Commutative Algebra

Stuart Martin

These notes, taken by Markus Himmel, will at times differ significantly from what was lectured. In particular, all errors are almost certainly my own.

Contents

CHAPTER 0

Introduction

Remark 0.0. Commutative algebra is the study of commutative rings developed from

(1) algebraic geometry and
(2) algebraic number theory

In (1) focus is on $k[X_1, \dots, X_n]$, the polynomial ring over the field k. In (2) focus is on $\mathbb{Z}$, the ring of rational integers. Modern development of (1) by Grothendieck encompasses much of (2).

Going back further, Hilbert wrote a series of papers on polynomial invariant theory, 1888-1893.

Example 0.1. Denote by Σ_n the symmetric group on $\{1, \dots, n\}$. Σ_n acts on $k[X_1, \dots, X_n]$ by permuting variables: given $\sigma \in \Sigma_n$, $f \in k[X_1, \dots, X_n]$, we set

$$(\sigma f)(X_1, \dots, X_n) \coloneqq f(X_{\sigma^{-1}(1)}, \dots, X_{\sigma^{-1}(n)}).$$

The action of Σ_n is via ring automorphisms so it makes sense to define the *ring of invariants*

$$S \coloneqq \{f \in k[X_1, \dots, X_n] \mid \forall \sigma \in \Sigma_n \colon \sigma f = f\}.$$

S is a ring, called the *ring of symmetric polynomials*. Consider the following elementary symmetric functions:

$$\begin{aligned} e_1(X_1, \dots, X_n) &= X_1 + \cdots + X_n), \\ e_2(X_1, \dots, X_n) &= \sum_{i<j} X_i X_j, \\ &\vdots \\ e_n(X_1, \dots, X_n) &= X_1 \cdot \cdots \cdot X_n. \end{aligned}$$

It turns out that S is generated as a ring by these e_i and the canonical map $k[Y_1, \dots, Y_n] \to S$ given by $Y_i \mapsto e_i$ is an isomorphism of rings.

Hilbert showed that S is finitely generated for many other groups. Among the way he proved a few very deep results.

- the basis theorem,
- the Nullstellensatz,
- the polynomial nature of the Hilbert function (and beginnings of dimension theory),
- the syzygy theorem (and beginnings of the homological theory of polynomial rings).

Remark 0.2. Emmy Noether (1921) extracted the key property that made the basis theorem work: we call a ring *noetherian* if every ideal is finitely generated. There are many properties that are equivalent to this.

Theorem 0.3. Hilbert's basis theorem states that if R is a commutative Noetherian ring, then so is $R[X]$.

Corollary 0.4. In particular, if k is a field, then $k[X_1, \dots, X_n]$ is noetherian.

Noether developed a theory of ideals for noetherian rings, for example the existence of a primary decomposition which generalises the factorisation into primes known from number theory.

Links between commutative algebra and algebraic geometry

Remark. Recall the fundamental theorem of algebra: a polynomial $f \in \mathbb{C}[X]$ is determined up to scalar multiples by its zeros up to multiplicity.

Given $f \in \mathbb{C}[X_1, \dots, X_n]$ we have a polynomial function $\mathbb{C}^n \to \mathbb{C}$ given by $(a_1, \dots, a_n) \mapsto f(a_1, \dots, a_n)$.

Different polynomials yield different functions, so $\mathbb{C}[X_1, \dots, X_n]$ can be viewed as the ring of polynomial functions on complex addine n-space.

Given $I \subseteq \mathbb{C}[X_1, \dots, X_n]$, define the set of common zeros

$$Z(I) = \{(a_1, \dots, a_n) \in \mathbb{C}^n \mid \forall f \in I\colon f(a_1, \dots, a_n) = 0\},$$

called an (affine) algebraic set, which is a subset of $\mathbb{C}^n$.

Remark. (1) One can replace I by the ideal generated by I and get the same algebraic set. Replacing an ideal by a generating set of the ideal leaves the algebraic set unchanged. Hilbert's basis theorem asserts that any algebraic set is the set of common zeros of a finite set of polynomials.

(2)
$$\bigcap_j Z(I_j) = Z(\bigcup_j I_j),$$
$$\bigcup_{j=1}^n Z(I_j) = Z(\prod_{j=1}^n I_j)$$

for ideals I_j. Define a topology of $\mathbb{C}^n$ with closed sets being the algebraic sets. This is the Zariski topology; it is coarser than the normal topology on $\mathbb{C}^n$.

(3) For $S \subseteq \mathbb{C}^n$ define

$$I(S) \coloneqq \{f \in \mathbb{C}[X_1, \dots, X_n] \mid \forall (a_1, \dots, a_n) \in S\colon f(a_1, \dots, a_n) = 0\}.$$

This is an ideal of $\mathbb{C}[X_1, \dots, X_n]$ and it is radical, i.e., if $f^r \in I(S)$ for some $r \geq 1$, then $f \in I(S)$.

The Nullstellensatz is a family of results asserting that the corrspondence

$$I \mapsto Z(I)$$
$$I(S) \leftarrow\!\shortmid S$$

gives a bijection between the radical ideals of $\mathbb{C}[X_1, \dots, X_n]$ and the algebraic subsets of $\mathbb{C}^n$. In particular, the maximal ideals of $\mathbb{C}[X_1, \dots, X_n]$ correspond to points in $\mathbb{C}^n$.

Dimension

Remark. A large section of the course treats dimension of rings:

- the maximal length of chains of prime ideals;
- in geometric context in terms of growth rates (uses Hilbert function);
- the transcendence degree of the field of fractions (of an integral domain).

Over commutative rings these all give the same answer. A fourth way uses homological algebra and gives the same answer at least for nice noetherian rings.

Most of the theory dates between 1920 and 1950.

Rings of dimension 0 are called artinian rings. In dimension 1, special things happen which are important in number theory; this is crucial in the study of algebraic curves.

CHAPTER 1

Noetherian Rings

Remark. Throughout the lecture, R is a commutative unital ring.

Lemma 1.1. Let M be a (left) R-module. The following are equivalent.

(i) all submodules of M (including M itself) are finitely generated,
(ii) the ascending chain condition (ACC) holds: there are no strictly increasing infinite chains of submodules.
(iii) maximum condition in submodules holds: any nonempty set $\mathcal{S}$ of submodules of M has a maximal element L, i.e., if $L' \in \mathcal{S}$ and $L \subseteq L'$, then $L = L'$.

Proof. If all submodules of M are finitely generated and $N_1 \subseteq N_2 \subseteq \dots$ is an increasing chain of submodules of M, define $N \coloneqq \bigcup_{i=1}^{\infty} N_i$. This is a submodule of M, so it is finitely generated with generators $m_1, \dots, m_k$. Each m_i lies in some N_{n_i}. If n is the maximum of all n_i, we have $N_n = N$ and the chain is stationary.

If the ACC holds and $\mathcal{S}$ is nonempty, let $M_0 \coloneqq \{0\}$. Proceed inductively. If M_i is maximal, we are done. Otherwise, there is some M_{i+1} such that $M_i \subsetneq M_{i+1}$. By the ACC, this process must terminate after a finite number of steps.

If the maximum condition holds and N is any submodule of M, define $\mathcal{S}$ to be the collection of finitely generated submodules of N. $\mathcal{S}$ is nonempty as it contains the zero module. Let L be a maximal member of $\mathcal{S}$. Let $x \in N$. Then $L + Rx$ is finitely generated and $L \subseteq L + Rx$, hence, $x \in L$ and therefore $N = L$. $\square$

Definition 1.2. An R-module is called noetherian if all of its submodules are finitely generated.

Lemma 1.3. Let N be a submodule of M. Then M is noetherian if and only if N and M/N are noetherian.

Proof. If M is noetherian, then in particular all submodules of N are finitely generated. Furthermore, all submodules of M/N are of the form Q/N, where Q is submodule of M containing N. Q is finitely generated, say by $x_1, \dots, x_r$. Then Q/N is generated by $x_1 + N, \dots, x_r + N$.

Conversely, if both N and M/N are noetherian, and $L_1 \subseteq L_2 \subseteq \dots$ is an increasing chain of submodules of M, define $Q_i \coloneqq L_i + N$ and $N_i \coloneqq L_i \cap N$. Then Q_i/N and N_i are chains of submodules of M/N and N, respectively, so they terminate and we find r such that $\forall i \geq r\colon Q_i/N = Q_r/N$ and s such that $\forall i \geq s\colon N_i = N_s$. Define $k \coloneqq \max\{r, s\}$.

We will show that $\forall i \geq k\colon L_i = L_k$. Indeed, let $\ell \in L_i$. Then $\ell + N \in Q_i/N = Q_k/N = (L_k + N)/N$, so there are $\tilde{\ell} \in N, \ell' \in L_k, \hat{\ell} \in N$ such that $\ell - \tilde{\ell} = \ell' + \hat{\ell}$. Rearranging, we find that $\ell - \ell' = \tilde{\ell} + \hat{\ell} \in N$, and since $L_k \subseteq L_i$ we conclude that $\ell - \ell' \in N \cap L_i = N \cap L_k$. Therefore, $\ell = (\ell - \ell') + \ell' \in L_k$ and we are done. $\square$

Alternative Proof. It suffices to show that if

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is a short exact sequence of R-modules, then B is noetherian if and only if both A and C are noetherian.

