Commutative Ring Theory

Kei Thoma

February 21, 2023

Contents

Notes taken from

- my courses
- Altman, Kleinman: A Term of Commutative Algebra
- Wikipedia
- Math Stackexchange

Chapter 1

To Do

1. add addendum
   (a) for abelian group
   (b) for semigroup
2. after definition of ring, add that identity and inverse are unique as a remark
3. after ring homomorphism, add general properties of image, kernel etc.

Part I

Rings

Chapter 2

Rings and Homomorphisms

Cheat Sheet

Definition 1. A ring is a set A equipped with two binary operations $+$ (addition) and $\cdot$ (multiplication) where $(A, +)$ is an abelian group, $(A, \cdot)$ is a commutative monoid, and the multiplication is distributive with respect to addition.

Definition and Theorems

Rings

Definition 2 (Ring)**.** A ring is a set A equipped with two binary operations $+$ (addition) and $\cdot$ (multiplication) satisfying the following three sets of axioms, called the ring axioms.

1. $(A, +)$ is an abelian group, i.e.
   (a) The operation $+$ is well-defined meaning for all pairs a and b of A, $a+b$ is defined and belongs to A.
   (b) (Associativity) For all a, b, and c in A, it is $(a+b)+c = a+(b+c)$.
   (c) (Identity Element) There exists an element 0 in A such that for all elements a in A, it is $0+a = a+0 = 0$.
   (d) (Inverse Element) For each a in A there exists an element $b \in A$ such that $a+b = b+a = 0$.
   (e) (Commutativity) For all a and b in A, it is $a+b = b+a$.
2. $(A, \cdot)$ is a semigroup, i.e.
   (a) The operation $\cdot$ is well-defined meaning for all pairs a and b of A, $a \cdot b$ is defined and belongs to A.
   (b) (Associativity) For all a, b, and c in A, it is $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. Multiplication is distributive with respect to addition, meaning that
   - $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in A$ (left distributivity).
   - $(b+c) \cdot a = (b \cdot a) + (c \cdot a)$ for all $a, b, c \in A$ (right distributivity).

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

Intuition. A ring may be understood as the generalization of the integers.
Another way to see rings is a less well behaved field where the theory of dividing is due to rings missing the multiplicative identity richer.

Remark. In this text, we will primarily be concerned with commutative unitary rings, and thus, for brevity sake, we simply write “ring” and mean a commutative unitary ring.

Example 2.1. Some important examples of rings include the following.

1. The prototypical example is the ring of integers $\mathbb{Z}$ with the two operations being of addition and multiplication.
2. Any field is a ring. In particular, the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are rings.
3. The zero ring or trivial ring is the unique ring consisting of one element 0 with the operations $+$ and $\cdot$ defined such that $0+0=0$ and $0 \cdot 0 = 0$. It is the unique ring in which the additive and the multiplicative identity coincide.
4. the set of polynomials
5. an example of a finite ring
6. If S is a set, then the power set $\mathcal{P}(S)$ of S becomes a ring if we define addition to be the symmetric difference of sets and multiplication to be intersection.

Example 2.2. Moreover, we have some examples of rings that are non-commutative or non-unitary.

1. Matrix ring is non-commutative

Example 2.3. Counterexamples of rings include the following.

1. The set of natural numbers $\mathbb{N}$ with the usual operations is not a ring, since $(\mathbb{N}, +)$ is not even a group.
2. Trivially, the emptyset regardless of the operations is not a ring.

Definition 3 (Subring)**.** A subset S of A is called a subring if any of the following equivalent conditions holds.

Proposition 4. Let A be a ring and R and S subrings of A.

1. (ANY?) intersection stable
2. cartesian product is again a ring

Example 4.1. 1. Complement, of course not.

2. union, of course not.
3. difference, of course not
4. symmetric difference, of course not

Ring Homomorphisms

Definition 5 (Ring Homomorphism)**.** A homomorphism from ring $(A, +, \cdot)$ to a ring $(B, \boxplus, \boxdot)$ is a map φ from A to B that preserves the ring operations.

Remark. A ring homomorphism induces a group homomorphism and a monoid homomorphism.

Example 5.1. examples of ring homomorphism.

Proposition 6. Let $f : A \to B$ be a ring homomorphism.

1. A ring homomorphism preserves the additive identity, i.e. $f(0_A) = 0_B$.

Image, Kernel, Preimage, and Cokernel

Proposition 7. Let $\varphi : A \to B$ a ring homomorphism, and S a subring of A.

1. A ring homomorphism preserves subrings, i.e. $\varphi(S)$ is a subring of B. In particular, $\operatorname{im}(\varphi)$ is a subring of B.

Remark. Let $\varphi : A \to B$ a ring homomorphism. The kernel is often not a subring.

Notes

Chapter 3

Ideals

Definition and Theorems

Ideals

Definition 8 (Ideal)**.** Let A be a ring. A subset $\mathfrak{a} \subset A$ is called an ideal if it satisfies the following two conditions.

1. $(\mathfrak{a}, +)$ is a subgroup of $(A, +)$.
2. For every $r \in A$ and every $x \in \mathfrak{a}$, it is $rx \in \mathfrak{a}$.

Given a subset $S \subset A$, by the ideal (S) that S generates, we mean the smallest ideal containing S. If an ideal is generated by a subset $S \subset A$, then the elements of this subset are called generators.
An ideal that is generated by a single element is called principal.
If an ideal $\mathfrak{a}$ is not the whole ring A, then the ideal is called proper.

Ideal Operations

Definition 9 (Ideal Operations)**.** Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of a ring A.

1. The sum of two ideals $\mathfrak{a}$ and $\mathfrak{b}$ is defined by
$$\mathfrak{a} + \mathfrak{b} = \{\, a + b \mid a \in \mathfrak{a} \text{ and } b \in \mathfrak{b} \,\} = (\mathfrak{a}, \mathfrak{b})$$
which is again an ideal. It is the smallest ideal in A that contains $\mathfrak{a}$ and $\mathfrak{b}$.
2. The product of an ideal
3. The intersection of
4. The radical of an ideal $\mathfrak{a}$ is defined by
$$\sqrt{\mathfrak{a}} = \{\, x \in A \mid x^n \in \mathfrak{a} \text{ for some } n \in \mathbb{N}^+ \,\}$$
which is again an ideal.
5. The transporter

Proof. We verify the statements made in the definition.

1. (a) "$\mathfrak{a} + \mathfrak{b}$ is an ideal.":

$\square$

Example 9.1. The union of two ideals is **not** an ideal in general. Consider (2) and (3) in $\mathbb{Z}$. If $(2) \cup (3)$ was an ideal, then $3 - 2 = 1$ would be contained in $(2) \cup (3)$. But $1 \notin (2)$ and $1 \notin (3)$, thus $1 \notin (2) \cup (3)$.

Proposition 10. Let $\mathfrak{a}$ be an ideal of A.

1. $\mathfrak{a} = A$ if and only if $1 \in \mathfrak{a}$ if and only if $\mathfrak{a}$ contains an unit.
2. $\mathfrak{a}^2 \subset \mathfrak{a}$.
3. $\mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a} + \mathfrak{b}$.
4. $\mathfrak{a} \subset \mathfrak{a} + \mathfrak{b}$ and $\mathfrak{b} \subset \mathfrak{a} + \mathfrak{b}$.

Proposition 11. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals of a ring A.

1. $\mathfrak{a} \subset \sqrt{\mathfrak{a}}$.
2. $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$.
3. If $\mathfrak{a} \subset \mathfrak{b}$, then $\sqrt{\mathfrak{a}} \subset \sqrt{\mathfrak{b}}$.
4. $\sqrt{\mathfrak{a}} = A$ if and only if $\mathfrak{a} = A$.
5. $\sqrt{\mathfrak{a} \cdot \mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$.
6. $\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$.
7. If $\mathfrak{a} = \mathfrak{p}^n$ for some prime ideal $\mathfrak{p}$ and $n \in \mathbb{N}^+$, then $\sqrt{\mathfrak{a}} = \mathfrak{p}$.

