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 5
Links between commutative algebra and algebraic geometry 6
Dimension 6

Chapter 1. Noetherian Rings 9
Minimal and associated primes 16

Chapter 2. Localisation 21
1. Localization of modules 22
2. A proof of the Nullstellensatz 24

Chapter 3. Tensor products 27
1. Restriction and extension of scalars 29

Chapter 4. Integrality and dimension 33
1. Integral extensions 34
2. Transcendence Degree 38

Exercises 43
Example Sheet 1 43
Example Sheet 2 49

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 $k[X_1, \ldots, X_n]$, 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 $\{1, \ldots, n\}$. Σ_n acts on $k[X_1, \ldots, X_n]$ by permuting variables: given $\sigma \in \Sigma_n$, $f \in k[X_1, \ldots, X_n]$, we set

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

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

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

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

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

It turns out that S is generated as a ring by these e_i and the canonical map $k[Y_1, \ldots, Y_n] \to S$ 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 $N_1 \subseteq N_2 \subseteq \ldots$ 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 $m_1, \ldots, m_k$. 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 $N = L$. □

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 $x_1, \ldots, x_r$. Then Q/N is generated by $x_1 + N, \ldots, x_r + N$.

Conversely, if both N and M/N are noetherian, and $L_1 \subseteq L_2 \subseteq \ldots$ 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. □

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 $b_1, \ldots, b_n$. 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 $c_1, \ldots, c_n$. Additionally, $f^{-1}(N)$ is finitely generated, say by $a_1, \ldots, a_m$. Pick preimages $b_1, \ldots, b_n$ 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 $N = \langle b_1, \ldots, b_n, f(a_1), \ldots, f(a_m) \rangle$ as required. □

Lemma 1.4. Let $M, N, M_1, \ldots$ 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

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

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 $m_1, \ldots, m_n$. 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 $\forall n \geq N : R_n = R_N$. 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 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 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. $\square$

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

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

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. $\square$

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 $T = Sx_1 + \cdots + Sx_m$. 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. ☐

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 $\sqrt{I}^m \subseteq I$. ☐

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 $J_1', J_2' \not\subseteq I$ 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 $I \in \mathcal{S}$. ☐

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 $p_1 \cdot \cdots \cdot p_m \subseteq \bigcap p_i = \sqrt{I} \subseteq p$, 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 $p_1, \ldots, p_n$ such that $p_1 \cdot \cdots \cdot p_n \subseteq \sqrt{I}$. Since there is some m such that $\sqrt{I}^m \subseteq I$, we have that $p_1^m \cdot \cdots \cdot p_n^m \subseteq I$ as required. $\square$

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

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

$$J \coloneqq \bigcap_{(a_1,\ldots,a_n) \in V(I)} (X_1 - a_1, \ldots, X_n - a_n),$$

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 $(X_1 - a_1, \ldots, X_n - a_n)$ (as we already know).

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

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

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

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 $\{(a_1, \ldots, a_n)\} \subseteq V(I)$, then $I = \sqrt{I} = I(V(I)) \subseteq I(\{(a_1, \ldots, a_n)\}) = (X_1 - a_1, \ldots, X_n - a_n)$. Conversely, if $I \subseteq (X_1 - a_1, \ldots X_n - a_n)$, then $\{(a_1, \ldots, a_n)\} \subseteq V(I)$. To see that $I(\{(a_1, \ldots, a_n)\}) = (X_1 - a_1, \ldots, X_n - a_n)$, 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 $p_1, \dots, p_n$ and natural numbers $s_1, \dots, s_n$ such that $p_1^{s_1} \cdot \dots \cdot p_n^{s_n} \subseteq I$. Additionally, we may assume that $i \neq j$ implies $p_i \neq p_j$.

Define

$$M := (p_2^{s_2} \cdot \dots \cdot p_n^{s_n} + I)/I$$

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

$$Jp_2^{s_2} \cdot \dots \cdot p_n^{s_n} \subseteq I \subseteq p_1,$$

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

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

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 in 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 $R = k[X_1, \dots, X_n]$, $p = (X_1 - \alpha_1, \dots, X_n - \alpha_n)$. Then we can interpret R_p as a subring of $k(X_1, \dots, X_n)$ consisting of those rational functions that are defined at $(\alpha_1, \dots, \alpha_n) \in k^n$, and the unique maximal ideal consists of those rational functions which are zero at $(\alpha_1, \dots, \alpha_n)$.

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 $I := \{r \in R \mid \frac{r}{1} \in J\}$. 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 $p := \{r \in R \mid \frac{r}{1} \in q\}$. 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, let p be 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 obvious) that 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 property 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.

Lemma 2.8. The following are equivalent for an R-module M.

(i) $M = 0$,
(ii) for all prime ideals p, we have $M_p = 0$,
(iii) for all maximal ideals q, we have $M_q = 0$.

Proof. It is obvious that (i) implies (ii) and (ii) implies (iii), so it will suffice to show that (iii) implies (i). Indeed, suppose that $M_q = 0$ for every maximal ideal q, but $M \neq 0$.

Let $0 \neq m \in M$. The annihilator $\{r \in R \mid rm = 0\}$ of m is a proper ideal of R, hence it is contained in a maximal ideal q of R. Since M_q is trivial, we have $\frac{m}{1} = 0$ in M_q, so there is some $s \in R \setminus q$ such that $sm = 0$ in R. But since $s \notin q$, we have $s \notin \operatorname{ann}(m)$, i.e., $sm \neq 0$, a contradiction. □

Lemma 2.9. Let $\varphi\colon M \to N$ be a homomorphism of R-modules. The following are equivalent.

(i) φ is injective,
(ii) $\varphi_p\colon M_p \to N_p$ is injective for all primes p of R,
(iii) $\varphi_q\colon M_q \to N_q$ is injective for all maximal ideals q of R.

Proof. (i) implies (ii) by exactness of localization. It is obvious that (ii) implies (iii).

Now assume that φ_q is injective for all maximal ideals q. The sequence

$$0 \longrightarrow \ker\varphi \xrightarrow{\ \iota\ } M \xrightarrow{\ \varphi\ } N$$

is exact. Hence

$$0 \longrightarrow (\ker\varphi)_q \xrightarrow{\ \iota_q\ } M_q \xrightarrow{\ \varphi_q\ } N_q$$

is exact for every maximal ideal q. By exactness, $(\ker\varphi)_q$ is isomorphic to $\ker\varphi_q$, which is trivial by assumption. Hence $(\ker\varphi)_q$ is trivial for every maximal ideal q, so by the previous result, we have $\ker\varphi = 0$ as required. □

Lemma 2.10. Let p be a prime ideal of R and S a multiplicatively closed subset of R such that $S \cap p = \varnothing$. By (2.5), $S^{-1}p$ is a prime ideal of $S^{-1}R$. Then $(S^{-1}R)_{S^{-1}p} \cong R_p$. In particular, if q is a prime ideal of R with $p \subseteq q$, then $(R_q)_{p_q} \cong R_p$, by taking $S = R \setminus q$.

Proof. On the second exercise sheet. □

2. A proof of the Nullstellensatz

Remark. Let k be a field and R a k-algebra which is also an integral domain. If R is a finite-dimensonal k-vector space, then R is a field: indeed, if $0 \neq r \in R$, then multiplication by r is a k-linear map. Since R is an integral domain, this map is injective, and since R is finite-dimensional, every injective map is surjective. Hence we find an inverse of r.

Theorem. 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 $k[X_1, \ldots, X_n]$ and $R = k[X_1, \ldots, X_n]/I$ then the intersection of the maximal ideals of R is 0.

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

Proof. Let p be any prime ideal of R and let $s \in R \setminus p$. The set $S \coloneqq \{1, s, s^2, \ldots\}$ is multiplicative, so we get a localization $S^{-1}R$ and a map $\theta\colon R \to S^{-1}R$. R is a finitely generated k-algebra and $S^{-1}R$ generated as a k-algebra by $\theta(R)$ and $1/s$. Hence $S^{-1}R$ is a finitely generated k-algebra. Let q be a maximal ideal of $S^{-1}R$ containing $S^{-1}p$. By the weak Nullstellensatz, $S^{-1}R/q$ is a finite field extension of k.

The ideal $p_1 \coloneqq \theta^{-1}(q)$ is a prime ideal containing p, and by the correspondence of prime dieals we know that p_1 does not meet S. Hence θ induces an injective k-vector space homomorphism $R/p_1 \to S^{-1}R/q$. Since $S^{-1}R/q$ is finite-dimensional, this implies that R/p_1 is also finite-dimensinoal.

By the remark, this implies that R/p_1 (which is an integral domain since p_1 is prime) is a field, hence p_1 is a maximal ideal. Hence, for any $s \notin p$, we find a maximal ideal containing p but not containing s, i.e.,

$$R \setminus p \subseteq \bigcup \{\text{complemenents of maximal ideals containing } p\}.$$

By elementary set theory, this means that

$$\bigcap \{\text{maximal ideals containing } p\} \subseteq p.$$

Since the converse inclusion is trivial, we have that p is the intersection of maximal ideals containing p. Hence the intersection of all primes is the same as the intersection of all maximals, which is what we wanted to show. $\square$

CHAPTER 3

Tensor products

Definition 3.1. If L, M, N are R-modules, then a function $\varphi\colon M \times N \to L$ is called R-bilinear if

$$\varphi(r_1 m_1 + r_2 m_2, n) = r_1 \varphi(m_1, n) + r_2 \varphi(m_2, n),$$
$$\varphi(m, r_1 n_1 + r_2 n_2) = r_1 \varphi(m, n_1) + r_2 \varphi(m, n_2).$$

Remark. The idea is to reduce the study of bilinear maps to the of linear (i.e, R-module) maps.

If $\varphi\colon M \times N \to T$ is bilinear and $\theta\colon T \to L$ is linear, then $\theta \circ \varphi$ is bilinear. Composition with φ gives a well defined function φ^* from R-linear maps $T \to L$ to bilinear maps $M \times N \to L$.

$$\begin{tikzcd} M \times N \arrow[r, "\varphi"] \arrow[dr, "\varphi^*(\theta)"'] & T \arrow[d, "\theta"] \\ & L \end{tikzcd}$$

We say that φ is universal if φ^* is a bijection for every L. If this happens that study of bilinear maps $M \times N \to L$ is reduced to the study if linear maps $T \to L$.

Lemma 3.2. (i) Given R-modules M, N, there is an R-module T and a universal map $\varphi\colon M \times N \to T$.

(ii) Given two universal maps $\varphi_1\colon M \times N \to T_1$, $\varphi_2\colon M \times N \to T - 2$, there is a unique isomorphism $\beta\colon T_1 \to T_2$ such that $\varphi_2 = \beta \circ \varphi_1$.

Proof. Let F be the free R-module on the generators $e_{(m,n)}$ indexed by pairs $(m, n) \in M \times N$. Let X be the R-submodule generated by all elements of the forms

$$e_{(r_1 m_1 + r_2 m_2, n)} - r_1 e_{(m_1,n)} - r_2 e_{(m_2,n)}, \quad e_{(m, r_1 n_1 + r_2 n_2)} - r_1 e_{(m,n_1)} - r_2 e_{(m,n_2)}.$$

Define $T \coloneqq F/X$ and write $m \otimes n$ for the image of the basis element $e_{(m,n)}$ in T. T is generated by elements of the form $m \otimes n$, and we have the relations

$$(r_1 m_1 + r_2 m_2) \otimes n = r_1(m_1 \otimes n) + t_2(m_2 \otimes n)$$
$$m \otimes (r_1 n_1 + r_2 n_2) = r_1(m \otimes n_1) + r_2(m \otimes n_2).$$

Define $\varphi M \times N \to T$ via $(m, n) \mapsto m \otimes n$ and note that φ is bilinear. Any map $\alpha\colon M \times N \to L$ extends to a map of R-modules $\overline{\alpha}\colon F \to L$ by sending $e_{(m,n)} \mapsto \alpha(m, n)$. If α is bilinear then $\overline{\alpha}$ vanishes on the generators of X, hence it induces a map of R-modules $\alpha'\colon T \to L$ such that $\alpha'(m \otimes n) = \alpha(m, n)$, and α' is uniquely determined by these relations. Hence φ is universal.

The proof of uniqueness is just the usual dance with universal properties. □

Definition 3.3. The module T is usually denoted $M \otimes_R N$ and is called the tensor product of M and N over R.

Remark. • We often drop the subscript R if it is clear what ring we are using.