If B is noetherian and N is a submodule of C, then $g^{-1}(N)$ is a submodule of B, thus finitely generated, say by $b_1, \dots, b_n$. If $c \in N$, then

$$c = f(\sum_{i=1}^{n} r_i b_i) = \sum_{i=1}^{n} r_i f(b_i),$$

so N is finitely generated. If N is a submodule of A, then it is isomorphic to a submodule of B, which is finitely generated, hence N is also finitely generated.

Assume that A and C are finitely generated and N is a submodule of B. Then $g(N)$ is finitely generated, say by $c_1, \dots, c_n$. Additionally, $f^{-1}(N)$ is finitely generated, say by $a_1, \dots, a_m$. Pick preimages $b_1, \dots, b_n$ such that $g(b_i) = c_i$. Now let $x \in N$. Then $g(x) = \sum_{i=1}^{n} r_i c_i$ and therefore $x - \sum_{i=1}^{n} r_i b_i \in \ker g = \operatorname{im} f$. Thus

$$x - \sum_{i=1}^{n} r_i b_i = f(\sum_{i=1}^{m} r_i' a_i).$$

Rearranging gives

$$x = \sum_{i=1}^{m} r_i' f(a_i) + \sum_{i=1}^{n} r_i b_i$$

and we conclude that $N = \langle b_1, \dots, b_n, f(a_1), \dots, f(a_m) \rangle$ as required. □

Lemma 1.4. Let $M, N, M_1, \dots$ be R-modules.

(i) $M \oplus N$ is noetherian if and only if both M and N are.
(ii) $M_1 \oplus \cdots \oplus M_n$ is noetherian if and only if all M_i are.
(iii) If M is noetherian then every homomorphic image is noetherian.
(iv) If M can be represented as the sum $M_1 + \cdots + M_n$, then M is noetherian if and only if each M_i is.

Proof.

(i) Apply the previous lemma to the split exact sequence

$$0 \longrightarrow N \xrightarrow{\iota} M \oplus N \xrightarrow{\pi} M \longrightarrow 0.$$

(ii) Induction.
(iii) If $\theta \colon M \to N$, apply the previous lemma to the short exact sequence

$$0 \longrightarrow \ker\theta \longrightarrow M \xrightarrow{\theta} \operatorname{im}\theta \longrightarrow 0.$$

(iv) If M is noetherian, then so is M_i as a submodule of M. If all M_i are notherian, then so is $M_1 \oplus \cdots \oplus M_n$, and since the map

$$M_1 \oplus \cdots \oplus M_n \to M_1 + \cdots + M_n,$$
$$(m_1, \dots, m_n) \mapsto m_1 + \cdots m_n$$

is surjective, $M_1 + \cdots + M_n$ is noetherian. □

Definition 1.5. A ring R is called noetherian if it is noetherian as a module over itself.

Lemma 1.6. If R is a noetherian ring and M is a finitely generated R-module. Then M is noetherian.

Proof. Assume M is generated by $m_1, \dots, m_n$. Then $R^n \cong R^{\oplus n}$ is noetherian and the map $R^n \to M$ given by $e_i \mapsto m_i$ is surjective, so M is noetherian. □

Theorem 1.7. If R is a noetherian ring, then $R[X]$ is also noetherian.

Proof. We will show that every ideal (i.e., submodule) of $R[X]$ is finitely generated. Let I be an ideal and let $I_n := \{f \in I \mid \deg f \leq n\}$. $0 \in I_n$ and $I_0 \subseteq I_1 \subseteq \cdots$ form an ascending chain.

Define R_n to be the set of coefficients of X^n appearing in elements of I_n.

If $a, b \in R_n$, then $a + b \in R_n$ and $ra \in R_n$ for any $r \in R$. Therefore, R_n is an ideal of R.

Furthermore, if $a \in R_n$, then $a \in R_{n+1}$ by multiplying the corresponding polynomial by X.

Since R is noetherian, the chain $R_0 \subseteq R_1 \subseteq \cdots$ terminates, so we have N such that $\forall n \geq N \colon R_n = R_N$. Each of $R_0, \ldots R_N$ is a finitely generated ideal of R, say R_j is generated by $a_{j1}, \ldots, a_{jk_j}$. There are polynomials $f_{j1}, \ldots, f_{jk_j}$ such that $\deg f_{ji} = j$ and leading coefficient of f_{ji} is a_{ji}.

We will show that the finite set $\{f_{jk} \mid 0 \leq j \leq N, 1 \leq k \leq k_j\}$ generates I.

We will use induction on $\deg f$, where $f \in I$. If $\deg f = 0$, then $f = a$ for some $a \in R$. By definition of R_0, $a \in R_0$, and a is in the ideal generated by the f_{0i}.

Assume next that $0 < \deg f \leq N$ and that the claim is true for smaller degrees. Let a be the leading coefficient of f. $a \in R_n$, so we may write

$$a = \sum_j r_{nj} a_{nj}.$$

Then

$$f - \sum_j r_{nj} f_{nj}$$

is in I and of smaller degree, so is expressible as a linear combination of the f_{ij}, so f is also expressible as a linear combination as well.

Finally, assume that $\deg f < N$ and that the claim is true for smaller degrees. If a is the leading coefficient of f, then $a \in R_n = R_N$, so we may write

$$a = \sum_j r_{Nj} a_{Nj}.$$

Then

$$f - X^{n-N} \sum_j r_{Nj} f_{Nj}$$

is in I and of smaller degree, so is expressible as a linear combination of the f_{ij}, so f is also expressible as a linear combination as well. $\square$

Remark. In practice one uses Gröbner bases for ideals, which are special generating sets that admit efficient algorithms.

Example.
- Fields are notherian.
- PIDs are noetherian.
- Let p be a prime number. $\{\frac{m}{n} \mid m, n \in \mathbb{Z}, p \nmid n\}$ is an example of a localization of $\mathbb{Z}$ (at p). All localizations of noetherian rings are noetherian.
- $k[X_1, X_2, \ldots]$ is not noetherian, as there are is an infinite chain $(X_1) \subsetneq (X_1, X_2) \subsetneq \cdots$.
- $k[X_1, \ldots, X_n]$ is noetherian, by Hilbert's basis theorem and induction.
- $\mathbb{Z}[X_1, \ldots, X_n]$ is noetherian: every finitely generated commutative ring is noetherian, since if R is generated by $r_1, \ldots, r_n$, we have a surjective map $\mathbb{Z}[X_1, \ldots, X_n] \to R$ given by $X_i \mapsto r_i$.
- Group algebras of free abelian groups of finite rank: if A is an abelian group, the group algebra of A is the free $\mathbb{Z}$-module with basis A. It is an A-algebra with the multplication defined as the $\mathbb{Z}$-bilinear continutation of $(a, b) \mapsto ab$. If A is generated by $g_1, \ldots, g_n$, then $\mathbb{Z}A$ is generated as a ring by $g_1, g_1^{-1}, \ldots, g_n, g_n^{-1}$.

- The ring of formal power series $k[[X]]$ is noetherian if k is noetherian, see below.

Here are some non-commutative rings which are left and right noetherian:

- The enveloping algebra of a finite dimensional Lie agebra.
- The Iwasawa algebras of compact p-adic groups.

THEOREM 1.8. If R is a noetherian ring, then the ring $R[[X]]$ of formal power series over R is noetherian.

PROOF 1. Adapt the proof of Hilbert's basis theorem, but use trailing coefficients rather than leading coefficients. See the first exercise sheet. □

THEOREM 1.9 (Cohen's theorem). If every prime ideal in a ring R is finitely generated, then R is noetherian.

PROOF. Assume that R is not noetherian. Let $\mathcal{S}$ be the collection of of non-finitely generated ideals of R. $\mathcal{S}$ is nonempty by assumption and partially ordered by inclusion. Furthermore, every chain of ideals in $\mathcal{S}$ has an upper bound (indeed, the union of an increasing chain of ideals in $\mathcal{S}$ is an ideal and not finitely generated, since otherwise all generators would lie in some member of the chain, which would then be finitely generated), so by Zorn's lemma there is a maximal member $I \in \mathcal{S}$. I has the property that it is not finitely generated, but every ideal J such that $I \subsetneq J$ is finitely generated.

We will now show that I is a prime ideal. Supppose a and b are such that $ab \in I$, $a \notin I$, $b \notin I$. Since I is maximally non-finitely-generated, $I + Ra$ is finitely generated, say by $i_1 + r_1 a, \cdots, i_1 + r_n a$. Define

$$J \coloneqq \{s \in R \mid sa \in I\}.$$

J is an ideal, and it satisfies $I \subsetneq I + Rb \subseteq J$ (here we use that $ab \in I$). Again by maximality of I, J is finitely generated. Therefore, if we can show that $I = Ri_1 + \cdots + Ri_n + Ja$, then I is finitely generated, a contradiction.