Proof. We verify each statement.

1. Let $x \in \mathfrak{a}$, then trivially, $x^1 \in \mathfrak{a}$, so $x \in \sqrt{\mathfrak{a}}$.

2. Since $\sqrt{\sqrt{\mathfrak{a}}} \supset \sqrt{\mathfrak{a}}$ from above, it suffices to verify the other inclusion. Let $x \in \sqrt{\sqrt{\mathfrak{a}}}$, then $x^n \in \sqrt{\mathfrak{a}}$ and in turn, $(x^n)^m \in \mathfrak{a}$. Thus, $x^{nm} \in \mathfrak{a}$, therefore, $x \in \sqrt{\mathfrak{a}}$.

3. Suppose $\mathfrak{a} \subset \mathfrak{b}$ and let $x \in \sqrt{\mathfrak{a}}$. Then, $x^n \in \mathfrak{a}$ for some $n \in \mathbb{N}^+$, thus $x^n \in \mathfrak{b}$. It follows that $x \in \sqrt{\mathfrak{b}}$.

4. "$\Rightarrow$": Let $\sqrt{\mathfrak{a}} = A$, then for all $x \in A$, we have that $x^n \in \mathfrak{a}$ for some $n \in \mathbb{N}^+$. In particular, $1^n \in \mathfrak{a}$, but $1^n = 1$ for all $n \in \mathbb{N}^+$. Thus, $\mathfrak{a} = A$.

   "$\Leftarrow$": On the other hand, let $\mathfrak{a} = A$. In general, it is $\mathfrak{a} \subset \sqrt{\mathfrak{a}}$, therefore $A \subset \sqrt{\mathfrak{a}}$ which immediately yields the desired equality $A = \sqrt{\mathfrak{a}}$.

5. "$\sqrt{\mathfrak{a} \cdot \mathfrak{b}} \subset \sqrt{\mathfrak{a} \cap \mathfrak{b}}$": If $x \in \sqrt{\mathfrak{a} \cdot \mathfrak{b}}$, then $x^n \in \mathfrak{a} \cdot \mathfrak{b}$ for some $n \in \mathbb{N}^+$. Since $\mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$, we have $x^n \in \mathfrak{a} \cap \mathfrak{b}$, and it follows that $x \in \sqrt{\mathfrak{a} \cap \mathfrak{b}}$.

   "$\sqrt{\mathfrak{a} \cdot \mathfrak{b}} \supset \sqrt{\mathfrak{a} \cap \mathfrak{b}}$": Let $x \in \sqrt{\mathfrak{a} \cap \mathfrak{b}}$, then $x^n \in \mathfrak{a} \cap \mathfrak{b}$ for some $n \in \mathbb{N}^+$. Hence it is $x^n \in \mathfrak{a}$ and $x^n \in \mathfrak{b}$, therefore $x^n \cdot x^n = x^{2n} \in \mathfrak{a} \cdot \mathfrak{b}$. Conclude $x \in \sqrt{\mathfrak{a} \cdot \mathfrak{b}}$.

   "$\sqrt{\mathfrak{a} \cap \mathfrak{b}} \subset \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$": If $x \in \sqrt{\mathfrak{a} \cap \mathfrak{b}}$, then $x^n \in \mathfrak{a} \cap \mathfrak{b}$, thus $x^n \in \mathfrak{a}$ and $x^n \in \mathfrak{b}$. We may write $x \in \sqrt{\mathfrak{a}}$ and $x \in \sqrt{\mathfrak{b}}$, therefore $x \in \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$.

   "$\sqrt{\mathfrak{a} \cap \mathfrak{b}} \supset \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$": Finally, let $x \in \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$. Then, $x\sqrt{\mathfrak{a}}$ and $x\sqrt{\mathfrak{b}}$, so $x^n \in \mathfrak{a}$ and $x^m \in \mathfrak{b}$ for some $n, m \in \mathbb{N}^+$. Say $n \geq m$, then $x^n \in \mathfrak{b}$. This yields $x^n \in \mathfrak{a} \cap \mathfrak{b}$, thus $x \in \sqrt{\mathfrak{a} \cap \mathfrak{b}}$.

6. "$\sqrt{\mathfrak{a}+\mathfrak{b}} \subset \sqrt{\sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}}$": Let $x \in \sqrt{\mathfrak{a}+\mathfrak{b}}$, then $x^n \in \mathfrak{a}+\mathfrak{b}$ for some $n \in \mathbb{N}^+$. By definition of sum of ideals, we have that $x^n = a + b$ for some $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. Since $\mathfrak{a} \subset \sqrt{\mathfrak{a}}$ and $\mathfrak{b} \subset \sqrt{\mathfrak{b}}$, we have $x^n \in \sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}$, thus $x \in \sqrt{\sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}}$.

   "$\sqrt{\mathfrak{a}+\mathfrak{b}} \supset \sqrt{\sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}}$": Now let $x \in \sqrt{\sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}}$, then $x^n \in \sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}$ for some $n \in \mathbb{N}^+$. Hence there exists $a \in \sqrt{\mathfrak{a}}$ and $b \in \sqrt{\mathfrak{b}}$ such that $x^n = a + b$. We have that $a^p \in \mathfrak{a}$ and $b^q \in \mathfrak{b}$ for some $p, q \in \mathbb{N}^+$. Consider

$$\begin{aligned}(x^n)^{(p+q-1)} &= (a+b)^{(p+q-1)} \\ &= \sum_{k=0}^{p+q-1} \binom{p+q-1}{k} a^k \cdot b^{p+q-1-k}.\end{aligned}$$

   For each $k \in \{0, 1, \ldots, p+q-1\}$, we have $a^k \in \mathfrak{a}$ or $b^{p+q-1} \in \mathfrak{b}$. Thus, the whole sum lies in $\mathfrak{a}+\mathfrak{b}$ or in other words $x^{n(p+q-1)} \in \mathfrak{a}+\mathfrak{b}$. Conclude $x \in \sqrt{\mathfrak{a}+\mathfrak{b}}$.

7. "$\sqrt{\mathfrak{a}} \subset \mathfrak{p}$": Let $x \in \sqrt{\mathfrak{a}}$, then $x^m \in \mathfrak{a}$ for some $m \in \mathbb{N}^+$. Because $\mathfrak{a} = \mathfrak{p}^n$, we have $x^m \in \mathfrak{p}^n$. We also have $\mathfrak{p}^n \subset \mathfrak{p}$, thus $x^m \in \mathfrak{p}$ and since $\mathfrak{p}$ is prime, $x \in \mathfrak{p}$.

   "$\sqrt{\mathfrak{a}} \supset \mathfrak{p}$": On the other hand, if $x \in \mathfrak{p}$, then $x^n \in \mathfrak{p}^n = \mathfrak{a}$, therefore $x \in \sqrt{\mathfrak{a}}$.

□

Proposition 12. 1. $\mathfrak{a} \subset (\mathfrak{a} : \mathfrak{b})$.

Example 12.1. Does $\sqrt{\mathfrak{a}^2} = \mathfrak{a}$ hold?

Proposition 13. Let $A_1, \ldots, A_n$ be rings for $n \in \mathbb{N}^+$ and denote $A := A_1 \times \cdots \times A_n$. The ideals in A are exactly in the form $\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$ where $\mathfrak{a}_i$ is an ideal in A_i for $1 \le i \le n$, i.e.

$$\{\text{ ideals in } A\} = \prod_{i=1}^{n} \{\text{ ideals in } A_i\}$$

Add stuff for spectrums XXX.

Prime Ideals

Definition 14 (Prime Ideals)**.**

Example 14.1. 1. The intersection of two prime ideals are not prime in general. Consider (2) and (3) in the ring $\mathbb{Z}$, then $(2) \cap (3) = (6)$ is not a prime ideal.

Lemma 15. An ideal $\mathfrak{a}$ of a ring A is prime if and only if $A/\mathfrak{a}$ is an integral domain.