- Not all elements of $M \otimes_R N$ are of the for $m \otimes n$. A general element if of the form $\sum_{i=1}^r m_i \otimes n_i$.
- If $R = k$ is a field and k^s, k^t are finite-dimensinal vector spaces over k, then the map $M \times N \to k^{st}$ given by numbering basis elements of k^{st} by pairs (i,j), $1 \le i \le s, 1 \le j \le t$ and sending $(a_i, b_j) \mapsto e_{(i,j)}$ is universal, hence $M \otimes N \cong k^{st}$.
- It is possible to define tensor products over non-commutative rings, where M is a right R-module and N is a left R-module. In this situation, $M \otimes N$ is only an abelian group, not necessarily and R-module. The construction is analogous, but you take the free abelian group instead of the free R-module and use the relations

$$\begin{aligned} e_{(m_1+m_2,n)} - e_{(m_1,n)} - e_{(m_2,n)} \\ e_{(m,n_1+n_2)} - e_{(m,n_1)} - e_{(m,n_2)} \\ e_{(mr,n)} - e_{(m,rn)}. \end{aligned}$$

  If M is an (R,S)-bimodule and N is an (S,T)-bimodule, then $M \otimes N$ becomes a (R,T)-bimodule.
- On the exercise sheed we will see that $\mathbb{Z}/r\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/s\mathbb{Z} \cong \mathbb{Z}/\gcd(r,s)\mathbb{Z}$.
- one can product a universal trilinear map $L \times M \times N \to T$, unique up to isomorphism, denoted by $L \otimes M \otimes N$.

Lemma 3.4. The following maps exist and are isomorphisms.

(i)
$$\begin{aligned} M \otimes N &\to N \otimes M \\ m\otimes &\mapsto n \otimes m, \end{aligned}$$

(ii)
$$\begin{aligned} (M \otimes N) \otimes L \to M \otimes (N \otimes L) &\to M \otimes N \otimes L \\ (m \otimes n) \otimes \ell \mapsto m \otimes (n \otimes \ell) &\mapsto m \otimes n \otimes \ell, \end{aligned}$$

(iii)
$$\begin{aligned} (M \oplus N) \otimes L &\to (M \otimes L) \oplus (N \otimes L) \\ (m,n) \otimes \ell &\mapsto (m \otimes \ell, n \otimes \ell), \end{aligned}$$

(iv)
$$\begin{aligned} R \otimes_R M &\to M \\ r \otimes m &\mapsto rm. \end{aligned}$$

Proof. (i) The map $M \times N \to N \otimes M$ given by $(m,n) \mapsto n \otimes m$ is bilinear, hence it induces the map $M \otimes N \to N \otimes M$ given by $m \otimes n \mapsto n \otimes m$. Swapping the roles of M and N yields an inverse.

(ii) Exercise (appears on the second example sheet).

(iii) We have a bilinear map

$$\begin{aligned} (M \oplus N) \times L &\to (M \otimes L) \oplus (N \otimes L) \\ ((m,n),\ell) &\mapsto (m \otimes \ell, n \otimes \ell). \end{aligned}$$

This map induces a linear map

$$\begin{aligned} (M \oplus N) \otimes L &\to (M \otimes L) \oplus (N \otimes L) \\ (m,n) \otimes \ell &\mapsto (m \otimes \ell, n \otimes \ell), \end{aligned}$$

and we will find an inverse. Indeed, the maps

$$\begin{aligned} M \times L &\to (M \oplus N) \otimes L \\ (m, \ell) &\mapsto (m, 0) \otimes \ell \end{aligned} \qquad \begin{aligned} N \times L &\to (M \oplus N) \otimes L \\ (n, \ell) &\mapsto (0, n) \otimes \ell \end{aligned}$$

are bilinear, and by the universal property of the tensor product and the universal property of the direct sum we obtain a linear map

$$\begin{aligned} \Psi \colon (M \otimes L) \oplus (N \otimes L) &\to (M \oplus N) \otimes L \\ (m \otimes \ell_1, n \otimes \ell_2) &\mapsto (m, 0) \otimes \ell_1 + (0, n) \otimes \ell_2. \end{aligned}$$

We trivially calculate that this is the required inverse.

(iv) Another exercise, cf. Proposition 2.14 in Atiyah-Macdonald.

□

Example. We have a natural bijection

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

Indeed, if $\varphi \colon M \times N \to L$ is a bilinear map, we get $\theta \colon M \to \mathrm{Hom}(N, L)$ as $m \mapsto (n \mapsto \varphi(m, n))$. Conversely, if $\theta \colon M \to \mathrm{Hom}(N, L)$ is linear, then we obtain a bilinear map $M \times N \to L$ by setting $(m, n) \mapsto \theta(m)(n)$.

1. Restriction and extension of scalars

Definition 3.5. If $\varphi \colon R \to T$ is a homomorphism of rings, and N is a T-module, then N may be regarded as an R-module via $rm := \varphi(r)m$. In particular, T itself is an R-module. This process is called restriction of scalars.

If M is an R-module, then $T \otimes_R M$ is an R-module. It is also a T-module via $t_1(t_2 \otimes m) := (t_1 t_2) \otimes m$.

Example. Localisation of a module is just extension of scalars using the map $R \to S^{-1}R$. Indeed, given an R-module M and a multiplicatively closed set S, we find an isomorphism of R-modules $f \colon S^{-1}R \otimes_R M \to S^{-1}M$ given by $\frac{r}{s} \otimes m \mapsto \frac{rm}{s}$.

Indeed, the map $S^{-1}R \times M \to S^{-1}M$, $(r/s, m) \mapsto (rm)/s$ is bilinear, so it induces f as above. It is obviously surjective. For injectivity, recall that a general element of the left hand side is of the form $\sum_{i=1}^n r_i/s_i \otimes m_i$. Let $s = s_1 \cdots s_n$ and $t_i = \prod_{j \neq i} s_j$. Then we may calculate

$$\sum \frac{r_i}{s_i} \otimes m_i = \sum \frac{r_i t_i}{s} \otimes m_i = \sum \frac{1}{s} \otimes r_i t_i m_i = \frac{1}{s} \otimes \sum r_i t_i m_i.$$

Hence, every element of the left hand side is of the form $1/s \otimes m$.

Suppose that $f(1/s) \otimes m) = 0$. Then $m/s = 0$ in $S^{-1}M$, i.e., we find $x \in S$ such that $xm = 0$. But then

$$\frac{1}{s} \otimes m = \frac{x}{sx} \otimes m = \frac{1}{sx} \otimes xm = \frac{1}{sx} \otimes 0 = 0,$$

and so f is injective.

Definition 3.6. Given R-linear maps $\theta \colon M_1 \to M_2$ and $\varphi \colon N_1 \to N_2$, the tensor product of θ and φ is the map

$$\begin{aligned} \theta \otimes \varphi \colon M_1 \otimes N_1 &\to M_2 \otimes N_2 \\ m_1 \otimes n_1 &\mapsto \theta(m_1) \otimes \varphi(n_1), \end{aligned}$$

which exists because $M_1 \times N_1 \to M_2 \otimes N_2$, $(m, n) \mapsto \theta(m) \otimes \varphi(n)$ is bilinear.

DEFINITION 3.7. Given a ring homomorphism $\varphi_1\colon R \to T_1$ (which in particular makes T_1 into an R-module), we say that T_1 together with φ_1 is an R-algebra. Given another ring homomorphism $\varphi_2\colon R \to T_2$, we can take the tensor product of the R-moodules T_1 and T_2 to give $T_1 \otimes_R T_2$. We can declare a product on $T_1 \times T_2$ by

$$\begin{aligned}(T_1 \otimes T_2) \times (T_1 \otimes T_2) &\to T_1 \otimes T_2\\ (t_1 \otimes t_2, t_1' \otimes t_2') &\mapsto t_1 t_1' \otimes t_2 t_2'.\end{aligned}$$

As usual, it needs to be checked that this map actually exists: first, we notice that multiplication is bilinear, hence it induces a map $T_1 \times T_i \to T_i$. The composite

$$(T_1 \otimes T_1) \times (T_2 \otimes T_2) \to T_1 \times T_2 \to T_1 \otimes T_2$$

is again bilinear, hence it induces a map

$$\begin{aligned}(T_1 \otimes T_1) \otimes (T_2 \otimes T_2) &\to T_1 \otimes T_2\\ (t_1 \otimes t_1') \otimes (t_2 \otimes t_2') &\mapsto t_1 t_1' \otimes t_2 t2'.\end{aligned}$$

By (3.4), we can reassociate and permute this to a map

$$(T_1 \otimes T_2) \otimes (T_1 \otimes T_2) \to T_1 \otimes T_2,$$

and we see that composition with the tensoring map gives exactly the map we postulated above. Hence the product exists, and $1 \otimes 1$ is the multiplicative identity. This makes $T_1 \otimes T_2$ into a ring and we have an R-algebra structure via $r \mapsto \varphi_1(r) \otimes 1 = 1 \otimes \varphi_2(r)$.

EXAMPLE.
(i) If k is a field then $k[X]$ is a k-algebra. We have an isomorphism $k[X] \otimes_k k[X] \cong k[X, Y]$.
(ii) We have an isomorphism $\mathbb{Q}[X]/(X^2 + 1) \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{C}[X]/(X^2 + 1)$.
(iii) We have $k[X]/(f) \otimes_k k[X]/(g) \cong k[X, Y]/(f(X), g(Y))$.

DEFINITION 3.8. If R is a k-algebra and M and N are R-modules, then $M \otimes_k N$ is an abelian group, and we can declare an R-module structure on it by defining $r(m \otimes n) \coloneqq rm \otimes rn$. This is called the diagonal action. If M and N are finitely generated as R-modules, then so is $M \otimes N$.

LEMMA 3.9. If

$$M_1 \xrightarrow{\theta} M \xrightarrow{\varphi} M_2 \longrightarrow 0$$

is a sequence of R-modules, then it is exact if and only if for all R-modules N, the sequence

$$0 \longrightarrow \operatorname{Hom}(M_2, N) \xrightarrow{\alpha} \operatorname{Hom}(M, N) \xrightarrow{\beta} \operatorname{Hom}(M_1, N)$$

is exact.

PROOF. First, assume that the first sequence is exact. Let N be an R-module. If $f \in \operatorname{Hom}(M_2, N)$, then $f \circ \varphi \in \operatorname{Hom}(M, N)$. This is the map $\alpha\colon \operatorname{Hom}(M_2, N) \to \operatorname{Hom}(M, N)$, and it is injective, since if $f \neq 0$, there is $m_2 \in M_2$ with $f(m_2) \neq 0$, but $m_2 = \varphi(m)$ for some $m \in M$, so $f(\varphi(m)) \neq 0$, hence α is injective.

If $g \in \operatorname{Hom}(M, N)$ then β sends it to $g \circ \theta \in \operatorname{Hom}(M_1, N)$. If $g \circ \theta = 0$, then $\theta(M_1) \subseteq \ker g$. By exactness, we have $\theta(M_1) = \ker \varphi$, so we conclude $\ker \varphi \subseteq \ker g$. Now φ factors as $M \to M/\ker \varphi \to M_2$, with the latter map being an isomorphism. Hence, g factors as $M \to M_2 \to M/\ker \varphi \to M/\ker g \to N$, where the first map is φ and the second map is the inverse of the isomorphism. Taking f to be the composite of the the latter maps, we have written $g = f \circ \varphi$ for $f \in \operatorname{Hom}(M_2, N)$, hence $\ker \beta \subseteq \operatorname{im} \alpha$. Since the reverse inclusion is trivial, we have exactness at $\operatorname{Hom}(M, N)$.

Conversely, suppose that the sequence of Homsets is exact. If the map $M_2 \to M_2/\operatorname{im}\varphi$ was nonzero, then by injectivity of α, so would be the composite $M \to M_2 \to M_2/\operatorname{im}\varphi$, which is obviously not the case. Hence φ is surjective.

We have $0 = \beta(\alpha(\mathrm{id}_{M_2})) = \varphi \circ \theta$, hence $\operatorname{im}\theta \subseteq \ker\varphi$. Let $p\colon M \to M/\operatorname{im}\theta$ be the projection. Then $p \circ \theta = 0$, i.e., $p \in \ker\beta = \operatorname{im}\alpha$, so we find $g\colon M_2 \to N$ $p = g \circ \varphi$. Then $\operatorname{im}\theta = \ker p \supseteq \ker\varphi$. Putting things together, we have exactness at M. □

REMARK.
- The functor $\operatorname{Hom}(-, N)$ is not exact. The failure of exactness is studied using cohomology.
- We do have an analogous statement for the other Hom functor: The sequence

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0$$

is exact if and only if

$$0 \longrightarrow \operatorname{Hom}(N, M_1) \longrightarrow \operatorname{Hom}(N, M) \longrightarrow \operatorname{Hom}(N, M_2)$$

is exact for all modules N.

LEMMA 3.10. If

$$M_1 \xrightarrow{\theta} M \xrightarrow{\varphi} M_2 \longrightarrow 0$$

is an exact sequence and N is an R-module, then

$$M_1 \otimes N \xrightarrow{\theta\otimes\mathrm{id}} M \otimes N \xrightarrow{\varphi\otimes\mathrm{id}} M_2 \otimes N \longrightarrow 0$$

$$N \otimes M_1 \xrightarrow{\mathrm{id}\otimes\theta} N \otimes M \xrightarrow{\mathrm{id}\otimes\varphi} N \otimes M_2 \longrightarrow 0$$

are exact.

