

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
Chapter 5. I -adic topology	45
1. Topology and completion	47
Exercises	53
Example Sheet 1	53
Example Sheet 2	59
Example Sheet 4	64

CHAPTER 0

Introduction

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

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

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

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

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

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

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

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

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

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

It turns out that S is generated as a ring by these e_i and the canonical map $k[Y_1, \dots, Y_n] \rightarrow S$ 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 $\mathbb{C}^n \rightarrow \mathbb{C}$ 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 affine n -space.

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

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

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)

$$\bigcap_j Z(I_j) = Z\left(\bigcup_j I_j\right),$$

$$\bigcup_{j=1}^n Z(I_j) = Z\left(\prod_{j=1}^n I_j\right)$$

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

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

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 correspondence

$$I \mapsto Z(I)$$

$$I(S) \leftarrow S$$

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

Dimension

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

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

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

Most of the theory dates between 1920 and 1950.

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

CHAPTER 1

Noetherian Rings

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

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

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

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

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

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

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

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

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

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

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

ALTERNATIVE PROOF. It suffices to show that if

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

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

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

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

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

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

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

Rearranging gives

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

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

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

- (i) $M \oplus N$ is noetherian if and only if both M and N are.
- (ii) $M_1 \oplus \dots \oplus M_n$ 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 $M_1 + \dots + M_n$, 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 $\theta: M \rightarrow N$, 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 noetherian, then so is $M_1 \oplus \dots \oplus M_n$, and since the map

$$\begin{aligned} M_1 \oplus \dots \oplus M_n &\rightarrow M_1 + \dots + M_n, \\ (m_1, \dots, m_n) &\mapsto m_1 + \dots + m_n \end{aligned}$$

is surjective, $M_1 + \dots + M_n$ is noetherian. \square

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

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

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

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 $I_0 \subseteq I_1 \subseteq \dots$ 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 $R_0 \subseteq R_1 \subseteq \dots$ terminates, so we have N such that $\forall n \geq N: R_n = R_N$. Each of R_0, \dots, R_N is a finitely generated ideal of R , say R_j is generated by a_{j1}, \dots, a_{jk_j} . There are polynomials f_{j1}, \dots, 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 noetherian.

- 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.
- $k[X_1, X_2, \dots]$ is not noetherian, as there is an infinite chain $(X_1) \subsetneq (X_1, X_2) \subsetneq \dots$.
- $k[X_1, \dots, X_n]$ is noetherian, by Hilbert's basis theorem and induction.
- $\mathbb{Z}[X_1, \dots, X_n]$ is noetherian: every finitely generated commutative ring is noetherian, since if R is generated by r_1, \dots, r_n , we have a surjective map $\mathbb{Z}[X_1, \dots, X_n] \rightarrow R$ 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 multiplication defined as the \mathbb{Z} -bilinear continuation of $(a, b) \mapsto ab$. If A is generated by g_1, \dots, g_n , then $\mathbb{Z}A$ is generated as a ring by $g_1, g_1^{-1}, \dots, g_n, g_n^{-1}$.

- 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 algebra.
- 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 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. Suppose 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 $i_1 + r_1a, \dots, i_n + r_na$. Define

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

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

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

$$t = u_1(i_1 + r_1a) + \dots + u_n(i_n + r_na)$$

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

$$t = u_1i_1 + \dots + u_ni_n + (u_1r_1 + \dots + u_nr_n)a.$$

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 $u_1r_1 + \dots + u_nr_n \in J$ by definition of J , so indeed $t \in Ri_1 + \dots + Ri_n + Ja$ and we are done. \square

LEMMA 1.10. Let p be a prime ideal of $R[[X]]$ and $\theta: R[[X]] \rightarrow R$ 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 $\theta(p) = Ra_1 + \dots + Ra_n$.

If $X \in p$, then p is generated by a_1, \dots, 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 $f \in Ra_1 + \dots + Ra_n + X$.

On the other hand, if $X \notin p$, let $f_1, \dots, f_n \in p$ have constant terms a_1, \dots, a_n (these exist by definition of θ). We will show that p is generated by f_1, \dots, 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 $h_j := \sum_{i=0}^{\infty} r_{i,j} X^i$. 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, \dots, f_n as required. \square

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 $s+t = m+n-1$. 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 $s = 0$. \square

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 $I := \bigcap_{p \text{ prime}} p$.