Proof. "$\Rightarrow$": Let $\mathfrak{a}$ be a prime ideal and consider two elements $x+\mathfrak{a}$ and $y+\mathfrak{a}$. If $(x+\mathfrak{a})(y+\mathfrak{a}) = 0$, then $xy + \mathfrak{a} = 0$, thus $xy \in \mathfrak{a}$. Since $\mathfrak{a}$ was prime, this implies $x \in \mathfrak{a}$ or $y \in \mathfrak{a}$. In either case, this means $(x+\mathfrak{a})$ or $y+\mathfrak{a}$ was already 0, and therefore $A/\mathfrak{a}$ has no nonzero zero divisors which means it is an integral domain.

"$\Leftarrow$": □

Example 15.1. For the ring of integers $\mathbb{Z}$, we have the prime spectrum

$$\operatorname{Spec}(\mathbb{Z}) = \{\, (0), (2), (3), (5), \dots \,\} = \{0\} \cup \{\, (p) \mid p \in \mathbb{Z} \text{ is prime} \,\}\,.$$

Example 15.2. Let k be an algebraically closed field. For the ring of polynomials $k[X]$, we have the prime spectrum

$$\operatorname{Spec}(k[X]) = \{(0)\} \cup \{\, (X - \lambda) \mid \lambda \in k \,\}\,.$$

Example 15.3. Let k be an algebraically closed field. For the ring of polynomials in two variables $k[X, Y]$, we have the prime spectrum

$$\operatorname{Spec}(k[X, Y]) = \{0\} \cup \{\, (X - \lambda, Y - \mu) \mid \lambda, \mu \in k \,\}\,.$$

Proposition 16. The preimage of a prime ideal is prime.

Maximal Ideals

Definition 17 (Maximal Ideals)**.**

Lemma 18. Every non-zero ring has a maximal ideal.

Proof. $\square$

Remark. Stated the lemma above differently, for any ring A, it is $\operatorname{Spm}(A) = \varnothing$ if and only if A is trivial.

Corollary 1. Any proper ideal is contained in a maximal ideal.

Lemma 19. An ideal $\mathfrak{a}$ of a ring A is maximal if and only if $A/\mathfrak{a}$ is a field.

Proof. "$\Rightarrow$": Let $\mathfrak{a}$ be a maximal ideal $\square$

Radical Ideals

Definition 20. An ideal $\mathfrak{a}$ is called a radical ideal if it coincides with its radical, i.e. if $\mathfrak{a} = \sqrt{\mathfrak{a}}$.

Principal Ideals

Move

Proposition 21. In a finite ring, every prime ring is maximal, i.e. if A is a finite ring, then

$$\operatorname{Spec}(A) = \operatorname{Spm}(A).$$

Proof. $\square$

Chapter 4

Anatomy of Rings

Zero Divisor

Definition 22 (Zero Divisor)**.** An element a of a ring A is called a zero divisor if one of the following equivalent conditions hold.

1. There exists a nonzero $x \in A$ such that $ax = 0$.
2. The map $A \to A$ that sends x to ax is not injective.

Group of Units

Definition 23 (Group of Units)**.**

Nilpotent Elements

Definition 24 (Nilpotent Element and Nilradical)**.** An element x of a ring A is called nilpotent if there exists some positive integer $n \in \mathbb{N}^+$, called the index or the degree, such that $x^n = 0$.
The set of all nilpotent elements is called the nilradical of the ring and is denoted by $\mathrm{Nil}(A)$.

Definition 25 (Reduced Ring)**.** A ring A is called reduced ring if it has no non-zero nilpotent elements.

Proposition 26. Let A and B be two rings and $A' \subset A$ be a subring of A.

1. If A is reduced, then A' is also reduced.
2. If A and B are reduced, then $A \times B$ is also reduced.
   (XXX DOES THIS ALSO HOLD FOR ARBITARY MANY PRODUCTS?)

Irreducible and Prime Elements

Definition 27 (Irreducible Element)**.** An element a of an integral domain A is a nonzero element that is

1. not invertible, i.e. a is not a unit, and
2. is not a product of two non-invertible elements.

REWRITE THIS DEFINITION

Definition 28 (Prime Element)**.** A non-zero non-unit element a of a ring A is called prime if whenever $a \mid bc$ for some b and c in A, then it implies $a \mid b$ or $a \mid c$.

Proposition 29. In an integral domain, every prime element is irreducible.

Example 29.1. The converse of the above proposition is not true in general.

4.1 Exercises and Notes

Example 29.2. Let K be a field and $A = {}^{K[X,Y]}/_{(X-XY^2,Y^3)}$.

1. Compute the nilradical $\mathrm{Nil}(A)$.

   Solution. Denote $(X - XY^2, Y^3) =: \mathfrak{a}$.

$$\begin{aligned} X + \mathfrak{a} &= XY^2 + \mathfrak{a} && \text{because } X - XY^2 \Rightarrow X \sim XY^2. \\ &= XY^2Y^2 + \mathfrak{a} && \text{because } XY^2 - XY^2Y^2 = Y^2(X - XY^2) = 0 \Rightarrow XY^2 \sim XY^2Y^2 \\ &= XY \cdot Y^3 + \mathfrak{a} \\ &= XY \cdot 0 + \mathfrak{a} \\ &= 0 + \mathfrak{a}. \end{aligned}$$

   Thus, $X \in (X - XY^2, Y^3)$. We have therefore the isomorphism ${}^{K[X,Y]}/_{(X-XY^2,Y^3)} \simeq {}^{K[Y]}/_{(Y^3)}$. [I WANT A ELEGANT REASON FOR THIS. PROBABLY ISOMORPHISM THEOREM.]

   Clearly, $Y \in \mathrm{Nil}(A)$ or in other words $(Y) \subset \mathrm{Nil}(A)$. But we also have that ${}^{K[Y]}/_{(Y)} = K$ which is a field, therefore (Y) is a maximal ideal. Because $1 \notin \mathrm{Nil}(A)$ conclude $\mathrm{Nil}(A) = (Y)$. $\square$

Chapter 5

Polynomial Rings

Chapter 6

Quotient

Lemma 30. We have

$$\{\,\text{Ideals of } A/\mathfrak{a}\,\} \cong \{\,\text{Ideals of } A \text{ that contain } \mathfrak{a}\,\}$$

Chapter 7

Localization

Definition and Theorems

Multiplicative Subsets

Definition 31 (Multiplicative Subset)**.** A subset S of a ring A is called a multiplicative subset if the following conditions hold.

1. $1 \in S$.
2. For all $x, y \in S$ it is $xy \in S$.

Example 31.1. Let A be a ring. Trivially, the following subsets of A.are multiplicative subsets.

1. A itself is a multiplicative subset.
2. $\{1\}$ is a multiplicative subset.
3. $\{0, 1\}$ is a multiplicative subset.

Example 31.2. Let A be a ring. Important examples of a multiplicative subset include the following.

1. The set of units $A^\times$ is a multiplicative subset.
2. The set of non-zero-divisors $A \setminus \mathrm{ZD}(A)$ is a multiplicative subset.

Proof. Let A be a ring.

1. We show $A^\times$ is a multiplicative subset. Clearly, 1 is a unit and thus lies in $A^\times$. Let x and y be units in A, then there are some x^{-1} and y^{-1} in A with $x \cdot x^{-1} = 1$ and $y \cdot y^{-1}$. Then, $xy \cdot x^{-1} \cdot y^{-1} = xx^{-1} \cdot yy^{-1} = 1$, so xy is a unit and $A^\times$ is multiplicatively closed.

□

Example 31.3. Let A be a ring. Other examples of multiplicative subsets are the following.

1. Let S be a multiplicative subset. Then, $S \cup \{0\}$ is also multiplicative subset.
2. For any element $x \in A$, the set generated by its power $\left\{1, x, x^2, x^3, \dots\right\}$ is a multiplicative subset.
3. For any ideal $\mathfrak{a} \subset A$, the set $1 + \mathfrak{a}$ is a multiplicative subset.

