Math 559: Commutative Algebra

Wolmer V. Vasconcelos

Set 1: The Basics

Fall 2009

Outline

1. General Orientation
2. Syllabus
3. Introduction
4. Chain Conditions
5. Prime Ideals
6. Primary Decomposition
7. Noetherian Rings
8. Graded Noetherian Rings
9. Commutative Artinian Rings
10. Modules of Fractions
11. Integral Extensions
12. Dedekind Domains
13. Valuation Rings
14. Homework

- Pre-requisites: One previous algebra course, e.g. Math 551 and a few topics of Math 552.
- Textbook: See Syllabus
- webpage:www.math.rutgers.edu/(tilde)vasconce
- email : vasconce AT math.rutgers.edu
- Office hours [H228]: TF 2:4, or by arrangement

Outline

1. General Orientation
2. **Syllabus**
3. Introduction
4. Chain Conditions
5. Prime Ideals
6. Primary Decomposition
7. Noetherian Rings
8. Graded Noetherian Rings
9. Commutative Artinian Rings
10. Modules of Fractions
11. Integral Extensions
12. Dedekind Domains
13. Valuation Rings
14. Homework

Syllabus

- Textbook: David Eisenbud, Commutative Algebra with a view to Algebraic Geometry, Springer.
- Prerequisites: Any graduate course in abstract algebra, or permisson of the instructor
- Course Description: Commutative algebra is broadly concerned with solutions of structured sets of polynomial and analytic equations, and the study of pathways to methods and algorithms that facilitate the efficient processing in large scale computations with such data. This course will be an introduction to commutative algebra, with applications to algebraic gometry, combinatorics and computational algebra.

Syllabus

1. (If needed by audience) Noetherian rings: Rings of polynomials, Hilbert basis theorem, Dedekind domains, Finitely generated algebras over fields, Noether normalization, Nullstellensatz.
2. The first part of the course will treat basic notions and results—chain conditions, prime ideals, flatness, Krull dimension, Hilbert functions.
3. Required material from Homological Algebra–such as the derived functors of Hom and tensor products–will be given in class, not assumed.
4. The other half of the course will study in more detail rings of polynomials and its geometry, and Gröbner bases. It will open the door to computational methods in algebra (a few will be studied). Some other applications will deal with counting solutions of certain linear diophantine equations.

Topics

1. Noetherian rings: Hilbert basis theorem, Artin-Rees theorem, Krull dimension, associated primes
2. Affine algebras over fields: Noether normalization, Nullstellensatz, finiteness of integral closure
3. Integral closure: Valuation rings, Dedekind domains, Cohen-Seidenberg theorems
4. Homological Algebra: flatness, projective and injective modules, the derived functions of Hom and $\otimes$, Koszul complexes
5. Hilbert functions: multiplicities, Hilbert coefficients
6. Gröbner basics: Buchberger's algorithm, calculus of syzygies
7. Cohen-Macaulay rings: Linkage, canonical module, Gorenstein rings

Outline

1. General Orientation
2. Syllabus
3. **Introduction**
4. Chain Conditions
5. Prime Ideals
6. Primary Decomposition
7. Noetherian Rings
8. Graded Noetherian Rings
9. Commutative Artinian Rings
10. Modules of Fractions
11. Integral Extensions
12. Dedekind Domains
13. Valuation Rings
14. Homework

Very Quick Intro

- Let $\mathbf{F}$ be a field and $\mathbf{f} = \{f_1, \ldots, f_m\}$ a set of polynomials of $\mathbf{F}[x_1, \ldots, x_d]$. For a diversity of reasons–algebraic, geometric and/or computational–it is of interest to understand the zero set $V(\mathbf{f})$ (in $\mathbf{F}$ or in one of its extensions). A common pathway to this goal is the examination of the ring $\mathbf{A} = \mathbf{F}[x_1, \ldots, x_d]/(\mathbf{f})$.
- An important example is:

  $$\mathbf{A} = \mathbb{C}[x, y]/(y^2 - x(x-1)(x-2))$$

  why?
- Other examples such as

  $$\mathbf{A} = \mathbb{C}[x, y]/(f_1, \ldots, f_m)$$

  present kind of structure: how are the f_i's related to each other.

Very Quick Intro

- Let $\mathbf{F}$ be a field. The group $GL_d(\mathbf{F})$ acts naturally on the polynomial ring $\mathbf{R} = \mathbf{F}[x_1, \ldots, x_d]$. For a subgroup $\mathbf{G} \subset GL_d(\mathbf{F})$, the ring of invariants is the algebra

  $$\mathbf{A} = \{f \in \mathbf{R} | s(f) = f, \quad s \in \mathbf{G}\}$$

  What is $\mathbf{A}$ like?
- Let $\mathbf{R}$ be a Noetherian local integral domain that contains a finite field. $\mathbf{A} = \mathbf{R}^+$ is the integral closure of $\mathbf{R}$ in the algebraic closure of the field of quotients of $\mathbf{R}$. Why is $\mathbf{R}^+$ interesting?
- What is a Cohen-Macaulay ring? If $\mathbf{A} = \mathbf{F}[y_1, \ldots, y_n]$ is a finitely generated integral domain over the field $\mathbf{F}$, then $\mathbf{A}$ is Cohen-Macaulay if for every Noether normalization

  $$\mathbf{S} = \mathbf{F}[x_1, \ldots, x_d] \hookrightarrow \mathbf{A},$$

  $\mathbf{A}$ is a free $\mathbf{S}$-module.

Outline

1. General Orientation
2. Syllabus
3. Introduction
4. **Chain Conditions**
5. Prime Ideals
6. Primary Decomposition
7. Noetherian Rings
8. Graded Noetherian Rings
9. Commutative Artinian Rings
10. Modules of Fractions
11. Integral Extensions
12. Dedekind Domains
13. Valuation Rings
14. Homework

Chain Conditions

At the heart of CA are the chain conditions:

Let R be a ring and let M be a left (right) R-module and denote by X the set of R-submodules of M ordered by inclusion.

A chain of submodules is a sequence

$$A_1 \subseteq A_2 \subseteq \cdots \subseteq A_n \subseteq \cdots$$

or

$$B_1 \supseteq B_2 \supseteq \cdots \supseteq B_n \supseteq \cdots$$

The first is called ascending, the other descending.

Noetherian Module

Definition

M is a Noetherian (Artinian) module if every ascending (descending) chain of submodules is stationary, that is $A_n = A_{n+1} = \ldots$ from a certain point on.

R is a left (right) Noetherian(Artinian) ring if the ascending (descending) chains of left (right) ideals are stationary.

Maximal/Minimal Condition

Definition

M is an R-module with the Maximal Condition (Minimal Condition) if every subset S of X (set of submodules ordered by inclusion) contains a maximum submodule (minimum submodule).

Proposition

Let M be an R-module. Then

1. *M is Noetherian iff M has the Maximal Condition.*
2. *M is Artinian iff M has the Minimal Condition.*

Proof

Let S be a set of submodules of M. If S contains no maximal element, we can build an ascending chain

$$A_1 \subsetneq A_2 \subsetneq \cdots \subsetneq A_n \subsetneq \cdots$$

contradicting the assumption that M is Noetherian. The converse has a similar proof.

Composition Series

Proposition

Let M be an R-module satisfying both chain conditions. Then there exists a chain of submodules

$$0 \subset M_1 \subset M_2 \subset \cdots \subset M_{n-1} \subset M_n = M$$

such that each factor M_i/M_{i-1} is a simple module.

Such sequences are called composition series of length n. The existence of one such series is equivalent to M being both Noetherian and Artinian.

Theorem (Jordan-Holder)

All composition series of a module M have the same length (called the length of M and denoted $\lambda(M)$).

Noetherian Module

Proposition

M is a Noetherian R-module iff every submodule is finitely generated.

Proof.

Suppose M is Noetherian. Let us deny. Let A be a submodule of M and assume it is not finitely generated. It would permit the construction of an increasing sequence of submodules of A,

$$(a_1) \subset (a_1, a_2) \subset \cdots \subset (a_1, a_2, \ldots, a_n) \subset \cdots ,$$

$a_{n+1} \in A \setminus (a_1, \ldots, a_n)$.
Conversely if $A_1 \subseteq A_2 \subseteq \cdots$ is an increasing sequence of submodules, let $B = \cup_{i \geq 1} A_i$ is a submodule and therefore $B = (b_1, \ldots, b_m)$. Each $b_i \in A_{n_i}$ for some n_i. If $n = \max\{n_i\}$, $A_n = A_{n+1} = \cdots$. □

SES

Proposition

Let R be a ring and

$$0 \to A \xrightarrow{\mathbf{f}} B \xrightarrow{\mathbf{g}} C \to 0$$

be a short exact sequence of R-modules (that is, $\mathbf{f}$ is 1-1, $\mathbf{g}$ is onto and Image $\mathbf{f} = \ker \mathbf{g}$). Then B is Noetherian (Artinian) iff A and C are Noetherian (Artinian).

Corollary

If R is a Noetherian (Artinian) ring, then any finitely generated R-module is Noetherian (Artinian).

Proof.

By the proposition, any f.g. free R-module $F = R \oplus \cdots \oplus R$ is Noetherian (Artinian). A f.g. R-module is a quotient of a f.g. free R-module. $\square$

Proof

Let $B_1 \subseteq B_2 \subseteq \cdots$ be an ascending sequence of submodules of B. Applying $\mathbf{g}$ to it gives an ascending sequence $\mathbf{g}(B_1) \subseteq \mathbf{g}(B_2) \subseteq \cdots$ of submodules of C.

There is also an ascending sequence of submodules of A by setting $A_i = \mathbf{f}^{-1}(B_i)$.
There is n such that both sequences are stationary from that point on: $\mathbf{g}(B_n) = \mathbf{g}(B_{n+1}) = \cdots$ and $\mathbf{f}^{-1}(B_n) = \mathbf{f}^{-1}(B_{n+1}) = \cdots$.

It follows easily that $B_n = B_{n+1} = \cdots$.

Class discussion

Let us prove the following characterization of Noetherian modules over commutative rings:

Definition

Let M be a module over the commutative ring R.The set I of elements $x \in R$ such that $xm = 0$ for all $m \in M$ is an ideal called the annihilator of M, $I = \operatorname{ann} M$.

Proposition

M is a Noetherian module if and only if M is finitely generated and $R/\operatorname{ann} M$ is a Noetherian ring.

Hints

If a module M is generated by $\{m_1, \ldots, m_n\}$ define the following mapping

$$\mathbf{f} : R \longrightarrow \underbrace{M \oplus \cdots \oplus M}_{\text{n copies}}, \quad \mathbf{f}(r) = (rm_1, \ldots, rm_n)$$

verify that

- $\mathbf{f}$ is a homomorphism, of kernel $\operatorname{ann} M$
- Form the appropriate embedding of $R/\operatorname{ann} M$ into the direct sum of the M's to argue one direction
- Use, for the other direction, that M is also a module over the ring $R/\operatorname{ann} M$

Quotient rings

Let I be a two-sided proper ideal of the R and denote by R/I the corresponding cosets $\{a+I : a \in R\}$.