PROOF. The second statement follows from the first statement by commutativity of tensor products.

Let N' be any R-module. By the previous lemma, we have an exact sequence

$$0 \to \operatorname{Hom}(M_2, \operatorname{Hom}(N, N')) \to \operatorname{Hom}(M, \operatorname{Hom}(N, N')) \to \operatorname{Hom}(M_1, \operatorname{Hom}(N, N')).$$

By the tensor-hom adjunction, we have $\operatorname{Hom}(M, \operatorname{Hom}(N, N')) \cong \operatorname{Hom}(M \otimes N, N')$, so we get an exact sequence

$$0 \longrightarrow \operatorname{Hom}(M_2 \otimes N, N') \longrightarrow \operatorname{Hom}(M \otimes N, N') \longrightarrow \operatorname{Hom}(M \otimes N, N').$$

The previous lemma yields the desired exact sequence (after we have verified that the maps are indeed what we expect). □

EXAMPLE. Again, observe that these are not short exact sequences. Applying $- \otimes N$ does not in general preserve injecivity of the left hand map. For example, consider the short exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$

Tensoring with $\mathbb{Z}/2\mathbb{Z}$, we obtain a sequence

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{0} \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

which fails to be exact. Hence exactness is not preserved.

Definition 3.11. An R-module N is called flat if given any short exact sequence

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0,$$

the sequence

$$0 \longrightarrow M_1 \otimes N \longrightarrow M \otimes N \longrightarrow M_2 \otimes N \longrightarrow 0$$

is exact.

Example.
- R is a flat R-module.
- R^n is a flat R-module.
- If $R = \mathbb{Z}$, $\mathbb{Q}$ is a flat $\mathbb{Z}$-module. In fact, it can be shown that every torsion-free abelian group is a flat $\mathbb{Z}$-module.

Homology measures the failure of a module to be flat.

CHAPTER 4

Integrality and dimension

Definition 4.1. The spectrum of R, denoted $\operatorname{Spec} R$, is $\{\mathfrak{p} \mid \mathfrak{p} \text{ prime ideal of } R\}$.

Definition 4.2. The length of a chain of prime ideals $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ is n.

Definition 4.3. The (Krull) dimension of R, denoted $\dim R$, is

$$\dim R = \begin{cases} \sup\{n \mid \exists \text{ chain of prime ideals of length } n\}, & \text{if it exists,} \\ \infty, & \text{otherwise.} \end{cases}$$

Definition 4.4. The height of $\mathfrak{p} \in \operatorname{Spec} R$, denoted $\operatorname{ht}(\mathfrak{p})$ or $\operatorname{ht}_R(\mathfrak{p})$, is

$$\sup\{n \mid \exists \text{ chain of prime ideals } \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}\}.$$

Remark. By the one-to-one correspondence bettwen primes with empty intersection with $R \setminus \mathfrak{p}$ and the primes of $R_{\mathfrak{p}}$, we have $\operatorname{ht}(\mathfrak{p}) = \dim R_{\mathfrak{p}}$.

Example.
- An artinian ring has dimension 0 (since all prie ideals are maximal). Conversely, it is possible to show that any noetherian ring of dimension 0 is artinian.
- We have $\dim \mathbb{Z} = 1$. Indeed, a chain of maximal length must be of the form $0 \subsetneq (p)$, where p is a prime number. Also, $\dim k[X] = 1$ is k is a field. THese are examples of Dedekind rings, i.e., integrally closed domains of dimension 1. Dedekind rings are essential ingredients of the theory of algebraic curves and number theory.
- The dimension of $k[X_1, \dots, X_n]$ is at least n, because we have the chain of prime ideals

  $$0 \subsetneq (X_1) \subsetneq (X_2) \subsetneq \cdots \subsetneq (X_1, \dots, X_n).$$

  Indeed, if k is a field, it is possible to show that the dimension is exactly n. To prove this, we need some results about the relationship between chains of prime ideals in subrings and chains in the whole ring under some cindition relating the subring to the larger rung.

Lemma 4.5. The height 1 primes of $k[X_1, \dots, X_n]$ are precisely those of the form (f) where f is irreducible.

Proof. Certainly such an ideal is prime, since $k[X_1, \dots, X_n]$ is a unique factorization domain.

If $\mathfrak{p}$ is a nonzero prime ideal, it contains such an (f), since if $g \in \mathfrak{p}$, then by primality, it contains at least one of its irreducible factors. This means that if a prime has height 1, then it must be of the form (f) with f irreducible.

Conversely, suppose that f is irreducible, and $0 \subsetneq \mathfrak{p} \subseteq (f)$ for some prime ideal $\mathfrak{p}$. Then by what we just saw, we find an irreducible h with $(h) \subseteq \mathfrak{p}$. In particular, $h \in (f)$. Since h is irreducible, we must have $(h) = (f)$, so $\mathfrak{p} = (f)$, so $\operatorname{ht}((f)) = 1$ as claimed. $\square$

1. Integral extensions

DEFINITION 4.6. If $R \subseteq S$ are rings, then $x \in S$ is called integral over R if there is some monic polynomial $f \in R[X]$ such that $f(x) = 0$.

EXAMPLE. Elements of $\mathbb{Q}$ which are integral over $\mathbb{Z}$ are precisely the elements of $\mathbb{Z}$: if $x = r/s$ is integral over $\mathbb{Z}$ with $\gcd(r, s) = 1$, then

$$0 = s^n f(x) = r^n + r_{n-1}s + \cdots + r_0 s^n = 0$$

for integers r_i. Thus $s \mid r^n$, but since $\gcd(r, s) = 1$, this means that $s = \pm 1$, hence $x = \pm r \in \mathbb{Z}$.

LEMMA 4.7. The following statements are equivalent for an element $x \in S$.

(i) x is integral over R,
(ii) the ring $R[x]$ (i.e., the subring of S generated by R and x) is finitely generated as an R-module,
(iii) $R[x]$ is contained in a subring T of S such that T is a finitely generated R-module.

PROOF. If x is integral, i.e., $f(x) = 0$ for monic $f \in R[X]$, we can write $x^{n+j} = -(r_{n-1}x^{n+j-1} + \cdots + r_0 x^j)$ for all $j \geq 0$, where $\deg f = n$. Hence, $R[X]$ is generated as an R-module by $1, x, \ldots, x^{n-1}$. This shows that (i) implies (ii).

Trivially, (ii) implies (iii).

Finally, let $y_1, \ldots, y_n$ generate T as an R-module. Then we find r_{ij} such that $xy_i = \sum_j r_{ij} y_j$. Then

$$\sum_j (x\delta_{ij} - r_i j) y_j = 0,$$

where δ is the Kronecker delta. Define a matrix A with coefficients in S via $a_{ij} = x\delta_{ij} - r_{ij}$. Then what we have just seen means that $Ay_i = 0$ for all i, so in particular $0 = \operatorname{adj}(A)Ay = (\det A)Iy = \det Ay$, where $y = (y_1, \ldots, y_n)^\top$. Since the y_i generate T, 1 is a linear combination of the y_i, so we find some row vector v such that $0 = \det Ayv = \det(A)1 = \det A$. But $\det A_{ij}$ is a monic polynomial expression in x with coefficients in R, so we are done. □

DEFINITION. Some authors use the phrase "S is finite over R" to say that S is finitely generated as an R-module, and the phrase "R is of finite type" if R is finitely generated as a k-algebra.

REMARK. This proof is very similar to a proof of Nakayama's lemma appearing in Atiyah-Macdonald.

Some authors say S is of finite type over R is S is generated as a ring by R and a finite set.

LEMMA 4.8. If $x_1, \ldots, x_m \in S$ are integral over R, then $R[x_1, \ldots, x_m]$ is a finitely generated R-module.

PROOF. We do induction on m. The case $m = 1$ is just 4.7. If the claim is true for m, since x_{m+1} is integral over R, it is definitely integral over $R[x_1, \ldots, x_m]$. Hence $R[x_1, \ldots, x_{m+1}$ is a finitely generated $R[x_1, \ldots, x_m]$-module, say with generators $z_1, \ldots, z_t$. By the inductive hypothesis, $R[x_1, \ldots, x_m]$ is finitely generated as an R-module, say by $y_1, \ldots, y_\ell$. Then $R[x_1, \ldots, x_{m+1}]$ is generated as an R-module by elements of the form $z_i y_j$ with $1 \leq i \leq t$ and $1 \leq y \leq \ell$. □

LEMMA 4.9. The set $T \subseteq S$ of elements integral over R forms a subring of S.

PROOF. Every element of R is integral over R. Furthermore, if $x, y \in T$, then by 4.8 we have that $R[x, y]$ is finitely generated. Since $x \pm y, xy \in R[x, y]$, these are integral by 4.7(iii). □

Definition 4.10. The subring of integral elements over R in S is called the integral closure of R in S. If the integral closure of R in S is just R, then we say that R is integrally closed in S. If the integral closure is the entirety of S, we say that S is integral over R.

If R is an integral domain, we say that R is integrally closed if it is integrally closed in its field of fractions.

Example.
- As we say, $\mathbb{Z}$ is integrally closed.
- $k[X_1, \dots, X_n]$ is integrally closed (in $k(X_1, \dots, X_n)$).
- If K is an algebraic number field with $[K : \mathbb{Q}] < \infty$, then the integral closure of $\mathbb{Z}$ in K is the ring of integers $\mathcal{O}_K$.
- Being integrally closed is a local property. This will be proved later.

Lemma 4.11. If $R \subseteq T \subseteq S$ are rings, T is integral over R and S is integral over T, then S is integral over R.

Proof. Take $x \in S$. By assumption, we have a relation $x^n + t_{n-1} + \cdots + t_0 = 0$ with $t_i \in T$. By (4.8), the subring $R[t_0, \dots, t_{n-1}]$ is a finitely generated R-module, and x is integral over it, so $R[t_0, \dots, t_{n-1}, x]$ is a finitely generated $R[t_0, \dots, t_{n-1}]$-module. As seen in the proof of (4.8), this implies that $R[t_0, \dots, t_{n-1}, x]$ is a finitely generated R-module, so by 4.7(iii), x is integral over R as required. □

Lemma 4.12. Let $R \subseteq T$ be rings such that T is integral over R.

(i) If $J \subseteq T$ is an ideal, then T/J is integral over $R/(J \cap R)$, where we identify $R/(J \cap R)$ with the subring $(R + J)/J$ of T/J.

(ii) If S is a multiplicatively closed subset of R, then $S^{-1}T$ is integral over $S^{-1}R$.

Proof. For (i), if $x \in T$, then we have an expression $x^n = r_{n-1}x^{n-1} + \cdots + r_0 = 0$ for some $r_i \in R$. Projecting onto T/J, this yields an equation $\overline{x}^n + \overline{r_{n-1}}\overline{x}^{n-1} + \cdots + \overline{r_0} = \overline{0}$ in T/J, such that $\overline{r_i} \in (R + J)/J$, hence $\overline{x}$ is interal over $(R + J)/J$ as required.

For (ii), let $x/s \in S^{-1}T$. Again we have $x^n = r_{n-1}x^{n-1} + \cdots + r_0 = 0$ for some $r_i \in R$. In particular, this implies

$$\left(\frac{x}{s}\right)^n + \frac{r_{n-1}}{s}\left(\frac{x}{s}\right)^{n_1} + \cdots + \frac{r_0}{s_n} = 0$$

in $S^{-1}T$, so x/s is integral over $S^{-1}R$. □

Lemma 4.13. Let $R \subseteq T$ both be integral domains such that T is integral over R. Then T is a field if and only if R is a field.

Proof. First assume that R is a field. Let $0 \neq t \in T$. Let $t^n + r_{n-1}t^{n-1} + \cdots + r_0 = 0$ be such that n is minimal among all monic expressions. We have $r_0 \neq 0$, otherwise we could factor out a t, so since T is a domain, $t^{n-1} + \cdots r_1 = 0$ would be a shorter expression, contradicting minimality. Then $s \coloneqq -r_0^{-1}(t^{n-1} + \cdots + r_1)$ satisfies $st = 1$, hence t has an inverse, so T is a field.

Conversely suppose that T is a field. Let $0 \neq x \in R$. Then x has an inverse x^{-1} in T. We find $r'_i \in R$ such that $x^{-m} + r'_m x^{-m+1} + \cdots r'_0 = 0$. Multiply by x^{m-1} and rearrange to find $x^{-1} = -(r'_m + r'_{m-1}x + \cdots + r'_0 x^{m-1}) \in R$, so R is a field. □

Lemma 4.14. Let $R \subseteq T$ be rings and T integral over R. Let $\mathfrak{q}$ be a prime ideal in T and set $\mathfrak{p} \coloneqq R \cap \mathfrak{q}$. Then $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.