Lemma 32. An ideal $\mathfrak{p}$ of a ring A is prime if and only if its complement $A \setminus \mathfrak{p}$ is a multiplicative subset.

Proof. Let A be a ring and $\mathfrak{p}$ be an ideal in A.

"$\Rightarrow$": Suppose $\mathfrak{p}$ is prime. By definition, $1 \notin \mathfrak{p}$, hence 1 lies in the complement $A \setminus \mathfrak{p}$. Now let $x, y \in A \setminus \mathfrak{p}$ and assume $xy \notin A \setminus \mathfrak{p}$. In this case, $xy \in \mathfrak{p}$ and since $\mathfrak{p}$ is prime, we must have $x \in \mathfrak{p}$ or $x \in \mathfrak{p}$ both of which are contradictions.

"$\Leftarrow$": On the other hand, let $A \setminus \mathfrak{p}$ be a multiplicative subset. Fix a $xy \in \mathfrak{p}$ and assume $x, y \notin \mathfrak{p}$. We have that $x, y \in A \setminus \mathfrak{p}$ and since $A \setminus \mathfrak{p}$ is a multiplicative subset, it is $xy \in A \setminus \mathfrak{p}$. This implies $xy \notin \mathfrak{p}$ which is a contradiction. □

Remark. The lemma does not imply that any complement of a multiplicative subset is a prime ideal. Only if the complement of a multiplicative subset is already an ideal it is prime. Thus, constructing multiplicative subsets through complements of primitive ideals are not exhaustive.

Example 32.1. Consider $\mathbb{Z}$ and the multiplicative subset $\{1\}$. The complement $\mathbb{Z} \setminus \{1\}$ is not an ideal.

Proposition 33. intersection is again multiplicative
cartesian product?

Example 33.1. subsets? unions symmetric difference

Localization

Definition 34 (Localization)**.** $S^{-1}A$ is again a ring.

Lemma 35 (Universal Property of Localization)**.** Let A and B be two rings, S a multiplicative subset of A, and $f : A \to B$ a ring homomorphism that maps every element of S to a unit in B. In this case, there exists a unique ring homomorphism $g : S^{-1}A \to B$ such that $f = g \circ \varphi$.

Lemma 36. Let A be a ring and S a multiplicative subset, then the following are equivalent.

1. $S^{-1}A = 0$.
2. S contains a nilpotent element.
3. $0 \in S$.

Proof. "1. $\Rightarrow$ 2.": Let $S^{-1}A = 0$, then for all $x \in A$ and $s \in S$ it is $(x, s) \sim (0, 1)$, thus $x \cdot u = 0$ for some $u \in S$. In particular, this holds for $x = 1$, therefore $1 \cdot u = 0$. Since a unit can never be a zero divisor, we must have $u = 0$ which is nilpotent and lies in S.

"1. $\Leftarrow$ 2.": On the other hand, let $x \in S$ be nilpotent, i.e. $x^n = 0$ for some $n \in \mathbb{N}^+$. Because S is multiplicatively closed $x^n = 0$ lies in S. Fix an element $(y, s) \in S^{-1}A$, then $y \cdot 1 \cdot 0 = 0 \cdot s \cdot 0$. Hence $(y, s) \sim (0, 1)$ and we have $S^{-1}A = 0$.

"2. $\Rightarrow$ 3.": Again, let $x \in S$ be nilpotent, thus $x^n = 0$ for some $n \in \mathbb{N}^+$. S is multiplicatively closed and we have $x^n = 0 \in S$.

"2. $\Leftarrow$ 3.": If $0 \in S$, then S simply contains a nilpotent element because 0 is nilpotent. $\square$

Example 36.1. Some concrete examples of localization include the following.

1.

Proposition 37. Let A be a ring. A is reduced if and only if all its localizations $A_\mathfrak{p}$ at $\mathfrak{p} \in \operatorname{Spec} A$ is reduced.

Proof. "$\Rightarrow$": We prove the statement by contrapositive. Let $A_\mathfrak{p}$ be not reduced for all $\mathfrak{p} \in \operatorname{Spec} A$. Thus, in all $A_\mathfrak{p}$, there is an element, say x/s that is nilpotent and not zero, i.e. $(x/s)^n = 0$ for some $n \in \mathbb{N}^+$. By the definition of localization, we get $x^n \cdot u = 0$ for some $u \in A \setminus \mathfrak{p}$. Now, $u \in A \setminus \mathfrak{p}$ cannot be zero, because if it was, $A_\mathfrak{p} = 0$ which is reduced. Thus, x is nilpotent and A is not reduced. $\square$

Interactions

Proposition 38. Let A be a ring and $S \subset A$ be a multiplicative subset that does not contain 0.

1. A is an integral domain if and only if $S^{-1}A$ is an integral domain.
2. A is a unique factorization domain if and only if $S^{-1}A$ is a unique factorization domain.

Proof. "$\Rightarrow$": Let A be an integral domain. Since S does not contain 0, the localization $S^{-1}A$ is a nonzero ring (see EXAMPLE). Let $(x, s) \in S^{-1}A \setminus \{0\}$ be a nonzero element and suppose there is a $(y, t) \in S^{-1}A$ with $(x, s) \cdot (y, t) = 0$. It is $(xy, st) = (0, 1)$ and thus $xy \cdot u = 0$ for some $u \in S$. Because x was nonzero and S does not contain 0 we must have $y = 0$. Hence $S^{-1}A$ is an integral domain.

"$\Leftarrow$": On the other hand, let $S^{-1}A$ be an integral domain. JUST USE THE CANONIC MAPPING $\varphi_S : A \longrightarrow S^{-1}A$. $\square$

Remark. In the lemma above, the condition $0 \notin S$ is required because if S contains 0, then $S^{-1}A = 0$ and by definition, an integral domain is a nonzero ring.

Proposition 39. Let A be a ring, S a multiplicative subset, and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ for $n \in \mathbb{N}^+$ ideals in A. It is

$$\left(\bigcap_{i=1}^{n} \mathfrak{a}_i\right) A_S = \left(\bigcap_{i=1}^{n} \mathfrak{a}_i A_S\right)$$

or written differently

$$(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n)\, A_S = \mathfrak{a}_1 A_S \cap \cdots \cap \mathfrak{a}_n A_S.$$

Proof. By induction, we reduce the case to $n = 2$, that is, we want to show $(\mathfrak{a}_1 \cap \mathfrak{a}_2)A_S = \mathfrak{a}_1 A_S \cap \mathfrak{a}_2 A_S$. The inclusion $(\mathfrak{a}_1 \cap \mathfrak{a}_2) \hookrightarrow \mathfrak{a}_1$ induces a natural inclusion $(\mathfrak{a}_1 \cap \mathfrak{a}_2)A_S \hookrightarrow \mathfrak{a}_1 A_S$

which can be extended to a injective map $f : (\mathfrak{a}_1 \cap \mathfrak{a}_2)A_S \to \mathfrak{a}_1 A_S \cap \mathfrak{a}_2 A_S$. It suffies to show f is surjective. Let $y \in \mathfrak{a}_1 A_S \cap \mathfrak{a}_2 A_S$. We have

$$y = \frac{a_1}{s} = \frac{a_2}{t}$$

with $a_1 \in \mathfrak{a}_2$, $a_2 \in \mathfrak{a}_2$, and $s, t \in S$. Thus it is $a_1 tu = a_2 su$ for some $u \in S$. Since a_1 lies in $\mathfrak{a}_1$, we have $a_1 tu \in \mathfrak{a}_1$, and similary $a_2 su \in \mathfrak{a}_2$, hence $a_1 tu \in \mathfrak{a}_1 \cap \mathfrak{a}_2$. But t and u are invertible in A_S, therefore

$$\frac{a_1}{s} = \frac{a_1 tu}{stu} \in (\mathfrak{a}_1 \cap \mathfrak{a}_2)A_S$$

thus f is surjective. □

Example 39.1. Consider $\mathbb{Q}[X]$

Exercises and Notes

Example 39.2. Let A_1 and A_2 be rings. Consider $A = A_1 \times A_2$ and set $S := \{ (1,1), (1,0) \}$. Prove $A_1 \simeq S^{-1}A$.