The quotient ring R/I is defined by the operations:

$$\begin{aligned}(a+I)+(b+I) &= (a+b)+I\\ (a+I)\times(b+I) &= ab+I\end{aligned}$$

This is a source to many new rings

Examples: Quotient rings

$$\begin{aligned}
(2) \subset \mathbb{Z} \quad &\Rightarrow \quad \mathbb{Z}_2 = \mathbb{Z}/(2) \\
(x^2 + x + 1) \subset \mathbb{Z}_2[x] \quad &\Rightarrow \quad \mathbb{Z}_2[x]/(x^2 + x + 1) = \mathbf{F}_4 \\
(x^2 + 1) \subset \mathbb{R}[x] \quad &\Rightarrow \quad \mathbb{C} = \mathbb{R}[x]/(x^2 + 1) \\
(1 + 3i) \subset \mathbb{Z}[i] \quad &\Rightarrow \quad \mathbb{Z}_{10} = R = \mathbb{Z}[i]/(1 + 3i)
\end{aligned}$$

$\mathbb{Z}[i]/(1+3i) \simeq \mathbb{Z}/(10)$

Consider the homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}[i] \to R = \mathbb{Z}[i]/(1+3i)$ induced by the embedding of $\mathbb{Z}$ in $\mathbb{Z}[i]$.We claim that φ is a surjection of kernel $10\mathbb{Z}$:

$$1+3i \equiv 0 \Rightarrow i(1+3i) \equiv 0 \Rightarrow i-3 \equiv 0 \Rightarrow i \equiv 3$$

$$a+bi \equiv a+3b \Rightarrow \varphi \text{ is surjection}$$

For n in kernel of φ,

$$\begin{aligned} n &= z(1+3i) = (a+bi)(1+31) \\ &= (a-3b) + \underbrace{(3a+b)i}_{=0} \quad \Rightarrow b = -3a \\ &= 10a \end{aligned}$$

Circle ring

Let $R = \mathbb{R}[x,y]/(x^2+y^2-1)$: the circle ring

- Consider the natural homomorphism

$$\mathbf{f} : \mathbb{R}[x,y] \longrightarrow \mathbb{R}[\cos t, \sin t], \quad \mathbf{f}(x) = \cos t, \mathbf{f}(y) = \sin t$$

  $\mathbb{R}[\cos t, \sin t]$ is the ring of trigonometric polynomials.
- $\mathbf{f}(x^2+y^2-1) = 0$ so there is an induced surjection

$$\varphi : \mathbb{R}[x,y]/(x^2+y^2-1) \to \mathbb{R}[\cos t, \sin t]$$

- φ is an isomorphism because: (i) $\mathbb{R}[\cos t, \sin t]$ is an infinite dimensional $\mathbb{R}$-vector space (why?); for any ideal L larger than (x^2+y^2-1), $\mathbb{R}[x,y]/L$ is a finite dimensional $\mathbb{R}$-vector space (why?).

- The circle ring $R = \mathbb{R}[\cos t, \sin t]$ contains as a subring $S = \mathbb{R}[\cos t]$. S is isomorphic to a polynomial ring over $\mathbb{R}$. As an S-module, R is generated by two elements

$$R = S \cdot 1 + S \cdot \sin t$$

- R as a $\mathbb{R}$-vector space has basis

$$\{\sin nt, \cos nt, \quad n \in \mathbb{Z}\}$$

$\mathbb{R}[x,y]/(xy)$

Exercise: Prove that

$$\mathbb{R}[x,y]/(xy) \simeq \{(p(x),q(y)) : p(0) = q(0))\}$$

Hint: Consider the homomorphism

$$\varphi : \mathbb{R}[x,y]/(xy) \to \mathbb{R}[x,y]/(y) \times \mathbb{R}[x,y]/(x)$$

$$\varphi(a+(xy)) = (a+(y), a+(x))$$

Check that φ is one-one and determine its image.

Outline

Some terminology in studying a commutative ring

Let R be a commutative ring

- $u \in R$ is a unit if there is $v \in R$ such that $uv = 1$
- $a \in R$ is a zero divisor if there is $0 \neq b \in R$ such that $ab = 0$: $\overline{2} \cdot \overline{3} = 0$ in $\mathbb{Z}_6$.
- $a \in R$ is nilpotent if there is $n \in \mathbb{N}$ such that $a^n = 0$: $\overline{2}^3 = 0$ in $\mathbb{Z}_8$.
- R is an integral domain if 0 is the only zero divisor, in other words, if $a, b \in R$ are not zero, then $ab \neq 0$.

Prime Ideals

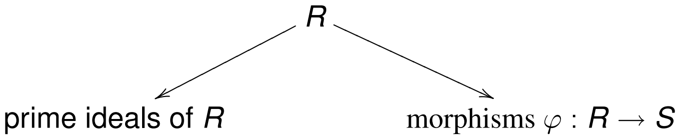
Definition

Let R be a commutative ring. An ideal P of R is prime if $P \neq R$ and whenever $a \cdot b \in P$ then $a \in P$ or $b \in P$.

Equivalently:

- R/P is an integral domain
- If I and J are ideals and $I \cdot J \subset P$ then $I \subset P$ or $J \subset P$

Prime ideals and homomorphisms



R

prime ideals of R

morphisms $\varphi : R \to S$

Prime ideals arise in issues of factorization and very importantly:

Proposition

Let $\varphi : R \to S$ be a homomorphism of commutative ring. If S is an integral domain, then $P = \ker(\varphi)$ is a prime ideal. More generally, if S is an arbitrary commutative ring and Q is a prime ideal, then $P = \varphi^{-1}(Q)$ is a prime ideal of R.

Proof. Inspect the diagram

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d] & S \arrow[d] \\
R/P \arrow[r, hook] & S/Q
\end{tikzcd}$$

Exercise

Consider the homomorphism of rings

$$\begin{array}{rcl} \varphi : k[x,y,z] & \longrightarrow & k[t] \\ x & \longrightarrow & t^3 \\ y & \longrightarrow & t^4 \\ z & \longrightarrow & t^5 \end{array}$$

Let P be the kernel of this morphism. Note that $x^3 - yz$, $y^2 - xz$ and $z^2 - x^2y$ lie in P.

Task: Prove that P is generated by these 3 polynomials.

Task: Describe the prime ideals of the ring

$$R = \mathbb{C}[x,y]/(y^2 - x(x-1)(x-2)).$$

Multiplicative Sets

Definition

A subset S of a commutative ring is multiplicative if $S \neq \emptyset$ and if $r, s \in S$ then $r \cdot s \in S$.

- If $a \in R$, $\{a^n : n \in \mathbb{N}\}$ is a multiplicative set.
- If P is a prime ideal of R, $S = R \setminus P$ is a multiplicative set.
- If I is a proper ideal of R, then

$$S = \{1 + a : a \in I\}$$

is a multiplicative set.

Formation of Prime Ideals

Proposition

Let S be a multiplicative set and P an ideal maximum with respect $S \cap P = \emptyset$. Then P is a prime ideal.

Proof. Deny: let $a, b \notin P$, $ab \in P$.

Consider the ideals $P + Ra$ and $P + Rb$. They are both larger than P and therefore meet S: there exist $p, q \in R$ with

$$x + pa, y + qb \in S, \quad x, y \in P$$

Multiplying we get

$$(x + pa)(y + qb) = xy + xqb + yqb + pqab \in S \cap P,$$

a contradiction.

Corollary

Every proper ideal I of a commutative ring is contained in a prime ideal.

Proof. Let $S = \{1\}$. This is a multiplicative set. An ideal M is proper if M is disjoint from S.

Among all proper ideals $I \subseteq J$ pick one that is maximum with respect being disjoint relative to S: How?

Let X be the set of proper ideals containing I. If $\{J_\alpha\}$ is a chain of elements in X, $\bigcup J_\alpha \in X$. By Zorn's Lemma, there are maximum elements in X.
No need if R is Noetherian.

Primary Ideal

Definition

Let R be a commutative ring. An ideal Q of R is primary if $Q \neq R$ and whenever $a \cdot b \in Q$ then $a \in Q$ or some power $b^n \in Q$.

Example: $Q = (x^2, y) \subset R = k[x, y]$, or $(p^n) \subset \mathbb{Z}$.
This is a far-reaching generalization of the notion of primary ideals of $\mathbb{Z}$

Radical of an Ideal

Definition

Let I be an ideal of the commutative ring R. The radical of I is the set

$$\sqrt{I} = \{x \in R : x^n \in I \quad \text{some } n = n(x)\}.$$

Proposition

$\sqrt{I}$ is an ideal.

Proof.

If $a, b \in \sqrt{I}$, $a^m \in I$, $b^n \in I$, then

$$(a+b)^{m+n-1} = \sum_{i+j=m+n-1} \binom{m+n-1}{i} a^i b^j \in I,$$

since $i \geq m$ or $j \geq n$.

Proposition

If I is a proper ideal of R,

$$\sqrt{I} = \bigcap P, \quad I \subseteq P \quad P \text{ prime ideal.}$$

Proof.

Deny it: Let $x \in \bigcap P \setminus \sqrt{I}$, that is for all n, $x^n \notin I$.

The set $\{x^n, n \in \mathbb{N}\}$ defines a multiplicative set S disjoint from I. By a previous proposition, there is a prime $P \supset I$ disjoint from S, a contradiction. □

Class discussion

Let R be a commutative ring and $S = R[x]$ the ring of polynomials in the indeterminate x.

- If I is an R-ideal, the set of all polynomials
$$a_n x^n + \cdots + a_0, \quad a_i \in I,$$
is an $R[x]$-ideal Notation: $I[x]$ or $I \cdot R[x]$.
- If P is a prime ideal of R, then $P[x]$ is a prime ideal of $R[x]$. $P[x]$ is the kernel of the homomorphism
$$\varphi : R[x] \longrightarrow R/P[x]$$
$$\varphi(a_n x^n + \cdots + a_0) = \overline{a_n} x^n + \cdots + \overline{a_0},$$
where $\overline{a}$ is the coset $a + P$ of R/P.

Radical of $R[x]$

Proposition

If N is the nilradical of R, then $N[x]$ is the nilradical of $R[x]$.

Proof. (One volunteer, please.)

Idempotents

Proposition

Let R be a commutative ring and $0 \neq e \in R$ satisfy $e = e^2$. Then there is a decomposition R into the direct product of rings $R \simeq Re \times R(1 - e)$.

Proof.

1. For any $x \in R$, $x = xe + x(1 - e)$, so $Re + R(1 - e) = R$. Furthermore if $a \in Re \cap R(1 - e)$, then a is annihilated by $1 - e$ and e, respectively. This means that $R = Re \oplus R(1 - e)$ as modules.
2. Since $Re \cdot R(1 - e) = 0$, we can view $R = Re \oplus R(1 - e)$ as $R = Re \times R(1 - e)$. Note that e is the identity in the ring Re, and $1 - e$ in $R(1 - e)$.

Outline

1. General Orientation
2. Syllabus
3. Introduction
4. Chain Conditions
5. Prime Ideals
6. **Primary Decomposition**
7. Noetherian Rings
8. Graded Noetherian Rings
9. Commutative Artinian Rings
10. Modules of Fractions
11. Integral Extensions
12. Dedekind Domains
13. Valuation Rings
14. Homework

Emmy Noether (1882-1935)

http://upload.wikimedia.org/wikipedia/commons/e/e5/Noether.jpg

Irreducible Ideal/Module

Definition

The ideal I of the commutative ring R is irreducible if

$$I = J \cap L \Rightarrow I = J \quad \text{or} \quad I = L.$$

Primary Decomposition

Theorem (Emmy Noether)

Every proper ideal I of a Noetherian ring R has a finite decomposition

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_n,$$

with Q_i primary.

To prove her theorems, Emmy Noether often proved a special case and derive the more general assertion, or proved a more general assertion and specialize.

Irreducible decomposition

Definition

The ideal I of the commutative ring R is irreducible if

$$I = J \cap L \Rightarrow I = J \quad \text{or} \quad I = L.$$

Theorem (Emmy Noether)

Every proper ideal I of a Noetherian ring R has a finite decomposition

$$I = J_1 \cap J_2 \cap \cdots \cap J_n,$$

with J_i irreducible. Moreover, every irreducible ideal J of R is primary.

Famous Proof

Proof. Deny the existence of the decomposition of I as a finite intersection of irreducible ideals. Among all such ideals, denote by (keep the notation) I a maximum one.
I is not irreducible, so there is

$$I = J \cap L,$$

with J and L properly larger. But then each admits finite decompositions as intersection of irreducible ideals. Combining we get a contradiction.