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 $J_1 \in \mathcal{S}$. \square

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

$$\sqrt{I} := \{r \in R \mid \exists n \in \mathbb{N}: r^n \in I\}$$

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 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 $R \rightarrow M/M_1$ 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. \square

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 $p = \{\frac{m}{n} \in \mathbb{Q} \mid p \mid n, p \nmid m\}$, 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 $(X) \supseteq (X^2) \subseteq \dots$.

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, $(x) \supseteq (x^2) \subseteq \dots$ becomes stationary, so there is a number n and some $y \in R$ such that $x^n = yx^{n+1}$. Rearranging, we have $x^n(1 - xy) = 0 \in p$. Since p is prime and $x \notin p$, $x^n \notin p$, so we must have $1 - xy \in p$, so $x + p$ has the inverse $y + p$ in R/p . Since x was arbitrary, R/p is a field, so p is maximal.

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

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

$$(1) \quad t_i = \sum_{j=1}^m s_{ij}x_j$$

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

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

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 $\varphi: R[X_1, \dots, X_k] \rightarrow S_0$. 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. \square

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 transcendental, 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. \square

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 $R := T/m$. 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 $\Phi: k \rightarrow k[X_1, \dots, X_n] \rightarrow k[X_1, \dots, X_n]/m$ is an isomorphism. Let $a_i := \Phi^{-1}(X_i)$. Then we have that $I := (X_1 - a_1, \dots, X_n - a_n) \subseteq \ker \Phi = m$.

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

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

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

Minimal and associated primes

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

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

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

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

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

Indeed, if I is not prime, then there are ideals $J'_1, J'_2 \not\subseteq I$ such that $J'_1 J'_2 \subseteq I$ (indeed we can find principal ideals that work). Defining $J_1 := J'_1 + I$, $J_2 := J'_2 + I$, we find that $I \subsetneq J_i$, but $J_1 J_2 \subseteq I$. Since I was maximal, we can write

$$\sqrt{J_1} = Q_1 \cap \cdots \cap Q_n, \quad \sqrt{J_2} = Q'_1 \cap \cdots \cap Q'_m,$$

where all Q_i, Q'_i are prime.

Now define

$$J := \sqrt{J_1} \cap \sqrt{J_2} = Q_1 \cap \cdots \cap Q_n \cap Q'_1 \cap \cdots \cap Q'_m.$$

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

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

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

REMARK. If we have written $\sqrt{I} = p_1 \cap \cdots \cap p_m$ 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 $p_i \not\subseteq p_j$ for all pairs $i \neq j$. Now if p is another prime ideal and $\sqrt{I} \subseteq p$, then $p_1 \cdots p_m \subseteq \bigcap p_i = \sqrt{I} \subseteq p$, some since p is prime, one of the p_i must be fully contained in p .

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

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

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

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

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

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

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

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

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

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

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

We further define

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

EXAMPLE. If p is a prime ideal of R , then $\text{Ass}(R/p) = \{p\}$. Indeed, if $r \in R$, then there are two cases. If $r \in p$, then $\text{ann}(r + p) = \text{ann}(0) = R$, 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 $\text{ann}(r) = p$.

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

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

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

PROOF. Suppose M is generated by m_1, \dots, m_k . Define $I_j := \text{ann}(m_j)$. Then

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

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

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

PROOF. Let $Q \in \text{ann}(m)$ 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 $r_1 \in \text{ann}(r_2 m)$. Since, $r_2 \notin Q$, we have that $r_2 m \neq 0$.

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

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

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

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 $\text{ann}(m_1)$ is a prime ideal. Set $M_1 = Rm_1$. Then the kernel of the map $R \rightarrow M_1$ given by $r \mapsto rm_1$ is precisely $\text{ann}(m_1)$, 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 $\text{ann}(m_{i+1} + M_i)$ is a prime ideal. Set $M_{i+1} := M_i + Rm_{i+1}$. Then the map $R \rightarrow M_{i+1}/M_i$ given by $r \mapsto rm_{i+1} + M_i$ is surjective and has kernel $\text{ann}(m_{i+1} + M_i)$. 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. \square

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

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

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

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

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

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

PROOF. Take a chain

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

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 $\text{Ass}(R/p_0) = \{p_0\}$.

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

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 $p_1^{s_1} \cdots p_n^{s_n} \subseteq I$. Additionally, we may assume that $i \neq j$ implies $p_i \neq p_j$.

