, denoted $\mathbb{Z}$, is the set $\mathbb{N} \times \mathbb{N} / \sim_{\mathbb{Z}}$.

1.5.1.1 Addition

Addition of integers $a = \langle m, n\rangle$ and $b = \langle p, q\rangle$ is defined as...

$$a +_{\mathbb{Z}} b = [\langle m + p, n + q\rangle]$$

Lemma 1.5.1. *Addition of integers ($+_{\mathbb{Z}}$) is well defined, i.e. if $\langle m, n\rangle \sim_{\mathbb{Z}} \langle m', n'\rangle$ and $\langle p, q\rangle \sim_{\mathbb{Z}} \langle p', q'\rangle$, then...*

$$\langle m + p, n + q\rangle \sim_{\mathbb{Z}} \langle m' + p', n' + q'\rangle$$

The integers under addition form an abelian group.

1.5.1.2 Multiplication

Multiplication of integers $a = \langle m, n\rangle$ and $b = \langle p, q\rangle$ is defined as...

$$a \cdot_{\mathbb{Z}} b = [\langle mp + nq, mq + np\rangle]$$

Lemma 1.5.2. *Multiplication of integers ($\cdot_{\mathbb{Z}}$) is well defined, i.e. if $\langle m, n\rangle \sim_{\mathbb{Z}} \langle m', n'\rangle$ and $\langle p, q\rangle \sim_{\mathbb{Z}} \langle p', q'\rangle$, then...*

$$\langle mp + nq, mq + np\rangle \sim_{\mathbb{Z}} \langle m'p' + n'q', m'q' + n'p'\rangle$$

The integers under multiplication form an abelian group.

1.5.1.3 Order

Order of integers $a = \langle m, n\rangle$ and $b = \langle p, q\rangle$ is defined as...

$$a <_{\mathbb{Z}} b \Leftrightarrow m + q \in p + n$$

Lemma 1.5.3. *Order of integers ($<_{\mathbb{Z}}$) is well defined, i.e. if $\langle m, n\rangle \sim_{\mathbb{Z}} \langle m', n'\rangle$ and $\langle p, q\rangle \sim_{\mathbb{Z}} \langle p', q'\rangle$, then...*

$$m + q \in p + n \Leftrightarrow m' + q' \in p' + n'$$

The order relation so defined linearly orders the integers.

1.5.2 The Rational Numbers

Let $\sim_{\mathbb{Q}}$ be the equivalence relation on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0_{\mathbb{Z}}\})$ for which...

$$\langle a, b\rangle \sim \langle c, d\rangle \Leftrightarrow a \cdot_{\mathbb{Z}} d = c \cdot_{\mathbb{Z}} b.$$

Then the set of *Rational Numbers*, denoted $\mathbb{Q}$, is the set $\mathbb{Z} \times (\mathbb{Z} \setminus \{0_{\mathbb{Z}}\} / \sim_{\mathbb{Q}}$.

1.5.2.1 Addition

Addition of rational numbers $p = \langle a, b\rangle$ and $q = \langle c, d\rangle$ is defined as...

$$p +_{\mathbb{Q}} q = [\langle ad + cb, bd\rangle]$$

Lemma 1.5.4. *Addition of rational numbers is well defined.*

The rational numbers under addition form an abelian group.

1.5.2.2 Multiplication

Multiplication of rational numbers $p = \langle a, b\rangle$ and $q = \langle c, d\rangle$ is defined as...

$$p \cdot_{\mathbb{Q}} q = [\langle ac, bd\rangle]$$

Lemma 1.5.5. *Multiplication of rational numbers is well defined.*

The rational numbers under addition and multiplication form a field.

1.5.2.3 Order

Order of rational numbers $p = \langle a, b\rangle$ and $q = \langle c, d\rangle$ is defined as...

$$p <_{\mathbb{Q}} q \Leftrightarrow ad < cb.$$

Lemma 1.5.6. *The order of rational numbers is well-defined.*

The order relation so defined linearly orders the rational numbers.

1.5.3 The Real Numbers with Cauchy Sequences

Define a *Cauchy sequence* to be a function $s : \omega \to \mathbb{Q}$ such that...

$$(\forall \varepsilon > 0)(\exists k \in \omega)(\forall m > k)(\forall n > k)|s_m - s_n| < \varepsilon.$$

Let C be the set of all Cauchy sequences. For $r, s \in C$, define $r \sim_{\mathbb{R}} s$ if and only if $|r_n - s_n|$ is arbitrarily small for large n.

With more work we can define $\mathbb{R} := C/\sim$.

1.5.4 The Real Numbers with Dedekind Cuts

A *Dedekind cut* is a subset x of $\mathbb{Q}$ such that:

1. $\emptyset \neq x \neq \mathbb{Q}$
2. x is "closed downward," i.e.,

$$q \in x \wedge r < q \Rightarrow r \in x.$$

3. x has no largest member

$\mathbb{R}$ is the set of Dedekind cuts.

1.5.4.1 Order

Define an ordering on $\mathbb{R}$ as...

$$x <_{\mathbb{R}} y \Leftrightarrow x \subset y$$

Proposition 1.5.1. *$<_{\mathbb{R}}$ is a linear ordering.*

Proof. $<_{\mathbb{R}}$ is clearly transitive; so it suffices to show that $<_{\mathbb{R}}$ satisfies trichotomy on $\mathbb{R}$. So consider $x, y \in \mathbb{R}$. Obviously *at most* one of the alternatives,

$$x \subset y, \quad x = y, \quad y \subset x,$$

can hold, but we must prove that at least one holds. Without loss of generality, suppose that the first two fail, i.e., that $x \nsubseteq y$.

Since $x \nsubseteq y$ there is some rational r in the relative complement $x \backslash y$. Consider any $q \in y$. If $r \subseteq q$, then since y is closed downward, we would have $r \in y$. But $r \notin y$, so we must have $q < r$. Since x is closed downward, it follows that $q \in x$. Since q was arbitrary (and $x \neq y$), we have $y \subset x$. □

Theorem 1.5.1 (Least Upper Bound Property)**.** *Any bounded nonempty subset of $\mathbb{R}$ has a least upper bound in $\mathbb{R}$.*

Proof. Let A be a set of real numbers. The least upper bound is just $\bigcup A$. □

1.5.4.2 Addition

Addition of real number x, y is defined as...

$$x +_{\mathbb{R}} y = q + r | q \in x \wedge r \in y$$

1.5.4.3 Multiplication

The *absolute value* of a real number x is defined as...

$$|x| = x \cup -x$$

Multiplication of real number x, y is defined as follows...

- If x and y are nonnegative real numbers, then...

$$x \cdot_{\mathbb{R}} y = 0_{\mathbb{R}} \cup \{rs | 0 \leq r \in x \wedge 0 \leq s \in y\}.$$

- It x and y are both negative real numbers, then...

$$x \cdot_{\mathbb{R}} y = |x| \cdot_{\mathbb{R}} |y|.$$

- If one of the real numbers x and y is negative and one is nonnegative, then...

$$x \cdot_{\mathbb{R}} y = -(|x| \cdot_{\mathbb{R}} |y|).$$

Real numbers under addition, multiplication, and their order relation form an ordered field.

1.6 Cardinality

1.6.1 Equinumerosity

Two sets A and B are *equinumerous*, denoted $A \approx B$, if and only if there is a bijection $f : A \to B$.

Proposition 1.6.1. *Equinumerosity is an equivalence relation. (See: isomorphism)*

Theorem 1.6.1 (Diagonalization)**.** *The set ω is not equinumerous to the set $\mathbb{R}$ of real numbers.*

Proof. Suppose for the sake of contradition that there is a bijection $f : \omega \to \mathbb{R}$. Thus we can imagine a list of successive values...

$$f(0) = 236.001\ldots$$

$$f(1) = -7.777\ldots$$

$$f(2) = 3.1415\ldots$$

$$\vdots$$

Then consider the real number $0.a_1a_2a_3\ldots$ where:

$$a_n = \begin{cases} 7 & \text{if the nth decimal of } f(n) \neq 7 \\ 6 & \text{otherwise.} \end{cases}$$

This number cannot be in the range of f, so it is not a bijection. ↯

Theorem 1.6.2 (Diagonalization)**.** *No set is equinumerous to its power set.*

Proof. Let $g : A \to \mathcal{P}(A)$. Consider...

$$B = \{x \in A | x \notin g(x)\}.$$

Then $B \subseteq A$, but for each $x \in A$,

$$x \in B \Leftrightarrow x \notin g(x).$$

Hence $B \notin \operatorname{ran} g$ and g is not a bijection. □

1.6.2 Finite/Infinite

A set is *finite* if and only if it is equinumerous to some natural number. Otherwise it is *infinite*.

Theorem 1.6.3 (Pigeonhole Principle)**.** *No natural number is equinumerous to a proper subset of itself.*

Proof. Suppose $f : N \to N$ is a bijection from a finite set to itself. We will show that ran f is all of the set n. This suffices to prove the theorem.

We use the induction on n. Define:

$$T = \{n \in \omega | \text{ every injection from } n \text{ into } n \text{ has range } n\}$$

We have that $0 \in T$; the only function from the set 0 into the set 0 is the empty function, which has range 0. Now suppose that $k \in T$ and that f is an injection from k^+ into $k+$. Note that the restriction $f\restriction_k$ maps k injectively into k^+. There are two cases...

Case I: The set k is closed under f. Then $f\restriction_k$ maps the set k into the set k. Then because $k \in T$ we may conclude that ran $(f\restriction_k) = k$. Since f is injective, the only possible value for $f(k)$ is the number k. Hence ran f is $k \cup \{k\}$, which is the set k^+.

Case II: Otherwise $f(p) = k$ for some number p less than k. In this case we interchange two values of teh functino. Define $\hat{f}$ by...

$$\hat{f}(p) = f(k),$$

$$\hat{f}(k) = f(p) = k,$$

$$\hat{f}(x) = f(x) \text{ for other } x \in k^+.$$

The $\hat{f}$ maps the set k^+ injectively into the set k^+, and the set k is closed under $\hat{f}$. So we can apply Case I.

Thus ran $f = k^+$. □

Corollary 1.6.1. *No finite set is equinumerous to a proper subset of itself.*

Corollary 1.6.2. *Any set equinumerous to a proper subset of itself is infinite.*

Corollary 1.6.3. *The set ω is infinite.*

Corollary 1.6.4. *Any finite set is equinumerous to a unique natural number.*

Lemma 1.6.1. *If C is a proper subset of a natural number n, the $C \approx m$ for some m less than n.*

Corollary 1.6.5. *Any subset of a finite set if finite.*

1.6.3 Cardinal Numbers

For any set A, the cardinal number of A, denoted card A, is a set...

1. For any sets A, B...

$$\text{card } A = \text{card } B \Leftrightarrow A \approx B.$$

2. For a finite set A, card A is the natural number n for which $A \approx n$.

(See: cardinal number definition using ordinals)

1.6.3.1 Cardinal Arithmetic

Let κ and λ be any cardinal numbers.

- $\kappa + \lambda = \text{card}(K \cup L)$, where K and L are any disjoint sets of cardinality κ and λ, respectively.
- $\kappa \cdot \lambda = \text{card}(K \times L)$, where K and L are any sets of cardinality κ and λ, respectively.
- $\kappa^\lambda = \text{card}^L K$, where K and L are any sets of cardinality κ and λ, respectively.

Proposition 1.6.2. *Assume that $K_1 \approx K_2$ and $L_1 \approx L_2$.*

1. *If $K_1 \cap L_1 = K_2 \cap L_2 = \emptyset$, then $K_1 \cup L_1 \approx K_2 \cup L_2$.*
2. *$K_1 \times L_1 \approx K_2 \times L_2$.*
3. *${}^{L_1}K_1 \approx^{L_2} K_2$.*

Proposition 1.6.3. *For any cardinal numbers κ, λ, and μ...*

- *$\kappa + \lambda = \lambda + \kappa$ and $\kappa \cdot \lambda = \lambda \cdot \kappa$.*
- *$\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$ and $\kappa \cdot (\lambda \cdot \mu) = (\kappa \cdot \lambda) \cdot \mu$.*
- *$\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$.*
- *$\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$.*
- *$(\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu$.*
- *$(\kappa^\lambda)^\mu = \kappa^{\lambda \cdot \mu}$*

Proposition 1.6.4. *Let m and n be finite cardinals. Then...*

- *$m + n = m +_\omega n$*
- *$m \cdot n = m \cdot_\omega n$*
- *$m^n = m^n$*

(See: natural number arithmetic.)

Corollary 1.6.6. *If A and B are finite, then $A \cup B$, $A \times B$, and ${}^BA$ are also finite.*

1.6.3.2 Ordering Cardinal Numbers

A set A is *dominated* by a set B (written $A \preceq B$) if and only if there is an injective function from A into B.

Theorem 1.6.4 (Schröder-Bernstein Theorem)**.** *If $A \preceq B$ and $B \preceq A$, then $A \approx B$.*

Proof. The proof is accomplished with mirrors. Given injections $f : A \to B$ and $g : B \to A$. Define C_n by recursion, using the formulas

$$C_0 = A \setminus \operatorname{ran} g \quad \text{and} \quad C_{n^+} = g[f[C_n]].$$

Thus C_0 is the troublesome part that keeps g from being a bijection. We bounce it back and forth, obtaining $C_1, C_2, \ldots$. This function showing that $A \approx B$ is the function $h : A \to B$ defined by...

$$h(x) = \begin{cases} f(x) & \text{if } x \in C_n \text{ for some } n, \\ g^{-1}(x) & \text{otherwise.} \end{cases}$$

Note that in the second case ($x \in A$ but $x \notin C_n$ for any n) it follows that $x \notin C_0$ and hence $x \in \operatorname{ran} g$. So $g^{-1}(x)$ makes sense in this case. We verify that h is indeed a bijection. Define $D_n = f[C_n]$, so that $C_{n^+} = g[D_n]$. Consider distinct $x, y \in A$. Since both f abd g^{-1} are injective, the only possible problem arises when, say, $x \in C_m$ and $y \in \bigcup_{n\in\omega} C_n$. In this case,

$$h(x) = f(x) \in D_m,$$

whereas,

$$h(y) = g^{-1}(y) \notin D_m,$$

lest $y \in C_{m^+}$. So $h(x) \neq h(x')$, showing h is injective.

Finally, we show h is surjective. Certainly each $D_n \subseteq \operatorname{ran} h$, because $D_n = h[C_n]$. Consider then a point y in $B \setminus \bigcup_{n\in\omega} D_n$. Where is $g(y)$? Certainly $g(y) \notin C_0$. Also $g(y) \notin C_{n^+}$, because $C_{n^+} = g[D_n]$, $y \notin D_n$, and g is injective. So $g(y) \notin C_n$ for any n. Therefore $h(g(y)) = g^{-1}(g(y)) = y$. This shows that $y \in \operatorname{ran} h$, thereby proving part (a). $\square$

Theorem 1.6.5 (Restated Schröder-Bernstein Theorem)**.** *For cardinal numbers κ and λ, if $\kappa \leq \lambda$ and $\lambda \leq \kappa$, then $\kappa = \lambda$.*

Proposition 1.6.5. *Let κ, λ and μ be cardinal numbers.*

- $\kappa \leq \lambda \Rightarrow \kappa + \mu \leq \lambda + \mu$
- $\kappa \leq \lambda \Rightarrow \kappa \cdot \mu \leq \lambda \cdot \mu$
- $\kappa \leq \lambda \Rightarrow \kappa^\mu \leq \lambda^\mu$
- $\kappa \leq \lambda \Rightarrow \mu^\kappa \leq \mu^\lambda$*; if not both κ and μ equal zero.*

1.6.3.3 Infinite Cardinal Arithmetic

Lemma 1.6.2. *For any infinite cardinal κ, we have $\kappa \cdot \kappa = \kappa$.*

Theorem 1.6.6 (Absorption Law of Cardinal Arithmetic)**.** *Let κ and λ be cardinal numbers, the larger of which is infinite and the smaller of which is nonzero. Then...*

$$\kappa + \lambda = \kappa \cdot \lambda = max(\kappa, \lambda).$$

1.7 Countable Sets

A set A is *countable* if and only if $A \preceq \omega$, i.e. if and only if card $A \leq \aleph_0$.

Theorem 1.7.1. *A countable union of countable sets is countable.*

Proof. We may suppose that $\notin \mathcal{A}$, for otherwise we could simply remove it without affecting $\bigcup \mathcal{A}$. We may further suppose that $\mathcal{A} \neq \emptyset$, since $\bigcup \emptyset$ is certainly countable. Thus $\mathcal{A}$ is a countable (but nonempty) function from $\omega \times \omega$ onto $\bigcup \mathcal{A}$. It is easy to find a function from ω onto $\omega \times \omega$, and the composition will map ω onto $\bigcup \mathcal{A}$, thereby showing that $\bigcup \mathcal{A}$ is countable. Since $\mathcal{A}$ is countable but nonempty, there is a function G from ω onto $\mathcal{A}$. We are given that each set $G(m)$ is countable and nonempty. Hence for each m there is a function from ω onto $G(m)$. We must then use the axiom of choice to select such a function for each m. Let $H : \omega \to^{\omega} (\bigcup \mathcal{A})$ be defined by...

$$H(m) = \{g | g \text{ is a function from } \omega \text{ onto } G(m)\}.$$

We know that $H(m)$ is nonempty for each m. Hence there is function F with domain ω such that for each m, $F(m)$ is a function from ω ontop $G(m)$. To conclude the proof we have only to let $f(m, n) = F(m)(n)$. Then f is a function from $\omega \times \omega$ onto $\bigcup \mathcal{A}$. $\square$

1.8 Axiom of Choice

(See: set axioms)

Theorem 1.8.1 (Axiom of Choice)**.** *The following statements are equivalent.*

1. *For any relation R, there is a function $F \subseteq R$ with dom F = dom R.*

2. *The Cartesian product of nonempty sets is always nonempty. That is, if H is a function with domain I and if $(\forall i \in I) H(i) \neq \emptyset$, then there is a function f with domain I such that $(\forall i \in I) f(i) \in H(i)$.*

3. *For any set A there is a function F (a "choice function" for A) such that $F(B) \in B$ for every nonempty $B \subseteq A$.*

4. *Let $\mathcal{A}$ be a set such that (a) each member of $\mathcal{A}$ is a nonempty set, and (b) any two distinct members of $\mathcal{A}$ are disjoint. Then there exists a set C containing exactly one element from each member of $\mathcal{A}$ (i.e., for each $B \in \mathcal{A}$ the set $C \cap B$ is a singleton $\{x\}$ for some x).*

There are other theorems that are equivalent to the axiom of choice.

Theorem 1.8.2 (Cardinal Comparability)**.** *For any sets C and D, either $C \preceq D$ or $D \preceq C$. For any two cardinal numbers κ and λ, either $\kappa \leq \lambda$ or $\lambda \leq \kappa$.*

Theorem 1.8.3 (Zorn's Lemma)**.** *Let $\mathcal{A}$ be a set such that for every chain $\mathcal{B} \subseteq \mathcal{A}$, we have $\bigcup \mathcal{B} \in \mathcal{A}$. ($\mathcal{B}$ is called a* chain *if and only if for any C and D in $\mathcal{B}$, either $C \subseteq D$ or $D \subseteq C$.) Then $\mathcal{A}$ contains an element M (a "maximal" element) such that M is not a subset of any other set in $\mathcal{A}$.*

1.9 Continuum Hypothesis

Proposition 1.9.1. *For any infinite set A, we have $\omega \preceq A$.*

Proposition 1.9.2. $\aleph_0 \leq \kappa$ *for any infinite cardinal* κ*.*

Corollary 1.9.1. *A set is infinite if and only if it is equinumerous to a proper subset of itself.*

The *continuum hypothesis* is:

$$\text{There is no set } \mathcal{S} \text{ such that } \aleph_0 \prec \text{card } \mathcal{S} \prec 2^{\aleph_0}.$$

1.10 Ordinal Numbers

1.10.1 Partial Orderings

A *partial ordering* is a relation R such that...

1. R is transitive
2. R is irreflexive, that is for all x we have $x \not{R} x$

Proposition 1.10.1. *Assume that $<$ is a partial ordering. Then for x, y, and z:*

1. At most *one of the alternatives,*

$$x < y, \;\; x = y, \;\; y < x,$$

can hold.

2. $x \leq y \leq x \Rightarrow x = y$.

1.10.2 Linear Orderings

A *linear ordering* is a partial ordering R that satisfies trichotomy.

1.10.3 Well Orderings

A *well ordering* is a linear ordering R on A such that every nonempty subset of A has a least element.

Theorem 1.10.1. *Let $<$ be a linear ordering on A. Then if is a well ordering if and only if there does not exist any function $f : \omega \to A$ with $f(n^+) < f(n)$ for every $n \in \omega$.*

Theorem 1.10.2 (Transifinite Induction Principle)**.** *Assume that $<$ is a well ordering on A. Assume that B is a subset of A with the special property that for every $t \in A$,*

$$\mathit{seg}\ t \subseteq B \Rightarrow t \in B.$$

Then B coincides with A.

Proof. If $B \subset A$, then $A \setminus B$ has a least element m. Bu the leastness, $y \in B$ for any $y < m$. But this is to say that seg $m \subseteq B$, so by assumption $m \in B$ after all. □

Proposition 1.10.2. *Assume that $<$ is a linear ordering on A. Further assume that the only subset of A such that $\forall\, t \in A,\ \mathit{seg}\ t \subseteq B \Rightarrow t \in B$ is A itself. Then $<$ is a well ordering on A.*

1.10.4 Transfinite Recursion

Theorem 1.10.3 (Transfinite Recursion Theorem Schema)**.** *For any formula $\gamma(x, y)$ the following is a theorem:*

Assume that $<$ is a well ordering on a set A. Assume that for any f there is a unique y such that $\gamma(f, y)$. Then there exists a unique function F with domain A such that. . .

$$\gamma(F \restriction\ \mathit{seg}\ t,\ F(t))$$

for all $t \in A$.

The following axiom is used to prove the transfinite recursion theorem schema.

For any formula $\varphi(x, y)$ not containing the letter B, the following is an axiom:

$$\begin{aligned}\forall[(\forall x \in A)\forall y_1 \forall y_2(\varphi(x, y_1) \wedge \varphi(x, y_2) \Rightarrow y_1 = y_2)\\ \Rightarrow \exists B \forall y(y \in B \Leftrightarrow (\exists x \in A)\varphi(x, y))].\end{aligned}$$

1.10.5 Epsilon Images

Let $<$ be a well ordering on A and let $\gamma(x, y)$ be the formulat $y =$ ran x. Then the transfinite recursion theorem gives an unique function E with domain A such that $\forall t \in A$:

$$\begin{aligned}E(t) &= \text{ ran } (E \restriction\ \text{seg } t)\\ &= E[\text{seg } t]\\ &= \{E(x) | x < t\}.\end{aligned}$$

The ϵ-image of $\langle A, < \rangle$ is the range of E.

Proposition 1.10.3. *Let $<$ be a well ordering on A and let E be as above and α its epsilon image.*

1. *$E(t) \notin E(t)$ for any $t \in A$.*
2. *E maps A bijectively to α.*
3. *For any s and t in A,*

$$s < t \text{ if and only if } E(s) \in E(t)$$

4. *α is a transitive set.*

1.10.6 Ordinal Numbers

Proposition 1.10.4. *Two well-ordered structures are isomorphic if and only if they have the same ϵ-image. That is, if $<_1$ and $<_2$ are well orderings on A_1 and A_2, respectively, then $\langle A_1, <_1 \rangle \cong \langle A_2, <_2 \rangle$ if and only if the ϵ-image of $\langle A_1, <_1 \rangle$ is the same as the ϵ-image of $\langle A_2, <_2 \rangle$.*

The *ordinal number* of $\langle A, < \rangle$ is its ϵ-image. An *ordinal number* is a set that is the ordinal number of some well-ordered structure.

1.10.7 Cardinal Numbers

Theorem 1.10.4 (Numeration Theorem)**.** *Any set is equinumerous to some ordinal number.*

For any set A, define the cardinal number of A (card A) to be the least ordinal equinumerous to A.

2 Combinatorics

2.1 Basic Methods

Use Cardinality to derive the most basic results.

2.1.1 Addition

Theorem 2.1.1 (Addition principle)**.** *If A and B are two disjoint finite sets, then...*

$$|A \cup B| = |A| + |B|.$$

Theorem 2.1.2 (Generalized addition principle)**.** *Let $A_1, A_2, \ldots, A_n$ be finite sets that are pairwise disjoint. Then...*

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i|$$

2.1.2 Subtraction

Theorem 2.1.3 (Subtraction principle)**.** *Let A be a finite set, and let $B \subseteq A$. Then $|A \setminus B| = |A| - |B|$.*

Proof. Observe $|A \setminus B| + |B| = |A|$ by the addition principle. □

2.1.3 Multiplication

Theorem 2.1.4 (Product principle)**.** *Let X and Y be two finite sets. Then $|X \times Y| = |X| \times |Y|$.*

Theorem 2.1.5 (Generalized product principle)**.** *Let $X_1, X_2, \ldots, X_n$ be finite sets. Then $|\bigtimes_{i \in I}^{n} X_i| = \prod_{i \in I}^{n} |X_i|$.*

2.1.4 Division

Theorem 2.1.6. *Let S and T be finite sets so that a d-to-one function $f : T \to S$ exists. Then*

$$|S| = \frac{|T|}{d}.$$

2.1.5 Binomial Coefficients

See permutations.

Theorem 2.1.7. *Let n be a positive integer, and let $k \leq n$ be a nonnegative integer. Then the number of all k-element subsets of $[n]$ is*

$$\binom{n}{k} = \frac{(n)_k}{k!} = \frac{n!}{k!(n-k)!}.$$

Note: $\binom{n}{k} = \binom{n}{n-k}$ exhibits duality.

Theorem 2.1.8 (Binomial theorem). *If n is a positive integer, then...*

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

Proof. The left-hand side of the equation contains the factor $(x+y)$ n times. To compute the product we choose an x or y term from each factor and multiply those n terms together, then do this in all 2^n possible ways, adding all the resulting products. It suffices to show that there are exactly $\binom{n}{k}$ products of the form $x^k y^{n-k}$, which is immediately obvious from the way we compute the product. □

Theorem 2.1.9. *Let n and k be nonnegative integers so that $k < n$. Then...*

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

Theorem 2.1.10. *For all positive integers n,*

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2.$$

2.1.6 Pigeonhole Principle

Theorem 2.1.11 (Pigeonhole Principle). *Let $A_1, A_2, \ldots, A_k$ be finite sets that are pairwise disjoint. Let us assume that*

$$|A_1 \cup A_2 \cup \cdots \cup A_k| > kr.$$

Then there exists at least one index i so that $|A_i| > r$. (See: Pigeonhole Priciple in Set Theory)

Example 2.1.11.1. *Consider the sequence $1, 3, 7, 15, 31, \ldots,$ in other words, the sequence whose ith element is $a_i = 2^i - 1$. Let q be any odd integer. Then our sequence contains an element that is divisible by q.*

Proof. Consider the first q elements of our sequence. If one of them is divisible by q, then we are done. If not, then consider their remainders modulo q. That is, let us write...

$$a_i = d_i q + r_i$$

where $0 < r_i < q$, and $d_i = \lfloor a_i/q \rfloor$. As the integers $r_1, r_2, \ldots, r_q$ all come from the open interval $(0, q)$, there are $q - 1$ possibilities for their values. On the other hand, their number is q, so, by the pigeonhole principle, there have to be two of them that are equal. Say these are r_n and r_m, with $n > m$. Then $a_n = d_n q + r_n$ and $a_m = d_m q + r_n$, so...

$$a_n - a_m = (d_n - d_m)q$$

or, after rearranging,

$$\begin{aligned}(d_n - d_m)q &= a_n - a_m \\ &= (2^n - 1) - (2^m - 1) \\ &= 2^m(2^{n-m} - 1) \\ &= 2^m a_{n-m}\end{aligned}$$

As the first expression of our chain of equations is divisible by q, so too must be the last expression. Note that 2^{n-m} is relatively prime to any odd number q, that is, the largest common divisor of 2^{n-m} and q is 1. Therefore, the equality $(d_n - d_m)q = 2^{n-m}a_{n-m}$ implies that a_{n-m} is divisible by q. □

2.2 Applications of Basic Methods

2.2.1 Inclusion-Exclusion

Theorem 2.2.1 (Inclusin-exclusion principle). *Let $A_1, A_2, \ldots, A_n$ be finite sets. Then...*

$$|A_1 \cup A_2 \cdots \cup A_n| = \sum_{j=1}^{n} (-1)^{j-1} \sum_{i_1, i_2, \ldots, i_j} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_j}|,$$

where $(i_1, i_2, \ldots, i_j)$ ranges all j-element subsets of $[n]$.

Proof. We prove the two follwoing claims:

1. If x is contained in the set represented on the left side of the equation, then the right side conts it exactly once.
2. If x is not contained in any A_i, then the right-hand side counts x zero times.

(1) Assume that x is contained in exactly k of the n A_i-sets, with $k > 0$. Certainly, x is not in any j-fold intersection where $j > k$. On the otherhand $j \le k$, then x is contained in exactly $\binom{k}{j}$ different j-fold intersections. If we take the signs into accoount, this means that the right side counts x exactly...

$$m = \sum_{j=1}^{k} (-1)^{j-1} \binom{k}{j}$$

times. Now we show that $m = 1$ necessarily. Observe...

$$1 - m = \sum_{j=0}^{k} (-1)^j \binom{k}{j} = (1 - 1)^k = 0,$$

since k is positive.

(2) We repeat the above argument with $k = 0$. Then the binomial theorem technique we use above gives us $(1 - 1)^0 = 1$, implying $m = 0$.

Thus the left-hand side and the right-hand side count the same objects. □

2.2.2 Multisets

Given a set A, a *multiset* is defined via a function $m : A \to \mathbb{N} \cup \{0\}$. It is a set containing $a \in A$ $m(a)$ many times.

2.2.2.1 Multinomial Coefficients

Theorem 2.2.2. *Given a multiset A of n elements over a k element sets. The number of ways to linearly order the elements of A is...*

$$\binom{n}{a_1, a_2, \ldots, a_k} = \frac{n!}{a_1!a_2!\ldots a_k!}.$$

2.2.3 Weak Compositions

Let $a_1, a_2, \ldots, a_k$ be nonnegative integers satisfying

$$\sum_{i=1}^{k} a_i = n.$$

Then the ordered k-tuple $(a_1, a_2, \ldots, a_k)$ is called a *weak composition* of n into k parts.

Theorem 2.2.3. *The number of weak compositions of n into k parts is...*

$$\binom{n+k-1}{n} = \binom{n+k-1}{k-1}.$$

Corollary 2.2.1. *The number of n-element multisets over a k-elemnt set is...*

$$\binom{n+k-1}{n} = \binom{n+k-1}{k-1}.$$

2.2.4 Compositions

Let $a_1, a_2, \ldots, a_k$ be positive integers satisfying

$$\sum_{i=1}^{k} a_i = n.$$

Then the ordered k-tuple $(a_1, a_2, \ldots, a_k)$ is called a *composition* of n into k parts.

Corollary 2.2.2. *The number of compositions of n into k parts is...*

$$\binom{n-1}{k-1}.$$

2.2.5 Stirling numbers of the second kind

Given a finite set A, $|A| = n$, the number of set partitions of A into $0 < k \leq n$ classes is denoted $S(n, k)$, the *Stirling number of the second kind.*

Theorem 2.2.4. *For all positive integers n and k satisfying $n \leq k$, the equality...*

$$S(n, k) = S(n-1, k-1) + kS(n-1, k)$$

Theorem 2.2.5. *For all positive integers n and k satisfying $n \geq k$.*

$$S(n+1, k) = \sum_{i=0}^{n} \binom{n}{i} S(n-i, k-1)$$

Theorem 2.2.6. *The number of surjections from $[n]$ to $[k]$ is equal to*

$$\sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n.$$

Corollary 2.2.3. *For all positive integers $k \leq n$,*

$$S(n, k) = \frac{1}{k!} \sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n.$$

2.2.5.1 Bell numbers

The number of all partitions of a finite set A, where $|A| = n$, is denoted $B(n)$ and is called a *Bell number.*

Theorem 2.2.7. *Set $B(0) = 1$. Then, for all positive integers n,*

$$B(n+1) = \sum_{k=0}^{n} B(k) \binom{n}{k}.$$

2.2.6 Partitions of integers

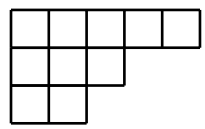
A *partition of an integer n* is a finite sequence $(a_1, a_2, \ldots, a_k)$ of positive integers satisfying $a_1 \geq a_2 \geq \cdots \geq a_k$ and $a_1 + a_2 + \cdot + a_k = n$.

Theorem 2.2.8. *As $n \to \infty$, the function $p(n)$ satisfies...*

$$p(n) \sim \frac{1}{4\sqrt{3}} \exp\left(\pi \sqrt{\frac{2n}{3}}\right)$$

2.2.7 Ferrers shapes

The *Ferrers shape* of the partition $(a_1, a_2, \ldots, a_k)$ is a row diagram of squares, with non-increasing amounts of squares in lower rows. For example the Ferrers shape fo $(5, 3, 2)$ is...



Proposition 2.2.1. *For all positive integers $k \leq n$, the number of partitions of n that have at least k parts is equal to the number of partitions of n in which the largest part is at least k.*

Proposition 2.2.2. *For every positive integer n, the number of partitions of n in which the first two parts are equal is equal to the number of partitions of n in which each part is at least 2.*

Lemma 2.2.1. *Let $m > k \geq 1$. Let S be the set of partitions of n into m parts, the smallest of which is equal to k, and let T be the set of partitions of n into $m-1$ parts, in which the kth part is larger than the $(k+1)$st part and the smallest part is at least k. Then $|S| = |T|$.*

2.2.8 Euler's totient function

For any positive integer n, let $\phi(n)$ denote the number of positive integers $k \leq n$ that are relatively prime to n.

Proposition 2.2.3. *Let $n = pq$, where p and q are distinct prinmes. Then $\phi(n) = (p-1)(q-1)$.*

Proof. Use the inclusion-exclusion principle on $[pq]$, followed by the subtraction principle. □

Proposition 2.2.4. *Let $n = p_1 p_2 \ldots p_t$, where the p_i are pairwise distinct primes. Then...*

$$\phi(n) = \prod_{i=1}^{t} (p_i - 1).$$

Lemma 2.2.2. *Let a and b be two positive integers whose greates common divisor is 1, and let $n = ab$. Then $\phi(n) = \phi(a)\phi(b)$.*

Proposition 2.2.5. *For any prime p, and any positive integer d,*

$$\phi(p^d) = (p-1)p^{d-1}.$$

Proposition 2.2.6. *Let $n = p_1^{d_1} p_2^{d_2} \ldots p_t^{d_t}$, where the p_i are distinct primes. Then...*

$$\phi(n) = \prod_{i=1}^{t} p_i^{d_i - 1}(p_i - 1)$$

2.3 Permutations

Given a set A, a *permutation* of A is a bijection $f : A \to A$.

Proposition 2.3.1. *Given a finite set A, if $n = |A|$ the number of permutations of A is $n!$.*

Intuitively permutations represent the reordering of an ordered list. Looking at the idea of "sub-orderings" of lists we come up with the following proposition...

Proposition 2.3.2 (k-lists)**.** *Let n and k be positive integers so that $n \geq k$. Then the number of injections $f : [k] \to [n]$ is...*

$$(n)_k := n(n-1)(n-2)\cdots(n-k+1).$$

2.4 Twelvefold Way

There are 12 fundamental counting problems. Sometimes they are formulated in terms of putting *balls* into *baskets*.

Let N and K be finite sets and n and k be their cardinality respectively...

2.4.1 Functions from K to N

Count with sequences of k elements in N, $|^K N|$.

2.4.2 Injections from K to N

Count with k-lists, $(n)_k$.

2.4.3 Surjections from K to N

Count with the number of surjections from $[k]$ to $[n]$, $\sum_{j=0}^{n} (-1)^j \binom{n}{j} (n-j)^k$.

2.4.4 Injections from K to N, up to a permutation of K

Count subsets, k-lists without order, $\binom{n}{k}$.

2.4.5 Functions from K to N, up to a permutation of K

Count multisets with k elements from N, $\binom{n+k-1}{k}$.

2.4.6 Surjections from K to N, up to a permutation of K

Count compositions of k into n parts, $\binom{k-1}{n-1}$.

2.4.7 Injections from K to N, up to a permutation of N

Provided $k \leq n$, there is only 1 of these.

2.4.8 Surjections from K to N, up to a permutation of N

Count partitions of K into n non-empty subsets, $S(k, n)$.

2.4.9 Functions from K to N, up to a permutation of N

Count all the partitions of K up to n classes, $\sum_{i=0}^{n} \binom{k}{i}$. If $k \leq n$, $B(k)$.

2.4.10 Functions from K to N, up to a permutation of K and N

Count partitions of k into $\leq n$ non-empty subsets, $\sum_{i=0}^{n} p_i(k)$.

2.4.11 Injections from K to N, up to a permutation of K and N

Provided $k \leq n$, there is only 1 of these.

2.4.12 Surjections from K to N, up to a permutation of K and N

Count partitions of k into n non-empty subsets, $p_n(k)$.

2.5 Graphs

A *graph* is an ordered pair $G = \langle V, E \rangle$ comprising a set V of *nodes* and E of *edges*, which are 2-element subsets of V.

Proposition 2.5.1. *Let $d_1, d_2, \ldots, d_n$ be the degrees of the vertices of a graph G on n vertices that has e edges. Then we have...*

$$d_1 + d_2 + \cdots + d_n = 2e.$$

2.5.1 Simple Graph

A *simple graph* is a graph that contains no loops and no multiple edges.

2.5.1.1 Walk

A *walk* is a series $e_1 e_2 \ldots e_k$ of edges that lead from a vertex to another one.

2.5.1.2 Cycle

A *cycle* is a walk whose starting point.

2.5.2 Graph Isomorphisms

An isomorphism f of two graphs G, H is a bijection from $V(G)$ to $V(H)$ such that if $\{a, b\} \in E(G)$, then $\{f(a), f(b)\} \in E(H)$.

2.5.2.1 Group of Automorphisms

Define the group of automorphisms of a graph G, $Aut(G)$, as normal.

Let J be a graph on n unlabeled vertices. Then define $\ell(J)$ as the number of possible ways to bijectively label J so that the resulting graphs are non-isomorphic.

Proposition 2.5.2. *For any graph H on vertex set $[n]$,*

$$|Aut(H)| \cdot \ell(H) = n!$$

2.5.3 Trees

A *tree* is a simple graph that is minimally connected.

2.5.3.1 Minimally Connected Graph

A *minimally connected* graph is contains the least number of edges in order to be connected.

Lemma 2.5.1. *Let G be a connected simple graph on n vertices. Then the following are equivalent.*

1. *The graph G is minimally connected.*
2. *There are no cycles in G.*
3. *The graph G has exactly $n-1$ edges.*

Proof. (1) $\Rightarrow$ (2) Assume there is a cycle C in G. Then G cannot be minimally connected since any one edge e of C can be omitted, and the obtained graph G' is still connected. Indeed, if a path uv used the edge e, then there would be a walk from u to v in which the edge e is replaced by the set edges of C that are different from e.

(2) $\Rightarrow$ (3) Pick any vertex $x \in G$ and start walking in some direction, never revisiting a vertex. As there is no cycle in G, eventually we will get stuck, meaning that we will hit a vertex of degree 1. This means that a connected simple graph with no cycles contains a vertex of degree 1. Removing such a vertex (and the only edge adjacent to it) from G, we get a graph $G*$ with one less vertex and one less edge, and the statement is proved by induction on n.

(3) $\Rightarrow$ (1) Suppose for the sake of contradiction that a graph on n vertices and $n-2$ edges cannot be connected. Let H be such a graph with a minimum number of vertices. Then H mus have more than 3 vertices. As H has $n-2$ edges, there has to be a vertex y of degree 1 in H, otherwise H would need to have at least n edges. Removing y from H, we get an even smaller counterexample for our statement, which is a contradiction. □

Theorem 2.5.1 (Cayley's formula)**.** *For all positive integers n, the number of all trees on vertex set $[n]$ is n^{n-2}.*

Proof. We need to prove that $T_n = n^{n-2}$, which is the number of all functions from $[n-2]$ to $[n]$. This is certainly equivalent to proving the identity...

$$n^2 T_n = n^n.$$

Here the right-hand side is the number of all functions from $[n]$ into $[n]$. The left-hand side, on the other hand, is equal to the number of all trees on $[n]$ in which we select two vertices, called Start and End (which may be identical). Let us call these trees *doubly rooted trees*.

We construct a bijection G to prove the above formula. Let $f \in End_{Set}([n])$ and draw its *short diagram*, that is, represent $x \in [n]$ as a vertex in a graph, where there is an arrow $\langle x, y \rangle$ if and only if $f(x) = y$. This creates two kinds of vertices, namely, those that are in a directed cycle and those that are not. Let C and N, respectively, denote these two subsets of $[n]$.

Now we start creating the doubly rooted tree $G(f)$. First, note that f acts as a permutation on C. If $C = \{c_1, c_2, \dots c_k\}$ so that $c_1 < c_2 < \cdots < c_k$, call $f(c_1)$ Start and $f(c_k)$ End, and create a path with vertices $f(c_1), f(c_2), \dots, f(c_k)$. Note that so far we have defined a graph with k vertices and $k-1$ edges.

If $x \in N$, then simply connect x to $f(x)$, just as in the short diagram of f. This will define $n-k$ more edges. Therefore, we now have a graph on $[n]$ that has $n-1$ edges and has two vertices (called Start and End, respectively). This is the graph that we want to call $G(f)$. In order to justify that name, we must prove that $G(f)$ is connected. This is true, however, since, in the short diagram of f, each directed path starting at any $x \in N$ must reach a vertex of C at some point (there is no other way it could end). So indeed, $G(f)$ is a doubly rooted tree for all $f \in End_{Set}([n])$.

In order to show that G is a bijection, we prove it has an inverse. Let t be a doubly rooted tree. Then there is a unique path p from Start to End in t. To find $f = G^{-1}(t)$, just put the vertices along p into C, and put all the other vertices to N. If $x \in N$, then define $f(x)$ as the unique neighbor of $x \in t$ that is closer to p than x. For the vertices $x \in C$, we define f so that the ith vertex of the Start-End path is the image of the ith smallest element of C. It is a direct consequence of the definition of G that this way we will get an $f \in End_{Set}([n])$ satisfying $G(f) = t$, and that this f is the only preimage of t under G. Therefore, G is a bijection. $\square$

3 Category Theory

3.1 Metacategories

3.1.1 Undefined notions

- *Objects:* $a, b, c \dots$
- *Arrows:* $f, g, h \dots$

3.1.2 Operations

Given $f : a \to b \dots$

- *Domain:* **dom**: arrows $\to$ objects, $f \mapsto a$
- *Codomain:* **cod**: arrows $\to$ objects, $f \mapsto b$
- *Identity:* **id**: objects $\to$ arrows, $a \mapsto \mathrm{id}_a = 1_a$
- *Composition:* **comp**: arrows $\times :$ arrows $\to$ arrows, $\langle g, f\rangle \mapsto g \circ f$, $g \circ f : \mathrm{dom} f \to \mathrm{cod} g$

$$\begin{tikzcd} & b \arrow[dr, "g"] & \\ a \arrow[ur, "f"] \arrow[rr, "g \circ f"] & & c \end{tikzcd}$$

3.1.3 Axioms

- *Associativity:* $a \xrightarrow{f} b \xrightarrow{g} c \xrightarrow{k} d$, $k \circ (g \circ f) = (k \circ g) \circ f$

$$\begin{tikzcd} a \arrow[r, "k\circ(g\circ f)=(k\circ g)\circ f"] \arrow[d, "f"] \arrow[dr, "g\circ f"] & d \\ b \arrow[ur, "k\circ g"] \arrow[r, "k\circ g"] & c \arrow[u, "k"'] \end{tikzcd}$$

- *Unit Law:* $1_a \circ f = f$ and $g \circ 1_b = g$

$$\begin{tikzcd} a \arrow[r, "f"] \arrow[dr, "f"] & b \arrow[d, "1_b"] \arrow[dr, "g"] & \\ & b \arrow[r, "g"] & c \end{tikzcd}$$

3.2 Categories

3.2.1 Directed Graph

- A - a set of arrows
- O - a set of objects
- $\mathbf{dom} : A \to O$, $\mathbf{cod} : A \to O$

3.2.1.1 Set of composable pairs of arrows

$$A \times_O A = \{\langle g, f\rangle | g, f \in A \text{ and } \mathbf{dom}(g) = \mathbf{cod}(f)\}$$

3.2.2 Categories

Add the following structure to a directed graph...

- $O \xrightarrow{id} A$, $c \mapsto id_C$
- $A \times_O A \xrightarrow{\circ} A$, $\langle g, f\rangle \mapsto g \circ f$

which satisfy $\forall a \in O$ and $\forall \langle g, f\rangle \in A \times_O A$...

- $\mathbf{dom}(\mathbf{id}(a)) = a = \mathbf{cod}(\mathbf{id}(a))$
- $\mathbf{dom}(g \circ f) = \mathbf{dom}(f)$
- $\mathbf{cod}(g \circ f) = \mathbf{cod}(g)$
- metacategorical axioms

3.2.3 Small categories

Small categories use small sets for their objects.

3.2.4 Hom Sets

$hom(b, c) = \{f | f \in C, \mathbf{dom}(f) = b, \mathbf{cod}(f) = c\}$

3.2.4.1 Alternate Definition of Categories

Small categories may be defined with hom-sets as follows...

1. A set of objects $a, b, c \ldots$
2. A function which assigns to each ordered pair $\langle a, b\rangle$ of objects a set $\hom(a, b)$
3. For each ordered triple $\langle a, b, c\rangle$ of objects a function

$$\hom(b, c) \times \hom(a, b) \to \hom(a, c)$$

called composition, and written $\langle g, f\rangle \to g \circ f$ for $g \in \hom(b, c)$, $f \in \hom(a, b)$

4. For each object b, an element $1_b \in \hom(b,b)$, called the identity of b.
5. If $\langle a,b\rangle \neq \langle a',b'\rangle$, then $\hom(a,b)\cap\hom(a',b') = \emptyset$

The above satisfy the meta-categorical axioms.

Functors in terms of hom-sets are the object function with a collection of functions
$$T_{c,c'} : \hom_C(c,c') \to \hom_B(Tc,Tc')$$
such that each $T_{c,c'}1_c = 1_{Tc}$ and every diagram...

$$\begin{tikzcd}
hom_C(c',c'') \times hom_C(c,c') \arrow[r, "\circ"] \arrow[d, "T_{c',c''}\times T_{c,c'}"] & hom_C(c,c'') \arrow[d, "T_{c',c''}"] \\
hom_B(Tc',Tc'') \times hom_B(Tc,Tc') \arrow[r, "\circ"] & hom_B(Tc,Tc'')
\end{tikzcd}$$

is commutative.

3.2.5 Groupoids

A category in which every arrow is an isomorphism.

3.3 Morphisms

Arrows in categories.

3.3.1 Isomorphisms

A morphism $f \in hom(b,c)$ that has a two-sided inverse $g \in hom(c,b)$ under composition such that
$$gf = 1_b,\ fg = 1_c.$$

Proposition 3.3.1. *The inverse of an isomorphism is unique.*

Proof. For inverses g_1, g_2 of f observe...
$$g_1 = g_1 1_c = g_1(fg_2) = (g_1 f)g_2 = 1_b g_2 = g_2$$
□

Proposition 3.3.2. *Supposing f^{-1} is the inverse of f...*

- *Each identity 1_c is an isomorphism and is its own inverse.*
- *If f is an isomorphism, then f^{-1} is an isomorphism and further $(f^{-1})^{-1} = f$.*
- *If $f \in hom(a,b)$, $g \in hom(b,c)$ are isomorphisms, then the composition gf is an isomorphism and $(gf)^{-1} = f^{-1}g^{-1}$.*

3.3.2 Automorphisms

An isomorphism of an object to itself. Denoted:

$$hom(c, c) = aut(c)$$

Observe $aut(c)$ is a group.