Irreducible $\Rightarrow$ Primary

1. Deny that proper irreducible ideals of Noetherian rings are primary. Let I be maximum such: There is $a, b \in R$, $ab \in I$, $a \notin I$ and $b^n \notin I$ for all $n \in \mathbb{N}$.
2. Consider the chain
$$\{r \in R : br \in I\} = I : b \subseteq I : b^2 \subseteq \cdots \subseteq I : b^n \subseteq I : b^{n+1}$$
that becomes stationary at $I : b^n = I : b^{n+1}$.
3. Define $J = I : b^n$ and $L = (I, b^n)$. Both ideals are larger than I. We claim that $I = J \cap L$.
4. If $x \in J \cap L$, $x = u + rb^n$, $u \in I$. Then $b^n x = b^n u + rb^{2n} \in I$, so $rb^n \in I$ and therefore $x \in I$.

Irredundant Primary Decomposition

A refinement in the primary decomposition

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_n$$

arises as follows. Suppose two of the Q_i have the same radical, say $\sqrt{Q_1} = \sqrt{Q_2} = P$. Then it easy to check that $Q_1 \cap Q_2$ is also P-primary. So collecting the Q_i with the same radical:

Theorem (Emmy Noether)

Every proper ideal I of a Noetherian ring R has a finite decomposition

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_n,$$

with Q_i primary ideals of distinct radicals. This decomposition is called irredundant.

It is known which Q_i are unique and which are not.

Minimal primes

An application of this theory is:

Corollary

Let $I = \bigcap_{i=1}^{n} J_i$ be a primary decomposition of the ideal I. Then any prime ideal P containing I contains one of the prime ideals $\sqrt{J_i}$. In particular, there is a minimal prime P containing I.

Proof.

Since

$$\prod_{i=1}^{n} J_i \subset \bigcap_{i=1}^{n} J_i = I \subset P,$$

P contains some J_i, and therefore $\sqrt{J_i}$.
The smallest among the $\sqrt{J_i}$ are the minimal primes of I.

□

Outline

1. General Orientation
2. Syllabus
3. Introduction
4. Chain Conditions
5. Prime Ideals
6. Primary Decomposition
7. **Noetherian Rings**
8. Graded Noetherian Rings
9. Commutative Artinian Rings
10. Modules of Fractions
11. Integral Extensions
12. Dedekind Domains
13. Valuation Rings
14. Homework

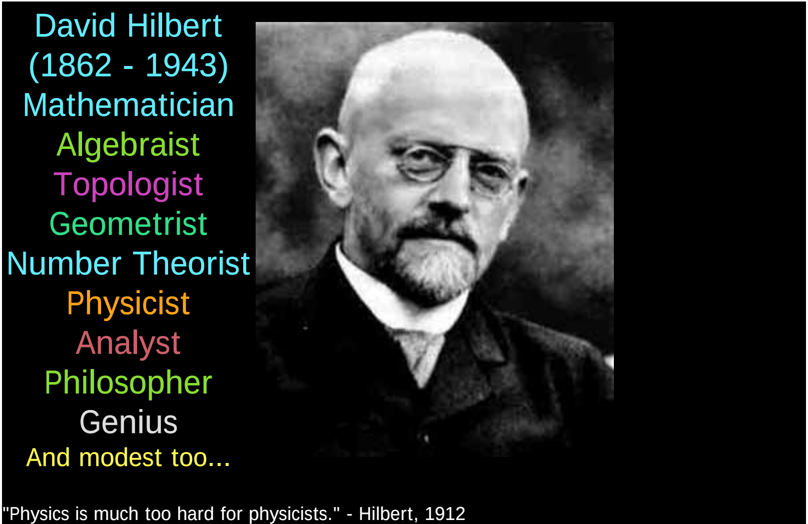
Noetherian Rings

At the heart of Commutative Algebra lies the notion of a Noetherian ring and the methods and processes that produce such rings. We will begin with a review of the following topics:

- Chain conditions
- Hilbert basis theorem, Cohen theorem, power series
- Primary decomposition
- Artin–Rees lemma
- Filtrations and Rees algebras

David Hilbert (1862-1943)

David Hilbert



"Physics is much too hard for physicists." - Hilbert, 1912

Hilbert Basis Theorem

Theorem (HBT)

If R is Noetherian then $R[x]$ is Noetherian.

1. If R is Noetherian and $x_1, \ldots, x_n$ is a set of independent indeterminates, then $R[x_1, \ldots, x_n]$ is Noetherian.
2. $\mathbb{Z}[x_1, \ldots, x_n]$ is Noetherian.
3. If k is a field, then $k[x_1, \ldots, x_n]$ is Noetherian.

Finitely Generated Algebras

If R is a commutative ring, a finitely generated R-algebra S is a homomorphic image of a ring of polynomials, $S = R[x_1, \ldots, x_n]/L$. If R is Noetherian, S is Noetherian as well. This is useful in many constructions.
If I is an R-ideal, the Rees algebra of I is the subring of $R[t]$ generated by all at, $a \in I$. It it denoted by $S = R[It]$. In general, subrings of Noetherian rings may not be Noetherian but Rees algebras are:

Exercise: If R is Noetherian, for every ideal I, $R[It]$ is Noetherian.

Proof of the HBT

Suppose the $R[x]$-ideal I is not finitely generated. Let $0 \neq f_1(x) \in I$ be a polynomial of smallest degree,

$$f_1(x) = a_1 x^{d_1} + \text{lower degree terms.}$$

Since $I \neq (f_1(x))$, let $f_2(x) \in I \setminus (f_1(x))$ of least degree. In this manner we get a sequence of polynomials

$$f_i(x) = a_i x^{d_i} + \text{lower degree terms,}$$

$$f_i(x) \in I \setminus (f_1(x), \ldots, f_{i-1}(x)), \quad d_1 \leq d_2 \leq d_3 \leq \cdots$$

Set $J = (a_1, a_2, \ldots,) = (a_1, a_2, \ldots, a_m) \subseteq R$

Let $f_{m+1}(x) = a_{m+1}x^{d_{m+1}} + \text{lower degree terms}$. Then

$$a_{m+1} = \sum_{i=1}^{m} s_i a_i, \quad s_i \in R.$$

Consider

$$\mathbf{g}(x) = f_{m+1} - \sum_{i=1}^{m} s_i x^{d_{m+1}-d_i} f_i(x).$$

$\mathbf{g}(x) \in I \setminus (f_1(x), \ldots, f_m(x))$, but $\deg \mathbf{g}(x) < \deg f_{m+1}(x)$, which is a contradiction.

Power Series Rings

Another construction over a ring R is that of the power series ring $R[[x]]$:

$$\mathbf{f}(x) = \sum_{n \geq 0} a_n x^n, \quad \mathbf{g}(x) = \sum_{n \geq 0} b_n x^n$$

with addition component wise and multiplication the Cauchy operation

$$\begin{aligned} \mathbf{f}(x)\mathbf{g}(x) = \mathbf{h}(x) &= \mathbf{h}(x) = \sum_{n \geq 0} c_n x^n \\ c_n &= \sum_{i+j=n} a_i b_{n-i} \end{aligned}$$

Theorem

If R is Noetherian then $R[[x]]$ is Noetherian.

Proposition

A commutative ring R is Noetherian iff every prime ideal is finitely generated.

Proof. If R is not Noetherian, there is an ideal I maximum with the property of not being finitely generated (Zorn's Lemma). We assume I is not prime, that is there exist $a, b \notin I$ such that $ab \in I$.

The ideals (I, a) and $I : a$ are both larger than I and therefore are finitely generated:

$$\begin{aligned} (I : a) &= (a_1, \dots, a_n) \\ (I, a) &= (b_1, \dots, b_m, a), \quad b_i \in I \end{aligned}$$

Claim: $I = (b_1, \dots, b_m, aa_1, \dots, aa_n)$

If $c \in I$,

$$c = \sum_{i=1}^{m} c_i b_i + ra, \quad r \in I : a$$

$R[[x]]$ is Noetherian

Proof. Let P be a prime ideal of $R[[x]]$. Set $\mathfrak{p} = P \cap R$. $\mathfrak{p}$ is a prime ideal of R and therefore it is finitely generated.

Denote by $\mathfrak{p}[[x]] = \mathfrak{p}R[[x]]$ the ideal of $R[[x]]$ generated by the elements of $\mathfrak{p}$. It consists of the power series with coefficients in $\mathfrak{p}$ and $R[[x]]/\mathfrak{p}[[x]]$ is the power series ring $R/\mathfrak{p}[[x]]$.

We have the embedding

$$P' = P/\mathfrak{p}[[x]] \hookrightarrow (R/\mathfrak{p})[[x]]$$

P' is a prime ideal of $R/\mathfrak{p}[[x]]$ and $P' \cap R/\mathfrak{p} = 0$. It will suffice to show that P' is finitely generated.

We have reduced the proof to the case of a prime ideal $P \subset R[[x]]$ and $P \cap R = (0)$.

If $x \in P$, $P = (x)$ and we are done.
For $\mathbf{f}(x) = a_0 + a_1 x + \cdots \in P$, let $J = (b_1, \ldots, b_m) \subset R$ be the ideal generated by all a_0,

$$\mathbf{f}_i = b_i + \text{higher terms} \in P.$$

Claim: $P = (\mathbf{f}_1, \ldots, \mathbf{f}_m)$.

From $a_0 = \sum_i s_i^{(0)} b_i$, we write

$$\mathbf{f}(x) - \sum_i s_i^{(0)} \mathbf{f}_i = x\mathbf{h} \quad \Rightarrow \mathbf{h} \in P.$$

We repeat with **h** and write

$$\mathbf{f}(x) = \sum_i s_i^{(0)}\mathbf{f}_i + x\sum_i s_i^{(1)}\mathbf{f}_i + x^2\mathbf{g}, \quad \mathbf{g} \in P.$$

Iterating we obtain

$$\mathbf{f}(x) = \sum_i (s_i^{(0)} + s_i^{(1)}x + s_i^{(2)}x^2 + \cdots)\mathbf{f}_i.$$

Symbolic Powers

Let R be a Noetherian ring, and let P be a prime ideal. Consider a primary decomposition of the nth power of P^n,

$$P^n = \bigcap_{i=1}^{m} J_i.$$

- Any prime ideal Q that ccntains P^n contains P: Thus P is the unique minimal prime of P^n.
- This means that $P_P^n = (J_i)_P$ for some i. Since $(P^n)_P$ is a power of the maximal ideal of the localization R_P, the corresponding ideal J_i is P-primary.

Definition

The P-primary component of P^n is independent of the primary decomposition. It is called the nth symbolic power of P: $P^{(n)}$.

Example/Exercise

Let $R = \mathbb{Q}[x, y, z]$. This ring has 3 types of prime ideals: principal ideals, maximal ideals, 'the others'. If P is any of the two first types, $P^{(n)} = P^n$. To find an example whose ordinary and symbolic powers differs, let us consider homomorphisms $\phi : R \to \mathbb{Q}[t]$.

For example, let ϕ be defined by $\phi(x) = t^3$, $\phi(y) = t^4$ and $\phi(z) = t^5$. The kernel is the prime ideal P generated by

$$P = (x^3 - yz, y^2 - xz, z^2 - x^2y)$$

1. Prove that P is generated by these polynomials.
2. Find $P^{(2)}$ and verify it is not P^2.

Outline

1. General Orientation
2. Syllabus
3. Introduction
4. Chain Conditions
5. Prime Ideals
6. Primary Decomposition
7. Noetherian Rings
8. **Graded Noetherian Rings**
9. Commutative Artinian Rings
10. Modules of Fractions
11. Integral Extensions
12. Dedekind Domains
13. Valuation Rings
14. Homework

Graded Rings

Let R be a ring and A an R-algebra. We say that A is a graded R-algebra if

$$A = \bigoplus_{n \in \mathbb{Z}} A_n, \quad A_m \cdot A_n \subset A_{m+n}$$

- Polynomials rings $R[x_1, \ldots, x_n]$ are major examples.
- The elements $x \in A_n$ are called n-forms or homogeneous of degree n.
- We usually assume $A_n = 0$ if $n < 0$. A notable exception is $A = k[x, x^{-1}]$, the ring of Laurent polynomials.

Homogeneous ideals

Definition

An ideal I of a graded algebra is said to be homogeneous if $I = \bigoplus_{n\in\mathbb{Z}} I_n$, $I_n \subset A_n$.