Define

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

and let $J := \text{ann}(M)$. Clearly, every element of $p_1^{s_1}$ annihilates M , so $p_1^{s_1} \subseteq J$. Furthermore, we have

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

but p_1 is prime and we cannot have $p_i^{s_i} \subseteq p_1$ for $i \neq 1$ as the p_i are minimal primes, so we must have $J \subseteq p_1$. In particular, $J \neq R$, so $M \neq 0$.

Invoke (1.29) to obtain a chain

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

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

Since $p_1^{s_1}$ annihilates M , in particular it annihilates M_j/M_{j-1} for every j . So we have $p_1^{s_1} \subseteq \text{ann}(M_j/M_{j-1}) = \text{ann}(R/q_j) = q_j$ 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 $rx \in M_j$, since q_{j+1} annihilates M_{j+1}/M_j . By the inductive hypothesis, $rsx = 0$, so $\prod_{k=1}^{j+1} q_k$ 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 $p_1 \in \text{Ass}(M)$. For this, take $x \in M_j \setminus M_{j-1}$. If $j = 1$, then $\text{ann}(x) = p_1$ (since $M_1 \cong R/p_1$), but $x \in M \subseteq R/I$, so $p_1 \in \text{Ass}(R/I)$.

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 $p_1 \subseteq \text{ann}(rx)$.

Note that $\text{ann}(rx + M_{j-1}) = p_1$ 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 $s \in \text{ann}(rx)$, then certainly $s \in \text{ann}(rx + M_{j-1}) = p_1$, so $\text{ann}(rx) \subseteq p_1$.

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

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

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 $\text{Ass}(R/I) = \{p, q\}$. 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 $M/N \rightarrow \bigoplus M/N_i$).

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 $\text{Ass}(M/N)$;
- (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 $\text{Ass}(R/I) = \{p, q\}$, 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 $(r_1, s_1) \equiv (r_2, s_2) \iff \exists x \in S: (r_1 s_2 - r_2 s_1)x = 0$. 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 $\frac{r_1}{s_1}$ and the quotient by $S^{-1}R$. We make $S^{-1}R$ into a ring by setting

$$\begin{aligned} \frac{r_1}{s_1} + \frac{r_2}{s_2} &:= \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}, \\ \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} &:= \frac{r_1 r_2}{s_1 s_2}. \end{aligned}$$

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

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

$$\begin{array}{ccc} R & \xrightarrow{\theta} & S^{-1}R \\ & \searrow \varphi & \downarrow \exists! \alpha \\ & & T \end{array}$$

is commutative.

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

Then we have

$$\forall r \in R: \alpha\left(\frac{r}{1}\right) = \alpha(\theta(r)) = \varphi(r),$$

$$\forall s \in S: \alpha\left(\left(\frac{s}{1}\right)^{-1}\right) = \alpha\left(\frac{s}{1}\right)^{-1} = \alpha(\theta(s))^{-1} = \varphi(s)^{-1}.$$

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

For existence, we define $\alpha\left(\frac{r}{s}\right) := \varphi(r)\varphi(s)^{-1}$. 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

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

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

$$\begin{aligned} \frac{m_1}{s_1} + \frac{m_2}{s_2} &:= \frac{s_2 m_1 + s_1 m_2}{s_1 s_2} \\ \frac{r_1}{s_1} \frac{m_2}{s_2} &= \frac{r_1 m_2}{s_1 s_2}. \end{aligned}$$

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

If $\theta: M_1 \rightarrow M_2$ is an R -linear map, then an $S^{-1}R$ -linear map $S^{-1}\theta: S^{-1}M_1 \rightarrow S^{-1}M_2$ is given by $\frac{m_1}{s} \mapsto \frac{\theta(m_1)}{s}$. This is functorial in the sense that if $\varphi: M_2 \rightarrow M_3$ 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 $\text{im}(S^{-1}\theta) \subseteq \ker(S^{-1}\varphi)$.