The inclusion "$\supseteq$" follows by definition of J, so let $t \in I \subseteq I + Ra$, so

$$t = u_1(i_1 + r_1 a) + \cdots + u_n(i_n + r_n a)$$

for suitable $u_i \in R$. We may rewrite this as

$$t = u_1 i_1 + \cdots + u_n i_n + (u_1 r_1 + \cdots + u_n r_n)a.$$

Since the whole right hand side is in I and everything but the last summand is also in I, the last summand is in I, so $u_1 r_1 + \cdots + u_n r_n \in J$ by definition of J, so indeed $t \in Ri_1 + \cdots + Ri_n + Ja$ and we are done. □

LEMMA 1.10. Let p be a prime ideal of $R[[X]]$ and $\theta\colon R[[X]] \to R$ given by $X \mapsto 0$. The p is a finitely generated ideal of $R[[X]]$ if and only if $\theta(p)$ is a finitely generated ideal of R.

PROOF. We already know that images of finitely generated ideals are finitely generated.

Conversely, suppose that $\theta(p) = Ra_1 + \cdots + Ra_n$.

If $X \in p$, then p is generated by $a_1, \ldots, a_n, X$: given any $f \in p$, we can find g such that $f - Xg \in R$ and so indeed $a_i \in p$ (!) and $f \in Ra_1 + \cdots + Ra_n + X$.

On the other hand, if $X \notin p$, let $f_1, \ldots, f_n \in p$ have constant terms $a_1, \ldots, a_n$ (these exist by definition of θ). We will show that p is generated by $f_1, \ldots, f_n$. Let $g_0 \in p$ and let $b = \sum_{i=1}^n b_i a_i$ be the constant term of g, so there is g_1 such that $g_0 - \sum_{i=1}^n r_{0,i} f_i = g_1 X$. We have $g_1 X \in p$, but since p is prime and $X \notin p$, we have $g_1 \in p$. Continuing inductively, we find $r_{j,i} \in R$ and $g_{j+1} \in p$ such that $g_j - \sum_{i=1}^n r_{j,i} f_i = g_{j+1} X$.

Define $h_j \coloneqq \sum_{i=0}^{\infty} r_{i,j} X^i$. We can calculate

$$\begin{aligned}\sum_{i=1}^{n} h_i f_i &= \sum_{i=1}^{n} \left(\sum_{j=0}^{\infty} r_{j,i} X^j \right) f_i \\ &= \sum_{i=1}^{n} \sum_{j=0}^{\infty} r_{j,i} f_i X^j \\ &= \sum_{j=0}^{\infty} \sum_{i=1}^{n} r_{j,i} f_i X^j \\ &= \sum_{j=0}^{\infty} X^j \sum_{i=1}^{n} r_{j,i} f_i \\ &= \sum_{j=0}^{\infty} X^j (g_j - g_{j+1} X) \\ &= g_0,\end{aligned}$$

so g_0 is in the span of $f_1, \ldots, f_n$ as required. □

LEMMA 1.11. The set $N(R)$ of all nilpotent elements of R is an ideal and $R/N(R)$ has no nonzero nilpotent elements.

PROOF. If $x \in N(R)$, then there is $m \in \mathbb{N}$ such that $x^m = 0$, which implies $(rx)^m = 0$, so $rx \in N(R)$. If $x, y \in N(R)$, there are $n, m \in \mathbb{N}$, $x^n = y^m = 0$. Then $(x+y)^{m+n-1}$ is a linear combination of terms $\lambda x^s y^t$ with $s + y = m + n - 1$. In particular, $s \geq n \vee t \leq m$, and so $(x+y)^{m+n-1} = 0$ and $x + y \in N(R)$.

Furthermore, if $s \in R/N(R)$, then $s = x + N(R)$. If s is nilpotent, i.e., $s^n = 0$, then $0 = s^n = (x + N(R))^n = x^n + N(R)$, i.e., $x^n \in N(R)$. That means that for some m we have $x^{nm} = 0$, so $x \in N(R)$, so $s = 0$. □

DEFINITION 1.12. The ideal $N(R)$ is called the nilradical of R.

THEOREM 1.13. The nilradical $N(R)$ is the intersection of all prime ideals of R.

PROOF. Define $I \coloneqq \bigcap_{p \text{ prime}} p$.

If $x \in N(R)$, i.e., $x^n = 0$, and p is prime, then $x^n = 0 \in p$, so $x \in p$. Hence, $N(R) \subseteq I$.

To show that $I \subseteq N(R)$, we will show that $x \notin N(R)$ implies $x \notin I$. Indeed, if $x \notin N(R)$, define $\mathcal{S}$ to be the collection of all ideals J that are disjoint from the set $\{x^n \mid n > 0\}$. We have $(0) \in \mathcal{S}$, so $\mathcal{S}$ is nonempty, and as usual, upper bounds of chains exist, so Zorn's lemma gives us a maximal member J_1 of $\mathcal{S}$. We have $x \notin J_1$, so if we can show that J_1 is prime, we are done.

Suppose $yz \in J_1$, $y, z \notin J_1$. Then $J_1 + Ry$ and $J_1 + Rz$ are strictly larger than J_1, so we find n, m such that $x^n \in J_1 + Ry$, $x^m \in J_1 + Rz$. This implies $x^{n+m} \in J_1 + Ryz$ (write $x^n = j_1 + r_1 y$, $x^m = j_2 + r_2 z$), but then $x^{n+m} \in J_1 + Ryz = J_1$, which is a contradiction because $J_1 \in \mathcal{S}$. □

DEFINITION 1.14. The raddical $\sqrt{I}$ of an ideal I is defined as

$$\sqrt{I} \coloneqq \{r \in R \mid \exists n \in \mathbb{N} \colon r^n \in I\}$$

We call an ideal radical if $I = \sqrt{I}$.

REMARK. It is unsubstantial whether 0 is allowed as an exponent or not: if $r^0 = 1 \in I$, then $I = R$, so $r^1 \in I$.

We have an equality $\sqrt{I} + I = N(R/I)$ of ideals of R/I.

$\sqrt{I}$ is the intersection of all prime ideals that contain I: $\sqrt{I}/I$ is the intersection of all prime ideals of R/I, then use the correspondence between prime ideals of R/I and prime ideals of R that contain I.

DEFINITION 1.15. The Jacobson radical $J(R)$ of R is the intersection of all maximal ideals of R.

REMARK. We have $N(R) \subseteq J(R)$.

THEOREM 1.16 (Nakayama's lemma). If M is a finitely generated R-module such that $J(R)M = M$, then $M = 0$.

PROOF. Suppose that $M \neq 0$. Define $\mathcal{S}$ to be the collection of proper submodules of M. Then $(0) \in \mathcal{S}$, and if we have an ascending chain of proper submodules, then the union is also a proper submodule (otherwise all generators would already lie in one of the proper submodules). So by Zorn, there is a maximal proper submodule M_1.

The the quotient M/M_1 is a simple module, as we can pullback any submodule of M/M_1 to a submodule of M lying between M_1 and M. If $0 \neq m \in M/M_1$, the submodule generated by m is all of M/M_1.

The homomorphism $R \to M/M_1$ of R-modules given by $r \mapsto rm + M_1$ is surjective. If I is the kernel of this map, then there is an isomorphism of R-modules $M/M_1 \cong R/I$, but since the former is a simple R-module, so is the latter. Now if J is an ideal of R/I, then it is also an R-submodule of R/I, which shows that R/I has only two ideals, so it is a field. This means that I is a maximal ideal.

Let $n \in M$. Since m generates M/M_1, we can write $n = rm + m'$ for some $r \in R$, $m' \in M_1$. If $i \in I$, then $in = rim + im' \in M'$, since $im \in M'$ by definition of I. This means that $IM \subseteq M_1$.

Since I is maximal, we have $J(R) \subseteq I$, and so

$$J(R)M \subseteq IM \subseteq M_1 \subsetneq M,$$

contrary to our assumption. □

REMARK. In a commutative ring, $N(R) \leq J(R)$. They are in general not equal, take for example $R_p = \{\frac{m}{n} \in \mathbb{Q} \mid p \nmid n\}$ for some prime p. This has a unique maximal ideal $p = \{\frac{m}{n} \in \mathbb{Q} \mid p \mid n, p \nmid n\}$, but it is an integral domain, so $N(R) = (0)$ while $J(R) = p$

On the other hand, for $R = k[X_1, \dots, X_n]/I$, where k is algebraically closed and I is any ideal, then we do indeed have $N(R) = J(R)$. This is Hilbert's Nullstellensatz.

EXAMPLE. A commutative ring is called artinian if it does not contain an infinite, strictly decreasing chain of ideals (equivalently, if every nonempty set of ideals has a minimal member). An R-module is called artinian if it satisfies that analogous property for submodules.