They are handy way to produce new graded algebras:

$$A/I = \bigoplus_n A_n/I_n$$

Proposition

An ideal I of a graded algebra A is homogeneous iff I s generated by a set $\{\mathbf{f}_\alpha\}$ of homogeneous forms $\mathbf{f}_\alpha$.

Proof. Left to reader/listener.

Graphs and Ideals

Let $G = \{V, E\}$ be a graph of vertex set $V = \{v_1, \ldots, v_n\}$ and edge set E. We will associate to G a graded algebra.

- Let $R = k[x_1, \ldots, x_n]$, one indeterminate to each vertex. To the edge $\{v_i, v_j\}$, we associate the monomial $x_i x_j$. The edge ideal of G is the ideal $I(G)$ generated by all $x_i x_j$'s.
- $I(G)$ is a homogeneous ideal. One expects the graded algebra $R/I(G)$ to reflect properties of the graph. For example, describe the minimal primes of $I(G)$ in graph theoretic info.

Graded Noetherian Rings

One of the first ‘practical’ uses of the Hilbert basis theorem was:

Proposition

Let $R = \sum_{n \geq 0} R_n$ be a positively graded commutative ring and set $R_+ = \sum_{n>0} R_n$. Then R is Noetherian if and only if R_0 is Noetherian and R_+/R_+^2 is a finitely generated R_0–module.

Proof. Suppose the conditions on R_0 and R_+ hold. Since R_+/R_+^2 is a direct sum of R_0–modules, there exists $r \in \mathbb{N}$ such that $R_n = \sum_{0<i<r} R_i R_{n-i}$ for $n \geq r$. Pick a finite set $\{b_1, \ldots, b_s\}$ of elements in $\bigcup_{0<i<r} R_i$ that generate R_+/R_+^2. The claim is that $R = R_0[b_1, \ldots, b_s]$. Since R_1 is a direct summand of R_+/R_+^2, it is finitely generated by the b_j of degree 1. The next summand, R_2/R_1^2 is generated by the images of the b_j of degree 2, while R_1^2 is generated by the 2-products of the earlier b_j’s.

From the exact sequence

$$0 \to R_1^2 \longrightarrow R_2 \longrightarrow R_2/R_1^2 \to 0,$$

it follows that R_2 consists of the degree 2 elements of $R_0[b_1, \ldots, b_s]$. We proceed in this fashion until $n = r$, when no new generators are needed.

For the converse, it suffices to note that $R_0 = R/R_+$ and that R_+/R_+^2 is an R–module annihilated by R_+. □

Outline

1. General Orientation
2. Syllabus
3. Introduction
4. Chain Conditions
5. Prime Ideals
6. Primary Decomposition
7. Noetherian Rings
8. Graded Noetherian Rings
9. **Commutative Artinian Rings**
10. Modules of Fractions
11. Integral Extensions
12. Dedekind Domains
13. Valuation Rings
14. Homework

Commutative Artinian Rings

Definition

The ring R is Artinian if it has the descending chain condition for ideals.

Besides fields, or finite rings, the simplest [yet not so simple] examples are algebras that are finite dimensional vector spaces over a field $\mathbf{K}$.

For non-commutative rings, this chain condition can be expressed in many forms [will explain later], but in the commutative case they just turn out to be a special type of Noetherian rings.

Elementary Properties

- Every prime ideal P of a commutative Artinian ring R is maximal: The quotient R/P is a domain so ETS Artinian domains are fields. If $a \neq 0$, the chain $(a) \supset (a^2) \supset \cdots$ stabilizes at $(a^n) = (a^{n+1})$, therefore $a^n = ra^{n+1}$ so $1 = ra$, since the ring is a domain.
- R has only a finite number of maximal ideals: Let $\{P_2, P_2, \ldots\}$ be distinct maximal ideals. Form the descending chain

  $$P_1 \supset P_1 \cdot P_2 \supset P_1 \cdot P_2 \cdot P_3 \supset \cdots$$

  that becomes stationary at

  $$P_1 \cdot P_2 \cdots P_n = P_1 \cdot P_2 \cdots P_n \cdot P_{n+1}$$

  Therefore P_{n+1} contains $P_1 \cdot P_2 \cdots P_n$, and thus $P_{n+1} = P_i$, $i \leq n$.

Jacobson Radical

Theorem

Let J be the intersection of all the maximal ideals of the Artinian ring R. Then $J^n = 0$ for some integer n.

Proof.

Consider the descending chain $J \supset J^2 \supset \cdots$ that stabilizes at $J^n = J^{n+1}$.

We claim that $J^n = 0$.

- We argue by contradiction. Consider the set of nonzero ideals L such that $J^n L \neq 0$. Note that by assumption J is one such ideal.

- Choose a minimum ideal L with this property. Now, let $x \in L$ such that $J^n x \neq 0$. This shows $L = Rx$ by the minimality hypothesis and $x = ax$, $a \in J^n$.

- This implies $(1 - a)x = 0$ and therefore $x = 0$ since $1 - a$ is invertible, a contradiction.

Partition of the Unity

If R is a commutative ring, a partition of the unity is an special decomposition of the form

$$R = J_1 + \cdots + J_n, \quad J_i \text{ ideals of } R$$

Suppose $I_1, \ldots, I_n$ is a set of a ideals that is pairwise co-maximal, meaning $I_i + I_j = R$, for $i \neq j$. This obviously is a partition of the unity.

Another arises from it [check!] if we set $J_i = \prod_{j \neq i} I_j$

$$R = J_1 + \cdots + J_n, \quad J_i \text{ ideals of } R$$

Chinese Remainder Theorem

Theorem

If I_i, $i \leq n$, is a family of ideals that is pairwise co-maximal, then for $I = I_1 \cap I_2 \cap \cdots \cap I_n$ there is an isomorphism

$$R/I \quad \approx \quad R/I_1 \times \cdots \times R/I_n.$$

Proof. Set $J_i = \prod_{j \neq i} I_j$. Note that $I_i + J_i = R$. Since $J_1 + \cdots + J_n = R$, there is an equation

$$1 \quad = \quad a_1 + \cdots + a_n, \quad a_i \in J_i$$

Note that for each i, $a_i \cong 1 \mod I_i$. Define a mapping **h** from R to $R/I_1 \times \cdots \times R/I_n$, by $\mathbf{h}(x) = (\overline{xa_1}, \ldots, \overline{xa_n})$. We claim that **h** is a surjective homomorphism of kernel I.

Proof Cont'd

1. Since $a_i \cong 1 \mod I_i$,

$$\mathbf{h}(x) = (\overline{xa_1}, \ldots, \overline{xa_n}) = (\overline{x}_1, \ldots, \overline{x}_n)$$

   which is clearly a homomorphism.

2. The kernel consists of the x such that $\overline{x}_i = 0$ for each i, that is $x \in I_i$ for each i–that is, $x \in I$.

3. To prove $\mathbf{h}$ surjective, for $u = (\overline{x_1}, \ldots, \overline{x_n})$, setting

$$x \quad = \quad x_1 a_1 + \cdots + x_n a_n$$

   gives $\mathbf{h}(x) = u$.

Structure of Artinian Rings

Theorem

Let R be a commutative Artinian ring, let $\{P_1, \ldots, P_n\}$ be the set of its maximal ideals, J its Jacobson radical and m an integer such that $J^m = 0$. Then

$$R \quad \approx \quad R/P_1^m \times \cdots \times R/P_n^m.$$

Moreover each R/P_i^m is Noetherian.

We apply CRT to the set of ideals $P_1^m, \ldots, P_n^m$ to obtain the decomposition. Now we must prove that each R/P_i^m is Noetherian.

Note that $S = R/P_i^m$ has a unique maximal ideal $M = P_i/P_i^m$, and that $M^m = 0$.

Proof Cont'd

1. Consider the chain of ideals $R \supset M \supset M^2 \supset M^{m-1} \supset M^m = 0$. To prove that R is Noetherian ETS each factor module M^i/M^{i+1} is Noetherian. [See last step]
2. We examine the factors M^i/M^{i+1}. This module is Artinian and is also annihilated by M. So it is actually an Artinian R/M-vector space, so must be finite dimensional, in particular it is a Noetherian module.
3. For example, suppose $M^3 = 0$. M^2 is annihilated by M, so it is a R/M-vector space, so it is also a Noetherian R-module.
4. Consider the exact sequence $0 \to M^2 \to M \to M/M^2 \to 0$. Both M^2 and M/M^2 are Noetherian, so M is Noetherian as well. The general case is similar.

Composition series

Theorem

If R is a commutative Artinian ring then there exists a tower of ideals

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = R$$

such that for all i, $M_i/M_{i-1} = R/P_i$ for some prime ideal P_i.

Proof. Left to reader.

Outline

1. General Orientation
2. Syllabus
3. Introduction
4. Chain Conditions
5. Prime Ideals
6. Primary Decomposition
7. Noetherian Rings
8. Graded Noetherian Rings
9. Commutative Artinian Rings
10. **Modules of Fractions**
11. Integral Extensions
12. Dedekind Domains
13. Valuation Rings
14. Homework

Modules of Fractions

Let R be a commutative ring, M an R-module and $S \subseteq R$ a multiplicative system.

On the set $M \times S$ define the following relation:

$$(a, r) \sim (b, s) \Leftrightarrow \exists t \in S : t(as - br) = 0$$

Why define it in this manner instead of the usual $as = br$?

Proposition

$\sim$ *is an equivalence relation.*

We focus on the properties of the set $S^{-1}M$ of equivalence classes. Actually, this is the initial step in the construction of a remarkable functor.

Properties

Proposition

Let R be a commutative ring, M an R-module and $S \subseteq R$ a multiplicative system. Denote the equivalence class of (a, r) in $S^{-1}M$ by $\overline{(a, r)}$ (or simply (a, r) or even a/r).

1. *The following operation is well-defined*

$$\overline{(a, r)} + \overline{(b, s)} = \overline{(sa + rb, rs)},$$

   and endows $S^{-1}M$ with a structure of abelian group.

2. *If $0 \notin S$, this construction applied to $R \times S$ gives rise to a ring structure on $S^{-1}R$ with multiplication $\overline{(x, r)} \cdot \overline{(y, s)} = \overline{(xy, rs)}$.*

3. *For $\overline{(x, r)} \in S^{-1}R$ and $\overline{(a, s)} \in S^{-1}M$, the operation $\overline{(x, r)} \cdot \overline{(a, s)} = \overline{(xa, rs)}$ defines an $S^{-1}R$-module structure on $S^{-1}M$.*

Module/Ring of Fractions

$S^{-1}R$ is called the ring of fractions of R relative to S. It is a refinement (due to Grell or Krull) of the classical formation of the field of fractions of an integral domain.
$S^{-1}M$ is called the module of fractions of M relative to S.

Another step:

Proposition

If $\varphi : M \to N$ is a homomorphism of R-modules, a homomorphism of $S^{-1}R$ modules $S^{-1}\varphi : S^{-1}M \to S^{-1}N$ is defined by

$$(S^{-1}\varphi)(a, s) = (\varphi(a), s).$$

Functorial Properties

This construction is a functor from the category of R-modules to the category of $S^{-1}R$-modules:

$$\begin{tikzcd} M \arrow[r, phantom, "\rightsquigarrow"] \arrow[d, "\varphi"'] & S^{-1}M \arrow[d, "S^{-1}\varphi"] \\ N \arrow[r, phantom, "\rightsquigarrow"] & S^{-1}N \end{tikzcd}$$

Proposition

If $\varphi : M \to N$ and $\psi : N \to P$ are R-homomorphisms of R-modules, then

1. $S^{-1}(\psi \circ \varphi) = S^{-1}\psi \circ S^{-1}\varphi$.
2. $S^{-1}(id_M) = id_{S^{-1}M}$.