Proof. By 4.12(i), $T/\mathfrak{q}$ is integral over $R/\mathfrak{p}$, and since $\mathfrak{p}$ and $\mathfrak{q}$ are prime, $T/\mathfrak{q}$ and $R/\mathfrak{p}$ are integral domains. The result now follows from 4.13. □

THEOREM 4.15 (Incomparability theorem). Let $R \subseteq T$ be rings with T integral over R. Let $\mathfrak{q} \subseteq \mathfrak{q}_1$ be prime ideals of T. Suppose $\mathfrak{q} \cap R = \mathfrak{p} = \mathfrak{q}_1 \cap R$. Then $\mathfrak{q} = \mathfrak{q}_1$.

In particular, every strict chain of primes in T will induce a strict chain of primes in R, hence $\dim R \geq \dim T$.

PROOF. Set $S \coloneqq R \setminus \mathfrak{p}$. By 4.12(ii), $S^{-1}T$ is integral over $R_\mathfrak{p}$. $R_\mathfrak{p}$ is local with the unique maximal ideal $S^{-1}\mathfrak{p}$. As seen in Chapter 2, the ideals $S^{-1}\mathfrak{q}$ and $S^{-1}\mathfrak{q}_1$ are prime ideals in $S^{-1}T$. But the assumption implies that $S^{-1}\mathfrak{q} \cap S^{-1}R = S^{-1}\mathfrak{p} = S^{-1}\mathfrak{q}_1 \cap S^{-1}R$.

By 4.14, $S^{-1}\mathfrak{q}$ and $S^{-1}\mathfrak{q}_1$ are both maximal, but $S^{-1}\mathfrak{q} \subseteq S^{-1}\mathfrak{q}_1$, so we have equality. Using the correspondence between prime ideals of $S^{-1}T$ and prime ideals of T that do not meed S, we clonclude $\mathfrak{q} = \mathfrak{q}_1$. $\square$

THEOREM 4.16 (Lying over theorem). Let $R \subseteq T$ be rings, T integral over R. Let $\mathfrak{p}$ be a prime ideal of R. Then there is some prime ideal $\mathfrak{q}$ of T with $\mathfrak{q} \cap R = \mathfrak{p}$. In this situation, we say that $\mathfrak{q}$ lies over $\mathfrak{p}$. In other words, the map $\operatorname{Spec} T \to \operatorname{Spec} R$ is surjective.

PROOF. Again, let $S \coloneqq R \setminus \mathfrak{p}$. Then $S^{-1}T$ is integral over $R_\mathfrak{p}$. By the correspondence, a maximal ideal of $S^{-1}T$ is of the form $S^{-1}\mathfrak{q}$, where $\mathfrak{q}$ is a prime ideal of T.

Then $S^{-1}\mathfrak{q} \cap S^{-1}R$ is maximal by 4.14, but then it must be the unique maximal ideal $S^{-1}\mathfrak{p}$ of $R_\mathfrak{p}$. So $S^{-1}\mathfrak{q} \cap S^{-1}R = S^{-1}\mathfrak{p}$, and by the correspondence we conclude $\mathfrak{q} \cap R = \mathfrak{p}$. $\square$

REMARK. The next two theorems are due to Cohen and Seidelberg (1946) and are called the "going up" and "going down" theorems. They allow us to move from chains of prime ideals of R to such chains in T, where $R \subseteq T$ is an integral extension. The second theorem requires stronger conditions.

THEOREM 4.17 (Going-up theorem). Let $R \subseteq T$ be an integral ring extension. Let $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ be a chain of prime ideals of R, and $\mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_m$, where $m < n$ a chain of prime ideals of T such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ $(1 \leq i \leq m)$.

Then the chain of $\mathfrak{q}$s extends to a chain $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for $1 \leq i \leq n$.

PROOF. By induction, it will be enough to consider the case $n = 2$, $m = 1$. Write $\overline{R}$ for $R/\mathfrak{p}_1$ and $\overline{T}$ for $T/\mathfrak{q}_1$. Then we have an integral extension $\overline{R} \subseteq \overline{T}$, using the fact that $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$ and 4.12(i). By the Lying over theorem, we find a prime ideal $\overline{\mathfrak{q}_2}$ of $\overline{T}$ such that $\overline{\mathfrak{q}_2} \cap \overline{R} = \overline{\mathfrak{p}_2}$. Lifting out of the quotient yields a prime ideal $\mathfrak{q}_2$ of T with $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ and $\mathfrak{q}_2 \cap R = \mathfrak{p}_2$. $\square$

THEOREM 4.18 (Going-down theorem). Let $R \subseteq T$ be an integral extension of integral domains, such that R is integrally closed. Let $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$ be a chain of prime ideals of R and $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$ $(m < n)$ be a chain of prime ideals of T such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for $1 \leq i \leq m$.

Then the chain of $\mathfrak{q}$s extends to a chain $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_n$ with $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ $(1 \leq i \leq n)$.

PROOF. By induction, it will be sufficient to consider the case $m = 1$, $n = 2$, i.e., we are given prime ideals $\mathfrak{p}_1 \supsetneq \mathfrak{p}_2$ of R and a prime ideal $\mathfrak{q}_1$ of T such that $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$. We need to produce a prime ideal $\mathfrak{q}_2 \subseteq \mathfrak{q}_1$ such that $\mathfrak{q}_2 \cap R = \mathfrak{p}_2$.

Let $S_1 = T \setminus \mathfrak{q}_1$ and $S_2 = R \setminus \mathfrak{p}_2$. $S \coloneqq S_1 S_2$ is a multiplicatively closed subset of T satisfying $S_1 \subseteq S$ and $S_2 \subseteq S$.

Assume for now that $T\mathfrak{p}_2 \cap S = \varnothing$ (we will prove this later). $T\mathfrak{p}_2$ is an ideal of T, so we have $S^{-1}(T\mathfrak{p}_2) \subseteq S^{-1}T$ is an ideal, and it is a proper ideal, since otherwise we would have $x \in T\mathfrak{p}_2$ and $s, y \in S$ such that $s(x - y) = 0$, but then

$sx = sy \in T\mathfrak{p}_2 \cap S = \varnothing$ (since $T\mathfrak{p}_2$ is an ideal and S is multiplicatively closed), a contradiction.

Hence $S^{-1}T\mathfrak{p}_2$ is contained in some maximal ideal $S^{-1}T$, which by 2.5, is of the form $S^{-1}\mathfrak{q}_2$ for some prime ideal $\mathfrak{q}_2$ of T satisfying $\mathfrak{q}_2 \cap S = \varnothing$. Furthermore, if $x \in T\mathfrak{p}_2$, then $x/1 \in S^{-1}(T\mathfrak{p}_2)$, i.e., we find $y \in \mathfrak{q}_2$, $s_1, s_2 \in S$ such that $s_2(y - xs_1) = 0$. Hence, $x(s_1 s_2) \in \mathfrak{q}_2$, but $\mathfrak{q}_2$ is prime, $s_1 s_2 \in S$ and $\mathfrak{q}_2 \cap S = \varnothing$, so $x \in \mathfrak{q}_2$. We conclude that $T\mathfrak{p}_2 \subseteq \mathfrak{q}_2$ and hence $\mathfrak{p}_2 \subseteq T\mathfrak{p}_2 \cap R \subseteq \mathfrak{q}_2 \cap R$. On the other hand, if $\mathfrak{q}_2 \cap R \nsubseteq \mathfrak{p}_2$, then we find $x \in \mathfrak{q}_2 \cap R$ such that $x \notin \mathfrak{p}_2$. The latter means that $x \in R \setminus \mathfrak{p}_2 = S_2 \subseteq S$, but then $x \in \mathfrak{q}_2 \cap S = \varnothing$, a contradiction. We conclude $\mathfrak{p}_2 = \mathfrak{q}_2 \cap R$.

Similarly, if $\mathfrak{q}_2 \nsubseteq \mathfrak{q}_1$, then we find $x \in \mathfrak{q}_2$ such that $x \notin \mathfrak{q}_1$. Then $x \in T \setminus \mathfrak{q}_1 = S_1 \subseteq S$, so $x \in \mathfrak{q}_2 \cap S = \varnothing$. This shows, $\mathfrak{q}_2 \subseteq \mathfrak{q}_1$, so $\mathfrak{q}_2$ has the desired properties.

It remains to show that $T\mathfrak{p}_2 \cap S = \varnothing$. Suppose $x \in T\mathfrak{p}_2 \cap S$. Using the definition of S and the fact that T is an integral domain, we see that $x \neq 0$. Lemma 4.22 with $I = \mathfrak{p}_2$ tells us that the integral closure of $\mathfrak{p}_2$ in T is $\sqrt{T\mathfrak{p}_2}$. In particular, x is in the integral closure of $\mathfrak{p}_2$. Lemma 4.23 then tells us that it is algebraic over K, the field of fractions of R, and the coefficients of the minimal polynomial f of x over K are contained in $\sqrt{\mathfrak{p}_2} = \mathfrak{p}_2$.

Since $x \in S$, it is of the form $x = rt$ with $t \in S_1$, $r \in S_2$. If r_i are the coefficients of f, then the minimal polynomial of $t = x/r$ over K has coefficients $r_i' := r_i/r^{n-i} \in K$. Since t is integral over R by assumption, we may apply 4.23 with $I = R$ and find that r_i' is in fact contained in R.

Now $r_i = r_i' r^{n-i} \in \mathfrak{p}_2$ and $r \notin \mathfrak{p}_2$ since $r \in S_2$, so we must have $r_i' \in \mathfrak{p}_2$. Since these coefficients belong to a monic polynomial killing t, this just means that t is integral over $\mathfrak{p}_2$. Hence, 4.22 tells us that $t \in \sqrt{T\mathfrak{p}_2}$. We have $\mathfrak{p}_2 \subseteq \mathfrak{p}_1 \subseteq \mathfrak{q}_1$, which implies $T\mathfrak{p}_2 \subseteq T\mathfrak{q}_1 = \mathfrak{q}_1$. Since $\mathfrak{q}_1$ is prime, this implies $\sqrt{T\mathfrak{p}_2} \subseteq \mathfrak{q}_1$, so we conclude $t \in \mathfrak{q}_1$. On the other hand, $t \in S_1 = T \setminus \mathfrak{q}_1$, so we have arrived at the desired contradiction. $\square$

Remark. Later we apply these to finitely generated k-algebras to prove the Noether Normalisation theorem. If T is a domain then T is integral over a subalgebra R isomorphic to a polynomial algebra.

Corollary 4.19. Let $R \subseteq T$ be an integral extension. Then $\dim R = \dim T$.

Proof. Take a chain $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_n$ of primes in T. Intersection with R yields a chain $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ of primes in R, with $\mathfrak{q}_i \cap R = \mathfrak{p}_i$, and this chain is strict by 4.15. Thus $\dim R \geq \dim T$.

Conversely, if $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ is a chain of primes in R. Then 4.16 yields $\mathfrak{q}_0$ lying over $\mathfrak{p}_0$, which we can complete using the going-up theorem. This chain is obviously strictly increasing, hence $\dim R \leq \dim T$. $\square$

Corollary 4.20. Let $R \subseteq T$ be an integral extension, where T is an integral domain and R is integrally closed. Let $\mathfrak{q}$ be a prime ideal of T. Then $\mathrm{ht}(\mathfrak{q} \cap R) = \mathrm{ht}(\mathfrak{q})$.

Proof. Take a chain $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_n = \mathfrak{q}$ in $\mathrm{Spec}(T)$. As above this yields a strict chain of prime ideals in R by defining $\mathfrak{p}_i := \mathfrak{q}_i \cap R$. Hence, $\mathrm{ht}(\mathfrak{q} \cap R) \geq \mathrm{ht}(\mathfrak{q})$.

Conversely, if we have a chain of prime ideals ending in $\mathfrak{q} \cap R$, then $\mathfrak{q}$ is the beginning of a lift which can be completed using 4.18. Hence $\mathrm{ht}(\mathfrak{q} \cap R) \leq \mathrm{ht}(\mathfrak{q})$. $\square$

Definition 4.21. If $I \subseteq R$ is an ideal and $R \subseteq T$, then $x \in T$ is called integral over I if it satisfies a monic equation $x^n + r_{n-1}x^{n-1} + \cdots + r_0 = 0$ with $r_i \in I$. The integral closure of I in T is the set of such x.

Lemma 4.22. Let $R \subseteq T$ be an integral extension. Let $I \subseteq R$ be an ideal. Then the integral closure of I in T is the radical $\sqrt{TI}$ (note that TI is an ideal of T) and this is closed under addition and multiplication. In particular, if $R = T$, then the integral closure of I in R is $\sqrt{I}$.

Proof. If x is integral over I, then by definition we get a description $x^n = -(a_1x^{n-1} + \cdots + a_n) \in TI$. Hence, $x \in \sqrt{TI}$.