Examples of artinian rings: $\mathbb{Z}/p\mathbb{Z}$, $k[X]/(f)$, where k is a field and $f \neq 0$. $k[X]$ is not artinian: we have the chain $(X) \supseteq (X^2) \subseteq \cdots$.

Recall that an ideal I is prime if and only iff R/I is an integral domain if and only if $I_1, I_2 \subseteq I$ implies that $I_1 \subseteq I \vee I_2 \subseteq I$.

We will now show that if R is artinian, then prime ideals are maximal, which in particular means that $N(R) = J(R)$. Indeed, let p be a prime ideal and $x \in R$ such that $x \notin p$. By the descending chain condition, $(x) \supseteq (x^2) \subseteq \cdots$ becomes stationary, so there is a number n and some $y \in R$ such that $x^n = yx^{n+1}$. Rearranging, we have $x^n(1 - xy) = 0 \in p$. Since p is prime and $x \notin p$, $x^n \notin p$, so we must have $1 - xy \in p$, so $x + p$ has the inverse $y + p$ in R/p. Since x was arbitrary, R/p is a field, so p is maximal.

THEOREM 1.17 (Artin-Tate lemma). Let $R \subseteq S \subseteq T$ be commutative rings. Suppose that R is noetherian, T is finitely generated as an R-algebra and T is a finitely generated S-module. Then S is a finitely generated R-algebra.

PROOF. Suppose T is generated as an R-algebra by $t_1 = 1, \dots, t_n \in T$. By assumption, we have $x_1 = 1 \dots, x_m \in T$ such that $T = Sx_1 + \dots + Sx_m$. Therefore, if $1 \leq i \leq n$, we may write

$$t_i = \sum_{j=1}^{m} s_{ij} x_j \tag{1}$$

for some $s_{ij} \in S$. Furthermore, $1 \leq i, j \leq m$, we find $s_{ijk} \in S$ satisfying

$$x_i x_j = \sum_{k=1}^{m} s_{ijk} x_k. \tag{2}$$

Define S_0 as the R-subalgebra of S generated by the s_{ij} and the s_{ijk}. We have $R \subseteq S_0 \subseteq S$. If $t \in T$, we may write t as a polynomial in the t_i. Since $t_1 = 1$, we may assume that this polynomial does not have a constant term. Substituting (1) and then repeatedly substituting (2), we find that T is finitely generated by the x_i as a S_0 module.

Next, we note that S_0 is a noetherian ring. Since S_0 is finitely generated as an R-algebra, we have a surjective homomorphism of rings $\varphi\colon R[X_1, \dots, X_k] \to S_0$. Then S_0 is isomorphic to a quotient of $R[X_1, \dots, X_k]$, which is noetherian by the Basissatz. Quotients of noetherian rings are noetherian rings: indeed, $R[X_1, \dots, X_n]/\ker\varphi$ is a noetherian $R[X_1, \dots, X_n]$-module, which implies that it is a $R[X_1, \dots, X_n]/\ker\varphi$-module.

As a finitely generated module over a noetherian ring, we find that T is a noetherian S_0-module. Since S is an S_0-submodule of T, we find that S is finitely generated as a S_0-module.

This allows us to write every element of S as a polynomial in the generators of S as an S_0-module and the s_{ij} and s_{ijk}, so S is a finitely generated R-algebra. □

LEMMA 1.18 (Zariski's lemma). If k is a field, and R is a finitely generated k-algebra which is a field, then R is a finite-dimensional k-vector space (i.e., a finite algebraic extension of k).

PROOF. Denote the generators of R as a k-algebra by $x_1, \dots, x_n \in R$. Suppose that R is not a finite algebraic extension of k. Then we may reorder the x_i such that there is an $1 \leq m \leq n$ such that $x_1, \dots, x_m$ is a transcendence basis, i.e., $x_1, \dots, x_m$ are all transcendent, but $k(x_1, \dots, x_m) \subseteq R$ is finite algebraic.

Therefore we have $k \subseteq k(x_1, \dots, x_m) \subseteq R$, and Artin-Tate tells us that $k(x_1, \dots, x_m)$ is a finitely generated k-algebra, say with generators $q_1, \dots, q_k$, where $q_i = f_i/g_i$ for some $f_i, g_i \in k[x_1, \dots, x_n]$ and $g_i \neq 0$. This means that we can write every element $q \in k(x_1, \dots, x_m)$ as

$$q = \frac{f}{q_1^{e_1} \cdots q_k^{e_k}}.$$

However, since $k[x_1, \dots, x_n]$ is a UFD, we can see that

$$\frac{1}{q_1 \cdots q_k + 1}$$

is not of this form, a contradiction. □

THEOREM 1.19 (Hilbert's Nullstellensatz (weak version)). Let k be a field, T a finitely generated k-algebra, and m a maximal ideal of T. Then T/m is a finite algebraic extension of k. In particular, if k is algebraically closed, and T is the polynomial algebra, then maximal ideals m are of the form $(X_1 - a_1, \dots, X_n - a_n)$.

PROOF. Let m be a maximal ideal of T. Define $R \coloneqq T/m$. This is a field. By Zariski's lemma, $k \subseteq T/m$ is a finite algebraic extension. If k is algebraically closed and $T = k[X_1, \dots, X_n]$, then this means that the map natural map $\Phi\colon k \to k[X_1, \dots, X_n] \to k[X_1, \dots, X_n]/m$ is an isomorphism. Let $a_i \coloneqq \Phi^{-1}(X_i)$. Then we have that $I \coloneqq (X_1 - a_1, \dots, X_n - a_n) \subseteq \ker \Phi = m$.

On the other hand the natural map $k \to k[X_1, \dots, X_n]/I$ is injective, because the kernel is not trivial and k is a field, and it is surjective, because every polynomial in the quotient by I "reduces" to an element of k, so I is maximal, so $I = m$ since $m \supseteq I$ is a proper ideal. $\square$

THEOREM 1.20. Let k be an algebraically closed field, and R a finitely generated k-algebra. Then $N(R) = J(R)$. Thus if I is a radical ideal of $k[X_1, \dots, X_n]$ and $R = k[X_1, \dots, X_n]/I$ then the intersection of the maximal ideals of R is 0.

Furthermore, any radical ideal is the intersection of the maximal ideals containing it.

Minimal and associated primes

LEMMA 1.21. If R is a noetherian ring, then any ideal I contains a power of its radical $\sqrt{I}$.

For $I = (0)$, this means that $N(R)$ is nilpotent.

PROOF. Since R is noetherian, $\sqrt{I}$ is finitely generated, say by $x_1, \dots, x_n$. Then we find natural numbers m_i such that $x_i^{m_i}$. If we define $m \coloneqq 1 + \sum_{i=1}^n (m_i - 1)$, then the binomial theorem tells us that elements of the form $x_1^{r_1} \cdot \dots \cdot x_n^{r_n}$ with $\sum_{i=1}^n r_i = m$ generate the ideal $\sqrt{I}^m$. By our choice of m, for some i we must have $r_i \geq m_i$, so every generator lies in I, so $\sqrt{I}^m \subseteq I$. $\square$

LEMMA 1.22. If R is noetherian, then every radical ideal of I is the intersection of finitely many primes.

PROOF. Let $\mathcal{S}$ be the set of radical ideals that are not the intersection of finitely many prime ideals. Suppose that $\mathcal{S}$ is nonempty. Since R is noetherian, $\mathcal{S}$ has a maximal member I. We will show that I is prime (a contradiction, since I is not the intersection of finitely many prime ideals).

Indeed, if I is not prime, then there are ideals $J_1', J_2' \nsubseteq I$ such that $J_1' J_2' \subseteq I$ (indeed we can find principal ideals that work). Defining $J_1 \coloneqq J_1' + I$, $J_2 \coloneqq J_2' + I$, we find that $I \subsetneq J_i$, but $J_1 J_2 \subseteq I$. Since I was maximal, we can write

$$\sqrt{J_1} = Q_1 \cap \dots \cap Q_n, \qquad \sqrt{J_2} = Q_1' \cap \dots \cap Q_m',$$

where all Q_i, Q_i' are prime.

Now define

$$J \coloneqq \sqrt{J_1} \cap \sqrt{J_2} = Q_1 \cap \dots \cap Q_n \cap Q_1' \cap \dots \cap Q_m'.$$

From the preceding lemma, we obtain n_1 and n_2 such that $J^{n_1} \subseteq J_1^{n_1} \subseteq J_1$ and $J^{n_2} \subseteq J_2^{n_2} \subseteq J_2$. Then we have $J^{n_1+n_2} \subseteq J_1 J_2 \subseteq I$. Since $I \in \mathcal{S}$, I is a radical ideal, which means that $J \subseteq I$.

On the other hand, $I \subseteq J_i \subseteq \sqrt{J_i}$, so $I \subseteq J$.