Short Exact Sequences

Proposition

Let R be a ring, $S \subseteq R$ a multiplicative set and

$$0 \to A \xrightarrow{\mathbf{f}} B \xrightarrow{\mathbf{g}} C \to 0$$

a short exact sequence of R-modules. Then

$$0 \to S^{-1}A \xrightarrow{S^{-1}\mathbf{f}} S^{-1}B \xrightarrow{S^{-1}\mathbf{g}} S^{-1}C \to 0$$

is a short exact sequence of $S^{-1}R$-modules. In other words, $M \rightsquigarrow S^{-1}M$ is an exact functor.

The submodules of $S^{-1}M$

Proposition

Let L' be a $S^{-1}R$-submodule of $S^{-1}M$. Let

$$L = \{m \in M : \text{for some } s \in S \quad (m, s) \in L'.$$

Then L is a submodule of M and $S^{-1}L = L'$.

Corollary

If M is a Noetherian (Artinian) R-module, then $S^{-1}M$ is a Noetherian (Artinian) $S^{-1}R$-module.

The ideals of $S^{-1}R$

According to the above, the proper ideals of $S^{-1}R$ are of the form

$$S^{-1}I = \{a/s : a \in I \quad s \in S, \quad I \cap S = \emptyset.\}$$

In the special case of $S = R \setminus \mathfrak{p}$, for a prime ideal $\mathfrak{p}$, one uses the notation $M_{\mathfrak{p}}$ for the module of fractions and $R_{\mathfrak{p}}$ for the ring of fractions.

If $R = \mathbb{Z}$ and $\mathfrak{p} = (2)$, $\mathbb{Z}_{(2)}$ consists of all rational numbers m/n, with n odd. Its ideals are ordered. The largest proper ideal is $\mathfrak{m} = 2\mathbb{Z}_{(2)}$ and the others

$$\mathbb{Z}_{(2)} \supsetneq \mathfrak{m} \supsetneq \mathfrak{m}^2 \supsetneq \mathfrak{m}^3 \supsetneq \cdots \supsetneq (0)$$

Tool

Proposition

If R is a commutative ring and S is a multiplicative set, then for any two submodules A and B of M,

$$S^{-1}(A \cap B) = S^{-1}A \cap S^{-1}B.$$

Proof.

The intersection $A \cap B$ can be defined by the exact sequence

$$0 \to A \cap B \longrightarrow A \oplus B \xrightarrow{\varphi} A + B \to 0,$$

where $\varphi(a, b) = a - b$.

Now apply the fact that formation of modules of fractions is an exact functor. □

Local Ring

Proposition

Let S be a multiplicative set of R. The ideal L of $S^{-1}R$ is prime iff $L = S^{-1}I$, for some prime I ideal of R with $I \cap S = \emptyset$.

Proof. Suppose I is as above. If $a/r \cdot b/s \in S^{-1}I$, $(ab, rs) \sim (c, t)$ for $c \in I$, $r, s, t \in S$. By definition, there is $u \in S$ such that $u(tab - rsc) = 0$. Since $S \cap I = \emptyset$, $tab - rsc \in I$ and therefore $tab \in I$. Thus $ab \in I$ and so $a \in I$ or $b \in I$. Therefore (a, r) or $(b, s) \in S^{-1}I$.

Corollary

The prime ideals of $R_{\mathfrak{p}}$ have the form $P = Q_{\mathfrak{p}}$, where Q is an ideal of R contained in $\mathfrak{p}$.

Local Ring

Definition

A commutative ring R is a local ring if it has a unique maximal ideal.

Example

If k is a field, $R = k[[x]]$, the ring of formal power series in x over k is a local ring. Its unique maximal ideal is $\mathfrak{m} = (x)$.

Definition

If R is a commutative ring and P a prime ideal, the ring of fractions R_P is a local ring called the localization of R at P.

The Prime Spectrum of a Ring

Definition

Let R be a commutative ring (with 1). The set of prime ideals of R is called the prime spectrum of R, and denoted $\operatorname{Spec}(R)$.

$\operatorname{Spec}(\mathbb{Z}) = \{(0), (2), (3), \ldots\}$, the ideals generated by the prime integers and 0.

Proposition

For each set $I \subset R$, set

$$V(I) = \{\mathfrak{p} \in \operatorname{Spec}(R) : I \subset \mathfrak{p}\}.$$

These subsets are the closed sets of a topology on $\operatorname{Spec}(R)$.

Note that $V(I) = V(I')$, where I' is the ideal of R generated by I.

Zariski Topology

Proof. This follows from the properties of the construction of the $V(I)$:

$$\begin{aligned} V(1) &= \emptyset \\ V(0) &= \operatorname{Spec}(R) \\ V(I \cap J) &= V(I) \cup V(J) \\ \bigcap_{\alpha} V(I_\alpha) &= V(\bigcup_{\alpha} I_\alpha). \end{aligned}$$

Example

Suppose $R_2, R_2, \ldots, R_n$ are commutative rings and $R = R_1 \times R_2 \times \cdots \times R_n$ is their direct product. Observe:

1. If $1 = e_1 + e_2 + \cdots + e_n$, $e_i \in R_i$, then $R_i = Re_i$ and $e_i e_j = 0$ if $i \neq j$
2. Because of $e_i e_j = 0$ for $i \neq j$, if P is a prime ideal of R and some $e_i \notin P$ then the other $e_j \in P$. This shows $P = R_1 \times \cdots \times P_i \times \cdots \times R_n$, where P_i is a prime ideal of R_i, $R/P = R_i/P_i$
3. $\mathrm{Spec}\,(R) = \mathrm{Spec}\,(R_1) \cup \cdots \cup \mathrm{Spec}\,(R_n)$
4. In particular, if $R_1 = R_2 = \cdots = R_n = \mathbf{K}$, $\mathbf{K}$ a field, the $\mathrm{Spec}\,(R)$ is a set of n points with the discrete topology.

Irreducible Representation

Proposition

Let I be an ideal of the Noetherian ring R and let

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_n,$$

be a primary representation. Then

$$V(I) = V(P'_1) \cup V(P'_2) \cup \cdots \cup V(P'_m),$$

where the P'_j are the minimal primes amongst the $\sqrt{Q_i}$, is the unique irreducible representation of $V(I)$.

Morphisms

Proposition

If R is a commutative ring, $\mathrm{Spec}\,(R)$ *is quasi-compact. (Not necessarilly Hausdorff.)*

Proof.

Let $\{D(I_\alpha)\}$ be an open cover of X

$$X = \bigcup_\alpha D(I_\alpha) = D(\sum_\alpha I_\alpha) = D(1).$$

This means that there is a finite sum

$$\sum_1^n I_{\alpha_i} = R, \quad \text{and therefore } X = \bigcup_{i=1}^n D(I_{\alpha_i}).$$

□

Proposition

If $\varphi : R \to S$ is a homomorphism of commutative rings $(\varphi(1_R) = 1_S)$, then the mapping

$$\Phi : \mathrm{Spec}\,(S) \to \mathrm{Spec}\,(R),$$

given by $\Phi(Q) = \varphi^{-1}(Q)$, is continuous.

Proof.

If $D(I)$ is an open set of $\mathrm{Spec}\,(R)$, $\varphi^{-1}(D(I)) = D(IS)$. □

Outline

1. General Orientation
2. Syllabus
3. Introduction
4. Chain Conditions
5. Prime Ideals
6. Primary Decomposition
7. Noetherian Rings
8. Graded Noetherian Rings
9. Commutative Artinian Rings
10. Modules of Fractions
11. **Integral Extensions**
12. Dedekind Domains
13. Valuation Rings
14. Homework

Integral Extensions

Let $R \hookrightarrow S$ be commutative rings.

Definition

$s \in S$ is integral over R if there is an equation

$$s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0, \quad a_i \in R.$$

Proposition

$s \in S$ is integral over R if and only if the subring $R[s]$ of S generated by s is a finitely generated R-module.

Would like to prove [as done first by Weierstrass] that if $s_1$and s_2 in S are integral over R then

- $s_1 + s_2$ is integral over R;
- $s_1 s_2$ is integral over R.

The key to their proof is the fact that both $s_1 + s_2$ and $s_1 s_2$ are elements of the subring $R[s_1, s_2]$ which is finitely generated as an R-module

$$R[s_1, s_2] = \sum_{i,j} R s_1^i s_2^j,$$

where i and j are bounded by the degrees of the equations satisfied by s_1 and s_2.

Integrality Criterion

Proposition

Let M be a finitely generated R-module and $S = R[u]$ a ring such that $uM \subset M$. If M is a faithful S-module then u is integral over R.

Proof. Let $x_1, \ldots, x_n$ be a set of R-generators of M. we have a set of relations with $a_{ij} \in R$

$$\begin{aligned} ux_1 &= a_{11}x_1 + \cdots + a_{1n}x_n \\ &\vdots \\ ux_n &= a_{n1}x_1 + \cdots + a_{nn}x_n \end{aligned}$$

Cayley-Hamilton

That is

$$\begin{array}{rcl} 0 & = & (a_{11}-u)x_1+\cdots+a_{1n}x_n \\ & \vdots & \\ 0 & = & a_{n1}x_1+\cdots+(a_{nn}-u)x_n \end{array}$$

Which we rewrite in matrix form

$$\begin{bmatrix} a_{11}-u & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn}-u \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} = \mathbf{A}[\mathbf{x}] = O.$$

Thus

$$(\mathrm{adj}\ \mathbf{A})\mathbf{A}[\mathbf{x}] = \det \mathbf{A} \cdot [\mathbf{x}] = O.$$

This means that $\det \mathbf{A}$ annihilates each generator x_i of M and therefore $\det \mathbf{A} = 0$.

But

$$\det \mathbf{A} = \pm u^n + \text{lower powers of } u \text{ with coefficients in } R$$

This shows that u is integral over R.

Principle of Specialization

Why are we allowed to write $\mathrm{adj}\ \mathbf{A} \cdot \mathbf{A} = \det \mathbf{A} \cdot \mathbf{I}$ when the entries of **A** lie in a commutative ring?

If $T = \mathbb{Z}[x_{ij},\ 1 \leq i, j \leq n]$ is a ring of polynomials in the indeterminates x_{ij}, and use them as the entries of a matrix **B**, certainly the formula $\mathrm{adj}\ \ \mathbf{B} \cdot \mathbf{B} = \det \mathbf{B} \cdot \mathbf{I}$ makes sense since T lies in a field.

Now define a ring homomorphism $\phi : T \to R$, with $\phi(x_{ij})$ the corresponding entry in **A**, to get the desired equality.

In our application, $M = R[s_1, s_2]$ and u is either $s_1 + s_2$ or $s_1 s_2$, and certainly M is faithful since $1 \in M$.

Corollary

If $R \hookrightarrow S$ are commutative rings, and $s_1, s_2, \dots, s_n$ are integral over R, then any element of $R[s_1, \dots, s_n]$ is integral over R. Moreover, if T is the set of elements of S integral over R, T is a subring. It is called the integral closure of R in S.

Definition

If $T = S$, S is called an integral extension of R.

Transitivity

Proposition

If $R \hookrightarrow S_1 \hookrightarrow S_2$ are commutative rings with S_1 integral over R and S_2 integral over S_1, then S_2 is integral over R.

Proof. Let $u \in S_2$ be integral over S_1

$$u^n + s_{n-1}u^{n-1} + \cdots + s_1 u + s_0 = 0, \quad s_i \in S_1.$$

It suffices to observe that

$$M = R[u, s_{n-1}, \ldots, s_1, s_0]$$

is a finitely generated R-module.

Surjections

Another use of the Cayley-Hamilton theorem is the following property of surjective epimorphims of modules:

Theorem

Let R be a commutative ring and M a finitely generated R. If $\varphi : M \to M$ is a surjective R-module homomorphism, then φ is an isomorphism.

Proof. We first turn M into a module over the ring of polynomials $S = R[t]$ by setting $t \cdot m = \varphi(m)$ for $m \in M$.

The assumption means that $tM = M$. Using the proof of Cayley-Hamilton, we have

$$\begin{bmatrix} ta_{11}-1 & \cdots & ta_{1n} \\ \vdots & \ddots & \vdots \\ ta_{n1} & \cdots & ta_{nn}-1 \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} = \mathbf{A}[\mathbf{x}] = O.$$

Which implies that $\det \mathbf{A}$ annihilates M. Since

$$\det \mathbf{A} = \pm 1 + t\mathbf{f}(t),$$

it is clear that $t \cdot m \neq 0$ for $m \neq 0$, that is φ is one-to-one.

