Commutative Algebra

Nutan Nepal

August 15, 2021

1

Notes 1.1. *Basic properties of ideals. (Matsumura 1)*

---

1. In a surjective ring homomorphism $f : A \to A/I$, the ideals J of A/I and the ideals $f^{-1}(J)$ of A are in one-to-one correspondence. (lattice isomorphism theorem) When we need to think about ideals of A containing I, we can work on A/I: if I' is any ideal of A then $f(I')$ is an ideal of A/I with $f^{-1}(f(I')) = I + I'$, and $f(I') = (I + I')/I$.

2. For $a \in A$, $(a) = (1)$ iff a has an inverse in A. If a is a unit and x is nilpotent, then $a + x$ is a unit.

3. Using Zorn's lemma on a set of proper ideals (ordered by inclusion) containing some ideal I, we see that there exists at least one maximal ideal M containing I. A/M is a field.

4. A proper ideal P is prime if $x, y \notin P \implies xy \notin P$. A/P is an integral domain.

5. If I is an ideal disjoint from a multiplicative set S, then $A - S$ has a maximal ideal containing I which is prime. (prove...)

6. If I is an ideal, then the radical of I

$$\sqrt{I} = \{a \in A : a^n \in I \text{ for some } n > 0\}$$

is also an ideal. If P is a prime ideal containing I then $\sqrt{I} \subset P$. Furthermore, if $x \notin \sqrt{I}$, then we can find a prime ideal containing $\sqrt{I}$ but not x. And hence,

$$\sqrt{I} = \bigcap_{P \supset I} P$$

7. The intersection of all prime ideals is nilradical $\text{nil}(A)$ and the intersection of all maximal ideals is Jacobson radical $\text{rad}(A)$. $x \in \text{rad}(A)$ iff $1 + Ax$ consists entirely of units of A.

8. $II' \subset I \cap I'$. If $I + I' = (1)$, then $II' = I \cap I'$. Also, if $I + I' = (1)$ and $I + I'' = (1)$, then $I + I'I'' = (1)$. Hence, for ideals I_i which are coprime in pairs

$$I_1 I_2 ... I_n = I_1 \cap I_2 \cap ... \cap I_n.$$

9. If $I + I' = (1)$, then $A/II' \simeq A/I \times A/I'$. This can be extended with n ideals like in 8.

10. A maximal ideal $\mathfrak{m}$ of A corresponds with the maximal ideal $\mathbf{m} = \mathfrak{m}B + (X_1, ..., X_n)$ of the ring $B = A[[X_1, ..., X_n]]$. Here, $\mathbf{m} \cap A = \mathfrak{m}$. These properties are not necessarily true in case of polynomial rings.

11. $a \in A$ is called irreducible element if a is not a unit of A and

$$a = bc \implies b \text{ or } c \text{ is a unit of A.}$$

a is irreducible iff aA is maximal among proper principal ideals and a is prime if aA is a prime ideal.

12. $A = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[X]/(X^2+5)$; then setting $k = \mathbb{Z}/2\mathbb{Z}$ we have

$$A/2A = \mathbb{Z}[X]/(2, X^2+5) = k[X]/(X^2-1) = k[X]/(X-1)^2.$$

Then $P = (2, 1-\sqrt{-5})$ is a maximal ideal of A containing 2.

Problems 1.2.

---

1. Let A be a ring, and $I \subset \text{nil}(A)$ an ideal made up of nilpotent elements. If $a \in A$ maps to a unit of A/I then a is a unit of A.
   - There exists $a' \in A$ such that $a \cdot a' + I \equiv 1$. So, $(a.a'-1)^n = 0$ for some n.