This means that $I = J$ is the intersection of finitely many prime ideals, which is a contradiction to $I \in \mathcal{S}$. $\square$

REMARK. If we have written $\sqrt{I} = p_1 \cap \dots \cap p_m$ with p_i prime (as we have just seen is always possible), then we can remove any p_i from the list if it is a superset of one of the others. Therefore, we may assume that $p_i \nsubseteq p_j$ for all pairs $i \neq j$. Now if p is another prime ideal and $\sqrt{I} \subseteq p$, then $p_1 \cdot \dots \cdot p_m \subseteq \bigcap p_i = \sqrt{I} \subseteq p$, some since p is prime, one of the p_i must be fully contained in p.

Definition 1.23. The minimal primes p over an ideal I of a noetherian ring are those prime ideals such that if p' is a prime ideal and $I \subseteq p' \subseteq p$, then $p = p'$.

If I is radical and we choose p_i as in the previous remark, then p_i is a minimal prime: indeed, if p' is prime such that $I \subseteq p' \subseteq p_i$, then by the remark some p_j satisfies $p_j \subseteq p' \subseteq p_i$, but due to the way we chose the p_i this means that $i = j$ and $p' = p_i$.

Lemma 1.24. Let I be an ideal of a noetherian ring. Then $\sqrt{I}$ is the intersection of the minimal primes over I. Furthermore, there is a finite product of minimal primes over I that is contained in I.

Proof. If p is a prime over I, then $\sqrt{I} \subseteq p$ as p is prime. This implies that the minimal primes over I are exactly the minimal primes over $\sqrt{I}$, so the intersection of the minimal primes over I is the intersection of the minimal primes over $\sqrt{I}$, which is $\sqrt{I}$ itself.

By a previous remark, we can find minimal primes $p_1, \dots, p_n$ such that $p_1 \cdot \dots \cdot p_n \subseteq \sqrt{I}$. Since there is some m such that $\sqrt{I}^m \subseteq I$, we have that $p_1^m \cdot \dots \cdot p_n^m \subseteq I$ as required. $\square$

Example. Recall that the Nullstellensatz gives a bijection between radical ideals $\mathbb{C}[X_1, \dots, X_n]$ and algebraic subsets of $\mathbb{C}^n$.

If I is a radical ideal of $\mathbb{C}[X_1, \dots, X_n]$, then $(a_1, \dots, a_n)$ is a common zero of all $f \in I$ if and only if $I \subseteq (X_1 - a_1, \dots, X_n - a_n)$[1]. Consider the ideal

$$J := \bigcap_{(a_1,\dots,a_n) \in V(I)} (X_1 - a_1, \dots, X_n - a_n),$$

This is a radical ideal (TODO: why?). The bijection in the Nullstellensatz tells us that $I = J$. Therefore, we may write any radical ideal as the intersection of maximal ideals it is contained in, which are all of the form $(X_1 - a_1, \dots, X_n - a_n)$ (as we already know).

Furthermore, Hilbert's Nullstellensatz tells us that if $J \subseteq \mathbb{C}[X_1, \dots, X_n]$ is an ideal, then $N(\mathbb{C}[X_1, \dots, X_n]/J) = J(\mathbb{C}[X_1, \dots, X_n]/J)$.

Definition 1.25. Let R be a noetherian ring and let M be a finitely generated R-module. We call a prime ideal p an associated prime of M if it is the annihilator of an element of M, i.e., there is $m \in M$ such that $p = \operatorname{ann}(m) = \{r \in R \mid rm = 0\}$.

We further define

$$\operatorname{Ass}(M) := \{p \mid p \text{ prime}, \exists m \in M : p = \operatorname{ann}(m)\}.$$

Example. If p is a prime ideal of R, then $\operatorname{Ass}(R/p) = \{p\}$ Indeed, if $r \in R$, then there are two cases. If $r \in p$, then $\operatorname{ann}(r + p) = \operatorname{ann}(0) = R$, which is not prime. Otherwise, if $r \notin p$, then if $0 + p = (s + p)(r + p)$, we have $rs \in p$, and since p is prime and $r \notin p$, we have $s \in p$. Conversely, p is trivially contained in the annihilator, and we conclude that $\operatorname{ann}(r) = p$.

Definition 1.26. If M is an R-module, then we call a submodule N of M p-primary (or just primary) if $\operatorname{Ass}(M/N) = \{p\}$ for a prime ideal p. Since ideals are just submodules, the definition extends to ideals.

---

[1] Indeed, if $\{(a_1, \dots, a_n)\} \subseteq V(I)$, then $I = \sqrt{I} = I(V(I)) \subseteq I(\{(a_1, \dots, a_n)\}) = (X_1 - a_1, \dots, X_n - a_n)$. Conversely, if $I \subseteq (X_1 - a_1, \dots X_n - a_n)$, then $\{(a_1, \dots, a_n)\} \subseteq V(I)$. To see that $I(\{(a_1, \dots, a_n)\}) = (X_1 - a_1, \dots, X_n - a_n)$, note that "$\supseteq$" is clear, but the latter is maximal as we have seen before.

LEMMA 1.27. If $\operatorname{ann}(M) \coloneqq \bigcap_{m \in M} \operatorname{ann}(m) = p$ for some prime ideal p, then we have $p \in \operatorname{Ass}(M)$.

PROOF. Suppose M is gneerated by $m_1, \ldots, m_k$. Define $I_j \coloneqq \operatorname{ann}(m_j)$. Then

$$\prod I_j \subseteq \bigcap I_j = \bigcap \operatorname{ann}(m_j) = \operatorname{ann}(M) = p.$$

Since p is prime, this forces $I_j \subseteq p$, but $p = \operatorname{ann}(M) \subseteq \operatorname{ann}(m_j) = I_j$, so $p = I_j$, hence $p \in \operatorname{Ass}(M)$. □

LEMMA 1.28. Let Q be maximal amogst the annihilators of nonzero elements of M. Then Q is prime, hence $Q \in \operatorname{Ass}(M)$.

PROOF. Let $Q \in \operatorname{ann}(m)$ and $r_1 \cdot r_2 \in Q$, but $q_2 \notin Q$. We will show that $r_1 \in Q$. Since $r_1 r_2 \in Q$ we have $r_1 r_2 m = 0$. This means that $r_1 \in \operatorname{ann}(r_2 m)$. Since, $r_2 \notin Q$, we have that $r_2 m \neq 0$.

We have $Q = \operatorname{ann}(m) \subseteq \operatorname{ann}(r_2 m)$, and since $r_2 m$ is nonzero as we have just seen, by maximality of Q, we have $Q = \operatorname{ann}(r_2 m)$. Hence, $r_1 \in \operatorname{ann}(r_2 m) = Q$ as required. □

LEMMA 1.29. Let M be a nonzero finitely generated module over a noetherian ring R. Then there is a chain

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_t = M$$

of submodules with $M_i / M_{i-1} \cong R/p_i$ for some prime ideal p_i.

PROOF. By the previous lemma we find $0 \neq m_1 \in M$ such that $\operatorname{ann}(m_1)$ is a prime ideal. Set $M_1 = Rm_1$. Then the kernel of the map $R \to M_1$ given by $r \mapsto rm_1$ is precisely $\operatorname{ann}(m_1)$, so $M_1 \cong R/p_1$ (as R-modules).

Similarly, if M_i is a proper submodule of M, then we find $m_{i+1} + M_i \in M/M_i$ such that $\operatorname{ann}(m_{i+1} + M_i)$ is a prime ideal. Set $M_{i+1} \coloneqq M_i + Rm_{i+1}$. Then the map $R \to M_{i+1}/M_i$ given by $r \mapsto rm_{i+1} + M_i$ is surjective and has kernel $\operatorname{ann}(m_{i+1} + M_i)$. Furthermore, $m_{i+1} \notin M_i$, since otherwise the annihilator of $m_{i+1} + M_i$ would be all of R. Therefore, M_i is a proper submodule of M_{i+1}.

By the ascending chain condition, this process terminates. □

LEMMA 1.30. If N is a submodule of a finitely generated module M over a noetherian ring R, then $\operatorname{Ass}(M) \subseteq \operatorname{Ass}(N) \cup \operatorname{Ass}(M/N)$.

PROOF. Let $\operatorname{ann}(m) \in \operatorname{Ass}(M)$ for some $m \in M$. Define $M_1 \coloneqq Rm \cong R/\operatorname{ann}(m)$.

Let $rm \in M_1$. It is trivial that $\operatorname{ann}(m) \subseteq \operatorname{ann}(rm)$. Conversely, if $s \in \operatorname{ann}(rm)$, then $srm = 0$, but $\operatorname{ann}(m)$ is prime and $rm \neq 0$, so we must have $s \in \operatorname{ann}(m)$. Hence $\operatorname{ann}(rm) = \operatorname{ann}(m)$.

Now if $M_1 \cap N \neq 0$, then by what we just saw there is $rm \in M_1 \cap N$ with $\operatorname{ann}(rm) = \operatorname{ann}(m)$, so $\operatorname{ann}(m) \in \operatorname{Ass}(N)$.