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 $tm \in \ker \varphi = \text{im } \theta$, so we find $m_1 \in M_1$ such that $\theta(m_1) = tm$. Then we can calculate in $S^{-1}M$ that

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

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

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 $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$. \square

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 $p \cap S = \emptyset$, 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 $1 \notin q$, 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. \square

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

PROOF. Using the previous lemma, a chain $J_1 \subseteq J_2 \subseteq \dots$ in $S^{-1}R$ lifts to a chain $I_1 \subseteq I_2 \subseteq \dots$ 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. \square

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 $s \notin \text{ann}(m)$, i.e., $sm \neq 0$, a contradiction. \square

LEMMA 2.9. Let $\varphi: M \rightarrow N$ be a homomorphism of R -modules. The following are equivalent.

- (i) φ is injective,
- (ii) $\varphi_p: M_p \rightarrow N_p$ is injective for all primes p of R ,
- (iii) $\varphi_q: M_q \rightarrow N_q$ 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. \square

LEMMA 2.10. Let p be a prime ideal of R and S a multiplicatively closed subset of R such that $S \cap p = \emptyset$. 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. \square

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-dimensional 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 $k[X_1, \dots, X_n]$ 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.

PROOF. Let p be any prime ideal of R and let $s \in R \setminus p$. The set $S := \{1, s, s^2, \dots\}$ is multiplicative, so we get a localization $S^{-1}R$ and a map $\theta: R \rightarrow S^{-1}R$. 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 $p_1 := \theta^{-1}(q)$ is a prime ideal containing p , and by the correspondence of prime ideals we know that p_1 does not meet S . Hence θ induces an injective k -vector space homomorphism $R/p_1 \rightarrow S^{-1}R/q$. Since $S^{-1}R/q$ is finite-dimensional, this implies that R/p_1 is also finite-dimensional.

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.,

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

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 $\varphi: M \times N \rightarrow L$ is called R -bilinear if

$$\begin{aligned}\varphi(r_1 m_1 + r_2 m_2, n) &= r_1 \varphi(m_1, n) + r_2 \varphi(m_2, n), \\ \varphi(m, r_1 n_1 + r_2 n_2) &= r_1 \varphi(m, n_1) + r_2 \varphi(m, n_2).\end{aligned}$$

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

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

$$\begin{array}{ccc} M \times N & \xrightarrow{\varphi} & T \\ & \searrow \varphi^*(\theta) & \downarrow \theta \\ & & L \end{array}$$

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

- LEMMA 3.2. (i) Given R -modules M, N , there is an R -module T and a universal map $\varphi: M \times N \rightarrow T$.
(ii) Given two universal maps $\varphi_1: M \times N \rightarrow T_1$, $\varphi_2: M \times N \rightarrow T_2$, there is a unique isomorphism $\beta: T_1 \rightarrow T_2$ 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 $T := F/X$ 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

$$\begin{aligned}(r_1 m_1 + r_2 m_2) \otimes n &= r_1 (m_1 \otimes n) + r_2 (m_2 \otimes n) \\ m \otimes (r_1 n_1 + r_2 n_2) &= r_1 (m \otimes n_1) + r_2 (m \otimes n_2).\end{aligned}$$

Define $\varphi: M \times N \rightarrow T$ via $(m, n) \mapsto m \otimes n$ and note that φ is bilinear. Any map $\alpha: M \times N \rightarrow L$ extends to a map of R -modules $\bar{\alpha}: F \rightarrow L$ by sending $e_{(m,n)} \mapsto \alpha(m, n)$. If α is bilinear then $\bar{\alpha}$ vanishes on the generators of X , hence it induces a map of R -modules $\alpha': T \rightarrow L$ 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. \square

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. \bullet 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 form $m \otimes n$. A general element is 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-dimensional vector spaces over k , then the map $M \times N \rightarrow k^{st}$ given by numbering basis elements of k^{st} by pairs (i, j) , $1 \leq i \leq s, 1 \leq j \leq t$ 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 an 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 sheet 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 construct a universal trilinear map $L \times M \times N \rightarrow T$, unique up to isomorphism, denoted by $L \otimes M \otimes N$.

LEMMA 3.4. The following maps exist and are isomorphisms.