2. Let $A_1, ..., A_n$ be rings; then the prime ideals of $A = A_1 \times \cdots \times A_n$ are of the form

$$P = A_1 \times \cdots \times A_{i-1} \times P_i \times A_{i+1} \times \cdots \times A_n,$$

   where P_i is a prime ideal of A_i.
   - For $A_1 \times A_2$, let $P = I_1 \times I_2$ be a prime ideal.Then, since the product of integral domains is not itself an integral domain, only one from I_1 or I_2 is prime. $(A_1 \times A_2)/(I_1 \times I_2) \simeq A_1/I_1 \times A_2/I_2$. This can be extended to n ideals in a similar fashion.

3. Let A and B be rings and $f : A \to B$ a surjective homomorphism.

   a. Prove that $f(\text{rad } A) \subset \text{rad } B$, and construct an example where the inclusion is strict.
      - If $x \in \text{rad } A$, then $f(1+Ax) = 1 + Bf(x)$ should be a set of units of B.

   b. Prove that if A is a semilocal ring then $f(\text{rad } A) = \text{rad } B$.

4. Let A be an integral domain. Then A is a UFD iff every irreducible element is prime and the principal ideals of A satisfy the ascending chain condition. (Equivalently, every non-empty family of principal ideals has a maximal element.)

5. Let $\{P_\lambda\}_{\lambda \in \Lambda}$ be a non-empty family of prime ideals, and suppose that the P_λ are totally ordered by inclusion; then $\bigcap P_\lambda$ is a prime ideal. Also, if I is any proper ideal, the set of prime ideals containing I has a minimal element.

6. Let A be a ring, $I, P_1, \ldots, P_r$ ideals of A, and suppose that $P_3, \ldots, P_r$ are prime, and that I is not contained in any of the P_i; then there exists an element $x \in I$ not contained on any P_i.

Notes 1.3. *Basic properties of modules (Matsumura 2)*

---

1. If N, N' are two submodules of an A-module M, the set $N : N' = \{a \in A : aN' \in N\}$ is an ideal of A and we can consider M as a module over $A/\text{ann}(M)$ where $\text{ann}(M) = 0 : M$.

   Theorem 1.1. *Suppose that M is an $A-$module generated by n elements and $\phi \in Hom_A(M, M)$; let I be an ideal of A such that $\phi(M) \subset IM$. Then there is a relation of the form*
   $$\phi^n + a_1\phi^{n-1} + \cdots + a_{n-1}\phi + a_n = 0,$$
   with $a_i \in I^i$ for $1 \leq i \leq n$.

2. (NAK.) Let M be a finite A-module and I an ideal of A. If $M = IM$ then there exists $a \in A$ such that $aM = 0$ and $a \equiv 1 \mod I$. If in addition $I \subset \text{rad } A$ then $M = 0$.

3. Let A be a ring and $I \subset \text{rad } A$ an ideal. If M is an A-module, $N \subset M$ a submodule such that M/N is finite over A. Then $M = N + IM$ implies $M = N$.

4. Let $(A, \mathfrak{m}, k)$ be a local ring and M a finite A-module. $\overline{M} = M/\mathfrak{m}M$ is a finite n-dimensional vector space over k.

   (i) If $\{\bar{u}_1, \ldots, \bar{u}_n\}$ is a basis of $\overline{M}$ then $\{u_1, \ldots, u_n\}$ is a minimal basis of M, where $u_i \in M$ is the inverse image of each $\bar{u}_i \in \overline{M}$. Every minimal basis of M is obtained this way and has n elements. (If A is not a local ring, then minimal bases of M do not necessarily have same number of elements.)

   (ii) If $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$ are both minimal bases of M, and $v_i = \sum a_{ij}u_j$ with $a_{ij} \in A$ then $\det(a_{ij})$ is a unit of A, so that (a_{ij}) is an invertible matrix.

5. If $f : M \to M$ is an A-linear map and f is surjective, then f is also injective. (thus an automorphism)

6. If $(A, \mathfrak{m})$ is a local ring A, then a projective module M (finite or not) over A is free. Any projective module is a direct sum of countably generated projective modules.

