

Part I

Topology

Definition 0.1 — Topology and Topological Space.

Let X be a nonempty set. A set \mathcal{T} of subsets of X is said to be a topology on X if

1. X and the empty set \emptyset belong to \mathcal{T}
2. the union of arbitrary many number of sets in \mathcal{T} belong to \mathcal{T}
3. the intersection of any two sets in \mathcal{T} belongs to \mathcal{T}

The pair (X, \mathcal{T}) is called a topological space.

Definition 0.2 — Discrete Topology.

Let X be any nonempty set and \mathcal{T} be the collection of all subsets of X . Then \mathcal{T} is called the discrete topology on the set X . The topological space (X, \mathcal{T}) is called a discrete space.

Definition 0.3 — Indiscrete Topology.

Let X be any nonempty set and $\mathcal{T} = \{\mathcal{T}, \emptyset\}$. Then \mathcal{T} is called the indiscrete topology and (X, \mathcal{T}) is said to be an indiscrete space.

Proposition 1. *If (X, \mathcal{T}) is a topological space such that for every $x \in X$ the singleton set $\{x\}$ is in \mathcal{T} then \mathcal{T} is the discrete topology.*

Definition 0.4 — .

Let (X, \mathcal{T}) be any topological space. Then the members of \mathcal{T} are said to be open sets.

Proposition 2. *If (X, \mathcal{T}) is any topological space, then*

1. X and \emptyset are open sets.
2. The union of arbitrary many number of open sets is an open set.
3. The intersection of finitely many number of open sets is an open set.

Definition 0.5 — .

Let (X, \mathcal{T}) be a topological space. A subset S of X is said to be a closed set in (X, \mathcal{T}) if its complement in X , namely $X - S$ is open in (X, \mathcal{T}) .

Proposition 3. *If (X, \mathcal{T}) is any topological space, then*

1. \emptyset and X are closed set.
2. The intersection of arbitrary many number of closed sets is a closed set.
3. The union of finitely many number of closed sets is a closed set.

Definition 0.6 — .

A subset S of a topological space (X, \mathcal{T}) is said to be clopen if it is both open and closed in (X, \mathcal{T}) .

Definition 0.7 — .

Let X be any nonempty set. A topology \mathcal{T} on X is called the finite-closed topology or the cofinite topology if the closed subsets of X are X and all finite subsets of X ; that is, the open sets are \emptyset and all subsets of X which have finite complements.

Definition 0.8 — Euclidean Topology.

A subset S of \mathbb{R} is said to be open in the euclidean topology on \mathbb{R} if for each $x \in S$, there exist $a, b \in \mathbb{R}$, with $a < b$, such that $x \in (a, b) \subseteq S$.

Proposition 4. *A subset S of \mathbb{R} is open if and only if it is a union of open intervals.*

Definition 0.9 — Basis for a Topology.

Let (X, \mathcal{T}) be a topological space. A collection \mathcal{B} of open subsets of X is said to be a basis for the topology \mathcal{T} if every open set is a union of members in \mathcal{B} .

Example 0.10. Let $\mathcal{B} = \{(a, b) \mid a, b \in \mathbb{R}, a < b\}$. Then \mathcal{B} is a basis for the euclidean topology on \mathbb{R} .

Example 0.11. Let (X, \mathcal{T}) be a discrete space and \mathcal{B} the family of all singleton subsets of X ; that is, $\mathcal{B} = \{\{x\} \mid x \in X\}$.

Example 0.12. Let $X = \{a, b, c, d, e, f\}$ and

$$\mathcal{T}_1 = \{X, \emptyset, \{a\}, \{c, d\}, \{a, c, d\}, \{b, c, d, e, f\}\} \quad (1)$$

Then $\mathcal{B} = \{a, c, d, b, c, d, e, f\}$ is a basis for \mathcal{T}_1 as $\mathcal{B} \subseteq \mathcal{T}_1$ and every member of \mathcal{T}_1 can be expressed as a union of members of \mathcal{B} . Note that \mathcal{T}_1 itself is also a basis for \mathcal{T}_1 .