Solution. I don't understand the solution? □

Example 39.3. Find all intermediate rings $\mathbb{Z} \subset A \subset \mathbb{Q}$, and describe each A as a localization of $\mathbb{Z}$. As a starter, prove $\mathbb{Z}\left[\frac{2}{3}\right] = S_3^{-1}\mathbb{Z}$ where $S_3 := \left\{ 3^i \mid i \in \mathbb{N}^+ \right\}$.

Chapter 8

Hierarchy of Rings

8.1 Integral Domains

Definitions and Theorems

Definition 40 (Integral Domains)**.** An integral domain A is a nonzero ring satisfying the following equivalent conditions.

1. The product of two nonzero elements is nonzero, i.e. for all a and b in A it is $ab \neq 0$.
2. The zero ideal (0) is a prime ideal.
3. Every nonzero element is cancellable under multiplication, i.e. $ab = ac$ implies $b = c$.

Lemma 41. Let A be a ring and $\mathfrak{p}$ an ideal. Then, $\mathfrak{p}$ is a prime ideal if and only if $A/\mathfrak{p}$ is an integral domain.

Proposition 42. Any finite integral domain is a field.

Proof. □

Interactions

Proposition 43. If A is an integral domain, and S a multiplicative subset that does not contain 0, then its localization $S^{-1}A$ is an integral domain.

Proof. Fix two elements x/s and y/t in $S^{-1}A$. If their product equals 0, we have

$$\frac{0}{1} = \frac{x}{s} \cdot \frac{y}{t} \iff xyu = 0 \text{ for some } u \in S$$

Since S does not contain 0, we must have $x = 0$ or $y = 0$, thus $S^{-1}A$ is an int domain. □

Example 43.1. The converse of the proposition above is not true, that is the localization $S^{-1}A$ being an integral domain does not imply A is an integral domain.

Notes

8.2 Unique Factorization Domains

Definitions and Theorems

Notes

8.3 Principal Ideal Domains

Definitions and Theorems

Definition 44 (Principal Ideal Domains)**.** A principal ideal domain is an integral domain in which every ideal is principal.

Lemma 45. In a principal ideal domain, all nonzero prime ideals are maximal and are generated by a prime element, i.e. if A is a principal ideal domain, then

$$\operatorname{Spec}(A) = \operatorname{Spm}(A) \cup \{(0)\} = \{\, (p) \mid p \text{ is a prime element in } A \,\}.$$

Lemma 46. Let A be a principal ideal domain and $\mathfrak{a}$ be an ideal in A. The quotient $A/\mathfrak{a}$ is a principal ideal ring.

Remark. In the above lemma, the quotient $A/\mathfrak{a}$ need not be an principal ideal domain because $A/\mathfrak{a}$ is not even be an integral domain if $\mathfrak{a}$ is not a prime ideal.

Example 46.1. $\mathbb{Z}/6\mathbb{Z}$ is a principal ideal ring, but not a principal ideal domain.

Proposition 47. Let A be a principal ideal domain and (x) an ideal in A. The proper ideals in $A/(x)$ are in the form (a) where $a \mid x$.

Notes

8.4 Euclidean Domains

Definitions and Theorems

Notes

Chapter 9

Classification of Rings

9.1 Definition and Theorems

9.1.1 Noetherian Ring

Lemma 48. All principal ideal domains are Noetherian.

Remark. By the lemma above, it follows that any

1. Euclidean domains
2. fields

are Noetherian.

Example 48.1.

Example 48.2.

Theorem 49 (Hilbert's Basis Theorem)**.** If A is a Noetherian ring, then the polynomial ring with finitely many variables $A[X_1, \ldots, X_n]$ is Noetherian. In particular, if A is Noetherian, so is $A[X]$.

Corollary 2. If A is Noetherian, the power series ring $A[[X]]$ is Noetherian.

Remark. The polynomial ring with infinitely many variables $A[X_1, X_2, \ldots]$ is never Noetherian.

9.2 Artinian Rings

Definition and Theorems

Definition 50 (Artinian Rings)**.**

Example 50.1.
1. Any field is Artinian.
2. Any finite ring is Artinian.

Proposition 51.
1. A quotient of an Artinian ring is Artinian.
2. A localization of an Artinian ring is Artinian.

Lemma 52. An integral domain is Artinian if and only if it is a field.

Proof. Let A be an integral domain.

"$\Rightarrow$": Since A is an Artinian, the descending chain

$$(x) \supset (x^2) \supset \cdots \supset (x^n) \supset (x^{n+1}) \supset \cdots$$

becomes stationary, that is $(x^n) = (x^{n+1})$ for some $n \in \mathbb{N}^+$. It follows that there is a $b \in A$ such that $x^n = bx^{n+1}$. We have

$$\begin{aligned} x^n = bx^{n+1} &\iff 0 = bx^{n+1} - x^n \\ &\iff 0 = bx^n(x-1) \end{aligned}$$

Since A is an integral domain, bx^n cannot be zero,thus $x - 1 = 0$ or in other words x is a unit. Hence A is a field.

"$\Leftarrow$": All fields are already Artinian. $\square$

Proposition 53. Let A be an Artinian ring. Then, we have the following

1. The spectrum $\operatorname{Spec}(A)$ of A and the maximal spectrum $\operatorname{Spm}(A)$ of A are both finite.
2. It is $\operatorname{Spec}(A) = \operatorname{Spm}(A)$.
3. For some $n \in \mathbb{N}^+$, it is $(\operatorname{Jac}(A))^n = 0$.
4. There are maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ in $\operatorname{Spm}(A)$ such that $\prod_{i=1}^n \mathfrak{m}_i = 0$.
5. A is Noetherian.
6. A has finite rank.

Proof.
1. Let $(\mathfrak{m}_k)_{i \in \mathbb{N}^+}$ be a sequence of maximal ideals and set

$$I_k = \prod_{i=1}^k \mathfrak{m}_i.$$

Since A is Artinian, the chain $I_0 \supset I_1 \supset \cdots \supset I_k \supset I_{k+1} \supset \cdots$ becomes stationary. Hence $I_k = I_{k+1}$ for some $k \in \mathbb{N}^+$.

2. Since $\operatorname{Spec}(A) \supset \operatorname{Spm}(A)$ is immediately clear, we show the other direction of the inclusion. Let $\mathfrak{p}$ be a prime ideal and consider $A/\mathfrak{p}$. It is an integral domain because $\mathfrak{p}$ is a prime ideal and it is also Artinian because a quotient of an Artinian ring is Artinian. Therefore, $A/\mathfrak{p}$ is a field, hence $\mathfrak{p}$ is a maximal ideal.

□

Lemma 54. A ring is Artinian if and only if it is Noetherian and $\operatorname{Spec}(A) = \operatorname{Spm}(A)$.

Theorem 55.

Exercise and Notes

Example 55.1. Given a prime $p \in \mathbb{Z}$, find all Artinian rings A with p^2 elements (up to isomorphisms).

Proof. Let A be an Artinian ring with p^2 elements where $p \in \mathbb{Z}$ is prime. By the structure theorem of Artinian rings, we have that A is a product of local Artinian rings. Since p^2 has two prime factors, this product can involve at most two factors. Thus, we have two cases.

Case 1: In this case, $A = A_1 \times A_2$ for two local Artinian rings A_1 and A_2 with both having exactly p elements. A ring with p elements is isomorphic to $\mathbb{F}_p$. We may conclude $A = \mathbb{F}_p \times \mathbb{F}_p$.

Case 2: If A has only one factor, A must be a local ring, i.e. it has a unique maximal ideal $\mathfrak{m}$ with $\mathfrak{m}^n = 0$ for some $\mathbb{N}^+$. Choose such n to be minimal and consider the chain $R \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset 0$. Taking the quotient at each step we obtain □

Chapter 10

Summary

Here, I want to summarize the interactions of structures

1. integral domains

2.