Jacobson Radical

Definition

Let R be a commutative ring. Its Jacobson radical is the intersection $\bigcap Q$ of all maximal (proper) ideals.

Example: If R is a local ring, its Jacobson radical is its unique maximal ideal $\mathfrak{m}$.

If $R = \mathbb{Z}$, or $R = k[t]$, polynomial ring over the field k, then (0) is the Jacobson radical: from the infinity of prime elements.

Proposition

The Jacobson radical J of R is the set

$$J' = \{a \in R : 1 + ra \quad \text{is invertible for all } r \in R\}.$$

Proof. If $a \in J$, then $1 + ra$ cannot be contained in any proper maximal ideal, that is it must be invertible.
Conversely, if $a \in J'$, suppose a does not belong to the maximal ideal Q. Therefore

$$(a, Q) = R$$

which means there is an equation $ra + q = 1$, $q \in Q$, and q would be invertible.

Nakayama Lemma

Theorem (Nakayama Lemma)

Let M be a finitely generated R module and J its Jacobson radical. If

$$M = JM,$$

then $M = 0$.

Proof. If M is cyclic, this is clear: $M = (x)$ implies $x = ux$ for some $u \in J$, so that $(1 - u)x = 0$, which implies $x = 0$ since $1 - u$ is invertible.

We are going to argue by induction on the minimal number of generators of M. Suppose $M = (x_1, \ldots, x_n)$. By assumption $x_1 \in JM$, that is we can write

$$x_1 = u_1 x_1 + u_2 x_2 + \cdots + u_n x_n, \quad u_i \in J.$$

Which we rewrite as

$$(1 - u_1)x_1 = u_2x_2 + \cdots + u_nx_n$$

This shows that $x_1 \in J(x_2, \ldots, x_n)$, and therefore $M = (x_2, \ldots, x_n)$.

Corollary

Let M be a finitely generated R module and N a submodule. If $M = N + JM$ then $M = N$.

Proof.

Apply the Nakayama Lemma to the quotient module M/N

$$M/N = N + JM/N = J(M/N).$$

□

.

Corollary

Let R be a commutative ring and M a finitely generated R-module. If for some ideal I, $IM = M$, then $(1 + a)M = 0$ for some $a \in I$.

Proof.

If $M = (x_1, \dots, x_n)$, from the proof of Cayley-Hamilton, there are $a_{ij} \in I$

$$\begin{bmatrix} a_{11} - 1 & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} - 1 \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} = \mathbf{A}[\mathbf{x}] = O.$$

Which implies that $\det \mathbf{A}$ annihilates M. Since $\det \mathbf{A} = \pm 1 + a, \quad a \in I$, done □

Corollary

Let R be a commutative ring and I a finitely generated ideal. Then $I = I^2$ if and only if I is generated by an idempotent, that is $I = Re$, $e^2 = e$.

Proof.

If $(1 + a)I = 0$, $I \subset (a)$ and $a^2 = a$. □

Integral Morphisms

Let $\varphi : R \to S$ an injective homomorphism of commutative rings.

Theorem (Lying-Over Theorem)

If S is integral over R then for each $\mathfrak{p} \in \operatorname{Spec}(R)$ there is $P \in \operatorname{Spec}(S)$ such that $\mathfrak{p} = P \cap R$, that is the morphism

$$\operatorname{Spec}(S) \to \operatorname{Spec}(R)$$

is surjective.

Proposition

If S is integral over R and T is a multiplicative set of R, then $T^{-1}S$ is integral over $T^{-1}R$.

Proof.

Let $s/t \in T^{-1}S$. s satisfies an equation

$$s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0, \quad a_i \in R.$$

Then

$$(s/t)^n + a_{n-1}/t(s/t)^{n-1} + \cdots + a_1/t^{n-1}s/t + a_0/t^n = 0,$$

$a_i/t^{n-i} \in T^{-1}R$.

□

Proof of Lying-Over

Suppose $\mathfrak{p} \in \operatorname{Spec}(R)$. Consider the integral extension $R_{\mathfrak{p}} \hookrightarrow S_{\mathfrak{p}}$.

The maximal ideal of $R_{\mathfrak{p}}$ is $\mathfrak{m} = \mathfrak{p} R_{\mathfrak{p}}$.

Claim: $\mathfrak{m} S_{\mathfrak{p}} \neq S_{\mathfrak{p}}$.

Otherwise we would have

$$\begin{aligned} 1 &\in \mathfrak{m} S \mathfrak{p} \\ 1 &= \sum_{i=1}^{n} a_i s_i / t_i, \quad a_i \in \mathfrak{m},\ s_i \in S,\ t_i \in R \setminus \mathfrak{p} \end{aligned}$$

1. Set $S' = R_{\mathfrak{p}}[s_1, \ldots, s_n]$.
2. S' is a finitely generated $R_{\mathfrak{p}}$-module with $S' = \mathfrak{m}S'$. By Nakayama Lemma, $S' = 0$.
3. Since $\mathfrak{m}S_{\mathfrak{p}} \neq S_{\mathfrak{p}}$, it is contained in a prime ideal P' of $S_{\mathfrak{p}}$. In particular, $P' \cap R_{\mathfrak{p}} = \mathfrak{m}$.
4. Since $P' = P_{\mathfrak{p}}$ for some $P \in \mathrm{Spec}\,(S)$, it is clear that $P \cap R = \mathfrak{p}$, as desired.

Going-Up Theorem

Theorem

Let $R \hookrightarrow S$ be an integral extension of commutative rings. Let $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ be prime ideals of R and suppose P_1 is a prime ideal of S such that $P_1 \cap R = \mathfrak{p}_1$. Then there is a prime ideal $P_1 \subsetneq P_2$ of S such that $P_2 \cap R = \mathfrak{p}_2$.

Proof. Consider the diagram

$$\begin{tikzcd}
R \arrow[r, hook] \arrow[d] & S \arrow[d] \\
R/\mathfrak{p}_1 \arrow[r, hook] & S/P_1
\end{tikzcd}$$

Now apply the Lying-Over theorem to the integral extension

$$R/\mathfrak{p}_1 \hookrightarrow S/P_1.$$

Going-Down Theorem

? Is there

Theorem (?Going-Down Theorem)

Let $R \hookrightarrow S$ be an integral extension of commutative rings. Let $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ be prime ideals of R and suppose P_2 is a prime ideal of S such that $P_2 \cap R = \mathfrak{p}_2$. Then there is a prime ideal $P_1 \subsetneq P_2$ of S such that $P_1 \cap R = \mathfrak{p}_1$.

Yes, but needs additional assumptions. Proof uses some basic Galois theory.

Outline

1. General Orientation
2. Syllabus
3. Introduction
4. Chain Conditions
5. Prime Ideals
6. Primary Decomposition
7. Noetherian Rings
8. Graded Noetherian Rings
9. Commutative Artinian Rings
10. Modules of Fractions
11. Integral Extensions
12. **Dedekind Domains**
13. Valuation Rings
14. Homework

Dedekind Domains

These are important rings. The interest springs from their sources:

- Number Theory: Rings of algebraic numbers: If **L** is a finite extension of $\mathbb{Q}$, R is the ring of elements of **L** integral over $\mathbb{Z}$.
- Algebraic Geometry: (Case of plane curve) $R = k[x, y]/(\mathbf{f}(x, y))$, or its integral closure.

Dedekind Domains

The formal definition is:

Definition

The integral domain $\mathfrak{D}$ is a Dedekind domain if every ideal is invertible.

- $\mathfrak{D}$ is a nice notation for D.D.'s, but we shall use plain R...
- The inverse of a fractionary ideal L is denoted L^{-1} (it is unique).
- Of course every fractionary ideal will be invertible as well.
- If R is a Dedekind domain, it is Noetherian.
- Besides PID's, what are they like?

Properties of D.D.'s

Theorem

If R is a Dedekind domain then every nonzero prime ideal is maximal.

Proof.

We will argue by contradiction. Let $P \subsetneq Q$ be distinct prime ideals. We are going to form the ring of fractions $S = R_Q$ (Recall ...). S is a local ring and P_Q and Q_Q are distinct prime ideals. They are both invertible. Thus

$$P_Q \quad = \quad Sa \subsetneq Sb = Q_Q$$

with $a = cb$, and therefore $c \in P_Q$ since $b \notin P_Q$. Thus

$$c = ra = b^{-1}a,$$

Factorization

Theorem

Let R be a Dedekind domain. Then any nonzero ideal I has a unique factorization

$$I = P_1^{e_1} \cdots P_n^{e_n},$$

where the P_i are distinct prime idealas.

Proof. Since R is Noetherian, I has a primary decomposition

$$I = Q_1 \cap \cdots \cap Q_n,$$

where the $P_i = \sqrt{Q_i}$ are distinct maximal ideals.

We want to argue that the intersection is actually a product.

Definition

Two ideals J and L are co-maximal if $J + L = R$.

Lemma

If J and L are co-maximal ideals, then $JL = J \cap L$.

Proof.

It is clear that $JL \subset J \cap L$. For the converse, let $x \in J \cap L$. Since $J + L = R$, there are $a \in J$ and $b \in L$ such that

$$\begin{array}{rcll} 1 & = & a+b, & \text{hence} \\ x & = & xa+xb, & \text{with} \quad xa, xb \in J \cap L \end{array}$$

□

Now we apply this to $I = Q_1 \cap L$, $L = Q_2 \cap \cdots \cap Q_n$. To see that Q_1 and L are co-maximal, deny. Then $Q_1 + L \subseteq M$ for some maximal ideal M. This ideal would contain $\sqrt{Q_1}$ and $Q_2 \cdots Q_n$. Thus M would contain two other maximal ideals, a contradiction.

Primary ideals

Proposition

Let R be a Dedekind domain. If Q is a P-primary ideal, then $Q = P^e$, for some $e \geq 1$.

Proof.

Since the radical of Q is P, some power of P is contained in Q, say $P^e \subseteq Q$, with e as small as possible. If the containement is proper, we have

$$P^e \cdot Q^{-1} \subsetneq Q \cdot Q^{-1} = R.$$

Therefore we must have

$$\begin{array}{rcll} P^e \cdot Q^{-1} & \subseteq & P & \text{and therefore} \\ P^{e-1} & \subseteq & Q & \text{which is a contradiction.} \end{array}$$

Corollary

If R is a Dedekind domain, the nonzero fractionary ideals form a multiplicative group $\mathbf{G}$*, with the nonzero principal fractionary forming a subgroup* $\mathbf{P}$*. The quotient* $\mathbf{G}/\mathbf{P}$ *is called the class group* $\mathbf{C}(R)$ *of R. R is a PID if and only if* $\mathbf{C}(R)$ *is trivial.*

Remarks

1. Recall that if $R \subset S$ are rings, an element $u \in S$ is integral over R if it satisfies a monic equation with coefficients in R, $u^n + r_1 u^{n-1} + \cdots + r_n = 0$, $r_i \in R$.
2. If every element of S that is integral over R already lies in R, R is said to be **integrally closed** in S.
3. If R is a domain of field of fractions $\mathbf{K}$ and $\mathbf{L}$ is a finite extension of $\mathbf{K}$, for any $u \in \mathbf{L}$ there is an equation $u^n + r_1 u^{n-1} + \cdots + r_n = 0$, $r_i \in \mathbf{K}$. Let $0 \neq d \in R$ such that $dr_i \in R$ (d is a **common denominator** of the r_i.) Then $d^n u^n + dr_1 d^{n-1} u^{n-1} + \cdots + d^n r_n = 0$, $r_i \in \mathbf{K}$, showing that du is integral over R.