(i)

$$\begin{aligned} M \otimes N &\rightarrow N \otimes M \\ m \otimes n &\mapsto n \otimes m, \end{aligned}$$

(ii)

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

(iii)

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

(iv)

$$\begin{aligned} R \otimes_R M &\rightarrow M \\ r \otimes m &\mapsto rm. \end{aligned}$$

PROOF. (i) The map $M \times N \rightarrow N \otimes M$ given by $(m, n) \mapsto n \otimes m$ is bilinear, hence it induces the map $M \otimes N \rightarrow N \otimes M$ 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

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

This map induces a linear map

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

and we will find an inverse. Indeed, the maps

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

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

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

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

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

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

1. Restriction and extension of scalars

DEFINITION 3.5. If $\varphi: R \rightarrow T$ 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 $R \rightarrow S^{-1}R$. Indeed, given an R -module M and a multiplicatively closed set S , we find an isomorphism of R -modules $f: S^{-1}R \otimes_R M \rightarrow S^{-1}M$ given by $\frac{r}{s} \otimes m \mapsto \frac{rm}{s}$.

Indeed, the map $S^{-1}R \times M \rightarrow S^{-1}M$, $(r/s, m) \mapsto (rm)/s$ 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 $\theta: M_1 \rightarrow M_2$ and $\varphi: N_1 \rightarrow N_2$, the tensor product of θ and φ is the map

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

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

DEFINITION 3.7. Given a ring homomorphism $\varphi_1: R \rightarrow T_1$ (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 $\varphi_2: R \rightarrow T_2$, we can take the tensor product of the R -modules T_1 and T_2 to give $T_1 \otimes_R T_2$. We can declare a product on $T_1 \otimes T_2$ by

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

$$(t_1 \otimes t_2, t'_1 \otimes t'_2) \mapsto t_1 t'_1 \otimes t_2 t'_2.$$

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

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

is again bilinear, hence it induces a map

$$(T_1 \otimes T_1) \otimes (T_2 \otimes T_2) \rightarrow T_1 \otimes T_2$$

$$(t_1 \otimes t'_1) \otimes (t_2 \otimes t'_2) \mapsto t_1 t'_1 \otimes t_2 t'_2.$$

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

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

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 $r(m \otimes n) := rm \otimes rn$. 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

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

is exact.

PROOF. First, assume that the first sequence is exact. Let N be an R -module. If $f \in \text{Hom}(M_2, N)$, then $f \circ \varphi \in \text{Hom}(M, N)$. This is the map $\alpha: \text{Hom}(M_2, N) \rightarrow \text{Hom}(M, N)$, 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 $g \in \text{Hom}(M, N)$ then β sends it to $g \circ \theta \in \text{Hom}(M_1, N)$. 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 $M \rightarrow M/\ker \varphi \rightarrow M_2$, with the latter map being an isomorphism. Hence, g factors as $M \rightarrow M_2 \rightarrow M/\ker \varphi \rightarrow M/\ker g \rightarrow N$, where the first map is φ and the second map is the inverse of the isomorphism. Taking f to be the composite of the latter maps, we have written $g = f \circ \varphi$ for $f \in \text{Hom}(M_2, N)$, hence $\ker \beta \subseteq \text{im } \alpha$. Since the reverse inclusion is trivial, we have exactness at $\text{Hom}(M, N)$.

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

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

REMARK. • The functor $\text{Hom}(-, N)$ 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

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

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

$$\begin{aligned} M_1 \otimes N &\xrightarrow{\theta \otimes \text{id}} M \otimes N \xrightarrow{\varphi \otimes \text{id}} M_2 \otimes N \longrightarrow 0 \\ N \otimes M_1 &\xrightarrow{\text{id} \otimes \theta} N \otimes M \xrightarrow{\text{id} \otimes \varphi} N \otimes M_2 \longrightarrow 0 \end{aligned}$$

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

$$0 \rightarrow \text{Hom}(M_2, \text{Hom}(N, N')) \rightarrow \text{Hom}(M, \text{Hom}(N, N')) \rightarrow \text{Hom}(M_1, \text{Hom}(N, N')).$$

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

$$0 \longrightarrow \text{Hom}(M_2 \otimes N, N') \longrightarrow \text{Hom}(M \otimes N, N') \longrightarrow \text{Hom}(M_1 \otimes N, N').$$

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

EXAMPLE. Again, observe that these are not short exact sequences. Applying $- \otimes N$ does not in general preserve injectivity 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 $\text{Spec } R$, 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 $\mathfrak{p} \in \text{Spec } R$, denoted $\text{ht}(\mathfrak{p})$ or $\text{ht}_R(\mathfrak{p})$, 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 between primes with empty intersection with $R \setminus \mathfrak{p}$ and the primes of $R_{\mathfrak{p}}$, we have $\text{ht}(\mathfrak{p}) = \dim R_{\mathfrak{p}}$.