3.3.3 Monomorphisms

A morphism $f \in hom(b, c)$ such that $\forall z \in C$ and $\forall \alpha', \alpha'' \in hom(z, b)$:

$$f \circ \alpha' = f \circ \alpha'' \Rightarrow \alpha' = \alpha''$$

3.3.4 Epimorphisms

A morphism $f \in hom(b, c)$ such that $\forall z \in C$ and $\forall \beta', \beta'' \in hom(b, z)$:

$$\beta' \circ f = \beta'' \circ f \Rightarrow \beta' = \beta''$$

3.3.5 Split Morphism

A morphism $f : b \to b$ such that $f^2 = f$ and there exist morphisms $g : b \to c$, $h : c \to b$ satisfying...

$$f = hg \quad \wedge \quad gh = 1_c$$

3.4 Some Objects in Categories

3.4.1 Initial Objects

We say that an object i of a category C is *initial* in C if for every object a of C there exists exactly one morphism $i \to a$ in C:

$$\forall a \in Obj(C) : \quad Hom_C(i, a) \text{ is a singleton.}$$

3.4.2 Final Objects

We say that an object f of a category C is *final* in C if for every object a of C there exists exactly one morphism $a \to f$ in C:

$$\forall a \in Obj(C) : \quad Hom_C(a, f) \text{ is a singleton.}$$

Proposition 3.4.1. *Let C be a category.*

- *If i_1, i_2 are both initial objects in C, then $i_1 \cong i_2$.*
- *If f_1, f_2 are both initial objects in C, then $f_1 \cong f_2$.*

3.4.3 Null Objects

An object that is both initial and terminal.

3.4.4 Group Objects

A *group object* in C consists of an object g of C and of morphisms...

$$m : g \times g \to g,\ e : 1 \to g,\ \iota : g \to g$$

in C such that the diagrams...

$$\begin{tikzcd}
(g \times g) \times g \arrow[r, "m \times \mathrm{id}_g"] \arrow[d] & g \times g \arrow[r, "m"] & g \arrow[d, "="] \\
g \times (g \times g) \arrow[r, "\mathrm{id}_g \times m"] & g \times g \arrow[r, "m"] & g
\end{tikzcd}$$

$$\begin{tikzcd}
1 \times g \arrow[r, "e \times \mathrm{id}_g"] \arrow[dr, "\cong"'] & g \times g \arrow[d, "m"] \\
& g
\end{tikzcd}
\qquad
\begin{tikzcd}
g \times 1 \arrow[r, "\mathrm{id}_g \times e"] \arrow[dr, "\cong"'] & g \times g \arrow[d, "m"] \\
& g
\end{tikzcd}$$

$$\begin{tikzcd}
g \arrow[r, "\Delta"] \arrow[d] & g \times g \arrow[r, "\mathrm{id}_g \times \iota"] & g \times g \arrow[d, "m"] \\
1 \arrow[rr, "e"] & & g
\end{tikzcd}
\qquad
\begin{tikzcd}
g \arrow[r, "\Delta"] \arrow[d] & g \times g \arrow[r, "\iota \times \mathrm{id}_g"] & g \times g \arrow[d, "m"] \\
1 \arrow[rr, "e"] & & g
\end{tikzcd}$$

commute.

3.5 Functors

Morphisms $T : C \to B$ with domain and codomain both categories. It consists of two suitably related functions

- object function T, $c \mapsto Tc$

- arrow function T, $f : c \to c' \mapsto Tf : Tc \to Tc'$

which satisfy...

- $T(1_c) = 1_c$
- $T(g \circ f) = Tg \circ Tf$

3.5.1 Full

$\forall c, c' \in C$ and $g : Tc \to Tc' \in B, \exists f : c \to c' \in C$ s.t. $g \in Tf$

3.5.2 Faithful

$\forall c, c' \in C$ and $f_1, f_2 : c \to c', Tf_1 = Tf_2 \Rightarrow f_1 = f_2$

3.5.3 Forgetful

A functor that drops some of the structure of its input. For example, the forgetful functor $U : \mathrm{Cat} \to \mathrm{Graph}$...

- $C \mapsto UC$ where UC is comprised of the underlying objects and arrows of the category
- $F : C \to C' \mapsto UF : UC \to UC'$ where UF is a morphism between corresponding graphs

3.5.3.1 Group Action

If G is a group and a an object of a category C, then a *group action* is a functor...

$$\sigma : G \to \mathrm{Aut}_C(a)$$

3.6 Natural Transformations

Given two functors $S, T : C \to B$ a *natural transformation* $\tau : S \dot{\to} T$ is a function which assigns to each object $c \in C$ an arrow

$$\tau_c = \tau c : Sc \to Tc$$

of B in such a way that every arrow $f : c \to c'$ in C yields a diagram...

$$\begin{tikzcd} c \arrow[d, "f"] \\ c' \end{tikzcd} \qquad \begin{tikzcd} Sc \arrow[r, "\tau c"] \arrow[d, "Sf"] & Tc \arrow[d, "Tf"] \\ Sc' \arrow[r, "\tau c'"] & Tc' \end{tikzcd}$$

which is commutative.

In the following diagram $\tau a, \tau b, \tau c$ are the components of the natural transformation.

$$
\begin{tikzcd}
a \arrow[dr, "f"] \arrow[dd, "h"'] & \\
& c \\
b \arrow[ur, "g"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
Sa \arrow[rr, "\tau a"] \arrow[dr, "Sf"] \arrow[dd, "Sh"'] & & Ta \arrow[dr, "Tf"] \arrow[dd, "Th"] & \\
& Sc \arrow[rr, "\tau c"] & & Tc \\
Sb \arrow[rr, "\tau b"] \arrow[ur, "Sg"] & & Tb \arrow[ur, "Tg"] &
\end{tikzcd}
$$

3.7 Duality

Statement $\sum$	Dual Statement $\sum^*$
$f : a \to b$	$f : b \to a$
$a = \text{dom} f$	$a = \text{cod} f$
$i = 1_a$	$i = 1_a$
$h = g \circ f$	$h = f \circ g$
f is a monomorphism	f is an epimorphism
u is a right inverse of h	u is a left inverse of h
f is invertible	f is invertible
f is a terminal object	f is an initial object

3.8 Contravariance and Opposites

3.8.1 Contravariant Functor

Given a functor $S : C^{op} \to B$ the *contravariant functor* $\overline{S} : C \to B$ satisfies. . .

- $\overline{S}f = Sf^{op}$,
- $c \mapsto \overline{S}c$,
- $f : a \to b \mapsto \overline{S}f : \overline{S}b \to \overline{S}a$,
- $\overline{S}(1_c) = 1_{\overline{S}c}$,
- $\overline{S}(fg) = (\overline{S}g)(\overline{S}f)$.

3.8.1.1 Covariant Hom-Functor

A hom-functor $C(a, -) = hom(a, -) : C \to \text{Set}$ satisfying. . .

- $b \mapsto hom(a, b)$
- $k : b \to b' \mapsto hom(a, k) : hom(a, b) \to hom(a, b')$; the right side maps $f \mapsto k \circ f$ and is denoted $k*$

3.8.1.2 Contravariant Hom-Functor

A hom-functor $C(-, b) = hom(-, b) : C^{op} \to \text{Set}$ satisfying...

- $a \mapsto hom(a, b)$
- $g : a \to a' \mapsto hom(g, a) : hom(a', b) \to hom(a, b)$; the right side maps $f \mapsto f \circ g$ and is denoted $g*$

The functions g^*, k^* defined above satify the following commutative diagram.

$$\begin{tikzcd}
hom(a', b) \arrow[r, "g*"] \arrow[d, "k*"] & hom(a, b) \arrow[d, "k*"] \\
hom(a', b') \arrow[r, "g*"] & hom(a, b')
\end{tikzcd}$$

3.9 Category Constructions

3.9.1 Products

Given categories B and C we construct the product category $B \times C$...

- Objects: pairs of objects $\langle b, c \rangle$ ($b \in B$ and $c \in C$)
- Arrows: $\langle b, c \rangle \to \langle b', c' \rangle$ are a pair $\langle f, g \rangle$ of arrows ($f \in B$ and $g \in C$)
- Composition: $\langle f', g' \rangle \circ \langle f, g \rangle = \langle f' \circ f, g' \circ g \rangle$

The corresponding universal property is: for any functors R and T, there is a unique functor F making the digram commute...

$$\begin{tikzcd}
& D \arrow[dl, "R"'] \arrow[d, dotted, "F"] \arrow[dr, "T"] & \\
B & B \times C \arrow[l, "P"] \arrow[r, "Q"'] & C
\end{tikzcd}$$

Note: $P\langle f, g \rangle = f$ and $Q\langle f, g \rangle = g$ are called the *projections* of the product.

3.9.1.1 Products of Functors

Given functors U and V, the functor product $U \times V$ satisfies...

- $(U \times V)\langle b, c \rangle = \langle Ub, Uc \rangle$ for objects
- $(U \times V)\langle f, g \rangle = \langle Uf, Ug \rangle$ for arrows

$$
\begin{tikzcd}
B & B \times C \arrow[l, "P"'] \arrow[r, "Q"] \arrow[d, dotted, "U\times V"] & C \arrow[d, "V"] \\
B \arrow[from=1-1, "U"] & B \times C \arrow[l, "P'"'] \arrow[r, "Q'"] & B
\end{tikzcd}
$$

3.9.1.2 Bifunctors

A functor $S : B \times C \to D$. Intuitively, "a functor of two variables."

Determined by the functors that result when any one object of exactly one of the categories is fixed. This is recorded more explicitly in the following proposition...

Proposition 3.9.1. *Let B, C, and D be categories. For all objects $c \in C$ and $b \in B$, let*

$$L_c : B \to D,\ M_b : C \to D$$

be functors such that $M_b(c) = L_c(b)$ for all b and c. Then there exists a bifunctor $S : B \times C \to D$ with $S(-, c) = L_c$ for all c and $S(b, -) = M_b$ for all b if and only if for every pair of arrows $f : b \to b'$ and $g : c \to c'$ one has

$$M_{b'}g \circ L_c f = L_{c'} f \circ M_b g.$$

These equal arrows in D are then the value $S(f, g)$ of the arrow function of S at f and g.

Proof. Observe...

$$\langle b', g\rangle \circ \langle f, c\rangle = \langle b' f, gc\rangle = \langle f, g\rangle = \langle fb, c' g\rangle = \langle f, c'\rangle \circ \langle b, g\rangle$$

(where b, b', c, c' are identity arrows).

This implies...

$$S(b', g)S(f, c) = S(f, c')S(b, g).$$

Which further implies...

$$
\begin{tikzcd}
S(b,c) \arrow[r, "S(b,g)"] \arrow[d, "S(f,c)"] & S(b,c') \arrow[d, "S(f,c')"] \\
S(b',c) \arrow[r, "S(b',g)"] & S(b',c')
\end{tikzcd}
$$

□

3.9.1.3 Natural transformations between bifunctors

Given $S, S' : B \times C \to D$. Consider $\alpha(b,c) : S(b,c) \to S'(b,c)$. We say α is *natural in* b if $\forall c \in C$ the components $\alpha(b,c)$ for all b define $\alpha(-,c) : S(-,c) \dot{\to} S'(-,c)$, a natural transformation of functors $B \to D$.

Proposition 3.9.2. *For bifunctors S, S', the function α displayed above is a natural transformation $\alpha : S \dot{\to} S'$ (i.e., of bifunctors) if and only if $\alpha(b,c)$ is natural in b for each $c \in C$ and natural in c for each $b \in B$.*

$$\begin{tikzcd}
S(b,c) \arrow[r, "\alpha(f,g)"] \arrow[d, "S(f,g)"] & S(b,c) \arrow[d, "S'(b,c)"] \\
S(b',c') \arrow[r, "\alpha(b',c')"] & S(b',c')
\end{tikzcd}$$

3.9.1.4 The Universal Natural Transformation

Given any natural transformation $\tau : S \dot{\to} T$ between $S, T : C \to B$ there is a unique functor $F : C \times 2 \to B$ with $F\mu c = \tau c$ for any object c.

- $F\langle f, 0\rangle = Sf$
- $F\langle f, 1\rangle = Tf$
- $F\langle f, \downarrow\rangle = Tf \circ \tau c = \tau c' \circ Sf$ (where $\downarrow : 0 \to 1$)

Observe $C \times 2$ below...

$$\begin{tikzcd}
c \arrow[rr, "\mu c"] \arrow[dd, "C\times 0 \text{ layer}"] \arrow[dr] & & c \arrow[dd] \arrow[dr, "C\times 1 \text{ layer}"] & \\
& c'' \arrow[rr, "\mu c''"] & & c'' \\
c' \arrow[rr, "\mu c'"] \arrow[ur] & & c' \arrow[ur] &
\end{tikzcd}$$

where $\mu c = \langle c, \downarrow\rangle$

3.9.2 Coproducts

Given categories B and C the dual of the product category is coproduct category $B \coprod C$.

The corresponding universal property is: for any functors R and T, there is a unique functor F making the digram commute...

$$\begin{tikzcd} B \arrow[r, "I"] & B\coprod C & C \arrow[l, "J"'] \\ & D \arrow[ul, "R"] \arrow[u, dotted, "F"] \arrow[ur, "T"'] & \end{tikzcd}$$

3.9.3 Quotients

The *quotient category* is specified in the following proposition.

Proposition 3.9.3. *For a given category C, let R be a function which assigns to each pair of objects a, b of C a binary relation $R_{a,b}$ on the hom-set $C(a,b)$. Then there exist a category C/R and a functor $Q = Q_R : C \to C/R$ such that...*

1. *If $fR_{a,b}f'$ in C, then $Qf = Qf'$.*
2. *If $H : C \to D$ is any functor from C for which $fR_{a,b}f'$ implies $Hf = Hf'$ for all f and f', then there is a unique functor $H' : C/R \to D$ with $H' \circ Q_R = H$.*

Moreover, the functor Q_R is a bijection on objects.

The corresponding universal property is represented in the following diagram...

$$\begin{tikzcd} C \arrow[r, "Q_R"] \arrow[dr, "H"'] & C/R \arrow[d, dotted, "H'"] \\ & D \end{tikzcd}$$

3.9.3.1 Congruence

A *congruence* is a relation R on a category C such that...

- $\forall a, b \in \mathrm{Obj}(C)$, $R_{a,b}$ is an equivalence relation
- if $f, f' : a \to b$ have $fR_{a,b}f'$, then for all $g : a' \to a$ and all $h : b \to b'$ one has $(hfg)R_{a',b'}(hf'g)$.

3.9.4 Free Categories

3.9.4.1 O-graph

The *O-graph* is a directed graph on a fixed set O of objects (not a simple graph).

We define the *product over O* as a set of composable pairs of arrows...

$$A \times_O B = \{\langle g, f\rangle | \delta_0 g = \delta_1 f, g \in A, f \in B\}$$

where δ_0, δ_1, resp., are functions representing the **dom**, **cod**, resp., operations.

A category with objects O is an O-graph equipped with two morphisms $c : A \times_O A \to A$ and $i : O \to A$ of O-graphs making the following diagrams commutative.

$$\begin{tikzcd}
(A \times_O A) \times_O A \arrow[r, "\cong"] \arrow[d, "c\times 1"] & A \times_O (A \times_O A) \arrow[r, "1\times c"] & A \times_O A \arrow[d, "c"] \\
A \times_O A \arrow[rr, "c"] & & A
\end{tikzcd}
\qquad
\begin{tikzcd}
O \times_O A \arrow[r, "i\times 1"] \arrow[d, "\cong"] & A \times_O A \arrow[d, "c"] & A \times_O O \arrow[l, "1\times i"'] \arrow[d, "\cong"] \\
A \arrow[r, "="] & A & A \arrow[l, "="]
\end{tikzcd}$$

3.9.4.2 Free Category

Let $C(G)$ be the *free category* generated by graph G, specified in the subsequent theorem. . .

Theorem 3.9.1. *Let $G = \{A \rightrightarrows O\}$ be a small graph. There is a small category $C(G)$ with O as its set of objects and a morphism $P : G \to UC$ of graphs from G to the underlying graph UC of C with the following property. Given any category B and any morphism $D : G \to UB$ of graphs, there is a unique functor $D' : C \to B$ with $(UD') \circ P = D$, as in the commutative diagram*

$$\begin{tikzcd}
C \arrow[d, dotted, "D'"] \\
B
\end{tikzcd}
\qquad
\begin{tikzcd}
G \arrow[r, "P"] \arrow[dr, "D"'] & UC \arrow[d, dotted, "UD'"] \\
& UB
\end{tikzcd}$$

In particular, if B had O as set of objects and D is a morphism of O-graphs, then D' is the identity on objects.

Corollary 3.9.1. *To any set X there is a monoid M and a function $p : X \to UM$, where UM is the underlying set of M, with the following universal property: for any monoid L and any function $h : X \to UL$ there is a unique morphism $h' : M \to L$ of monoids with $h : Uh' \circ p$.*

$$Hom_{Cat}(C(G), B) \cong Grph(G, UB),\ D' \mapsto D = UD' \circ P$$

3.9.5 Comma Categories

3.9.5.1 Category of objects unber b $(b \downarrow C)$

Objects $\langle f, c\rangle$:

$$\begin{tikzcd}
b \arrow[d, "f"] \\
c
\end{tikzcd}$$

Arrows $\langle f, c\rangle \xrightarrow{h} \langle f', c'\rangle$:

$$\begin{tikzcd} & b \arrow[dl, "f'"'] \arrow[dr, "f"] & \\ c \arrow[rr, "h"] & & c' \end{tikzcd}$$

3.9.5.2 Category of objects over a $(C \downarrow a)$

Objects $\langle f, c\rangle$:

$$\begin{tikzcd} c \arrow[d, "f"] \\ a \end{tikzcd}$$

Arrows $\langle f, c\rangle \xrightarrow{h} \langle f', c'\rangle$:

$$\begin{tikzcd} c \arrow[rr, "h"] \arrow[dr, "f"'] & & c' \arrow[dl, "f'"] \\ & a & \end{tikzcd}$$

3.9.5.3 Category of objects S-unber b $(b \downarrow S)$

Given a functor $S : D \to C$.

Objects $\langle f, Sd\rangle$:

$$\begin{tikzcd} b \arrow[d, "f"] \\ Sd \end{tikzcd}$$

Arrows $\langle f, Sd\rangle \xrightarrow{Sh} \langle f', Sd'\rangle$:

$$\begin{tikzcd} & b \arrow[dl, "f'"'] \arrow[dr, "f"] & \\ Sd \arrow[rr, "Sh"] & & Sd' \end{tikzcd}$$

3.9.5.4 Category of objects T-over a $(T \downarrow a)$

Given a functor $T : E \to C$.

Objects $\langle f, Te\rangle$:

$$\begin{tikzcd} Te \arrow[d, "f"] \\ a \end{tikzcd}$$

Arrows $\langle f, Te\rangle \xrightarrow{Th} \langle f', Te'\rangle$:

$$\begin{tikzcd} Te \arrow[rr, "Th"] \arrow[dr, "f"'] & & Te' \arrow[dl, "f'"] \\ & a & \end{tikzcd}$$

3.9.5.5 Comma Category $(T \downarrow S)$

Given functors $S : D \to C$ and $T : E \to C$.

Objects $\langle e, d, f\rangle$:

$$\begin{tikzcd} Te \arrow[d, "f"] \\ Sd \end{tikzcd}$$

where $d \in$Obj(D), $e \in$Obj(E), $f : Te \to Sd$.

Arrows $\langle e, d, f\rangle \xrightarrow{\langle k,h\rangle} \langle e', d', f'\rangle$:

$$\begin{tikzcd} Te \arrow[r, "Tk"] \arrow[d, "f"] & Te' \arrow[d, "f'"] \\ Sd \arrow[r, "Sh"] & Sd' \end{tikzcd}$$

where $k : e \to e'$, $h : d \to d'$ such that $f' \circ Tk = Sh \circ f$.

Composition $\langle k', h'\rangle \circ \langle k, h\rangle = \langle k' \circ k, h' \circ h\rangle$ when defined.

$$\begin{tikzcd} & & & T \downarrow S \arrow[dlll, "P"'] \arrow[d, "Q"] \arrow[drrr, "R"] & & & \\ E \arrow[r, "T"'] & C & & C^2 \arrow[ll, "C^{d_0}"] \arrow[rr, "C^{d_1}"'] & & C & D \arrow[l, "S"] \end{tikzcd}$$

P and Q are the *projections* of the comma category. C^{d_0}, C^{d_1}, resp., send arrows to domain, codomain, resp.

$$
\begin{tikzcd}
 & & \langle e, d, f : Te \to Sd \rangle \arrow[dll, mapsto] \arrow[d, mapsto] \arrow[drr, mapsto] & & \\
e \arrow[r, mapsto] & Te & (f : Te \to Sd) \arrow[l, mapsto] \arrow[r, mapsto] & Sd & d \arrow[l, mapsto]
\end{tikzcd}
$$

3.10 Higher Level Categories

3.10.1 Functor Categories

A *functor category* is a category whose objects are functors and whose arrows are natural transformations. Since compositions of natural transformations are natural transformations, composition can be defined as in the following diagram...

$$
\begin{tikzcd}
Rc \arrow[r, "Rf"] \arrow[d, "\sigma c"] \arrow[dd, bend right, "(\tau\circ\sigma)c"'] & Rc' \arrow[d, "\sigma c'"'] \arrow[dd, bend left, "(\tau\circ\sigma)c'"] \\
Sc \arrow[r, "Sf"] \arrow[d, "\tau c"] & Sc' \arrow[d, "\tau c'"'] \\
Tc \arrow[r, "Tf"] & Tc'
\end{tikzcd}
$$

3.10.2 2-Categories

3.10.2.1 Vertical Composition

For natural transformations τ and σ, we have "vertical" composition $\tau\dot{\sigma}$, as in the following diagram...

$$
\begin{tikzcd}
C \arrow[r] \arrow[d, "\sigma"] \arrow[dd, bend right, "\tau\sigma"'] & B \arrow[d, "\sigma"] \arrow[dd, bend left, "\tau\sigma"] \\
C \arrow[r] \arrow[d, "\tau"] & B \arrow[d, "\tau"] \\
C \arrow[r] & B
\end{tikzcd}
$$

3.10.2.2 Horizontal Composition

We can also define "horizontal" composition for natural transformations τ and τ', $\tau' \circ \tau$, as in the following commutative diagrams...

$$
\begin{tikzcd}
C \arrow[r, "S"] \arrow[d, "\tau"] & B \arrow[r, "S'"] \arrow[d, bend right, "\tau"'] \arrow[d, bend left, "\tau'"] & A \arrow[d, "\tau'"] \\
C \arrow[r, "T"] & B \arrow[r, "T'"] & A
\end{tikzcd}
$$

$$
\begin{tikzcd}
S'Sc \arrow[r, "\tau' Sc"] \arrow[d, "S'\tau c"] \arrow[dr, dotted, "(\tau'\circ\tau)c"] & T'Sc \arrow[d, "T'\tau c"] \\
S'Tc \arrow[r, "\tau' Tc"] & T'Tc
\end{tikzcd}
$$

The next diagram shows $\tau' \circ \tau : S'S \dot{\to} T'T$ is natural.

$$
\begin{tikzcd}
c \arrow[d, "f"] & S'Sc \arrow[r, "S'\tau c"] \arrow[d, "S'Sf"] & S'Tc \arrow[r, "\tau' Tc"] \arrow[d, "S'Tf"] & T'Tc \arrow[d, "T'Tf"] \\
b & S'Sb \arrow[r, "T'\tau b"] & S'Tb \arrow[r, "\tau' Tb"] & T'Tb
\end{tikzcd}
$$

So $\tau' \circ \tau = (T' \circ \tau) \cdot (\tau' \circ S) = (\tau' \circ T) \cdot (S' \circ \tau)$, which leads into our next concept.

3.10.2.3 Interchange Law

For natural transformations $\sigma, \sigma', \tau, \tau'$ satisfying…

$$
\begin{tikzcd}
C \arrow[r] \arrow[d, "\sigma"] & B \arrow[r] \arrow[d, bend right, "\sigma"'] \arrow[d, bend left, "\sigma'"] & A \arrow[d, "\sigma'"] \\
C \arrow[r] \arrow[d, "\tau"] & B \arrow[r] \arrow[d, bend right, "\tau"'] \arrow[d, bend left, "\tau'"] & A \arrow[d, "\tau'"] \\
C \arrow[r] & B \arrow[r] & A
\end{tikzcd}
$$

the *interchange law* is $(\tau' \cdot \sigma') \circ (\tau \cdot \sigma) = (\tau' \circ \tau) \cdot (\sigma' \circ \sigma)$.

The proof of the interchange law derives from the following diagram. Intuitively, the interchange law occurs along the dotted diagonal lines.

$$
\begin{tikzcd}
S'Sc \arrow[r, "\sigma' S"] \arrow[d, "S'\sigma"] \arrow[dr, dotted] \arrow[ddrr, dotted, bend left] & T'Sc \arrow[r, "\tau' S"] \arrow[d, "T'\sigma"] & R'Sc \arrow[d, "R'\sigma'"] \\
S'Tc \arrow[r, "\sigma' T"] \arrow[d, "S'\tau"] & T'Tc \arrow[r, "\tau' T"] \arrow[d, "T'\tau"] \arrow[dr, dotted] & R'Tc \arrow[d, "R'\tau'"] \\
S'Rc \arrow[r, "\sigma' R"] & T'Rc \arrow[r, "\tau' R"] & R'Rc
\end{tikzcd}
$$

Theorem 3.10.1. *The collection of natural transformations in the set of arrows of two different categories under two different operations of composition, $\cdot$ and $\circ$, which satisfy the interchange law. Moreover, any arrow (transformation) which is an identity for the composition $\circ$ is also an identity for the composition $\cdot$.*

3.10.2.4 Double Category

The set of arrows for two different compositions with two different compositions which together satisfy the interchange law.

3.10.2.5 2-Category

A double category in which every identiy arrow for the first composition is also an identity for the second composition.

4 Category Examples

4.1 The category Set

- Objects: Sets
- Arrows: Functions

4.1.1 Morphisms

Proposition 4.1.1. *A function is injective if and only if it is a monomorphism.*

Proposition 4.1.2. *A function is surjective if and only if it is a monomorphism.*

Theorem 4.1.1 (Canonical Decomposition in Set)**.** *Let $f : A \to B$ be any function, and define $\sim$ as above. Then f decomposes as follows:*

$$\begin{tikzcd} A \arrow[r, two heads] \arrow[rrr, bend left, "f"] & (A/\sim) \arrow[r, "\sim", "f"'] & \mathrm{im} f \arrow[r, hook] & B \end{tikzcd}$$

where the first function is the canonical projection $A \to A/\sim$, the third function is the inclusion im$f \subseteq B$, and the bijection $\tilde{f}$ in the middle is defined by

$$\tilde{f}([a]_\sim) := f(a)$$

for all $a \in A$.

4.1.2 Universal Objects

Proposition 4.1.3. *$\emptyset$ is an initial object in Set.*

Proposition 4.1.4. *Singletons are final objects in Set.*

Proposition 4.1.5. *Cartesian products are products in Set.*

Proposition 4.1.6. *Disjoint unions are coproducts in Set.*

Proposition 4.1.7. *Given a set A and an equivalence relation $\sim$ on A, $(A/\sim)$ is a quotient in Set.*

4.2 The category Grp

- Objects: Groups
- Arrows: Homomorphisms

4.2.1 Morphisms

Proposition 4.2.1. *The following are equivalent:*

1. *φ is a monomorphism*
2. *$ker\varphi = \{e_G\}$*
3. *$\varphi : G \to G'$ is injective (as a set function)*

Proof. (1) $\Rightarrow$ (2): Consider the two parallel compositions...

$$\ker\varphi \underset{e}{\overset{\iota}{\rightrightarrows}} G \xrightarrow{\varphi} G'$$

where ι is the inclusion and e is the trivial map. Both $\varphi \circ \iota$ and $\varphi \circ e$ are the trivial map; since φ is a monomorphism, this implies $\iota = e$. But then $\ker\varphi$ is trivial.
(2) $\Rightarrow$ (3): Observe...

$$\begin{aligned}\varphi(g_1) = \varphi(g_2) \Rightarrow \varphi(g_1)\varphi(g_2)^{-1} = e_G \Rightarrow \varphi(g_1 g_2^{-1}) = e_{G'} \\ \Rightarrow g_1 g_2^{-1} \in \ker\varphi \overset{!}{\Rightarrow} g_1 g_2^{-1} = e_G \Rightarrow g_1 = g_2.\end{aligned}$$

(3) $\Rightarrow$ (1): If φ is injective, then it satisfies the defining property for monomorphisms in Set. $\square$

4.2.2 Isomorphism Theorems

Theorem 4.2.1 (Canonical Decomposition in Grp)**.** *Every group homomorphism $\varphi : G \to G'$ may be decomposed as follows:*

$$\begin{tikzcd} G \arrow[r, two heads] \arrow[rrr, bend left, "\varphi"] & (G/\ker\varphi) \arrow[r, "\sim", "\tilde{\varphi}"'] & \mathrm{im}\varphi \arrow[r, hook] & G' \end{tikzcd}$$

where the isomorphism $\tilde{\varphi}$ in the middle is the homomorphism induced by φ as in 5.5.1.

Corollary 4.2.1 (First Isomorphism Theorem in Grp)**.** *Suppose $\varphi : G \to G'$ is a surjective group homomorphism. Then*

$$G' \cong \frac{G}{ker\varphi}.$$

Theorem 4.2.2 (Second Isomorphism Theorem in Grp)**.** *Let H, K be subgroups of a group G, and assume that H is normal in G. Then...*

- *HK is a subgroup of G, and H is normal in HK*

- *$H \cap K$ is normal in K, and*

$$\frac{HK}{H} \cong \frac{K}{H \cap K}.$$

Proof. To verify that HK is a subgroup of G when H is noraml, note that HK is the union of all cosets Hk, wiht $k \in K$; that is,

$$HK = \pi^{-1}(\pi(K)),$$

where $\pi : G \to G/H$ is the canonical projection. Since $\pi(K)$ is a subgroup of G/H, HK is a subgroup by 5.4.2. It is clear that H is normal in HK.

For the second part, consider the homomorphism...

$$\varphi : K \to HK/H$$

sending $k \in K$ to the coset Hk. This homomorphism is *surjective*: indeed, every element of HK/H may be written as a coset

$$Hhk, \;\; h \in H, \, k \in K;$$

but $Hhk = Hk$, so $Hhk = \varphi(k)$ is the image of φ. By 4.2.1,

$$\frac{HK}{H} \cong \frac{K}{\ker\varphi}.$$

To complete the proof note...

$$\ker\varphi = \{k \in K | \varphi(k) = e\} = \{k \in K | Hk = H\} = \{k \in K | k \in H\} = H \cap K.$$

□

Theorem 4.2.3 (Third Isomorphism Theorem in Grp)**.** *Let H be a normal subgroup of a group G, and let N be a subgroup of G containing H. Then N/H is normal in G/H if and only if N is normal in G, and in this case*

$$\frac{G/H}{N/H} \cong \frac{G}{N}$$

Proof. If N is normal, then consider the projection $\pi_N : G \to \frac{G}{N}$. The subgroup H is contained in $N = \ker\varphi$, so by 5.5.1 we get an induced homomorphism $\varphi' : \frac{G}{H} \to \frac{G}{N}$. The subgroup N/H of G/H is a kernel of φ'; therefore it is normal.

Conversely, if N/H is normal in G/H, consider the composition...

$$G \twoheadrightarrow \frac{G}{H} \twoheadrightarrow \frac{G/H}{N/H}.$$

The kernel of this homomorphism is N, therefore N is normal. Further, this homomorphism is surjective; hence the stated isomorphism $(G/H)/(N/H) \cong G/N$ follows immediately from 4.2.1. □

4.2.3 Universal Objects

Proposition 4.2.2. *Trivial groups are null objects in Grp.*

Proposition 4.2.3. *Grp has products. (See Group Products)*

Proposition 4.2.4. *Grp has coproducts. (See Free Group Products)*

4.3 The category Ab

- Objects: Abelian Groups
- Arrows: Homomorphisms

4.3.1 Morphisms

Proposition 4.3.1. *The following are equivalent:*

1. φ *is an epimorphism*
2. *coker*$\varphi = \{e_{G'}\}$
3. $\varphi : G \to G'$ *is surjective (as a set function)*

Proof. (1) $\Rightarrow$ (2): Assume (1) holds, and consider the two parallel compositions. . .

$$G \xrightarrow{\varphi} G' \overset{\pi}{\underset{e}{\rightrightarrows}} \mathrm{coker}\varphi$$

where π is the canonical projection and e is the trivial map. Both $\pi \circ \varphi$ and $e \circ \varphi$ are the trivial map; since φ is an epimorphism, this implies $\pi = e$. But $\pi = e$ implies that cokerφ is trivial.
(2) $\Rightarrow$ (3): If coker$\varphi = G'/\mathrm{im}\varphi$ is trivial, then im$\varphi = G'$; hence φ is surjective.
(3) $\Rightarrow$ (1): If φ is surjective, then it satisfies the universal property for epimorphisms in Set: for any set Z and any two set-functions α' and $\alpha'' : G' \to Z$,

$$\alpha' \circ \varphi = \alpha'' \circ \varphi \Leftrightarrow \alpha' = \alpha''.$$

This must hold in particular if Z is endowed with a group structure and α', α'' are group homomorphisms, so φ is an epimorphism in Grp. □

4.3.2 Universal Objects

Proposition 4.3.2. *Trivial groups are null objects in Ab.*

Proposition 4.3.3. *Ab has products and coproducts. They are the same construct and are called* Direct Sums, *denoted* $G \oplus H$. *(See Group Products)*

4.4 The category Ring

- Objects: Rings
- Arrows: Ring homomorphisms

4.4.1 Morphisms

Proposition 4.4.1. *For a ring homomorphism $\varphi : R \to S$, the following are equivalent:*

1. *φ is a monomorphism;*
2. *$ker\varphi = \{0\}$;*
3. *φ is injective (as a set-function).*

Proof. Only (1) $\Rightarrow$ (2) warrants serious attention. Assume $\varphi : R \to S$ ois a monomorphism and $r \in \ker\varphi$. Applying the extension property given from the universal property of polynomial rings, we obtain unique ring homomorphisms $ev_r : \mathbb{Z}[x] \to R$ such that $ev_r(x) = r$ and $ev_0 : \mathbb{Z}[x] \to R$ such that $ev(x) = 0$. Consider the parallel ring homomorphisms:

$$\mathbb{Z}[x] \underset{ev_0}{\overset{ev_r}{\rightrightarrows}} R \xrightarrow{\varphi} S,$$

since $\varphi(r) = 0 = \varphi(0)$, the two compositions $\varphi \circ ev_r$, $\varphi \circ ev_0$ agree (because they agree on $\mathbb{Z}$ and they agree on x); hence $ev_r = ev_0$ since φ is a monomorphism. Therefore...

$$r = ev_r(x) = ev_0(x) = 0,$$

showing $r \in \ker\varphi$. ∎

In Ring, epimorphisms need not be surjective.

Proposition 4.4.2. *The function $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$ is an epimorphism.*

Proof. Suppose α_1 and α_2 are parallel ring homomorphisms...

$$\mathbb{Z} \hookrightarrow \mathbb{Q} \underset{\alpha_2}{\overset{\alpha_1}{\rightrightarrows}} R$$

and α_1, α_2 agree on $\mathbb{Z}$. Then α_1, α_2 must agree on $\mathbb{Q}$: because for $p, q \in \mathbb{Z}, q \neq 0$,

$$\alpha_i\left(\frac{p}{q}\right) = \alpha_i(p)\alpha_i(q^{-1}) = \alpha(p)\alpha(q)^{-1}$$

is the same for both. ∎

4.4.2 Isomorphism Theorems

Theorem 4.4.1 (Canonical Decomposition in Ring)**.** *Every ring homomorphism $\varphi : R \to S$ may be decomposed as follows:*

$$\begin{tikzcd} R \arrow[r, two heads] \arrow[rrr, bend left, "\varphi"] & (R/\ker\varphi) \arrow[r, "\sim", "\tilde{\varphi}"'] & \mathrm{im}\varphi \arrow[r, hook] & S \end{tikzcd}$$

where the isomorphism $\tilde{\varphi}$ in the middle is the homomorphism induced by φ as in 8.4.1.

Corollary 4.4.1. *Suppose $\varphi : R \to S$ is a surjective ring homomorphism. Then*

$$S \cong \frac{R}{ker\varphi}.$$

Note: The 'second isomorphism' theorem doesn't quite make sense in the context of Ring.

Theorem 4.4.2. *Let I is an ideal of a ring R, and let J be an ideal of R containing I. Then J/I is an ideal of R/I, and...*

$$\frac{R/I}{J/I} \cong \frac{R}{J}$$

4.4.3 Universal Objects

Proposition 4.4.3. *Zero rings are final objects in Ring.*

Proposition 4.4.4. *The ring of integers $\mathbb{Z}$ is an initial object in Ring.*

Proof. Observe $\varphi : \mathbb{Z} \to R$ defined by $(\forall n \in \mathbb{Z}) : \quad \varphi(n) = n \cdot 1_R$ is a ring homomorphism by...

$$\varphi(mn) = \sum_{i=1}^{mn} 1_R = \sum_{i=1}^{m} (\sum_{j=1}^{n} 1_R) \stackrel{!}{=} (\sum_{i=1}^{m} 1_R) \cdot (\sum_{j=1}^{n} 1_R) = \varphi(m) \cdot \varphi(n),$$

(where ! occurs via the distributivity axiom) and is unique, since it is determined by the requirement that $\varphi(1) = 1_R$ and by the fact that φ preserves addition. □

4.5 The category R-Mod

- Objects: R-modules (where R is commutative)
- Arrows: R-module homomorphisms

4.5.1 Morphisms

Proposition 4.5.1. *The following hold in R-Mod:*

- *kernels and cokernels exists*
- *φ is a monomorphism $\Leftrightarrow$ ker φ is trivial $\Leftrightarrow$ φ is injective as a set function*
- *φ is an epimorphism $\Leftrightarrow$ coker φ is trivial $\Leftrightarrow$ φ is surjective as a set function*

Further, every monomorphism identifies its source with the kernel of some morphism, and every epimorphism identifies its target with the cokernel of some morphism.

4.5.2 Isomorphism Theorems

Theorem 4.5.1 (Canonical Decomposition in R-Mod)**.** *Every R-module homomorphism $\varphi : M \to M'$ may be decomposed as follows:*

$$\begin{tikzcd} M \arrow[r, two heads] \arrow[rrr, bend left, "\varphi"] & (M/\ker\varphi) \arrow[r, "\sim", "\tilde{\varphi}"'] & \operatorname{im}\varphi \arrow[r, hook] & M' \end{tikzcd}$$

where the isomorphism $\tilde{\varphi}$ in the middle is the homomorphism induced by φ as in 10.3.1.

Corollary 4.5.1. *Suppose $\varphi : M \to M'$ is a surjective R-module homomorphism. Then…*

$$M' \cong \frac{M}{ker\varphi}.$$

Theorem 4.5.2. *Let N, P be submodules of an R-module M. Then…*

- *$N + P$ is a submodule of M;*
- *$N \cap P$ is a submodule of P, and*

$$\frac{N+P}{N} \cong \frac{P}{N \cap P}.$$

Theorem 4.5.3. *Let N be a submodule of an R-module M, and let P be a submodule of M containing N. Then P/N is an ideal of M/N, and…*

$$\frac{M/N}{P/N} \cong \frac{M}{P}.$$

4.5.3 Universal Objects

Proposition 4.5.2. *Trivial groups have a unique module structure over any ring R and is a null object in R-Mod.*

R-Mod is a similar category to that of Ab, note…

Proposition 4.5.3. *$Hom_{R-Mod}(M, N)$ is an object in R-Mod.*

Proposition 4.5.4. *R-Mod has products and coproducts. See .*

5 Group Theory

5.1 Definition

A *group* is a groupoid with a single object.

A *group* $\langle G, \boldsymbol{\cdot} \rangle$ is a set G endowed with the binary operation $\boldsymbol{\cdot}$ such that...

1. the operation $\cdot$ is *associative*
2. there exists an *identity element* e_G for $\boldsymbol{\cdot}$
3. every element in G has an *inverse* with respect to $\boldsymbol{\cdot}$

We can repeated elements as follows...

- $g^n = g \boldsymbol{\cdot} g \cdots g \boldsymbol{\cdot} g$ (n times)
- $g^{-n} = g^{-1} \boldsymbol{\cdot} g^{-1} \cdots g^{-1} \boldsymbol{\cdot} g^{-1}$ (n times)

Proposition 5.1.1. *The identity $e_G \in G$ of a group is unique.*

Proof. If h is another identity, then $h = e_G h = e_G$. □

Proposition 5.1.2. *Inverses in a group G are unique.*

Proposition 5.1.3 (Cancellation)**.** *Let G be a group. Then $\forall a, g, h \in G \ldots$*

$$ga = ha \Rightarrow g = h, \quad ag = ah \Rightarrow g = h.$$

5.2 Order

5.2.1 Order of an element

The *order of an element* $g \in G$, denoted $|g|$, is the smallers positive integer n such that $g^n = e$.
g has *finite order* if any such integer exists.

g has *infinite order* if no such integer exists, denoted $|g| = \infty$.

Lemma 5.2.1. *If $g^n = e$ for some positive integer n, then $|g|$ is a divisor of n.*

Proof. As observed, $n \geq |g|$ for $n \in \mathbb{Z}$, that is $n - |g| \geq 0$. Since $\mathbb{Z}$ is a Euclidean domain, there must exist an integer $m > 0$ such that...

$$r = n - |g| \cdot m \geq 0 \text{ and } n - |g| \cdot (m+1) < 0,$$

that is, $r < |g|$. Note that...

$$g^r = g^{n-|g| \cdot m} = g^n \cdot (g^{|g|})^{-m} = e \cdot e^{-m} = e.$$

By definition of order, $|g|$ is the smallest positive integer such that $g^{|g|} = e$. Since r is smaller than $|g|$ and $g^r = e$, r cannot be positive; hence $r = 0$ necessarily. So $n = |g| \cdot m$. □

Corollary 5.2.1. *Let g be an element of finite order, and let $N \in \mathbb{Z}$. Then...*

$$g^N = e \Leftrightarrow N \textit{ is a multiple of } |g|$$

5.2.2 Order of a group

If G is finite as a set, its *order* $|G|$ is the number of its elements; we write $|G| = \infty$ if G is infinite.

Proposition 5.2.1. *Let $g \in G$ be an element of finite order. Then g^m has finite order $\forall m \geq 0$, and in fact*

$$|g^m| = \frac{lcm(m, |g|)}{m} = \frac{|g|}{gcd(m, |g|)}.$$

Proof. The order of g^m is the least positive d for which...

$$g^{md} = e.$$

In other words, $m|g^m|$ is the smallest multiple of m which is also a multiple of $|g|$:

$$m|g^m| = \operatorname{lcm}(m, |g|).$$

□

Proposition 5.2.2. *If $gh = hg$, then $|gh|$ divides $lcm(|g|, |h|)$.*

Proof. Observe...

$$(gh)^{\operatorname{lcm}(m,n)} = (gh)(gh)\cdots(gh) = gg\cdots g{\cdot}hh\cdots h = g^{\operatorname{lcm}(m,n)}h^{\operatorname{lcm}(m,n)} = e.$$

□

5.2.3 Index of a subgroup

The *index* of H in G, denoted $[G : H]$, is the number of elements $|G/H|$ of G/H, when this is finite, and ∞ otherwise.

Lemma 5.2.2. *Let H be a subgroup of a group G. Then $\forall g \in G$ the functions*

$$H \to gH,\ h \mapsto gh,$$

$$H \to Hg,\ h \mapsto hg$$

are bijections.

Proof. Surjectiveness is clear and cancellation implies that they are injective. □

5.2.4 Lagrange's Theorem

Corollary 5.2.2. *If G is a finite group and $H \subseteq G$ is a subgroup, then $|G| = [G : H] \cdot |H|$. In particular, $|H|$ is a divisor of $|G|$.*

Proof. Indeed, G is the disjoint union of $|G/H|$ distinct cosets gH, and $|gH| = |H|$ by 5.2.2. $\square$

Corollary 5.2.3. *If $g \in G$, then $a \cdot |g| = |G|$ for some positive integer a.*

5.2.5 Cauchy's Theorem

Theorem 5.2.1 (Cauchy's Theorem)**.** *Let G be a finite group, and let p be a prime divisor of $|G|$. Then G contains an element of order p.*

Proof (James McKay). Consider the set S of ordered p-tuples of elements of G:

$$(a_1, \dots, a_p)$$

such that $a_1 \cdots a_p = e$. I claim that $|S| = |G|^{p-1}$: indeed, once $a_1, \dots, a_{p-1}$ are chosen (arbitrarily), then a_p is determined as it is the inverse of $a_1 \cdots a_{p-1}$.

Therefore, p divides the order of S as it divides the order of G.

Also note that if $a_1 \cdots a_p = e$, then...

$$a_2 \cdots a_p a_1 = e$$

(even if G is not commutative): because if a_1 is a let-inverse to $a_2 \cdots a_p$, then it is also a right-inverse to it.

Therefore, we may act with the group $\mathbb{Z}/p\mathbb{Z}$ on S: given $[m] \in \mathbb{Z}/p\mathbb{Z}$, with $0 \le m < p$, act by $[m]$ on...

$$(a_1, \dots, a_p)$$

by sending it to...

$$(a_{m+1}, \dots, a_p, a_1, \dots, a_m):$$

as we just observed, this is still an element of S.

Now via 5.7.2 we have...

$$|Z| \equiv |S| \equiv 0 \bmod p,$$

where Z is the set of fixed points of this action. Fixed points are p-tuples of the form...

$$(a, \dots, a);$$

and note that $Z \neq \emptyset$, since $\{e, \dots, e\} \in Z$. Since $p \ge 2$ and p divides $|Z|$, we conclude that $|Z| > 1$; therefore there exists some element in Z of the form, with $a \neq e$.

This says that there exists an $a \in G$, $a \neq e$, such that $a^p = e$, proving the statement. $\square$

Corollary 5.2.4. *Let G be a finite group, let p be a prime divisor of $|G|$, and let N be the number of cyclic subgroups of G of order p. Then $N \equiv 1$ mod p.*

5.3 Homomorphism

For groups $\langle G, \cdot_G \rangle$, $\langle H, \cdot_H \rangle$, a *group homomorphism*...

$$\varphi : \langle G, \cdot_G \rangle \to \langle H, \cdot_H \rangle$$

is a set-function preserving the binary operations of the groups, i.e. the following diagram commutes...

$$\begin{array}{ccc} G \times G & \xrightarrow{\varphi \times \varphi} & H \times H \\ \big\downarrow{\cdot_G} & & \big\downarrow{\cdot_H} \\ G & \xrightarrow{\quad \varphi \quad} & H \end{array}$$

i.e. $\forall a, b \in G$ we have $\varphi(a \cdot_G b) = \varphi(a) \cdot_H \varphi(b)$.

Proposition 5.3.1. *Let $\varphi : G \to H$ be a group homomorphism. Then...*

- $\varphi(e_G) = e_H$
- $\forall g \in G, \varphi(g^{-1}) = \varphi(g)^{-1}$.