	Integral Domain	Unique Factorization Domain	Principal Ideal Domain
Polynomial Ring	$\Longleftrightarrow$	$\Downarrow \quad \not\Rightarrow$	$\not\Downarrow$

Part II

Modules

Chapter 11

Modules

Definition and Theorems

Introduction

Definition 56 (Module).

Example 56.1. 1. If A is a field, then an A-module is a vector space.

2. A $\mathbb{Z}$-module is just an abelian group.

Definition 57 (Submodules)**.** Let M be an A-module. A subset N of M is called a submodule if $(N, +)$ is a subgroup of M and for all $n \in N$ and for all $a \in A$ it is $a \cdot n \in N$.

Proposition 58. Let A be a ring. If A is viewed as a module over itself, then its submodules are exactly its ideals, i.e.

$$\{ N \mid N \text{ is a submodule of } A \} = \{ \mathfrak{a} \mid \mathfrak{a} \text{ is an ideal of } A \} .$$

Definition 59 (Homomorphism of Modules).

Proposition 60. Let M and N be an A-module, and $\varphi : M \to N$ be an A-module homomorphism.

1. $\operatorname{im}(\varphi)$ is a submodule of M.
2. $\ker(\varphi)$ is a submodule of N.
3. For any submodule N' of N, its preimage $\varphi^{-1}(N')$ is a submodule of M.

Free and Finitely Generated

Definition 61. An A-module is finitely generated if there exists a finite set $\{m_1, \ldots, m_n\}$ with $n \in \mathbb{N}^+$ in M such that for any x in M, there exits $\lambda_1, \ldots, \lambda_n$ in A with

$$x = \lambda_1 m_1 + \cdots + \lambda_n m_n$$

Lemma 62. An A-module is finitely generated if and only if there exists a surjective A-module homomorphism

$$A^n \longrightarrow M$$

for some $n \in \mathbb{N}^+$.

Definition 63. Let M be an A-module. A set $B \subset M$ is a basis of M if

1. B is a generating set for M
2. B is linearly independent

A free module is a module with a basis.

Remark. An A-module being free does **not** imply the module being finitely generated. Similary, an A-module being finitely generated does **not** imply the module being free.

Example 63.1. Two examples to illustrate the remark above.

1. As an $\mathbb{Z}$-module, $\mathbb{Z}/2\mathbb{Z}$ is finitely generated but is not free.
2. As an $\mathbb{Z}$-module, $\bigoplus_{\mathbb{N}} \mathbb{Z}$ is free, but is not finitely generated.

Proof. 1. $\{1\}$ is a generating set of $\mathbb{Z}/2\mathbb{Z}$ since $1 \cdot 1 = 1$ and $2 \cdot 1 = 0$. However, $\{1\}$ and ... □

Lemma 64. Let A be an integral domain. Then, an ideal $\mathfrak{a}$ of A is a free A-module if and only if it is principal.

Proof. "⇒": Let $\mathfrak{a}$ be a free A-module.
"⇐": If $\mathfrak{a} = (a)$ for some $a \in A$, then $\{a\}$ is a generating set of $\mathfrak{a}$ □

Torsion and Annihilator

Definition 65.

$$\operatorname{Tor}(M) = \{\, m \in M \mid \text{there is an } a \in A \setminus \{0\} \text{ such that} a \cdot m = 0 \,\}$$

Example 65.1. 1. Let $\mathbb{Z}$ be a module over itself. It is $\operatorname{Tor}(\mathbb{Z}) = \{0\}$.

2. Let $n \in \mathbb{N}^+$ and consider the $\mathbb{Z}$-module $\mathbb{Z}^n$. It is

Lemma 66. If M is a free A-module, then it is torsion-free, i.e. $\operatorname{Tor}(M) = \{0\}$.

Proof. Let M be a free A-module and fix an element $m \in M$. Since M is free, m may be written as

$$m = \sum_{i=1}^{n} \lambda_i m_i$$

where $\lambda_i \in A$ and $m_i \in M$ with $1 \leq i \leq n$. If m is a torsion element, then there is some $a \in A$ such that $am = 0$, thus it is

$$0 = am = a \sum_{i=1}^{n} \lambda_i m_i = \sum_{i=1}^{n} a\lambda_i m_i$$

But m_i are linearly independent, therefore $m = 0$. □

Example 66.1. The converse of the above lemma is false. Consider $\mathbb{Q}$ as a $\mathbb{Z}$-module. It is torsion-free, but not free.

Definition 67 (Annihilator)**.**

Definition 68 (Radical)**.**

Definition 69 (Simple Modules)**.** Let A be a ring. A nonzero A-module M is called simple if the only submodules are $\{0\}$ and M itself.

Example 69.1. If M is a simple A-module, then any $f \in \mathrm{Hom}_A(M, M) \setminus \{0\}$ is an isomorphism.

Proof. Fix an $f \in \mathrm{Hom}_A(M, M) \setminus \{0\}$. Since $\ker(f)$ is a submodule of M, it must be either $\{0\}$ or whole M. But $\ker(f) = M$ would mean that $f = 0$ which was explicitly excluded, thus $\ker(f) = \{0\}$. By the isomorphism theorem, we also have $\mathrm{im}(f) \cong M/\ker(f) \cong M$. Therefore, f is bijective. □

Definition 70 (Indecomposable)**.** Let A be a ring. A nonzero A-module M is called indecomposable if it cannot be written as a direct sum of two non-zero submodules.

Proposition 71. Every simple module is indecomposable.

Example 71.1. Not all indecomposable modules are simple. For example, $\mathbb{Z}$ is indecomposable, but is not simple.

Theorem 72. Let A be a principal ideal domain, and M a finitely generated A-module. Then, $M \cong \mathrm{Tor}(M) \oplus R^n$ for some $n \in \mathbb{N}_0$.

11.1 Exercises and Notes

Example 72.1. Let $f : M \to N$ be a surjective homomorphism of two finitely generated A-modules.

1. If $N \cong A^n$ is a free A-module, show that $M \cong \ker(f) \oplus N$.

   Proof. Since N is finitely generated, let $(e_1, \dots, e_n)$ be a set of generators. □

Example 72.2. Let A be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals, M and N A-modules. Set

$$\Gamma_{\mathfrak{a}}(M) := \left\{ m \in M \mid \mathfrak{a} \subset \sqrt{\operatorname{Ann}(m)} \right\}.$$

Prove the following statements.

1. If $\mathfrak{a} \supset \mathfrak{b}$, then $\Gamma_{\mathfrak{a}}(M) \subset \Gamma_{\mathfrak{b}}(M)$.

   Proof. The proof is a matter of verification. Let $m \in \Gamma_{\mathfrak{a}}(M)$. It is

   $$\begin{aligned} m \in \Gamma_{\mathfrak{a}}(M) &\Rightarrow \mathfrak{a} \subset \sqrt{\operatorname{Ann}(m)} \\ &\Rightarrow \text{For all } a \in \mathfrak{a} \text{ there is a } n \in \mathbb{N}^+ \text{ such that } a^n \in \operatorname{Ann}(m). \\ &\Rightarrow \text{For all } a \in \mathfrak{a} \text{ there is a } n \in \mathbb{N}^+ \text{ such that } a^n \cdot m = 0. \end{aligned}$$

   Since $\mathfrak{a} \supset \mathfrak{b}$, the last statement is true for all $a \in \mathfrak{b}$. We have

   $$\begin{aligned} &\Rightarrow \text{For all } a \in \mathfrak{b} \text{ there is a } n \in \mathbb{N}^+ \text{ such that } a^n \cdot m = 0. \\ &\Rightarrow \text{For all } a \in \mathfrak{b} \text{ there is a } n \in \mathbb{N}^+ \text{ such that } a^n \in \operatorname{Ann}(m). \\ &\Rightarrow \mathfrak{b} \subset \sqrt{\operatorname{Ann}(m)} \\ &\Rightarrow m \in \Gamma_{\mathfrak{b}}(M) \end{aligned}$$