Conversely, if $x \in \sqrt{TI}$, then we have $x^n = \sum_i t_i r_i$ for some $n \in \mathbb{N}$, $r_i \in I$ and $t_i \in T$. Since $R \subseteq T$ is integral, using 4.8 we find that $M := R[t_1, \ldots, t_n]$ is finitely generated as an R-module. Observe that $x^n M - \sum_i r_i(t_i M) \subseteq IM$. Let $y_1, \ldots, y_s$ be a generating set for M. We may write $x^n y_j = \sum_\ell r_{j\ell} y_\ell$ for suitable $r_{j\ell} \in I$ (first write $t_i y_j$ as an R-linear combination of the y_j and then multiply with r_i to obtain an I-linear combination. Summing up, we get $x^n y_j$ as required). Rearrange to obtain

$$\sum_\ell (x^n \delta_{j\ell} - r_{j\ell}) y_\ell = 0,$$

and an argument identical to that in the proof of 4.7 yields that x^n, and hence x, is integral over I. □

Lemma 4.23. Let $R \subseteq T$ be integral domains, R integrally closed, and let $x \in T$ be integral over an ideal I of R. Then x is algebraic over the field of fractions K of R, and if $f := X^n + r_{n-1}X^{n-1} + \cdots + r_0$ is the minimal polynomial of x over K, then $r_i \in \sqrt{I}$ for all i.

Proof. Certaily x is algebraic over K, since x is integral over I. It remains to show that the coefficients r_i are in $\sqrt{I}$. By the previous result, it will be sufficient to show that they are integral over I, since in that case they will be contained in R, since R is integrally closed, and 4.22 with $T = R$ yields the desired result.

To show that the r_i are integral over I, consider the extension $K \subseteq L$, where L is a splitting field of f. If y is a root of f, then there is a K-automorphism of L sending $x \mapsto y$ (cf. Galois theory). Since x is integral over R, it satisfies some monic equation $x^m + s_{m-1}x^{m-1} + \cdots + s_0 = 0$ with $s_i \in I$. Applying the automorphism (which fixes K, so inparticular I), yields $y^m + s_{m-1}y^{m-1} + \cdots + s_0 = 0$, so y is integral over I.

Since $f = \prod_y (X - y)$ for the roots y, the coefficients r_i are expressible as sums and products of the y. By 4.22, sums and products of elements integral over an ideal are again integral over the ideal, so we are done. □

2. Transcendence Degree

Definition. If k is a field, then an affine algebra over k is just a k-algebra which is finitely generated as a k-algebra (i.e., there is a surjective map $k[X_1, \ldots, X_n] \to A$ for some n). Our main result will be:

Theorem 4.24. Let T be an affine algebra which is also an integral domain with fraction field K. Then $\dim T = \operatorname{tr deg}_k K$, where $\operatorname{tr deg}_k K$ is the so-called transcendence degree of K over k.

Proof. We proceed by induction over $r := \operatorname{tr deg}_k K$. For $r = 0$, there is nothing to do.

By Noether Normalisation, we find algebraically independent elements $x_1, \ldots, x_r \in T$ such that T is integral over $R = k[x_1, \ldots, x_r]$, This implies that K is algebraic over $k(x_1, \ldots, x_r)$, which in turn implies that $\operatorname{tr deg}_k(K) = \operatorname{tr deg}_k k(x_1, \ldots, x_r) = r$. By 4.19, $\dim T = \dim R = \dim k[X_1, \ldots, X_r]$.

Thus, it remains to show that $\dim k[X_1, \ldots, X_r] = r$. We have already seen that $\dim k[X_1, \ldots, X_r] \geq r$. Take a chain $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_s$ of primes in R.

Since R is an integral domain, we may assume that $\mathfrak{p}_0 = 0$. Furthermore, we may assume using Lemma 4.5 that $\mathfrak{p}_1 = (f)$.

As shown in an example below, we have $\operatorname{tr}\deg_k(K_f) = r-1$, where K_f is the field of fractions of $R/(f)$. By induction, we find $\dim R/(f) = r-1$.

Next, consider the chain

$$\mathfrak{p}_1/\mathfrak{p}_1 \subsetneq \mathfrak{p}_2/\mathfrak{p}_1 \subsetneq \cdots \subseteq \mathfrak{p}_s/\mathfrak{p}_1.$$

This is again a chain of prime ideals (since $\mathfrak{p}_1 \subseteq \mathfrak{p}_i$ and the quotient map is surjective) in $R/(f)$ of length $s-1$. Hence $s-1 \leq r-1$ and so $s \leq r$, so we conclude $\dim R = r$ as required. □

Definition. We say that $x_1, \dots, x_n$ are algebraically indepdendent over k if the ring map $k[X_1, \dots, X_n] \to k[x_1, \dots, x_n]$ which sends $X_i \mapsto x_i$ is an isomorphism. In this situation, $k[x_1, \dots, x_n]$ may be regarded as a polynomial algebra.

As in linear algebra, we consider maximal algebraically indepdendent sets: they all have the same size (we will not prove this here). Such a set is called a transcendence basis over k and the transcendence degree is the cardinality.

There are some concepts that carry over from linear algebra: an algebraically independent set can be thought of like a linearly independent set, the algebraic closure of a set S is like the span of S and transcendence degree is like dimension.

Example. Let $L = k(X_1, \dots, X_n)$ be the fraction field of $k[X_1, \dots, X_n]$ and $f \in k[X_1, \dots, X_n]$ an irreducible polynomial. Define K to be the field of fractions of $k[X_1, \dots, X_n]/(f)$. Then we have $\operatorname{tr}\deg_k L = n$, since $X_1, \dots, X_n$ is a maximal algebraically independent set, and $\operatorname{tr}\deg K = n-1$, since K is algebraic over $k(X_1, \dots, X_{i-1}, X_{i+1}, X_n)$, where X_i is a variable that appears in some term in f.

Theorem 4.25 (Noether Normalisation). Let T be an affine algebra. Then T is integral over a subalgebra of the form $R = k[x_1, \dots, x_r]$, where $x_1, \dots, x_r \in T$ are algebraically indepdendent.

Proof. Since T is affine, we have $T = k[a_1, \dots, a_n]$ for some $n \in \mathbb{N}$, $a_i \in T$. We proceed by induction on n. Let r denote the maximal number of algebraically independent elements of $\{a_i\}$. Without loss of generality, $r \geq 1$, since otherwise all elements of T are integral over k (the kernel of the map $k[X] \to k[a]$ contains a monic polynomial for every a), so $R = k$ will do the trick.

If $r = n$, there is nothing to do. Reorder the a_i in such a way that $a_1, \dots, a_r$ are algebraically indepdent and $a_{r+1}, \dots, a_n$ are algebraically dependent on $a_1, \dots, a_r$ over k.

In particular, we find $0 \neq f \in k[X_1, \dots, X_r, X_n]$ such that $f(a_1, \dots, a_r, a_n) = 0$ (this exists because $a_1, \dots, a_r, a_n$ are algebraically dependent). Then f is a sum of terms of the form $\lambda_\ell X_1^{\ell_1} \cdots X_r^{\ell_r} X_n^{\ell_n}$, where $\ell = (\ell_1, \dots, \ell_r, \ell_n)$ and $\ell_i \in \mathbb{N}_0$.

We claim that there are positive integers $m_1, \dots, m_r$ such that $\varphi\colon \ell \mapsto m_1\ell_1 + \cdots + m_r\ell_r + \ell_n$ is injective for those ℓ with $\lambda_\ell \neq 0$.

Since there are only finitely many ℓ such that $\lambda_\ell = 0$, there are only finitely many $d = \ell - \ell'$ with $\lambda_\ell \neq 0$ and $\lambda_{\ell'} \neq 0$. Writing $d = (d_1, \dots, d_r, d_n)$, consider the finitely many $d = (d_1, \dots, d_r) \neq 0$ obtained in this way (observe that we have dropped the final component). Vectors in $\mathbb{Q}^n$ that are orthogonal to one of these r-tuples lie in finitely many $(r-1)$-dimensional subspaces. Hence it is possible to pick $(q_1, \dots, q_r)$ such that each q_i satisfies $q_i > 0$ and $\sum q_i d_i \neq 0$ for all of the finitely many $(d_1, \dots, d_r) \neq 0$. Multiplying by a sufficiently large positive integer, we obtain $(m_1, \dots, m_r) \in \mathbb{Z}_{\geq 0}^r$ satisfying $|\sum m_i d_i| > |d_n|$ for all of the $(d_1, \dots, d_r) \neq 0$

Now if ℓ and ℓ' are such that $\varphi(\ell) = \varphi(\ell')$, define $d = \ell - \ell'$ such that $\varphi(d) = 0$. Notice that this implies $d_1 = \ldots = d_r = 0$, since otherwise we would have $\varphi(d) \neq 0$ by the inequality of absolute values. But then $0 = \varphi(d) = d_n$, hence $\ell = \ell'$. This completes the proof of the claim.

Pick $m_1, \dots, m_r$ as in the claim and set

$$g(X_1, \dots, X_n) \coloneqq f(X_1 + X_n^{m_1}, \dots, X_r + X_n^{m_r}, X_n).$$

Thus, g is a sum of the form

$$\sum_{l\colon \lambda_\ell \neq 0} \lambda_\ell (X_1 + X_n^{m_1})^{\ell_1} \cdots (X_r + X_n^{m_r})^{\ell_r} X_n^{\ell_n}.$$

By our choice of m_i, different terms will have different powers of x_n. Hence, there will be a single term with the highest power of X_n. Viewing g as a polynomial in X_n, the leading coefficient is one of the λ_ℓ, so in particular it is an element of k.

Next, define $b_i \coloneqq a_i - a_n^{m_i}$ $(1 \leq i \leq r)$ and $h(X_n) \coloneqq g(b_1, \dots, b_r, X_n)$.

Then the leading coefficient of h is once again in k and all coefficients are elements of $k[b_1, \dots, b_r]$. Moreover, we may calculate

$$h(a_n) = g(b_1, \dots, b_r, a_n) = f(a_1, \dots, a_r, a_n) = 0,$$

using the definition of g and the defining property of f.

Now divide h by its leading coefficient to find that a_n is integral over $k[b_1, \dots, b_r]$. Additionally, for each $i \leq r$, $a_i = b_i + a_n^{m_i}$ is also integral over $k[b_1, \dots, b_r]$ (recall that sums and products of integral elements are integral).

This means that T is integral over $S \coloneqq k[b_1, \dots, b_r, a_{r+1}, \dots, a_{n-1}]$. Since that is one generator less than before, we find that S is integral over some polynomial algebra R, so T is also integral over R. □

Corollary 4.26. If $\mathfrak{q}$ is a prime of an affine domain T, then we have

$$\operatorname{ht}(\mathfrak{q}) + \dim(T/\mathfrak{q}) = \dim T.$$

Proof. Define $m \coloneqq \operatorname{ht}(\mathfrak{q})$ and pick a chain

$$\mathfrak{q}_0 \subsetneq \cdots \subseteq \mathfrak{q}_m = \mathfrak{q}$$

of primes of maximal length. By Noether normalization, we find some polynomial subsalgebra R of T such that T is integral over R. We have $\dim T = \dim R$ by 4.19 and $\dim T = \dim R = \operatorname{tr}\deg K$, where K is the field of fractions of T, by 4.24. Furthermore, $\dim R$ is the number if indeterminates of R.

Write $\mathfrak{p}_i \coloneqq \mathfrak{q}_i \cap R$. By maximality of the chain, we must have $\operatorname{ht}(\mathfrak{q}_1) = 1$. Since R is a UFD, it is integrally closed (the proof for $R = \mathbb{Z}$ generalized to any UFD), hence 4.20 tells us that $\operatorname{ht}(\mathfrak{p}_1) = 1$. But by 4.5 this implies $\mathfrak{p}_1 = (f)$ for an irreducible polynomial f. By a previous calculation, we conclude that the transcendence degree of the field of fractions of $R/\mathfrak{p}_1$ is $\dim R - 1$.

Now $\operatorname{ht}(\mathfrak{q}/\mathfrak{q}_1) = m - 1$ (TODO: why? Maybe you can make some argument comparing chains in T and $T/\mathfrak{q}_1$ work, but doesn't that just prove the entire lemma?), and $R/\mathfrak{p}_1 \subseteq T/\mathfrak{q}_1$ is an integral extension, so $\dim(T/\mathfrak{q}_1) = \dim(R/\mathfrak{p}_1) = \dim T - 1$ (4.19 and 4.24). Finally, the rings $(T/\mathfrak{q}_1)/(\mathfrak{q}/\mathfrak{q}_1)$ and $T/\mathfrak{q}$ are isomorphic, so putting things together and applying the inductive hypothesis, we find

$$(m-1) + \dim(T/\mathfrak{q}) = \dim T - 1,$$

and adding 1 on both sides yields the claim. □

Theorem 4.27. Let R be a noetherian integral domain that is integrally closed in its field of fractions K. Let L be a separable extension over K, and let T_1 be the integral closure of R in L. Then T_1 is a finitely generated R-module.