Proof. For the first item observe...

$$e_H \ldots \varphi(e_G) = \varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G) \Rightarrow e_H = \varphi(e_G).$$

For the second item observe...

$$\varphi(g^{-1}) \cdot \varphi(g) = \varphi(g^{-1} \cdot g) = \varphi(e_G) = e_H = \varphi(g)^{-1} \cdot \varphi(g) \Rightarrow \varphi(g^{-1}) = \varphi(g)^{-1}$$

□

5.3.1 Some Important Morphisms

5.3.1.1 Trivial Morphism

Because $\{*\}$ is a null object in Grp (and Ab) we are guaranteed unique morphisms...

$$\varphi : G \to \{*\},\ \psi : \{*\} \to H.$$

We call the resulting composition $\psi \circ \varphi : G \to H$ the *trivial morphism.*

5.3.1.2 Exponential Map

Given a group G, the *exponential map* is the homomorphism $\epsilon : \mathbb{Z} \to G$ defined by $z \mapsto g^z$.

5.3.2 Interaction with order

Proposition 5.3.2. *Let $\varphi : G \to H$ be a group homomorphism, and let $g \in G$ be am element of finite order. Then $|\varphi(g)|$ divides $|g|$.*

Proof. Observe, $\varphi(g)^{|g|} = e_H$ and apply 5.2.1. □

5.3.3 Isomophisms

Proposition 5.3.3. *Let $\varphi : G \to H$ be a group homomorphism. Then φ is an isomorphism of groups if and only if it is a bijection.*

Two groups G, H are *isomorphic* if there is an isomorphism between them.

Proposition 5.3.4. *Let $\varphi : G \to H$ be an isomorphism.*

- $(\forall g \in G) : |\varphi(g)| = |g|$;
- *G is commutative if and only if H is commutative.*

5.4 Subgroup

Let $\langle G, \cdot \rangle$ be a group, and $\langle H, \cdot \rangle$ another group, whose underlying set H is a subset of G.

$\langle H, \cdot \rangle$ is a *subgroup* of G if the inclusion function $\iota : H \hookrightarrow G$ is a group homomorphism.

Proposition 5.4.1. *A nonempty subset H of a group G is a subgroup if and only if $(\forall a, b \in H) :\ ab^{-1} \in H$.*

Lemma 5.4.1. *If $\{H_\alpha\}_{\alpha \in A}$ is any family of subgroups of a group G, then...*

$$H = \bigcap_{\alpha \in A} H_\alpha$$

is a subgroup of G.

Lemma 5.4.2. *Let $\varphi : G \to G'$ be a group homomorphism, and let H' be a subgroup of G'. Then $\varphi^{-1}(H')$ is a subgroup of G.*

5.4.1 Normal Subgroup

A subgroup N of a group G is *normal* if $\forall g \in G$, $\forall n \in N$,

$$gng^{-1} \in N.$$

5.4.2 Kernel of a Homomorphism

The *kernel* of $\varphi : G \to G'$, $\ker\varphi$, is the subgroup of G consiting of...

$$\ker\varphi := \{g \in G | \varphi(g) = e_{G'}\} = \varphi^{-1}(e_{G'}).$$

Proposition 5.4.2. *Let $\varphi : G \to G'$ be a homomorphism. Then the inclusion $\iota : \ker\varphi \hookrightarrow G$ is final in the category of group homomorphisms $\alpha : K \to G$ such that $\varphi \circ \alpha$ is the trivial morphism. In other words the following diagram commutes.*

$$\begin{tikzcd} K \arrow[r, "\alpha"] \arrow[rr, bend left, "0"] \arrow[dr, "\exists!\bar{\alpha}"'] & G \arrow[r, "\varphi"] & G' \\ & \ker\varphi \arrow[u, hook, "\iota"'] & \end{tikzcd}$$

Lemma 5.4.3. *If $\varphi : G \to G'$ is any group homomorphism, then* $\ker\varphi$ *is a normal subgroup of* G*.*

Proof. Since $\ker\varphi$ is a subgroup by the previous proposition, we need only verify it is normal. Observe $\forall g \in G, \forall n \in \ker\varphi \ldots$

$$\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g^{-1}) = \varphi(g)e_{G'}\varphi(g)^{-1} = e_{G'},$$

proving that $gng^{-1} \in \ker\varphi$. □

5.4.3 Image of a Homomorphism

The *image* of $\varphi : G \to G'$, $\mathrm{im}\varphi$, is the subgroup of G' consiting of...

$$\mathrm{im}\varphi := \{\varphi(g) | g \in G\}.$$

5.4.4 Subgroup generated by a subset

If $A \subseteq G$, we are guaranteed a unique group homomorphism

$$\varphi_A : F(A) \to G$$

extending the inclusion map, by the universal property of free groups. Then $\mathrm{im}\varphi_A$ is the *subgroup generated by* A in G, denoted $\langle A \rangle$.

This subgroup may also be constructed as...

$$\langle A \rangle = \bigcap_{H \text{ subgroup of } G, H \supseteq A} H.$$

5.4.4.1 Finitely Generated

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

5.4.5 Commutator Subgroup

Let G be a group. The *commutator* subgroup of G, denoted $[G, G]$, is the subgroup generated by all elements...

$$[g, h] = ghg^{-1}h^{-1}$$

with $g, h \in G$.

Lemma 5.4.4. *Let $\varphi : G_1 \to G_2$ be a group homomorphism. Then $\forall g, h \in G_1$ we have...*

$$\varphi([g,h]) = [\varphi(g), \varphi(h)]$$

and $\varphi(G_1') \subseteq G_2'$.

Proposition 5.4.3. *Let G' be the commutator subgroup of G. Then...*

- *$[G,G]$ is normal in G;*
- *the quotient $G/[G,G]$ is commutative;*
- *if $\alpha : G \to A$ is a homomorphism of G to a commutative group, then $[G,G] \subseteq ker\ \alpha$;*
- *the natural projection $G \to G/[G,G]$ is universal in the category of group homomorphisms $G \to A$ where A is an abelian group*

5.5 Group Constructions

5.5.1 Product of Groups

Let G and H be two groups. Define $G \times H := \{(g,h) | g \in G, h \in H\}$ with the operation $(g_1, h_1) \cdot_{G\times H} (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$. Then $G \times H$ is the product group of the groups G and H.

5.5.2 Semidirect Product

5.5.2.1 Motivating Theorems

Lemma 5.5.1. *Let N, H be normal subgroups of a group G. Then...*

$$[N,H] \subseteq N \cap H.$$

Proof. It suffices to verify this on generatros, that is, it suffices to check that

$$[n,h] = n(hnh^{-1}h^{-1}) = (nhn^{-1})h^{-1} \in N \cap H$$

for all $n \in N$, $h \in H$. But the first expression and the normality of N show that $[n,h] \in N$; the second expression and the normality of H show that $[n,h] \in H$. □

Corollary 5.5.1. *Let N, H be normal subgroups of a group G. Assume $N \cap H = \{e\}$. Then N, H commute with each other:*

$$(\forall n \in N)(\forall h \in H)\ nh = hn.$$

Proposition 5.5.1. *Let N, H be normal subgroups of a group G, such that $N \cap H = \{e\}$. Then $NH \cong N \times H$.*

Proof. Consider the function...

$$\varphi : N \times H \to NH$$

defined by $\varphi(n, h) = nh$. Under the stated hypothesis, φ is a group homomorphism: indeed...

$$\begin{aligned}\varphi((n_1, h_1) \cdot (n_2, h_2)) &= \varphi((n_1 n_2, h_1 h_2)) \\ &= n_1 n_2 h_1 h_2 \\ &= n_1 h_1 n_2 h_2\end{aligned}$$

since N, H commute by the previous corrolary...

$$= \varphi((n_1, h_1)) \cdot \varphi((n_2, h_2)).$$

The homomorphism φ is surjective by definition of NH. To verify it is injective, consider its kernel:

$$\ker \varphi = \{(n, h) \in N \times H | nh = e\}.$$

If $nh = e$, then $n \in N$ and $n = h^{-1} \in H$; thus $n = e$ since $N \cap H = \{e\}$. Usint the same token for h, we conclude $h = e$; hence $(n, h) =$ the identity in $N \times H$, proving that φ is injective.

Thus φ is an isomorphism, as needed. $\square$

5.5.2.2 Definition

Let N, H be any two groups and let...

$$\Theta : H \to \mathrm{Aut}_{Grp}(N), \ h \mapsto \theta_h$$

be an arbitrary homomorphism. Define an operation $\bullet_\theta$ on the set $N \times H$ as follows: for $n_1, n_2 \in N$ and $h_1, h_2 \in H$, let...

$$(n_1, h_1) \bullet_\theta (n_2, h_2) := (n_1 \theta_{h_1}(n_1), h_1 h_2).$$

This structure is a group and is called the of N and H, denoted $N \rtimes_\Theta H$.

Proposition 5.5.2. *Let N, H be groups, and let $\Theta : H \to Aut_{Grp}(N)$ be a homomorphism; let $G = N \rtimes_\Theta H$ be the corresponding semidirect product. Then...*

- *G contains isomorphic copies of N and H*
- *the natural projection $G \to H$ is a surjective homomorphism, with kernel N; thus N is normal in G, and the sequence*

  $$1 \to N \to N \rtimes_\Theta H \to H \to 1$$

  is (split) exact;

- $N \cap H = \{e_G\}$
- $G = NH$
- *the homomorphism θ is realized by conjugation in G: that is, for $h \in H$ and $n \in N$ we have...*
$$\theta_h(n) = hnh^{-1}$$
in G.

Proposition 5.5.3. *Let N, H be subgroups of a group G, with N normal in G. Assume that $N \cap H = \{e\}$, and $G = NH$. Let $\gamma : H \to Aut_{Grp}(N)$ be defined by conjugation: for $h \in H$, $n \in N$,*

$$\gamma_h(n) = hnh^{-1}.$$

Then $G \cong N \rtimes_\gamma H$.

5.5.3 Free Product of Groups

5.5.4 Free Groups

$F(A)$ is a free group on a set A if there is a set-function $j : A \to F(A)$ such that, for all groups G and set-functions $f : A \to G$, there exists a unique group homomorphism $\varphi : F(A) \to G$ such that the following diagram commutes.

$$\begin{tikzcd} F(A) \arrow[r, "\varphi"] & G \\ A \arrow[u, "j"] \arrow[ur, "f"'] & \end{tikzcd}$$

5.5.4.1 Concrete construction

Consider the set A as an 'alphabet' and construct 'words' whose letters are elements of A or 'inverses' of elements of A. That is, a *word* on A is an ordered list
$$(a_1, a_2, \ldots, a_n)$$
, which we denote by the juxtaposition

$$w = a_1 a_2 \ldots a_n,$$

where each letter is either an element of A or an inverse of an element in A. Denote the set of words on A as $W(A)$.

Define an 'elementary' reduction $r : W(A) \to W(A)$: given $w \in W(A)$, search for the first occurrence (from left to right) of a pair aa^{-1} or $a^{-1}a$, and let $r(w)$ be the word obtained by removing such a pair.

Note that $r(w) = w$ precisely when 'no cancellation is possible'; We say that w is a 'reduced word' in this case.

Lemma 5.5.2. *If $w \in W(A)$ has length n, then $r^{\lfloor \frac{n}{2} \rfloor}(w)$ is a reduced word.*

Proof. Indeed, either $r(w) = w$ or the length of $r(w)$ is less than the length of w; but one cannot decrease the length of w more than $n/2$ times, since each non-identity application of r decreases the length by two. □

Now define the 'reduction' $R : W(A) \to W(A)$ by setting $R(w) = r^{\lfloor \frac{n}{2} \rfloor}(w)$, where n is the length of w. By the lemma, $R(w)$ is always a reduced word.

Let $F(A)$ be the set of reduced words on A, that is, the image of the reduction map R we have just defined.

Define a binary operation on $F(A)$ by juxtaposition and reduction: $w \cdot w' = R(ww')$. $F(A)$ is a group under this operation.

Proposition 5.5.4. *The pair $(j, F(A))$ satisfies the universal property for free groups on A.*

5.5.5 Quotient Group

5.5.5.1 Quotient Group by $\sim$

Proposition 5.5.5. *The operation...*

$$[a] \cdot [b] := [ab]$$

defines a group structure on $G/\sim$ if and only if $\forall a, a', g \in G$

$$a \sim a' \Rightarrow ga \sim ga' \text{ and } ag \sim a'g.$$

In this case the quotient function $\pi : G \to G/\sim$ is a homomorphism and is universal with respect to homomorphisms $\varphi : G \to G'$ such that $a \sim a' \Rightarrow \varphi(a) = \varphi(a')$.

5.5.5.2 Cosets

Proposition 5.5.6. *Let $\sim$ be an equivalence relation on a group G, satisfying $(\forall g \in G) : \ a \sim b \Rightarrow ga \sim gb$. Then...*

- *the equivalence class of e_G is a subgroup of H of G; and*
- $a \sim b \Leftrightarrow a^{-1}b \in H \Leftrightarrow aH = bH$.

Proof. Let $H \subseteq G$ be the equivalence class of the identity; $H \neq \emptyset$ as $e_G \in H$. For $a, b \in H$, we have $e_G \sim b$ and hence $b^{-1} \sim e_G$; hence $ab^{-1} \sim a$; and hence...

$$ab^{-1} \sim a \sim e_G$$

by the transitivity of $\sim$ and since $a \in H$. This shows $ab^{-1} \in H$ for all $a, b \in H$, proving that H is a subgroup.

Next, assume $a, b \in G$ and $a \sim b$. Multiplying on the left by a^{-1}, implies $e_G \sim a^{-1}b$, that is, $a^{-1}b \in H$. Since H is closed under the operation, this implies $a^{-1}bH \subseteq H$, hence $bH \subseteq aH$; as $\sim$ is symmetric, the same reasoning gives $aH \subseteq bH$; and hence $aH = bH$. Thus, we have proved...

$$a \sim b \Rightarrow a^{-1}b \in H \Rightarrow aH = bH.$$

Finally, assume $aH = bH$. Then $a = ae_G \in bH$, and hence $a^{-1}b \in H$. By definition of H, this means $e_G \sim a^{-1}b$. Multiplying on the left by a shows that $a \sim b$. $\square$

The *left-cosets* of a subgroup H in a group G are the sets aH, for $a \in G$. The *right-cosets* of H are the sets Ha, $a \in G$.

Proposition 5.5.7. *If H is any subgroup of a group G, the relation $\sim_L$ defined by*

$$(\forall a, b \in G):\ a \sim_L b \Leftrightarrow a^{-1}b \in H$$

is an equivalence relation satisfying $(\forall g \in G):\ a \sim b \Rightarrow ga \sim gb$.

Taking the previous two propositions together we get...

Proposition 5.5.8. *There is a bijection between the set of subgroups of G and equivalence relations on G satisfying $(\forall g \in G):\ a \sim b \Rightarrow ga \sim gb$; for the relation $\sim_L$ corresponding to a subgroup H, $G/\sim_L$ may be described as the set of left-cosets aH of H.*

Similar statements exist for right cosets and the property $(\forall g \in G):\ a \sim b \Rightarrow ag \sim bg$ leading to...

Proposition 5.5.9. *There is a bijection between the set of subgroups of G and equivalence relations on G satisfying $(\forall g \in G):\ a \sim b \Rightarrow ag \sim bg$; for the relation $\sim_R$ corresponding to a subgroup H, $G/\sim_R$ may be described as the set of left-cosets Ha of H.*

Proposition 5.5.10. *The relations $\sim_L$, $\sim_R$ corresponding to subgroups of H coincide if and only if H is normal.*

5.5.5.3 Definition

Let H be a normal subgroup of G. The *quotient group of G modulo H*, denoted G/H, is the group $G/\sim$ obtained from the relation $\sim$ as defined in the previous propositions. In terms of cosets, the product in G/H is defined by

$$(aH)(bH) := (ab)H.$$

The identity element is H.

5.5.5.4 Universal Property

Theorem 5.5.1. *Let H be a normal subgroup of a group G. Then for every group homomorphism $\varphi : G \to G'$ such that $H \subseteq ker\varphi$ there exists a unique group homomorphism $\tilde{\varphi} : G/H \to G'$ so that the diagram*

$$\begin{tikzcd} G \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & G' \\ & G/H \arrow[ur, "\exists!\tilde{\varphi}"'] & \end{tikzcd}$$

commutes.

5.6 Presentations

A *presentation* of a group G is an explicit isomorphism...

$$G \cong \frac{F(A)}{R}$$

where A is a set and R is a subgroup of 'relations.' In other wordsd, a presentation is an explicit surjection...

$$\varphi : F(A) \twoheadrightarrow G$$

of which R is the kernel.

To create a presentation it is enough to list 'enough' relations, i.e create a set $\mathcal{R}$ of words, and then let R be the smallest normal subgroup of $F(A)$ containing $\mathcal{R}$. We can then denote a presentation by $\langle A|\mathcal{R}\rangle$.

5.6.1 Finitely Presented

A group is *finitely presented* if it admits a presentation $\langle A|\mathcal{R}\rangle$ in which both A and $\mathcal{R}$ are finite.

5.7 Group Actions

An action of a group G on a set A is a set-function...

$$\rho : G \times A \to A$$

such that $\rho(e_G, a) = a$ for all $a \in A$ and...

$$(\forall g, h \in G), (\forall a \in A) : \rho(gh, a) = \rho(g, \rho(h, a)).$$

5.7.1 Natural Action

Every group G acts in a natural way on the underlying set G. The action $\rho : G \times G \to G$ is simply the operation in the group...

$$(\forall g, a \in G) : \rho(g, a) = ga$$

Theorem 5.7.1 (Cayley's theorem)**.** *Every group acts faithfully on some set. That is, every group may be realized as a subgroup of a permutation group.*

Proof. The natural action acts faithfully on $Aut_{Set}(G)$. $\square$

5.7.2 Transitive Actions

An action of a group G on a (nonempty) set A is *transitive* if $\forall a, b \in A, \exists g \in G$ such that $b = ga$.

5.7.3 Orbit

The *orbit* of $a \in A$ under an action of a group G is the set...

$$O_G(a) := \{ga | g \in G\}.$$

5.7.4 Stabilizer Subgroup

Let G act on a set A, and let $a \in A$. The *stabilizer subgroup* of a consists of the elements of G which fix a:

$$\mathrm{Stab}_G(a) := \{g \in G | ga = a\}.$$

5.7.5 Category G-Set

The functor category of group actions. Thus morphisms are commutative diagrams such as...

$$\begin{tikzcd} G \times A \arrow[r, "\mathrm{id}_G \times \varphi"] \arrow[d, "\rho"] & G \times A' \arrow[d, "\rho'"] \\ A \arrow[r, "\varphi"] & A' \end{tikzcd}$$

Intuitively, we think of these objects as sets endowed with a group action, i.e. *G-sets*. Arrows are morphisms (functions) such as φ above which preserve the group action. They are called *G-equivariant*.

Proposition 5.7.1. *Every transitive left-action of G on a nonempty set A is isomorphic to the left-multiplication of G on G/H, for H = the stabilizer of any $a \in A$.*

Proof. Let G act transitively on a set A, let $a \in A$ be any element, and let $H = \mathrm{Stab}_G(a)$. I claim that there is an equivariant bijection...

$$\varphi : G/H \to A$$

defined by...

$$gH \mapsto ga$$

for all $g \in G$.

First of all φ is well-defined: if $g_1H = g_2H$, then $g_1^{-1}g_2 \in H$, hence $(g_1^{-1}g_2)a = a$, and it follows that $g_1a = g_2a$ as needed. To verify that φ is bijective, define a function $\psi : A \to G/H$ by sending an element ga of A to gH; ψ is well-defined becasue if $g_1a = g_2a$, then $g^{-1}(g_2a) = a$, so $g_1^{-1}g_2 \in H$ and $g_1H = g_2H$. It is clear that φ and ψ are inverses of each other; hence φ is a bijection.

Equivariance is immediate: $\varphi(g'(gH)) = g'ga = g'\varphi(gH)$. □

Corollary 5.7.1. *If O is an orbit of the action of a finite group G on a set A, then O is a finite set and...*

$$|O| \text{ divides } |G|.$$

Proof. Use Lagrange's theorem (5.2.2) and the previous theorem. □

Proposition 5.7.2. *Suppose a group G acts on a set A, and let $a \in A$, $g \in G$, $b = ga$. Then...*

$$Stab_G(b) = gStab_G(a)g^{-1}.$$

Proof. Observe if $h \in \mathrm{Stab}_G(a)$, then...

$$(ghg^{-1})(b) = gh(g^{-1}g)a = gha = ga = b,$$

proving $\supseteq$. For $\subseteq$ note $a = g^{-1}b$ apply the same argument. □

5.7.6 Fixed Point Set

The set of *fixed points* of a group action is...

$$Z = \{a \in S | (\forall g \in G) : ga = a\}$$

Proposition 5.7.3. *Let S be a finite set, and let G be a group acting on S. Then...*

$$|S| = |Z| + \sum_{a \in A} [G : Stab_G(a)]$$

where $A \subseteq S$ has exactly one element for each nontrivial orbit of the action.

Proof. The orbits form a partition of S, and Z collects the trivial orbits; hence...

$$|S| = |Z| + \sum_{a \in A} |O_a|,$$

where O_a denotes the orbit of a. By 5.7.1, the order $|O_a|$ equals the index of the stabilizer of a, yielding the statement. □

Corollary 5.7.2. *Let G be a p-group acting on a finite set S, and let Z be the fixed point set of the action. Then...*

$$|Z| \equiv |S| \text{ mod } p.$$

5.7.7 Center

For the action $\sigma : G \to S_G$, the *center* of G, denoted $Z(G)$, is the subgroup ker σ of G.

Concretely...

$$Z(G) = \{g \in G | (\forall a \in G) : ga = ag\}.$$

Lemma 5.7.1. *Let G be a finite group, and assume $G/Z(G)$ is cyclic. Then G is commutative (and hence $G/Z(G)$ is in fact trivial).*

Proof. As $G/Z(G)$ is cyclic, there exists an element $g \in G$ such that the class $gZ(G)$ generates $G/Z(G)$. Then $\forall a \in G$...

$$aZ(G) = (gZ(G))^r$$

for some $r \in \mathbb{Z}$; that is, there is an element $z \in Z(G)$ of the center such that $a = g^r z$.

If now a, b are in G, use this fact to write...

$$a = g^r z,\ b = g^s w$$

for some $s \in \mathbb{Z}$ and $w \in Z(G)$; but then...

$$ab = (g^r z)(g^s w) = g^{r+s} zw = (g^s w)(g^r z) = ba,$$

where I have used the fact that z and w commute with every element of G. As a and b were arbitrary, this proves that G is commutative. $\square$

5.7.8 Conjugation Action

Every group G acts by conjugation on the underlying set G. The action $\rho : G \times G \to G$ is the operation in the group...

$$(\forall g, a \in G) : \rho(g, h) = ghg^{-1}$$

5.7.8.1 Centralizer and Normalizer

The *centralizer* (or *normalizer*) $Z_G(a)$ for $a \in G$ is its stabilizer under conjugation. Concretely...

$$Z_G(a) = \{g \in G | gag^{-1} = a\}.$$

The *normalizer* $N_G(A)$ of A is its stabilizer under conjugation.

The *centralizer* $Z_G(A) \subseteq N_G(A)$ fixing each element of A.

5.7.8.2 Conjugacy Class

The *conjugacy class* of $a \in G$ is the orbit $[a]$ of a under the conjugation action.

Two elements a, b of G are conjugate if they belong to the same conjugacy class.

Proposition 5.7.4 (Class Formula)**.** *Let G be a finite group. Then...*

$$|G| = |Z(G)| + \sum_{a \in A} [G : Z(a)],$$

where $A \subseteq G$ is a set containing one representative for each nontrivial conjugacy class in G.

Lemma 5.7.2. *Let $H \subseteq G$ be a subgroup. Then (if finite) the number of subgroups conjugate to H equals the index $[G : N_G(H)]$ of the normalizer of H in G.*

Corollary 5.7.3. *If $[G : H]$ is finite, then the number of subgroups conjugate to H is finite and divides $[G : H]$.*

Proof.

$$[G : H] = [G : N_G(H)] \cdot [N_G(H) : H]$$

□

5.8 Sylow Theorems

5.8.1 p-Sylow subgroups

A *p-Sylow subgroup* of a finite group G is a subgroup of order p^r, where $|G| = p^r m$ and $\gcd(p, m) = 1$. That is, $P \subseteq G$ is a p-Sylow subgroup if it is a p-group and p does not divide $[G : P]$.

5.8.2 Sylow I

Theorem 5.8.1 (First Sylow Theorem)**.** *Every finite group contains a p-Sylow subgroup, for all primes p.*

Sylow I follows from the following...

Proposition 5.8.1. *If p^k divides the order of G, then G has a subgroup of order p^k.*

Proof. If $k = 0$, there is nothing to prove, so we may assume $k \geq 1$ and in particular that $|G|$ is a multiple of p.

Argue by induction on $|G|$: if $|G| = p$, again there is nothing to prove; if $|G| > p$ and G contains a proper subgroup H such that $[G : H]$ is relatively prime to p, then p^k divides the order of H, and hence H contains a subgroup of order p^k by induction hypothesis, and thus so does G.

Therefore, we may assume that all proper subgroups of G have index divisible by p. By the class formula, p divides the order of the center $Z(G)$. By Cauchy's theorem, $\exists a \in Z(G)$ such that a has order p. The cyclic subgroup $N = \langle a \rangle$ is contained in $Z(G)$, and hence it is normal in G. Now consider the quotient G/N.

Since $|G/N| = |G|/p$ and p^k divides $|G|$ by hypothesis, we have that p^{k-1} divides the order of G/N. By the induction hypothesis, we may conclude that G/N contains a subgroup of order p^{k-1}. By the structure of the subgroups of a quotient, this subgroup must be of the form P/N, for P a subgroup of G.

But then $|P| = |P/N| \cdot |N| = p^{k-1} \cdot p = p^k$, as needed. $\square$

5.8.3 Sylow II

Theorem 5.8.2 (Second Sylow Theorem)**.** *Let G be a finite group, let P be a p-Sylow subgroup, and let $H \subseteq G$ be a p-group. Then H is contained in a conjugate of P: there exists $g \in G$ such that $H \subseteq gPg^{-1}$.*

Proof. Act with H on the set of left-cosets of P, by left-multiplication. Since there are $[G : P]$ cosets and p does not divide $[G : P]$, we know this action must have fixed points: let gP be one of them. This means that $\forall h \in H$:

$$hgP = gP;$$

that is, $g^{-1}hgP = P$ for all h in H; that is, $g^{-1}Hg \subseteq P$; that is, $H \subseteq gPg^{-1}$, as needed. $\square$

Lemma 5.8.1. *Let H be a p-group contained in a finite group G. Then...*

$$[N_g(H) : H] \equiv [G : H] \ mod\ p.$$

Proof. I H is trivial, then $N_G(H) = G$ and the two numbers are equal.

Assume then that H is nontrivial, and act with H on the set of left-cosets of H in G, by left-multiplication. The fixed points of this action are the cosets gH such that $\forall h \in H$...

$$hgH = gH,$$

that is, such that $g^{-1}hg \in H$ for all $h \in H$; in other words, $H \subseteq gHg^{-1}$, and hence $gHg^{-1} = H$. This means precisely that $g \in N_G(H)$. Therefore, the set of fixed points of the action consists of the set of cosets of H in $N_G(H)$.

The statement then follows immediately from 5.7.2. $\square$

Proposition 5.8.2. *Let H be a p-subgroup of a finite group G, and assume that H is not a p-Sylow subgroup. Then there exists a p-subgroup H' of G containing H, such that $[H' : H] = p$ and H is normal in H'.*

Proof. Since H is not a p-Sylow subgroup of G, p divides $[N_G(H) : H]$, by the previous lemma. Since H is normal in $N_G(H)$, we may consider the quotient group $N_G(H)/H$, and p divides the order of this group. By 5.2.1, $N_G(H)/H$ has an element of order p; this generates a subgroup of order p of $N_G(H)/H$, which must be of the form H'/H for a subgroup H' of $N_G(H)$.

It is straightforward to verify that H' satisfies the stated requirements. $\square$

5.8.4 Sylow III

Theorem 5.8.3 (Third Sylow Theorem)**.** *Let p be a prime integer, and let G be a finite group of order $|G| = p^r m$. Assume that p does not divide m. Then the number of p-Sylow subgroups N_p satisfies...*

- $N_p|m$;
- $N_p \equiv 1$ *mod* p.

Proof. Let N_p denote the number of p-Sylow subgroups of G.

By 5.8.2, the p-Sylow subgroups of G are the conjugates of any given p-Sylow subgroup P. By 5.7.2, N_p is the index of the normalizer $N_G(P)$ of P; thus by 5.7.3 it divides the index m of P. In fact,

$$m = [G : P] = [G : N_G(P)] \cdot [N_G(P) : P] = N_p \cdot [N_G(P) : P].$$

Now, by 5.8.1 we have...

$$m = [G : P] \equiv [N_G(P) : P] \bmod p;$$

multiplying by N_p, we get...

$$mN_p \equiv m \bmod p.$$

Since $m \not\equiv 0 \bmod p$ and p is prime, this implies...

$$N_p \equiv 1 \bmod p,$$

as needed. □

5.9 Simple Groups

A group G is *simple* if it is nontrivial and its only normal subgroups are $\{e\}$ and G itself.

Proposition 5.9.1. *Let G be a group of order mp^r, where p is a prime integer and $1 < m < p$. Then G is not simple.*

Proof. By the third Sylow theorem, the number N_p of p-Sylow subgroups divides m and is of the form $1 + kp$. Since $m < p$, this forces $k = 0$, $N_p = 1$. Therefore G has a normal subgroup of order p^r; hence it is not simple. □

5.10 Series of Gropus

5.10.1 Series of Subgroups

A *series* of subgroups G_i of a group G is a decreasing sequence of subgroups starting from G:

$$G = G_0 \supset G_1 \supset G_2 \cdots$$

The *length* of a series is the number of strict inclusions.

5.10.2 Normal Series

A series of subgroups for which G_{i+1} is normal in G_i for all i.

5.10.2.1 Maximal Length

The *maximal length* of a normal series G can be denoted $l(G)$ (if finite). Then number $l(G)$ is a measure of how far G is from being simple; $l(G) = 1$ if and only if G is simple.

5.10.3 Composition Series

A *composition series* for G is a normal series...

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$$

such that the successive quotients G_i/G_{i+1} are simple.

Theorem 5.10.1 (Jordan-Hölder Theorem)**.** *Let G be a group, and let...*

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\},$$

$$G = G'_0 \supset G'_1 \supset G'_2 \supset \cdots \supset G'_m = \{e\}$$

be two composition series for G. Then $m = n$, and the lists of quotient groups $H_i = G_i/G_{i+1}$, $H'_i = G'_i/G'_{i+1}$ agree (up to isomorphism) after a permutation of the indices.

Proof. Let...

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$$

be a composition series. Argue by induction on n: if $n = 0$, then G is trivial, and there is nothing to prove. Assume $n > 0$, and let...

$$G = G'_0 \supset G'_1 \supset G'_2 \supset \cdots \supset G'_m = \{e\}$$

be another composition series for G. If $G_1 = G'_1$, then the result follows from the induction hypothesis, since G_1 has a composition series of length $n-1 < n$.

We may then assume $G_1 \neq G'_1$. Note that $G_1G'_1 = G$: indeed, $G_1G'_1$ is normal in G, and $G_1 \subset G_1G'_1$; but there are no proper normal subgroups between G_1 and G since G/G_1 is simple.

Let $K = G_1 \cap G'_1$. The distinct subgroups $G_i \cap K$ determine a composition series...

$$K \supset K_1 \supset K_2 \supset \cdots \supset K_r = \{e\}$$

of K (verified in the next proof). By the second isomorphism theorem,

$$\frac{G_1}{K} = \frac{G_1}{G_1 \cap G'_1} \cong \frac{G_1G'_1}{G_1} = \frac{G}{G'_1} \text{ and } \frac{G'_1}{K} \cong \frac{G}{G_1}$$

are simple. Therefore, we hve two new composition series for G: which only differ at the first step. These two series trivially have the same length and the same quotients.

Now I claim that the first of these two seires has the same length and quotients as the first series. Indeed,

$$G_1 \supset K \supset K_1 \supset K_2 \supset \cdots \supset K_r = \{e\}$$

is a composition series for G_1: by the induction hypothesis, it must have the same length and quotients as the composition series...

$$G_1 \supset G_2 \supset \cdots \supset G_n = \{e\};$$

verifying the claim.

By the same token, applying the induction hypothesis to the series...

$$G'_1 \supset K \supset K_1 \supset K_2 \cdots \supset K_{n-2} = \{e\},$$

shows that the second series has the same length and quotients as the second series, and the statement follows. □

Proposition 5.10.1. *Let G be a group, and let N be a normal subgroup of G. Then G has a composition series if and only if both N and G/N have composition series. Further, if this is the case, then...*

$$l(G) = l(N) + l(G/N),$$

and the composition factors of G consist of the collection of composition factors of N and of G/N.

Proof. If G/N has a composition series, the subgroups appearing in it correspond to subgroups of G containing N, with isomorphic quotients, by the third isomorphism theorem. Thus, if both G/N and N have composition series, juxstaposing them produces a composition series for G, with the stated consequence on composition factors.

The converse is a little trickier. Assume that G has a composition series...

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$$

and that N is a normal subgroup of G. Intesecting the series with N give a sequence of subgroups of G. Intersecting the series with N gives a sequence of subgroups of the latter:

$$N = G \cap N \supseteq G_1 \cap N \supseteq \cdots \supseteq \{e\} \cap N = \{e\}$$

such that $G_{i+1} \cap N$ is normal in $G_i \cap N$, for all i. I claim that this becomes a composition series for N once repetitions are eliminated. Indeed, this follows once we establish that...

$$\frac{G_i \cap N}{G_{i+1} \cap N}$$

is either trivial (so that $G_{i+1} \cap N = G_i \cap N$, and the corresponding inclusion may be ommitted) or isomorphic to $\frac{G_i}{G_{i+1}}$ (hence simple, and one of the composition factors of G). To see this, consider the homomorphism...

$$G_i \cap N \hookrightarrow G_i \twoheadrightarrow \frac{G_i}{G_{i+1}} :$$

the kernel is clearly $G_{i+1} \cap N$; therefore (by the first isomorphism theorem) we have an injective homomorphism...

$$\frac{G_i \cap N}{G_{i+1} \cap N} \hookrightarrow \frac{G_i}{G_{i+1}}$$

identifying $(G_i \cap N)/(G_{i+1} \cap N)$ with a subgroup of G_i/G_{i+1}. Now, this subgroup is *normal* (because N is normal in G) and G_i/G_{i+1} is simple, our claim follows.

As for G/N, obtain a sequence of subgroups from a composition series for G:

$$\frac{G}{N} \supseteq \frac{G_1 N}{N} \supseteq \frac{G_2 N}{N} \supseteq \cdots \frac{\{e_G\}N}{N} = \{e_{G/N}\},$$

such that $(G_{i+1}N)/N$ is normal in $(G_i N)/N$. As above, we have to check that...

$$\frac{(G_i N)/N}{(G_{i+1}N)/N}$$

is either trivial or isomorphic to G_i/G_{i+1}. By the third isomorphism theorem, this quotient is isomorphic to $(G_i N)/(G_{i+1}N)$. This time, consider the homomorphism...

$$G_i \hookrightarrow G_i N \twoheadrightarrow \frac{G_i N}{G_{i+1} N} :$$

this is *surjective*, and the subgroup G_{i+1} of the source is sent to the identity element in the target; hence there is an onto homomorphism

$$\frac{G_i}{G_{i+1}} \twoheadrightarrow \frac{G_i N}{G_{i+1} N}$$

Since G_i/G_{i+1} is simple, it follows that $(G_i N)/(G_{i+1}N)$ is either trivial or isomorphic to it, as needed.

Summarizing, we have shown that if G has a composition series and N is normal in G, then both N and G/N have composition series. The first part of the argument yields the statement on lengths and composition factors, concluding the proof. $\square$

5.10.4 Refinement of a Series

Proposition 5.10.2. *Any two normal series of a finite group ending with $\{e\}$ admit equivalent refinements.*

Proof. Refine the series to a composition series; then apply the Jordan-Hölder theorem. $\square$

5.10.5 Derived Series

Let G be a group. The *derived* series of G is the sequence of subgroups...

$$G \supseteq [G, G] = H \supseteq [H, H] = J \supseteq [J, J] \supseteq \cdots$$

5.10.6 Solvable

A group is *solvable* if its derived series terminate with the identity.

Proposition 5.10.3. *For a finite group G, the following are equivalent...*

1. *All composition factors of G are cyclic.*

2. *G admits a cyclic series ending in $\{e\}$.*

3. *G admits an abelian series ending in $\{e\}$.*

4. *G is solvable.*

Proof. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) are trivial.

(3) $\Rightarrow$ (1) Refine the abelian series to a composition series (simple abelian groups are cyclic p-groups).

(4) $\Rightarrow$ (3) The derived series is abelian, by 5.4.3.

(3) $\Rightarrow$ (4) Let...

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$$

be an abelian series. Then $G^{(i)} \subseteq G_i$ for all i, where $G^{(i)}$ denotes the i-th 'iterated' commutator subgroup.

This can be verified by induction. For $i = 1$, G/G_1 is commutative; thus $[G, G] \subseteq G_1$, by the 5.4.3. Assuming we know $G^{(i)} \subseteq G_i$, the fact that G_i/G_{i+1} is abelian implies $[G_i, G_i] \subseteq G_{i+1}$, and hence...

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \subseteq [G_i, G_i] \subseteq G_{i+1},$$

as claimed.

In particular we obtained that $G^{(n)} \subseteq G_n = \{e\}$: that is, the derived series terminates at $\{e\}$, as needed. □

Corollary 5.10.1. *Let N be a normal subgroup of a group G. Then G is solvable if and only if both N and G/N are solvable.*

Proof. This follows immediately from 5.10.1 and the formulation of solvability in terms of composition factors given in the previous proposition. □

6 Abelian Group Theory

6.1 Definition

An *abelian group* is a group such that $\cdot$ (which we denote $+$ for general abelian groups) is commutative.

In this context we write:

- $ng = g + g \cdots g + g$ (n times)
- $-ng = -g - g \cdots - g - g$ (n times)

6.2 Homomorphisms of Abelian Groups

Proposition 6.2.1. *For any two abelian groups G, H, $Hom_{Ab}(G, H)$ is an abelian group under addition inherited from H.*

Proof. Define the operation $\varphi + \psi$ for $\varphi, \psi \in \mathrm{Hom}_{Ab}(G, H)$, where...

$$(\varphi + \psi)(g) = \varphi(g) +_H \psi(g).$$

Observe that $\varphi + \psi$ is a homomorphism...

$$\begin{aligned}(\varphi + \psi)(a +_G b) = \varphi(a +_G b) + \psi(a +_G b) &= (\varphi(a) +_H \varphi(b)) +_H (\psi(a) +_H \psi(b)) \\ &\overset{!}{=} (\varphi(a) +_H \psi(a)) +_H (\varphi(b) +_H \psi(b)) = (\varphi + \psi)(a) +_H (\varphi + \psi)(b)\end{aligned}$$

From here it is easy to show that $\mathrm{Hom}_{Ab}(G, H)$ is an abelian group. □

Note: By the same logic, if A is a set and H an abelian group, then H^A is an abelian group.

In fact, by adding the additional operation $\circ$ (treated as multiplication), we transform $\mathrm{End}_{Ab}(G) := \mathrm{Hom}_{Ab}(G, G)$ into a ring.

Proposition 6.2.2. *$End_{Ab}(\mathbb{Z}) \cong \mathbb{Z}$ as rings.*

Proof. Consider the function...

$$\varphi : \mathrm{End}_{Ab}(\mathbb{Z}) \to \mathbb{Z}$$

defined by...

$$\varphi(\alpha) = \alpha(1)$$

for all group homomorphisms $\alpha : \mathbb{Z} \to \mathbb{Z}$. Then φ is a group homomorphism: the addition in $\mathrm{End}_{Ab}(\mathbb{Z})$ is defined so that $\forall n \in \mathbb{Z}$...

$$(\alpha + \beta)(n) = \alpha(n) + \beta(n);$$

in particular...

$$\varphi(\alpha + \beta) = (\alpha + \beta)(1) = \alpha(1) + \beta(1) = \varphi(\alpha) + \varphi(\beta).$$

Further, φ is a ring homomophism. Indeed, for $\alpha, \beta \in \mathrm{End}_{Ab}(\mathbb{Z})$ denote $\alpha(1)$ by a; then...

$$\alpha(n) = n\alpha(1) = na = an$$

for all $n \in \mathbb{Z}$; in particular,

$$\alpha(\beta(1)) = a\beta(1) = \alpha(1)\beta(1).$$

Therefore,

$$\varphi(\alpha \circ \beta) = (\alpha \circ \beta)(1) = \alpha(\beta(1)) = \alpha(1)\beta(1) = \varphi(\alpha)\varphi(\beta)$$

as needed. Also, $\varphi(\mathrm{id}_{\mathbb{Z}}) = id_{\mathbb{Z}}(1) = 1$.

Finally, φ has an inverse: for $a \in \mathbb{Z}$, the $\psi(a)$ be the homomorphism $\alpha : \mathbb{Z} \to \mathbb{Z}$ defined by...

$$(\forall n \in \mathbb{Z}) : \ \alpha_a(n) = an.$$

This inverse is a ring homomorphism...

- $\psi(a + b) = \alpha_{a+b} = \alpha_a + \alpha_b = \psi(a) + \psi(b)$;
- $\psi(a \cdot b) = \alpha_{a \cdot b} = \alpha_a \circ \alpha_b = \psi(a) \circ \psi(b)$;
- $\psi(1) = \alpha_1 = \mathrm{id}_{\mathbb{Z}}$.

□

Proposition 6.2.3. *Let R be a ring. Then the function $r \mapsto \lambda_r$ is an injective ring homomorphism...*

$$\lambda : R \to End_{Ab}(R).$$

Proof. For any $r \in R$ and for all $a, b \in R$, distributivity gives...

$$\lambda_r(a + b) = r(a + b) = ra + rb = \lambda_r(a) + \lambda_r(b) :$$

this shows that λ_r is indeed an endomorphism of the *group* $\langle R, + \rangle$, that is, $\lambda_r \in \mathrm{End}_{Ab}(R)$.

The function $\lambda : R \to \mathrm{End}_{Ab}(R)$ defined by the assignment $r \mapsto \lambda_r$ is clearly injective, since $r \neq s$, then...

$$\lambda_r(1) = r \neq s = \lambda_s(1),$$

so that $\lambda_r \neq \lambda_s$.

Now we show that λ is a homomorphism. Additive preservation follows from 6.2.1 and distributivity. Associativity can be used to show that multiplication is preserved. The identity is clearly preserved. □

6.3 Abelian Subgroups

Every subgroup of an abelian group is normal.

6.3.1 Cokernel of a Homomorphism

The *cokernel* of $\varphi : G \to G'$, cokerφ, is $\frac{G'}{\text{im}\varphi}$.

Proposition 6.3.1. *Let $\varphi : G \to G'$ be a homomorphism. Then the projection $\pi : G' \twoheadrightarrow coker\varphi$ is final in the category of group homomorphisms $\alpha : G' \to L$ such that $\alpha \circ \varphi$ is the trivial morphism. In other words the following diagram commutes.*

$$\begin{tikzcd}
G \arrow[r, "\varphi"'] \arrow[rr, bend left, "0"] & G' \arrow[r, "\alpha"'] \arrow[d, two heads, "\pi"'] & L \\
& \text{coker}\varphi \arrow[ur, "\exists!\overline{\alpha}"'] &
\end{tikzcd}$$

6.4 Abelian Group Constructions

6.4.1 Free Abelian Groups

Proposition 6.4.1. *For every set A, $F^{ab}(A) \cong \mathbb{Z}^{\oplus A}$.*

Proof. Note that every element of $\mathbb{Z}^{\oplus A}$ may be written uniquely as a finite sum...

$$\sum_{a\in A} m_a j(a), \quad m_a \neq 0 \text{ for only finitely many } a.$$

Now let $f : A \to G$ be any function from A to the abelian group G. Define $\varphi : \mathbb{Z}^{\oplus A} \to G$ by...

$$\varphi(\sum_{a\in A} m_a j(a)) := \sum_{a\in A} m_a f(a).$$

This definition is force by the homomorphism condition and the univeral property of free groups and is thus unique.

It is also a homomorphism...

$$\varphi(\sum_{a\in A} m'_a j(a)) + \varphi(\sum_{a\in A} m''_a j(a)) = \sum_{a\in A} m'_a j(a) + \sum_{a\in A} m''_a j(a) \stackrel{!}{=} \sum_{a\in A}(m'_a + m''_a) f(a)$$

because G is commutative,

$$= \varphi(\sum_{a\in A}(m'_a + m''_a) j(a)) = \varphi(\sum_{a\in A} m'_a f(a) + \sum_{a\in A} m''_a f(a))$$

as needed. $\square$

Note: $H^{\oplus A}$ is a subgroup of H^A.

6.5 Classification of Finite Abelian Groups

Lemma 6.5.1. *Let G be an abelian group, and let H, K be subgroups such that $|H|$, $|K|$ are relatively prime. Then $H + K \cong H \oplus K$.*

Proof. By Lagrange's theorem, $H \cap K = \{0\}$. Since subgroups of abelian groups are automatically normal, the statement follows from 5.5.1. $\square$

Corollary 6.5.1. *Every finite abelian group is the direct sum of its nontrivial Sylow subgroups.*

Lemma 6.5.2. *Let p be a prime integer and $r \geq 1$. Let G be a noncyclic abelian group of order p^{r+1}, and let $g \in G$ be an element of order p^r. Then there exists an element $h \in G$, $h \notin \langle g \rangle$, such that $|h| = p$.*

Proof. Denote $\langle g \rangle$ by K, and let h' be any element of G, $h' \notin K$. The subgroup K is normal in G since G is abelian; the quotient group G/K has order p. Since $h' \notin K$, the coset $h' + K$ has order p in G/K; that is, $ph' \in K$. Let $k = ph'$.

Note that $|k|$ divides p^r; hence it is a power of p. Also $|k| \neq p^r$, otherwise $|h'| = p^{r+1}$ and G would be cyclic, contrary to the hypothesis.

Therefore $|k| = p^s$ for some $s < r$; k generates a subgroup $\langle k \rangle$ of the cyclic group K, or order p^s. By 7.3.5, $\langle k \rangle = \langle p^{r-s} r \rangle$. Since $s < r$, $\langle k \rangle \subseteq \langle pg \rangle$; thus, $k = mpg$ for some $m \in \mathbb{Z}$.

Then let $h = h' - mg$: $h \neq 0$ (since $h' \notin K$), and...

$$ph = ph' - p(mg) - k - k = 0,$$

showing that $|h| = p$, as stated. $\square$

Lemma 6.5.3. *Let G be an abelian p-group, let $g \in G$ be an element of maximal order. Then the exact sequence...*

$$0 \to \langle g \rangle \to G \to G/\langle g \rangle \to 0$$

splits.

Proof. Argue by induction on the order of G; the case $|G| = p^0 = 1$ requires no proof. Thus we will assume that G is nontrivial and that the statement is true for every p-group smaller that G.

Let $g \in G$ be an element of maximal order, say p^r, and denote by K the subgroup $\langle g \rangle$ generated by g; this subgroup is normal, as G is abelian. If $G = K$, then the statement holds trivially. If not, G/K is a nontrivial p-group, and hence it contains an element of order p by Cauchy's theorem. This element generates a subgroup of order p in G/K, corresponding to a subgroup G' of G of order p^{r+1}, containing K. This subgroup is not cyclic (otherwise the order of g is not maximal).