On the other hand, if $M_1 \cap N = 0$, then $r \in \operatorname{ann}(m + N)$ iff $r \cdot m \in N$ iff $r \cdot m = 0$, so $\operatorname{ann}(m) = \operatorname{ann}(m + N) \in \operatorname{Ass}(M/N)$. □

LEMMA 1.31. If R is a notherian ring and M is finitely generated, then $\operatorname{Ass}(M)$ is finite.

PROOF. Take a chain

$$M_0 = 0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_t = M.$$

such that $M_{i+1}/M_i \cong R/p_i$ for $i \geq 0$.

We will show inductively that $M_{i+1} = 0$ for $i \geq 0$. Indeed, if $i = 0$, then $M_i \cong R/p_0$, and we have previously calculated that $\operatorname{Ass}(R/p_0) = \{p_0\}$.

If $i > 0$, then M_i is a submodule of M_{i+1}. By the previous lemma, we have $\mathrm{Ass}(M_{i+1}) \subseteq \mathrm{Ass}(M_i) \cup \mathrm{Ass}(M_{i+1}/M_i)$. The former is finite by the inductive hypothesis, while the latter is a one-element set. □

Proposition 1.32. Each minimal prime over an ideal I is an associated prime of R/I.

Proof. By (1.24), we find minimal primes $p_1, \ldots, p_n$ and natural numbers $s_1, \ldots, s_n$ such that $p_1^{s_1} \cdot \cdots \cdot p_n^{s_n} \subseteq I$. Additionally, we may assume that $i \neq j$ implies $p_i \neq p_j$.

Define
$$M := (p_2^{s_2} \cdot \cdots \cdot p_n^{s_n} + I)/I$$
and let $J := \mathrm{ann}(M)$. Clearly, every element of $p_1^{s_1}$ annihilates M, so $p_1^{s_1} \subseteq J$. Furthermore, we have
$$Jp_2^{s_2} \cdot \cdots \cdot p_n^{s_n} \subseteq I \subseteq p_1,$$
but p_1 is prime and we cannot have $p_i^{s_i} \subseteq p_1$ for $i \neq 1$ as the p_i are minimal primes, so we must have $J \subseteq p_1$. In particular, $J \neq R$, so $M \neq 0$.

Invoke (1.29) to obtain a chain
$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_t = M$$
of submodules with $M_i/M_{i-1} \cong R/q_i$ for some prime ideal q_i.

Since $p_1^{s_1}$ annihilates M, in particular it annihilates M_j/M_{j-1} for every j. So we have $p_1^{s_1} \subseteq \mathrm{ann}(M_j/M_{j-1}) = \mathrm{ann}(R/q_j) = q_j$ for every j. Since q_j is prime, we conclude $p_1 \subseteq q_j$ for every j.

On the other hand, $\prod q_j \subseteq J$: by induction on j assume that $\prod_{k=1}^{j} q_k$ annihilates M_j. If $x \in M_{j+1}$ and $r \in \prod k = 1^j q_k$, and $s \in q_{j+1}$ then $sx \in M_j$, since q_{j+1} annihilates M_{j+1}/M_j. By the inductive hypothesis, $rsx = 0$, so $\prod_{k=1}^{j+1} q_j$ annihilates M_{j+1}.

Hence $\prod q_j \subseteq J \subseteq p_1$, so there is some j such that $q_j \subseteq p_1$, but we have seen that $p_1 \subseteq q_j$, so there is j such that $q_j = p_1$. Let j be the least such j. In particular, $\prod_{k<j} q_k \subsetneq p_1$.

We will now show that $p_1 \in \mathrm{Ass}(M)$. For this, take $x \in M_j \setminus M_{j-1}$. If $j = 1$, then $\mathrm{ann}(x) = p_1$ (since $M_1 \cong R/p_1$), but $x \in M \subseteq R/I$, so $p_1 \in \mathrm{Ass}(R/I)$.

On the other hand, if $j > 1$, choose some $r \in (\prod_{k<j} q_k) \setminus p_1$ (this is indeed nonempty, since otherwise one of the q_k would be contained in p_1). Note that if $s \in p_1 = q_j$, then $r(sx) = 0$ (this is just the induction we did earlier). So we have $s(rx) = 0$, which means that we have $p_1 \subseteq \mathrm{ann}(rx)$.

Note that $\mathrm{ann}(rx + M_{j-1}) = p_1$ since $rx + M_{j-1} \neq 0$, but $M_j/M_{j-1} \cong R/q_j = R/p_1$. Since $r \notin p_1$, we conclude that $rx \notin M_{j-1}$. Now if $s \in \mathrm{ann}(rx)$, then certainly $s \in \mathrm{ann}(rx + M_{j-1}) = p_1$, so $\mathrm{ann}(rx) \subseteq p_1$.

Putting the last two paragraphs together, we have $\mathrm{ann}(rx) = p_1$, so $p_1 \in \mathrm{Ass}(M) \subseteq \mathrm{Ass}(R/I)$.

By changing the order of the p_i, we see that $p_j \in \mathrm{Ass}(R/I)$ for every j, completing the proof. □

Example 1.33. The converse of the previous theorem fails in general. For example, take $R = k[X, Y]$, $p = (X, Y) > q = (X)$ and $I = pq = (X^2, XY)$.

We have $\sqrt{I} = q$. Since this is a prime, (1.24) tells us that q is the only minimal prime over q. It is possible to show that $\mathrm{Ass}(R/I) = \{p, q\}$. In particular, I is not primary, but we can write
$$I = (X^2, XY, Y^2) \cap (X),$$
where $(X^2, XY, Y^2) = (X, Y)^2$ is p-primary and (X) is q-primary. This is an example of a primary decomposition.

DEFINITION 1.34. If R is a noetherian ring, M is a finitely generated R-module and $N \subseteq M$ is a submodule, then a primary decomposition of N consists of submodules $N_1, \dots, N_s$ of M containing N such that N_i is p_i-primary, where the p_i are pairwise distinct, such that $N = \bigcup_{i=1}^{n} N_i$ (in particular, this means that there is an embedding $M/N \to \bigoplus M/N_i$).

REMARK. This primary decomposition exists (which we will not show) and is not necessarily unique. However, Atiyah-Macdonald Chapter 4 contains two uniqueness theorems for finitely generated modules over noetherian rings:

(1) the p_i occurring in a primary decomposition are unique and are precisely $\mathrm{Ass}(M/N)$;
(2) the N_j belonging to p_j which are minimal elements of the set $\{p_i\}$ are unique. The N_j belonging to the rest of the p_j (which are called embedded), are not necessarily unique.

In the previous example, q is minimal and p is embedded, Hence, the ideal (X) is unique and the decomposition shows that $\mathrm{Ass}(R/I) = \{p, q\}$, which is rather tricky to prove from first principles.

CHAPTER 2

Localisation

Remark. As always, all rings R are commutative with unity.

Let S be a multiplicatively closed subset of R (i.e., S is closed under multiplication and $1 \in S$. We define a relation $\equiv$ on $R \times S$ by saying that $(r_1, s_1) \equiv (r_2, s_2) \iff \exists x \in S\colon (r_1 s_2 - r_2 s_1)x = 0$. Reflexivity and symmetry are immediate, for transitivity, assume that

$$(r_1 s_2 - r_2 s_1)x = 0 = (r_2 s_3 - r_3 s_2)y.$$

Multiplying the left hand side with $s_3 y$ and the right hand side with $s_1 x$ and the subtracting the two yields the desired identity

$$(r_1 s_3 - r_3 s_1)s_2 xy = 0,$$

since $s_2 xy \in S$.

This shows that $\equiv$ is an equivalence relation, and we will denote equivalence classes of (r_1, s_1) by $\frac{r_1}{s_2}$ and the quotient by $S^{-1}R$. We make $S^{-1}R$ into a ring by setting

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{r_1 s_2 + r_2 s_1}{s_1 s_2},$$
$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}.$$

Furthermore, we have a ring homohmorphism $R \to S^{-1}R$ given by $r \mapsto \frac{r}{1}$.

Lemma 2.1. Let $\varphi\colon R \to T$ be a ring homomorphism with $\varphi(s)$ a unit int T for all $s \in S$. Then there is a unique homomorphism of rings $\alpha\colon S^{-1}R \to T$ such that $\varphi = \alpha \circ \theta$, i.e., the diagram

$$\begin{tikzcd} R \arrow[r, "\theta"] \arrow[dr, "\varphi"'] & S^{-1}R \arrow[d, dotted, "\exists!\alpha"] \\ & T \end{tikzcd}$$

is commutative.

Proof. We will first show uniqueness. Suppose we have $\alpha\colon S^{-1}R \to T$ satisfying $\alpha \circ \theta = \varphi$.