Proposition 5. *Let X be a nonempty set and let \mathcal{B} be a collection of subsets of X . Then \mathcal{B} is a basis for a topology on X if and only if \mathcal{B} has the following properties:*

1. $X = \bigcup_{B \in \mathcal{B}} B$
2. for any $B_1, B_2 \in \mathcal{B}$ the set $B_1 \cap B_2$ is a union of members of \mathcal{B}

Proposition 6. *Let (X, \mathcal{T}) be a topological space. A family \mathcal{B} of open subsets of X is a basis for \mathcal{T} if and only if for any point x belonging to any open set U there is a $B \in \mathcal{B}$ such that $x \in B \subseteq U$*

Proposition 7. *Let \mathcal{B} be a basis for a topology \mathcal{T} on a set X . Then a subset U of X is open if and only if for each $x \in U$ there exists a $B \in \mathcal{B}$ such that $x \in B \subseteq U$.*

Proposition 8. *Let \mathcal{B}_1 and \mathcal{B}_2 be bases for topologies \mathcal{T}_1 and \mathcal{T}_2 respectively, on a nonempty set X . Then $\mathcal{T}_1 = \mathcal{T}_2$ if and only if*

1. for each $B \in \mathcal{B}_1$ and each $x \in B$, there exists a $B' \in \mathcal{B}_2$ such that $x \in B' \subseteq B$
2. for each $B \in \mathcal{B}_2$ and each $x \in B$, there exists a $B' \in \mathcal{B}_1$ such that $x \in B' \subseteq B$

Part II

Other Stuff

Definition 0.13 — Euler Totient Function.

The Euler totient function counts the positive integers up to a given integer n that are relatively prime to n .

Part III

Commutative Rings

Chapter 1

Rings and Ideals

1.1 Cheat Sheet

Definition 1.1 — Ring.

A ring is a set R equipped with two binary operations $+$ (addition) and \cdot (multiplication) satisfying the following three sets of axioms, called the ring axioms.

1. $(R, +)$ is an abelian group.
2. (R, \cdot) is a semigroup.
3. Multiplication is distributive with respect to addition, meaning that
 - $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in R$ (left distributivity).
 - $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ for all $a, b, c \in R$ (right distributivity).

A ring is called unitary if it contains the multiplicative identity and commutative if multiplication is commutative.

Definition 1.2 — Unit.

Definition 1.3 — Zerodivisors.

Definition 1.4 — Nilpotent.

Definition 1.5 — Idempotent.

Definition 1.6 — Ideal.

Definition 1.7 — Operations on Ideals.

Let R be a ring $\{\mathfrak{a}_i\}_{i \in I}$ be a collection of ideals in R .

1.

$$\sum_{i \in I} \mathfrak{a}_i = \left\{ \sum_{i \in I} a_i \mid a_i \in \mathfrak{a}_i \text{ for all } i \in I, \text{ and } a_i = 0 \text{ for almost all } i \right\} \quad (1.1)$$

2. The transporter of two ideals is defined By

$$(\mathfrak{a} : \mathfrak{b}) := \{ x \in R \mid x\mathfrak{b} \subset \mathfrak{a} \} \quad (1.2)$$

Definition 1.8 — Prime Ideal.

Definition 1.9 — Maximal Ideal.

Definition 1.10 — Quotient Ring.

Given a ring A and two-sided ideal \mathfrak{a} in A , we may define an congruence relation \sim on A as follows:

$$x \sim y :\iff x - y \in \mathfrak{a}. \quad (1.3)$$

The equivalence class of the element x in A is given by

$$[x] = x + \mathfrak{a} := \{x + a \mid a \in \mathfrak{a}\} \quad (1.4)$$

and the set of all such equivalence classes is denoted by A/\mathfrak{a} ; it becomes a ring, the factor ring or the quotient ring of A modulo \mathfrak{a} , if one defines

1. $(a + \mathfrak{a}) + (b + \mathfrak{a}) = (a + b) + \mathfrak{a}$
2. $(a + \mathfrak{a})(b + \mathfrak{a}) = (ab) + \mathfrak{a}$

The map $\pi : R \longrightarrow A/\mathfrak{a}$, $x \mapsto \pi(x) := x + \mathfrak{a}$ is a surjective ring homomorphism and is sometimes called the natural quotient map or the canonical homomorphism.