Recall that separability always holds in characteristic 0.

Proof. We will make use of the trace function. There are many ways to define it (cf. Galois theory). We will use it as a black box with the following property (cf.

Reid 8.13): if $K \subseteq L$ is separable, then the map $L \times L \to K$ given by $(x,y) \mapsto \mathrm{Tr}(xy)$ is a non-degenerate symmetric K-bilinear form.

Pick a K-basis $z_1, \ldots, z_n$ of L. Each z_i is algebraic over K, so it satisfies a monic polynomial with coefficients in K, say

$$z_i^n + \frac{r_{n-1}}{s_{n-1}} z_i^{n-1} + \cdots + \frac{r_0}{s_0} = 0.$$

By multiplying with the product of the denominators, we can define t_i such that we have an equation of the form

$$t_n z_i^n + t_{n-1} z_i^{n-1} + \cdots + t_0 = 0.$$

Finally, define $y_i \coloneqq t_n z_i$. Then we have

$$\begin{aligned} y_i^n + t_{n-1} y_i^{n-1} + t_n t_{n-2} y_i^{n-2} + t_n^2 t_{n-3} y_i^{n-3} + \cdots + t_n^{n-1} t_0 \\ = t_n^{n-1}(t_n z_n + t_{n-1} z_{n-1} + \cdots t_0) = 0. \end{aligned}$$

□

Corollary 4.28. IfL is any number field, then the integral closure of $\mathbb{Z}$ in L is a finitely generated abelian group.

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 $(r, s) = (r, s') \cdot (1, 0) + (r', s) \cdot (0, 1) \in I$. $\square$

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 $r_1, \ldots, r_n$ and so is I_2, say by $s_1, \ldots, s_m$. 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 $(r_1, 0), \ldots, (r_n, 0), (0, s_1), \ldots, (0, s_n)$. $\square$

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 $S \coloneqq \bigcap_{P \in \mathcal{S}'} P$. 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 $\mathcal{S}_x \coloneqq \{P \in \mathcal{S}' \mid x \in P\}$ and $\mathcal{S}_y \coloneqq \{P \in \mathcal{S}' \mid y \in P\}$. We claim that it is true that

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

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. $\square$

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

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

Exercise 8.

Exercise. Let A be a Noetherian ring and $f \in A[[X]]$. Then f is nilpotent if and only if all of its coefficients are nilpotent.

Solution. First assume that f is nilpotent. Write $f = \sum_{i=0}^{\infty} a_i X^i$ for some $a_i \in A$. We will argue by induction. Since f is nilpotent, there is some $k \in \mathbb{N}$ such that $f^k = 0$. The constant term of f^k is a_0^k, hence a_0 is nilpotent.

Next, assume that $a_0, \dots, a_n$ are nilpotent for some $n \in \mathbb{N}$. Then they are also nilpotent as elements of $A[[X]]$. Since the set of nilpotent elements forms an ideal, we have that $g \coloneqq \sum_{i=0}^{n} a_i X^i$ is nilpotent, so $f - g = \sum_{i=n+1}^{\infty} a_i X^i$ is nilpotent, i.e., there is some k such that $(f-g)^k = 0$. But the $X^{k(n+1)}$-coefficient of $(f-g)^k$ is just a_{n+1}^k, hence a_{n+1} is nilpotent.

Next, assume that $f = \sum_{i=0}^{\infty} a_i X^i$ and every a_i is nilpotent. Denote by I the ideal of A generated by all a_i. Then $I \subseteq N(A)$. Since $N(A) = \sqrt{0}$, by Lemma 1.21, there is some natural number n such that $N(A)^n \subseteq (0)$. Since $I^n \subseteq N(A)^n$, this implies that $I^n = (0)$. Since the coefficients of f^n are elements of I^n, we conclude that $f^n = 0$, so f is nilpotent. □

Exercise 9.

Exercise. Let A be a ring and M an R-module.

(i) $M[X]$ is an $A[X]$-module,
(ii) If P is a prime ideal in A, then $P[X]$ is a prime ideal in $A[X]$. If Q is a maximal ideal of A, is $Q[X]$ a maximal ideal of $A[X]$?
(iii) Let M be a noetherian A-module. Then $M[X]$ is a noetherian $A[X]$-module.

Solution. For the second part, let P be a prime ideal in A. $P[X]$ is obviously an ideal of $A[X]$. Let $f, g \in A[X]$ such that $fg \in P[X]$. We can write

$$f = \sum_{i=0}^{n} a_i X_i, \quad g = \sum_{i=0}^{m} b_i X_i,$$

and also define $a_i = 0$ for $i > n$ and $b_i = 0$ for $i > m$. Suppose that $f \notin P[X]$ and $g \notin P[X]$. Then we find i and j such that $a_i \notin P$, $b_j \notin P$. Choose i and j to be minimal among the possible i and j. Then the coefficient of fg for X^{i+j} is given by

$$\left(\sum_{k=0}^{i-1} a_k b_{i+j-k}\right) + a_i b_j + \left(\sum_{k=i+1}^{i+j} a_k b_{i+j-k}\right).$$

The coefficient is in P, and so are the sums on the left and the right, by minimality of i and j. But then $a_i b_j \in P$, so $a_i \in P$ or $b_j \in P$, a contradiction. Hence $f \in P[X]$ or $g \in P[X]$.

Let Q be a maximal ideal of A. Then $1 \notin Q$, hence $1 \notin Q[X]$ and $X \notin Q[X]$, hence $1 \notin (Q[X], X)$, but $X \in (Q[X], X)$. We conclude that $Q[X] \subsetneq (Q[X], X) \subsetneq A[X]$, so $Q[X]$ is not a maximal ideal.

The proof of the third part is almost identical to the proof of Hilbert's basis theorem. We will show that every submodule of $M[X]$ is finitely generated. Let N be an $A[X]$-submodule of $M[X]$ and define $N_n := \{f \in N \mid \deg f \leq n\}$. We have $0 \in N_n$ and $N_0 \subseteq N_1 \subseteq \cdots$ form an ascending chain.

Define M_n to be the set of coefficients of X^n appearing in elements of N_n. If $m + n \in M_n$ and $a \in A$, then $m + n \in M_n$ and $am \in M_n$. Therefore M_n is an A-submodule of M.

Furthermore, if $m \in M_n$, then $m \in M_{n+1}$ by multiplying the corresponding polynomial by X.

Since M is noetherian, the chain $M_0 \subseteq M_1 \subseteq \cdots$ terminates, so we have k such that $\forall n \geq k$: $M_n = M_k$. Each of $M_0, \ldots, M_k$ is a finited generated submodule of M, say M_j is generated by $m_{j1}, \ldots, m_{j\ell_j}$. There are polynomials $f_{j1}, \ldots, f_{j\ell_j} \in N$ such that $\deg f_{ji} = j$ and the leading coefficient of f_{ji} is m_{ji}.

We will show that the finite set $\{f_{ji} \mid 0 \leq j \leq N, 1 \leq i \leq \ell_j\}$ generated N.

We will use induction on $\deg f$, where $f \in N$. If $\deg f = 0$, then $f = m$ for some $m \in M$. By definition of M_0, $m \in M_0$, and m is in the submodule generated by the f_{0i}.

Assume next that $0 < \deg f \leq k$ and that the claim is true for smaller degrees. Let m be the leading coefficient of f. Then $m \in M_n$ so we may write

$$m = \sum_j a_{nj} m_{nj}.$$

Then

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

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

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

$$m = \sum_j a_{kj} m_{kj}.$$

Then

$$f - X^{n-k} \sum_j a_{kj} f_{kj}$$

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

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 $r \in J(R)$. □

Exercise 11.

Exercise. Any field K which is finitely generated as a ring is a finite field.

Solution. Suppose that K has characteristic zero. Then we can identify $\mathcal{Q}$ with a subfield of K. Since K is finitely generated as a $\mathbb{Z}$-algebra (this is just a different way of saying that K is finitely generated as a ring), it is certainly finitely generated as a $\mathbb{Q}$-algebra. By Zariski's lemma, K is a finite-dimensional $\mathbb{Q}$-vector space.

Hence, all assumptions for the Artin-Tate lemma for the chain $\mathbb{Z} \subseteq \mathbb{Q} \subseteq K$ are satisfied, so we find that $\mathbb{Q}$ is a finitely generated $\mathbb{Z}$-algebra. This is of course nonsense: if we had finitely many generators, then only finitely many primes could appear as divisors of denominators in $\mathbb{Q}$.

Therefore, K has characteristic $p > 0$ and is a finitely generated $\mathbb{Z}$-algebra, so K is also a finitely generated $\mathbb{Z}/p\mathbb{Z}$-algebra. Hence, by Zariski's lemma, K is a finite-dimensional $\mathbb{Z}/p\mathbb{Z}$-vector space, hence K is finite. □

Exercise 12.

Exercise. Let I be an ideal contained in the Jacobson radical of A, and let M be an A-module and N be a finitely generated A-module. Let $\theta\colon M \to N$ be a homomorphism of A-modules. If the induced map $M/IM \to N/IN$ is surjective, then θ is surjective.

Solution. Let $n \in N$. By surjectivity of the induced map, we find $m \in M$ such that $\theta(m) + IN = n + IN$. Hence we find $i \in I$ and $n_1 \in N$ such that $\theta(m) = n + in_1$, hence $n + \theta(M) = i(-n_1) + \theta(M)$. Since n was arbitrary, we conclude

$$\frac{N}{\theta(M)} \subseteq I\frac{N}{\theta(M)} \subseteq J(A)\frac{N}{\theta(M)} \subseteq \frac{N}{\theta(M)}.$$

Since N is finitely generated, so is $N/\theta(M)$, and by Nakayama's lemma, we must have $N/\theta(M) = 0$, so θ is surjective. □

Exercise 13.

Exercise. In the ring A, let Σ be the set of all ideals in which every element is a zero-divisor. Show that the set Σ has maximal elements and that every maximal element of Σ is a prime ideal. Hence show that the set of zero-divisors in A is a union of prime ideals.

Solution. For a zero divisor $a \in A$ denote by Σ_a the set of ideals containing a in which every element is a zero divisor (notice that $\Sigma = \Sigma_0$). Since $(a) \in \Sigma_a$, we know that Σ_a is nonempty. Furthermore, the union of a chain of ideals in Σ_a is once again an element of Σ_a, hence Σ_a admits a maximal element I_a by Zorn's lemma.

Let $x, y \in A$ such that $xy \in I_a$, $x \notin I_a$ and $y \notin I_a$. Then The ideals $I_a + Ax$ and $I_a + Ay$ contain non-zero-divsors u and v. Write $u = i + u_1x$ and $v = j + u_2y$ with $i, j \in I_a$, $u_1, u_2 \in A$. Then $uv = ij + iu_2y + ju_1x + u_1u_2xy \in I_a$, hence uv is a zero divisor, but then u and v are also zero divisors, a contradiction.

Hence I_a is prime and if Z is the set of zero divisors, then we find that

$$Z = \bigcup_{a \in Z} I_a$$

as required. □

Exercise 15.

Lemma. Let $q_1, \dots, q_n$ be pairwise distinct maximal ideals of a ring A. Then we have

$$\bigcap_{i=1}^{n} q_i = \prod_{i=1}^{n} q_i.$$

Proof. We will procedd by induction on n. The claim is obviously true for $n = 1$. Suppose that

$$Q \coloneqq \bigcap_{i=1}^{n} q_i = \prod_{i=1}^{n} q_i$$

and q_{n+1} is a maximal ideal distinct from the q_i. We have $Q \nsubseteq q_{n+1}$, because otherwise there would be some $i \leq n$ such that $q_i \subseteq q_{n+1}$, since q_{n+1} is prime. But then we would have $q_i = q_{n+1}$, a contradiction. Hence $Q + q_{n+1} = A$ by maximality of q_{n+1}, so we find $u \in Q$ and $v \in q_{n+1}$ such that $u + v = 1$. It is obvious that $Qq_{n+1} \subseteq Q \cap q_{n+1}$. Conversely, let $x \in Q \cap q_{n+1}$. Then $x = x(u + v) = xu + xv \in Qq_{n+1}$, so the claim follows. □

Lemma. Let A be an artinian ring. Then A has finitely many maximal ideals.

Proof. Otherwise, let $q_1, q_2, \dots$ denote pairwise distinct maximal ideals of A. Define $Q_n \coloneqq \bigcap_{i=1}^{n} q_i$. Then $Q_n \supsetneq Q_{n+1}$, since otherwise we would have $Q_n \subseteq q_{n+1}$, but by the preceding lemma and primality of q_{n+1}, this would imply that $q_i \subseteq q_{n+1}$ for some $i \leq n$, hence $q_i = q_{n+1}$, which is not the case. Therefore, the Q_i form a strictly descending chain, which cannot exist since A is artinian. □

Exercise. Let A be an artinian ring. Then A is noetherian.