Then we have

$$\forall r \in R\colon \alpha(\frac{r}{1}) = \alpha(\theta(r)) = \varphi(r),$$
$$\forall s \in S\colon \alpha((\frac{s}{1})^{-1}) = \alpha(\frac{s}{1})^{-1} = \alpha(\theta(s))^{-1} = \varphi(s)^{-1}.$$

Thus, $\alpha(\frac{r}{s}) = \alpha(\frac{r}{1})\alpha(\frac{1}{s}) = \varphi(r)\varphi(s)^{-1}$ is uniquely determined by φ.

For existence, we define $\alpha(\frac{r}{s}) := \varphi(r)\varphi(s)^{-1}$. We need to show that this is well-defined. If $\frac{r_1}{s_1} = \frac{r_2}{s_2}$, then we find $x \in S$ such that $(r_1 s_2 - r_2 s_1)x = 0$. Applying φ, we find $(\varphi(r_1)\varphi(s_2) - \varphi(r_2)\varphi(s_1))\varphi(x) = 0$. Since $\varphi(x)$ is a unit, we can cancel it and since the $\varphi(s_i)$ are units, we can rewrite this two the required relation $\varphi(r_1)\varphi(s_1)^{-1} = \varphi(r_2)\varphi(s_2)^{-1}$.

It is also possible to check that α is indeed a homomorphism of rings. $\square$

Example. (1) If R is an integral domain and $S = R \setminus \{0\}$, then $S^{-1}R$ is just the field of fractions of R.
(2) We have that $S^{-1}R$ is the zero ring if and only if $0 \in S$.
(3) If I is an ideal of R, then $S = 1 + I$ is multiplicatively closed.
(4) Let p be a prime ideal. Then $S = R \setminus p$ is multiplicatively closed (indeed, if $x, y \in S$, then if $xy \in R \setminus S = p$, then $x \in p = R \setminus S$ or $y \in p = R \setminus S$, which is not possible). We write R_p for $S^{-1}R$, and the process of passing from R to R_p is called localisation at p. The elements $\frac{r}{s}$ with $r \in p$ form an ideal of R_p. This is a unique maximal ideal in R_p: if $\frac{r}{s}$ satisfies $r \notin p$, then $r \in S$, so $\frac{r}{s}$ has an inverse in R_p and is not part of any maximal ideal.

Definition 2.2. A ring with a unique maximal ideal is called local.

Remark. Some authors require a local ring to also be noetherian. We do not.

Example. (1) Let $R = \mathbb{Z}$, and p prime number. Then (p) is a prime ideal, and we have $R_{(p)} = \{\frac{m}{n} \mid p \nmid n\} \subseteq \mathbb{Q}$.
The maximal ideal is given by $\{\frac{m}{n} \mid p \mid m, p \nmid n\}$.
(2) Let $R = k[X_1, \ldots, X_n]$, $p = (X_1 - \alpha_1, \ldots, X_n - \alpha_n)$. Then we can interpret R_p as a subring of $k(X_1, \ldots, X_n)$ consisting of those rational functions that are defined at $(\alpha_1, \ldots, \alpha_n) \in k^n$, and the unique maximal ideal consists of those rational functions which are zero at $(\alpha_1, \ldots, \alpha_n)$.

1. Localization of modules

Definition. Given a left R-module M, define a relation $\equiv$ on $M \times S$, where S is a multiplicatively closed subset $S \subseteq R$ by

$$(m_1, s_1) \equiv (m_2, s_2) \iff \exists x \in S\colon x(m_1 s_2 - m_2 s_1) = 0.$$

This is again an equivalence relation with $\frac{m}{s}$ denoting the equivalence class of (m, s). The quotient is denoted by $S^{-1}M$. $S^{-1}M$ has the structure of an $S^{-1}R$-module via

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} := \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}$$
$$\frac{r_1}{s_1}\frac{m_2}{s_2} = \frac{r_1 m_2}{s_1 s_2}.$$

Again, we write M_p in the case $S = R \setminus p$ for a prime ideal p.

If $\theta\colon M_1 \to M_2$ is an R-linear map, then an $S^{-1}R$-linear map $S^{-1}\theta\colon S^{-1}M_1 \to S^{-1}M_2$ is given by $\frac{m_1}{s} \mapsto \frac{\theta(m_1)}{s}$. This is functorial in the sense that if $\varphi\colon M_2 \to M_3$ is another R-linear map then $S^{-1}(\varphi \circ \theta) = S^{-1}\varphi \circ S^{-1}\theta$.

Lemma 2.3. If

$$M_1 \xrightarrow{\theta} M \xrightarrow{\varphi} M_2$$

is exact at M, then

$$S^{-1}M_1 \xrightarrow{S^{-1}\theta} S^{-1}M \xrightarrow{S^{-1}\varphi} S^{-1}M_2$$

is exact at $S^{-1}M$.

Proof. By functoriality, we have

$$(S^{-1}\varphi) \circ (S^{-1}\theta) = S^{-1}(\varphi \circ \theta) = S^{-1}0 = 0,$$

hence $\operatorname{im}(S^{-1}\theta) \subseteq \ker(S^{-1}\varphi)$.

Now suppose $\frac{m}{s} \in \ker(S^{-1}\varphi) \subseteq S^{-1}M$. This means that $\frac{\varphi(m)}{s} = 0$ in $S^{-1}M_2$. By definition of localization, this means that there is $t \in S$ such that $t\varphi(m) = 0$ in

M_2. By linearity, $0 = t\varphi(m) = \varphi(tm)$, hence $tm \in \ker\varphi = \operatorname{im}\theta$, so we find $m_1 \in M_1$ such that $\theta(m_1) = tm$. Then we can calculate in $S^{-1}M$ that

$$\frac{m}{s} = \frac{tm}{ts} = \frac{\theta(m_1)}{ts} = (S^{-1}\theta)(\frac{m_1}{ts}),$$

hence $\frac{m}{s} \in \operatorname{im} S^{-1}\theta$, and we conclude that $\ker S^{-1}\varphi = \operatorname{im} S^{-1}\theta$ as claimed. □

Remark. If $N \subseteq M$ is a submodule, then $S^{-1}N \subseteq S^{-1}M$ is a submodule in the natural way. In particular, if $I \subseteq R$ is an ideal, then $S^{-1}I$ is an ideal of $S^{-1}R$.

Lemma 2.4. Let $N \subseteq M$ be a submodule. Then $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.

Proof. Applying the previous lemma to the short exact sequence

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{\varepsilon} M/N \longrightarrow 0$$

yields exactness of

$$0 \longrightarrow S^{-1}N \xrightarrow{S^{-1}\iota} S^{-1}M \xrightarrow{S^{-1}\varepsilon} S^{-1}(M/N) \longrightarrow 0.$$

Since $S^{-1}\iota$ is just the inclusion $S^{-1}N \subseteq S^{-1}M$, we find that $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$. □

Lemma 2.5. (i) Every ideal in $S^{-1}R$ is of the form $S^{-1}I$ for some ideal I of R.
(ii) The prime ideals of $S^{-1}R$ are in one-to-one correspondence with the prime ideals of R that do not meet S.

Proof. For the first part, let J be an ideal of $S^{-1}R$ and define $I \coloneqq \{r \in R \mid \frac{r}{1} \in J\}$. This is clearly an ideal. Now if $\frac{r}{s} \in J$, then $\frac{r}{1} = \frac{s}{1}\frac{r}{s} \in J$, hence $r \in I$, so $\frac{r}{s} \in S^{-1}I$ and $J \subseteq S^{-1}I$.

Conversely, if $\frac{r}{s} \in S^{-1}I$, i.e., $r \in I$ and $s \in S$, then $\frac{r}{1} \in J$, so $\frac{r}{s} = \frac{1}{s}\frac{r}{1} \in J$.

Hence, $S^{-1}I = J$, completing the first part.

Let q be a prime ideal of $S^{-1}R$ and set $p \coloneqq \{r \in R \mid \frac{r}{1} \in q\}$. By the previous part, p is an ideal and $q = S^{-1}p$.

The ideal p is prime, since if $xy \in p$, then $\frac{xy}{1} = \frac{x}{1}\frac{y}{1} \in q$, so either $\frac{x}{1}$ or $\frac{y}{1}$ is in q, hence, $x \in p$ or $y \in p$.

Furthermore, we have $p \cap S = \varnothing$, since if $r \in S \cap p$, then $\frac{r}{1} \in q$ by definition of p and $\frac{1}{r}$ is valid element of $S^{-1}R$, so $1 = \frac{1}{r}\frac{r}{1} \in q$ since q is an ideal, but q is prime, so $1 \neq q$, a contradiction.

Conversely, if p is a prime ideal of R that does not meet S. If $\frac{r}{s}, \frac{x}{y} \in S^{-1}R$ such that $\frac{rx}{sy} \in S^{-1}p$, then by definition of localisation we have $zrx \in p$ for some $z \in S$. Since $z \in S$, we have $z \notin p$, so since p is prime, we must have $rx \in p$. Again since p is prime, we find that $r \in p$ or $x \in p$, so $\frac{r}{s} \in S^{-1}p$ or $\frac{x}{y} \in S^{-1}p$, so $S^{-1}p$ is prime.