Proposition 9 (Universal Property). *Let A and B be rings, \mathfrak{a} an ideal, and $f : A \longrightarrow B$ a ring homomorphism with $\mathfrak{a} \subseteq \text{Ker}(f)$. Then there exists a unique ring homomorphism $\tilde{f} : A/\mathfrak{a} \longrightarrow B$ such that $f = \tilde{f} \circ \pi$.*

Theorem 1.11. *There is a bijection between the sets*

$$\{ \mid \} \quad (1.5)$$

Definition 1.12 — Integral Domain.

Theorem 1.13. • *prime ideal, quotient is integral domain*

- *same as above, but if prime maximal, then quotient is a fields*
- *Maximal ideals are prime ideals.*

Definition 1.14 — Unique Factorization Domain.**Definition 1.15 — Principal Ideal Domain.**

Proposition 10. *Commutative Rings \supset Unique Factorization Domain \supset Principal Ideal Domain \supset Fields*

Theorem 1.16. • *prime ideal, quotient is integral domain*

- *same as above, but if prime maximal, then quotient is a fields*
- *Maximal ideals are prime ideals.*
- *There is a 1:1 correspondence*

$$\{ \text{Ideals in } A/\mathfrak{a} \} \longleftrightarrow \{ \mathfrak{b}/\mathfrak{a} \mid \mathfrak{a} \subseteq \mathfrak{b} \subseteq A \} \quad (1.6)$$

Proof. For the last point, it is easier to understand with extension and contraction. □

1.2 Examples

Example 1.17. 1. \mathbb{Z}

2. All fields.
3. Let S be any set, then $(\mathcal{P}(S), \Delta, \cap)$ is a ring.
4. continuous $f : I \longrightarrow \mathbb{R}$ with a real interval I forms a ring.
5. cartesian product of rings

Example 1.18. Let S be any set, then $(2^S, \Delta, \cap)$ is a ring.

1. $0 = \emptyset$ and $-A = A$

2. The neutral element of the multiplication is S .
3. $(2^S)^\times = \{S\}$
4. $\text{ZD}(2^S) = 2^S - S$ since $A \cap A^c = \emptyset$ (also minus the empty set) (this seems to be true for all boolean rings)
5. $\text{Nil}(2^S) = \emptyset$ (seems to be true for all boolean rings)
6. $\langle A \rangle = 2^A$ contains all subset of A

Example 1.19 (Integral Domains). 1. $\mathbb{Z}[i]$ the Gaussian integers, $(\mathbb{Z}[i])^\times = \{\pm 1, \pm i\}$

2. $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \mid \gcd(a, n) = 1\}$, $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$ (Euler totient function)

1.3 Proofs

1.4 Exercises

Exercise 1.20. Let $\varphi : R \rightarrow R'$ be a ring homomorphism, $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ ideals of R , and $\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3$ ideals of R' . Prove the following statements. Prove the following statements:

1. $(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e$

Proof. We show $(\mathfrak{a}_1 + \mathfrak{a}_2)^e \subseteq \mathfrak{a}_1^e + \mathfrak{a}_2^e$. Let $x \in (\mathfrak{a}_1 + \mathfrak{a}_2)^e$, then we have for some index set I

$$x = \sum_{i \in I} \lambda_i x_i, \quad (1.7)$$

where $\lambda_i \in R'$ and $x_i \in \varphi(\mathfrak{a}_1 + \mathfrak{a}_2)$ for all $i \in I$. For each $i \in I$ we find and $a_{i,1}, a_{i,2} \in \mathfrak{a}$ such that $x_i = \varphi(a_{i,1} + a_{i,2})$, hence

$$x = \sum_{i \in I} \lambda_i (a_{i,1} + a_{i,2}) \quad (1.8)$$

$$= \sum_{i \in I} \lambda_i (\varphi(a_{i,1}) + \varphi(a_{i,2})) \quad (\text{by linearity}) \quad (1.9)$$