EXAMPLE.

- An artinian ring has dimension 0 (since all prime 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, $\dim k[X] = 1$ if 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 condition relating the subring to the larger ring.

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 $\text{ht}((f)) = 1$ 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

$$0 = s^n f(x) = r^n + r_{n-1}s + \cdots + r_0s^n = 0$$

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 $x^{n+j} = -(r_{n-1}x^{n+j-1} + \cdots + r_0x^j)$ for all $j \geq 0$, where $\deg f = n$. Hence, $R[X]$ is generated as an R -module by $1, x, \dots, x^{n-1}$. This shows that (i) implies (ii).

Trivially, (ii) implies (iii).

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

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

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 $0 = \operatorname{adj}(A)Ay = (\det A)Iy = \det A y$, where $y = (y_1, \dots, y_n)^\top$. Since the y_i generate T , 1 is a linear combination of the y_i , so we find some row vector v such that $0 = \det A y v = \det(A)1 = \det A$. But $\det A_{ij}$ is a monic polynomial expression in x with coefficients in R , so we are done. \square

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 if S is generated as a ring by R and a finite set.

LEMMA 4.8. If $x_1, \dots, x_m \in S$ are integral over R , then $R[x_1, \dots, x_m]$ 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 $R[x_1, \dots, x_m]$. Hence $R[x_1, \dots, x_{m+1}]$ is a finitely generated $R[x_1, \dots, x_m]$ -module, say with generators z_1, \dots, z_t . By the inductive hypothesis, $R[x_1, \dots, x_m]$ is finitely generated as an R -module, say by y_1, \dots, y_ℓ . Then $R[x_1, \dots, x_{m+1}]$ is generated as an R -module by elements of the form $z_i y_j$ with $1 \leq i \leq t$ and $1 \leq j \leq \ell$. \square

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). \square

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 $x^n + t_{n-1}x^{n-1} + \dots + t_0 = 0$ 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. \square

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 $x^n = r_{n-1}x^{n-1} + \dots + r_0 = 0$ for some $r_i \in R$. Projecting onto T/J , this yields an equation $\bar{x}^n + \bar{r}_{n-1}\bar{x}^{n-1} + \dots + \bar{r}_0 = \bar{0}$ in T/J , such that $\bar{r}_i \in (R + J)/J$, hence \bar{x} is integral over $(R + J)/J$ as required.

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

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

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

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 $t^n + r_{n-1}t^{n-1} + \dots + r_0 = 0$ 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, $t^{n-1} + \dots + r_1 = 0$ would be a shorter expression, contradicting minimality. Then $s := -r_0^{-1}(t^{n-1} + \dots + r_1)$ 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 $x^{-m} + r'_m x^{-m+1} + \dots + r'_0 = 0$. Multiply by x^{m-1} and rearrange to find $x^{-1} = -(r'_m + r'_{m-1}x + \dots + r'_0 x^{m-1}) \in R$, so R is a field. \square

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 $\mathfrak{p} := R \cap \mathfrak{q}$. 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. \square

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 $S := R \setminus \mathfrak{p}$. 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 meet S , we conclude $\mathfrak{q} = \mathfrak{q}_1$. \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 $\text{Spec } T \rightarrow \text{Spec } R$ is surjective.

PROOF. Again, let $S := R \setminus \mathfrak{p}$. 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 $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$, 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 \bar{R} for R/\mathfrak{p}_1 and \bar{T} for T/\mathfrak{q}_1 . Then we have an integral extension $\bar{R} \subseteq \bar{T}$, 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 $\bar{\mathfrak{q}}_2$ of \bar{T} such that $\bar{\mathfrak{q}}_2 \cap \bar{R} = \bar{\mathfrak{p}}_2$. 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 $S_2 = R \setminus \mathfrak{p}_2$. $S := S_1 S_2$ is a multiplicatively closed subset of T satisfying $S_1 \subseteq S$ and $S_2 \subseteq S$.

Assume for now that $T\mathfrak{p}_2 \cap S = \emptyset$ (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

$sx = sy \in T\mathfrak{p}_2 \cap S = \emptyset$ (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 $\mathfrak{q}_2 \cap S = \emptyset$. 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, $x(s_1s_2) \in \mathfrak{q}_2$, but \mathfrak{q}_2 is prime, $s_1s_2 \in S$ and $\mathfrak{q}_2 \cap S = \emptyset$, 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 $\mathfrak{q}_2 \cap R \not\subseteq \mathfrak{p}_2$, 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 $x \in \mathfrak{q}_2 \cap S = \emptyset$, a contradiction. We conclude $\mathfrak{p}_2 = \mathfrak{q}_2 \cap R$.