7. Let M be a projective module over a local ring A, and $x \in M$. Then there exists a direct summand of M containing x which is a free module.

8. A simple A-module $M \neq 0$ has no submodules other than 0 and itself; $M \simeq A/\mathfrak{m}$ with $\mathfrak{m}$ a maximal ideal of A. A composition series of M is a chain $M = M_0 \supset M_1 \supset M_2 \ldots \supset M_r = 0$ where every M_i/M_{i+1} is a simple module. If a composition series exist then r is called the length and is an invariant (independent of the composition series chosen).

9. If $0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow \cdots \longrightarrow M_n \longrightarrow 0$ is an exact sequence of A-modules and each M_i has finite length $l(M_i)$ then
$$\sum_{i=1}^{n} (-1)^i l(M_i) = 0.$$

10. An A-module M is of **finite presentation** if there exists an exact sequence of the form
$$A^p \longrightarrow A^q \longrightarrow M \longrightarrow 0.$$
If $0 \longrightarrow K \longrightarrow N \longrightarrow M \longrightarrow 0$ is an exact sequence, M is of finite presentation and N is finitely generated, then K is also finitely generated.

$$\begin{array}{ccccccc} A^p & \xrightarrow{g} & A^q & \xrightarrow{f} & M & \to & 0 \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \alpha} & & \| & & \\ 0 \to K & \xrightarrow{\psi} & N & \xrightarrow{\varphi} & M & \to & 0 \end{array}$$

Notes 1.4. *Story of Commutative Algebra. (Eisenbud 1)*

---

1. Gauss proved that $\mathbb{Z}[i]$ is a UFD and used this on 1928 paper on biquadratic residues to prove results about ordinary numbers.

2. Euler, Gauss, Dirichlet, and Kummer, then, used this idea for $\mathbb{Z}[\zeta]$, with ζ a *nth* root of unity, to prove some special cases of Fermat's last theorem. The idea required factorization of $x^n + y^n$ over $\mathbb{Z}[\zeta]$.

3. $\mathbb{Z}[\zeta]$ doesn't always have unique factorization. (first example n=23) The search for generalization of unique factorization birthed Dedekind's idea of ideals of a ring.

4. This search culminated in two major theories: Dedekind's unique factorization of ideals into prime ideals (Dedekind domains); and Kronecker's theory of polynomial rings and Lasker's theory of primary decomposition in them.

   a. Dedekind represented an element $r \in R$ by the ideal (r) and found conditions under which a ring has unique factorization of ideals into prime ideals. (the ring of all integers in any number field)

b. Kronecker put the notion of adjoining the root of polynomial to a field k on firm footing by introducing the ring $k[x]$, with the desired ring being $k[x]/f(x)$. There is no way to factorize ideals in a polynomial rings but Lasker later showed how to generalize unique factorization into "primary decomposition".

5. [Algebraic Curves and Function Theory] Around 1860, Abel, Jacobi and Riemann made entirely new view of algebraic curves possible. From 1875-1882, Kronecker, Wierstrass, Dedekind, and Weber discovered that algebraic techniques that were developed to handle number fields could be applied to geometrically defined fields, thus pioneering the "arithmetic approach to function theory."

6. [Invariant Theory] After Plücker introduced projective coordinates around 1830, people were interested in the geometric invariant properties under certain classes of transformations. One way to express such an invariant property leads to finding an associative number which is invariant under choice of coordinates.

   a. Mathematicians realized that the invariance under choice of coordinates was the invariance under an action of a group ($\mathrm{GL}_n(k)$ or $\mathrm{SL}_n(k)$).
   b. The general problem, then, became finding the set of invariants (a subalgebra of S) S^G under "nice" action of a group G of automorphisms of polynomial ring $S = k[x_1, \ldots, x_n]$. The **fundamental problem of invariant theory** was the problem of existence of finite systems of generators of S^G.
   c. In a series of papers from 1888 to 1893, Hilbert showed that the ring of invariants is finitely generated in a wide range of cases. Aside from this, Hilbert proved four major results (the basis theorem, the Nullstellensatz, the polynomial nature of the Hilbert function and the syzygy theorem), all of which played enormous role in development of commutative algebra.