Solution. By the second lemma, A has finitely many maximal ideals $q_1, \dots, q_n$. By a result from the lecture, since A is artinian, we have $N(A) = J(A)$, hence $\sqrt{0} = \bigcap_{i=1}^n q_i = \prod_{i=1}^n q_i$, where we have used the first lemma in the second step. Define $Q_m := \prod_{i=1}^n q_i^m = \sqrt{0}^m$. The Q_i form a decreasing chain of ideals. Since A is artinian, this chain terminates, say at Q_k. We claim that $Q_k = 0$. Indeed, assume that there is some $0 \neq a \in Q_k$. Since $a \in \sqrt{0}$, $a_\ell = 0$ for some ℓ. But then...? $\square$

Exercise 4.

Exercise. If A is a noetherian ring, then $A[[X]]$ is a noetherian ring.

Solution. Let $I \subseteq A[[X]]$ be an ideal. For a natural number n define $R(n)$ to be the set of trailing coefficients of elements of the form $a_n X^n +$ higher order terms in $I \cap (X^n)$. As in the proof of Hilbert's basis theorem, we have $R(0) \subseteq \dots$. Since A is noetherian, wie find N such that $R(n) = R(N)$ for all $n \geq N$. For $0 \leq i \leq N$, $R(i)$ is finitely generated, say by r_{ij}, $0 \leq i \leq N$, $1 \leq j \leq k_i$. We find $f_{ij} \in I$ such that $f_{ij} = r_{ij} X^i +$ higher order terms. We claim that I is generated by the f_{ij}. Indeed, if $f \in I$, we can choose c_{ij} for $1 \leq i \leq N$, $1 \leq j \leq k_i$ such that $f' := f - \sum_{i,j} c_{ij} f_{ij} \in (X^{N+1})$.

Now let $g_i \in A[[X]]$, $1 \leq i \leq k_N$. Write $f' = \sum_{j=N+1}^\infty a_j X^j$, $f_{Ni} = \sum_{j=N}^\infty b_{ij} X^j$, $g_i = \sum_{j=0}^\infty c_{ij} X^j$. For any k, the k-th coefficient of $\sum_{i=1}^{k_N} f_{Ni} g_i$ is given by

$$\begin{aligned}
\sum_{t=1}^{k_N} \sum_{i+j=k} b_{ti} c_{tj} &= \sum_{t=1}^{k_N} \sum_{i=1}^{k} b_{ti} c_{t(k-1)} \\
&= \left(\sum_{t=1}^{k_N} \sum_{i=N+1}^{k} b_{ti} c_{t(k-i)} \right) + \sum_{t=1}^{k_N} r_{Nt} c_{t(k-N)}.
\end{aligned}$$

Hence, we can define the g_i inductively in such a way that the k-th coefficient of $\sum f_{Ni} g_i$ is precisely a_k: since $R(k) = R(N)$, there is a choice of $c_{t(k-N)}$ that works. Therefore, $f' = \sum f_{Ni} g_i$, so f is indeed in the span of the f_{ij}, hence I is finitely generated. $\square$

Lemma. If $\varphi \colon R \to S$ is a surjective homomorphism of rings and R is noetherian, then S is noetherian.

Proof. Any chain of ideals I_i of R can be pulled back to a chain $\varphi^{-1}(I_i)$ of ideals in R. Since R is noetherian, this chain terminates, but since $I_i = \varphi(\varphi^{-1}(I_i))$ by surjectivity of φ, the chain I_i terminates as well. $\square$

Exercise. If A is a ring and $A[X]$ or $A[[X]]$ is noetherian, then so is A.

Solution. There are surjective maps $A[X] \to A$ and $A[[X]] \to A$ sending a polynomial or formal power series to its constant term, hence the claim follows using the previous lemma. $\square$

Exercise 14.

Exercise. If M, M', M'' have finite length and we have a short exact sequence

$$0 \longrightarrow M' \xrightarrow{\iota} M \xrightarrow{\varphi} M'' \longrightarrow 0,$$

then $\ell(M') - \ell(M) + \ell(M'') = 0$

Solution. If

$$M' = M'_0 \supset M'_1 \supset \cdots \supset M'_n = 0$$

and

$$M'' = M''_0 \supset M''_1 \supset \cdots \supset M''_m = 0$$

are composition series, then

$$M = \varphi^{-1}(M_0'') \supset \cdots \supset \varphi^{-1}(M_m'') = \iota(M_0') \supset \cdots \supset \iota(M_n') = 0$$

is a composition series, since φ induces an isomorphism

$$\frac{\varphi^{-1}(M_i')}{\varphi^{-1}(M_{i+1}')} \to \frac{M_i'}{M_{i+1}'}.$$

Hence $\ell(M) = \ell(M') + \ell(M'')$. □

Exercise. If V is a k-vector space, the following are equivalent:

(1) V has finite dimension,
(2) V has finite length,
(3) V satisfies the ascending chain condition,
(4) V satisfies the descending chain condition.

Solution. If V has a finite basis $v_1, \ldots, v_n$, then defining $V_i \coloneqq \langle v_1, \ldots, v_{n-i} \rangle$ gives a composition series, hence (1) implies (2).

(2) implies (3) and (2) implies (4) by part (i) of the exercise.

If V is not finite-dimensional, then choose a basis B and let $v_1, v_2, \ldots \in B$ pairwise distinct. Then

$$\langle v_1 \rangle \subsetneq \langle v_1, v_2 \rangle \subsetneq \ldots$$

is an infinite strictly ascending chain and

$$\langle B \rangle \supsetneq \langle B \setminus \{v_1\} \rangle \supsetneq \ldots$$

is an infinite strictly descending chain. Hence (3) implies (1) and (4) implies (1). □

Exercise. If A is a ring in which the zero ideal is a product $P_1 \cdots P_n$ of not necessarily distinct maximal ideals, then A is noetherian iff A is artinian

Solution. Consider the chain

$$A \supseteq P_1 \supseteq P_1 P_2 \supseteq \cdots \supseteq P_1 \cdots P_n = 0.$$

The A-module $A_i \coloneqq P_1 \cdots P_i / P_1 \cdots P_{i+1}$ is an A/P_{i+1}-vector space in the obvious way. If A is noetherian or artinian, then so is A_i (since it is a quotient of a submodule of A), and by part (iii) we obtain a composition series for A_i, using that an A-submodule is the same thing as a A/P_{i+1}-submodule.

Pulling back the composition series along the projection for every i and stitching together the results, we obtain a composition series for A. Again by part (i), we find that A is both noetherian and artinian. □

Example Sheet 2

Exercise 1.

Exercise. If S is a multiplicatively closed subset of a ring R, and M is a finitely generated R-module, then $S^{-1}M = 0$ if and only if there is some $s \in S$ such that $sM = 0$.

Solution. If $S^{-1}M = 0$, then for all $m \in M$ we have $(m, 1) \sim (0, 1)$, hence we find $s \in S$ such that $sm = 0$. In partiular, if M is generated by $m_1, \ldots, m_n$, we find s_i such that $s_i m_i = 0$. Define $s \coloneqq \prod s_i$, then for any $m \in M$, we find $r_i \in R$ such that $sm = s(r_1 m_1 + \cdots + r_n m_n) = 0$, so $sM = 0$.

The converse direction is trivial. □

Exercise 2.

Exercise. Let I be an ideal of R, and define $S \coloneqq 1+I$. Then $S^{-1}I \subseteq J(S^{-1}R)$.

Solution. Let $i/s \in S^{-1}I$ and let $r/t \in S^{-1}R$. Then

$$\alpha \coloneqq 1 - \frac{i}{s}\frac{r}{t} = 1 - \frac{ri}{st} = \frac{st - ri}{st}.$$

We have $st \in 1 + I$ and $ri \in I$, hence $st - ri \in 1 + I$, so α is a unit. By Exercise 10 on Example Sheet 1 we have $i/s \in J(S^{-1}R)$. $\square$

Exercise 3.

Exercise. A multiplicatively closed set is saturated if and only if $R \setminus S$ is a union of prime ideals.

Solution. If S is saturated and $x \in R \setminus S$, let Σ denote the set of ideals I such that $I \subseteq R \setminus S$ and $x \in I$.

If $y \in R$, then $xy \in R \setminus S$, since otherwise we would have $x \in S$ by saturation of S. Hence $(x) \in \Sigma$.

The set Σ admits upper bounds, as the union of a chain of ideals once again is an ideal in Σ.

Hence we have a maximal element $I \in \Sigma$, which is prime, since if $ab \in I$ and $a \notin I$, $b \notin I$, then $I + Ra$ and $I + Rb$ both intersect nontrivially with S, so for $s_1 \in S \cap I + Ra, s_2 \in S \cap I + Rb$ we have $s_1 s_2 \in S \cap I = \varnothing$, a contradiction.

Hence every element of $R \setminus S$ is contained in a prime ideal which is fully contained in $R \setminus S$, so $R \setminus S$ is the union of these prime ideals.

Conversely, if $R \setminus S$ is the union of prime ideals and $xy \in S$, then if $x \notin S$, then x was contained in one of the ideals, and by the ideal property, so would be xy, a contradiction. Hence $x \in S$ and symmetrically $y \in S$. $\square$

Exercise. If S is a multiplicatively closed subset of R, there is a unique smallest saturated multiplicatively closed subset S' containing S, and it is given as thr complement in R of the union of the prime ideals which do not meet S.

Solution. Define S' as the complement of the unions of the prime ideals which do not meet S. The set S' is multiplicatively closed (since the ideals are prime) and saturated by (i). Furthermore, by definition have $R \setminus S' \subseteq R \setminus S$, hence $S \subseteq S'$.

Let S'' be a saturated multiplicatively closed subset satisfying $S \subseteq S''$. By (i), $R \setminus S''$ is a union of prime ideals p_i. Let $p_i \subseteq R \setminus S'' \subseteq R \setminus S$ be one of these prime ideals. Then $p_i \cap S = \varnothing$, so $p_i \subseteq R \setminus S'$. Hence we have $R \setminus S'' \subseteq R \setminus S'$, so $S' \subseteq S''$, completing the proof that S' is minimal. $\square$

Exercise 4.

Exercise. Let S, T be two multiplicatively closed subsetes of R, and let U be the image of T in $S^{-1}R$. Then $(ST)^{-1}R$ and $U^{-1}S^{-1}R$ are isomorphic as rings.

Solution. Consider the following commutative diagram.

$$\begin{tikzcd}
R \arrow[r, "\alpha"] \arrow[dr, "\beta"] & S^{-1}R \arrow[r, "\delta"] \arrow[d, "\gamma"] & U^{-1}S^{-1}R \arrow[dl, shift right, "\Phi"'] \\
& (ST)^{-1}R \arrow[ur, shift right, "\Psi"'] &
\end{tikzcd}$$

The maps α, β and δ are localization maps. Since $S \subseteq ST$, $\beta(s)$ is a unit for every $s \in S$, hence from the universal property of localization we have $\gamma \colon S^{-1}R \to (ST)^{-1}R$ satisfying $\gamma \circ \alpha = \beta$. An element of U is of the form $\alpha(t)$ for some $t \in T$.

We have $\gamma(\alpha(t)) = \beta(t)$, which is invertible, hence again from the universal property we have a map $\Phi\colon U^{-1}S^{-1}R \to (ST)^{-1}R$ such that $\Phi \circ \delta = \gamma$. We know how this map is defined: if $r \in R$, $s \in S$, $t \in T$, we have

$$\Phi\left(\frac{r/s}{\alpha(t)}\right) = \gamma(r/s)\gamma(\alpha(t))^{-1} = \beta(r)\beta(s)^{-1}\beta(t)^{-1} = \frac{r}{1}\frac{1}{s}\frac{1}{t} = \frac{r}{st}.$$

Next, let $st \in ST$. We have

$$\delta(\alpha(st)) = \delta(\alpha(s))\delta(\alpha(t)) = \frac{s/1}{1}\frac{\alpha(t)}{1}.$$

This has the inverse

$$\frac{1/s}{1}\frac{1}{\alpha(t)},$$

so it is a unit, and the universal property yields $\Psi\colon (ST)^{-1}R \to U^{-1}S^{-1}R$ satisfying $\Psi \circ \beta = \delta \circ \alpha$. Again, if $r \in R$, $s \in S$ and $t \in T$, we have

$$\Psi\left(\frac{r}{st}\right) = \delta(\alpha(r))\delta(\alpha(st))^{-1} = \frac{r/1}{1}\frac{1/s}{1}\frac{1}{\alpha(t)} = \frac{r/s}{\alpha(t)},$$

where we have used our inverse calculation from above.