$$= \sum_{i \in I} \lambda_i \varphi(a_{i,1}) + \lambda_i \varphi(a_{i,2}) \quad (\text{by distributivity}) \quad (1.10)$$

$$= \sum_{i \in I} \lambda_i \varphi(a_{i,1}) + \sum_{i \in I} \lambda_i \varphi(a_{i,2}) \quad (\text{reordering the sum}). \quad (1.11)$$

$$(1.12)$$

The last term is exactly the elements expressed by $\mathfrak{a}_1^e + \mathfrak{a}_2^e$, therefore, $(\mathfrak{a}_1 + \mathfrak{a}_2)^e \subseteq \mathfrak{a}_1^e + \mathfrak{a}_2^e$.

I think the above proof should work into both directions. If not, just notice that $\mathfrak{a}_1^e \subseteq (\mathfrak{a}_1 + \mathfrak{a}_2)^e$. \square

2. $(\mathfrak{b}_1 + \mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c + \mathfrak{b}_2^c$

Proof. We have

$$(\mathfrak{b}_1 + \mathfrak{b}_2)^c = \{x \in A \mid \exists b_1 \in \mathfrak{b}_1 \exists b_2 \in \mathfrak{b}_2 : \varphi(x) = b_1 + b_2\}. \quad (1.13)$$

Now let $x \in \mathfrak{b}_1^c + \mathfrak{b}_2^c$, then $x = a_1 + a_2$ where $\varphi(a_1) \in \mathfrak{b}_1$ and $\varphi(a_2) \in \mathfrak{b}_2$. It is

$$\varphi(x) = \varphi(a_1 + a_2) \quad (1.14)$$

$$= \varphi(a_1) + \varphi(a_2) \quad (\text{by additivity}) \quad (1.15)$$

Since $\varphi(a_1) \in \mathfrak{b}_1$ and $\varphi(a_2) \in \mathfrak{b}_2$ we have that $x \in (\mathfrak{b}_1 + \mathfrak{b}_2)^c$. \square

Chapter 2

Radicals

2.1 Cheat Sheet

2.2 Proofs

2.3 Exercises

Exercise 2.1. Let R be a ring, $\mathfrak{a} \subset \text{Jac}(R)$ an ideal, $u \in R$, and $u + \mathfrak{a}$ its residue in R . Prove that $u \in R^\times$ if and only if $u + \mathfrak{a} \in (R/\mathfrak{a})^\times$. What if $\mathfrak{a} \not\subset \text{Jac}(R)$?

Proof. If $u \in R^\times$, then we have immediately $u \in (R/\mathfrak{a})^\times$ without using the condition $\mathfrak{a} \subset \text{Jac}(R)$.

On the contrary, let $u + \mathfrak{a}$ be a unit

□

Chapter 3

Zariski Topology

Definition 3.1 — Spectrum.

Let R be a ring. We denote the set of all prime ideals of R by $\text{Spec}(R)$ and the set of all maximal ideals of R by $\text{Spm}(R)$.

Definition 3.2 — Variety.

Let R be a ring and \mathfrak{a} an ideal in R . Let $\mathbf{V}(\mathfrak{a})$ denote the subset of $\text{Spec}(R)$ consisting of those primes that contain \mathfrak{a} , i.e.

$$\mathbf{V}(\mathfrak{a}) := \{ \mathfrak{p} \in \text{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \}. \quad (3.1)$$

We call $\mathbf{V}(\mathfrak{a})$ the variety of \mathfrak{a} .