That is, we are in the situation of 5.4.2: hence we can conclude that there is an element $h \in G'$ (and hence $h \in G$) with $h \notin K$ and $|h| = p$. Let $H = \langle h \rangle \subseteq G$ be the subgroup generated by h, and note that $K \cap H = \{0\}$.

Now work modulo H. The quotient group G/H has smaller size that G, and $g + H$ generates a cyclic subgroup $K' = (K + H)/H \cong K/(K \cap H) \cong K$ of maxiaml order in G/H. By the induction hypothesis, there is a subgroup L' of G/H such that $K' + L' = G/H$ and $K' \cap L' = \{0_{G/H}\}$. This subgroup L' corresponds to a subgroup L of G containing H.

Now: (i) $K + L = G$ and (ii) $K \cap L = \{0\}$. Indeed, we have the following: (i) For any $a \in G$, there exist $mg + H \in K'$, $l + H \in L'$ such that $a + H = mg + l + H$ (since $K' + L' = G/H$). This implies $a - mg \in L$, and hence $a \in K + L$ as needed. (ii) If $a \in K \cap L$, then $a + H \in K' \cap L' = \{0_{G/H}\}$, and hence $a \in H$. In particular, $a \in K \cap H = \{0\}$, forcing $a = 0$, as needed.

(i) and (ii) imply the lemma, as observed in the comments following the statement. □

Corollary 6.5.2. *Let G be a finite abelian group. Then G is a direct sum of cyclic groups, which may be assumed to be cyclic p-groups.*

Proof. As noted in 6.5.1, G is a direct sum of p-groups (as a consequence of the Sylow theorems). I claim that every abelian p-group P is a direct sum of cyclic p-groups.

To establish this, argue by induction on $[P]$. There is nothing to prove if P is trivial. If P is not trivial, let g be an element of P of maximal order. By the previous lemma

$$P = \langle g \rangle \oplus P'$$

for some subgroup P' of P; by the induction hypothesis P' is a direct sum of cyclic p-groups, concluding the proof. □

Restated more precisely (and more famously) we have. . .

Theorem 6.5.1 (Classification of Finite Abelian Groups)**.** *Let G be a finite nontrivial abelian group. Then. . .*

- *there exist prime integers $p_1, \dots, p_r$ and positive integers n_{ij} such that $|G| = \prod_{i,j} p_i^{n_{ij}}$ and. . .*
$$G \cong \bigoplus_{i,j} \frac{\mathbb{Z}}{p_i^{n_{ij}}\mathbb{Z}}$$
- *there exist positive integers $1 < d_1 | \cdots | d_s$ such that $|G| = d_1 \dots d_s$ and*
$$G \cong \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_s\mathbb{Z}}.$$

Further, these decompositions are uniquely determined by G.

7 Group Examples

7.1 Trivial Group

$G = \{e\}$.

7.2 p-groups

7.2.1 Definition

A *p-group* is a finite group whose order is a power of a prime integer p.

Corollary 7.2.1. *Let G be a nontrivial p-group. Then G has a nontrivial center. (See: 5.7.4)*

7.3 Cyclic Groups

7.3.1 Modular Arithmetic

Let $n \in \mathbb{Z}^+$. Consider the equivalence relation on $\mathbb{Z}$ defined by...

$$a \equiv b \text{ mod } n \Leftrightarrow n|(b-a) \Leftrightarrow b - a \in n\mathbb{Z}.$$

It is called *congruence modulo n*.

7.3.2 Definition

Let $\mathbb{Z}/n\mathbb{Z} = \{[z]_{\text{mod } n} | z \in \mathbb{Z}\}$.

Lemma 7.3.1. *Addition ($[a]_n + [b]_n := [a+b]_n$) is well defined on $\mathbb{Z}/n\mathbb{Z}$.*

Thus $C_n := \langle \mathbb{Z}/n\mathbb{Z}, + \rangle$ is a *finite cyclic group*. We take $\langle \mathbb{Z}, + \rangle$ to be the *infinite cyclic group*.

Proposition 7.3.1. *The order of $[m]_n$ in $\mathbb{Z}/n\mathbb{Z}$ is 1 if $n|m$, and more generally...*

$$|[m]_n| = \frac{n}{gcd(m,n)}.$$

Proof. If $n|m$, then $[m]_n = [0]_n$. If $n \nmid m$, $[m]_n = m[1]_n$ and apply 5.2.1. $\square$

Corollary 7.3.1. *The class $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $gcd(m,n) = 1$.*

The *cyclic groups* are an isomorphism class. Explicitly...

A group G is *cyclic* if it is isomorphic to $\mathbb{Z}$ or C_n
for some positive interger n.

Proposition 7.3.2. *If $|G| = p$ is a prime integer, then necessarily $G \cong \mathbb{Z}/p\mathbb{Z}$.*

Proof. Use Lagrange's theorem (5.2.3). $\square$

Proposition 7.3.3. *Assume $p < q$ are prime integers and $q \not{e}quiv1]$ mod p. Let G be a group of order pq. Then G is cyclic.*

Proof. By the third Sylow theorem, G has a uique (hence normal) subgroup H of order p. Indeed, the number N_p of p-Sylow subgroups must divide q, and q is prime, so $N_p = 1$ or q. Necessarily $N_p \equiv 1 \bmod p$, and $q \not\equiv 1 \bmod p$ by hypothesis; therefore $N_p = 1$.

Since H is normal, conjugation gives an action of G on H, hence a homomorphism $\gamma : G \to \mathrm{Aut}(H)$. Now H is cyclic of order p, so $|\mathrm{Aut}(H)| = p - 1$; the order of $\gamma(G)$ must divide both pq and $p - 1$, and it follows that γ is the trivial map.

Therefore, conjugation is trivial on H: that is, $H \subseteq Z(G)$. By 5.7.1, G is abelian.

Finally, an abelian group of order pq, with $p < q$ primes, is necessarily cyclic: indeed it must contain elements g, h of order p, q, respectively, and then $|gh| = pq$. □

7.3.3 Presentation

We say that a group is *cyclic* when it is generated by exactly one of its elements.
Finite: $\langle x | x^n \rangle$

Infinite: $\langle x \rangle$

7.3.4 Subgroups

Proposition 7.3.4. *Let $G \subseteq \mathbb{Z}$ be a subgroup. Then $G = d\mathbb{Z}$ for some $d \geq 0$.*

Proof. If $G = \{0\}$, then $G = 0\mathbb{Z}$. If not, note that if $a \in G$ and $a < 0$, then $-a \in G$ and $-a > 0$. We can then let d be the *smallest positive integer* in G and $G = d\mathbb{Z}$.

The inclusion $d\mathbb{Z} \subseteq G$ is clear. To verify $G \subseteq d\mathbb{Z}$, let $m \in G$, and apply 'division with remainder' to write...

$$m = dq + r,$$

with $0 \leq r < d$. Since $m \in G$ and $d\mathbb{Z} \subseteq G$ and since G is a subgroup, we see that...

$$r = m - dq \in G.$$

But d is the smallest *positive* integer in G, and $r \in G$ is smaller that d; so r cannot be positive. This shows $r = 0$, that is, $m = qd \in d\mathbb{Z}$; $G \subseteq d\mathbb{Z}$ follows. □

Proposition 7.3.5. *Let $n > 0$ be an integer and let $G \subseteq \mathbb{Z}/n\mathbb{Z}$. Then G is the cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ generate by $[d]_n$, for some divisor d of n.*

Proof. Let $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the quotient map, and consider $G' := \pi_n^{-1}(G)$. By 5.4.2, G' is a subgroup of $\mathbb{Z}/n\mathbb{Z}$; by 7.3.4, G' is a *cyclic* subgroup of $\mathbb{Z}$, generated by a nonnegative integer d. It follows that…

$$G = \pi_n(G') = \pi_n(\langle d \rangle) = \langle [d]_n \rangle$$

; thus G is indeed a cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$, generated by a class $[d]_n$. Further, since $n \in G'$ (because $\pi_n(n) = [n]_n = [0]_n \in G$) and $G' = d\mathbb{Z}$, we see that d divides n, as claimed. □

7.4 Multiplicative group of integers modulo n

7.4.1 Definition

Let $(\mathbb{Z}/n\mathbb{Z})^* := \{[m]_n \in \mathbb{Z}/n\mathbb{Z} | \gcd(m, n) = 1\}$.

Lemma 7.4.1. *Multiplication ($[a]_n \cdot [b]_n := [a \cdot b]_n$) is well defined on $\mathbb{Z}/n\mathbb{Z}$.*

Proposition 7.4.1. *Multiplication makes $(\mathbb{Z}/n\mathbb{Z})^*$ into a group.*

7.4.2 Applications

Theorem 7.4.1 (Fermat's Little Theorem)**.** *Let p be a prime integer, and let a be any integer. Then $a^p \equiv a \bmod p$.*

Proof. This is immediate if $p|a$. If $p \nmid a$, then $a \in (\mathbb{Z}/n\mathbb{Z})^*$, which has order $p-1$. Thus…

$$[a]_p^{p-1} = [1]_p$$

via Lagrange's theorem (5.2.3). □

7.5 Symmetric Group

7.5.1 Definition

Let A be a set. The *symmetric group*, or *group of permutations* of A, denoted S_A, is the group $Aut_{Set}(A)$. The group of permutations of the set $[n]$ is denoted by S_n.

7.5.2 Cycle

A (nontrivial) *cycle* is an element of S_n with exactly one nontrivial orbit. For distinct $a_1, \ldots, a_r$ in $\{1, \ldots, n\}$, the notation…

$$(a_1 a_2 \ldots a_r)$$

denotes the cycle in S_n with nontrivial orbit $\{a_1, \ldots, a_r\}$, acting as…

$$a_1 \mapsto a_2 \mapsto \cdots \mapsto a_r \mapsto a_1.$$

In this case, r is the *length* of the cycle. A cycle of length r is called an r-cycle.

7.5.2.1 Disjoint Cycles

Two cycles are *disjoint* if their nontrivial orbits are. The following lemma depends on this definition.

Lemma 7.5.1. *Disjoint cycles commute.*

Lemma 7.5.2. *Every $\sigma \in S_n$, $\sigma \neq e$, can be written as a product of disjoint nontrivial cycles, in a unique way up to permutations of the factors.*

Proof. As we have seen, every $\sigma \in S_n$ determines a partition of $\{1, \ldots, n\}$ into orbits under the action of $\langle\sigma\rangle$. If $\sigma \neq e$, then $\langle\sigma\rangle$ has nontrivial orbits. As σ acts as a cycle on each orbit, it follows that σ may be written as a product of cycles.

Uniqueness is an exercise. □

7.5.3 Type

The *type* of $\sigma \in S_n$ is the partition of n given by the sizes of the orbits of the action of $\langle\sigma\rangle$ on $\{1, \ldots, n\}$.

See integer partitions and Ferrer's diagrams.

Lemma 7.5.3. *Let $\tau \in S_n$, and let $(a_1, \ldots, a_r)$ be a cycle. Then...*

$$\tau(a_1 \ldots a_r)\tau^{-1} = (a_1\tau^{-1} \ldots a_r\tau^{-1})$$

where $a_i\tau^{-1} = \tau^{-1}(a_i)$.

Proof. This is verified by checking that both sides act in the same way on $\{1, \ldots, n\}$. For example, for $1 \leq i \leq r$...

$$(a_i\tau^{-1})(\tau(a_1 \ldots a_r)\tau^{-1}) = a_i(a_1 \ldots a_r)\tau^{-1} = a_{i+1}\tau^{-1}$$

as it should; the other cases are similar. □

Proposition 7.5.1. *Two elements of S_n are conjugate in S_n if and only if they have the same type.*

Proof. The 'only if' part of this statement follows immediately from...

$$\tau(a_1 \ldots a_r) \cdots (b_1 \cdots b_s)\tau^{-1} = (a_1\tau^{-1} \cdots a_r\tau^{-1}) \ldots (b_1\tau^{-1} \ldots b_s\tau^{-1}).$$

Conjugating a permutation yields a permutation of the same type.

As for the 'if' part, suppose...

$$\sigma_1 = (a_1 \ldots a_r)(b_1 \ldots b_s) \cdot (c_1 \ldots c_t)$$

and

$$\sigma_2 = (a'_1 \ldots a'_r)(b'_1 \ldots b'_s) \cdot (c'_1 \ldots c'_t)$$

are two permutations with the same type, written in cycle notation, with $r \geq s \geq \cdots \geq t$. Let τ be any permutation such that $a_i = a'_i\tau$, $b_j = b'_j\tau, \ldots, c_k = c'_k\tau$ for all $i, j, \ldots, k$. Then the previous lemma implies $\sigma_2 = \tau\sigma_1\tau^{-1}$, so σ_1 and σ_2 are conjugate, as needed. □

Corollary 7.5.1. *The number of conjugacy classes in S_n equals the number of partitions of n.*

7.6 Alternating Group

Let...

$$\Delta_n = \prod_{i \leq i < j \leq n} (x_i - x_j) \in \mathbb{Z}[x_1, \ldots, x_n].$$

7.6.1 Sign of a permutation

The *sign* of a permutation $\sigma \in S_n$, denoted $(-1)^\sigma$, is determined by the action of σ on Δ_n:

$$\Delta_n \sigma = (-1)^\sigma \Delta_n.$$

We say that a permutation is *even* if if its sign is $+1$ and *odd* if its sign is -1.

7.6.2 Transposition

A *transposition* is a cycle of length 2.

Lemma 7.6.1. *Transpositions generate S_n.*

Proof. Indeed, by 7.5.2 it suffices to show that every *cycle* is a product of transpositions, and indeed...

$$(a_1 \ldots a_r) = (a_1 a_2)(a_1 a_3) \cdots (a_1 a_r),$$

as may be checked by applying both sides to every element of $\{1, \ldots, n\}$. □

Lemma 7.6.2. *Let $\sigma = \tau_1 \cdots \tau_r$ be a product of transpositions. Then σ is even, resp. odd, according to whether r is even, resp., odd.*

Proof. This follows immediately from the facts that ε is a homomorphism and the sign of a transposition is -1: indeed, (ij) acts on Δ_n by permuting its factors and changing the sign of an odd number of factors (for $i < j$, the factor $(x_i - x_j)$ and the pairs of factors $(x_i - x_k)$, $(x_k - x_j)$ for all $i < k < j$). □

7.6.3 Definition

The *alternating group* on $\{1, \ldots, n\}$, denoted A_n, consists of all even permutations $\sigma \in S_n$.

The alternating group is a *normal* subgroup of S_n, and...

$$[S_n : A_n] = 2$$

for $n \geq 2$.

7.6.4 Conjugacy

Lemma 7.6.3. *Let $n \geq 2$, and let $\sigma \in A_n$. Then $[\sigma]_{A_n} = [\sigma]_{S_n}$ or size of $[\sigma]_{A_n}$ is half the size of $[\sigma]_{S_n}$, according to whether the centralizer $Z_{S_n}(\sigma)$ is not or is contained in A_n.*

Proof. Not that...

$$Z_{A_n}(\sigma) = A_n \cap Z_{S_n}(\sigma) :$$

this follows immediately from the definition of centralizer. Now recall that the centralizer of σ is its stabilizer under conjugation, and therefore the size of the conjugacy class of σ equals the index of its centralizer.

If $Z_{S_n}(\sigma) \subseteq A_n$, then $Z_{A_n}(\sigma) = Z_{S_n}(\sigma)$, so that...

$$[S_n : Z_{S_n}(\sigma)] = [S_n : Z_{A_n}(\sigma)] = [S_n : A_n][A_n : Z_{A_n}(\sigma)] = 2 \cdot [A_n : Z_{A_n}(\sigma)];$$

therfore, $[\sigma]_{A_n}$ is half the size of $[\sigma]_{S_n}$ in this case.

If $Z_{S_n} \not\subseteq A_n$, then note that $A_n Z_{S_n}(\sigma) = S_n$: indeed, $A_n Z_{S_n}(\sigma)$ is a subgroup of S_n, and it properly contains A_n, so it must equal S_n as A_n has index 2 in S_n. By index considerations...

$$[A_n : Z_{A_n}(\sigma)] = [A_n : A_n \cap Z_{S_n}(\sigma)] = [A_n Z_{S_n}(\sigma) : Z_{S_n}(\sigma)] = [S_n : Z_{S_n}(\sigma)],$$

so the classes have the same size. Since $[\sigma]_{A_n} \subseteq [\sigma]_{S_n}$ in any case, it follows that $[\sigma]_{A_n} = [\sigma]_{S_n}$, completing the proof. $\square$

Proposition 7.6.1. *Let $\sigma \in A_n$, $n \geq 2$. Then the conjugacy class σ in S_n splits into two conjugacy classes in A_n precisely if the type of σ consists of distinct odd numbers.*

Proof. By the previous lemma, we have to verify that $Z_{S_n}(\sigma)$ is contained in A_n precisely when the stated condition is satisfied; that is, we have to show that...

$$\sigma = \tau\sigma\tau^{-1} \Rightarrow \tau \text{ is even}$$

precisely when the type of σ consists of distinct odd numbers.

Write σ in cycle notation (including cycles of length 1):

$$\sigma = (a_1 \dots a_\lambda)(b_1 \dots b_\mu) \cdots (c_1 \dots c_\nu),$$

and recall that...

$$\tau\sigma\tau^{-1} = (a_1\tau^{-1} \dots a_\lambda\tau^{-1})(b_1\tau^{-1} \dots b_\mu\tau^{-1}) \cdots (c_1\tau^{-1} \dots c_\nu\tau^{-1}).$$

Assume that $\lambda, \mu, \dots, \nu$ are odd and distinct. If $\tau\sigma\tau^{-1} = \sigma$, then conjugation by τ must preserve each cycle in σ, as all cycle lengths are distinct:

$$\tau(a_1 \dots a_\lambda)\tau^{-1} = (a_1 \dots a_\lambda), \text{ etc.}$$

that is,

$$(a_1\tau^{-1} \dots a_\lambda\tau^{-1}) = (a_1 \dots a_\lambda), \text{ etc.}$$

This means that τ acts as a cyclic permutation on (e.g.) $a_1, \dots, a_\lambda$ and therefore in the same way as a power of $(a_1 \dots a_\lambda)$. It follows that...

$$\tau = (a_1 \dots a_\lambda)^r (b_1 \dots b_\mu)^s \dots (c_1 \dots c_\nu)^t$$

for suitable $r, s, \dots, t$. Since all cycles have odd lengths, each cycle is an even permutation; and τ must then be even as it is a product of evne permutations. This proves that $Z_{S_n}(\sigma) \subseteq A_n$ if the stated condition holds.

Conversely, assume that the stated condition does not hold: that is, either some of the cycles in the cycle decomposition have even length or all have odd length but two of the cycles have the same length.

In the first case, let τ be an even-length cycle in the cycle decomposition of σ. Note that $\tau\sigma\tau^{-1} = \sigma$: indeed, τ commutes with itself and with all cycles in σ other than τ. Since τ has even length, then it is odd as permutation: this shows that $Z_{S_n}(\sigma)\ \not{s}ubseteqA_n$, as needed.

In the second case, without loss of generality assume $\lambda = \mu$, and consider the odd permutation...

$$\tau = (a_1 b_1)(a_2 b_2) \cdots (a_\lambda b_\lambda) :$$

conjugating by τ simply interchanges the first two cycles in σ; hence $\tau\sigma\tau^{-1} = \sigma$. As τ is odd, this again shows that $Z_{S_n}(\sigma) \nsubseteq A_n$, and we are done. □

7.6.5 Simplicity

Corollary 7.6.1. *The alternating group A_5 is a simple noncommutative group of order* 60*.*

Proof. A normal subgroup of A_5 is necessarily the union of conjugacy classes, contains the identity, and has order equal to a divisor of 60. The divisors of 60 other than 1 and 60 are...

$$2, 3, 4, 5, 6, 10, 12, 15, 20, 30;$$

counting the elements other than the identity would give one of...

$$1, 2, 3, 4, 5, 9, 11, 14, 19, 29$$

as a sum of numbers $\neq 1$ from the class formula for A_5. But the simply does not happen.

□

Lemma 7.6.4. *The alternating group A_n is generated by* 3*-cycles.*

Proof. Since every even permutation is a product of an even number 2-cycles, it suffices to show that every product of two 2-cycles may be written as product of 3-cycles. Therefore, consider a product...

$$(ab)(cd)$$

with $a \neq b$, $c \neq d$. If $(ab) = (cd)$, then this product is the identity, and their is nothing to prove. If $\{a, b\}, \{c, d\}$ have exactly one element in common, then we may assume $c = a$ and observe...

$$(ab)(ab) = (abd).$$

It $\{a, b\}, \{c, b\}$ are disjoint, then...

$$(ab)(cd) = (abc)(adc),$$

and we are done. □

Proposition 7.6.2. *Let $n \geq 5$. If a normal subgroup of A_n contains a 3-cycle, then it contains all 3-cycles.*

Proof. Normal subgroups are unions of conjugacy classes, so we just need to verify that 3-cycles form a conjugacy class in A_n, for $N \geq 5$. But they do in S_n, and the type of a 3-cycle is $[3, 1, 1, \dots]$ for $n \geq 5$; hence the conjugacy class does not split in A_n, by 7.6.1. □

Theorem 7.6.1. *The alternating group A_n is simple for $n \geq 5$.*

Proof. We have already checked this for $n = 5$ and $n = 6$. For $n > 6$, let N be a nontrivial normal subgroup of A_n; we will show that necessarily $N = A_n$, by proving that N contains 3-cycles.

Let $\tau \in N$, $\tau \neq (1)$, and let $\sigma \in A_n$ be a 3-cycle. Since the center of A_n is trivial and 3-cycles generate A_n, we may assume that τ and σ do not commute, that is, the commutator...

$$[\tau, \sigma] = \tau(\sigma\tau^{-1}\sigma^{-1}) = (\tau\sigma^{-1})\sigma^{-1}$$

is not the identity. This element is in N and is a product of two 3-cycles.

Therefore, replaceing τ by $[\tau, \sigma]$ if necessary, we may assume that $\tau \in N$ is a nonindentity permutation acting on ≤ 6 elements: that is, on a subset of a set $T \subseteq \{1, \dots, n\}$ with $|T| = 6$. Now we may view A_6 as a subgroup of A_n, by letting it act on T. The subgroup $N \cap A_6$ of A_g is then normal (because N is normal) and nontrivial (because $\tau \in N \cap A_6$ and $\tau \neq (1)$). Since A_6 is simple, this implies $N \cap A_6 = A_6$. In particular, N contains 3-cycles.

By 7.6.2, this implies that N contains *all* 3-cycles. By , it follows that $N = A_n$, as needed. □

7.6.6 Solvability

Corollary 7.6.2. *For $n \geq 5$, the group S_n is not solvable.*

Proof. Since A_n is simple, the sequence...

$$S_n \supset A_n \supset \{(1)\}$$

is a composition series for S_n. It follows that the composition factors of S_n are $\mathbb{Z}/2\mathbb{Z}$ and A_n. By 5.10.3, S_n is not solvable. □

7.7 Dihedral Group

7.7.1 Definition

Intuitively, this group captures the rigid motions (flips and rotations) of regular polygons in the 2D plane. It is denoted D_{2n}, where n is the number of sides/angles of the polygon, and contains $2n$ elements, n rotations and n flips.

7.7.2 Presentation

$\langle x, y | x^2, y^n, xyxy \rangle$

Proposition 7.7.1. *Let q be an odd prime, and let G be a noncommutative group of order $2q$. Then $G \cong D_{2q}$.*

Proof. By Cauchy's theorem, $\exists y \in G$ such that y has order q. By the third Sylow theorem, $\langle y \rangle$ is the unique subgroup of order q in G (and is therefore normal). Since G is not commutative and in particular it is not cyclic, it has no elements of order $2q$; therefore, every element in the complement of $\langle y \rangle$ has order 2; let x be any such element.

The conjugate xyx^{-1} of y by x is an element of order q, so $xyx^{-1} \in \langle y \rangle$. Thus, $xyx^{-1} = y^r$ for some r between 0 and $q-1$.

Now observe that...

$$(y^r)^r = (xyx^{-1})^r = xy^r x^{-1} = x^2 y (x^{-1})^2 = y$$

since $|x| = 2$. Therefore, $y^{r^2-1} = e$, which implies...

$$q | (r^2 - 1) = (r-1)(r+1)$$

by 5.2.1. Since q is prime, this says that $q|(r-1)$ or $q|(r+1)$; since $0 \le r \le q-1$, it follows that $r = 1$ or $r = q-1$.

If $r = 1$, then $xyx^{-1} = y$; that is, $xy = yx$. But then the order of xy is $2q$, and G is cyclic, a contradiction.

Therefore $r = q-1$, and we have established the relations...

$$\begin{cases} x^2 = e, \\ y^q = e, \\ yx = xy^{q-1}. \end{cases}$$

□

These are the relations satisfied by generators x, y of D_{2q}; the statement follows.

7.8 General Linear Group

7.8.1 Definition

The nth general linear group over the ring R, denoted $\mathrm{GL}_n(R)$ is the group of units in $\mathcal{M}_n(R)$, that is, the group of invertible $n \times n$ matrices with entries in R.

8 Ring Theory

8.1 Definitions

A *ring* $\langle R, +, \cdot \rangle$ is an abelian group $\langle R, + \rangle$ endowed with a *second* binary operation $\cdot$, satisfying on its onw the requirements of being associative and having a two-sided identity, i.e.

- $(\forall r, s, t \in R): \quad (r \cdot t) \cdot t = r \cdot (s \cdot t)$
- $(\exists 1_R \in R)(\forall r \in R): \quad r \cdot 1_R = r = 1_R \cdot r$

which make $\langle R, \cdot \rangle$ a *monoid*, and further interacting with $+$ via the following *distributive properties*:

$$(\forall r, s, t \in R): \quad (r + s) \cdot t = r \cdot t + s \cdot t \text{ and } t \cdot (r + s) = t \cdot r + t \cdot s.$$

Lemma 8.1.1. *In a ring R,*

$$0 \cdot r = r = r \cdot 0$$

and

$$r + (-1) \cdot r = 0$$

for all $r \in R$.

Proof. Observe...

$$r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0 \Rightarrow 0 = r \cdot 0$$

and...

$$r + (-1) \cdot r = (1) \cdot r + (-1) \cdot r = (1 - 1) \cdot r = 0 \cdot r = 0$$

□

8.1.1 Divisor

Let $a, b \in R$. We say a *divides* b, denoted $a|b$, if $b \in (a)$, that is...

$$\exists c \in R \, , b = ac.$$

8.1.1.1 Associates

Two elements $a, b \in R$ are *associtates* if $(a) = (b)$, that is, $a|b$ and $b|a$.

8.1.2 Commutative Rings

A ring R is *commutative* if $(\forall r, s \in R): \; r \cdot s = s \cdot r$.

8.1.3 Subrings

A *subring* S of a ring R is a ring whose underlying set is a subset of R and such that the inclusion function $S \hookrightarrow R$ is a ring homomorphism.

8.1.4 Characteristic

Let R be a ring and consider the unique ring homomorphism $\phi : \mathbb{Z} \to R$. Then $\ker\phi = n\mathbb{Z}$ for some n. The *characteristic* of R is this nonnegative integer n.

8.2 Ideals

Let R be a ring. A subgroup I of $\langle R, + \rangle$ is a *left-ideal* of R if $rI \subseteq I$ for all $r \in R$; that is,

$$(\forall r \in R)(\forall a \in I) : \ ra \in I;$$

it is a *right-ideal* if $Ir \subseteq I$ for all $r \in R$; that is,

$$(\forall r \in R)(\forall a \in I) : \ ar \in I.$$

A *two-sided ideal* is a subgroup I which is both a left- and a right-ideal.

Some important features to keep in mind about ideals are...

- If $\{I_\alpha\}_{\alpha \in A}$ is a collection of ideals of a ring R. Then the intersection $\bigcap_{\alpha \in A}(I_\alpha)$ is an ideal of R; the largest ideal contained in all of the ideals I_α.
- If I, J are ideals of R, then IJ denotes the ideal *generated* by all products ij with $i \in I, j \in J$. More generally, if $I_1, \dots, I_n$ are ideals in R, then the 'product' $I_1 \cdots I_n$ denotes the ideal generated by all products $i_1 \cdots i_n$ with $i_k \in I_k$.

8.2.1 Principal Ideals

Let $a \in R$ be any element of a ring. Then the subset $I = Ra$ of R is a left-ideal of R and aR is a right-ideal.

If R is commutative, then we write (a) for the ideal. It is called the *principal ideal* generated by a.

Some important features to keep in mind about principal ideals are...

- $(a_\alpha)_{\alpha \in A} := \sum_{\alpha \in A}(a_\alpha)$ the ideal *generated by the elements* a_α
- $(R/(a))/(\bar{b}) \cong R/(a, b)$ where $(\bar{b})$ is the class of $b \in R/(a)$

8.2.2 Finitely Generated

An ideal I of a commutative ring R is *finitely generated* if $I = (a_1, \dots, a_n)$ for some $a_1, \dots, a_n \in R$.

8.2.3 Prime Ideals

Let $I \neq (1)$ be an ideal of a commutative ring R. I is a *prime ideal* if R/I is an integral domain.

Proposition 8.2.1. *Let $I \neq (1)$ be an ideal of a commutative ring R. Then I is prime if and only if for all $a, b \in R$...*

$$ab \in I \Rightarrow (a \in I \text{ or } b \in I).$$

Proof. The ring R/I is an integral domain if and only if $\forall \overline{a}, \overline{b} \in R/I$...

$$\overline{a} \cdot \overline{b} \Rightarrow (\overline{a} = 0 \text{ or } \overline{b} = 0).$$

This condition translates immediately to the given condition in R. □

8.2.4 Maximal Ideals

Let $I \neq (1)$ be an ideal of a commutative ring R. I is a *maximal ideal* if R/I is a field.

Proposition 8.2.2. *Let $I \neq (1)$ be an ideal of a commutative ring R. Then I is maximal if and only if for all ideals J or R...*

$$I \subseteq J \Rightarrow (I = J \text{ or } J = R).$$

Proof. As for maximality, the given condition follows from the correspondence between ideals of R/I and ideals of R containing I and the observation that a commutative ring is a field if and only if its ideals are (0) and (1). □

Existence of maximal ideals is equivalent to the axiom of choice, so we are justified in proving the following with Zorn's Lemma.

Proposition 8.2.3. *Let $I \neq (1)$ be a proper ideal of a commutative ring R. Then there exists a maximal ideal m of R containing I.*

8.2.5 Chinese Remainder Theorem

Lemma 8.2.1. *Let $I_1, \ldots, I_k$ be ideals of R such that $I_i + I_k = (1)$ for all $i = 1, \ldots, k-1$. Then $(I_1 \ldots I_k - 1) + I_k = (1)$.*

Lemma 8.2.2. *Let $I_1, \ldots, I_k$ be ideals of R such that $I_i + I_j = (1)$ for all $i \neq j$. Then $I_1 \cdots I_k = I_1 \cap \cdots \cap I_k$.*

Theorem 8.2.1. *Let $I_1, \ldots, I_k$ be ideals of R such that $I_i + I_j = (1)$ for all $i \neq j$. Then the natural homomorphism...*

$$\varphi : R \to \frac{R}{I_1} \times \cdots \times \frac{R}{I_k}$$

is surjective and induces an isomorphism...

$$\tilde{\varphi} : \frac{R}{I_1 \cdots I_k} \xrightarrow{\sim} \frac{R}{I_1} \times \cdots \times \frac{R}{I_k}.$$

Proof. Argue by induction on k. By the former two lemmas we only need to show that the natural homomorphism...

$$R \to \frac{R}{I_1 \cdots I_{k-1}} \times \frac{R}{I_k}$$

is surjective. By Lemma 6.2, $(I_1 \dots I_{k-1}) + I_k = (1)$; thus we are reduced to the case of two ideals.

Let then I, J be ideals of a commutative ring R, such that $I + J = (1)$, and let $r_I, r_J \in R$; we have to verify that $\exists r \in R$ such that $r \equiv r_I \bmod I$ and $r \equiv r_J \bmod J$. Since $I + J = (1)$, there are $a \in I$, $b \in J$ such that $a + b = 1$. Let $r = ar_J + br_I$: then...

$$r = ar_J + (1-a)r_I = r_I + a(r_J - r_I) \equiv r_I \bmod I$$

as $a \in I$, and...

$$r = (1-b)r_J + br_I = r_J + b(r_I - r_J) \equiv r_J \bmod J$$

as $b \in J$, as needed, and completing the proof. □

8.3 Ring Homomorphisms

A *ring homomorphism* is a function $\varphi : R \to S$ if it preserves both ring operations and the identity element. That is...

- $(\forall a, b \in R) : \varphi(a+b) = \varphi(a) + \varphi(b)$
- $(\forall a, b \in R) : \varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi(1_R) = 1_S$.

8.4 Ring Constructions

8.4.1 Products

If R_1, R_2 are rings, then the product ring $R_1 \times R_2$ may be defінted by endowing the direct product of groups $R_1 \times R_2$ with componentwise multiplication.

8.4.2 Quotients

Let R be a ring and $I \subseteq R$ be an ideal. The quotient group R/I is compatible with ring structure (determined by the natural projection) and is called the *quotient ring* of R *modulo* I.

Theorem 8.4.1. *Let I be a two-sided ideal of a ring R. Then for every ring homomorphism $\varphi : R \to S$ such that $I \subseteq ker\varphi$ there exists a unique ring homomorphism $\tilde{\varphi} : R/I \to S$ so that the diagram...*

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & S \\ & R/I \arrow[ur, "\exists!\tilde{\varphi}"'] & \end{tikzcd}$$

commutes.

8.5 Integral Domains

8.5.1 Zero-divisors

An element a in a ring R is a *left-zero-divisor* if there exist elements $b \neq 0$ in R for which $ab = 0$.

Proposition 8.5.1. *In a ring R, $a \in R$ is not a left- (resp., right-) zero-divisor if and only if left (resp., right) multiplication by a is an injective function $R \to R$.*

Proof. ($\Rightarrow$) Assume a is not a left-zero-divisor and $ab = ac$ for $b, c \in R$. Then, by distributivity,

$$a(b - c) = ab - ac = 0,$$

and this implies $b - c = 0$ since a is not a left-zero-divisor; that is, $b = c$.

($\Leftarrow$) If a is a left-zero-divisor, then $\exists b \neq 0$ such that $ab = 0 = a \cdot 0$; this shows that left-multiplication is not injective in this case. $\square$

8.5.2 Definition

An *integral domain* is a nonzero commutative ring R (with 1) such that...

$$(\forall a, b \in R): \quad ab = 0 \Rightarrow a = 0 \text{ or } b = 0.$$

Proposition 8.5.2. *Assume R is a finite commutative ring; then R is an integral domain if and only if it is a field.*

Proof. ($\Rightarrow$) If $a \in R$ is a non-zero-divisor, then multiplication by a in R is injective by 8.5.1; hence it is surjective, as the ring is finite, by the pigeonhole principle; hence a is a unit via 8.10.1.

($\Leftarrow$) This direction is obvious. $\square$

Corollary 8.5.1. *Let I be an ideal of a commutative ring R. If R/I is finite, then I is prime if and only if it is maximal.*

8.5.3 Associates in Integral Domains

Lemma 8.5.1. *Let a, b be nonzero elements of an integral domain R. Then a and b are associates if and only if $a = ub$, for u a unit in R.*

8.5.4 Prime Element

An element $a \in R$ of an integral domain is *prime* if (a) is prime; that is, a is not a unit and...

$$a|bc \Rightarrow (a|b \text{ or } a|c).$$

8.5.5 Irreducible Element

An element $a \in R$ of an integral domain is *irreducible* if a is not a unit and...

$$a = bc \Rightarrow (b \text{ is a unit or } c \text{ is a unit}).$$

Lemma 8.5.2. *Let R be an integral domain, and let $a \in R$ be a nonzero prime element. Then a is irreducible.*

8.5.6 Factorization

An element $r \in R$ of an integral domain has a *factorization into irreducibles* if there exist irreducible elements $q_1, \dots, q_n$ such that $r = q_1 \cdots q_n$.

8.5.7 Domain with factorization

An integral domain R is a *domain with factorization* if every nonzero, nonunit element $r \in R$ has a factorization into irreducibles.

Proposition 8.5.3 (Ascending Chain Condition)**.** *Let R be an integral domain, and let r be a nonzero, nonunit element of R. Assume that every ascending chain of principal ideals...*

$$(r) \subseteq (r_1) \subseteq (r_2) \subseteq (r_1) \subseteq \cdots$$

stabilizes. Then r has a factorization into irreducibles.

8.5.8 Greatest Common Divisor

Let R be an integral domain, and let $a, b \in R$. An element $d \in R$ is a *greatest common divisor* (often abbreviated 'gcd') of a and b if $(a, b) \subseteq (d)$ and (d) is the smallest principal ideal in R with this property.

8.5.9 Field of Fractions

See the construction of rational numbers. The contruction is entirely analogous, but with a general ring instead of $\mathbb{Z}$.

We can also define the *field of fractions* with category theory. Consider a category such that...

- objects are pairs (i, K), where K is a field and $i : R \hookrightarrow K$ is an injective ring homomorphism.

- morphisms $(i, K) \to (j, L)$ are determined by a homomorphism of fields $\alpha : K \to L$

Then the *field of fractions* $K(R)$ of R is an initial object of this category.

8.6 Noetherian Rings

A commutative ring R is *Noetherian* if every ideal of R is finitely generated.

Proposition 8.6.1. *Let R be a commutative ring, and let M be an R-module. Then the following are equivalent:*

1. *M is Noetherian, that is, every submodule of M is finitely generated*
2. *Every ascending chain of submodules of M stabilizes*
3. *Every nonempty family of submodules of M has a maximal elemnt with respect to inclusion.*

Lemma 8.6.1 (Hilbert's Basis Theorem)**.** *R Noetherian $\Rightarrow$ $R[x]$ Noetherian.*

Proof. Assume R is Noetherian, and let I be and ideal of $R[x]$. We have to prove that I is finitely generated.

Consider the following subset of R:

$$A = \{0\} \cup \{a \in R | a \text{ is a leading coefficient of an element of } I\}.$$

It is clear that A is an *ideal* of R; since R is Noetherian, A is finitely generated. Thus there exist elements $f_1(x), \dots, f_r(x) \in I$ whose leading coefficients $a_1, \dots, a_r$ generate A as an ideal of R.

Now let d_0 be the degree of $f_d(x)$, and let d be the maximum among these degrees. Consider the sub-R module...

$$M = \langle 1, x, x^2, \dots, x^{d-1} \rangle \subseteq R[x],$$

that is, the R-module consisting of polynomials of degree $< d$. Since M is finitely generated as a module over R, it is Noetherian as an R-module (10.4.1). Therefore, this submodule...

$$M \cap I$$

of M is finitely generated over R, say by $g_1(x), \dots, g_s(x) \in I$.

Observe that...

$$I = \{f_1(x), \dots, f_r(x), g_1(x), \dots, g_s(x)\}$$

by the following: let $\alpha(x) \in I$ be an arbitrary polynomial. If $\deg\alpha(x) \geq d$, let a be the leading coefficient of $\alpha(x)$. Then $a \in A$, so $\exists b_1, \dots, b_r \in R$ such that...

$$a = b_1 a_1 + \cdots + b_r a_r.$$

Letting $e = \deg\alpha(x)$, so that $e \geq d_i$ for all i, this says that...

$$\alpha(x) - b_1 x^{e-d_1} f_1(x) - \cdots - b_r x^{e-d_r} f_r(x)$$

has degree $< e$. Iterating this procedure, we obtain a finite list of polynomials $\beta_1(x), \ldots, \beta_r(x) \in R[x]$ such that...

$$\alpha(x) - \beta_1(x) f_1(x) - \cdots - \beta_r(x) f_r(x)$$

has degree $< d$. But this places this element in $M \cap I$; therefore $\exists c_1, \ldots, c_s \in R$ such that...

$$\alpha(x) - \beta_1(x) f_1(x) - \cdots - \beta_r(x) f_r(x) = c_1 g_1(x) + \cdots + c_s g_s(x),$$

and we are done, since this verifies that... $\alpha(x) = \beta_1(x) f_1(x) + \cdots + \beta_r(x) f_r(x) + c_1 g_1(x) + \cdots + c_s g_s(x) \in (f_1(x), \cdots, f_r(x), g_1(x), \cdots, g_s(x))$, completing the proof. $\square$

The following theorem is a consequence with little effort.

Theorem 8.6.1. *Let R be a Noetherian ring, and let J be an ideal of the polynomial ring $R[x_1, \ldots, x_n]$. Then the ring $R[x_1, \ldots, x_n]/J$ is Noetherian.*

8.6.1 Factorization in Noetherian domains

The following is corrolary of the ascending chaing condition (8.5.3)...

Proposition 8.6.2. *Let R a Noetherian domain. Then factorizations exist in R.*

8.7 Unique Factorization Domains

8.7.1 Definition

An integral domain R is a *unique factorization domain* if every nonzero, nonunit element $r \in R$ has a unique factorization into irreducibles.

Lemma 8.7.1. *Let R be a UFD, and let a, b, c be nonzero elements of R. Then...*

- *$(a) \subseteq (b) \Leftrightarrow$ the multiset of irreducible factors of b is contained in the multiset of irreducible factors of a;*
- *a and b are associates (that is, $(a) = (b)$) $\Leftrightarrow$ the two multisets coincide;*
- *the irreducible factors of a product bc are the collection of all irreducible factors of b and of c.*

Lemma 8.7.2. *Let R be a UFD, and let a, b be nonzero elements of R. Then a, b have a greatest common divisor.*

Lemma 8.7.3. *Let R be a UFD, and let a be an irreducible element of R. Then a is prime.*

Theorem 8.7.1. *An integral domain R is a UFD if and only if…*

- *the a.c.c for principal ideals holds in R and*
- *every irreducible element of R is prime.*

8.8 Principal Ideal Domains

An integral domain R is a *PID* if every ideal of R is principal.

Proposition 8.8.1. *$\mathbb{Z}$ is a PID.*

Proof. Let $I \subseteq \mathbb{Z}$ be an ideal. Since I is a subgroup, $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$, by 7.3.4. Since $n\mathbb{Z} = (n)$, this shows that I is principal. □

Proposition 8.8.2. *Let R be a PID, and let I be a nonzero ideal in R. Then I is prime if and only if it is maximal.*

Proof. Maximal ideals are prime in every ring, so we only need to verify that nonzero prime ideals are maximal in a PID; we will use the characterization of prime and maximal ideals obtained in 8.2.1 and 8.2.2. Let $I = (a)$ be a prime ideal in R, with $a \neq 0$, and assume $I \subseteq J$ for an ideal of R. As R is a PID, $J = (b)$ for some $b \in R$. Since $I = (a) \subseteq (b) = J$, we have that $a = bc$ for some $c \in R$. But then $b \in (a)$ or $c \in (a)$, since $I = (a)$ is prime.

If $b \in (a)$, then $(b) \subseteq (a)$; and $I = J$ follows. If $c \in (a)$, then $c = da$ for some $d \in R$. But then…

$$a = bc = bda,$$

from which $bd = 1$ since cancellation by the nonzero a holds in R (since R is an integral domain). This implies that b is a unit, and hence $J = (b) = R$.

That is, we have shown that if $I \subseteq J$, then either $I = J$ or $J = R$; thus I is maximal, by 8.2.2. □

8.8.1 Factorization

Proposition 8.8.3. *If R is a PID, then it is a UFD.*

8.9 Euclidean Domains

8.9.1 Euclidean Valuation

A *Euclidean valuation* of an integral domain R is a function $v : R \setminus \{0\} \to \mathbb{Z}^{\geq 0}$ satisfying the following property: for all $a \in R$ and all nonzero $b \in R$ there exist $q, r \in R$ such that…

$$a = qb + r,$$

with either $r = 0$ or $v(r) < v(b)$.

8.9.2 Definition

An integral domain R is a *Euclidean domain* if it admits a Euclidean valuation.

Proposition 8.9.1. *Let R be a Euclidean domain. Then R is a PID.*

8.9.3 Euclidean Algorithm

Lemma 8.9.1. *Let $a = bq + r$ in a ring R. Then $(a, b) = (b, r)$.*

Corollary 8.9.1. *Assume $a = bq + r$. Then a, b have a gcd if and only if b, r have a gcd, and in this case $gcd(a, b) = gcd(b, r)$.*

Proposition 8.9.2. *Given two elements $a, b \in R$, with $b \neq 0$, we can apply division with remainder repeatedly:*

$$a = bq_1 + r_1,$$

$$b = r_1 q_2 + r_2,$$

$$r_1 = r_2 q_3 + r_3,$$

$$\dots$$

as long as the remainder r_i is nonzero.

In a Euclidean domain this process terminates.

Proposition 8.9.3. *The final remainder in the process above, r_{N-1}, is a gcd of a, b.*

8.10 Division Rings

8.10.1 Units

An element u of a ring R is a *left-unit* if $\exists v \in R$ such that $uv = 1$; it is a *right-unit* if $\exists v \in R$ such that $vu = 1$. *Units* are two sided units.

Proposition 8.10.1. *In a ring R:*

- *u is a left- (resp., right-) unit if and only if left- (resp., right-) multiplication by u is a surjective function $R \to R$*
- *if u is a left- (resp., right-) unit, then right- (resp., left-) multiplication by u is injective; that is, u is not a right- (resp., left-) zero-divisor;*
- *the inverse of a two-sided unit is unique;*
- *two-sided units form a group under multiplication.*

8.10.2 Definition

A *division ring* is a ring in which every nonzero element is a two-sided unit.

8.11 Polynomial Rings

8.11.1 Polynomials

Let R be a ring. A *polynomial* $f(x)$ in the *indeterminate* x and with *coefficients* in R is a finite linear combination of nonnegative 'powers' of x with coefficients in R:

$$f(x) = \sum_{i \geq 0} a_i x^i = a_0 + a_q x + a_2 x^2 + \cdots ,$$

where all a_i are elements of R and we require $a_i = 0$ for $i \gg 0$.

Two polynomials are taken to be equal if...

$$\sum_{i \geq 0} a_i x^i = \sum_{i \geq 0} b_i x^i \Leftrightarrow (\forall i \geq 0) : \quad a_i = b_i.$$

NOTE: a polynomial *actually is* an element of the infinite direct sum of the group $\langle R, + \rangle$.

Operations on polynomials are defined as follows: if...

$$f(x) = \sum_{i \geq 0} a_i x^i \text{ and } g(x) = \sum_{i \geq 0} b_i x^i$$

then...

$$f(x) + f(x) := \sum_{i \geq 0} (a_i + b_i) x^i$$

and...

$$f(x) \cdot f(x) := \sum_{k \geq 0} \sum_{i+j=k} a_i b_i x^{i+j}.$$

8.11.1.1 Monic

A *monic* polynomial is a polynomial...

$$f(x) = x^d + a_{d-1]} x^{d-1} + \cdots + a_1 x + a_0$$

where the leading coefficient is 1.

Lemma 8.11.1. *Let $f(x)$ be a monic polynomial, and assume...*

$$f(x) q_1(x) + r_1(x) = f(x) q_2(x) + r_2(x)$$

with both $r_1(x)$ and $r_2(x)$ polynomials of degree $<$ deg$f(x)$. Then $q_1(x) = q_2(x)$ and $r_1(x) = r_2(x)$.

Proof. Indeed, we have...

$$f(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x);$$

if $r_2(x) \neq r_1(x)$, then $r_2(x) - r_1(x)$ has degree $<$ deg$f(x)$, while $f(x)(q_1(x) - q_2(x))$ has degree $\geq f(x)$, giving a contradiction. Therefore $r_1(x) = r_2(x)$, and $q_1(x) = q_2(x)$ follows right away since monic polynomials are non-zero-divisors. ☐

8.11.2 Universal Property

Let $\mathcal{R}_A$ be the category of commutative rings under a set A so that...