7. A graded ring is a ring R together with the direct sum decomposition

$$R = R_0 \oplus R_1 \oplus R_2 \oplus \cdots \text{ as abelian groups,}$$

such that $R_i R_j \subset R_{i+j}$ for $i, j \geq 0$.

The Basis Theorem & Finite Generation of Invariants

Theorem 1.2 (Hilbert Basis Theorem)**.** *If a ring R is Noetherian, then the polynomial ring $R[x]$ is Noetherian.*

Corollary 1.3. *Any homomorphic image of a Noetherian ring is Noetherian. Furthermore, if R_0 is a Noetherian ring, and R is a finitely generated algebra over R_0, then R is Noetherian.*

Proposition 1.4. *If R is a Noetherian ring and M is a finitely generated R-module, then M is Noetherian.*

Corollary 1.5. *Let k be a field, $S = k[x_1, \ldots, x_r]$ be a polynomial ring graded by degree, and R a k-subalgebra of S. If R is a summand of S, in the sense that there is a map of R-modules $\varphi : S \to R$ that preserves degrees and takes each element of R to itself, then R is a finitely generated k-algebra.*

Hilbert's finiteness result follows by taking $R = S^G$ above.

8. Given a subset $I \subset k[x_1, \ldots, x_n]$, the algebraic subset of k^n

$$Z(I) = \{(a_1, \ldots, a_n) \in k^n | f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}$$

is called **algebraic variety** if it is **irreducible** (not the union of two smaller algebraic subsets). Taking algebraic sets as closed sets, we obtain **Zariski topology** on k^n. Given a set $X \subset k^n$,

$$I(X) = \{f \in k[x_1, \ldots, x_n] | f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in X\}$$

is an ideal of $k[x_1, \ldots, x_n]$. Identifying polynomial functions that agree at all points of a set X, we get the **coordinate ring** $A(X) = k[x_1, \ldots, x_n]/I(X)$ of X which is reduced. The ideals $I(X)$ are all radical ideals, but not all radical ideals can appear as $I(X)$ (but in an algebraically closed field, all radical ideals appear as such).

The Nullstellensatz

Theorem 1.6 (Nullstellensatz)**.** *Let k be an algebraically closed field. If $I \subset k[x_1, \ldots, x_n]$ is an ideal, then*

$$I(Z(I)) = \sqrt{I}.$$

Thus the correspondences $I \mapsto Z(I)$ and $X \mapsto I(X)$ induces a bijection between the collection of algebraic subsets of $\mathbf{A}_k^n$ and radical ideals of $k[x_1, \ldots, x_n]$.

Corollary 1.7. *A system of polynomial equations $\{f_1 = 0, \ldots, f_m = 0\}$ over an algebraically closed field k has no solutions in k^n iff 1 can be expressed as a linear combination $1 = \sum p_i f_i$ with polynomial coefficients p_i.*

Corollary 1.8. *If k is an algebraically closed field and A is a k-algebra, then $A = A(X)$ for some algebraic set X iff A is reduced and finitely generated as k-algebra.*

Corollary 1.9. *Let k be an algebraically closed field and let $X \subset \mathbf{A}^n$ be an algebraic set. Every maximal ideal of $A(X)$ is of the form $\mathfrak{m}_p := (x_1 - a_1, \ldots, x_n - a_n)/I(X)$ for some $p = (a_1, \ldots, a_n) \in X$.*

Corollary 1.10. *The category of affine algebraic sets and morphisms (over an algebraically closed field k) is equivalent to the affine k-algebras with the arrows reversed.*

9.