Proposition 11. *Let R be a ring, and \mathfrak{a} and \mathfrak{b} two ideals in R .*

1. *If $\mathfrak{a} \subset \mathfrak{b}$, then $\mathbf{V}(\mathfrak{b}) \subset \mathbf{V}(\mathfrak{a})$.*
2. *If $\mathbf{V}(\mathfrak{b}) \subset \mathbf{V}(\mathfrak{a})$, then $\mathfrak{a} \subset \sqrt{\mathfrak{b}}$.*
3. *$\mathbf{V}(\mathfrak{a}) = \mathbf{V}(\mathfrak{b})$ if and only if $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$.*
4. *$\mathbf{V}(\mathfrak{a}) \cup \mathbf{V}(\mathfrak{b}) = \mathbf{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathbf{V}(\mathfrak{a}\mathfrak{b})$.*
5. *For any index set I , it is $\bigcap_{i \in I} \mathbf{V}(\mathfrak{a}_i) = \mathbf{V}(\sum_{i \in I} \mathfrak{a}_i)$.*
6. *$\mathbf{V}(\langle 0 \rangle) = \text{Spec}(R)$.*

Definition 3.3 — Zariski Topology.

Declaring $\mathbf{V}(\mathfrak{a})$ to be closed sets induces a topology on $\text{Spec}(R)$, the Zariski topology.

Given an element $f \in R$, we call the open set

$$\mathbf{D}(f) := \text{Spec}(R) - \mathbf{V}(\langle f \rangle) \quad (3.2)$$

a principal open set. These sets form a basis for the topology of $\text{Spec}(R)$; indeed, given any prime $\mathfrak{a} \not\subset \mathfrak{p}$, there is an $f \in \mathfrak{a} - \mathfrak{p}$, and so $\mathfrak{p} \in \mathbf{D}(f) \subset \text{Spec}(R) - \mathbf{V}(\mathfrak{a})$. Further, $f, g \notin \mathfrak{p}$ if and only if $fg \notin \mathfrak{p}$ for any $f, g \in R$ and prime \mathfrak{p} , in other words

$$\mathbf{D}(f) \cap \mathbf{D}(g) = \mathbf{D}(fg) \quad (3.3)$$

3.1 Proofs

Proposition 12. *Let R be a ring, and \mathfrak{a} and \mathfrak{b} two ideals in R .*

1. *If $\mathfrak{a} \subset \mathfrak{b}$, then $\mathbf{V}(\mathfrak{b}) \subset \mathbf{V}(\mathfrak{a})$.*
2. *If $\mathbf{V}(\mathfrak{b}) \subset \mathbf{V}(\mathfrak{a})$, then $\mathfrak{a} \subset \sqrt{\mathfrak{b}}$.*
3. *$\mathbf{V}(\mathfrak{a}) = \mathbf{V}(\mathfrak{b})$ if and only if $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$.*
4. *$\mathbf{V}(\mathfrak{a}) \cup \mathbf{V}(\mathfrak{b}) = \mathbf{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathbf{V}(\mathfrak{a}\mathfrak{b})$.*

Proof.

$$\mathbf{V}(\mathfrak{a}) \cup \mathbf{V}(\mathfrak{b}) = \{ \mathfrak{p} \in \text{Spec}(R) \mid \mathfrak{a} \subset \mathfrak{p} \} \cup \{ \mathfrak{p} \in \text{Spec}(R) \mid \mathfrak{b} \subset \mathfrak{p} \} \quad (3.4)$$

$$= \{ \mathfrak{p} \in \text{Spec}(R) \mid \mathfrak{a} \subset \mathfrak{p} \text{ or } \mathfrak{b} \subset \mathfrak{p} \} \quad (3.5)$$

$$= \{ \mathfrak{p} \in \text{Spec}(R) \mid \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{p} \} \quad (3.6)$$

$$= \mathbf{V}(\mathfrak{a} \cap \mathfrak{b}) \quad (3.7)$$

□

5. For any index set I , it is $\bigcap_{i \in I} \mathbf{V}(\mathfrak{a}_i) = \mathbf{V}(\sum_{i \in I} \mathfrak{a}_i)$.

6. $\mathbf{V}(R) = \emptyset$.

Proof. $\mathbf{V}(R) = \{ \mathfrak{p} \in \text{Spec}(R) \mid R \subset \mathfrak{p} \} = \emptyset$ because by definition a prime ideal must not be the whole ring. □

7. $\mathbf{V}(\langle 0 \rangle) = \text{Spec}(R)$.