Hence, the mappings $p \mapsto S^{-1}p$ and $q \mapsto \{r \in R \mid \frac{r}{1} \in q\}$ are inverse bijections (one half is given by the first part of the proof, the other half is obvois) the preserve primality in both directions. □

Lemma 2.6. If R is noetherian, then $S^{-1}R$ is noetherian.

Proof. Using the previous lemma, a chain $J_1 \subseteq J_2 \subseteq \ldots$ in $S^{-1}R$ lifts to a chain $I_1 \subseteq I_2 \subseteq \ldots$ in R such that $J_i = S^{-1}I_i$ for each i. Since R is noetherian, the chain $\{I_i\}$ terminates, so the chain $\{J_i\} = \{S^{-1}I_i\}$ must terminate as well. □

Definition 2.7. A propert P of a ring R or R-module M is called local if R or M has the property P if and only if R_p (resp. M_p) has property P for each prime ideal p of R.

Exercises

Example Sheet 1

Exercise 1.

LEMMA. Let R and S be (commutative unital) rings. Denote by $\mathcal{I}_R$ the set of ideals of R. Then there is a bijective correspondence

$$\begin{aligned} \mathcal{I}_{R\times S} &\leftrightarrow \mathcal{I}_R \times \mathcal{I}_S, \\ I &\mapsto (\pi_1(I), \pi_2(I)), \\ I_1 \times I_2 &\leftarrow\!\shortmid (I_1, I_2). \end{aligned}$$

PROOF. We need to show the following.

(i) If I is an ideal of $R \times S$, then $\pi_1(I)$ is an ideal of R and $\pi_2(I)$ is an ideal of S,

(ii) if I_1 is an ideal of R, I_2 is an ideal of S, then $I_1 \times I_2$ is an ideal of $R \times S$,

(iii) if I is an ideal of $R \times S$, then $I = \pi_1(I) \times \pi_2(I)$ and

(iv) if I_1 is an ideal of R, I_2 is an ideal of S, then $I_1 = \pi_1(I_1 \times I_2)$ and $I_2 = \pi_2(I_1 \times I_2)$.

Indeed (i) follows from surjectivity of the projection and (ii) and (iv) are obvious. It remains to show (iii).

If $(r, s) \in I$, then $r = \pi_1((r, s)) \in \pi_1(I)$ and $s = \pi_2((r, s)) \in \pi_2(I)$, so $(r, s) \in \pi_1(I) \times \pi_2(I)$.

Conversely, if $(r, s) \in \pi_1(I) \times \pi_2(I)$, then there are r', s' such that $(r, s') \in I$ and $(r', s) \in I$. We conclude that $(r, s) = (r, s') \cdot (1, 0) + (r', s) \cdot (0, 1) \in I$. □

EXERCISE. The direct product of finitely many noetherian rings is noetherian.

SOLUTION. Since the terminal object in the category of rings is the zero ring, which is noetherian, by induction it suffices to show that if R and S are noetherian, then $R \times S$ is noetherian.

Let I be an ideal of $R \times S$. We have to show that I is finitely generated. By the Lemma, $I = I_1 \times I_2$ for an ideal I_1 of R and an ideal I_2 of S. Since R and S are noetherian, I_1 is finitely generated, say by $r_1, \dots, r_n$ and so is I_2, say by $s_1, \dots, s_m$. Then if $(r, s) \in I_1 \times I_2$, we have

$$(r, s) = (\sum_{i=1}^{n} \lambda_i r_i, \sum_{i=1}^{m} \lambda_i' s_i) = \sum_{i=1}^{n} (\lambda_i, 0)(r_i, 0) + \sum_{i=1}^{m} (0, \lambda_i')(0, s_i),$$

so $I_1 \times I_2$ is finitely generated by $(r_1, 0), \dots, (r_n, 0), (0, s_1), \dots, (0, s_n)$. □

Exercise 3.

EXERCISE. The set of prime ideals in a non-zero rings possesses a minimal member with respect to inclusion.

SOLUTION. Denote the set of prime ideals of A by $\mathcal{S}$. Since A is nonzero, (0) is a proper ideal, which is contained in a maximal ideal, hence $\mathcal{S}$ is nonempty.

The set $\mathcal{S}$ is partially ordered using the relation "$\supseteq$". Let $\mathcal{S}' \subseteq \mathcal{S}$ denote a totally ordered subset of $\mathcal{S}$. We will show that $\mathcal{S}'$ admits an upper bound. Indeed, define $S := \bigcap_{P \in \mathcal{S}'} P$. S is obviously an ideal, and we will show that it is prime. Assume that $x, y \in A$ such that $xy \in S$. Since every $P \in \mathcal{S}'$ is prime, we may write $\mathcal{S}' = \mathcal{S}_x \cup \mathcal{S}_y$, where $\mathcal{S}_x := \{P \in \mathcal{S}' \mid x \in P\}$ and $\mathcal{S}_y := \{P \in \mathcal{S}' \mid y \in P\}$. We claim that it is true that

$$(\forall P \in \mathcal{S}'\ \exists P' \in \mathcal{S}_x \colon P' \subseteq P) \vee (\forall P \in \mathcal{S}'\ \exists P' \in \mathcal{S}_y \colon P' \subseteq P). \tag{$\star$}$$

Indeed, the negation of this statement is

$$(\exists P \in \mathcal{S}'\ \forall P' \in \mathcal{S}_x \colon P' \nsubseteq P) \wedge (\exists Q \in \mathcal{S}'\ \forall Q' \in \mathcal{S}_y \colon Q' \nsubseteq Q),$$

but then $P \cap Q$, which is either P or Q, since $\mathcal{S}'$ is totally ordered, is part of neither $\mathcal{S}_x$ nor $\mathcal{S}_y$, which is a contradiction.

Therefore, without loss of generality, we may assume that the left hand side of ($\star$) is true (the case where the right hand side is true works exactly the same). Since $P' \in \mathcal{S}_x$ and $P' \subseteq P$ implies $P \in \mathcal{S}_x$, we have that $\mathcal{S}' = \mathcal{S}_x$, so $x \in S$, and S is indeed a prime ideal, and therefore every chain in $\mathcal{S}$ admits an upper bound.

Applying Zorn's lemma gives a maximal element of $\mathcal{S}$, which is precisely a minimal prime ideal of A. □

Exercise 7.

Exercise. Let M be a noetherian A-module and θ be an endomorphism.

(i) If θ is surjective, then it is an isomorphism.
(ii) If M is artinian and θ is injective, then it is an isomorphism.

[Hint: in (i) consider the submodules $\ker \theta^n$; in (ii), consider the quotient modules $\operatorname{coker} \theta^n$.]

Solution. For (i), assume that θ is not injective. Then there is some $x \in \ker \theta \setminus \{0\}$. Let $n \in \mathbb{N}$. Since θ is surjective, so is θ^n, so there is some $y \in M$ such that $\theta^n(y) = x$. Therefore, $y \in \ker \theta^{n+1} \setminus \ker \theta^n$ and we have an infinite strictly increasing chain

$$\ker \theta \subsetneq \ker \theta^2 \subsetneq \ker \theta^3 \subsetneq \cdots .$$

For (ii), assume that θ is not surjective. This means that there is some $x \notin \operatorname{im} \theta$. Let $n \in \mathbb{N}$. Then we have $\theta^n(x) \in \operatorname{im} \theta^n$. Suppose that $\theta^n(x) \in \operatorname{im} \theta^{n+1}$. Then there would be $y \in M$ such that $\theta^{n+1}(y) = \theta^n(x)$. By injectivity of θ, this means that $\theta(y) = x$, a contradiction. Therefore, $\theta^n(x) \in \operatorname{im} \theta^n \setminus \operatorname{im} \theta^{n+1}$ and we have an infinite strictly decreasing chain

$$\operatorname{im} \theta \supsetneq \operatorname{im} \theta^2 \supsetneq \operatorname{im} \theta^3 \supsetneq \cdots .$$ □

Exercise 10.

Exercise. An element r lies in the Jacobson radical of A iff $1 - rs$ is a unit for all s in A.

Solution. Let $r \in J(A)$ and $s \in A$. Then $rs \in J(A)$, so rs is contained in every maximal ideal of A. If $1 - rs$ were contained in a maximal ideal M, then we would have $1 \in M$, a contradiction. So $1 - rs$ is not contained in any maximal ideal, so $(1 - rs)$ is not contained in any maximal ideal, so we must have $(1 - rs) = (1)$, hence $1 - rs$ is a unit.

Conversely, assume that $1 - rs$ is a unit for every s, and let M be a maximal ideal of A. Suppose that $r \notin M$. Then $A = M + Ar$, so we find $m \in M$ and $s \in A$ such that $1 = m + rs$, but then $m = 1 - rs$ is a unit, a contradiction. Hence $r \in M$ and therefore $r \in J(R)$. □