Hence, Φ and Ψ are two-sided inverses of each other, finishing the proof. □

Exercise 5.

Exercise. Let R be a ring. Suppose that for each prime ideal P the local ring R_P has no non-zero nilpotent element. Then R has no nonzero nilpotent element.

Solution. Let $x \in R$ be a nilpotent element. Consider the ideal $\operatorname{ann}(x) = \{r \in R \mid rx = 0\}$. If $\operatorname{ann}(x) \neq R$, then $\operatorname{ann}(x) \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Then $\mathfrak{m}$ is prime. Let $\varphi\colon R \to R_{\mathfrak{m}}$. Since x is nilpotent, we find n such that $x^n = 0$. Then $\varphi(x)^n = \varphi(x^n) = 0$, hence $\varphi(x) = 0$. By definition of localization, this means that there is some $s \in R \setminus \mathfrak{m}$ such that $sx = 0$. But then $s \in \operatorname{ann}(x)$, which is a contradiction. Hence we must have $\operatorname{ann}(x) = R$, in particular $x = 1 \cdot x = 0$. □

Exercise. There is a ring R such that R is not an integral domain, but for every prime ideal P of R, R_P is an integral domain.

Solution. Define $R \coloneqq \mathbb{Z}/6\mathbb{Z}$. The prime ideals of R are (2) and (3). By writing down all elements and checking the relations between them, we can check that the localizations at both of them are fields, hence integral domains. □

Exercise 7.

Exercise. Suppose $R \neq 0$ and let Σ be the set of mall multiplicatively closed subsets S of R such that $0 \notin S$. Then Σ has maximal elements, and $S \in \Sigma$ is maximal if and only if $R \setminus S$ is a minimal prime ideal of R.

Solution. The union of a chain in Σ is again an element of Σ, and the singleton set $\{1\}$ is an element of Σ. Hence, Σ admits maximal elements by Zorn's lemma.

If $S \in \Sigma$ is maximal, we claim that $I \coloneqq R \setminus S$ is a prime ideal. If $r, s \in I$, then SM_r and SM_s, where $M_r \coloneqq \{1, r, r^2, \ldots\}$, are multiplicatively closed subsets. Since $r, s \notin S$, these are strictly larger than S, hence must contain 0, i.e., we find natural numbers n, m and $x, y \in S$ such that $xr^n = 0 = ys^m$. Then $xy(r+s)^{n+m} = 0$ by the binomial theorem, so we must have $r + s \in I$, since otherwise we would have $0 \in S$, a contradiction.

If $r \in R$, $t \in I$, then again we find $n \in \mathbb{N}$ and $x \in S$ such that $xt^n = 0$. Then $r^n x t^n = 0$, so if we have $rt \in S$, then $0 \in S$, hence $rt \in I$. This makes I into an ideal.

Next, let $r, s \in R$ such that $rs \in I$. Again, this means that we find $n \in \mathbb{N}$ and $t \in S$ such that $(rs)^n t = 0$. If r and s were both in S, this would again lead to the contradiction $0 \in S$, hence $r \in I \vee s \in I$, making I into a prime ideal.

It remains to show that I is minimal. If $\mathfrak{p} \subseteq I$ is a prime ideal, then $R \setminus \mathfrak{p}$ is multiplicative, does not contain 0, and satisfies $S \subseteq R \setminus \mathfrak{p}$. By maximality of S, we find $S = R \setminus \mathfrak{p}$, so $\mathfrak{p} = I$.

Conversely, assume that $R \setminus S$ is a minimal prime ideal. Then S is multiplicative, because $R \setminus S$ is prime. Suppose S is not maximal. Then we have $S \subsetneq S'$ for some maximal element S' of Σ. Then by what we have just shown, $R \setminus S'$ is a minimal prime ideal, but then $R \setminus S$ cannot be a minimal prime, since it is a strict superset of $R \setminus S'$. □

Exercise. Every minimal prime ideal of R is contained in D, the set of zero divisors of R.

Solution. Let $a \in S_0$ be a non-zero-divisor and let S be a maximal element of Σ. Then SM_a cannot contain 0, since S does not contain 0 and M_a does not contain zero divisors. Hence $S \subseteq SM_a \in \Sigma$, which implies $SM_a = S$ by maximality. In particular, $a \in S$, so $S_0 \subseteq S$ for every maximal element S of Σ.

Now if $\mathfrak{p}$ is a minimal prime ideal, then $R \setminus \mathfrak{p}$ is a maximal element of Σ. Hence we have $S_0 \subseteq R \setminus \mathfrak{p}$. Taking complements, we obtain $\mathfrak{p} \subseteq R \setminus S_0 = D$ as required. □

Exercise. (i) S_0 is the largest multiplicatively closed subset of R for which the homomorphism $R \to S_0^{-1}R$ is injective.
(ii) Every element in $S_0^{-1}R$ is either a zero-divisor or a unit.
(iii) Every ring in which every non-unit is a zero-divisor is equal to its total ring of fractions satisfies that $R \to S_0^{-1}R$ is bijective.

Solution. For (i), let S be any multiplicatively closed set. We claim that $\varphi \colon R \to S^{-1}R$ is injective if and only if S contains no zero divisors.

Indeed, $\varphi(r) = 0$ if and only if $r/1 = 0/1 \in S^{-1}R$, i.e., if and only if there exists $s \in S$ such that $rs = 0$. So there is some nonzero r satisfying $\varphi(r) = 0$ if and only if S contains a zero divisor.

Since S_0 is the largest multiplicatively closed subset without zero divisors, the claim follows.

For (ii), let $r/s \in S_0^{-1}R$. If $r \in S_0$, then r/s is a unit, since $r/s \cdot s/r = 1$. Conversely, if $r \notin S_0$, then r is a zero divisor, so we find $0 \neq q \in R$ such that $rq = 0$. Since S_0 does not contain zero divisors, we have $q/1 \neq 0 \in S^{-1}R$. Then $r/s \cdot q/1 = 0/s = 0 \in S^{-1}R$, so r/s is a zero divisor.

For (iii), observe that if every non-unit is a zero divisor, every non-zero-divisor is a unit. Hence the universal property of localisation yields a map θ making the diagram

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[dr, "\mathrm{id}"'] & S_0^{-1}R \arrow[d, "\theta"] \\ & R \end{tikzcd}$$

commute. It remains to verify that $\varphi \circ \theta = \mathrm{id}_{S_0^{-1}R}$. Indeed, if $r \in R$ and $s \in S_0$, then $\varphi(\theta(r/s)) = \varphi(rs^{-1}) = (rs^{-1})/1$. But since $1(rs^{-1}s - r) = 0 \in R$, we have $r/s = (rs^{-1})/1 \in S_0^{-1}R$, completing the proof. □

Exercise 8.

Exercise. If $m, n \in \mathbb{Z}$ are coprime, then $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ is trivial.

Solution. Bézout's lemma yields $a, b \in \mathbb{Z}$ such that $am + bn = 1$. The module $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ is generated by elements of the form $x \otimes y$, $x \in \mathbb{Z}/m\mathbb{Z}$, $y \in \mathbb{Z}/n\mathbb{Z}$. For any such element, we have

$$\begin{aligned} x \otimes y &= (am + bn)(x \otimes y) = am(x \otimes y) + bn(x \otimes y) = a(mx \otimes y) + b(x \otimes ny) \\ &= a(0 \otimes y) + b(x \otimes 0) = 0. \end{aligned}$$

□

Exercise 11.

Exercise. Let M_i $(i \in I)$ be a family of R-modules and let M be their direct sum. Then M is flat if and only if each M_i is flat.

Solution. The proof of the distributive property for tensor products generalizes without changes to yield an isomorphism

$$\begin{aligned} A \otimes \bigoplus_i M_i &\to \bigoplus_i A \otimes M_i \\ a \otimes m_i &\mapsto a \otimes m_i, \end{aligned}$$

where $a \in A$ and $m_i \in M_i$.

Since a sequence of direct sums of maps is exact if and only if the corresponding sequences are exact, the claim follows. □

Exercise. $R[X]$ is a flat R-algebra.

Solution. $R[X]$ is an R-algebra. Flatness is a property of R-modules, and as an R-module, we have $R[X] \cong \bigoplus_{n\in\mathbb{N}} R$. Since R is flat, the claim follows. □

Exercise 14.

Exercise. The torsion elements of M form a submodule $T(M)$ of M.

Solution. If $m \in T(M)$, i.e., we find $0 \neq r \in A$ such that $rm = 0$ and $s \in A$, then $sm \in T(M)$, since $rsm = srm = s0 = 0$.

If $m, n \in T(M)$, i.e., we find $0 \neq r, s \in A$ such that $rm = 0 = sn$, then $rs \neq 0$ since A is an integral domain, so $m+n \in T(M)$, since $rs(m+n) = srm+rsn = 0$. □

Exercise. If M is an A-module, then $M/T(M)$ is torsion-free.

Solution. If $m + T(M) \in M/T(M)$ satisfies $r(m + T(M)) = 0$ for $r \neq 0$, then $rm \in T(M)$, hence we find $s \neq 0$ such that $srm = 0$. Since A is an integral domain, $sr \neq 0$, hence $m \in T(M)$, so $m + T(M) = 0$, so $T(M/T(M)) = 0$ as claimed. □

Exercise. If $f\colon M \to N$ is a homomorphism of A-modules, then $f(T(M)) \subseteq T(N)$.

Solution. Let $m \in T(M)$, i.e., we find $0 \neq r \in A$ such that $rm = 0$. Then $rf(m) = f(rm) = f(0) = 0$, hence $f(m) \in T(N)$. □

Exercise. If

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$$

is exact, then

$$0 \longrightarrow T(M') \xrightarrow{f|_{T(M')}} T(M) \xrightarrow{g|_{T(M)}} T(M'')$$

is exact.

Solution. It is obvious that $f|_{T(M')}$ is injective and that $\operatorname{im} f|_{T(M')}$ is contained in $\ker g|_{T(M)}$.

Let $m \in \ker g|_{T(M)}$. By exactness of the original sequence, we find $m' \in M'$ such that $f(m') = m$. Since $m \in T(M)$, we find $0 \neq r \in A$ such that $0 = rm = rf(m') = f(rm')$. By injectivity of f, we conclude $rm' = 0$, so $m' \in T(M')$, so $m = f|_{T(M')}(m')$, so $m \in \operatorname{im} f|_{T(M')}$. □

Exercise 15.

Exercise. If S is a multiplicatively closed subset of an integral domain A, then $T(S^{-1}M) = S^{-1}T(M)$ as $S^{-1}R$-submodules of $S^{-1}M$.

Solution. The claim is trivial if $0 \in S$. Hence, in the remainder, we will assume that $0 \notin S$.

Let $m/s \in T(S^{-1}M)$, i.e., we find $0 \neq r/t \in S^{-1}R$ such that $rm/st = 0/1$, i.e., there is some $u \in S$ such that $urm = 0$. Observe that $r \neq 0$, otherwise we would have $r/t = 0 \in S^{-1}R$, and $u \neq 0$, since $u \in S$. Since A is an integral domain, this implies that $ru \neq 0$, hence $m \in T(M)$, so $m/s \in S^{-1}T(M)$.

Conversely, let $m/s \in S^{-1}(T(M))$. This means that we find $0 \neq r \in A$ such that $rm = 0$. Then $r/1 \cdot m/s = 0/s = 0 \in S^{-1}M$, i.e., $m/s \in T(S^{-1}M)$, completing the proof. □

Exercise. The following are equivalent for a module M over an integral domain A.

(a) M is torsion-free,
(b) $M_{\mathfrak{p}}$ is torsion-free for all prime ideals $\mathfrak{p}$,
(c) $M_{\mathfrak{m}}$ is torsion-free for all maximal ideals $\mathfrak{m}$.

Solution. To show that (a) implies (b), notice that from the previous result we have $T(M_{\mathfrak{p}}) = T(M)_{\mathfrak{p}}$ as $S^{-1}R$-submodules of $M_{\mathfrak{p}}$. But the right hand side is trivial as $T(M) = 0$.

The implication from (b) to (c) is trivial.

Finally, assume that $T(M_{\mathfrak{m}})$ is trivial for all maximal ideals $\mathfrak{m}$. Let $m \in T(M)$. Consider the annihilator $\operatorname{ann}(m) = \{r \in R \mid rm = 0\}$. Suppose $\operatorname{ann}(m)$ is a proper ideal. Then $\operatorname{ann}(m) \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. By Exercise 14(ii) and our assumption, m is in the kernel of the map $M \to M_{\mathfrak{m}}$, so we find $s \in R \setminus \mathfrak{m}$ such that $sm = 0$. But then $s \in \operatorname{ann}(m) \cap R \setminus \mathfrak{m} = \varnothing$, a contradiction. We conclude $\operatorname{ann}(m) = R$, so in particular $m = 1 \cdot m = 0$, i.e., M is torsion-free. □