Proof. $\mathbf{V}(\langle 0 \rangle) = \{ \mathfrak{p} \in \text{Spec}(R) \mid \langle 0 \rangle \subset \mathfrak{p} \} = \text{Spec}(R)$ because all ideals contain the zeroideal. □

Proposition 13. *The Zariski topology is indeed a topology.*

Proof.

□

3.2 Exercises

Exercise 3.4. Let R be a ring and $\mathfrak{p}, \mathfrak{q} \in \text{Spec}(R)$. Show:

1. The closure $\overline{\{\mathfrak{p}\}}$ of \mathfrak{p} is equal to $\mathbf{V}(\mathfrak{p})$; that is, $\mathfrak{q} \in \overline{\{\mathfrak{p}\}}$ if and only if $\mathfrak{p} \subseteq \mathfrak{q}$.

Proof. Let $\mathfrak{q} \in \overline{\{\mathfrak{p}\}}$. If $f \in R - \mathfrak{p}$, then $\mathfrak{q} \in \mathbf{D}(f)$. □

Exercise 3.5. Describe $\text{Spec}(\mathbb{R})$, $\text{Spec}(\mathbb{Z})$, $\text{Spec}(\mathbb{C}[X])$, and $\text{Spec}(\mathbb{R}[X])$.

Proof. 1. $\text{Spec}(\mathbb{R}) = \{ \langle 0 \rangle \}$ because the only ideals in a field are the zeroideal and the field itself.

2. $\text{Spec}(\mathbb{Z}) = \{ p\mathbb{Z} \mid p \text{ is a prime number} \}$.

3. $\text{Spec}(\mathbb{C}[X]) = \{ \langle X - z \rangle \mid z \in \mathbb{C} \}$ because $\mathbb{C}[X]$ is a PID and because of the fundamental theorem of algebra.

4. $\text{Spec}(\mathbb{R}[X])$ has the ideals above and all polynomials of degree two with complex roots.

For any PID R , the points x_p of $\text{Spec}(R)$ represents the ideals $\langle p \rangle$ with p prime or 0. The closed sets are the $\mathbf{V}(\langle a \rangle)$ with $a \in R$; moreover, $\mathbf{V}(\langle a \rangle) = \emptyset$ if a is a unit, $\mathbf{V}(\langle 0 \rangle) = R$, and $\mathbf{V}(\langle a \rangle) = x_{p_1} \cup \dots \cup x_{p_s}$ if $a = p_1^{n_1} \dots p_s^{n_s}$ with p_i a prime and $n_i \leq 1$. □

Exercise 3.6. Let R be a ring, and let $X_1, X_2 \subset \text{Spec}(R)$ closed subsets. Show that the following four statements are equivalent:

1. Then $X_1 \sqcup X_2 = \text{Spec}(R)$; that is, $X_1 \cup X_2 = \text{Spec}(R)$ and $X_1 \cap X_2 = \emptyset$.
2. There are complementary idempotents $e_1, e_2 \in R$ with $\mathbf{V}(\langle e_i \rangle) = X_i$.

Proof. "1. to 2." Since X_1 and X_2 are closed subsets, there are ideals \mathfrak{a}_1 and \mathfrak{a}_2 such that

$$\text{Spec}(R) = \mathbf{V}(\mathfrak{a}_1) \cup \mathbf{V}(\mathfrak{a}_2) = \mathbf{V}(\mathfrak{a}_1 \mathfrak{a}_2) \quad (3.8)$$

$$\emptyset = \mathbf{V}(\mathfrak{a}_1) \cap \mathbf{V}(\mathfrak{a}_2) = \mathbf{V}(\mathfrak{a}_1 + \mathfrak{a}_2) \quad (3.9)$$

If two variety are equal, the radical of the generating ideals are equal, hence $\sqrt{\langle 0 \rangle} = \sqrt{\mathfrak{a}_1 \mathfrak{a}_2}$ and $\sqrt{R} = \sqrt{\mathfrak{a}_1 + \mathfrak{a}_2}$. □

Part IV

Modules