Similarly, if $\mathfrak{q}_2 \not\subseteq \mathfrak{q}_1$, 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 $x \in \mathfrak{q}_2 \cap S = \emptyset$. This shows, $\mathfrak{q}_2 \subseteq \mathfrak{q}_1$, so \mathfrak{q}_2 has the desired properties.

It remains to show that $T\mathfrak{p}_2 \cap S = \emptyset$. 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 $\text{ht}(\mathfrak{q} \cap R) = \text{ht}(\mathfrak{q})$.

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

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 $\text{ht}(\mathfrak{q} \cap R) \leq \text{ht}(\mathfrak{q})$. \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 $x^n = -(a_1x^{n-1} + \dots + a_n) \in TI$. 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 $M := R[t_1, \dots, t_n]$ is finitely generated as an R -module. Observe that $x^n M - \sum_i r_i (t_i M) \subseteq IM$. Let y_1, \dots, 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 . \square

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 $f := X^n + r_{n-1}X^{n-1} + \dots + r_0$ is the minimal polynomial of x over K , then $r_i \in \sqrt{I}$ for all i .

PROOF. Certainly 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 $x^m + s_{m-1}x^{m-1} + \dots + s_0 = 0$ with $s_i \in I$. Applying the automorphism (which fixes K , so in particular I), yields $y^m + s_{m-1}y^{m-1} + \dots + s_0 = 0$, 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. \square

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 $k[X_1, \dots, X_n] \rightarrow A$ 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 $\dim T = \text{tr deg}_k K$, where $\text{tr deg}_k K$ is the so-called transcendence degree of K over k .

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

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

Thus, it remains to show that $\dim k[x_1, \dots, x_r] = r$. We have already seen that $\dim k[x_1, \dots, x_r] \geq r$. Take a chain $\mathfrak{p}_0 \subsetneq \dots \subsetneq \mathfrak{p}_s$ 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 $\text{tr deg}_k(K_f) = r - 1$, 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. \square

DEFINITION. We say that x_1, \dots, x_n are algebraically independent over k if the ring map $k[X_1, \dots, X_n] \rightarrow k[x_1, \dots, x_n]$ 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 independent 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 $\text{tr deg}_k L = n$, since X_1, \dots, X_n is a maximal algebraically independent set, and $\text{tr deg } K = n - 1$, 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 independent.

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 $k[X] \rightarrow k[a]$ 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 independent 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 $\varphi: \ell \mapsto m_1 \ell_1 + \cdots + m_r \ell_r + \ell_n$ 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 $d_1 = \dots = d_r = 0$, 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

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

Thus, g is a sum of the form

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

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

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 $S := k[b_1, \dots, b_r, a_{r+1}, \dots, a_{n-1}]$. 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 . \square

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

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

PROOF. Define $m := \text{ht}(\mathfrak{q})$ 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 $\dim T = \dim R = \text{tr deg } K$, where K is the field of fractions of T , by 4.24. Furthermore, $\dim R$ is the number of indeterminates of R .

Write $\mathfrak{p}_i := \mathfrak{q}_i \cap R$. By maximality of the chain, we must have $\text{ht}(\mathfrak{q}_1) = 1$. 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 $\text{ht}(\mathfrak{p}_1) = 1$. 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 $\text{ht}(\mathfrak{q}/\mathfrak{q}_1) = m - 1$ (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. \square

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 $L \times L \rightarrow K$ given

by $(x, y) \mapsto \text{Tr}(xy)$ is a non-degenerate symmetric K -bilinear form. Furthermore, the trace of an element x is an integer multiple of a coefficient of the minimal polynomial of x .

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

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

By multiplying with the product of the denominators, we find $t_i \in R$ such that we have an equation of the form

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

Finally, define $y_i := t_n z_i$. Then we have

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

Therefore, $y_i \in T_1$, and the y_i still form a K -basis of L . By non-degeneracy, we find a K -basis x_1, \dots, x_n such that $\text{Tr}(x_i y_j) = \delta_{ij}$.