   Thus, $\Gamma_{\mathfrak{a}}(M) \subset \Gamma_{\mathfrak{b}}(M)$. □

2. If $M \subset N$, then $\Gamma_{\mathfrak{a}}(M) = \Gamma_{\mathfrak{a}}(N) \cap M$.

   Proof. Again, the proof is a matter of verification.
   "$\subset$": $M \subset N$ implies $\Gamma_{\mathfrak{a}}(M) \subset \Gamma_{\mathfrak{a}}(N)$. Moreover, it is $\Gamma_{\mathfrak{a}}(M) \subset M$. Thus, $\Gamma_{\mathfrak{a}}(M) \subset \Gamma_{\mathfrak{a}}(N) \cap M$.
   "$\supset$": Let $m \in \Gamma_{\mathfrak{a}}(N) \cap M$. It is

   $$\begin{aligned} m \in \Gamma_{\mathfrak{a}}(N) \cap M &\Rightarrow \mathfrak{a} \subset \sqrt{\operatorname{Ann}(m)} \text{ and } m \in M. \\ &\Rightarrow m \in \Gamma_{\mathfrak{a}}(M). \end{aligned}$$

   Hence, $\Gamma_{\mathfrak{a}}(N) \cap M \subset \Gamma_{\mathfrak{a}}(M)$. □

3. In general, it is $\Gamma_{\mathfrak{a}}(\Gamma_{\mathfrak{b}}(M)) = \Gamma_{\mathfrak{a}+\mathfrak{b}}(M) = \Gamma_{\mathfrak{a}}(M) \cap \Gamma_{\mathfrak{b}}(M)$.
4. In general, it is $\Gamma_{\mathfrak{a}}(M) = \Gamma_{\sqrt{\mathfrak{a}}}(M)$.
5. If $\mathfrak{a}$ is finitely generated, then

   $$\Gamma_{\mathfrak{a}}(M) = \bigcup_{n \geq 1} \{ m \in M \mid \mathfrak{a}^n m = 0 \}.$$

Example 72.3. Let A be a ring, M a module, $x \in \operatorname{Rad}(M)$, and $m \in M$. If $(1+x)m = 0$, then $m = 0$.

Proof. By definition of radical of a module, it is

$$\operatorname{Rad}\left({}^{A}/_{\operatorname{Ann}(M)}\right) = {}^{\operatorname{Rad}(M)}/_{\operatorname{Ann}(M)}.$$

Thus, if $x \in \operatorname{Rad}(M)$, then its residue $x' := x + \operatorname{Ann}(M)$ lies in $\operatorname{Rad}\left({}^{A}/_{\operatorname{Ann}(M)}\right)$ which means x' is nilpotent. SOME THEOREM yields $(1 + x')$ is an unit in ${}^{A}/_{\operatorname{Ann}(M)}$. □

Chapter 12

Tensor Product

12.1 Definition and Theorems

Definition 73. Let M and N be A-modules. Their tensor product is a pair $(M \otimes_A N, \theta)$ where

1. $M \otimes_A N$ is an A-module.
2. $\theta : M \times N \to M \otimes_A N$ is an A-bilinear mapping.

satisfying the universal property, for every pair (P, ω) of an A-module and an A-bilinear mapping $\omega : M \times N \to P$, there exists a unique A-module homomorphism $f : M \otimes_A N \to P$ with $\omega = f \circ \theta$.

Definition 74. Let M and N be A-modules. Their tensor product is the pair $(M \otimes_A N, \theta)$, where

1. $M \otimes_A N$ is the quotient of the free A-module $A^{M \times N}$ on the direct product $M \times N$, by the submodule generated by the set of elements of the form:

$$\begin{gathered}(\lambda m_1 + m_2, n) - \lambda(m_1, n) - (m_2, n) \\ (m, \lambda n_1 + n_2) - \lambda(m, n_1) - (m, n_2)\end{gathered}$$

   for $m, m_1, m_2 \in M$; $n, n_1, n_2 \in N$; and $\lambda \in A$, where we denote (m, n) for its image under the canonical mapping $M \times N \to A^{(M \times N)}$.

2. $\theta : M \times N \to M \otimes_A N$ is the composition of the canonical mapping $M \times N \to A^{(M \times N)}$ with the quotient module homomorphism $A^{(M \times N)} \to M \otimes_A N$.

Example 74.1. It is $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z} = 0$.

Proof. Let's show this in multiple concrete ways.
Method 1: I want to do this conretely. First, we have

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{ (0,0); (0,1); , (0,2); (1,0); (1,1); (1,2) \} .$$

Thus, the elements of $\mathbb{Z}^{(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})}$ are in the form

$$(x_{(0,0)}, x_{(0,1)}, x_{(0,2)}, x_{(1,0)}, x_{(1,1)}, x_{(1,2)})$$

where $x_{(i,j)} \in \mathbb{Z}$ with $i \in \{0, 1\}$ and $j \in \{0, 1, 2\}$.

Now, we want to find the submodule generated by the rules in the definition.

1. Set $m_1 = m_2 = n = \lambda = 0$, then
$$(0 \cdot 0 + 0, 0) + 0 \cdot (0, 0) - (0, 0) = (0, 0) = 1 \cdot (0, 0) \to (1, 0, 0, 0, 0, 0).$$
2. Set $m = n_2 = 0$, $n_1 = 1$, and $\lambda = 2$, then
$$\begin{aligned}(0, 2 \cdot 1 + 0) - 2 \cdot (0, 1) - (0, 0) &= (0, 2) - (2 \cdot 0, 1) \\ &= (0, 2) - (0, 1) \\ &= (0, 1) \\ &= 1 \cdot (0, 1) \\ &\to (0, 1, 0, 0, 0, 0)\end{aligned}$$
3. I think the rest is clear for now.

We may conclude that the submodule generated by the rules defined is the whole module, thus $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z} = 0$.
Method 2: https://www.math.brown.edu/reschwar/M153/tensor.pdf □

Proposition 75. Let A be a ring, and M, N and P be A-modules.

1. (identity) $A \otimes_A M = M$.
2. (commutative law) $M \otimes_A N = N \otimes_A M$.

Proof. As in the proposition, let A be a ring, and M, N and P be A-modules.

1. Define $\beta : A \times M \to M$ by $\beta(x, m) := xm$. Clearly, β is bilinear.

□

12.2 Exercises and Notes

Example 75.1. Let $A \to B \to C$ be ring homomorphisms and M and N be A-modules. Show the following.

1. $(M \otimes_A B) \otimes_B C \cong M \otimes_A C$

   Proof. It is

$$\begin{aligned}(M \otimes_A B) \otimes_B C &\cong M \otimes_A (B \otimes_B C) \\ &\cong M \otimes_A C\end{aligned}$$

   □

2. $(M \otimes_A N) \otimes_A B \cong (M \otimes_A B) \otimes_B (N \otimes_A B)$

   Proof. trivial □

Example 75.2. Let A be a ring.

1. If M, N are A-modules, then $\mathrm{Hom}_A(M, N)$ may be viewed as an A-module via

$$a \cdot \varphi := (m \mapsto a \cdot \varphi(m))$$

   for $a \in A$ and $\varphi \in \mathrm{Hom}_A(M, N)$.

   Proof. this is trivial □

2. If M, N, L are A-modules, then there exists a natural isomorphism of A-modules

$$\mathrm{Hom}_A(L \otimes_A M, N) \cong \mathrm{Hom}_A(L, \mathrm{Hom}_A(M, N))$$

Example 75.3. Let A be a ring, $\mathfrak{a}$ an ideal of A, and M an A-module.