- Objects: (j, R) such that $j : A \to R$
- Arrows: $(j_1, R_1) \to (j_2, R_2)$ representing...

$$\begin{tikzcd} A \arrow[d, "j_1"] \arrow[dr, "j_2'"] & \\ R_1 \arrow[r, "\varphi"] & R_2 \end{tikzcd}$$

Proposition 8.11.1. *$(i, \mathbb{Z}[x_1, \cdots, x_n])$ is initial in $\mathcal{R}_A$.*

Proof. Let (j, R) be an arbitrary object of $\mathbb{R}_A$; we have to show that there is a unique morphism $(i, \mathbb{Z}[x_1, \cdots, x_n]) \to (j, R)$.

The key point is that the requirements posed on φ force its definition. The postulated commutativity of the diagram means that $\varphi(x_k) = j(a_k)$ for $k = 1, \cdots, n$. Then, since φ must be a ring homomorphism, necessarily...

$$\begin{aligned} \varphi(\sum m_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n}) &= \sum \varphi(m_{i_1 \dots i_n}) \varphi(x_1)^{i_1} \cdots \varphi(x_n)^{i_n} \\ &= \sum \iota(m_{i_1 \dots i_n}) j(x_1)^{i_1} \cdots j(x_n)^{i_n}, \end{aligned}$$

where $\iota : \mathbb{Z} \to R$ is the unique ring homomorphism (as $\mathbb{Z}$ is initial in Ring).

Thus, if φ exists, then it is unique. On the other hand, the formula we just obtained clearly preserves the operations and sends 1 to 1, so it does define a ring homomorphism, concluding the proof. $\square$

8.11.2.1 Evaluation Map and Polynomial Functions

Let $\alpha : R \to S$ be a fixed ring homomorphism, and $s \in S$ be an element commuting with $\alpha(r)$ for all $r \in R$. Then there is a unique ring homomorphism $\overline{\alpha} : R[x] \to S$ extending α and sending x to s.

This we get an '*evaluation map*' over commutative rings...

$$f(x) = \sum_{i \geq 0} a_i x^i \text{ and } r \in R \Rightarrow f(r) = \sum_{i \geq 0} a_i r^i \in R.$$

This may be viewed as $\overline{\alpha}(f(x))$, where $\overline{\alpha}$ is obtained with $id_R : R \to R$ and $s = r$.

Thus, every polynomial $f(x)$ determines a *polynomial function* $f : R \to R$ defined by $r \mapsto f(r)$.

8.11.3 Quotients of Polynomial Rings

Assume that R is a commutative ring. Via 8.11.1, if $f(x)$ is monic, then for every $g(x) \in R[x]$ there exists a unique polynomial $r(x)$ of degree $< \deg f(x)$ and such that...

$$g(x) + (f(x)) = r(x) + (f(x))$$

as cosets of the principal ideal $(f(x))$ in $R[x]$.

Proposition 8.11.2. *Let R be a commutative ring, and let $f(x) \in R[x]$ be a monic polynomial of degree d. Then the function...*

$$\varphi : R[x] \to R^{\oplus d}$$

defined by sending $g(x) \in R[x]$ to the remainder of the division of $g(x)$ by $f(x)$ induces an isomorphism of abelian groups...

$$\frac{R[x]}{(f(x))} \cong R^{\oplus d}$$

Proof. The given function φ is well-defined by 8.11.1, and it is surjective since it has a right inverse...

$$\psi((r_0, r_1, \dots, r_{d-1})) = r_0 + r_1 x + \cdots + r_{d-1} x^{d-1}.$$

The function φ is a homomorphism of abelian groups. Indeed, if...

$$g_1(x) = f(x)q_1(x) + r_1(x) \text{ and } g_2 = f(x)q_2(x) + r_2(x)$$

with deg $r_1(x) < d$, deg $r_2(x) < d$, then...

$$g_1(x) + g_2(x) = f(x)(q_1(x) + q_2(x)) + (r_1(x) + r_2(x))$$

and deg $(r_1(x) + r_2(x)) < d$: this implies via 8.11.1...

$$\varphi(g_1(x) + g_2(x)) = r_1(x) + r_2(x) = \varphi(g_1(x)) + \varphi(g_2(x)).$$

By the first isomorphism theorem for abelian groups, then, φ induces an isomorphism...

$$\frac{R[x]}{\ker\varphi} \cong R^{\oplus d}.$$

On the other hand, $\varphi(g(x)) = 0$ if and only if $g(x) = f(x)q(x)$ for some $q(x) \in R[x]$, that is, if and only if $g(x)$ is in the principal ideal generated by $f(x)$. This shows $\ker\varphi = (f(x))$, concluding the proof. □

8.11.4 Ideals in Polynomial Rings

Lemma 8.11.2. *Let R be a ring, and let I be an ideal of R. Then...*

$$\frac{R[x]}{IR[x]} \cong \frac{R}{I}[x].$$

Corollary 8.11.1. *If I is a prime ideal of R, then $IR[x]$ is prime in $R[x]$.*

8.11.5 Primitivity

Let $f \in R[x]$ be a polynomial. Then...

- f is *very primitive* if for all prime ideals p of R, $f \notin pR[x]$.
- f is *primitive* if for all principal prime ideals p of R, $f \notin pR[x]$.

Lemma 8.11.3. *Let R be a commutative ring. Then for $f, g \in R[x]$...*

$$fg \text{ is primitive} \Leftrightarrow \text{ both } f \text{ and } g \text{ are primitive.}$$

Lemma 8.11.4. *Let R be a commutative ring and $f = a_0 + a_1x + \cdots + a_dx^d \in R[x]$.*

- *f is very primitive if and only if $(a_0, \ldots, a_d) = (1)$.*
- *If R is a UFD, then f is primitive if and only if $gcd(a_0, \ldots, a_d) = 1$.*

8.11.6 Content

Let R be a UFD. The *content* of a nonzero polynomial $f \in R[x]$, denoted cont_f, is the gcd of its coefficients.

Lemma 8.11.5. *Let R be a UFD, and let $f \in R[x]$. Then...*

- *$(f) = (cont_f)(\underline{f})$, where $\underline{f}$ is primitive;*
- *if $(f) = (c)(g)$, with $c \in R$ and g is primitive, then $(c) = (cont_f)$.*

Proposition 8.11.3 (Gauss's lemma)**.** *Let R be a UFD, and let $f, g \in R[x]$. Then...*

$$(cont_{fg}) = (cont_f)(cont_g).$$

Corollary 8.11.2. *Let R be a UFD, and let $f, g \in R[x]$. Assume $(f) \subseteq (g)$. Then $(cont_f) \subseteq (cont_g)$.*

8.11.7 Field of rational functions

The field of *rational functions* with coefficients in R is the field of fractions of the ring $R[x]$. This field is denoted $R(x)$.

8.11.8 Factorization in polynomial rings

Lemma 8.11.6. *Let R be a UFD, and let $K = K(R)$ be its field of fractions. For nonzero $f, g \in R[x]$, denote by $(f), (g)$ the principal ideals $fR[x], gR[x]$ in $R[x]$, and denote by $(f)_K$, $(g)_K$ the principal ideals $fK[x], gK[x]$ in $K[x]$. Assume...*

- *$(cont_g) \subseteq (cont_f)$and*
- *$(g)_K \subseteq (f)_K$.*

Then $(g) \subseteq (f)$.

Proposition 8.11.4. *Let R be a UFD, and let K be its field of fractions. Let $f \in R[x]$ be a nonconstant, irreducible polynomial. Then f is irreducible as an element of $K[x]$.*

Corollary 8.11.3. *Let R be a UFD and K the field of fractions of R. Let $f \in R[x]$ be a nonconstant polynomial. Then f is irreducible in $R[x]$ if and only if it is irreducible in $K[x]$ and primitive.*

The preceding results all lead to the following result...

Theorem 8.11.1. *Let R be a UFD; then $R[x]$ is a UFD.*

8.11.9 Irreducibility in polynomial rings

Lemma 8.11.7. *Let R be an integral domain, and let $f \in R[x]$ be a polynomial of degree n. Then the number of roots of f, counted with multiplicity, is at most n.*

Proof. Replace R by its field of fractions K. And observe K is a UFD. □

Corollary 8.11.4. *Let R be an infinite integral domain, and let $f, g \in R[x]$ be polynomials. Then $f = g$ if and only if the evaluation functions $r \mapsto f(r)$, $r \mapsto g(r)$ agree.*

Proposition 8.11.5. *Let k be a field. A polynomial $f \in k[x]$ of degree 2 or 3 is irreducible if and only if it has no roots.*

Proposition 8.11.6. *Let R be a UFD, and let K be its field of fractions. Let...*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x],$$

and let $c = \frac{p}{q} \in K$ be a root of f, with $p, q \in R$, gcd$(p,q) = 1$. Then $p|a_0$ and $q|a_n$ in R.

8.11.10 Eisenstein's Criterion

Proposition 8.11.7. *Let R be a commutative ring, and let $\boldsymbol{p}$ be a prime ideal of R. Let...*

$$f = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$$

be a polynomial, and assume that...

- $a_n \notin \boldsymbol{p}$;
- $a_i \in \boldsymbol{p}$ *for* $i = 0, \ldots, n-1$;
- $a_0 \notin \boldsymbol{p}^2$

Then f is not the product of polynomials of degree $< n$ in $R[x]$.

8.11.11 Cyclotomic Polynomials

Cyclotomic polynomials are polynomials...

$$f(x) = 1 + x + x^2 + \cdots + x^{p-1} \in \mathbb{Z}[x].$$

for a prime integer p.

Proposition 8.11.8. *The cyclotomic polynomial f above is irreducible.*

Proof. Observe $f(x)$ is irreducible $\Leftrightarrow$ $f(x+1)$ is irreducible. Also observe $f(x) = \frac{(x^p-1)}{(x-1)}$. Then...

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1)-1} = x^{p-1} + \binom{p}{p-1} x^{p-2} + \cdots + \binom{p}{3} x^2 + \binom{p}{2} x + \binom{p}{1};$$

Eisenstein's criterion proves that this is irreducible, since $\binom{p}{1} = p$ and $p | \binom{p}{k}$ for $k = 1. \ldots, p-1$. $\square$

9 Field Theory

9.1 Definitions

A *field* is a nonzero commutative ring R (with 1) in which every nonzero element is a unit.

9.2 Finite Subgroups of Multiplicative Groups of Fields

Lemma 9.2.1. *Let G be a finite abelian group, and assume that for every integer $n > 0$ the number of elements $g \in G$ such that $ng = 0$ is an most n. Then G is cyclic.*

Proof. By 6.5.1...
$$G \cong \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_s\mathbb{Z}}$$
for some positive integers $1 < d_1|\cdots|d_s$. But if $s > 1$, Then $|G| > d_s$ and $d_s g = 0$ for all $g \in G$ (so that the order of g divides d_s), contradicting the hypotheses. Therefore $s = 1$; that is, G is cyclic. □

Proposition 9.2.1. *Let F be a field, and let G be a finite subgroup of the multiplicative group $(F^*, \cdot)$. Then G is cyclic.*

Proof. A polynomial $f(x) \in F[x]$ is divisible by $(x - a)$ if and only if $f(a) = 0$; since a nonzero polynomial of degree n over a field can have as most n linear factors, this shows that if $f(x) \in F[x]$ has degree n, then $f(a) = 0$ for at most n distinct elements $a \in F$. Thus, for every n there are at most n elements $a \in F$ such that $a^n - 1 = 0$, that is, at most n elements $a \in G$ such that $a^n = 1$. The preceding lemma implies then that G is cyclic. □

9.3 Algebraically Closed Fields

A field k is *algebraically closed* if all irreducible polynomials in $k[x]$ have degree 1.

Lemma 9.3.1. *A field k is algebraically closed if and only if every nonconstant polynomial $f \in k[x]$ factors completely as a product of linear factors, if and only if every nonconstant polynomial $f \in k[x]$ has a root in k.*

Proposition 9.3.1. *Let k be an algebraically closed field. Then k is infinite.*

Proof. Adapt Euclid's proof of the infinitude of primes. □

9.3.1 Polynomials Over Fields

Proposition 9.3.2. *Every polynomial $f \in \mathbb{R}[x]$ of degree ≥ 3 is reducible.*

The nonconstant irreducible polynomials in $\mathbb{R}[x]$ are precisely the polynomials of degree 1 and the quadratic polynomials...

$$f = ax^2 + bx + c$$

with $b^2 - 4ac < 0$.

Proof. Use the fundamental theorem of algebra and apply complex conjugation to any complex root to find a linear factor. $\square$

Corollary 9.3.1. *Every polynomial $f \in \mathbb{R}[x]$ of odd degree has a real root.*

Proposition 9.3.3. *Let $f \in \mathbb{Z}[x]$ be a primitive polynomial, and let p be a prime integer. Assume $f \bmod p$ has the same degree as f and is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$. Then f is irreducible in $\mathbb{Z}[x]$.*

Corollary 9.3.2. *There are irreducible polynomials in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ of arbitrarily large degree.*

9.4 Field Extensions

Proposition 9.4.1. *Let k be a field, and let $f(t) \in k[t]$ be a nonzero irreducible polynomial. Then...*

$$F := \frac{k[t]}{(f(t))}$$

is a field, endowed with a natural homomorphism $i : k \hookrightarrow F$ (obtained as the composition $k \to k[x] \to F$) realizing it as an extension of k. Further,

- *$f(x) \in k[x] \subseteq F[x]$ has a root in F, namely the coset of t;*
- *if $k \subseteq K$ is any extension in which f has a root, then there exists a homomorphism $j : F \to K$ such that the diagram*

$$\begin{tikzcd} k \arrow[rr, hook] \arrow[dr, hook, "i"'] & & K \\ & F \arrow[ur, hook, "j"'] & \end{tikzcd}$$

commutes.

A field extension $k \subseteq F$ is *finite*, of *degree* n, if F has (finite) dimension dim $F = n$ as a vector space over k. The extension is *infinite* otherwise. The degree is denoted $[F : k]$.

9.4.1 Simple Extensions

A field extension $k \subseteq F$ is *simple* is there exists an element $\alpha \in F$ such that $F = k(\alpha)$, the smallest subfield of F containing both k and α.

Proposition 9.4.2. *Let $k \subseteq k(\alpha)$ be a simple extension. Consider the evaluation map $\epsilon : k[t] \to k(\alpha)$, defined by $f(t) \to f(\alpha)$. Then we have the following:*

- *ϵ is injective if and only if $k \subseteq k(\alpha)$ is an infinite extension. In this case, $k(\alpha)$ is isomorphic to the field of rational functions $k(t)$*
- *ϵ is not injective if and only if $k \subseteq k(\alpha)$ is finite. In this case, there exists a unique monic irreducible nonconstant polynomial $p(t) \in k[t]$ of degree $n = [k(\alpha) : k]$ such that...*

$$k(\alpha) \cong \frac{k[t]}{(p(t))}.$$

Via this isomorphism, α corresponds to the coset of t. The polynomial $p(t)$ is the monic polynomial of smallest degree in $k[t]$ such that $p(\alpha) = 0$ in $k(\alpha)$.

Proof. Apply the first isomorphism theorem and examine the kernel in each case. The bit about the field of fractions is to account for the fact that $k[t]$ is an integral domain and not (quite) a field. $\square$

Proposition 9.4.3. *Let $k_1 \subseteq F_1 = k_1(\alpha_1)$, $k_2 \subseteq F_2 = k_2(\alpha_2)$ be two finite simple extensions. Let $p_1(t) \in k_1[t]$, resp., $p_2(t) \in k_2[t]$, be the minimal polynomials of α_1, resp., α_2. Let $i : k_1 \to k_2$ be an isomorphism, such that...*

$$i(p_1(t)) = p_2(t).$$

Then there exists a unique isomorphism $j : F_1 \to F_2$ agreeing with i on k_1 and such that $j(\alpha_1) = \alpha_2$.

9.4.2 Group of Automorphisms of an Extension

Let $k \subseteq F$ be a field extension. The *group of automorphisms* of the extension, denoted $\mathrm{Aut}_k(F)$, is the group of field automorphisms $j : F \to F$ such that $j \restriction k = \mathrm{id}_k$.

Corollary 9.4.1. *Let $k \subseteq F = k(\alpha)$ be a simple finite extension, and let $p(x)$ be the minimal polynomial of α over k. Then $|Aut_k(F)|$ equals the number of distinct roots of $p(x)$ in F, in particular,*

$$|Aut_k(F)| \leq [F : k],$$

wiht equality if and only if $p(x)$ factors over F as a product of distinct linear polynomials.

9.4.3 Algebraic Extensions

Let $k \subseteq F$ be a field extension, and let $\alpha \in F$. Then α is *algebraic* over k, *of degree* n if $n = [k(\alpha) : k]$ is finite; α is *transcendental* over k otherwise.

The extension $k \subseteq F$ is *algebraic* if every $\alpha \in F$ is algebraic over k.

Lemma 9.4.1. *Let $k \subseteq F$ be a finite extension. Then every $\alpha \in F$ is algebraic over k, of degree $\leq [F : k]$.*

Proposition 9.4.4. *Let $k \subseteq E \subseteq F$ be field extensions. Then $k \subseteq F$ is finite if and only if both $k \subseteq E$ and $E \subseteq F$ are finite. In this case,*

$$[F : k] = [F : E][E : k].$$

Corollary 9.4.2. *Let $k \subseteq F$ be a finite extension, and let E be an intermediate field (that is, $k \subseteq E \subseteq F$). Then both $[E : k]$ and $[F : E]$ divide $[F : k]$.*

9.4.4 Finitely Generated Extension

A field extension $k \subseteq F$ is *finitely generated* if there exist $\alpha_1, \ldots, \alpha_n \in F$ such that...

$$F = k(\alpha_1)(\alpha_2)\ldots(\alpha_n) = k(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Proposition 9.4.5. *Let $k \subseteq F = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ be a finitely generated field extension. Then the following are equivalent:*

1. *$k \subseteq F$ is a finite extension*
2. *$k \subseteq F$ is an algebraic extension*
3. *Each α_i is algebraic over k.*

If these conditions are satisfied, then $[F : k] \leq$ the product of the degrees of α_i over k.

Corollary 9.4.3. *Let $k \subseteq F$ be a field extension. Let...*

$$E = \{\alpha \in F | \alpha \text{ is algebraic over } k\}.$$

Then E is a field.

Corollary 9.4.4. *Let $k \subseteq E \subseteq F$ be field extensions. Then $k \subseteq F$ is algebraic if and only if both $k \subseteq F$ and $E \subseteq F$ are algebraic.*

9.4.5 Algebraic Closure

Lemma 9.4.2. *For a field K, the following are equivalent:*

- *K is algebraically closed.*
- *K has no nontrivial extensions.*

- *If $K \subseteq L$ is any extension and $\alpha \in L$ is algebraic over K, then $\alpha \in K$.*

An *algebraic closure* of a field k is an algebraic extension $k \subseteq \overline{k}$ such that $\overline{k}$ is algebraically closed.

Theorem 9.4.1. *Every field k admits an algebraic closure $k \subseteq \overline{k}$; this extension is unique up to isomorphism.*

Proof. The algebraic closure is constructed in the remaining theorems and observations of this section. $\square$

First we tackle existence...

Lemma 9.4.3. *Let k be a field. Then there exists an extension $k \subseteq K$ such that every nonconstant polynomial $f(x) \in k[x]$ has at least one root in K.*

Proof. $\square$

Last we tackle uniqueness...

10 Modules

10.1 Definitions

An *left-action* of a ring R on M is a homomorphism of rings...

$$\sigma : R \to \mathrm{End}_{Ab}(M)$$

We say σ makes M into a *left-R-module*.

A left-R-module structure on an abelian group M consists of a map $R \times M \to M$, $(r, m) \mapsto rm$, such that...

- $r(m + n) = rm + rn$
- $(r + s)m = rm + sm$
- $(rs)m = r(sm)$
- $1m = m$

Proposition 10.1.1. *Every abelian group is a $\mathbb{Z}$-module, in exactly one way.*

Proof. Let G be an abelian group. A $\mathbb{Z}$-module structure on G is a ring homomorphism...

$$\mathbb{Z} \to \mathrm{End}_{Ab}(G).$$

Since $\mathbb{Z}$ is initial in Ring, there exists exactly one such homomorphism, proving the statement. $\square$

10.2 Homomorphisms of R-modules

A *homomorphism of R-modules* is a homomorphism of abelian groups which is compatible with the module structure. That is, if M, N are R-modules and $\varphi : M \to N$ is a function, then φ is a homomorphism of R-modules if and only if...

- $(\forall m_1 \in M)(\forall m_2 \in M) : \varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$;
- $(\forall r \in R)(\forall m \in M) : \varphi(rm) = r\varphi(m)$.

10.3 Constructions

10.3.1 Products and Coproducts

Proposition 10.3.1. *The direct sum $M \oplus N$ satisfies the universal properties of both the product and the coproduct of M and N.*

10.3.2 Quotient Modules

Theorem 10.3.1. *Let N be a submodule of an R-module of M. Then for every homomorphism of R-modules $\varphi : M \to P$ such that $N \subseteq ker\varphi$ there exists a unique homomorphism of R-modules $\tilde{\varphi} : M/N \to P$ so that the diagram...*

$$\begin{tikzcd} M \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & P \\ & M/N \arrow[ur, "\exists!\tilde{\varphi}"'] & \end{tikzcd}$$

commutes.

10.4 Submodules

A *submodule* N of an R-module M is an R-module such that the inclusion $N \subseteq M$ is an R-module homomorphism.

10.4.1 Generated Submodules

Let M be an R-module, and let $A \subseteq M$. By the universal property of free modules, there is a unique homomorphism of R-modules...

$$\varphi_A : R^{\oplus A} \to M.$$

The *submodule generated by* A in M, denoted $\langle A \rangle$, is the image of this homomorphism.

Thus...

$$\langle A \rangle = \{\sum_{a \in A} r_a a | r_a \neq 0 \text{ for only finitely many elements } a \in A\}.$$

10.4.1.1 Finitely Generated

The module M is *finitely generated* if $M = \langle A \rangle$ for a *finite* set A.

Alternatively, the module M is *finitely generated* if there is an onto homomorphism of R-modules...

$$R^{\oplus n} \twoheadrightarrow S.$$

10.4.2 Noetherian Modules

An R-module M is *Noetherian* if every submodule of M is finitely generated as an R-module.

Proposition 10.4.1. *Let M be an R-module, and let N be a submodule of M. Then M is Noetherian if and only if both N and M/N are Noetherian.*

Proof. If M is Noetherian, then so is M/N, and so if N (because every submodule of N is a submodule of M, so it is finitely generated because M is Noetherian).

For the converse, assume N and M/N are Noetherian, and let P be a submodule of M; we have to prove that P is finitely generated. Since $P \cap N$ is a submodule of N and N is Noetherian, $P \cap N$ is finitely generated. Thus...

$$\frac{P}{P \cap N} \cong \frac{P + N}{N},$$

and hence $P/(P \cap N)$ is isomorphic to a submodule of M/N. Since M/N is Noetherian, this shows that $P/(P \cap N)$ is finitely generated.

It follows that P itself is finitely generated. $\square$

Corollary 10.4.1. *Let R be a Noetherian ring, and let M be a finitely generated R-module. Then M is Noetherian (as an R-module).*

Proof. Indeed, by hypothesis there is an onto homomorphism $R^{\oplus n} \twoheadrightarrow M$ of R-modules; hence M is isomorphic to a quotient of $R^{\oplus n}$. By the previous proposition, it suffices to prove that $R^{\oplus n}$ is Noetherian.

This may be done by induction. The statement is true for $n = 1$ by hypothesis. For $n > 1$, assume we know that $R^{\oplus(n-1)}$ is Noetherian; since $R^{\oplus(n-1)}$ may be viewed as a submodule of $R^{\oplus n}$, in such a way that...

$$\frac{R^{\oplus n}}{R^{\oplus(n-1)}} \cong R,$$

and R is Noetherian, it follows that $R^{\oplus n}$ is Noetherian, again by applying the previous proposition. $\square$

10.5 Free Modules

A free R-module on the set A, $F^R(A)$, an R-module together with a set function $j : A \to F^R(A)$ making the following diagram commute.

$$\begin{tikzcd}
F^R(I) \arrow[r, "\exists!\varphi"] & M \\
I \arrow[u, "j"] \arrow[ur, "i"'] &
\end{tikzcd}$$

Proposition 10.5.1. $F^R(I) \cong R^{\oplus I}$.

10.5.1 Linearly Independent

We say that the indexed set $i : I \to M$ is *linearly independent* if φ in the above diagram is injective.

10.5.2 Generating Set

We say that the indexed set $i : I \to M$ *generates* M if φ is surjective.

The following lemma is equivalent to the axiom of choice and so the use of Zorn's lemma cannot be avoided entirely.

Lemma 10.5.1. *Let M be an R-module, and let $S \subseteq M$ be a linearly independent subset. Then there exists a maximal linearly independent subset of M containing S.*

10.5.3 Basis

An indexed set $B \to M$ is a *basis* if it generates M and is linearly independent.

Lemma 10.5.2. *An R-module M is free if and only if it admits a basis. In fact, $B \subseteq M$ is a basis if and only if the natural homomorphism $R^{\oplus B} \to M$ is an isomorphism.*

Proposition 10.5.2. *Let R be an integral domain, and let M be a free R-module. Let B be a maximal linearly independent subset of M, and let S be a linearly independent subset. Then $|S| \leq |B|$.*

In particular, any two maximal linearly independent subsets of a free module over an integral domain have the same cardinality.

Proof. By taking fields of fractions, the general case over an integral domain is easily reduced to the case of vector spaces over a field. We may then assume that $R = k$ is a field and $M = V$ is a k-vector space.

We have to prove that there is an injective map $j : S \hookrightarrow B$, and this can be done by an inductive process, replacing elements of B by elements of S 'one-by-one.' For this, let $\leq$ be a well-ordering on S, let $v \in S$, and assume we have defined j for all $w \in S$ with $w < v$. Let B' be the set obtained from B by replacing all $j(w)$ by w, for $w < v$, and assume (inductively) that B' is still a maximal linearly independent subset of V. Then I claim that $j(v) \in B$ may be defined so that...

- $j(v) \neq j(w)$ for all $w < v$;
- the set B" obtained from B' by replacing $j(v)$ by v is still a maximal linearly independent subset.

Transfinite induction then shows that j is defined and injective on S, as needed.

To verify my claim, since B' is a maximal linearly independent set, $B' \cup \{v\}$ is linearly dependent (as an indexed set), so that there exists a linear dependence relation...

$$c_0 v + c_1 b_1 + \cdots + c_t b_t = 0$$

with not all c_t equal to zero and the b_t distinct in B'. Necessarily $c_0 \neq 0$ (because B' is linearly independent); also, necessarily not all the b_i with $c_i \neq 0$ are elements of S (because S is linearly independent). Without loss of generality we may then assume that $c_1 \neq 0$ and $b_1 \in B' \backslash S$. This guarantees that $b_1 \neq j(w)$ for all $w < v$; I set $j(v) = b_1$.

All that is left now is the verification that the set B'' obtained by replacing b_1 by v in B' is a maximal linearly independent subset. But by using to write

$$v = -c_0^{-1} c_1 b_1 - \cdots - c_0^{-1} c_t b_t,$$

this is an easy consequence of the fact that B' is a maximal linearly independent subset. □

Corollary 10.5.1. *Let R be an integral domain, and let A, B be sets. Then...*

$$F^R(A) \cong F^R(B) \Leftrightarrow \text{ there is a bijection } A \cong B.$$

10.5.4 Rank

Let R be an integral domain. The *rank* of a free R-module M, denoted $\mathrm{rk}_R M$, is the cardinality of a maximal linearly independent subset of M.

Proposition 10.5.3. *Let R be an integral domain, and let M be a free R-module; assume that M is generated by S : $M = \langle S \rangle$. Then S contains a maximal linearly independent subset of M.*

10.6 Homomorphisms of free modules

If F is a free module, then there is a set A determined up to bijection/choice-of-basis (see 10.5.2) such that $F \cong R^{\oplus A}$.

So we can understand $\mathrm{Hom}_R(F_1, F_2)$ in terms of $\mathrm{Hom}_R(R^{\oplus A_1}, R^{\oplus A_2})$ up to the choice of isomorphisms $F_1 \cong R^{\oplus A_1}$ and $F_2 \cong R^{\oplus A_2}$ (i.e. choice of basis.) In the case that A_1 and A_2 are finite we can simply describe $\mathrm{Hom}_R(R^n, R^m)$ as an R-module, for every choice of $m, n \in \mathbb{Z}$ in order to understand thes morphisms. This can be done with matrices with entries in R.

10.6.1 Matrices

An $m \times n$ *matrix* with entries in R is a choice of mn elements in R. It is commonly denoted as...

$$(r_{ij})_{i=1,\ldots,m;\, j=1,\ldots,n} = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mn} \end{pmatrix}$$

The set $\mathcal{M}_{m,n}(R)$ of $m \times n$ matrices with entries in R is an R-module under entrywise addition...

$$(a_{ij}) + (b_{ij}) := (a_{ij} + b_{ij})$$

and the action...

$$r(a_{ij}) := (r a_{ij})$$

for $r \in R$.

We can also define multiplication between $m \times p$ matrices and $p \times n$ matrices...

$$A_{m\times p} \cdot B_{p\times n} = (a_{ik}) \cdot (b_{kj}) := \left(\sum_{k=1}^{p} a_{ik} b_{kj} \right).$$

This multiplication is associative.

Thus the set $\mathcal{M}_n(R)$ of $n \times n$ matrices with entries in R is an R-algebra with the identity element...

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

A *column n-vector* is a $n \times 1$ matrix and a *row m-vector* is a $1 \times m$ matrix. These structures can stand in for elements of $\mathbf{v} \in R^n$ (or R^m as the case may be). Thus we can act on R^n with an $m \times n$ matrix, by left-multiplication...

$$A \cdot \mathbf{v} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} a_{11}v_1 + a_{12}v_2 + \cdots + a_{1n}v_n \\ a_{21}v_1 + a_{22}v_2 + \cdots + a_{2n}v_n \\ \vdots \\ a_{m1}v_1 + a_{m2}v_2 + \cdots + a_{mn}v_n \end{pmatrix} \in R^m.$$

Lemma 10.6.1. *For all $m \times n$ matrices A with entries in R:*

- *The function $\varphi : R^n \to R^m$ defined by $\varphi(\boldsymbol{v}) = A \cdot \boldsymbol{v}$ is a homomorphism of R-modules.*
- *Every R-module homomorphism $R^n \to R^m$ is determined in this way by a unique $m \times n$ matrix.*

Corollary 10.6.1. *The correspondence introduced in the previous lemma gives an isomorphism of R-modules...*

$$\mathcal{M}_{m,n}(R) \cong \mathrm{Hom}_R(R^n, R^m).$$

Lemma 10.6.2. *The following diagram commutes...*

$$\begin{tikzcd} \mathcal{M}_{m,p}(R) \times \mathcal{M}_{p,n}(R) \arrow[r] \arrow[d, "\sim"] & \mathcal{M}_{m,n}(R) \arrow[d, "\sim"] \\ \mathrm{Hom}_R(R^n, R^m) \times \mathrm{Hom}_R(R^n, R^p) \arrow[r] & \mathrm{Hom}_R(R^n, R^m) \end{tikzcd}$$

10.6.2 Change of Basis

Let F be a finitely generated free module and choose two (finite) bases A, B for F. Then the two bases correspond to two isomorphisms...

$$R^{\oplus A} \xrightarrow{\varphi} F,\ R^{\oplus B} \xrightarrow{\psi} F.$$

Then...

$$R^{\oplus A} \xrightarrow{\psi^{-1}\circ\varphi} R^{\oplus B}$$

is an isomorphism, which corresponds to a matrix N_A^B, the *matrix of the change of basis.*

Proposition 10.6.1. *Let $\alpha : F \to G$ be a homomorphism of finitely generated free modules, and let P be a matrix repéresenting it with respect to any choice of bases for F and G. Then the matrices representing α with respect to any other choice of bases are all and only the matrices of the form...*

$$M \cdot P \cdot N$$

where M and N are invertible matrices.

10.6.3 Equivalent Matrices

Two matrices $P, Q \in \mathcal{M}_{m,n}(R)$ are equivalent *if they represent the same homomorphism of free modules $R^n \to R^m$ up to a choice of basis.*

10.6.4 Elementary Operations

In this section we detail the elementary operations that can be performed on an $m \times n$ matrix P. The examples given are to 4×4 invertible matrices that operate on the rows of an $4 \times n$ matrix. They should suggest an easy generalization to larger invertible matrices and operations on columns.

The Elementary operations on a matrix are...

- switching two rows (or columns) of P; **Example.**

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

  switches the second and fouth row

- add to one row (resp., column) a multiple of another row (resp., column); **Example:**

$$\begin{pmatrix} 1 & 0 & c & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

  adds to the first row the c-multiple of the third column

- multiply all entries in one row (or column) of P by a unit of R. **Example:**

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & u & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

  multiplies the second row by the unit u

Proposition 10.6.2. *Two matrices $P, Q \in \mathcal{M}_{m,n}(R)$ are equivalent if Q may be obtained from P by a sequence of elementary operations.*

10.6.5 Gaussian Elimination over Euclidean domains

We give a 2×2 example, which generalizes easily. Let...

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(R),$$

for a Euclidean domain R, with Euclidean valuation N. After switching rows and/or columns if necessary, we may assume that $N(a)$ is the minimum of the valuations of all entries in the matrices. Division with remainder gives... $b = aq + r$ with $r = 0$ or $N(r) < N(a)$. Adding to the second column the $(-q)$-multiple of the first produces the matrix...

$$\begin{pmatrix} a & r \\ c & d - qc \end{pmatrix}.$$

If $r \neq 0$, so that $N(r) < N(a)$, we begin again and shuffle rows and columns so that the (1,1) entry has minimum valuation. This process may be repeated, but after a finite number of steps the (1,2) entry will have to vanish.

Trivial variations of the same procedure will clear the (2,1) entry as well, producing a matrix...

$$\begin{pmatrix} e & 0 \\ 0 & f \end{pmatrix}.$$

Now we may assume that e divides f in R, with no remainder. Indeed, otherwise we can add the second row to the first,

$$\begin{pmatrix} e & f \\ 0 & f \end{pmatrix},$$

and start all over with this new matrix. Again, the effect of all the operations will be to decrease the valuation of the $(1,1)$ entry, so after a final number of steps we must reach the condition $e|f$.

Proposition 10.6.3. *Let R be a Euclidean domain, and let $P \in \mathcal{M}_{m,n}(R)$. Then P is equivalent to a matrix of the form...*

$$\left(\begin{array}{ccc|c} d_1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & 0 \\ 0 & \cdots & d_r & 0 \\ \hline 0 & \cdots & 0 & 0 \end{array}\right),$$

with $d_1 | \cdots | d_r$.

This is called the Smith normal form *of the matrix.*

10.6.6 The Determinant

Let $A = (a_{ij}) \in \mathcal{M}_n(R)$ be a square matrix. Then the *determinant* of A is the element...

$$\det(A) = \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i=1}^{n} a_{i\sigma(i)} \in R.$$

Some properties of the determinant are...

- $\det(A) = \det(A^t)$
- If two rows or columns of a matrix A agree, then $\det(A) = 0$
- Suppose $A = (a_{ij})$ and $B = (b_{ij})$ agree on all but at most one row. Then $\det(C) = \det(A) + \det(B)$.

Lemma 10.6.3. *Let A be a square matrix with entries in an integral domain R.*

- *Let A' be obtained from A by switching two rows to two columns. Then* $\det(A^t)$ = -$\det(A)$.
- *Let A' be obtained from A by adding to a row (resp. column) a multiple of another row (resp. column). Then* $\det(A^t) = \det(A)$.
- *Let A' be obtained from A by multiplying a row (resp. column) by an element $c \in R$. Then* $\det(A') = c\det(A)$.

In other words, the effect of an elementary operation on $\det(A)$ *is the same as multiplying* $\det(A)$ *by the determinant of the corresponding elementary matrix.*

10.6.7 Cofactors of a square matrix

If $A \in \mathcal{M}_n(R)$, the *cofactors* of A are the $(n-1) \times (m-1)$ minores of A, corrected by sign. More precisely, for $A = (a)_{ij}$, I will let...

$$A^{ij} := (-1)^{i+j}\det \begin{pmatrix} a_{11} & \cdots & a_{1j-1} & a_{1j+1} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{i-11} & \cdots & a_{i-1j-1} & a_{i-1j+1} & \cdots & a_{i-1n} \\ a_{i+11} & \cdots & a_{i+1j-1} & a_{i+1j+1} & \cdots & a_{i+1n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nj-1} & a_{nj+1} & \cdots & a_{nn} \end{pmatrix}$$

Lemma 10.6.4. *With notation as above,*

- *for all $i = 1, \ldots, n$, det$(A) = \sum_{j=1}^{n} a_{ij} A^{(ij)}$,*

- *for all* $j = 1, \dots, n$, $det(A) = \sum_{i=1}^{n} a_{ij} A^{(ij)}$.

Corollary 10.6.2. *Let* R *be a commutative ring and* $A \in \mathcal{M}_n(R)$. *Then...*

$$A \cdot \begin{pmatrix} a^{(11)} & \cdots & a^{(n1)} \\ \vdots & \ddots & \vdots \\ a^{(1n)} & \cdots & a^{(nn)} \end{pmatrix} = \begin{pmatrix} a^{(11)} & \cdots & a^{(n1)} \\ \vdots & \ddots & \vdots \\ a^{(1n)} & \cdots & a^{(nn)} \end{pmatrix} \cdot A = \det(A) \cdot I_n.$$

The matrix of cofactors above is called the *adjoint matrix* of A. Note...

$$A^{-1} = \det(A)^{-1} \begin{pmatrix} a^{(11)} & \cdots & a^{(n1)} \\ \vdots & \ddots & \vdots \\ a^{(1n)} & \cdots & a^{(nn)} \end{pmatrix}.$$

Proposition 10.6.4 (Cramer's rule)**.** *Assume* $\det(A)$ *is a unite, and let* $A^{(j)}$ *be the matrix obtained by replacing the* j*-th column of* A *by the column vector* b*. Then...*

$$x_j = \det(A)^{-1} \det(A^{(j)}).$$

10.7 Presentations

10.7.1 Torsion

An element $m \in M$ of an R-module is a *torsion* element if $\{m\}$ is linearly dependent.

The subset of torsion elements of M is denoted $\mathrm{Tor}_R(M)$.

A module M is *torsion-free* if $\mathrm{Tor}_R(M) = \{0\}$.

A *torsion* module is a module M in which every element is a torsion element.

Lemma 10.7.1. *Submodules and direct sums of torsion-free modules are torsion-free. Free modules over an integral domain are torsion-free.*

10.7.2 Cyclic

An R-module M is *cyclic* if it is generated by a singleton, that is, if $M \cong R/I$ for some ideal I of R.

Lemma 10.7.2. *Let* R *be an integral domain. Assume that every cyclic* R*-module is torsion-free. Then* R *is a field.*

10.7.3 Annihilator

The *annihilator* of an R-module M is...

$$\mathrm{Ann}_R(M) := \{r \in R | \forall m \in M, rm = 0\}.$$

10.7.4 Definition of Presentation

An R-module M is finitely presented if for some positive integers m, n there is an exact sequence...

$$R^n \xrightarrow{\varphi} R^m \longrightarrow M \longrightarrow 0.$$

Such a sequence is called a *presentation* of M.

Lemma 10.7.3. *If R is a Noetherian ring, then every finitely generated R-module is finitely presented.*

Lemma 10.7.4. *Let A, B be matrices with entries in an integral domain R, and let M, N denote the corresponding R-modules. Then $M \oplus N$ corresponds to the block matrix...*

$$\left(\begin{array}{c|c} A & 0 \\ 0 & B \end{array}\right).$$

10.7.5 Resolution

A *resolution* of an R-module M by finitely generated free modules is an exact complex...

$$\cdots \longrightarrow R^{m_3} \longrightarrow R^{m_2} \longrightarrow R^{m_1} \longrightarrow R^{m_0} \longrightarrow M \longrightarrow 0.$$

Proposition 10.7.1 (Characterization of a Field)**.** *Let R be an integral domain. Then R is a field if and only if every finitely generated R-module is free. That is for a finitely generated R-module M there is an exact sequence...*

$$0 \longrightarrow R^m \longrightarrow M \longrightarrow 0.$$

Proposition 10.7.2 (Characteriztion of a PID)**.** *Let R be an integral domain. Then R is a PID if and only if for every finitely generated R-module M and every epimorphism...*

$$R^{m_0} \xrightarrow{\pi_0} M \longrightarrow 0,$$

there exist a free R-module R^{m_1} and an R-module homomorphism $\pi_1 : R^{m_1} \to R^{m_0}$ such that the sequence...

$$0 \longrightarrow R^{m_1} \xrightarrow{\pi_1} R^{m_0} \xrightarrow{\pi_0} M \longrightarrow 0$$

is exact.

Proposition 10.7.3. *Let A be a matrix with entries in an integral domain R, and let B be obtained from A by any sequence of the following operations:*

- *switch two rows or two columns;*
- *add to one row (resp., column) a multiple of another row (resp., column);*
- *multiply all entries in one row (or column) by a unit R;*
- *if a unit is the only nonzero entry in a row (or column), remove the row and column containing that entry.*

Then B represents the same R-module as A, up to isomorphism.

10.8 Classification of Finitely Generated Modules over PIDs

Lemma 10.8.1. *Let R be a PID, let F be a finitely generated free module over R, and let $M \subseteq F$ be a nonzero submodule. Then there exist $a \in R$, $x \in F$, $y \in M$, and submodules $F' \subseteq F$ and $M' \subseteq M$, such that $y = ax \neq 0$, $M' = F' \cap M$, and...*

$$F = \langle x \rangle \oplus F',\ M = \langle y \rangle \oplus M'.$$

Proof. For all $\varphi \in \mathrm{Hom}_R(F, R)$, $\varphi(M)$ is a submodule of R, that is, an ideal. The family of all these ideals is nonempty, and PIDs are Noetherian; therefore there exists a maximal element in the family, say $\alpha(M)$, for a homomorphism $\alpha : M \to R$. The fact that $M \neq 0$ implies immediately that some $\varphi(M) \neq 0$; hence $\alpha(M) \neq 0$.

Since R is a PID, $\alpha(M)$ is principal: $\alpha(M) = (a)$ for some $a \in R$, $a \neq 0$. Since $a \in \alpha(M)$, there exists an element $y \in M$, $y \neq 0$, such that $\alpha(y) = a$. These are the elements a, y mentioned in the statement.

I claime that a divides $\varphi(y)$ for all $\varphi \in \mathrm{Hom}_R(F, R)$. Indeed, let b be a generator of $(a, \varphi(y))$, and let $r, s \in R$ such that $b = ra + s\varphi(y)$; consider the homomorphism $\psi := r\alpha + s\varphi$. Since $a \in (b)$, we have $\alpha(M) \subseteq (b)$. On the other hand...

$$b = ra + s\varphi(y) = (r\alpha + s\varphi)(y) = \psi(y) \in \psi(M);$$

therefore $(b) \subseteq \psi(M)$. It follows that $\alpha(M) \subseteq \psi(M)$, and by maximality $\alpha(M) = \psi(M)$; hence $(a) = (b)$, and in particular $a|\varphi(y)$, as claimed.

Let $y = (s_1, \ldots, s_n)$ as an element of $F = R^n$. Each s_i is the iamge of y by a homomorphism $F \to R$, so a divides all of them by what we just proved. Therefore $\exists r_1, \ldots, r_n \in R$ such that $s_i = ar_i$; let...

$$x = (r_1, \ldots, r_n) \in F.$$

This is the element x mentioned in the statement. By construction, $y = ax$. Further, $a = \alpha(y) = \alpha(ax) = a\alpha(x)$; since R is an integral domain and $a \neq 0$, this implies $\alpha(x) = 1$.

Finally, we let $F' = \ker\alpha$ and $M' = F' \cap M$, and we can proceed to verify the direct sums.

First, every $z \in F$ may be written as...

$$z = \alpha(z)x + (z - \alpha(z)x);$$

by linearity...

$$\alpha(z - \alpha(z)x) = \alpha(z) - \alpha(z)\alpha(x) = \alpha(z) - \alpha(z) = 0,$$

that is, $z - \alpha(z)x \in \ker\alpha$. This implies that $F \in \langle x \rangle + F'$. On the other hand, $rx \in F' \Rightarrow \alpha(rx) = 0 \Rightarrow r\alpha(x) = 0 \Rightarrow r = 0$: that is, $\langle x \rangle \cap F' = 0$. Therefore...

$$F = \langle x \rangle \oplus F',$$

as claimed.

Second, if $z \in M$, then a divides $\alpha(z)$: indeed, $\alpha(z) \in \alpha(M) = (a)$. Writing $\alpha(z) = ca$, we have $\alpha(z)x = cax = cy$; splitting z as above, we note...

$$z - \alpha(z)x = z - cy \in M \cap F' = M',$$

and this leads as before to...

$$M = \langle y \rangle \oplus M',$$

concluding the proof. □

Proposition 10.8.1. *Let R be a PID, let F be a finitely generated free module over R, and let $M \subseteq F$ be a submodule. Then M is free.*

Proof. Use the previous lemma iteratively until all the generators are exhausted. □

Corollary 10.8.1. *Let R be a PID, let F be a finitely generated free module over R, and let $M \subseteq F$ be a submodule. Then there exist a basis $(x_1, \ldots, x_n)$ of F and nonzero elements $a_1, \ldots, a_m$ of R ($m \leq n$) such that $(a_1x_1, \ldots, a_mx_m)$ is a basis of M. Further, we may assume $a_1|a_2|\cdots|a_m$.*

10.8.1 Rank of a finitely generated module

Let R be an integral domain. The *rank* rk$M$ of a finitely generated R-module M is the maximum number of linearly independent elements in M.

Theorem 10.8.1 (Classification of finitely generated modules over PIDs)**.** *Let R be a PID, and let M be a finitely generated R-module. Then the following hold:*

- *There exist distinct prime ideals $(q_1), \ldots, (q_n) \subseteq R$, positive integers r_{ij}, and an isomorphism...*

$$M \cong R^{rkM} \oplus \left(\bigoplus_{i,j} \frac{R}{(q_i^{r_{ij}})} \right).$$

- *Ther exist nonzero, nonunit ideals $(a_1), \ldots (a_m)$ of R, such that $(a_1) \supseteq (a_2) \supseteq \cdots \supseteq (a_m)$, and an isomorphism...*

$$M \cong R^{rkM} \oplus \frac{R}{(a_1)} \oplus \cdots \oplus \frac{R}{(a_m)}.$$

These decompositions are unique.

The proof of this theorem follows from the previous lemmas in a manner similar to 6.5.1 with the role of 6.5.1 taken over by the Chinese remainder theorem.

Lemma 10.8.2. *Let M be a torsion module, expressed as above (with* rk $M = 0$*). Then* $\mathrm{Ann}(M) = (a_m)$*. Further, the prime ideals (q_i) are precisely the prime ideals of R containing* $\mathrm{Ann}(M)$*.*

10.9 Linear Transformations

A linear transformation is an R-module homomorphism $\varphi \in \mathrm{End}_R(F)$ of a free module F acting on F.

10.9.1 Similar Matrices

Two square matrices $A, B \in \mathcal{M}_n(R)$ are *similar* if they represent the same homomorphism $\varphi \in \mathrm{End}_R(F)$ of a free rank-n module F to itself, up to the choice of a basis for F.