Characterization of D.D.'s

Theorem

Let R be an integral domain of field of fractions $\mathbf{K}$. The following are equivalent:

1. *R is a Dedekind domain.*
2. *R is a Noetherian ring in which every nonzero prime ideal is maximal and R is integrally closed in $\mathbf{K}$.*
3. *R is Noetherian and for each prime ideal P the localization R_P is a PID.*

We will check the equivalences:

$$(1) \Leftrightarrow (2) \Leftrightarrow (3)$$

Some remarks on localization

- If R is an integral domain then

$$R = \bigcap_P R_P, \quad \text{all maximal ideals } P$$

Indeed, if x is contained in each R_P,

$$x = a/b, \quad b \notin P,$$

the set (an ideal) of all elements d (denominators) such that $dx \in R$ is not contained in any maximal ideal of R, so must be R.

- If each R_P is integrally closed, then their intersection will also be such: If $z \in \mathbf{K}$ is integral over R, it is also integral over the larger R_P. Thus $z \in R_P$.

Characterization of a PID with a unique maximal ideal

Proposition

Let R be a Noetherian domain with a unique nonzero prime ideal $\mathfrak{m}$. R is a PID if and only if R is integrally closed.

Proof. ETS that if R is integrally closed then $\mathfrak{m}$ is invertible.

- Let $0 \neq x \in \mathfrak{m}$. Then the radical $\sqrt{(x)}$ of (x) is $\mathfrak{m}$.
- Let n be the smallest integer such that $\mathfrak{m}^n \subset (x)$. Consider the product
$$(1/x)\mathfrak{m}^{n-1}\mathfrak{m} \subset R$$
- If $(1/x)\mathfrak{m}^{n-1}\mathfrak{m} = R$, $\mathfrak{m}$ is invertible.

- If not, $(1/x)\mathfrak{m}^{n-1}\mathfrak{m} \subset \mathfrak{m}$.
- Recall the Cayley-Hamilton for modules: If E is a faithful, finitely generated R-module and z is an element of a larger ring such that $z \cdot M \subset M$, then z is integral over R.
- This implies that $(1/x)\mathfrak{m}^{n-1}$ is integral over R, therefore is contained in R, since it is integrally closed, that is $\mathfrak{m}^{n-1} \subset (x)$, which contradicts the choice of n.

Taylor expansion

It is useful to keep in mind the formula for the Taylor expansion of a polynomial $\mathbf{f}(x, y)$ around the point (a, b)

Use the notation

$$b_{mn} = \frac{\partial^{m+n}\mathbf{f}}{\partial^m x \partial^n y}(a, b)$$

$$\begin{aligned} \mathbf{f}(x, y) &= \mathbf{f}(a, b) + b_{10}(x - a) + b_{01}(y - b) \\ &+ 1/2(b_{20}(x - a)^2 + 2b_{11}(x - a)(y - b) + b_{02}(y - b)^2) \\ &+ \text{higher powers} \end{aligned}$$

Elliptic curve

Let us first consider the following example,

$$R \quad = \quad \mathbf{C}[x, y]/(\mathbf{f}(x, y)), \quad \mathbf{f}(x, y) = y^2 - x(x-1)(x-2).$$

By the Nullstellensatz its maximal ideals are of the form $M = (x - \alpha, y - \beta)$, where $\beta^2 - \alpha(\alpha - 1)(\alpha - 2) = 0$. We claim that R_M is a PID. Write the polynomial $\mathbf{f}(x, y)$ as a combination of $x - \alpha$ and $y - \beta$

$$\begin{aligned} \mathbf{f}(x, y) &= A(x, y)(x - \alpha) + B(x, y)(y - \beta) \\ \frac{\partial \mathbf{f}}{\partial x}(\alpha, \beta) &= A(\alpha, \beta) \\ \frac{\partial \mathbf{f}}{\partial y}(\alpha, \beta) &= B(\alpha, \beta) \end{aligned}$$

Elliptic curve cont'd

If one of the partial derivatives is not zero at (α, β), in the ring R $\overline{A(x, y)}$ or $\overline{B(x, y)}$ are not in M, therefore one or the other is a unit in R_M so that the maximal ideal MR_M is generated by $\overline{y - \beta}$ or $\overline{x - \alpha}$:

$$\overline{\mathbf{f}(x, y)} = 0 = \overline{A(x, y)(x - \alpha)} + \overline{B(x, y)(y - \beta)}$$

It is easy to check that the conditions always holds since the partial derivatives are $2y$ and $(x - 1)(x - x) + x(x - 2) + x(x - 1)$.

Volunteer please

Need someone to sketch the graph of the curve

$$y^2 = x(x-1)(x-2)$$

Geometric DD's

Let $\mathbf{f}(x, y) \in R = \mathbb{C}[x, y]$ be an irreducible polynomial. The algebraic variety

$$V(\mathbf{f}) = \{(a, b) \in \mathbb{C} : \mathbf{f}(a, b) = 0\}$$

is called a (plane) curve.

- We know that every maximal ideal of $\mathbb{C}[x, y]$ is of the form $M = (x - a, y - b)$, for $a, b \in \mathbb{C}$
- Thus if $\mathbf{f} \in M$ is a combination of the polynomials, $x - a$ and $y - b$, $\mathbf{f} = \mathbf{g}(x - a) + \mathbf{h}(y - b)$, so $\mathbf{f}(a, b) = 0$
- Conversely, if $\mathbf{f}(a, b) = 0$, writing the Taylor expansion of $\mathbf{f}(x, y)$ at $a, b)$ we get

  $$\mathbf{f}(x, y) = \sum_{m+n \geq 0} a_{mn}(x - a)^m (y - b)^n, \quad a_{mn} \in \mathbb{C}$$

  showing $\mathbf{f} \in (x - a, y - b)$.
- So points in $\mathbf{f} = 0$ and maximal ideals of $R/(\mathbf{f})$ correspond.

Let us determine when $R/(\mathbf{f})$ is a Dedekind domain. For that we define the ideal (Jacobian)

$$J(\mathbf{f}) = (\mathbf{f}, \frac{\partial \mathbf{f}}{\partial x}, \frac{\partial \mathbf{f}}{\partial y})$$

Theorem

$R/(\mathbf{f})$ is a Dedekind domain iff $J(\mathbf{f}) = (1)$.

Note what this means, if (a, b) is a point of the curve, $\mathbf{f}(a, b) = 0$, that is $\mathbf{f} \in M = (x - a, y - b)$, but because the ideal $J(\mathbf{f}) = (1)$, either $\frac{\partial \mathbf{f}}{\partial x}(a, b) \neq 0$ or $\frac{\partial \mathbf{f}}{\partial y}(a, b) \neq 0$. This means $\mathbf{f}(x, y) = 0$ has a tangent at (a, b).

Proof

- We are going to prove that for every maximal ideal M of $R = \mathbb{C}[x, y]/(\mathbf{f})$, R_M is a PID. For that, by a previous result, it will be enough to prove that the maximal ideal MR_M is principal.
- Since M is generated by the cosets of $x - a$ and $y - b$ for (a, b) such that $\mathbf{f}(a, b) = 0$, it will be enough to show that $x - a$ is a multiple of $y - b$ in R_M, or vice-versa.
- We are going to make use of the fact that one of the partial derivatives $\frac{\partial \mathbf{f}}{\partial x}(a, b)$ or $\frac{\partial \mathbf{f}}{\partial y}(a, b)$ is nonzero.

Proof cont'd

- Suppose $\frac{\partial \mathbf{f}}{\partial x}(a,b) \neq 0$. Let us write the Taylor expansion of $\mathbf{f}(x,y)$ at (a,b) (using that $\mathbf{f}(a,b) = 0$.
- We collect first the terms in which $x - a$ appears alone

$$(x-a)\,\underbrace{[\frac{\partial \mathbf{f}}{\partial x}(a,b) + 1/2a_{2,0}(x-a) + \text{higher powers of } (x-a)]}$$

$$+(y-b)[\text{polynomial expression in } x-a \text{ and } y-b]$$

- Since this is the coset of $\mathbf{f}(x, y)$, it is zero.
- Note that the coefficient of $x - a$

  $$\frac{\partial \mathbf{f}}{\partial x}(a, b) + 1/2a_{2,0}(x - a) + \text{higher powers of } (x - a)$$

  is a sum of an invertible element (the derivative) plus an element of MR_M, so it is an invertible element of R_M.
- This shows that $x - a$ is a multiple of $y - b$, and therefore MR_M is a principal ideal.

Creation of new D.D.'s

Theorem

Let R be a Dedekind domain of field of fractions $\mathbf{K}$ *and let* $\mathbf{L}$ *a finite extension of* $\mathbf{K}$*. The integral closure* $\mathbf{A}$ *of R in* $\mathbf{L}$ *is a Dedekind domain.*

The main burden is to show that $\mathbf{A}$ is a Noetherian ring. We will give a proof in case $\mathbf{L}$ is a separable extension, when one has that $\mathbf{A}$ is a finitely generated R-module. To get that we replace $\mathbf{L}$ by $\mathbf{M}$ its split closure over $\mathbf{K}$, and show that the integral closure $\mathbf{B}$ of R in $\mathbf{M}$ is a finitely generated R-module. Note that $\mathbf{A}$ is an R-submodule of $\mathbf{B}$.

Exercise

- Let $\mathbf{D}$ be a Dedekind domain of field of fractions $\mathbf{K}$. Prove that any ring $\mathbf{R} \subset \mathbf{S} \subset \mathbf{K}$ is a Dedekind domain.

Noetherianess of the integral closure

Theorem

Let R be an integrally closed Noetherian domain of field of fractions $\mathbf{K}$ *and let* $\mathbf{L}$ *a finite Galois extension of* $\mathbf{K}$*. The integral closure* $\mathbf{A}$ *of R in* $\mathbf{L}$ *is a Noetherian domain.*

Proof

- Let $\mathbf{G}$ be the Galois group of $\mathbf{L}$ over $\mathbf{K}$. The **trace** is the function $u \in \mathbf{L} \to \mathbf{T}(u) = \sum_{\sigma \in \mathbf{G}} \sigma(u)$. Since the extension is Galois and $\mathbf{T}(u)$ is fixed by $\mathbf{G}$, $\mathbf{T}(u) \in \mathbf{K}$.
- If u is integral over R, there is an equation $u^m + c_1 u^{m-1} + \cdots + c_m = 0$, with $c_i \in R$. Thus for any $\sigma \in \mathbf{G}$, $\sigma(u)$ is also integral over R and therefore $\mathbf{T}(u)$ is in $\mathbf{K}$ and integral over R, thus $\mathbf{T}(u) \in R$ since R is integrally closed.
- Define the quadratic form $\mathbf{S}(u, v) = \mathbf{T}(uv)$ on $\mathbf{L}$. $\mathbf{S}$ is nondegenerate: If $u \neq 0$ we cannot have $\mathbf{T}(uv) = 0$ for all v, by the linear independence of automorphisms.

Proof cont'd

- Let $x_1, \ldots, x_n$ be a basis of **L** over **K**. By multiplying the x_i by nonzero elements of R we may assume that $x_i \in \mathbf{A}$.
- Let $y_1, \ldots, y_n$ be a basis of **L** dual to the x_i, that is $\mathbf{T}(x_i y_j) = \delta_{ij}$.
- For $u \in \mathbf{A}$, write $u = r_1 y_1 + \cdots + r_n y_n$. Then $\mathbf{T}(ux_i) = r_i \mathbf{T}(x_i y_i) = r_i$. Since $\mathbf{T}(ux_i) \in R$, this shows that **A** is contained in the finitely generated R-module $Ry_1 + \cdots + Ry_n$, and thus **A** is Noetherian as an R-module and hence a Noetherian ring as well.

Examples

- The most famous example obtained in this fashion is $\mathbb{Z}[i]$: Gaussian integers. It is the integral closure of $\mathbb{Z}$ in $\mathbf{Q}(i)$.
- The more general quadratic extension $\mathbf{Q}(\sqrt{m})$, m a squarefree integer is easy to examine. $z = a + b\sqrt{m}$, $a, b \in \mathbf{Q}$, is integral over $\mathbb{Z}$ iff $2a$ and $a^2 - b^2m$ are integers. Thus a is an integer (and b is integer) or a is $1/2$ integer and b also a $1/2$ integer, depending on the residue class of m mod 4.
- If $m = 3$, $\mathbf{A} = \mathbb{Z}[\sqrt{3}]$; if $m = 5$, $\mathbf{A} = \mathbb{Z}[1/2 + 1/2\sqrt{5}]$; if $m = -5$, $\mathbf{A} = \mathbb{Z}[\sqrt{-5}]$.