1. Show that $M/\mathfrak{a}M \cong M \otimes_A A/\mathfrak{a}$.

   Proof. Define $\varphi : M \otimes_A A/\mathfrak{a} \to M/\mathfrak{a}M$ by

$$m \otimes_A \overline{x} \mapsto x \cdot m + \mathfrak{a}M.$$

   φ is an homomorphism because

   (a) $\varphi((m_1 \otimes_A \overline{x_1}) + (m_2 \otimes_A \overline{x_2})) =$

   □

Chapter 13

Nakayama's Lemma

Proposition 76. Let M be a finitely generated A-module, and $\mathfrak{a}$ an ideal of A. Then, $\mathfrak{a}M = M$ if and only if there exists $a \in \mathfrak{a}$ such that $(1 + a)M = 0$.

Proof. "$\Rightarrow$": Let $\mathfrak{a}M = M$, so for all $a \in \mathfrak{a}$ and $m, m' \in M$, it is $am = m'$, in particular, we have $-am = m$. Rewriting the equation yields $0 = am + m = (1 + a)m$. Therefore, it is $(1 + a)M = 0$.

"$\Leftarrow$": On the other hand, if there is an $a \in \mathfrak{a}$ such that $(1 + a)M = 0$, then for all $m \in M$ it is $0 = (1 + a)m = m + am$ and rewriting it gives $m = -am$. So any m is contained in $\mathfrak{a}M$, i.e. $M \subset \mathfrak{a}M$. Trivially, it is also $M \subset \mathfrak{a}M$, hence we have $\mathfrak{a}M = M$. □

Theorem 77. Let M be a finitely generated A-module. If there is an ideal $\mathfrak{a}$ in A with $\mathfrak{a} \in \mathrm{Jac}(A)$ such that $\mathfrak{a}M = M$, then $M = 0$.

Proof. □

Theorem 78. Let A be a local ring, $\mathfrak{m}$ the maximal ideal of A, and $k = A/\mathfrak{m}$, and M a finitely generated A-module. Then we have the following.

1. For all submodules N of M with $M = N + \mathfrak{m}M$ it is $N = M$.

Chapter 14

Exact Sequences

14.1 Definition and Theorems

Definition 79. Exact at, exact sequence, short exact sequence

Example 79.1. Let M and N be A-modules. Then, the sequence

$$0 \to M \to M \oplus N \to N \to 0$$

is short exact.

Lemma 80. If $0 \to M \to N \to P \to 0$ is exact, and M and P are finitely presented, then N is finitely presented.

Proof. □

Proposition 81. Let M be an A-module, m_λ with $\lambda \in \Lambda$ a set of generators. Then there is an exact sequence $0 \to K \to A^{\oplus \Lambda} \to M \to 0$

14.2 Notes and Exercises

Chapter 15

Noetherian Modules

Definition 82. An A-module M is called Noetherian if one of the following equivalent conditions hold.

1. Its submodules satisfies the asending chain condition, i.e. MISSING.
2. All submodules of M are finitely generated.

Proof. "$\Rightarrow$": Let M be an A-module that satisfies the ascending chain condition and assume a submodule N is not finitely generated. In this case, we may construct a chain of submodules

$$N_1 \subset N_2 \subset \cdots N_i \subset \cdots$$

where $N_i = (n_1, n_2, \ldots, n_{i-1})$ with $n_i \in N$ and $n_i \notin N_i$ for all $i \in \mathbb{N}^+$. This chain never stabilizes, thus N must be finitely generated.
"$\Leftarrow$": □

Lemma 83. Let $0 \to M \to N \to P \to 0$ be an exact sequence of A-modules. Then N is Noetherian if and only if M and P are Noetherian.

Proof. Let $0 \to M \to N \to P \to 0$ be an exact sequence of A-modules.
"$\Rightarrow$": Let N be Noetherian.

1. We show that M is Noetherian by verifying all its submodules are finitely generated. Let M' be a submodule of M. In that case, $\alpha(M')$ is a submodule of N and thus finitely generated. α restricted
2. We show that P is Noetherian by verifying all its submodules are finitely generated. Let P' be a submodule of P. Since β is surjective, we have $P' = \beta\left(\beta^{-1}(P')\right)$. $\beta^{-1}(P')$ is a submodule of N and it is finitely generated because N is Noetherian.

□

Proposition 84. *The property Noetherian is stable under intersection, direct sum,addition, and localization.* Let M be an A-module, N_1 and N_2 submodules of M.

1. If N_1 and N_1 are Noetherian, so is $N_1 \cap N_2$, $N_1 \oplus N_2$, and $N_1 + N_2$.

Proof. 1. Since all submodules of a Noetherian module is again Noetherian, $N_1 \cap N_2$ is Noetherian because it is a submodule of M which is Noetherian.

2. Consider the sequence $0 \to N_1 \to N_1 \oplus N_2 \to N_2 \to 0$.

3.

$\square$

Example 84.1. Let M be an A-module, and N_1 and N_2 submodules of M. In general, $N_1 \otimes N_2$ is not Noetherian.

Chapter 16

Artinian Modules

16.1 Definition and Theorems

Definition 85 (Artinian Module)**.**

Example 85.1 (Examples of Artinian Modules)**.**

1. For $n \in \mathbb{N}^+$, $\mathbb{Z}/n\mathbb{Z}$ is Artinian.

Example 85.2 (Counterexamples of Artinian Modules)**.**

1. $\mathbb{Z}$ is not Artinian.

Lemma 86. Let $0 \to M \to N \to P \to 0$ be an exact sequence of A-modules. Then N is Artinian if and only if M and P are Artinian.

Proposition 87. The property of Artinian is stable under intersection, direct sum, addition, localization,

Unorganized

Example 87.1. Let A be a local ring with maximal ideal $\mathfrak{m}$.

1. What do the simple A-module look like?

   Proof. Let M be a simple A-module. Since M is simple, the only proper submodule is the zero-module. □

Length

Example 87.2. Let M be an A-module.

1. If M is simple, then any nonzero element $m \in M$ generates M.

   Proof. Fix an element $m \in M$ and assume m does not generate whole M. In that case, there must be a $m' \in M$ such that $m \neq \lambda m'$ for all $\lambda \in A$. Then, (m) is non-zero, but also not whole M which is a contradiction. □

2. M is simple if and only if $M \cong A/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, and if so, then $\mathfrak{m} = Ann(M)$.

   Proof. We first show that M is simple if and only if $M \cong A/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. "⇒": Let M be simple. By the statement above, M is cyclic. □

Example 87.3. Let k be a field. Is $X = \operatorname{Spec}(k[X,Y]/(xy-1))$ with the Zariski-topology connected?

Example 87.4. If $A_\mathfrak{p}$ is reduced at all $\mathfrak{p} \in \operatorname{Spec}(A)$, then A is reduced.

Proof. THIS IS A WRONG PROOF!

Denote the canonic $\varphi_\mathfrak{p} : A \to A_\mathfrak{p}$. Assume $x \in A$ with $x^n = 0$. It is

$$0 = \varphi(0) = \varphi(x^n) = (\varphi(x))^n$$

but since $A_\mathfrak{p}$ is reduced, conclude $\varphi(x) = 0$, so $x = 0$.

The issue with this proof is that for example $\varphi(x) \cdot \varphi(x)^2 = 0$ because $\varphi(x)$ and $\varphi(x)^2$ are zero divisors. □

Proposition 88. Let A be a ring. Then, the following are equivalent.

1. A is reduced.
2. $A_\mathfrak{p}$ is reduced for all prime ideals $\mathfrak{p} \in \operatorname{Spec}(A)$.
3. $A_\mathfrak{m}$ is reduced for all maximal ideals $\mathfrak{m} \in \operatorname{Spm}(A)$.

Proof. "2 ⇒ 1": Assume $x \in A$ is nilpotent and nonzero. □

Chapter 17

Length

17.0.1 Definition and Theorems

Definition 89 (Simple Modules)**.**

Definition 90. Let M be an A-module. We call a chain of submodules

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

a composition series of length n if **each** successive quotient M_{i-1}/M_i is simple.
We define the length $l(M)$ to be the infimum of all those length, i.e.

$$l(M) := \inf \{ n \mid M \text{ has a composition series of length } n \} .$$

By convention, if M has no composition series, then $l(M) := \inf$.