Proposition 10.9.1. *Two matrices $A, B \in \mathcal{M}_n(R)$ are similar if and only if there exists an invertible matrix P such that…*

$$B = PAP^{-1}.$$

10.9.2 Similar Homomorphisms

Two R-module homomorphisms of a free module F to itself…

$$\alpha, \beta : F \to F,$$

are *similar* if there exists an automorphism $\pi : F \to F$ such that…

$$\beta = \pi \circ \alpha \circ \pi^{-1}.$$

10.9.3 Determinant of a Homomorphism

Let $\alpha \in \mathrm{End}_R(F)$. The *determinant* of α is $\det(\alpha) := \det(A)$, where A is the matrix representing α with respect to any choice of basis of F.

Proposition 10.9.2. *Let α be a linear transformation of a free R-module $F \cong R^n$. Then $det(\alpha) \neq 0$ if and only if α is injective.*

Proof. Use the field of fractions of R. □

10.9.4 Trace

The *trace* of a square matrix $A = (a_{ij}) \in \mathcal{M}_n(R)$ is…

$$\mathrm{tr}(A) := \sum_{i=1}^{n} a_{ii}.$$

Let $\alpha \in \mathrm{End}_R(F)$. The *trace* of α is defined to be $\mathrm{tr}(\alpha) := \mathrm{tr}(A)$, where A is the matrix representing α with respect to any choice of basis of F.

Lemma 10.9.1. *Let $A, B \in \mathcal{M}_n(R)$. Then $tr(AB) = tr(BA)$.*

10.9.5 Characteristic Polynomial

Let F be a free R-module, and let $\alpha \in \mathrm{End}_R(F)$. Denote by I the identity map $F \to F$. The *characteristic polynomial* of α is the polynomial...

$$P_\alpha(t) := \det(tI - \alpha) \in R[t].$$

Proposition 10.9.3. *Let F be a free R-module of rank n, and let $\alpha \in End_R(F)$.*

- *The characteristic polynomial $P_\alpha(t)$ is a monic polynomial of degree n.*
- *The coefficient of t^{n-1} in $P_\alpha(t)$ equals $-tr(\alpha)$.*
- *The constant term of P_α equals $(-1)^\alpha det(\alpha)$.*
- *If α and β are similar, then $P_\alpha(t) = P_\beta(t)$.*

10.9.6 Annihilator Ideal

Given $\alpha \in \mathrm{End}_R(F)$, where F is a free R-module, the *annihilator ideal of α* is...

$$\mathcal{I}_\alpha := \{f \in R[t] | f(\alpha) = 0\}.$$

Lemma 10.9.2. *If α and β are similar, then $\mathcal{I}_\alpha = \mathcal{I}_\beta$.*

Theorem 10.9.1 (Cayley-Hamilton Theorem)**.** *Let $P_\alpha(t)$ be the characteristic polynomial of the linear transformation $\alpha \in End_R(F)$. Then...*

$$P_\alpha(\alpha) = 0.$$

10.9.7 Minimal Polynomial

Let F be a free R-module, and let $\alpha \in \mathrm{End}_R(F)$. Let K be the field of fractions of R. The *minimal polynomial* of α is the monic generator $m_\alpha(t) \in K[t]$ of $\mathcal{I}_\alpha^{(K)}$.

10.9.8 Eigenvalues

Let F be a free R-module, and let $\alpha \in \mathrm{End}_R(F)$. A scalar $\lambda \in R$ is an *eigenvalue* for α if there exists $\mathbf{v} \in F$, $[v] \neq 0$, such that...

$$\alpha(\mathbf{v}) = \lambda \mathbf{v}.$$

Lemma 10.9.3. *Let F be a finitely generated R-module, and let $\alpha \in End_R(F)$. Then the set of eigenvalues of α is precisely the set of roots in R of the characteristic polynomial $P_\alpha(t)$.*

10.9.8.1 Algebraic Multiplicity

The *algebraic multiplicity* of an eigenvalue of a linear transformation α of a finitely generated free module is its multiplicity as a root of the characteristic polynomial of α.

Corollary 10.9.1. *The number of eigenvalues of a linear transformation of R^n is at most n. If the base ring R is an algebraically closed field, then every linear transformation has exactly n eigenvalues (counted with algebraic multiplicity)*

10.9.9 Eigenvector

Let λ be an eigenvalue of a linear transformation α of a free R-module F. Then a nonzero $\mathbf{v} \in F$ is an *eigenvector* for α, corresponding to the eigenvalue λ, if $\alpha(\mathbf{v}) = \lambda\mathbf{v}$, that is, if $\mathbf{v} \in \ker(\lambda I - \alpha)$.

10.9.10 Eigenspace

The *eigenspace* corresponding to the eigenvalue λ is the submodule $\ker(\lambda I - \alpha)$.

10.9.10.1 Geometric Multiplicity

The *geometric multiplicity* of an eigenvalue is the rank of its eigenspace.

10.9.11 Diagonalizable

A matrix A is diagonalizable if it admits a spectral decomposition. That is it is similar to a diagonal matrix...

$$\begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

where $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of α.

11 Linear Algebra

11.1 Definitions

11.1.1 Vector Space

A *k-vector space* is a module over a field k.

Lemma 11.1.1. *Let k be a field and let V be a k-vector space. Let B be a maximal linearly independent subset of V; then B is a basis of V.*

Proposition 11.1.1. *Let k be a field, and let V be a k-vector space. Let S be a linearly independent set of vectors of V. Then there exists a basis B of V containing S.*

In particular, V is free as a k-module.

Proof. Put 10.5.1, 10.5.2, and 11.1.1 together. □

Lemma 11.1.2. *Let k be a field, and let V be a k-vector space. Let B be a minimal generating set for V; then B is a basis of V.*

Every set generating V contains a basis of V.

11.1.2 Dimension

Let k be a field. The *dimension*, $\dim_k V$, of a k-vector space V is it's rank.

11.1.3 General Linear Group over a Field

Proposition 11.1.2. *Let k be a field, and let $n \geq 0$ be an integer. Then $GL_n(k)$ is generated by elementary matrices.*

Thus two matrices are equivalent over a field if and only if they are linked by a sequence of elementary operations.

Proposition 11.1.3. *Over a field, every $m \times n$ matrix is equivalent to a matrix of the form...*

$$\left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$$

(where $r \leq \min(m, n)$ and 0 stands for null matrices of appropriate sizes.)

11.1.4 Column/Row Space of a Matrix

The *column* (resp. *row*) *space* of a matrix P over a field k is the span of the columns (resp. rows) of P.

11.1.5 Column/Row Rank of a Matrix

The *column* (resp. *row*) *rank* of a matrix P is the dimension of the column (resp. row) space of P.

Proposition 11.1.4. *The row rank of a matrix over a field k equals its column rank.*

Thus the *rank* of $M \in \mathcal{M}_{m,n}(k)$ (k is a field) is the dimension of its column (or, equivalently, row) space.

11.1.6 Rank and Nullity of a linear map

Let $\alpha : V \to W$ be a linear map between finite-dimensional vector spaces over a field k. Then the *rank* of α, denoted rk α, is the dimension of im α. The *nullity* of α is dim(ker α).

Proposition 11.1.5. *Let $\alpha : V \to W$ be a linear map of finite-dimensional vector spaces. Then...*

$$(\textit{rank of } \alpha) + (\textit{nullity of } \alpha) = \textit{dim } V.$$

11.2 Canonical Forms

Giving a linear transformation α on a free R-module F is the same as giving an $R[t]$-module sructure on F, compatible with its R-module structure. The action of a polynomial...

$$f(t) = r_m t^m + r_{m-1} t^{m-1} + \cdots + r_0$$

on F is: for every $\mathbf{v} \in F$, set...

$$f(t)(\mathbf{v}) := r_m \alpha^m(\mathbf{v}) + r_{m-1}\alpha^{m-1}(\mathbf{v}) + \cdots + r_0\mathbf{v}.$$

We can recover the linear transformation α by multiplication by t:

$$\mathbf{v} \mapsto t\mathbf{v}.$$

Lemma 11.2.1. *Let α, β be linear transformations of a free R-module F. Then the corresponding $R[t]$-module structures on F are isomorphic if and only if α and β are similar.*

Corollary 11.2.1. *There is a one-to-one correspondence between the similarity classes of R-linear transformations of a free R-module F and the isomorphism classes of $R[t]$-module structures on F.*

11.2.1 Companion Matrix of a polynomial

Suppose V is a cyclic $k[t]$-module...

$$V \cong \frac{k[t]}{(f(t))},$$

where $f(t)$ is a nonconstant monic polynomial. Choosing the basis...

$$1,\, t,\, \cdots,\, t^{n-1}$$

of V. Multiplication by t on V acts as...

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -r_0 \\ 1 & 0 & 0 & \dots & 0 & -r_1 \\ 0 & 1 & 0 & \dots & 0 & -r_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & -r_{n-2} \\ 0 & 0 & 0 & \dots & 1 & -r_{n-1} \end{pmatrix}.$$

This matrix is the *companion matrix* of the polynomial $f(t)$, denoted $C_{f(t)}$.

We can now restate 10.8.1 in a very useful way...

Theorem 11.2.1. *Let k be a field, and let V be a finite-dimensional vector space. Let α be a linear transformation on V, and endow V with the corresponding $k[t]$-module structure. Then the following hold:*

- *There exist distinct monic irreducible polynomials $p_1(t), \dots, p_s(t) \in k[t]$ and positive integers r_{ij} such that...*

  $$V \cong \bigoplus_{i,j} \frac{k[t]}{(p_i(t)^{r_{ij}})}$$

  as $k[t]$-modules.

- *There exist monic nonconstant polynomials $f_1(t), \dots, f_m(t) \in k[t]$ such that $f_1(t)|\cdots|f_m(t)$ and...*

  $$V \cong \frac{k[t]}{(f_1(t))} \oplus \cdots \oplus \frac{k[t]}{(f_m(t))}$$

  as $k[t]$-modules.

Via these isomorphisms, the action of α on V corresponds to multiplication by t.

Further, two linear transformations α, β are similar if and only if they have the same collections of invariants $p_i(t)^{r_{ij}}$ ('elementary divisors'), $f_i(t)$ ('invariant factors').

11.2.2 Rational Canonical Forms

The *rational canoncial form* of a linear transformation α of a vector space V is the block matrix...

$$\left(\begin{array}{c|c|c} C_{f_1(t)} & & \\ \hline & \ddots & \\ \hline & & C_{f_m(t)} \end{array}\right)$$

where $f_1(t), \ldots, f_m(t)$ are the invariant factors of α.

Corollary 11.2.2. *Every linear transformation admits a rational canonical form. Two linear transformations have the same rational canonical form if and only if they are similar.*

Proposition 11.2.1. *Let $f_1(t)|\cdots|f_m(t)$ be the invariant factors of a linear transformation α on a vector space V. Then the minimal polynomial $m_\alpha(t)$ equals $f_m(t)$, and the characteristic polynomial $P_\alpha(t)$ equals the product $f_1(t)\cdots f_m(t)$.*

Proposition 11.2.2. *Let $A \in \mathcal{M}_n(k)$ be a square matrix. Then A is similar to its transpose.*

Proof. If B is similar to A and we can prove that B is similar to its transpose B^t, then A is similar to its transpose A^t: because $B = PAP^{-1}$, $B^t = QBQ^{-1}$ give...

$$A^t = (P^tQP)A(P^rQP)^{-1}.$$

Therefore, it suffices to prove the statement for matrices in rational canonical form.

Further, to prove the statement for a block matrix, it clearly suffices to prove it for each block; so we may assume that A is the companion matrix C of a polynomial $f(t)$. Since the characteristic and minimal polynomials of the transpose C^t coincide with those of C, they are both equal to $f(t)$. It follows that the rational canonical form of C^t is again the companion matrix to $f(t)$; therefore C^t and C are similar, as needed. $\square$

Lemma 11.2.2. *Assume that the characteristic polynomial $P_\alpha(t)$ factors completely; that is,*

$$P_\alpha(t) = \prod_{i=1}^{s}(t-\lambda_i)^{m_i}$$

where λ_i, $i = 1, \ldots, s$, are the distinct eigenvalues of α (and m_i are their algedbraic multiplicities). Then $p_i(t) = (t-\lambda_i)$, and $m_i = \sum_j r_{ij}$.

In this situation, the minimal polynomial of α equals...

$$m_\alpha(t) = \prod_{i=1}^{s}(t-\lambda_i)^{max_j\{r_{ij}\}}.$$

11.2.3 Jordan Block corresponding to an eigenvalue

Assuming that the characteristic polynomial factors completely over k, the basic cyclic blocks of a linear transformation α are in fact of the form...

$$\frac{k[t]}{((t-\lambda)^r)}$$

for some $\lambda \in k$ and $r > 0$. This time we choose the basis...

$$(t-\lambda)^{r-1},\ (t-\lambda)^{r-2},\ \cdots,\ (t-\lambda)^0 = 1.$$

Multiplication by t on V acts as...

$$\begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{pmatrix}$$

This matrix is the *Jordan block* of size r corresponding to λ, denoted $J_{\lambda,r}$.

11.2.4 Jordan Canonical Form

The *Jordan canonical form* of a linear transformation α of a vector space V is the block matrix...

$$\left(\begin{array}{c|c|c} J_{\lambda_1,(r_{1j})} & & \\ \hline & \ddots & \\ \hline & & J_{\lambda_s,(r_{sj})} \end{array}\right)$$

where $(t-\lambda_i)^{r_{ij}}$ are the elementary divisors of α.

Proposition 11.2.3. *The geometric multiplicity of λ as an eigenvalue of α equals the number of Jordan blocks corresponding to λ in the Jordan canonical form of α.*

Corollary 11.2.3. *Assume the characteristic polynomial of $\alpha \in End_k(V)$ factors completely over k. Then α is diagonalizable if and only if the geometric and algebraic multiplicities of all its eigenvalues coincide.*

Proposition 11.2.4. *Assume the characteristic polynomial of $\alpha \in End_k(V)$ factors completely over k. Then α is diagonalizable if and only if the minimal polynomial of α has no multiple roots.*

11.3 Simplicial Complexes

11.3.1 General Position

A set of vectors $S = \{v_0, \ldots, v_n\}$ in $\mathbb{R}^N$ for N large is in *general position* if the set $\{v_0 - v_n, v_1 - v_n, \ldots, v_{n-1} - v_n\}$ is linearly independent.

11.3.2 Simplex

A set of vectors $\{v_0, \ldots, v_n\}$ in general position is called an *n-simplex*. It determines the following subset of $\mathbb{R}^N$...

$$\Delta^n[S] = \{t_0 v_0 + t_1 v_1 + \cdots + t_n v_n \in \mathbb{R}^N | t_i \geq 0,\, t_0 + \cdots + t_n = 1\}$$

called the convex hull of $\{v_0, \ldots, v_n\}$.

11.3.3 Barycentric Coordinantes

The *barycentric coordinates* of $p \in \Delta^n$, an n-simplex, is the list of coefficients $(t_0, t_1, \ldots, t_n)$ such that...

$$p = t_0 v_0 + \cdots + t_n v_n.$$

Proposition 11.3.1. *Let Δ^n denote the subspace of $\mathbb{R}^{n+1}$ given by $\Delta^n = \{(t_0, \ldots, t_n) \in \mathbb{R}^{n+1} | t_0 + \cdots + t_n = 1, t_i \geq 0\}$. If $S = \{v_0, \ldots, v_n\}$ is a set of vectors in general position in $\mathbb{R}^N$, then $\Delta^n[S]$ is homeomorphic to Δ^n.*

Proposition 11.3.2. *The points $p \in \Delta^n[S]$ with barycentric coordinates that satisfy $t_i > 0$ for all i form an open subset of $\Delta^n[S]$ (as a subspace of $\mathbb{R}^N$); p is in the boundary of $\Delta^n[S]$ if and only if $t_i = 0$ for some i.*

11.3.3.1 Barycenter of a simplex

The *barycenter* of an n-simplex Δ^n is...

$$\beta_n = \sum_{i=0}^{n} \frac{1}{n+1} e_i = \left(\frac{1}{n+1}, \frac{1}{n+1}, \ldots, \frac{1}{n+1} \right).$$

11.3.4 Geometric Simplicial Complex

A *geometric simplicial complex* is a finite collection K of simplices in $\mathbb{R}^N$ satisfying...

1. if $S = \{v_0, \ldots, v_n\}$ in in K and $T \prec S$, then T is also in K;
2. for S and T in K, if $\Delta^n[S] \cap \Delta^m[T] \neq \emptyset$, then $\Delta^n[S] \cap \Delta^m[T] = \Delta^k[U]$ for some U in K (intersect along a common face)

The dimension of one of these complexes is the largest n for which there is an n-simplex in K.

11.3.5 Realization of a Geometric Simplicial Complex

$$|K| = \bigcup_{S \in K} \Delta^n[S] \subseteq \mathbb{R}^N.$$

Called the of K, or the underlying space of K, the geometric carrier of K, or the polyhedron determined by K.

11.3.6 Abstract Simplicial Complex

A finite collection of sets...

$$L = \{S_\alpha | S_\alpha = \{v_{\alpha 0}, \ldots, v_{\alpha n_\alpha}, 1 \leq \alpha \leq N\}\}$$

is an *abstract simplicial complex* if whenever $T = \{v_{j0}, \ldots, v_{jk}\}$ is a subset of S and S is in L, then T is also in L.

11.3.7 Triangulable

A topological space X is said to be *triangulable* if there is an abstract simplicial complex K and a homeomorphism $f : X \to |K|$.

11.3.8 Subcomplex

If K is an abstract simplicial complex and L is a subset of simplices in K, then L is a *subcomplex* of K if whenever $S \prec T$ and $T \in L$, then $S \in L$.

11.3.9 Simplicial Mappings

Let K and L be two simplicial complexes. A *simplicial mapping* is a function $\phi : K \to L$ satisfying, for all $n \geq 0$, if $S = \{v_0, \ldots, v_n\}$ is an n-simplex in K, then $\{\phi(v_0), \ldots, \phi(v_n)\}$ is a (possibly degenerate) simplex in L.

11.3.10 Barycentric Subdivision

Let K be a simplicial complex. The *barycentric subdivision* of K, denoted sd K, is the simplicial complex whose simplices are given by...

$$\{\beta(S_0), \beta(S_1), \ldots, \beta(S_r)\}, \text{ where } S_i \in K \text{ and } S_0 \succ S_1 \succ \cdots \succ S_r.$$

Here $\beta(S)$ is the barycenter of $\Delta^n[S]$ for S in K. If $\phi : K \to L$ is a simplicial mapping, then the barycentric subdivision of ϕ is the simplicial mapping sd ϕ : sd $K \to$ sd L given on vertices by sd $\phi(\beta(S)) = \beta(\phi(S))$.

11.3.11 Diameter of a Simplex

Let K be a simplicial complex, realized in $\mathbb{R}^N$. Then...

$$\text{diam } S = \max\{||v_i - v_j|| \,|\, i \neq j,\, S = \{v_0, \ldots, v_q\}\}.$$

Proposition 11.3.3. *If S is a q-simplex in K, a geometric simplicial complex, then for any simplex $T \in sd\ K$ with $\Delta^p[T] \subseteq \Delta^q[S]$, we have diam $T \leq \frac{q}{q+1}$ diam S.*

Proof. We proceed by induction on q. If $q = 1$, then $\Delta^1[S]$ is a line segment and the simplices of the barycentric subdivision are halves of the segment with diameter equal to $\frac{1}{2}$ the length of the segment. Assume the result for simplices of dimension less than $q \geq 2$.

A p-simplex $T \in \text{sd } K$ can be written as...

$$T = \left\{ v_{\sigma(0)}, \frac{v_{\sigma(0)} + v_{\sigma(1)}}{2}, \cdots, \frac{v_{\sigma(0)} + v_{\sigma(1)} + \cdots + v_{\sigma(p)}}{p+1} \right\},$$

where σ is some permutation of $(0, 1, \ldots, q)$. If $p < q$, then we are done because T is simplex in the barycentric subdivision of a face of S. When $P = q$, write the vertices of T as $T = \{w_0, w_1, \ldots, w_q\}$. The diameter of T is given by $||w_{i_0} - q_{j_0}|| = \max\{||w_i - w_j|| \,|\, w_i, w_j \in T\}$. If i_0 and j_0 are less than q, then the diameter of T is achieved on the face $\partial_q T$ and we deduce...

$$||w_{i_0} - q_{j_0}|| \leq \frac{q-1}{q} \text{diam } \partial_q S \leq \frac{q}{q+1} \text{diam } S.$$

If one of i_0 or j_0 is q, then we first observe the following estimate...

$$\begin{aligned} ||v_i - \frac{v_{\sigma(0)} + v_{\sigma(1)} + \cdots + v_{\sigma(q)}}{q+1}|| &= ||\sum_{j=0}^{q} \frac{1}{q+1}(v_i - v_j)|| \\ &\leq \sum_{j=0}^{q} \frac{1}{q+1} ||v_i - v_j|| \\ &\leq \frac{q}{q+1} \max\{||v_i - v_j||\} \\ &= \frac{q}{q+1} \text{diam } S. \end{aligned}$$

This proes the proposition. □

11.3.12 Mesh

The *mesh* of a simplex K is...

$$\text{mesh}(K) = \max\{\text{diam } S \,|\, S \in K\}.$$

Corollary 11.3.1. *If K has dimension q, then...*

$$\mathit{mesh}(\mathit{sd}\ K) \leq \frac{q}{q+1} \mathit{mesh}(K).$$

Theorem 11.3.1. *If K is a geometric simplicial complex, then $|sd\ K| = |K|$.*

Proof. Suppose $p \in |K|$. Then we can write $p = \sum_{i=0}^{q} t_i v_i \in \Delta^q[S]$ with $S = \{v_0, \ldots, v_q\}$. Permute the values $\{t_i\}$ to bring them into descending order:

$$t_{\sigma(0)} \geq t_{\sigma(1)} \geq \cdots \geq t_{\sigma(q)} \geq 0.$$

Next solve the matrix equation...

$$\begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{q+1} \\ 0 & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{q+1} \\ 0 & 0 & \frac{1}{3} & \cdots & \frac{1}{q+1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & \frac{1}{q+1} \end{pmatrix} \begin{pmatrix} s_0 \\ s_1 \\ s_2 \\ \vdots \\ s_q \end{pmatrix} = \begin{pmatrix} t_{\sigma(0)} \\ t_{\sigma(1)} \\ t_{\sigma(2)} \\ \vdots \\ t_{\sigma(q)} \end{pmatrix}.$$

The solution exists and is unique. Furthermore, by solving from the bottom up, the solution satisfies $s_q = (q+1)t_{\sigma(q)}$ and $s_{j-1} = j(t_{\sigma(j-1)} - t_{\sigma(j)}) \geq 0$. Summing the values of s_j we get...

$$\begin{aligned}
\sum_{j=0}^{q} s_j &= s_0 + 2\left(\frac{1}{2}s_1\right) + 3\left(\frac{1}{3}s_2\right) + \cdots + (q+1)\left(\frac{1}{q+1}s_q\right) \\
&= \left(s_0 + \frac{1}{2}s_1 + \frac{1}{3}s_2 + \cdots + \left(\frac{1}{q+1}\right)s_q\right) \\
&+ \left(\frac{1}{2}s_1 + \frac{1}{3}s_2 + \cdots + \left(\frac{1}{q+1}\right)s_q\right) \\
&+ \cdots + \left(\frac{1}{q+1}\right)s_q \\
&= t_{\sigma(0)} + t_{\sigma(1)} + \cdots + t_{\sigma(q)} \\
&= t_0 + \cdots + t_q = 1
\end{aligned}$$

□

Thus $(s_0, \ldots, s_q)$ are the barycentric coordinates of p in the simplex with...

$$\begin{aligned}
p = s_0 v_{\sigma(0)} &+ s_1\left(\frac{v_{\sigma(0)} + v_{\sigma(1)}}{2}\right) + s_2\left(\frac{v_{\sigma(0)} + v_{\sigma(1)} + v_{\sigma(2)}}{3}\right) \\
&+ \cdots + s_q\left(\frac{v_{\sigma(0)} + v_{\sigma(1)} + \cdots + v_{\sigma(q)}}{q+1}\right).
\end{aligned}$$

Thus p lies in the q-simplex $\Delta^q[T]$, where $T \in \text{sd } K$ is given by...

$$T = \{\beta(\{v_{\sigma(0)}\}), \ldots, \beta(\{v_{\sigma(0)}, \ldots, v_{\sigma(q)}\})\}.$$

This proves that $|K| \subseteq |\text{sd } K|$. The inclusion $|\text{sd } K| \subseteq |K|$ follows by rewriting the expression for a point in the barycentric coordinates of sd K in terms of the contributing vertices of K by rearranging terms.

11.3.13 Star of a vertex

The *star* of v is...

$$\text{star}_K(v) = \bigcup_{\{v\} \prec S} \Delta^n[S].$$

11.3.14 Open star of a vertex

The *open star* of v is...

$$\text{O}_K(v) = \bigcup_{\{v\} \prec S} \text{int}\Delta^n[S].$$

Lemma 11.3.1. *Suppose $v_0, v_1, \ldots, v_n$ are vertices in a simplicial complex K. Then $\{v_0, \ldots, v_q\}$ is a simplex in K if and only if $\bigcap_{i=0}^q O_K(v_i) \neq \emptyset$. If $p \in |K|$, then $p \in O_K(v)$ if and only if $p = \sum_{i=0}^q t_i v_i$ with $v = v_j$ for some $0 \leq j \leq q$ and $t_j \neq 0$.*

11.3.15 Simplicial Approximation

If K and L are simplicial complexes and $f : |K| \to |L|$ is continuous function, then a simplicial mapping $\phi : K \to L$ is a *simplicial approximation* to f if whenever $p \in |K|$, then $f(p) \in \Delta^q[T]$ for $T \in L$ implies $|\phi|(p) \in \Delta^q[T]$.

Proposition 11.3.4. *A simplicial mapping $\phi : K \to L$ is a simplicial approximation to a continuous mapping $f : |K| \to |L|$ if and only if, for any vertex v of K, we have...*

$$f(O_K(v)) \subseteq O_L(\phi(v)),$$

that is, the image of the open star of v under f is contained in the open star of $\phi(v)$, a vertex of L.

Theorem 11.3.2 (Simplicial Approximation Theorem)**.** *Given two simplicial complexes K and L and a continuous mapping $f : |K| \to |L|$, then there is a nonnegative integer r and a simplicial mapping $\phi : sd^r K \to L$ with ϕ a simplicial approximation to f.*

Proposition 11.3.5. *If a simplicial mapping $\phi : K \to L$ is a simplicial approximation to a continuous mapping $f : |K| \to |L|$, then $|\phi|$ is homotopic to f.*

11.3.16 Contiguous Mappings

Two simplicial mappings $\phi, \psi : K \to L$ are said to be *contiguous* if, for all simplices $S \in K$, the set $\phi(S) \cup \psi(S)$ is a simplex in L.

Lemma 11.3.2. *Suppose $f : |K| \to |L|$ is a continuous function for which $\phi, \psi : K \to L$ are simplicial approximations to f. Then ϕ and ψ are contiguous.*

Proposition 11.3.6. *Contiguous simplicial mappings have homotopic realizations.*

Theorem 11.3.3. *Suppose that f and g are continuous mappings $|K| \to |L|$ and f is homotopic to g. Then there exist simplicial mappings $\phi, \psi : sd^N K \to L$ with ϕ a simplicial approximation to f, ψ a simplicial approximation to g, and there is a sequence of simplicial mappings $\phi = \phi_0, \phi_1, \ldots, \phi_{n-1}, \phi_n = \psi$ with ϕ_i contiguous to ϕ_{i+1} for $0 \leq i \leq n-1$.*

12 Algebras

12.1 Definitions

Let R be a commutative ring. An *R-algebra* is a ring homomorphism $\alpha : R \to S$ such that $\alpha(R)$ is contained in the center of S.

12.2 Homomorphisms of R-algebras

A *homomorphism of R-algebras* is a ring homomorphism which is compatible with the algebra structure. That is, if M, N are R-algebras and $\varphi : M \to N$ is a function, then φ is a homomorphism of R-algrbras if and only if…

- $(\forall m_1 \in M)(\forall m_2 \in M) : \varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$;
- $(\forall m_1 \in M)(\forall m_2 \in M) : \varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2)$;
- $(\forall r \in R)(\forall m \in M) : \varphi(rm) = r\varphi(m)$.

12.3 Free Algebras

A free R-algebra on the set A, $F^{R-alg}(A)$, an R-algebra together with a set function $j : A \to F^{R-alg}(A)$ making the following diagram commute.

$$\begin{tikzcd} F^{R-alg}(A) \arrow[r, "\exists!\varphi"] & M \\ A \arrow[u, "j"] \arrow[ur, "f"'] & \end{tikzcd}$$

Proposition 12.3.1. *$R[A]$ is a free commutative R-algebra on the set A.*

Proof. We have to show that $R[A]$ satisfies the diagram above. Since S is an R-algebra, we have a fixed homomorphism of ring $\alpha : R \to S$. Then we may construct $\varphi : R[A] = R[x_1, \ldots, x_n] \to S$ by extending α n times: extending $R[x_1, \ldots, x_{n-1}]$ to $R[x_1, \ldots, x_n]$ mapping x_n to $f(n)$. Note that each extension is uniquely determined by its requirements.

It is fairly simple to show that φ is the required homomorphism past this point. ☐

12.3.1 Finite Type

The module M is of *finite type* if there is an onto homomorphism of R-algebras…

$$R[x_1, \ldots, x_n] \twoheadrightarrow S.$$

13 Topology

13.1 Topological Spaces

13.1.1 Topological Space

Let X be a set and $\mathcal{T}$ a collection of subsets of X called *open sets*. The collection $\mathcal{T}$ is called a *topology* on X if...

1. we have that $\emptyset \in \mathcal{T}$ and $X \in \mathcal{T}$,
2. the union of an arbitrary collection of memebers of $\mathcal{T}$ is in $\mathcal{T}$,
3. the finite intersection of members of $\mathcal{T}$ is in $\mathcal{T}$.

The pair $\langle X, \mathcal{T} \rangle$ is called a *(topological) space.*

13.1.1.1 Finer

Given two topologies $\mathcal{T}, \mathcal{T}'$ on a given set X we say $\mathcal{T}$ is *finer* than $\mathcal{T}'$ if $\mathcal{T}' \subseteq \mathcal{T}$.

13.1.1.2 Coarser

Given two topologies $\mathcal{T}, \mathcal{T}'$ on a given set X we say $\mathcal{T}$ is *coarser* than $\mathcal{T}'$ if $\mathcal{T} \subseteq \mathcal{T}'$.

13.1.2 Basis

A collection of subsets, $\mathcal{B}$, of a set X is a *basis for a topology on X* if

1. for all $x \in X$, there is a $B \in \mathcal{B}$ with $x \in B$,
2. $x \in B_1 \in \mathcal{B}$ and $x \in B_2 \in \mathcal{B}$, then there is some $B_3 \in \mathcal{B}$ with $x \in B_3 \subseteq B_1 \cap B_2$.

Proposition 13.1.1. *If $\mathcal{B}$ is a basis for a topology on a set X, then the collection of subsets...*

$$\mathcal{T}_{\mathcal{B}} = \{\bigcup_{\alpha \in A} B_\alpha | A \text{ is any index set and } B_\alpha \in \mathcal{B} \text{ for all } \alpha \in A\}$$

is a topology on X called the topology generated by the basis *$\mathcal{B}$.*

Proposition 13.1.2. *If $\mathcal{B}_1$ and $\mathcal{B}_2$ are bases for topologies on a set X, and for all $x \in X$ and $x \in B_1 \in \mathcal{B}_1$, there is a B_2 with $x \in B_2 \subseteq B_1$ and $B_2 \in \mathcal{B}_2$, then $\mathcal{T}_{\mathcal{B}_2}$ is finer than $\mathcal{T}_{\mathcal{B}_1}$.*

13.1.3 Continuity

Let $\langle X, \mathcal{T} \rangle$ and $\langle Y, \mathcal{T}' \rangle$ be topological spaces and $f : X \to Y$ a function. We say that f is *continuous* if whenever V is open in Y, $f^{-1}(V)$ is open in X.

Proposition 13.1.3. *If $\mathcal{T}$ and $\mathcal{T}'$ are topologies on a set X, then the identity mapping $id : \langle X, \mathcal{T} \rangle \to \langle X, \mathcal{T}' \rangle$ is continuous if and only if $\mathcal{T}$ is finer that $\mathcal{T}'$.*

Theorem 13.1.1. *Given two continuous functions $f : X \to Y$ and $g : Y \to Z$, the composite function $g \circ f : X \to Z$ is continuous.*

Theorem 13.1.2. *Let X, Y be topological space and $f : X \to Y$ a function. Then the following are equivalent:*

1. *f is continuous.*
2. *If K is closed in Y, then $f^{-1}(K)$ is closed in X.*
3. *If $A \subseteq X$, then $f(\text{cls } A) \subseteq \text{cls } f(A)$.*

Corollary 13.1.1. *If $f : X \to Y$ is a continuous function and $\{x_n\}$ is a sequence in X converging to x, then the sequence $\{f(x_n)\}$ converges to $f(x)$. Furthermore, if X is first countable, then the converse holds.*

13.1.3.1 Open Mappings

A continuous function $f : X \to Y$ such that $f(U) \subseteq Y$ is open when U is open in X.

13.1.4 Homeomorphism

A function $f : \langle X, \mathcal{T}_X \rangle \to \langle Y, \mathcal{T}_Y \rangle$ is a *homeomorphism* if f is continuous, bijective, and has a continuous inverse. In other words, a homeomorphism is an isomorphism in the category **Top**.

13.1.4.1 Homeomorphic Spaces

We say $\langle X, \mathcal{T}_X \rangle$ and $\langle Y, \mathcal{T}_Y \rangle$ are *homeomorphic topological spaces* if there is a homeomorphism $f : \langle X, \mathcal{T}_X \rangle \to \langle Y, \mathcal{T}_Y \rangle$.

13.2 Geometric Notions

13.2.1 Closed Subset

A subset K of X is *closed* if its complement in X is open.

13.2.2 Limit Point

If $A \subseteq X$, where X is a topological space and $x \in X$, then x is a *limit point* of A, if, whenever $U \subset X$ is open and $x \in U$, there is some $y \in U \cap A$, with $y \neq x$.

Proposition 13.2.1. *A subset K of a topological space $\langle X, \mathcal{T} \rangle$ is closed if and only if it contains all of its limit points.*

13.2.3 Interior

The *interior* of A is the largest open set contained in A, that is,

$$\text{int } A = \bigcup_{U \subseteq A, \text{open}} U.$$

13.2.4 Closure

The *closure* of A is the smalles closed set in X containing A, that is,

$$\text{cls } A = \bigcap_{K \supseteq A, \text{closed}} K.$$

Proposition 13.2.2. *If $A \subset X$, where X is a topological space, then $clsA = A \cup A'$, where…*

$$A' = \{\textit{limit points of } A\}.$$

A' is called the derived set *of A.*

13.2.5 Boundary

Let A be a subset of X, a topological space. A point $x \in X$ is in the *boundary* of A, if for any open set $U \subset X$ with $x \in U$, we have $U \cap A \neq \emptyset$ and $U \cap (X \setminus A) \neq \emptyset$. Thus…

$$\text{bdy } A = \{\text{boundary points of } A\}.$$

Proposition 13.2.3. cls $A =$ int $A \cup$ bdy A.

13.2.6 Convergence

A sequence $\{x_n\}$ of points in a topological space X is said to *converge to a point* $x \in X$, if for any open set U containing x, there is a positive integer N so that $x_n \in U$ whenever $n \geq N$.

The following lemma emerges out of the intuition of metric spaces…

Lemma 13.2.1 (The Sequence Lemma)**.** *If $A \subseteq X$, where X is a first countable space, then x is in* cls A *if and only if some sequence of points in A converges to x.*

Proof. If $\{x_n\}$ is a sequence of points in A converging to x, then any open set V containing x meets the sequence and we see either $x \in \mathit{int}\, A$ or $x \in \mathit{bdy}\, A$, so $x \in \mathit{cls}\, A$.

Converserly, if $x \in \mathit{cls}\, A$, consider the collection $\{U_i^x | i = 1, 2, \dots\}$ given by the condition of first countability. Then $A \cap U_1^x \cap \cdots \cap U_n^x$. The sequence $\{x_n\}$ converges to x: If V is open in X and $x \in V$, then there is U_j^x with $x \in U_j^x \subset V$. But then $A \cap U_1^x \cap \cdots \cap U_m^x \subseteq U_j^x \subseteq V$ for all $m \geq j$, and so $x_m \in V$ for $m \geq j$. ∎

13.3 Separation

13.3.1 T1

A topological space X satisfies the T_1 axiom if given two points $x, y \in X$, there are open sets U, V with $x \in U, y \notin U$ and $y \in V, x \notin V$.

Proposition 13.3.1. *A space X satisfies the T_1 axiom if and only if any finite subset of points in X is closed.*

13.3.2 Hausdorff (T2)

A topological space is said to satisfy the *Hausdorff condition* if given two points $x, y \in X$ there are open set U, V with $x \in U, y \in V$, and $U \cap V = \emptyset$.

Theorem 13.3.1. *In a Hausdorff space, the limit of a sequence is unique.*

13.3.3 Separable

13.3.3.1 Dense

A subset A of a topological space X is *dense* if cls $A = X$.

13.3.3.2 Definition

A topological space is *separable (or Fréchet)* if it has a countable dense subset.

Theorem 13.3.2. *A seperable metric space is second countable.*

Proof. Suppose A is a countable dense subset of $\langle X, d\rangle$. Consider the collection of open balls...

$$\{B(a, p/q)|a \in A, p/q > 0, p/q \in \mathbb{Q}\}.$$

If U is an open set in X and $x \in U$, then there is an $\varepsilon > 0$ with $B(x, \varepsilon) \subseteq U$. Since cls $A = X$, there is a point $a \in A \cap B(x, \varepsilon/2)$. Consider $B(a, p/q)$ where p/q is rational and $d(a, x) < p/q < \varepsilon/2$. Then $x \in B(a, p/q)$ where p/q is rational and $d(a, x) < p/q < \varepsilon/2$. Then $x \in B(a, p/q) \subset B(x, \varepsilon) \subseteq U$. Repeat this procedure for each $x \in U$ to show $U \subseteq \bigcup_a B(a, p/q) \subseteq U$ and this collection of open balls is a basis for the topology on X. The collection is countable since a countable union of countable sets is countable. □

13.4 Connectedness

13.4.1 Disconnected

A space X is *disconnected* by a separation $\{U, V\}$ if U and V are open, nonempty, and disjoint ($U \cap V = \emptyset$) subsets of X with $X = U \cup V$.

13.4.2 Connected

A space X exists is it has no separations.

Theorem 13.4.1. *A space X is connected if and only if whenever $X = A \cup B$ with A, B nonempty, then $A \cap (\text{cls } B) \neq \emptyset$ or $(\text{cls } A) \cap B \neq \emptyset$.*

Theorem 13.4.2. *If $f : X \to Y$ is continuous and X is connected, then $f(X)$, the image of X in Y, is connected.*

Lemma 13.4.1. *If $\{A_i | i \in J\}$ is a collection of connected subspaces of a space X with $\bigcap_{i \in J} A_i \neq \emptyset$, then $\bigcup_{i \in J} A_i$ is connected.*

Proposition 13.4.1. *If $W \subseteq (\mathbb{R}, \text{ usual})$ is connected, then $W = (a, b), [a, b), (a, b], [a, b]$ for $-\infty \leq a \leq b \leq \infty$.*

Proposition 13.4.2. *If A is a connected subspace of a space X and $A \subseteq B \subseteq \text{cls } A$, then B is connected.*

13.4.3 Connected Component

Define an equivalence relation on a space X as $x \sim y \Leftrightarrow x \in A$ and $y \in A$ where A is a connected subset of X. An equivalence class $[x]$ under this relation is called a *connected componenet* of X.

13.4.4 Path Connected

A space X is *path-connected* if, for any $x, y \in X$, there is a continuous function $\lambda : [0, 1] \to X$ with $\lambda(0) = x$, $\lambda(1) = y$. Such a function λ is called a *path* joining x to y in X.

Proposition 13.4.3. *If X is path-connected, then it is connected.*

Theorem 13.4.3. *If X is path-connected and $f : x \to Y$ is continuous, then $f(X) \subseteq Y$ is path-connected.*

Lemma 13.4.2. *If $\{A_i | i \in J\}$ is a collection of path-connected subsets of a space X and $\bigcap_{i \in J} A_i \neq \emptyset$, then $\bigcup_{i \in J} A_i$ is path-connected.*

13.4.4.1 Path Component

Define an equivalence relation on a space X as $x \approx y$ if and only if there is a path $\lambda : [0, 1] \to X$ with $\lambda(0) = x$ and $\lambda(1) = y$. An equivalence class under this relation is called a *path component*.

The *set of path components* $\pi_0(X)$ is the set of equivalence classes under the relation $\approx$. If $f : X \to Y$ is a continuous function, then f induces a well-defined mapping $\pi_0(f) : \pi_0(X) \to \pi_0(Y)$, given by $\pi_0(f)([x]) = [f(x)]$.

13.4.5 Locally Path-Connected

A space X is *locally path-connected* if, for every $x \in X$ and $x \in U$ an open set in X, there is an open set $V \subseteq X$ with $x \in V \subseteq U$ and V path-connected.

Proposition 13.4.4. *If X is locally path-connected, then path components of X are open.*

Corollary 13.4.1. *If X is connected and locally path-connected, then it is path-connected.*

13.5 Compactness

Given a topological space X and a subset $K \subseteq X$, a collection of subsets $\{C_i \subseteq X | i \in J\}$ is a *cover* of K if $K \subseteq \bigcup_{i \in J} C_i$. A cover is an *open cover* if every C_i is open in X. The cover $\{C_i | i \in J\}$ of K has a *finite subcover* if ther are members of the collection $C_{i_1}, \ldots, C_{i_n}$ with $K \subseteq C_{i_1} \cup \cdots \cup C_{i_n}$. A subset $K \subseteq X$ is compact if any open cover of K has a finite subcover.

Theorem 13.5.1 (THe Heine-Borel Theorem)**.** *The closed interval* $[0, 1]$ *is a compace subspace of* $(\mathbb{R},$ *usual*$)$*.*

Proof. Suppose $\{U_i | i \in J\}$ is an open cover of $[0, 1]$. Define...

$$T = \{x \in [0, 1] | [0, x] \text{ has a finite subcover from } \{U_i\}\}.$$

Certainly $0 \in T$ since $0 \in \bigcup U_i$ and so in some U_j. We show $1 \in T$. Since every element of T is less than or equal to 1, T has a least upper bound s. Since $\{U_i\}$ is a cover of $[0, 1]$, $s \in U_j$ for some $j \in J$. Since U_j is open, $(s - \varepsilon, s + \varepsilon) \subseteq U_j$ for some $\varepsilon > 0$. Because s is a least upper bound, $s - \delta \in T$ for some $0 < \delta < \varepsilon$ and so $[0, s - \delta]$ has a finite subcover. It follows that $[0, s]$ has a finite subcover by simply adding U_j to the finite subcover of $[0, s - \delta]$. If $s < 1$, then there is an $\eta > 0$ with $s + \eta \in (s - \varepsilon, s + \varepsilon) \cap [0, 1]$, and so $s + \eta \in T$, which contradicts the fact that s is a least upper bound. Hence $s = 1$. □

Theorem 13.5.2. *If $f : X \to Y$ is a continuous function and X is compact, then $f(X) \subseteq Y$ is compact.*

Proposition 13.5.1. *If X is a compact space and $K \subseteq X$ is a closed subset, then K is compact.*

Proposition 13.5.2. *If X is Hausdorff and $K \subseteq X$ is compact, then K is closed in X.*

Corollary 13.5.1. *If $K \subseteq \mathbb{R}^n$ is compact, K is closed and bounded.*

Theorem 13.5.3 (The Extreme Value Theorem)**.** *If $f : X \to \mathbb{R}$ is a continuous function and X is compact, then there are points $x_m, x_M \in X$ with $f(x_m) \leq f(x) \leq f(x_M)$ for all $x \in X$.*

Proof. By 13.5.2, $f(X)$ is a compact subset of $\mathbb{R}$ and so $f(X)$ is closed and bounded. The boundedness implies that the greatest lower bound of $f(X)$ and the least upper bound of $f(X)$ exist. Since $f(X)$ is closed, the values $\text{glb} f(X)$ and $\text{lub} f(X)$ are in $f(X)$ and so $\text{glb} f(X) = f(x_m)$ for some $x_m \in X$; also $\text{lub} f(X) = f(x_M)$ for some $x_M \in X$. It follows that $f(x_m) \leq f(x) \leq f(x_M)$ for all $x \in X$. $\square$

Proposition 13.5.3. *if $R = \{x_\alpha | \alpha \in J\}$ is an infinite subset of a compact space X, then R has a limit point.*

Proposition 13.5.4 (Greatest Theorem of Elementary Topology)**.** *If $f : X \to Y$ is a continuous bijection, X is compact, and Y is Hausdorff, the f is a homeomorphism.*

13.5.1 Locally Compact

A space X is *locally compact* if for any $x \in U \subset X$, where U is an open set, there is an open set V satisfying $x \in V \subseteq \text{cls}\, V \subseteq U$ with $\text{cls}\, V$ compact.

13.6 Constructions

13.6.1 Subspace Topology

Let X be a topological space with topology $\mathcal{T}$ and A, a subset of X. The *subspace topology* on A is given by $\mathcal{T}_A = \{U \cap A | U \in \mathcal{T}\}$.

Proposition 13.6.1. *The collection $\mathcal{T}_A$ is a topology on A and with this topology the inclusion $\iota : A \to X$ is continuous.*

Proposition 13.6.2. *Suppose $X = A \cup B$ is a space, A, B are open subsets of X, and $f : A \to Y$, $g : B \to Y$ are continuous functions (where A and B have the subspace topologies). If $f(x) = g(x)$ for all $x \in A \cap B$, then $F = f \cup g : X \to Y$ is a continuous function, where F is defined by...*

$$F(x) = \begin{cases} f(x), & \text{if } x \in A, \\ g(x), & \text{if } x \in B. \end{cases}$$

13.6.2 Product Topology

Given topological spaces X and Y, the set $X \times Y$ is a topological space under the topology generated by the basis...

$$\mathcal{B} = \{U \times V | U \text{ open in } X, V \text{ open in } Y\}.$$

Proposition 13.6.3. *Given three topological spaces X, Y, and Z, and a function $f : Z \to X \times Y$, then f is continuous if and only if $\pi_1 \circ f : Z \to X$ and $\pi_2 \circ f : Z \to Y$ are continuous.*

Proposition 13.6.4. *If X and Y are separable spaces, so is $X \times Y$.*

Proposition 13.6.5. *If X and Y are connected spaces, then $X \times Y$ is connected.*

Proposition 13.6.6. *If X and Y are path-connected, then so is $X \times Y$.*

Proposition 13.6.7. *If X and Y are compact spaces, then $X \times Y$ is compact.*

Corollary 13.6.1. *If $K \subseteq \mathbb{R}^n$, then K is compact if and only if K is closed and bounded.*

13.6.2.1 Infinite Product Topology

For a family of sets $\{X_\alpha\}_{\alpha \in J}$, the set $\prod_{\alpha \in J} X_\alpha$ is a topological space under the following two topologies...

- $\mathcal{T}_{box}$, the topology generated by the basis:

$$\mathcal{B} = \{\prod_{\alpha \in J} U_\alpha | U_\alpha \subset X_\alpha \text{ for all } \alpha, \text{ each } U_\alpha \text{ open in } X_\alpha\}.$$

- $\mathcal{T}_{prod}$, the topology generated by the basis:

$$\mathcal{B} = \{S_1 \cap S_2 \cap \cdots \cap S_n | n \geq 1, S_i \in \mathcal{S}\},$$

  where $\mathcal{S}$ is the subbasis of subseets $S \ \prod_{\alpha \in J} V_\alpha$, where for each $\beta \in J$, V_β is open in X_β and $V_\gamma = X_\gamma$ for all but finitely many $\gamma \in J$.