Infinitely generated modules

Theorem

Let R be a DD. Then any submodule of a free module is a direct sum of ideals.

Done already. Recall the idea:
Proof. Let F be a free module with basis $\{e_i, i \in I\}$, and suppose the index set I is well-ordered. For each $i \in I$ set

$$F_i = \bigoplus_{j<i} Re_j,$$

with $F_0 = 0$ and $F_{i+1} = \bigoplus_{j \leq i} Re_j$.

For a submodule M of F each $x \in M \cap F_{i+1}$ has a unique expression $x = y + re_i$, where $y \in F_i$ and $r \in R$. If $\phi_i : M \cap F_{i+1} \to R$ is defined by $\phi_i(x) = r$, there is a SES

$$0 \to M \cap F_i \longrightarrow M \cap F_{i+1} \longrightarrow I_i \to 0,$$

where $I_i = \text{image } \phi_i$.

To make the point clear, suppose

$$F = Re_1 \oplus \cdots \oplus Re_{n-1} \oplus Re_n = F' \oplus Re_n$$

gives $0 \to M \cap F' \longrightarrow M \longrightarrow I_n e_n \to 0$, and therefore $M \simeq I_n e_n \oplus M \cap F'$. Now use induction.
Same in general case: Since I_i is projective (as R is a D.D.), the sequence splits: $M \cap F_{i+1} = (M \cap F_i) \oplus C_i$, $C_i \simeq I_i$.
We claim $M = \bigoplus_i C_i$. Same proof from now on

Torsion and Torsionfree Modules

- Let R be an integral domain and M an R-module. The torsion submodule of M is the set
$$T(M) = \{x \in M : rx = 0, \quad 0 \neq r \in R\}$$
- $T(M)$ is a submodule of M. If $T(M) = M$, M is said to be a **torsion module.** If $T(M) = 0$, M is called **torsionfree.**
- $T(M/T(M)) = 0$, that is $M/T(M)$ is torsionfree.
- A set $\{x_1, \ldots, x_n\} \subset M$ is linearly independent if $\sum_i r_i x_i = 0$, $r_i \in R$, implies $r_i = 0$.
- The largest cardinality of the sets of linearly independent elements of M is the **torsionfree rank** of M.
- A nonzero ideal I of R has torsionfree rank 1: If $0 \neq x, y \in I$, $xy - yx = 0$ is a relation.

Proposition

If M is a finitely generated torsionfree module of rank n, then there is an embedding

$$M \quad \hookrightarrow \quad R^n.$$

Proof.

Let $M = (y_1, \ldots, y_m)$ and let $\{x_1, \ldots, x_n\}$ be a linearly independent set of elements of M.

For each y_j, we have a relation

$$c_j y_j + \sum_i a_{ij} x_i = 0, \quad c_j \neq 0$$

Let $c = \prod_j c_j$ and consider the elements $z_i = \frac{x_i}{c}$ of the module of fractions $c^{-1}M$. The z_i are linearly independent over R and each generator of M is contained in the free module

Structure of finitely generated modules

Theorem

Let R be a Dedekind domain and M a finitely generated R-module. Then

$$M \simeq T \oplus P,$$

where T is the torsion submodule of M and $P = M/T$ is a projective R-module. Moreover:

1. $P \simeq \underbrace{R \oplus \cdots \oplus R}_{\text{free}} \oplus I$, *where I is a unique ideal up to isomorphism.*
2. $T \simeq R/I_1 \oplus \cdots \oplus R/I_m$, $I_1 \subseteq \ldots \subseteq I_m$, *where the I_i are uniquely defined.*

Proof

- In the exact sequence $0 \to T \longrightarrow M \longrightarrow M/T \to 0$, $P = M/T$ is torsionfree, so embeds into a finitely generated free R-module (**why?**).
- P is projective, so the sequence splits: $M \simeq T \oplus P$.
- P we know is isomorphic to a direct of ideals. One improves this to a direct sum of a free and **one** ideal. This ideal is unique up to isomorphism. We will describe it later: it is called the **determinant** of the module M.
- T is actually a module over a PID S derived from R.

Outline

1. General Orientation
2. Syllabus
3. Introduction
4. Chain Conditions
5. Prime Ideals
6. Primary Decomposition
7. Noetherian Rings
8. Graded Noetherian Rings
9. Commutative Artinian Rings
10. Modules of Fractions
11. Integral Extensions
12. Dedekind Domains
13. **Valuation Rings**
14. Homework

Valuation Rings

Definition

An integral domain **A** of field of fractions **K** is a valuation ring of **K** if for $0 \neq x \in \mathbf{K}$, $x \in \mathbf{A}$ or $x^{-1} \in \mathbf{A}$.

Examples

- **A**: the set of all rational numbers a/b, b odd.
- If k is a field and $\mathbf{A} = k[[x]]$, the ring of formal power series.

Properties of Valuation Rings

Proposition

Let $\mathbf{A}$ *be a valuation ring of field of fractions* $\mathbf{K}$*. Then*

1. $\mathbf{A}$ *is a local ring;*
2. *Any ring* $\mathbf{A} \subset \mathbf{A}' \subset \mathbf{K}$ *is a valuation ring;*
3. $\mathbf{A}$ *is integrally closed;*
4. *If* I *is a finitely generated ideal of* $\mathbf{A}$ *then* I *is principal.*

Proof. (1) Let $\mathfrak{m}$ be the set of non-units of $\mathbf{A}$. We must show that $\mathfrak{m}$ is an ideal. Clearly if $\mathbf{x} \in \mathfrak{m}$ and $r \in \mathbf{A}$, $rx \in \mathfrak{m}$.

Let $x, y \in \mathfrak{m}$; must show $x + y \in \mathfrak{m}$. We may assume $x, y \neq 0$. If $x/y = r \in \mathbf{A}$,

$$x + y = y(r + 1) \in \mathfrak{m}.$$

If $y/x \in \mathbf{A}$ argue similarly.

(2) Obvious.

(3) Let $x \in \mathbf{K}$ be integral over $\mathbf{A}$:

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0, \quad b_i \in \mathbf{A}.$$

If $x \in \mathbf{A}$, NTS.
If $x^{-1} \in \mathbf{A}$,

$$x = -(b_1 + b_2 x^{-1} + \cdots + b_n (x^{-1})^{n-1}) \in \mathbf{A}.$$

(4) Enough to show that $I = (x, y)$ is either (x) or (y): seen above.

Construction of Valuation Rings

Theorem

Let $\mathbf{R}$ *be an integral domain of field of fractions* $\mathbf{K}$*. If* I *is a proper ideal of* $\mathbf{R}$ *there is a valuation ring* $\mathbf{A}$ *of* $\mathbf{K}$*,* $\mathbf{R} \subset \mathbf{A}$*, such that* $I\mathbf{A} \neq \mathbf{A}$*.*

Proof. We may assume that I is a maximal ideal $\mathfrak{m}$. We may also replace $\mathbf{R}$ by $\mathbf{R}_{\mathfrak{m}}$, which is a local ring. We still denote by $\mathfrak{m}$ its maximal ideal.

We are going to produce $\mathbf{A}$ using Zorn's Lemma.

- Consider the set $\mathcal{A}$ of local rings of $\mathbf{K}$ of the form $(\mathbf{R}', \mathfrak{m}')$, where $\mathbf{R} \subset \mathbf{R}'$, $\mathfrak{m} \subset \mathfrak{m}'$. Order these rings by

$$(\mathbf{R}', \mathfrak{m}') \leq (\mathbf{R}'', \mathfrak{m}'') \Leftrightarrow \mathbf{R}' \subset \mathbf{R}'', \mathfrak{m}' \subset \mathfrak{m}''$$

- It is clear that the union of a chain $(\mathbf{R}_n, \mathfrak{m}_n)$ of such rings is a local ring of the same kind.

- Let $(\mathbf{A}, M)$ be a maximal element. We claim that **A** s a valuation ring of **K.**

- Let $0 \neq x \in \mathbf{K}$ and suppose neither x nor x^{-1} lies in **A.** Consider the two subrings $\mathbf{A}_1 = \mathbf{A}[x]$ and $\mathbf{A}_2 = \mathbf{A}[x^{-1}]$ of **K**.

- If $M\mathbf{A}_1 \neq \mathbf{A}_1$ (or similarly $M\mathbf{A}_2 \neq \mathbf{A}_2$), we could localize $\mathbf{A}_1$ at a prime ideal containing M and obtain an extension in $\mathcal{A}$ properly larger than **A.**

- The equalities $\mathbf{A}_1 = M\mathbf{A}_1$ and $\mathbf{A}_2 = M\mathbf{A}_2$ means that there are equations

$$\begin{aligned} 1 &= \sum_{i=0}^{m} a_i x^i \\ 1 &= \sum_{j=0}^{n} b_j x^{-j} \end{aligned}$$

  where $a_i, b_j \in M$.

- In each of these equations, say, we could rewrite as $1 - a_0 = \sum_{i=1}^{m} a_i x^i$ and as $1 - a_0$ is invertible we could assume the summations run from 1 on.

- Thus the second equation, $1 = \sum_{j=1}^{n} b_j x^{-j}$ would give rise to the equality

$$x^m = \sum_{j=1}^{m} b_j x^{m-j}$$

  which says that x is integral over $\mathbf{A}$.

- Now we appeal to the going up theorem: Since $\mathbf{A}[x]$ is an integral extension of $\mathbf{A}$, $M\mathbf{A}[x] \neq \mathbf{A}[x]$, which is a contradiction.

One application:

The integral closure of a domain

Theorem

Let $\mathbf{R}$ *be an integral domain of field of fractions* $\mathbf{K}$*. The integral closure of* $\mathbf{R}$ *is the intersection of the valuation rings of* $\mathbf{K}$ *containing* $\mathbf{R}$*.*

Proof. Let $\mathbf{B}$ be the integral closure of $\mathbf{R}$ and $\mathbf{C}$ the intersection of the valuation rings of $\mathbf{K}$ that contain $\mathbf{R}$.

Suppose $x \in \mathbf{C} \setminus \mathbf{B}$. Then $x \notin \mathbf{B}[x^{-1}]$. This means that x^{-1} is contained in some maximal ideal of $\mathbf{B}[x^{-1}]$. By the construction there is a valuation ring V such that $x^{-1}V \neq V$. But $x \in V$, which is a contradiction. □

Outline

1. General Orientation
2. Syllabus
3. Introduction
4. Chain Conditions
5. Prime Ideals
6. Primary Decomposition
7. Noetherian Rings
8. Graded Noetherian Rings
9. Commutative Artinian Rings
10. Modules of Fractions
11. Integral Extensions
12. Dedekind Domains
13. Valuation Rings
14. **Homework**

Homework

- Find the kernel of the homomorphism ($\mathbf{K}$ is a field)

  $$\varphi : \mathbf{K}[x, y, z] \longrightarrow \mathbf{K}[t],$$

  defined by $\varphi(x) = t^4$, $\varphi(y) = t^5$ and $\varphi(z) = t^7$. What do you think is true in general?
- Show that $R = \mathbb{C}[x, y]/(y^2 - x(x-1)(x-2))$ is a Dedekind domain. [Show that $y^2 - x(x-1)(x-2)$ is irreducible, use the Nullstellensatz to describe the maximal ideals of R, and show that for each such ideal P, R_P is a discrete valuation domain.]
- If R is a Dedekind domain, prove that for each nonzero ideal I, R/I is a principal ideal ring. Derive from this the fact that every ideal of R can be generated by 2 elements.
- Show that an invertible ideal of a local integral domain is principal.

- Let I be a finitely generated ideal of the commutative ring **R**. Prove that if $I^2 = I$, then $I = \mathbf{R}e$, $e^2 = e$.