Proposition 13.6.8. *Let X be a space and for all $\alpha \in J$, let $X_\alpha = X$. Define the function...*

$$\Delta : X \to \prod_{\alpha \in J} X_\alpha$$

by $\Delta(x) : \alpha \mapsto x \in X_\alpha = X$. This function is continuous when $\prod_{\alpha \in J} X_\alpha$ has the product topology.

This proposition highlights the difference between $\mathcal{T}_{box}$ and $\mathcal{T}_{prod}$. Consider $\Delta : (\mathbb{R}, \text{usual}) \to (\mathbb{R}^\omega, \mathcal{T}_{box})$. Let...

$$W = (-1, 1) \times (-1/2, 1/2) \times (-1/3, 1/3) \times \cdots$$

be an open set in $\mathcal{T}_{box}$. Then $\Delta^{-1}(W) = \{0\}$, which is not open.

13.6.3 Quotient Topology

A subset $V \subset [X]$ is open in the *quotient topology* on $[X]$ if $\pi^{-1}(V)$ is open in X. The space $[X]$ with this topology is called a *quotient space* of X.

13.6.3.1 Quotient Map

An surjective map $f : X \to Y$ is called a *quotient map* when V is open in Y if and only if $f^{-1}(V)$ is open in X.

Theorem 13.6.1. *Let $\sim$ be an equivalence relation in a space X that is Hausdorff. Then $[X]$ is Hausdorff if and only if the graph of $\sim$, $\{(x, y) | x \sim y, x, y \in X\}$, is closed in $X \times X$.*

13.7 Examples

13.7.1 Topology Examples

13.7.1.1 Indiscrete Topology

For any set X, $\mathcal{T} = \{\emptyset, X\}$.

13.7.1.2 Discrete Topology

For any set X, $\mathcal{T} = \mathcal{P}(X)$.

13.7.1.3 Order Topology

Let X be a nonempty, linearly ordered set. Let $\mathcal{B}$ be the collection of all sets of the following types:

1. All open intervals (a, b) in X.
2. All intervals of the form $[a_0, b)$, where a_0 is the smallest element (if any) of X.
3. All intervals of the form $(a, b_0]$, where b_0 is the largest element (if any) of X. The collection $\mathcal{B}$ is a basis for a topology on X, which is called the *order topology.*

13.7.1.4 Finite Complement Topology

Given an infinte set X, define $\mathcal{T}_{FC} = \{U \subseteq X | U = \emptyset \text{ or } X \setminus U \text{ is finite}\}$.

13.7.1.5 Included Point Topology

Let X be a pointed set with $x_0 \in X$ the chosen point. Then we can define a topology...

$$\mathcal{T}_{IP} = \{\emptyset \text{ or } U \subset X \text{ with } x_0 \in U\}.$$

In this space, a constant sequence converses to every point except x_0.

13.7.1.6 Compact-open Topology

Suppose $K \subseteq X$ and $U \subseteq Y$. Let $S(K, U) = \{f : X \to Y, \text{ continuous with } f(K) \subseteq U\}$. The collection $\mathcal{S} = \{S(K, U) | K \subseteq X \text{ compact}, U \subseteq Y \text{ open}\}$ is a subbasis for the topology $\mathcal{T}_{\mathcal{S}}$ on $\mathrm{Hom}(X, Y)$ called the *compact-open topology.* We denoted the space $(\mathrm{Hom}(X, Y), \mathcal{T}_{\mathcal{S}})$ as $\mathrm{map}(X, Y)$.

Theorem 13.7.1. *The following apply to map(X, Y)...*

1. *If X is locally compact and Hausdorff, then the evaluation mapping...*

$$e : X \times map(X, Y),\ e(x, f) = f(x),$$

is continuous.

2. *If X is locally compact and Hausdorff and Z is another space, then a function $F : X \times Z \to Y$ is continuous if and only if its adjoint map $\hat{F} : Z \to map(X, Y)$, defined by $\hat{F}(z)(x) = F(x, z)$, is continuous.*

13.7.2 Space Examples

13.7.2.1 Torus

Define $A = \{0\} \times [0,1] \cup [0,1] \times \{0\}$ and $B = \{1\} \times [0,1] \cup [0,1] \times \{1\}$; then take the mapping $h : A \to B$ by $h((0,t)) = (1,t)$ and $h((t,0)) = (t,1)$. Define $\forall (u,v),(u',v') \in I^2$ the equivalence relation $(u,v) \sim_h (u',v') \Leftrightarrow f(u,v) = (u',v')$ or $f(u',v') = (u,v)$. Then the torus is $I^2/\sim_h$.

Alternatively, if we consider the torus as $T^2 = S^1 \times S^1$, we can define a function $f : I^2 \to T^2$ as $(u,v) \mapsto (e^{2\pi i u}, e^{2\pi i v}) \in S^1 \times S^1$. Since $e^{2\pi i 0} = e^{2\pi i 1}$ we get $f(u,v) = f(u',v')$ if and only if $(u,v) \sim_h (u',v')$. This leads to a homeomorphismj $\hat{f} : [I^2]_h \to T^2$ via universal properties.

13.7.2.2 Möbius Strip

Let $A = \{0\} \times [0,1]$, $B = \{1\} \times [0,1]$ and $h : A \to B$, $(0,t) \mapsto (1, 1-t)$. Then $[I^2]_h$ represents the Möbius band.

13.7.2.3 Projective Space

The space $[S^n]$ where $x \sim \pm x$. Denoted $\mathbb{R}P^n$.

13.7.2.4 Cone

The *cone* on a topological space X is given by $[X \times [0,1]]$ where $(x,t) \sim (x',t')$ if $(x,t) = (x',t')$ or $x, x' \in X$ and $t = t' = 0$. We write $CX = [X \times [0,1]]$ for the cone on X.

13.7.2.5 Suspension

The *suspension* of X, denoted $\sum X$, is the quotient of $X \times [0,1]$, where we identify the subsets $X \times \{0\}$ and $X \times \{1\}$ each to a point.

Proposition 13.7.1. *The $(n+1)$-sphere S^{n+1} is homeomorphic to $\sum S^n$.*

Proof. Consider the function $\sigma : S^n \times [0,1] \to S^{n+1}$ given by...

$$\sigma(x_0, \ldots, x_n, t) = (\sqrt{1-(1-2t)^2}x_0, \ldots \sqrt{1-(1-2t)^2}x_n, 1-2t).$$

This function is continuous as the calculus tells us. Notice that... $\sigma(x_0, \ldots, x_n, 0) = (0, 0, \ldots, 0, 1)$, $\sigma(x_0, \ldots, x_n, 1) = (0, 0, \ldots, -1)$. Thus σ factors through $[S^n \times [0,1]] = \sum S^n$.

$$\begin{tikzcd} S^n \times [0,1] \arrow[r, "\sigma"] \arrow[d, "\pi"] & S^{n+1} \\ \pi(S^n \times [0,1]) \arrow[ur, "\hat{\sigma}"'] & \end{tikzcd}$$

The function $\hat{\sigma}$ is a bijection away from the 'poles' $(0,\dots,0,\pm 1)$. The classes remaining, $[S^n \times \{0\}]$ and $[S^n \times \{1\}]$, each go to the respecitve poles. To finish the proof we only need to show that σ is a quotient map. Let $S^n \times [0,1]$ get its topology as a subspace of $\mathbb{R}^{n+2}$. A basic open set in $S^n \times [0,1]$ takes the form $W = (S^n \times [0,1]) \cap [(a_1,b_1) \times \cdots \times (a_{n+2}, b_{n+2})]$. Restricting (or extending) σ to W takes it to an open set and the image is easily determined to be the intersection of $\sigma(W)$ with S^{n+1}. Thus σ is open. $\square$

13.7.2.6 Pointed Suspension

The *pointed suspension* (SX, sx_0) has $[sx_0] = X \times \{0\} \cup X \times \{1\} \cup x_0 \times [0,1]$, and the rest of the equivalence classes are the same as $\sum X$.

Proposition 13.7.2. *There is a bijection between set...*

$$Hom((SX, sx_0), (Y, y_0)) \cong Hom((X, x_0), Hom((S^1, 1), (Y, y_0))).$$

Proof. Let $f : (SX, sx_0) \to (Y, y_0)$. Untangling the suspension coordinate we can write f in the composite...

$$X \times [0,1] \xrightarrow{\pi} SX \xrightarrow{f} Y$$

and for each $x \in X$ associate the mapping $x \mapsto \tilde{f}(t) = f \circ \pi(x,t)$. It follows that $\tilde{f}(0) = \tilde{f}(1) = f(sx_0) = y_0$ by the definition of the canoncial projection for the equivalence relation. The inverse is as follows: given $F : (X, x_0) \to \mathrm{Hom}((S^1, 1), (Y, y_0))$, then define $\hat{F} : (SX, sx_0) \to (Y, y_0)$ by $\hat{F}(x,t) = F(x)(e^{2\pi i t})$. An explicit calculation shows these processes to be inverses and the proposition is proved. $\square$

13.7.2.7 One-point Compactification

Let X be a locally compact, Hausdorff space. Adjoin a point not in X, denoted by ∞, to form $Y = X \cup \{\infty\}$. Topologize Y by two kinds of open sets:

1. $U \subseteq X \subseteq Y$ and U is open in X.
2. $Y \setminus K$, where K is compact in X.

The space Y with this topology is called the *one-point compactification* of X.

Theorem 13.7.2. *If X is locally compact and Hausdorff, X is not compact, and $Y = X \cup \{\infty\}$ is the one-point compactification, then Y is a compact Hausdorff space, X is a subspace of Y, and* $\mathrm{cls} X = Y$.

13.8 Topological Properties

A property of a space $\langle X, \mathcal{T}_X \rangle$ is said to be a *topological property* if, whenever $\langle Y, \mathcal{T}_Y \rangle$ is homeomorphic to $\langle X, \mathcal{T}_X \rangle$, then the space $\langle Y, \mathcal{T}_Y \rangle$ also has the property.

13.8.1 First Countable

A topological space is *first countable* if for each $x \in X$ there is a collection of open sets $\{U_i^x | i = 1, 2, 3, \dots\}$ such that, for any V open in X with $x \in V$, there is one of these open sets U_j^x with $x \in U_j^x \subseteq V$.

13.8.2 Second Countable

A space that has a countable set as a basis for its topology.

13.8.3 Connectedness

Connectedness is a topological property.

13.8.4 Connected Componenents

The cardinality of the set of connected components of a space X is a topological invariant.

13.8.5 Path-connectedness

Path-connectedness is a topological property.

13.8.6 Fundamental Group

The fundamental group is a topological invariant of a space.

13.9 Hereditary

A given property is *hereditary* if in a given topological space X with such a property each of its subsets A also has the same property under the subspace topology.

Proposition 13.9.1. *Metrizability is hereditary.*

Proposition 13.9.2. *The Hausdorff condition is hereditary.*

14 Metric Spaces

14.1 Definition

A *metric space* $\langle X, d\rangle$ is a set X together with a *metric* $d : X \times X \to \mathbb{R}$ satisfying...

1. $d(x, y) \geq 0$ for all $x, y \in X$ and $d(x, y) = 0$ if and only if $x = y$.
2. $d(x, y) = d(y, x)$ for all $x, y \in X$.
3. (*The Triangle Inequality*): $d(x, y) + d(y, z) \geq d(x, z)$ for all $x, y, z \in X$.

14.1.1 Open Ball

The *open ball* of radius $\varepsilon > 0$ centered at a point x in a metric space $\langle X, d\rangle$ is given by...

$$B_\varepsilon(x) = \{y \in X | d(x, y) < \varepsilon\}.$$

Open balls form the basis for a topology on X called the *metric topology.*

A set U of a metric space (X, d) is *open* if for any $u \in U$, there is $\varepsilon > 0$ so that $B_\varepsilon(x) \subseteq U$.

14.1.2 Bounded

A subset A of a metric space (X, d) is *bounded* if there is some number M such that...

$$d(a_1, a_2) \leq M$$

for every pair a_1, a_2 of points of A.

If A is bounded and nonempty, the *diameter* of A is defined to be the numbed...

$$\text{diam } A = \sup\{d(a_1, a_2) | a_1, a_2 \in A\}.$$

14.1.3 Continuity

Suppose $\langle X, d_X\rangle$ and $\langle Y, d_Y\rangle$ are two metric spaces and $f : X \to Y$ is a function. Then f is *continuous at* $x \in X$ if for any $\epsilon > 0$, there is a $\delta > 0$ so that $B_\delta(x) \subset f^{-1}(B_\varepsilon(f(x)))$.

The function f is *continuous* if it is continous at x for all $x \in X$.

Theorem 14.1.1. *A function $f : X \to Y$ between metric spaces $\langle X, d\rangle$ and $\langle Y, d\rangle$ is continuous if and only if for any open subset V of Y, the subset $f^{-1}(V)$ is open in X.*

14.2 Examples

14.2.1 Euclidean Metric Space

If for $x, y \in \mathbb{R}^n$...

$$d(x,y) = ||x-y|| = \sqrt{(x_1-y_1)^2 + \cdots + (x_n-y_n)^n},$$

then $\langle \mathbb{R}^n, d \rangle$ is a metric space.

14.2.2 Box Metric Space

If for $x, y \in \mathbb{R}^n$...

$$d(x,y) = \max\{|x_1-y_1|, \ldots, |x_n-y_n|\},$$

then $\langle \mathbb{R}^n, d \rangle$ is a metric space. The metric d is also called the *square metric*

The set of open balls for the previous two metrics form bases that generate the same topology.

14.2.3 Standard Bounded Metric corresponding to a metric

Let X be a metric space with metric d. Define $\overline{d} : X \times X \to \mathbb{R}$ by the equation...

$$\overline{d}(x,y) = \min\{d(x,y), 1\}.$$

Then $\overline{d}$ is a metric that induces the same topology as d.

14.2.4 Bounded Real Functions Metric Space

Let $\mathrm{Bdd}([0,1], \mathbb{R})$ denote the set of *bounded functions* $f : [0,1] \to \mathbb{R}$. If for $f, g \in \mathrm{Bdd}([0,1], \mathbb{R})$...

$$d(f,g) = \mathrm{lub}_{t \in [0,1]}\{f(t) - g(t)\},$$

then $\langle \mathrm{Bdd}([0,1], \mathbb{R}), d \rangle$ is a metric space.

14.2.5 Discrete Metric space

Let X be any set and define...

$$d(x,y) = \begin{cases} 0, & \text{if } x = y, \\ 1, & \text{if } x \neq y. \end{cases}$$

Then $\langle X, d \rangle$ is a metric space.

14.3 Convergence

We can use the sequence lemma to prove the following...

Theorem 14.3.1. *Let $f : X \to Y$. If the function f is continuous, then for every convergent sequence $x_n \to x$ in X, the sequence $f(x_n)$ converges to $f(x)$. The converse holds if X is metrizable.*

As in the sequence lemma, we only need to assume the first countability axiom to prove the converse.

14.3.1 Uniform Convergence

Let $f_n : X \to Y$ be a sequence of functions form the set X to the metric space Y. Let d be the metric for Y. We say that the sequence (f_n) *converges uniformly* to the function $f : X \to Y$ if given $\varepsilon > 0$, there exists an integer N such that...

$$d(f_n(x), f(x)) < \varepsilon$$

for all $n > N$ and all x in X.

Theorem 14.3.2 (Uniform Limit Theorem). *Let $f_n : X \to Y$ be a sequence of continuous functions from the topological space X to the metric space Y. If (f_n) converges uniformly to f, then f is continuous.*

Proof. Let V be open in Y; let x_0 be a point of $f^{-1}(V)$. We wish to find a neighborhood U of x_0 such that $f(U) \subseteq V$.

Let $y_0 = f(x_0)$. First choose ε so that $B_\varepsilon(y_0)$ is contained in V. Then using uniform convergence, choose N so that for all $n \geq N$ and all $x \in X$,

$$d(f_n(x), f(x)) < \varepsilon/3.$$

Finally, using continuity fo f_N, choose a neighborhood U of x_0 such that f_N carries U into the $\varepsilon/3$ ball in Y centered at $f_N(x_0)$.

We claim that f carries U into $B(y_0, \varepsilon)$ and hence into V, as desired. For this purpose, note that if $x \in U$, then...

$$d(f(x), f_N(x)) < \varepsilon/3 \text{ (by choice of } N\text{)},$$

$$d(f_N(x), f_N(x_0)) < \varepsilon/3 \text{ (by choice of } U\text{)},$$

$$d(f_N(x_0), f(x_0)) < \varepsilon/3 \text{ (by choice of } N\text{)}.$$

Adding and using the triangle inequality, we see that $d(f(x), f(x_0)) < \varepsilon$, as desired. □

14.3.2 Lebesgue's Lemma

14.3.2.1 Diameter

The *diameter* of a subset A of a metric space X is defined by diam $A = \sup\{d(x,y)|x,y \in A\}$.

Lemma 14.3.1 (Lebesgue's Lemma)**.** *Let X be a compact metric space and $\{U_i|i \in J\}$ an open cover. Then there is a real number $\delta > 0$ (*the Lebesgue number*) such that any subset of X of diameter less than δ is contained in some U_i.*

Proof. Define the continuous function $d(-,A) : X \to \mathbb{R}$ by $d(x,A) = \inf\{d(x,a)|a \in A\}$. In addition, if A is closed, then $d(x,A) > 0$ for $x \notin A$. Fiven an open cover $\{U_i|i \in J\}$ of the compact space X, there is a finite subcover $\{U_{i_1},\ldots,U_{i_n}\}$. Define $\varphi_j(x) = d(x, X \setminus U_{i_j})$ for $j = 1,2,\ldots,n$ and let $\varphi(x) = \max\{\varphi_1(x),\ldots,\varphi_n(x)\}$. Since each $x \in X$ lies in some U_{i_j}, $\varphi(x) \geq \varphi_j(x) > 0$. Furthermore, φ is continuous so $\varphi(X) \subseteq \mathbb{R}$ is compact, and $0 \notin \varphi(X)$. Let $\delta = \min\{\varphi(x)|x \in X\} > 0$. FOr any $x \in X$, consider $B(x,\delta) \subseteq X$. We know $\varphi(x) = \varphi_j(x)$ for some j. For that j, $d(x, X \setminus U_{i_j}) \geq \delta$, which implies $B(x,\delta) \subseteq U_{i_j}$. □

14.4 Compactness

15 Real Analysis

15.1 The Real Numbers

15.2 Consequences of Connectedness

15.2.1 Linear Continuum

A nonempty, linearly ordered set L having more than one element is called a *linear continuum* if the following hold:

1. L has the least upper bound property.
2. If $x < y$, there exists z such that $x < z < y$.

Theorem 15.2.1. *If L is a linear continuum in the order topology, then L is connected, and so are intervals and rays in L.*

Proof. A subspace Y of L is said to be *convex* if for every pair of points a, b in Y with $a < b$, the entire interval $[a, b]$ of points of L lies in Y. We prove that if Y is a convex subspace of L, then Y is connected.

So suppose that Y is the union of the disjoint nonempty sets A and B, each of which is open in Y. Choose $a \in A$ and $b \in B$; suppose for convenience that $a < b$. The interval $[a, b]$ of points of L is contained in Y. Hence $[a, b]$ is the union of the disjoint sets...

$$A_0 = A \cap [a, b] \text{ and } B_0 = B \cap [a, b],$$

each of which is open in $[a, b]$ in the subspace topology, which is the same as the order topology. The sets A_0 and B_0 are nonempty because $a \in A_0$ and $b \in B_0$. Thus, A_0 and B_0 constitute a separation of $[a, b]$.

Let $c = \sup A_0$. We show that c belongs neither to A_0 nor to B_0, which contradicts the fact that $[a, b]$ is the union of A_0 and B_0.

Case I. Suppose $c \in B_0$. Then $c \neq a$, so either $c = b$ or $a < c < b$. In either case, it follows from the fact that B_0 is open in $[a, b]$ that there is some interval of the form $(d, c]$ contained in B_0. If $c = b$, we have a contradiction at once, for d is a smaller upper bound on A_0 that c. If $c < b$, we note that $(c, b]$ does not intersect A_0 (because c is an upper bound on A_0). Then...

$$(d, b] = (d, c] \cup (c, b]$$

does not interset A_0. Again, d is a smaller upper bound on A_0 than c, contrary to construction.

Case II. Suppose that $c \in A_0$. Then $c \neq b$, so either $c = a$ or $a < c < b$. Because A_0 is open in $[a, b]$, there must be some interval of the form $[c, e)$ contained in A_0. Because of the order property (2) of the linear continuum L, we can choose a point z of L such that $c < z < e$. Then $z \in A_0$, contrary to the fact that c is an upper bound for A_0. □

Corollary 15.2.1. *The real line $\mathbb{R}$ is connected and so are intervals and rays in $\mathbb{R}$.*

15.2.2 Intermediate Value Theorem

Theorem 15.2.2 (Intermediate Value Theorem)**.** *If $f : [a, b] \to \mathbb{R}$ is continuous function and $f(a) < c < f(b)$ or $f(a) > c > f(b)$, then there is a value $x_0 \in [a, b]$ with $f(x_0) = c$.*

Corollary 15.2.2. *Suppose $g : S^1 \to \mathbb{R}$ is continuous. Then there is a point $x_0 \in S^1$ with $g(x_0) = g(-x_0)$.*

Proof. Define $\hat{g} : S^1 \to \mathbb{R}$ by $\hat{g} = g(x) - g(-x)$. Wrap $[0, 1]$ onto S^1 by $w(t) = (\cos(2\pi t), \sin(2\pi t))$. Then $w(0) = -w(1/2)$.

Let $F = \tilde{g} \circ w$. It follows that...

$$\begin{aligned} F(0) = \tilde{g}(w(0)) &= g(w(0)) - g(-w(0)) \\ &= -[g(-w(0)) - g(w(0))] \\ &= -[g(w(1/2)) - g(-w(1/2))] \\ &= -F(1/2). \end{aligned}$$

If $F(0) > 0$, then $F(1/2) < 0$ and since F is continuous, it must take the value 0 for some t between 0 and $1/2$. Similarly for $F(0) < 0$. If $F(t) = 0$, then let $x_0 = w(t)$ and $g(x_0) = g(-x_0)$. $\square$

16 Homotopy

16.1 Definition

16.1.1 Homotopy of functions

A *homotopy* between functions $f, g : X \to Y$ is a continuous function $H : X \times [0,1] \to Y$ with $H(x,0) = f(x)$, $H(x,1) = g(x)$. We say that f is *homotopic* to g if there is a homotopy between them, denoted $f \simeq g$. (See: Compact Open Topology)

Proposition 16.1.1. *Suppose that X is a locally compact and Hausdorff space.*

1. *If $(Hom(X,Y), \mathcal{T})$ is another topology on $Hom(X,Y)$ and the evaluation map...*

$$e : X \times (Hom(X,Y), \mathcal{T}) \to Y$$

is continuous, then $\mathcal{T}$ contains the compact-open topology.

2. *If Y is locally compact and Hausdorff, then the composition of functions...*

$$\circ : map(X,Y) \times map(Y,Z) \to map(X,Z)$$

is continuous.

3. *If Y is Hausdorff, then the space $map(X,Y)$ is Hausdorff.*

Theorem 16.1.1. *Homotopy is an equivalence relation on $Hom_{\mathrm{Top}}(X,Y)$.*

Proposition 16.1.2. *Continuous mappings $F : W \to X$ and $G : Y \to Z$ induce well-defined functions $F^* : [X,Y] \to [W,Y]$ and $G_* : [X,Y] \to [X,Z]$ by $F^*([h]) = [h \circ F]$ and $G_*([h]) = [G \circ h]$ for $[h] \in [X,Y]$.*

16.1.2 Space of Based Loops

Suppose X is a space and $x_0 \in X$ is a choice of base point in X. The *space of based loops* in X is the subspace of $\mathrm{map}([0,1], X)$...

$$\Omega(X, x_0) = \{\lambda \in \mathrm{map}([0,1], X) | \lambda(0) = \lambda(1) = x_0\}.$$

Composition of loops determines a binary operation $* : \Omega(X,x_0) \times \Omega(X,x_0) \to \Omega(X,x_0)$.

16.1.2.1 Loop Homotopy

Given two based loops λ and μ, a *loop homotopy* between them is a homotopy of paths $H : [0,1] \times [0,1] \to X$ with $H(t,0) = \lambda(t)$, $H(t,1) = \mu(t)$, and $H(0,s) = H(1,s) = x_0$. That is, for each $s \in [0,1]$, the path $t \mapsto H(t,s)$ is a loop at x_0.

Theorem 16.1.2. *Loop homotopy is an equivalence relation on $\Omega(X, x_0)$.*

$\pi_1(X, x_0) = [\Omega(X, x_0)]$ denotes the set of equivalence classes under loop homotopy.

16.2 Fundamental Group

Theorem 16.2.1. *Composition of loops induces a group structure on* $\pi_1(X, x_0)$ *with identity element* $[s_{x_0}(t)]$ *and inverses given by* $[\lambda]^{-1} = [\lambda^{-1}]$.

$\pi_1(X, x_0)$ is called the *fundamental group of* X *at the base point* x_0.

Theorem 16.2.2. *Let* (X, x_0) *and* (Y, y_0) *be pointed spaces. Then* $\pi_1(X \times Y, (x_0, y_0))$ *is isomorphic to* $\pi_1(X, x_0) \times \pi_1(Y, y_0)$*, the direct product of these two groups.*

Theorem 16.2.3. *If* G *is a topological group, then* $\pi_1(G, e)$ *is an abelian group.*

Corollary 16.2.1. $\pi_1(S^1, 1)$ *is abelian.*

16.3 Retractions

16.3.1 Retract

A subspace $A \subseteq X$ is a retract of X if there is a continuous function, the retraction, $r : X \to A$ for which $r(a) = a$ for all $a \in A$.

16.3.1.1 Deformation Retract

The subset $A \subseteq X$ is a *deformation retraction* if A is a retract of X and the composition $\iota \circ r : X \to A \hookrightarrow X$ is homotopic to the identity on X via a homotopy that fixes A, that is, there is a homotopy $H : X \times [0, 1] \to X$ with...

$$H(x, 0) = x,\ H(x, 1) = r(x), \text{ and } H(a, t) = a$$

for all $a \in A$ and all $t \in [0, 1]$.

Proposition 16.3.1. *If* $A \subseteq X$ *is a retract with retraction* $r : X \to A$*, then the inclusion* $\iota : A \to X$ *induces an injective homomorphism* $\iota_* : \pi_1(A, a) \to \pi_1(X, a)$ *and the retraction induces a surjective homomorphism* $r_* : \pi_1(X, a) \to \pi_1(A, a)$.

16.3.1.2 Contractible

A space is *contractible* if it is a deformation retract of one of its points.

Theorem 16.3.1. *If* A *is a deformation retract of* X*, then the inclusion* $\iota : A \to X$ *induces an isomorphism* $\iota_* : \pi_1(A, a) \to \pi_1(X, a)$.

Lemma 16.3.1. *If* $f, g : (X, x_0) \to (Y, y_0)$ *are continuous functions, homotopic through basepoint preserving maps, then* $f_* = g_* : \pi_1(X, x_0) \to \pi_1(Y, y_0)$.

16.3.1.3 Simply-Connected

A space X is said to be *simply-connected* if it is path-connected and $\pi_1(X) = \{e\}$.

Theorem 16.3.2. *Suppose $X = U \cup V$, where U and V are open, simply-connected subspaces and $U \cap V$ is path-connected. Then X is simply-connected.*

Proof. Choose a point $x_0 \in U \cap V$ as basepoint. Let $\lambda : [0,1] \to X$ be a loop based at x_0. Since λ is continuous, $\{\lambda^{-1}(U), \lambda^{-1}(V)\}$ is an open cover of the compact space $[0,1]$. The Lebesgue Lemma gives points $0 = t_0 < t_1 < t_2 < \cdots < t_n = 1$ with $\lambda([t_{i-1}, t_i]) \subseteq U$ or V. We can join x_0 to $\lambda(t_i)$ by a path γ_i. Define for $i \geq 1$,

$$\lambda_i(s) = \lambda((t_i - t_{i-1})s + t_{i-1}),\ 0 \leq s \leq 1,$$

for the path along λ joining $\lambda(t_{i-1})$ to $\lambda(t_i)$.

Then $\lambda \simeq \lambda_1 * \lambda_2 * \cdots * \lambda_n$ and, furthermore,

$$\lambda \simeq (\lambda_1 * \gamma_1^{-1}) * (\gamma_1 * \lambda_2 * \gamma_2^{-1}) * (\gamma_2 * \lambda_3 * \gamma_3^{-1}) * \cdots * (\gamma_{n-1} * \lambda_n).$$

Each $\gamma_i * \lambda_{i+1} * \gamma_{i+1}^{-1}$ lies in U or V. Since U and V are simply-connected, each of these loops is homotoplic to the constant map. Thus $\lambda \simeq c_{x_0}$. It follows that $\pi_1(X, x_0) \cong \{e\}$. □

Corollary 16.3.1. $\pi_1(S^n) \cong \{e\}$ *for* $n \geq 2$.

Corollary 16.3.2. $\pi_1(\mathbb{R}^n \setminus \{0\}) \cong \{e\}$ *for* $n \geq 3$.

16.4 Covering Spaces

Let X be a space. A *covering space* of X is a path-connected space $\tilde{X}$ and a mapping $p : \tilde{X} \to X$ such that, for every $x \in X$, there is an open, path-connected subset U with $x \in U$ for which each path component of $p^{-1}(U)$ is homeomorphic to U by restriction of the mapping p. Such open sets are called *elementary neighborhoods*.

16.4.1 Path Lifting

Lemma 16.4.1. *Let $p : \tilde{X} \to X$ be covering space and let $\tilde{x}_0 \in \tilde{X}$ with $p(\tilde{x}_0) = x_0 \in X$. If $\lambda : [0,1] \to X$ is any path with $\lambda(0) = x_0$, then there exists a unique path $\tilde{\lambda} : [0,1] \to \tilde{X}$ with $\tilde{\lambda}(0) = \tilde{x}_0$ and $p \circ \tilde{\lambda} = \lambda$.*

Proof. Cover X by elementary neighborhoods. If $\lambda([0,1]) \subseteq U$ for some elementary neighborhood, then $x_0 \in U$ and $\tilde{x}_0 \in p^{-1}(U)$. It follows that $\tilde{x}_0$ lies in some component C_0 of $p^{-1}(U)$ that is homeomorphis to U via $(p \restriction_{C_0})^{-1}(x_0) = \tilde{x}_0$, since $\tilde{x}_0$ is the only point in $\tilde{X}$ corresponding to x_0 in this component. Finally, $p \circ \tilde{\lambda} = p \circ (p \restriction_{C_0})^{-1} \circ \lambda = \lambda$.

If $\lambda([0,1]) \not\subseteq U$, consider the collection...

$$\{\lambda^{-1}(U') \subseteq [0,1] | U',\ \text{an elementary neighborhood}\}.$$

This is a cover of $[0,1]$, which is a compact metric space, and so by Lebesgue's Lemma we can choose $0 = t_0 < t_1 < \cdots < t_{n-1} < t_n = 1$ with each $\lambda([t_{i-1}, t_i])$ a subset of some elementary neighborhood (take $t_i - t_{i-1} < \delta$, the Lebesgue number). Using the argument above, lift λ on $[0, t_1]$. Then take $\lambda(t_1)$ as x_0 and $\tilde{\lambda}(t_1)$ as $\tilde{x}_0$ and lift λ to $[t_1, t_2]$. Continuing in this manner, we construct $\tilde{\lambda}$ on $[0,1]$ with $\tilde{\lambda}(0) = \tilde{x}_0$ and $p \circ \tilde{\lambda} = \lambda$.

Uniqueness is guaranteed by the following lemma. □

Lemma 16.4.2. *Let $p : \tilde{X} \to X$ be a covering space and Y a connected, locally connected space. Given two mappings $f_1, f_2 : Y \to \tilde{X}$ with $p \circ f_1 = p \circ f_2$, then the set...*

$$\{y \in Y | f_1(y) = f_2(y)\}$$

is either empty or all of Y.

Proof. Consider the subset of Y given by $B = \{y \in Y | f_1(y) = f_2(y)\}$. We show that B is both open and closed. If $y \in \operatorname{cls} B$, consider $x = p \circ f_1(y) = p \circ f_2(y)$ and U an elementary neighborhood containing x. The subset $(p \circ f_1)^{-1}(U) \cap (p \circ f_2)^{-1}(U)$ contains y. Because Y is locally connected, there is an open set W for which $y \in W \subseteq (p \circ f_1)^{-1}(U) \cap (p \circ f_2)^{-1}(U)$ with W connected. Then $f_1(W)$ and $f_2(W)$ are connected subsets of $p^{-1}(U) \subseteq \tilde{X}$. Since W is open and $y \in \operatorname{cls} B$, there is a point $z \in W$ with $z \in B$. Thus $f_1(z) = f_2(z)$ and $f_1(W) \cap f_2(W) \neq \emptyset$; therefore, $f_1(W)$ and $f_2(W)$ must lie in the same component of $p^{-1}(U)$. Since $p \circ f_1(y) = p \circ f_2(y)$ and the component in which we find both $f_1(y)$ and $f_2(y)$ is homeomorphic to U by the restriction of p, we have $f_1(y) = f_2(y)$. Thus $y \in B$ and B is closed.

If we let $y \in B$, the argument above shows that the sets $f_1(W)$ and $f_2(W)$ lie in the same component C_0 of $p^{-1}(U)$. It follows that, for all $w \in W$,

$$f_1(w) = (p \restriction_{C_0})^{-1} \circ p \circ f_1(w) = (p \restriction_{C_0})^{-1} \circ p \circ f_2(w) = f_2(w)$$

and so W is contained in B. Thus B is open.

The only subsets of Y that are both open and closed are Y itself and $\emptyset$ and so we have proved the lemma. □

16.4.2 Homotopy Lifting

Theorem 16.4.1. *Let $p : \tilde{X} \to X$ be a covering space and let $\eta_0, \eta_1 : [0,1] \to \tilde{X}$ be two paths in $\tilde{X}$ with $\eta_0(0) = \eta_1(0) = \tilde{x}_0$. If $p \circ \eta_0(1) = x_1 = p \circ \eta_1(1)$ and $p \circ \eta_0 \simeq p \circ \eta_1$ via a homotopy that fixes the endpoints of the paths in X, then $\eta_1 \simeq \eta_2$ in $\tilde{X}$ and, in particular, $\eta_0(1) = \eta_1(1)$.*

Proof. Let $H : [0,1] \times [0,1] \times X$ be a homotopy between $p \circ \eta_0$ and $p \circ \eta_1$. In this case, we have, for all $s, t \in [0,1]$,

$$H(s,0) = p \circ \eta_0(s), \qquad H(0,t) = p(\tilde{x}_0),$$
$$H(s,1) = p \circ \eta_1(s), \qquad H(1,t) = p \circ \eta_0(1) = p \circ \eta_1(1).$$

Since $[0,1] \times [0,1]$ is a compact metric space, when we cover it by the collection $\{H^{-1}(U) | U$, an elementary neighborhood of $X\}$, we can apply Lebesgue's Lemma to get $\delta > 0$ for which any subset of $[0,1] \times [0,1]$ of diameter $< \delta$ lies in some $H^{-1}(U)$. If we subdivide the interval $[0,1]$,

$$0 = s_0 < s_1 < \cdots < s_{m-1} < s_m = 1$$

and

$$0 = t_0 < t_1 < \cdots < t_{n-1} < t_n = 1,$$

so that $s_i - s_{i-1} < \delta/2$ and $t_j - t_{j-1} < \delta/2$, then H maps each subrectangle $[s_{i-1}, s_i] \times [t_{j-1}, t_j]$ into an elementary neighborhood for all i and j.

To construct the lifting $\hat{H} : [0,1] \times [0,1] \to \tilde{X}$ and show it is a homotopy between η_0 and η_1, begin by lifting H on $[0, s_1] \times [0, t_1]$ to $\tilde{X}$ by using $\hat{H} = (p \restriction_{C_{11}})^{-1} \circ H$, where C_{11} is the component of $p^{-1}(U_{11})$ containing $\eta_0(0)$ and $H([0, s_1] \times [0, t_1]) \subseteq U_{11}$, an elementary neighborhood. Having done this, extend $\hat{H}$ next to $[s_1, s_2] \times [0, t_1]$. Notice that $\hat{H}$ has been defined on the line segment $\{s_1\} \times [0, t_1]$ which is connected and this determines the component of $p^{-1}(U_{21})$ for the elementary neighborhood U_{21} which contains $H([s_1, s_2] \times [0, t_1])$. Once the component, say C_{21}, is determined, extend $\hat{H}$ by $\hat{H} = (p \restriction C_{21})^{-1} \circ H$. Continue in this manner until $\hat{H}$ is defined on $[0,1] \times [0, t_1]$. Next, extend to $[0,1] \times [t_1, t_2]$ using the fact that the value of $\hat{H}$ has been determined on each successive subrectangle along the left until $\hat{H}$ is defined on $[0,1] \times [0,1]$. By the preceding lemma, $\hat{H}$ is unique fulfilling the condition $\hat{H}(0,0) = \eta(0)$. Since $\eta_0(s)$ is also a lift of $H(s,0)$, we have that $\hat{H}(s,0) = \eta_0(s)$. The condition $H(0,t) = p \circ \eta_0(0)$ implies that $\hat{H}(0,t) = \eta_0(0)$, that is, the homotopy $\hat{H}$ is constant on the subset $\{0\} \times [0,1]$. Thus, the lift $\hat{H}(s,1)$ of the path $p \circ \eta_1(s)$ in X begins at $\eta_0(0) = \eta_1(0)$, and $\eta_1(s)$ is also such a lift. By uniqueness, $\hat{H}(s,1) = \eta_1(s)$. Finally, $H(1,t) = p \circ \eta_0(1) = p \circ \eta_1(1)$ for all $t \in [0,1]$, $\hat{H}(1,t) = \eta_0(1)$, and we conclude that $\eta_0(1) = \eta_1(1)$ since $\hat{H}(1,t)$ is constant. □

16.4.3 Fundamental Group Computations

Corollary 16.4.1. *Suppose $p : \tilde{X} \to X$ is a covering space:*

1. *If $\eta : [0,1] \to \tilde{X}$ is a loop at $\tilde{x}_0$ and $p \circ \eta$ is homotopic to the constant loop c_{x_0} for $x_0 = p(\tilde{x}_0)$, then $\eta \simeq c_{\tilde{x}_0}$.*

2. *The induced homomorphism $p_* : \pi_1(\tilde{X}, \tilde{x}_0) \to \pi_1(X, x_0)$ is injective.*

3. *For all $x \in X$, the subsets $p^{-1}(\{x\})$ of $\tilde{X}$ have the same cardinality.*

Proof. (1) One life of c_{x_0} is simply the constant path $c_{\tilde{x}_0}$. By the homotopy lifting theorem, $p \circ \eta \simeq p \circ c_{\tilde{x}_0} = c_{x_0}$ implies $\eta \simeq c_{\tilde{x}_0}$.

(2) If $p_*([\lambda]) = p_*([\mu])$, then, because p_* is a homomorphism, $p_*([\lambda]*[\mu^{-1}]) = [c_{x_0}]$, that is, $p\circ(\lambda*\mu^{-1}) \simeq c_{x_0}$. By (1), $\lambda*\mu^{-1} \simeq c_{\tilde{x}_0}$ or $\lambda \simeq \mu$, that is, $[\lambda] = [\mu]$.

(3) Suppose x_0 and x_1 are in X and $\lambda : [0,1] \to X$ is a path joining x_0 to x_1. Suppose $y \in p^{-1}(\{x_0\})$. We define a mapping $A : p^{-1}(\{x_0\}) \to p^{-1}(\{x_1\})$ by lifting λ to $\lambda_y : [0,1] \to \tilde{X}$ with $\lambda_y(0) = y$. Define $A(y) = \lambda_y(1)$. SInce λ_y is uniquely determined by being a lift of $p \circ \lambda_y = \lambda$ with $\lambda_y(0) = y$, the function A is well defined. By the path lifting 'uniqueness' lemma, lifts of λ beginning at different elements in $p^{-1}(\{x_0\})$ must end at different points in $p^{-1}(\{x_1\})$ and so A is injective. Using lifts of λ^{-1} we deduce that A is surjective. (Notice that a different choice of λ might give a different one-one correspondence A.) □

Theorem 16.4.2. *$\pi_1(S^1) \cong \mathbb{Z}$.*

Proof. If $\beta : [0,1] \to S^1$ is any loop at $1 \in S^1$, then the lift of β to $\hat{\beta} : [0,1] \to \mathbb{R}$ satisfies $\hat{\beta}(1) \in \mathbb{Z}$. The properties of liftings determine a function $\Xi : \pi_1(S^1) \to \mathbb{Z}$ given by $[\beta] \mapsto \hat{\beta(1)}$.

Let $\alpha : [0,1] \to S^1$ be given by $\alpha(t) = (\cos(2\pi t), \sin(2\pi t))$. Since $\alpha = w \restriction_{[0,1]}$, we see that one lift of α to $\mathbb{R}$ is just the identity and $\hat{\alpha}(1) = 1$. It follows that α is not homotopic to the constant map at 1, c_1. Next consider α^n for $n \in \mathbb{Z}$, given by $\alpha^n(t) = (\cos(2\pi nt), \sin(2\pi nt))$. By the same argument for α, $\hat{\alpha}^n(1) = n$ and so the mapping $\Xi : \pi_1(S^1) \to \mathbb{Z}$ is surjective. Since each $\alpha^n \not\simeq c_1$ for $n \neq 0$, the subgroup generated by $[\alpha]$, isomorphic to $\mathbb{Z}$, is a subgroup of $\pi_1(S^1)$.

To finish the proof, we show that if β is any loop based at 1 in S^1, then $\beta \simeq \alpha^n$ for some $n \in \mathbb{Z}$. Let $U_1 = \{(x,y) \in S^1 | y > -1/10\}$ and $U_2 = \{(x,y) \in S^1 | y < 1/10\}$. The pair $\beta^{-1}(U_1)$, $\beta^{-1}(U_2)$ is an open cover of $[0,1]$ and by Lebesgue's Lemma we can subdivide $[0,1]$ as $0 = t_0 < t_1 < \cdots < t_{m-1} < t_m = 1$ so that…

i) $\beta([t_i, t_{i+1}]) \subseteq U_1$ or $\beta([t_i, t_{i+1}]) \subseteq U_2$ for $0 \leq i < m$.

Form the union of consecutive subintervals when both are mapped to the same U_j, $j = 1$ or 2. In detail, let $s_0 = 0$ and $s_1 = t_{i_1}$, where $\beta([0, t_{i_1}]) \subseteq U_{j_1}$ for j_1 one of 1 or 2 and $\beta([t_{i_1}, t_{i_1+1}]) \not\subseteq U_{j_1}$. Let $U_{j_2} \neq U_{j_1}$ and $\beta([t_{i_1}, t_{i_1+1}]) \subseteq U_{j_2}$. Then let $s_1 = t_{i_2}$, where $\beta([t_{i_1}, t_{i_2}]) \subseteq U_{j_2}$ but $\beta([t_{i_2}, t_{i_2+1}]) \not\subseteq U_{j_2}$. Continue in this manner to get…

$$0 = s_0 < s_1 < \cdots < s_{k-1} < s_k = 1$$

so that

ii) $\beta([s_{j-1}, s_j])$ and $\beta([s_j, s_{j+1}])$ are not both contained in the same U_k, for $k = 1, 2$.

Let $\beta_j : [0,1] \to S^1$ denote the reparameterization of $\beta \restriction_{[s_j, s_{j+1}]}$ so that $\beta \simeq \beta_0 * \beta_1 * \cdots * \beta_{k-1}$, and each β_j is a path in exactly one of U_1 or U_2. Furthermore, $\beta(s_j) \in U_1 \cap U_2$, a subspace of two components, one of which contains $1 = e^{2\pi i0}$ and the other $-1 = e^{\pi i}$. For $0 < j < m$ choose a path $\lambda_j : [0,1] \to U_1 \cap U_2$ with $\lambda_j(0) = \beta(s_j) = \beta_{j-1}(s_j)$ and $\lambda_j(1) = 1$ or -1, depending on the component. Define…

$$\gamma_1 = \beta_0 * \lambda_1,$$

$$\gamma_j = \lambda_{j-1}^{-1} * \beta_{j-1} * \lambda_j \text{ for } 1 < j < k,$$

$$\gamma_k = \lambda_{m-1}^{-1} * \beta_{k-1}.$$

By cancelling $\lambda_j * \lambda_j^{-1}$, $\beta \simeq \gamma_1 * \gamma_2 * \cdots * \gamma_k$. Consider the paths γ_l. If γ_l is a closed path, it lies in U_1 or U_2, which are simply-connected and so $\gamma_l \simeq c_1$ or $\gamma_l \simeq c_{-1}$. If γ_l is not closed, then it crosses between the components of $U_1 \cap U_2$. It follows that $\gamma_l \simeq \eta_1^{\pm 1}$ or $\gamma_l \simeq \eta_2^{\pm 1}$, where $\eta_1(t) = (\cos(\pi t), \sin(\pi t))$, the path joining 1 to -1 in U_1, and $\eta_2(t) = (\cos(\pi t + \pi), \sin(\pi t + \pi))$, the path joining -1 to 1 in U_2. Making the cancellations of the type $\eta_1\eta_1^{-1} \simeq c_1$ or $\eta_2\eta_2^{-1} \simeq c_{-1}$, we are left with three possibilities:

$$\beta \simeq c_1, \ \beta \simeq \eta_1 * \eta_2 * \eta_1 * \eta_2 * \cdots * \eta_1 * \eta_2, \text{ or}$$

$$\beta \simeq \eta_2^{-1} * \eta_1^{-1} * \eta_2^{-1} * \cdots * \eta_2^{-1} * \eta_1^{-1},$$

after cancelling out $c_{\pm 1}$. The ordering is determined by the fact that β begins and ends at 1, and each γ_l either joins 1 to -1, joins -1 to 1, or it simply stays put. After cancellation of the paths that stay put or products of paths that are homotopic to the constant path, we are left with such a product in that order. Finally, $w \restriction_{[0,1]} = \alpha \simeq \eta_1 * \eta_2$ and so $\beta \simeq \alpha^n$ for some $n \in \mathbb{Z}$. □

Theorem 16.4.3. *$\pi_1(\mathbb{R}P^2) \cong \mathbb{Z}/2\mathbb{Z}$.*

Proof. Consider the model of the projective plane given by the *di-gon*, a disk with each point on the boundary identified with the point symmetric with respect to the origin. Let $s_0 \in \mathbb{R}P^2$ be the point $x_0 = [\pm(1,0,0)]$. Let $p : S^2 \to \mathbb{R}P^2$ denote the covering space $p(\mathbf{x}) = [\pm\mathbf{x}]$. Let the loop a in $\mathbb{R}P^2$ denote half of the equator, and lift a to S^2. We get a path $\hat{a}$ from $(1,0,0)$ to $(-1,0,0)$ along the equator of S^2. By the corollary at the beginning of this subsection, $a \not\simeq c_{x_0}$. In the di-gon representation of $\mathbb{R}P^2$, $a * a = a^2$ surrounds the disk, and so a^2 can be contracted to c_{x_0} by shrinking to the center of the disk and translating over to x_0. If follows that $\pi_1(\mathbb{R}P^2)$ contains $\mathbb{Z}/2\mathbb{Z}$. To finish, we need show that any loop at x_0 is homotopic to a^n for some $n \in \mathbb{Z}$. Using the di-gon we see that away from the image of the path a^2 a path lies in the contractible interior of a disk. The disk can be used to push any loop onto a as often as it crosses between the copies of x_0. Thus we see that any loop based at x_0 is homotopic to a^n for some $n \in \mathbb{Z}$ and so homotopic to a or c_{x_0}. This implies that…

$$\pi_1(\mathbb{R}P^2) = \langle [a] \rangle / ([a]^2 = [c_{x_0}]) \cong \mathbb{Z}/2\mathbb{Z}.$$

□

16.5 Applications

Theorem 16.5.1 (Brouwer's Theorem in dimension 2)**.** *The two-disk* $e^2 = \{\boldsymbol{x} \in \mathbb{R}^2 | ||\boldsymbol{x}|| \leq 1\} \subseteq \mathbb{R}^2$ *has the fixed point property.*

Proof. Suppose $f : e^2 \to e^2$ is a continuous function without a fixed point. Then for each $\mathbf{x} \in e^2$, $f(\mathbf{x}) \neq \mathbf{x}$. Define $g : e^2 \to S^1$ by...

$$g(\mathbf{x}) = \text{ intersection of the ray from } f(\mathbf{x}) \text{ to } \mathbf{x} \text{ with } S^1.$$

To see that $g(\mathbf{x})$ is continuous on e^2, we apply some vector geometry: write $Q = f(\mathbf{x})$, $Z = g(\mathbf{x})$. Let $O = (0,0)$ and define $X = (\mathbf{x} - Q)/||\mathbf{x} - Q||$. Then, $g(\mathbf{x}) = Z = Q + tX$ for some $t \geq 0$ for which $Q + tX \in S^1$, that is, $(Q + tX) \cdot (Q + tX) = 1$. This condition can be rewritten to solve for t, namely,

$$(Q + tX) \cdot (Q + tX) = t^2(X \cdot X) + 2t(Q \cdot X) + Q \cdot Q = 1.$$

The quadratic formula gives...

$$\begin{aligned} t_{\mathbf{x}} &= -Q \cdot X + \sqrt{(Q \cdot X)^2 + 1 - Q \cdot Q} \\ &= -f(\mathbf{x}) \cdot \frac{\mathbf{x} - f(\mathbf{x})}{||\mathbf{x} - f(\mathbf{x})||} + \sqrt{\left(f(\mathbf{x}) \cdot \frac{\mathbf{x} - f(\mathbf{x})}{||\mathbf{x} - f(\mathbf{x})||}\right)^2 + 1 - f(\mathbf{x}) \cdot f(\mathbf{x})}. \end{aligned}$$

Note that this choice of signs gives $t_{\mathbf{x}} \geq 0$, and $t_{\mathbf{x}} = 0$ implies $f(\mathbf{x}) = \mathbf{x}$. Since we have assumer that this doesn't happen, $t_{\mathbf{x}} > 0$. Furthermore, $t_{\mathbf{x}}$ is a continuous function of $\mathbf{x}$. We can write $g(\mathbf{x})$ explicitly as...

$$g(\mathbf{x}) = f(\mathbf{x}) = t_{\mathbf{x}} \frac{\mathbf{x} - f(\mathbf{x})}{||\mathbf{x} - f(\mathbf{x})||}$$

and so $g(\mathbf{x})$ is continuous.

By the definition of the mapping g, if $\mathbf{x} \in S^1 \subseteq e^2$, then $g(\mathbf{x}) = \mathbf{x}$. We have constructed a continuous mapping $g : e^2 \to S^1$ for which $g \circ i = \mathrm{id}_{S^1}$, that is, the identity mapping on S^1 can be factored:

$$\mathrm{id}_{S^1} : S^1 \xrightarrow{i} e^2 \xrightarrow{g} S^1.$$

The composite leads to a composite of group homomorphisms and fundamental groups:

$$\mathrm{id} : \pi_1(S^1) \xrightarrow{i_*} \pi_1(e^2) \xrightarrow{g_*} \pi_1(S^1).$$

However, $\pi_1(e^2) = \{[c_1]\}$ and so $g_* \circ i_*([\alpha]) = [c_1] \neq [\alpha]$ and $g_* \circ i_* \neq \mathrm{id}$, a contradiction. Therefore, a continuous function $f : e^2 \to e^2$ without fixed points is not possible. □

Corollary 16.5.1. S^1 *is not a retract of* e^2*.*

Proposition 16.5.1 (The Borsuk-Ulam Theorem for $n = 2$)**.** *There does not exist a continuous function* $f : S^2 \to S^1$ *that satisfies* $f(-\boldsymbol{x}) = -f(\boldsymbol{x})$ *for all* $\boldsymbol{x} \in S^2$*.*

Proof. Assume such a function exists. The condition satisfied by f can be written $f(\pm\mathbf{x}) = \pm f(\mathbf{x})$. It follows that f induces $\hat{f} : \mathbb{R}P^2 \to \mathbb{R}P^1$ and $\hat{f}$ fits into a diagram:

$$\begin{array}{ccc} S^2 & \xrightarrow{f} & S^1 \\ \downarrow p & & \downarrow \overline{p} \\ \mathbb{R}P^2 & \xrightarrow{\hat{f}} & \mathbb{R}P^1 \end{array}$$

for which $\overline{p} \circ f = \hat{f} \circ p$. Consider the induced homomorphism $\hat{f}_* : \pi_1(\mathbb{R}P^2) \to \pi_1(\mathbb{R}P^1)$. Via considerations of fundamental groups, $\hat{f}_*$ is a homomorphism $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$. However, any such homomorphism must be the trivial homomorphism. Let $\lambda : [0,1] \to S^2$ denote a path from the North Pole to the South Pole along a meridian of constant longitude. It follows that $[p \circ \lambda] = [\alpha]$, a generator for $\mathbb{Z}/2\mathbb{Z} \cong \pi_1(\mathbb{R}P^2)$. Since the North and South Poles are antipodal, these points are identified in $\mathbb{R}P^1$ after passage through f and $\overline{p}$. Hence $[\overline{p} \circ f \circ \lambda]$ is nontrivial in $\pi_1(\mathbb{R}P^1)$. But $[\overline{p} \circ f \circ \lambda] = [\hat{f} \circ p \circ \lambda] = \hat{f}_*([p \circ \lambda]) = 0$, a contradiction. □

Corollary 16.5.2. *If $f : S^2 \to \mathbb{R}^2$ is a continuous function such that $f(-\boldsymbol{x}) = -f(\boldsymbol{x})$ for all $\boldsymbol{x} \in S^2$, then $f(\boldsymbol{x}) = (0,0)$ for some $\boldsymbol{x} \in S^2$.*

The following theorem follows from the above development of the Borsuk-Ulam theorem.

Theorem 16.5.2. *If $f : S^2 \to \mathbb{R}^2$ is a continuous function, then there exists a point $\boldsymbol{x} \in S^2$ with $f(\boldsymbol{x}) = f(-\boldsymbol{x})$.*

Corollary 16.5.3. *No subset of $\mathbb{R}^2$ is homeomorphic to S^2.*

16.6 Homotopy Type

16.6.1 Homotopy Equivalent

Two spaces are *homotopy equivalent*, denoted $X \simeq Y$, if there are mappings $f : X \to Y$ and $g : Y \to X$ with $g \circ f \simeq \mathrm{id}_X$ and $f \circ g \simeq \mathrm{id}_Y$.

Proposition 16.6.1. *In a set of topological spaces, homotopy equivalence is an equivalence relation.*

16.6.2 Definition

Proposition 16.6.2. *If X and Y are homotopy-equivalent spaces via mappings $f : X \to Y$ and $g : Y \to X$, then the induced mappings $f_* : \pi_1(X, x_0) \to \pi_1(Y, f(x_0))$ and $g_* : \pi_1(Y, y_0) \to \pi_1(X, g(y_0))$ are isomorphisms.*

16.6.3 Homotopy Invariance

A topological property that does not very over homotopy type.

The fundamental group is a homotopy invariant.

17 Homology

17.1 Complexes

A *chain complex* of R-modules is a sequence of R-modules and R-module homomorphisms...

$$\cdots \xrightarrow{d_{i+2}} M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} \cdots$$

such that $(\forall i) : d_i \circ d_{i+1} = 0$.

17.1.1 Exactness

- A complex...

  $$\cdots \to 0 \to L \xrightarrow{\alpha} M \to \cdots$$

  is *exact* at L if and only if α is a monomorphism.

- A complex...

  $$\cdots \to M \xrightarrow{\beta} N \to 0 \to \cdots$$

  is *exact* at N if and only if β is an epimorphism.

- A *short exact sequence* is an exact complex of the form...

  $$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0.$$

17.1.2 Split

A short exact sequence...

$$0 \to M_1 \to N \to M_2 \to 0,$$

splits if the following diagram commutes.

$$\begin{tikzcd}
0 \arrow[r] & M_1 \arrow[r] \arrow[d, "\sim"] & N \arrow[r] \arrow[d, "\sim"] & M_2 \arrow[r] \arrow[d, "\sim"] & 0 \\
0 \arrow[r] & M_1' \arrow[r] & M_1' \oplus M_2' \arrow[r] & M_2' \arrow[r] & 0
\end{tikzcd}$$

Proposition 17.1.1. *Let $\varphi : M \to N$ be an R-module homomorphism. Then...*

- *φ has a left inverse if and only if the sequence...*

  $$0 \to M \xrightarrow{\varphi} N \to coker\varphi \to 0$$

  splits.

- *φ has a right inverse if and only if the sequence...*

  $$0 \to ker\varphi \to M \xrightarrow{\varphi} N \to 0$$

  splits.

17.2 Definitions

The *i-th homology* of a complex...

$$M_\bullet : \cdots \xrightarrow{d_{i+2}} M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} \cdots$$

of R-modules is the R-module...

$$H_i(M_\bullet) := \frac{\ker d_i}{\operatorname{im} d_{i+1}}.$$

Lemma 17.2.1 (Snake Lemma)**.** *Given two short exact sequences linked together by homomorphisms as in the following commutative diagram...*

$$\begin{tikzcd}
0 \arrow[r] & L_1 \arrow[r, "\alpha_1"] \arrow[d, "\lambda"] & M_1 \arrow[r, "\beta_1"] \arrow[d, "\mu"] & N_1 \arrow[r] \arrow[d, "\nu"] & 0 \\
0 \arrow[r] & L_0 \arrow[r, "\alpha_0"] & M_0 \arrow[r, "\beta_0"] & N_0 \arrow[r] & 0
\end{tikzcd}$$

We are guaranteed an exact sequence...

$$0 \to \mathit{ker}\ \lambda \to \mathit{ker}\ \mu \to \mathit{ker}\ \nu \xrightarrow{\delta} \mathit{coker}\ \lambda \to \mathit{coker}\ \mu \to \mathit{coker}\ \nu \to 0.$$

Corollary 17.2.1. *In the same as the snake lemma, assume μ is surjective and ν is injective. Then λ is surjective and ν is an isomorphism.*

17.3 Euler Characteristic

Proposition 17.3.1. *Let...*

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$$

be a short exact sequence of finite-dimensional vector spaces. Then...

$$\mathit{dim}(V) = \mathit{dim}(U) + \mathit{dim}(W).$$

Or equivalently...

$$\mathit{dim}(V/U) = \mathit{dim}(V) - \mathit{dim}(U).$$

Consider a complex of finite-dimensional vector spaces and linear maps...

$$V_\bullet : 0 \longrightarrow V_N \xrightarrow{\alpha_N} V_{N-1} \xrightarrow{\alpha_{N-1}} \cdots \xrightarrow{\alpha_2} V_2 \xrightarrow{\alpha_1} V_0 \longrightarrow 0.$$

The *Euler characteristic* of $V_\bullet$ is the integer...

$$\chi(V_\bullet) := \sum_i (-1)^i \dim(V_i).$$

Proposition 17.3.2. *With notation as above,*

$$\chi(V_\bullet) = \sum_{i=0}^{N} (-1)^i \mathit{dim}(H_i(V_\bullet)).$$

In particular, if $V_\bullet$ is exact, then $\chi(V_\bullet) = 0$.

Proof. Use induction on the length of the complex $V_\bullet$. □

17.3.1 Grothendieck Group

Consider the category k-Vect^f of finite-dimensional k-vector spaces. Each object V of k-Vect^f determines an isomorphism class $[V]$. Let $F(k\text{-Vect}^f)$ be the free abelian group on the set of these isomorphism classes; further, let E be the subgroup generated by the elements...

$$[V] - [U] - [W]$$

for all short exact sequences...

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$$

in k-Vect^f. The quotient group...

$$K(k\text{-Vect}^f) := \frac{F(k\text{-Vect}^f)}{E}$$

is called the *Grothendieck group* of the category k-Vect^f. The element determined by V in the Grothendieck group is still denoted $[V]$.

A *Grothendieck group* may be defined for any category admitting a notion of exact sequence.

Every complex $V_\bullet$ determines an element in $K(k\text{-Vect}^f)$, namely...

$$\chi_K(V_\bullet) := \sum_i (-1)^i [V_i] \in K(k\text{-Vect}^f).$$

Proposition 17.3.3. *With notation as above, we have the following:*

- χ_K *'is an Euler characteristic', in the sense that it satisfies the formula given in the previous proposition...*

$$\chi(V_\bullet) = \sum_{i=0} (-1)^i [H_i(V_\bullet)].$$

- χ_K *is a 'universal Euler characteristic', in the following sense. Let G be an abelian group, and let δ be a function associating an element of G to each finite-dimensional vector space, such that $\delta(V) = \delta(V')$ if $V \cong V'$ and $\delta(V/U) = \delta(V) - \delta(U)$. For $V_\bullet$ a complex, define...*

$$\chi(V_\bullet) = \sum_{i=0} (-1)^i \delta(V_i).$$

Then δ induces a (unique) group homomorphism...

$$K(k\text{-}Vect^f) \to G$$

mapping $\chi_K(V_\bullet)$ to $\chi_G(V_\bullet)$.

- *In particular,* $\delta = \dim$ *induces a group homomorphism...*

$$K(k\text{-}Vect^f) \to \mathbb{Z}$$

such that $\chi_K(V_\bullet) \mapsto \chi(V_\bullet)$.

- *This is in fact an isomorphism.*

17.4 Applications to Simplicial Complexes

17.4.1 Space of p-chains

Suppose K is a simplicial complex. Then...

$$K_p = \{S \in K | \dim S = p \text{ and } S \text{ is nondegenerate}\}$$

forms a basis for the space of p-chains of K. The field we use for the rest of these notes is $\mathbb{F}_2$. Thus the space is...

$$C_p(K; \mathbb{F}_2) = \mathbb{F}_2[K_p].$$

A simplicial mapping $\phi : K \to L$ induces a linear mapping $\phi_* : C_p(K; \mathbb{F}_2) \to C_p(L; \mathbb{F}_2)$ defined on a p-simplex as...

$$\phi_*(\{v_0, \ldots, v_p\}) = \begin{cases} \phi(v_0), \ldots, \phi(v_p) & \text{if } \{\phi(v_0), \ldots, \phi(v_p)\} \text{ is nondegenerate in } L, \\ \mathbf{0} & \text{if } \{\phi(v_0), \ldots, \phi(v_p)\} \text{ is degenerate in } L. \end{cases}.$$

17.4.2 Boundary Homomorphisms

Given the simplex $S = \{v_0, \ldots, v_p\}$ the face opposing vertex v_i is given by...

$$\partial_i(S) = \{v_0, \ldots, \hat{v_i}, \ldots, v_p\} \subset S.$$

We can define a mapping $\partial : K_p \to C_{p-1}(K; \mathbb{F}_2)$ by summing all the $(p-1)$ faces of a p-simplex. The extension of this map to...

$$\partial : C_p(K; \mathbb{F}_2) \to C_{p-1}(K; \mathbb{F}_2)$$

given by...

$$\partial(S) = \sum_{i=0}^{p} \partial_i(S), \text{ for } S \in K_p.$$

is called the *boundary homomorphism.*

Proposition 17.4.1. *If* $\phi : K \to L$ *is a simplicial mapping, then...*

$$\partial \circ \phi_* = \phi_* \circ \partial : C_p(K; \mathbb{F}_2) \to C_{p-1}(K; \mathbb{F}_2).$$

Furthermore, the composite $\partial \circ \partial : C_p(K; \mathbb{F}_2) \to C_{p-1}(K; \mathbb{F}_2)$ *is the zero mapping.*

17.4.3 Space of p-cycles

The *space of p-cycles* is the kernel of the boundary homomorphism...

$$Z_p(K) = \ker \partial : C_p \to C_{p-1} = \{c \in C_p(K; \mathbb{F}_2) | \partial(c) = \mathbf{0}\}.$$

17.4.4 Space of p-boundaries

The *space of p-boundaries* is the image of the boundary homomorphism...

$$B_p(K) = \partial(C_{p+1}(K; \mathbb{F}_2)) = \{b \in C_p(K; \mathbb{F}_2) | b = \partial(c), \text{ for some } c \in C_{p+1}(K; \mathbb{F}_2)\}.$$

Since $\partial \circ \partial = 0$ we have $B_p(K) \subseteq Z_p(K)$ and can thus define the homology on a chain complex of boundary homomorphisms.

17.4.5 Chain Homotopies

Homology is a functor on chain complexes, that is, if $\phi : K \to L$ is a simplicial mapping, then...

$$H(\phi) : H_p(K; \mathbb{F}_2) \to H_p(L; \mathbb{F}_2) \text{ given by } H(\phi)(c + B_p(K)) = \phi_*(c) + B_p(L)$$

is a linear map and H satisfies the functor properties.

Given two simplicial mappings ϕ and $\psi : K \to L$, there is a *chain homotopy* between them if there is a linear mapping $h : C_p(K; \mathbb{F}_2) \to C_{p+1}(L; \mathbb{F}_2)$ for each p which satisfies...

$$\partial \circ h + h \circ \partial = \phi_* + \psi_*.$$

Theorem 17.4.1. *If there is a chain homomtopy between ϕ and ψ, then $H(\phi) = H(\psi)$.*

Corollary 17.4.1. *If ϕ and $\psi : K \to L$ are simplicial mappings, and ϕ is contiguous to ψ, then $H(\phi) = H(\psi) : H_p(K; \mathbb{F}_2) \to H_p(L; \mathbb{F}_2)$ for all p.*

Corollary 17.4.2. *If ϕ and $\psi : K \to L$ are simplicial approximations of a continuous mapping $f : |K| \to |L|$, then $H(\phi) = H(\psi) : H_p(K; \mathbb{F}_2) \to H_p(L; \mathbb{F}_2)$, for all p.*

17.4.6 Topological Invariance

Theorem 17.4.2. *There is an isomorphism of vector spaces for all $p \geq 0$...*

$$H_p(sd\ K; \mathbb{F}_2) \cong H_p(K; \mathbb{F}_2).$$

Proof. This proof is lengthy and used the *method of acyclic models.* Look up elsewhere. $\square$

Theorem 17.4.3 (Topological Invariance of Homology)**.** *Suppose K and L are simplicial complexes with $|K|$ and $|L|$ homeomorphic. Then, for all p, the vector spaces $H_p(K;\mathbb{F}_2)$ and $H_p(K;\mathbb{F}_2)$ are isomorphic.*

Proof. This proof is also lengthy and involves the previous theorem. Also look it up. □

Corollary 17.4.3. *The Euler Poincaré characteristic is a topological invariant of a triangulable space.*

Theorem 17.4.4. *There are only five Platonic solids.*

Proof. A polyhedron P need not be a simplicial complex, since the faces can be polygons not necessarily triangles. However, if we subdivide each constituent polygon into triangles, we get a simplicial complex. This means Eulers formula for P computes the same result as the Euler-Poincaré characteristic $\chi(P)$. Thus since P has a realization homeomorphic to S^2, we know that $\chi(P) = 2$.

Suppose each face has M edges and, at each vertex, N faces meet. This gives us...

$$Mn_2/2 = n_1$$

where n_2 is the number of faces and n_1 is the number of edges. Also we get...

$$Nn_0/2 = n_1$$

where n_0 is the number of vertices. Putting these relations into Euler's formula we get...

$$\begin{aligned} 2 &= n_0 - n_1 + n_2 \\ &= (2n_1/N) - n_1 + (2n_1/M) \\ &= n_1((2/N) + (2/M) - 1). \end{aligned}$$

It follows that...

$$\frac{n_1}{2} = \frac{MN}{2M + 2N - MN}.$$

If $N = 1$ or $N = 2$, there would be a boundary and so the polyhedron would fail to be a sphere. Since a Platonic solid encloses space, $N > 2$. Also $M \geq 3$ since each face is a polygon. Finally, n_1 must be an integer which is at least M.

These facts forces $M < 6$. To see this, suppose $M \geq 6$ and $N > 2$. Then $2 - N < 0$ and we have...

$$0 < 2M + 2N - MN = 2N + M(2 - M) \leq 2N + 6(2 - N) = 12 - 4N.$$

This implies that $4N < 12$, or that $N < 3$, which is impossible because N is an integer and $N > 2$.

Setting $M = 3$ we get $n_1 = 6N/(6-N)$, which is an integer when $N = 3, 4, 5$. The case $N = 3$, $M = 3$ is realized by the tetrehedron, $N = 4$ and $M = 3$ is realized by the octahedron, and for $N = 5$, $M = 3$ by the icosahedron.

For $M = 4$ we have $n_1 = 8N/(8-2N) = 4N/(4-N)$, and so $N = 3$ is the only case of interest which is realized by the cube. Finally, for $M = 5$ we have $n_1 = 10N/(10-3N)$ and so $N = 3$ is the only possible case, which gives the dodecahedron. $\square$

Theorem 17.4.5. *If K is a simplicial complex, then $dim_{\mathbb{F}_2} H_0(K;\mathbb{F}_2) = \#\pi_0(|K|)$, the number of path components of $|K|$.*

Proof. This is lengthy and should be looked up. $\square$

Theorem 17.4.6 (Brouwer Fixed Point Theorem)**.** *If $e^n = \{x \in \mathbb{R}^n \mid ||x|| \leq 1\}$ denotes the n-disk and $f : e^n \to e^n$ is a continuous mapping, then there is a point $x_0 \in e^n$ with $f(x_0) = x_0$, that is, e^n has the fixed point property.*

Proof. Suppose that $f : e^n \to e^n$ is a continuous mapping without fixed points. If $y \in e^n$, then $y \neq f(y)$. Join $f(y)$ to y and continue this ray until it meets $S^{n-1} = \mathrm{bdy} e^n$ and denote this point by $g(y)$. We can characterize $g(y)$ by $g(y) = (1-t)f(y) + ty$, where $t > 0$ and $||g(y)|| = 1$. Because we are in a nicely behaved inner porduct space, the argument for hte case of $n = 2$ carries over exactly to prove that $g : e^n \to S^{n-1}$ is continuous. Furthermore, by the definition of g, $g \circ i : S^{n-1} \to S^{n-1}$ is the identity when $i : S^{n-1} \to e^n$ is the inclusion of the boundary.

Apply homology to this composite $\mathrm{id}_{S^{n-1}} = g \circ i$ to obtain $H(\mathrm{id}_{S^{n-1}})$, an isomorphism, written as $H(g) \circ H(i)$. However, $H_{n-1}(S^{n-1};\mathbb{F}_2) \neq \{0\}$ while $H_{n-1}(e^n;\mathbb{F}_2) = \{0\}$, because e^n is homeomorphic to Δ^n. Thus, $H(i) : H_{n-1}(e^n;\mathbb{F}_2) \to H_{n-1}(e^n;\mathbb{F}_2)$ is the zero homomorphism $[c] \mapsto 0$. An isomorphism...

$$H(\mathrm{id}_{S^{n-1}} : H_{n-1}(S^{n-1};\mathbb{F}_2) \to H_{n-1}(S^{n-1};\mathbb{F}_2)$$

cannot be factored as $H(g) \circ ([c] \mapsto 0)$; and so a continuous mapping $f : e^n \to e^n$ without fixed points cannot exist. $\square$

18 Fundamental Theorem of Algebra

Theorem 18.0.1. *If $p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$ is a polynomial with complex coefficients, then there is a complex number z_0 with $p(z_0) = 0$.*

18.1 Gauss's Incomplete Proof

Proof. Let $p(z) = z^n + a_{n-1}a^{n-1} + \cdots + a_1 z + a_0$ be a complex monic polynomial of degree n. We begin with some estimates. We can write the complex numbers in polar form, $z = re^{i\theta}$ and $a_j = s_j e^{i\psi_j}$, and make the substitution...

$$p(z) = r^n e^{ni\theta} + r^{n-1}s_{n-1}e^{(n-1)i\theta + i\psi_{n-1}} + \cdots + rs_1 e^{i\theta + i\psi_1} + s_0 e^{i\psi_0}.$$

Writing $e^{i\beta} = \cos(\beta) + i\sin(\beta)$ and $p(z) = T(z) + iU(z)$, we have...

$$\begin{aligned} T(z) &= r^n \cos(n\theta) + r^{n-1}s_{n-1}\cos((n-1)\theta + \psi_{n-1}) \\ &\quad + \cdots + rs_1\cos(\theta + \psi_1) + s_0\cos(\psi_0), \\ U(z) &= r^n \sin(n\theta) + r^{n-1}s_{n-1}\sin((n-1)\theta + \psi_{n-1}) \\ &\quad + \cdots + rs_1\sin(\theta + \psi_1) + s_0\sin(\psi_0). \end{aligned}$$

Thus a root of $p(z)$ is a complex number $z_0 = re^{i\theta_0}$ with $T(z_0) = 0 = U(z_0)$.

Suppose $S = \max\{s_{n-1}, s_{n-2}, \ldots, s_0\}$ and $R = 1 + \sqrt{2}S$. Then if $r > R$, we can write...

$$\begin{aligned} 0 < 1 - \frac{\sqrt{2}S}{r-1} &= 1 - \sqrt{2}S\left(\frac{1}{r} + \frac{1}{r^2} + \frac{1}{r^3} + \cdots\right) \\ &< 1 - \sqrt{2}S\left(\frac{1}{r} + \frac{1}{r^2} + \cdots + \frac{1}{r^n}\right) \end{aligned}$$

Multiplying through by r^n, we deduce...

$$\begin{aligned} 0 &< r^n - \sqrt{2}S(r^{n-1} + r^{n-2} + \cdots + r + 1) \\ &\le r^n - \sqrt{2}(s_{n-1}r^{n-1} + s_{n-2}r^{n-2} + \cdots + s_1 r + s_0). \end{aligned}$$

The $\sqrt{2}$ factor is related to the trigonometric form of $T(z)$ and $U(z)$.

Fix a circle in the complex plane given by $z = re^{i\theta}$ for $r > R$. Denote points P_k on this circle with special values:

$$P_k = r\left(\cos\left(\frac{(2k+1)\pi}{4n}\right) + i\sin\left(\frac{(2k+1)\pi}{4n}\right)\right).$$

When we evaluate $T(P_{2k})$, the leading term is $r^n\cos(n((4k+1)\pi/4n)) = (-1)^k r^n(\sqrt{2}/2)$. Thus we can write $(-1)^k T(P_{2k})$ as...

$$\frac{r^2}{\sqrt{2}} + (-1)^k s_{n-1}r^{n-1}\cos\left((n-1)\left(\frac{(4k+1)\pi}{4n} + \psi_{n-1}\right)\right) + \cdots + (-1)^k s_0\cos(\psi_0).$$

Since $(-1)^k \cos\alpha \geq -1$ for all α and $r > R$, we find that...

$$(-1)^k T(P_{2k}) \geq \frac{r^n}{\sqrt{2}} - (s_{n-1}r^{n-1} + \cdots + s_1 r + s_0) > 0.$$

Similarly, in $T(P_{2k+1})$, the leading term is $(-1)^{k+1}r^n\sqrt{2}/2$ and the same estimate give $(-1)^{k+1}T(P_{2k+1}) > 0$.

The estimates imply that the value of $T(z)$ alternates in sign at $P_0, P_1, \ldots, P_{4n-1}$. Since $T(re^{i\theta})$ varies continuously in θ, $T(z)$ has a zero between P_{2k} and P_{2k+1} for $k = 0, 1, 2, \ldots 2n-1$. We note that these are all of the zeros of $T(z)$ on this circle. To see this, write...

$$\cos\theta + i\sin\theta = \frac{1-\zeta^2}{1+\zeta^2} + i\frac{2\zeta}{1+\zeta^2}, \text{ where } \zeta = \tan(\theta/2).$$

Thus $T(z)$ can be written in the form...

$$r^n\left(\frac{1-\zeta^2}{1+\zeta^2}\right)^n + s_{n-1}\cos(\psi_{n-1})r^{n-1}\left(\frac{1-\zeta^2}{1+\zeta^2}\right)^{n-1} + \cdots + s_1\cos(\psi_1)r\left(\frac{1-\zeta^2}{1+\zeta^2}\right) + s_0\cos(\psi_0),$$

that is, $T(z) = f(\zeta)/(1+\zeta^2)^n$, where $f(\zeta)$ is a polynomial of degree less than or equal to $2n$. Since $T(z)$ has $2n$ zeros, $f(\zeta)$ has degree $2n$ and has exactly $2n$ roots. Since $T(z)$ has $2n$ zeros, $f(\zeta)$ has degree $2n$ and has exactly $2n$ roots. Thus we can name the zeros of $T(z)$ on the circle of radius r by $Q_0, Q_1, \ldots, Q_{2n-1}$ with Q_k between P_{2k} and P_{2k+1}.

Let $Q_k = re^{i\phi_k}$. Then $n\phi_k$ lies between $\frac{\pi}{4} + k\pi$ and $\frac{3\pi}{4} + k\pi$. It follows from properties of the sine function that $(-1)^k \sin(n\phi_k) \geq \sqrt{2}/2$. From this estimate we find that...

$$\begin{aligned}(-1)^k U(Q_k) &\geq (-1)^k r^n \sin(n\phi_k) - s_{n-1}r^{n-1} - \cdots s_0 \\ &\geq \frac{r^n}{\sqrt{2}} - s_{n-1}r^{n-1} - \cdots - s_0 > 0.\end{aligned}$$

Then $U(z)$ is positive at Q_{2k} and negative at Q_{2k+1} for $0 \leq k \leq n-1$, and by continuity $U(z)$ is zero between consecutive pairs of Q_j. This gives us points q_i, for $i = 0, 1, \ldots, 2n-1$ with q_i, between Q_i and Q_{i+1} and $U(q_i) = 0$.

The game is clear now - a zero of $p(z)$ is a value z_0 with $T(z_0) = U(z_0)$. Gauss argued that, as the radius of the circle varied, the distinguished points Q_j and q_k would form curves. As the radius grew smaller, the points Q_k determine regions whose boundary is where $T(z) = 0$. The curve of q_j, where $U(z) = 0$, must cross some curve of Q_j's, and so give us a root of $p(z)$. The geometric properties of curves of the type given by $T(z) = 0$ and $U(z) = 0$ are need to complete this part of the argument and require real analysis. The identification of the curves and reducing the existence of a root to the necessary intersection of curves are served up by connectedness. □

18.2 Homotopy Proof

Proof. Recall that $\mathbb{C} \cong \mathbb{R}^2$ and the nth power mapping $h : z \mapsto z^n$ induces a mapping $h : S^1 \to S^1$ which can be written as $e^{i\theta} \mapsto e^{in\theta}$. Lifting this mapping to the covering space $w : \mathbb{R} \to S^1$, it represents $n \in \mathbb{Z} \cong \pi_1(S^1)$ via the identification of $\pi_1(S^1)$ with $\mathbb{Z}$ given by $[\beta] \mapsto \hat{\beta}(1)$.

Viewed as a mapping, $h : S^1 \to S^1$, h induces the homomorphism $h_* : \pi_1(S^1) \to \pi_1(S^1)$. The law of exponents implies that...

$$h_*(\theta \mapsto e^{\pi im\theta}) = (\theta \mapsto (e^{\pi im\theta})^n = e^{\pi inm\theta}),$$

that is, h_* is multiplication by n.

We first consider a special case of the theorem - suppose...

$$|a_{n-1}| + |a_{n-2}| + \cdots + |a_0| < 1.$$

Suppose $p(z)$ has no root in $e^2 = \{z \in \mathbb{C} | \, |z| \leq 1\}$. Define the mapping $\hat{p} : e^2 \to \mathbb{R}^2 \setminus \{0\}$ by $\hat{p}(z) = p(z)$. Restricting to $S^1 = \partial e^2$ we get $\hat{p} \restriction: S^1 \to \mathbb{R}^2 \setminus \{\mathbf{0}\}$. Since $\hat{p} \restriction$ can be extended to e^2, it follows that $\hat{p} \restriction$ is homotopic to a constant map. However, consider the mapping...

$$F(z,t) = z^n + t(a_{n-1}z^{n-1} + \cdots + a_0),$$

which gives a homotopy between $F(z,0) = z^n$ and $F(z,1) = p(z)$. If $F(z,t)$ never vanishes on S^1, the homotopy implies $\hat{p} \restriction \simeq z^n$. To establish this condition, for $|z| = 1$ we estimate...

$$\begin{aligned} |F(z,t)| &\geq |z^n| - |t(a_{n-1}z^{n-1} + \cdots + a_0)| \\ &\geq 1 - t(|a_{n-1}z^{n-1}| + \cdots + |a_0|) \\ &= 1 - t(|a_{n-1} + \cdots + |a_0|) > 0. \end{aligned}$$

As a class in $\pi_1(S^1)$, $[(z \mapsto z^n)]$ is not homotopic to the constant map while $\hat{p} \restriction$ is, so we get a contradiction.

To reduce the general case to this special case, let $t \in \mathbb{R}$, $t \neq 0$, and let $u = tz$. So...

$$\begin{aligned} p(u) &= u^n + a_{n-1}u^{n-1} + \cdots + a_1u + a_0 \\ &= (tz)^n + a_{n-1}(tz)^{n-1} + \cdots + a_1tz + a_0. \end{aligned}$$

If $p(u) = 0$, then...

$$z^n + \frac{a_{n-1}}{t}z^{n-1} + \cdots + \frac{a_1}{t^{n-1}}z + \frac{a_0}{t^n} = 0.$$

So given a zero for $p(u)$ we get a zero for $\tilde{p}_t(z)$ with $\tilde{p}_t(z) = z^n + \frac{a_{n-1}}{t}z^{n-1} + \cdots + \frac{a_0}{t^n}$ and vice versa. Taking t large enough we can guarantee...

$$|\frac{a_{n-1}}{t}| + \cdots + |\frac{a_1}{t^{n-1}}| + |\frac{a_0}{t^n}| < 1$$

and we can apply the special case. $\square$

18.3 Sketch of Proof in Complex Analysis

Let $f \in \mathbb{C}[x]$ be a nonconstant polynomial; the task consists of proving that f has a root in $\mathbb{C}$. Whatever $f(0)$ is, we can find an $r \in \mathbb{R}$ large enough that $|f(z)| > |f(0)|$ for all z on the circle $|z| = r$ (since f is nonconstant, $\lim_{z\to\infty}|f(z)| = +\infty$). The disk $|z| \leq r$ is compact, so the continuous function $|f(z)|$ has a minimum on it; by the choice of r, it must be somewhere in the interior of the disk, say at $z = a$. The *minimum modulus principle* then implies that $f(z) = 0$.

19 Dimension

19.1 Dimensions are Equinumerous

Theorem 19.1.1. *There is a one-to-one correspondence* $\mathbb{R} \to \mathbb{R} \times \mathbb{R}$.

Proof. Since the mapping $f : \mathbb{R} \to (0,1)$ given by $r \mapsto \frac{1}{\pi}(\arctan(r) + \frac{\pi}{2})$ is a bijection, it is sufficient to find a bijection $(0,1) \to (0,1) \times (0,1)$. For this we use the Schröder-Bernstein Theorm.

Observe that $g : (0,1) \to (0,1) \times (0,1)$ given by $t \mapsto (t,t)$ is an injection. So the only real work is in constructing an injection $(0,1) \times (0,1) \to (0,1)$.

To start things off, introduce the following injection $I : (0,1) \to (0,1) \cap (\mathbb{R} \setminus \mathbb{Q})$...

$$I(r) = \begin{cases} [0; a_1+2, a_2+2, \ldots, a_n+2, 2, 2, \ldots] & \text{if } r = [0; a_1, a_2, \ldots, a_n], \\ [0; a_1+2, a_2+2, a_3+2, \ldots] & \text{if } r = [0; a_1, a_2, a_3, \ldots]. \end{cases}$$

Composed with another injection, $t : (0,1) \cap (\mathbb{R} \setminus \mathbb{Q}) \times (0,1) \cap (\mathbb{R} \setminus \mathbb{Q}) \to (0,1)$ given by $([0; a_1, a_2, \ldots], [0; a_1, a_2, \ldots]) \mapsto [0; a_1, b_1, a_2, b_2, \ldots]$, we get our desired injection $t \circ (I \times I)$. $\square$

Corollary 19.1.1. *There is a bijection* $f : \mathbb{R}^m \to \mathbb{R}^n$ *for all positive integers* m *and* n.

19.2 Space Filling Curves

19.2.1 Peano Curve

19.2.1.1 Ternary Expansion

$$r = 0.t_1t_2t_3\cdots = \sum_{i=1}^{\infty} t_i/3^i, \text{ where } t_i \in \{0,1,2\}$$

Such a representation is unique except in the special cases:

$$r = 0.t_1t_2\ldots t_n222\cdots = 0.t_1t_2\cdots t_{n-1}(t_n+1)000\cdots, \text{ where } t_n \neq 2.$$

19.2.2 Definition

Let $\sigma \in S_3$ such that $\sigma(0) = 2$, $\sigma(1) = 1$, $\sigma(2) = 0$. We let σ act on $r = 0.t_1t_2t_3\cdots$ as...

$$1 - r = 0.222\cdots - 0.t_1t_2t_3\cdots = 0.(\sigma t_1)(\sigma t_2)(\sigma t_3)\cdots$$

Then the peano curve $PE : [0,1] \to [0,1] \times [0,1]$ is defined as...

$$PE(0.t_1t_2\cdots t_n\cdots) = (0.a_1a_2\cdots a_n\cdots, 0.b_1b_2\cdots b_n\cdots)$$

where...

$$a_n = \sigma^{t_2+t_4+\cdots+t_{2(n-1)}}(t_{2n-1})$$

$$b_n = \sigma^{t_1+t_3+\cdots+t_{2n-1}}(t_{2n})$$

Observe that the Peano Curve definition can be written recursively as...

$$PE(0.t_1t_2t_3\cdots) = (0.t_1, \sigma^{t_1}t_2) + (\sigma^{t_2}, \sigma^{t_1}) \circ \frac{PE(0.t_3t_4t_5\dots)}{3}$$

Theorem 19.2.1. *The function $PE : [0,1] \to [0,1] \times [0,1]$ is well defined, continuous, and surjective.*

Proof. We show the PE is well defined. Using the recursive definition, we reduce the question of well-definedness to comparing the values $PE(0.0222\cdots)$ and $PE(0.1000\cdots)$ and the values $PE(0.1222\cdots)$ and $PE(0.2000\cdots)$. Applying the definition we find...

$$PE(0.0222\cdots) = (0.0222\cdots, 0.222\cdots)$$

and...

$$PE(0.1000\cdots) = (0.1000\cdots, 0.222\cdots).$$

The ambiguity in ternary expansions implies $PE(0.0222\cdots) = PE(0.1000\cdots)$.

Similarly we have...

$$PE(0.1222\cdots) = (0.1222\cdots, 0.000\cdots)$$

and...

$$PE(0.2000\cdots) = (0.2000\cdots, 0.000\cdots),$$

and so $PE(0.1222\cdots) = PE(0.2000\cdots)$.

We next show that PE is surjective. Suppose $(u,v) \in [0,1] \times [0,1]$. We write...

$$(u,v) = (0.a_1a_2a_3\cdots, 0.b_1b_2b_3\cdots).$$

Let $t_1 = a_1$. Then $t_2 = \sigma^{t_1}b_1$. Since $\sigma \circ \sigma = id$, we have $\sigma^{t_1}t_2 = \sigma^{t_1} \circ \sigma^{t_1}b_1 = b_1$. Next let $t_3 = \sigma^{t_2}a_2$. Continue in this manner to define...

$$t_{2n-1} = \sigma^{t_2+t_4+\cdots+t_{2(n-1)}}a_n, \quad t_{2n} = \sigma^{t_1+t_3+\cdots+t_{2n-1}}b_n.$$

Then $PE(0.t_1t_2t_3\cdots) = (0.a_1a_2a_3\cdots, 0.b_1b_2b_3\cdots) = (u,v)$ and PE is surjective.

Finally, we show PE is continuous. We use the fact that $[0,1]$ is a first countable space and show that for all $r \in [0,1]$, whenever $\{r_n\}$ is sequence of points in $[0,1]$ with $\lim_{n\to\infty} r_n = r$, then $\lim_{n\to\infty} PE(r_n) = PE(r)$.

Suppose $r = 0.t_1t_2t_3\cdots$ has a unique ternary representation. For any $\varepsilon > 0$, we can choose $N > 0$ with $\varepsilon > 1/3^N > 0$. Then the value of $PE(r)$ is determined up to the first N ternary digits in each coordinate by the first $2N$ digits of the ternary expansion of r. For any sequence $\{r_n\}$ converging to r, there is an index $M = M(2N)$ with the property that for $m > M$, the first $2N$ ternary digits of r_m

agree with those of r. It follows that the first N ternary digits of each coordinate of $PE(r_m)$ agree with those of $PE(r)$ and so $\lim_{n\to\infty} PE(r_n) = PE(r)$.

In the case that r has two ternary representations,

$$r = 0.t_1t_2t_3\cdots t_N000\cdots = 0.t_1t_2t_3\cdots(t_N-1)222\cdots,$$

with $t_N \neq 0$, we can apply the familiar trick of the calculus of considering convergence from above or below the valur r. Suppose $\{r_n\}$ is a sequence in $[0,1]$ with $\lim_{n\to\infty} r_n = r$ and $r \le r_n$ for all n. Then for some index M, when $m > M$ we have $r_m = 0.t_1t_2t_3\cdots t_N t'_{N+1}t'_{N+2}\cdots$. We can now argue as above that $\lim_{n\to\infty} PE(r_n) = PE(r)$. On the other side, for a sequence $\{s_n\}$ with $\lim_{n\to\infty} s_n = r$ and $s_n \le r$ for all n, we compare s_n with $r = 0.t_1t_2t_3\cdots(t_N-1)222\cdots$. Once again, we eventually have that $s_m = 0.t_1t_2t_3\cdots(t_N-1)t''_{N+1}t''_{N+2}\cdots$. Convergence of the series $\{s_n\}$ implies that more of the ternary expansion agrees with r as n grows larger, and so $\lim_{n\to\infty} PE(r_n) = PE(r)$. Since convergence from each side implies general convergence, we have proved that PE is continuous. $\square$

19.3 Connectedness

Lemma 19.3.1. *If $f : X \to Y$ is a homeomorphism and $x \in X$, then f induces a homeomorphism between $X \setminus \{x\}$ and $Y \setminus \{f(x)\}$.*

Theorem 19.3.1 (Invariance of Dimension for $(1,n)$)**.** *$\mathbb{R}$ is not homeomorphic to $\mathbb{R}^n$, for $n > 1$.*

Proof. Suppose we had a homeomorphism $h : \mathbb{R} \to \mathbb{R}^n$. By composing with a translation we arrange that $h(0) = \mathbf{0} = (0,0,\ldots,0) \in \mathbb{R}^n$. By the previous lemma, we consider the homeomorphism $h\restriction : \mathbb{R}\setminus\{0\} \to \mathbb{R}^n \setminus \{\mathbf{0}\}$. But $\mathbb{R}\setminus\{0\}$ has two connected components. To demonstrate invariance of dimension in this case we show for $n > 1$ that $\mathbb{R}^n\setminus\{\mathbf{0}\}$ has only one component. Fix the connected subset of $\mathbb{R}^n\setminus\{\mathbf{0}\}$ has only one component. Fix the connected subset of $\mathbb{R}^n\setminus\{\mathbf{0}\}$, given by...

$$Y = \{(x_1, 0, \ldots, 0) | x_1 > 0\}.$$

This is an open ray, which we know to be connected. We can express $R^n \setminus \{\mathbf{0}\}$ as a union:

$$\mathbb{R}^n \setminus \{\mathbf{0}\} = \bigcup_{r>0} rS^{n-1} \cup Y,$$

where $rS^{n-1} = \{(a_1,\ldots,a_n) \in \mathbb{R}^n | a_1^2 + \cdots + a_n^2 = r^2\}$. Each subset in the union is connected since it is the union of a homeomorphic copy of S^{n-1} and Y with nonempty intersection. The intersetion of all the sets in the union is Y and so, by 13.4.1, $\mathbb{R}^n \setminus \{\mathbf{0}\}$ is connected and thus has only one component. $\square$

19.4 Homotopy

Theorem 19.4.1 (Invariance of Dimension for $(2,n)$)**.** *For $n \neq 2$, $\mathbb{R}^n$ and $\mathbb{R}^2$ are not homeomorphic.*

Proof. We assume that $n \geq 2$ since the case of $n = 1$ is covered in the preceding section. If $\mathbb{R}^n \cong \mathbb{R}^2$, then, by composing with a translation if needed, we can choose a homeomorphism $f : \mathbb{R}^n \to \mathbb{R}^2$ for which $f(\mathbf{0}) = (0, 0)$. Such a mapping induces a homeomorphsim $\mathbb{R} \setminus \{\mathbf{0}\} \cong \mathbb{R}^2 \setminus \{(0, 0)\}$. Since S^{n-1} is a deformation retract of $\mathbb{R}^n \setminus \{\mathbf{0}\}$, by 16.3.1, $\pi_1(\mathbb{R}^n \setminus \{\mathbf{0}\}) \cong \pi_1(S^{n-1})$. For $n > 2$, 16.3.1 states that $\pi_1(S^{n-1}) \cong \{e\}$, while, for $n = 2$, $\pi_1(S^1) \cong \mathbb{Z}$. Since the fundamental group is a topological invariant, it must be the case that $n = 2$. □

19.5 Homology

Theorem 19.5.1 (Invariance of Dimension for (m, n))**.** *If $\mathbb{R}^m$ is homeomorphic to $\mathbb{R}^n$, then $m = n$.*

Proof. We make this a question about simplicial complexes by using the one-point compactification. If $\mathbb{R}^n$ is homeomorphic to $\mathbb{R}^m$, then their one-point compactifications are homeomorphic. Since $\mathbb{R}^l \cup \{\infty\}$ is homeomorphic to S^l, it follows that $\mathbb{R}^n \cong \mathbb{R}^m$ implies $S^n \cong S^m$.

By the topological invariance of homology, and the homeomorphism $S^n \cong |\text{bdy } \Delta^{n+1}|$, we have...

$$H_p(S^n; \mathbb{F}_2) \cong H_p(\text{bdy } \Delta^{n+1}; \mathbb{F}_2) \cong \begin{cases} \mathbb{F}_2, & p = 0, n, \\ \{0\}, & \text{else.} \end{cases}$$

If $S^n \cong S^m$, then $H_p(S^n; \mathbb{F}_2) \cong H_p(S^m; \mathbb{F}_2)$ for all p and, by out computation of the homology of spheres, this is only possible if $n = m$. □

20 Algebraic Geometry

References

[1] John McCleary. *A First Course in Topology: Continuity and Dimension* American Mathematical Society, 2006.

[2] Miklós Bóna. *Introduction to Enumerative and Analytic Combinatorics: Second Edition* CRC Press, 2016.

[3] Paolo Aluffi. *Algebra: Chapter 0* American Mathematical Society, 2009.

[4] Saunders Mac Lane. *Categories for the Working Mathematician: Second Edition* Springer-Verlag, 1998.

[5] Herbert B. Enderton. *Elements of Set Theory* Academic Press, 1977.

[6] Stephen Abbott *Understanding Analysis* Springer, 2015.