Let $x \in T_1$. Then may write $x = \sum \lambda_i x_i$ for some $\lambda_i \in K$. Then we may calculate

$$\text{Tr}(xy_j) = \sum_i \lambda_i \text{Tr}(x_i y_j) = \sum_i \lambda_i \delta_{ij} = \lambda_j.$$

On the other hand, $xy_j \in T_1$, since the integral closure is a subalgebra. By (4.23) with $I = R$, the minimal polynomial of xy_j has coefficients in R , so in particular $\lambda_j = \text{Tr}(xy_j) \in R$. Therefore, $x \in \sum R x_i$, so we have an inclusion of R -submodules $T_1 \subseteq \sum R x_i$. But $\sum R x_i$ is a finitely generated module over a Noetherian ring, so it is Noetherian itself. Hence, T_1 is finitely generated. \square

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

THEOREM 4.29 (Krull's Hauptidealsatz). If R is a noetherian ring, $a \in R$ is not a unit and \mathfrak{p} is a minimal prime over (a) , then $\text{ht}(\mathfrak{p}) \leq 1$.

PROOF. Let a be a non-unit and \mathfrak{p} a minimal prime over (a) . The localisation $R_{\mathfrak{p}}$ has the unique maximal ideal $\mathfrak{p}_{\mathfrak{p}} = S^{-1}\mathfrak{p}$ (with $S = R \setminus \mathfrak{p}$) and it is a minimal prime over $S^{-1}(a) = (a)_{\mathfrak{p}}$ (2.5!). Even further, we have $\text{ht}(\mathfrak{p}_{\mathfrak{p}}) = \text{ht}(\mathfrak{p})$ (2.5 again), so we may replace R by $R_{\mathfrak{p}}$, i.e., we are allowed to assume that R is local with maximal ideal \mathfrak{p} .

Suppose $\text{ht}(\mathfrak{p}) > 1$, i.e., we find prime ideals $\mathfrak{q}, \mathfrak{q}'$ such that $\mathfrak{q}' \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$. The ring $R/(a)$ is local with the unique maximal ideal $\mathfrak{p}/(a)$. Now a prime ideal in $R/(a)$ pulls back to a prime between (a) and \mathfrak{p} in R , so we conclude that $\mathfrak{p}/(a)$ is actually the only non-zero prime of $R/(a)$. Thus $N(R/(a)) = \mathfrak{p}/(a)$ is nilpotent (1.21). Pulling this back, we conclude that $\mathfrak{p} \subseteq (a)$ for some n . Consider the chain

$$R \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \dots \supseteq \mathfrak{p}^n.$$

Since R is noetherian, each factor is a finitely-generated R/\mathfrak{p} -vector space, so we can stitch together the descending chain conditions to find that R/\mathfrak{p}^n is artinian (cf. example sheet 1). In particular, this implies that $R/(a)$ is artinian.

Next, define $I_n := \{r \in R \mid r/1 \in S^{-1}\mathfrak{q}^n\}$, where $S = R \setminus \mathfrak{q}$. We get a chain

$$\mathfrak{q} = I_1 \supseteq I_2 \supseteq \dots,$$

on R , which we may project to a chain

$$(I_1 + (a))/(a) \supseteq (I_2 + (a))/(a) \supseteq \dots$$

in $R/(a)$. But the latter is artinian, hence this chain must terminate, so we find m such that $I_m + (a) = I_{m+1} + (a)$.

We will now show that in fact $I_m = I_{m+1}$. Indeed, let $r \in I_m$. Since $I_m + (a) = I_{m+1} + (a)$, this means that we find $t \in I_{m+1}$, $x \in R$ such that $r = t + ax$. Rearranging, we have $ax = r - t \in I_m$, but $a \notin \mathfrak{q}$ (\mathfrak{p} is minimal over (a) !). By definition of I_m , this means $\frac{ax}{1} \in S^{-1}\mathfrak{q}^m$. By definition of localization, this means that we find $q \in \mathfrak{q}^m$, $s, t \in S$ such that $t(axs - q) = 0$. This means that $\frac{x}{1} = \frac{q}{as} \in S^{-1}\mathfrak{q}^m$, and thus $x \in I_m$. This means that $r + I_{m+1} = a(x + I_{m+1})$ as elements of the R -module I_m/I_{m+1} , but since $a \in \mathfrak{p}$, we conclude $I_m/I_{m+1} = \mathfrak{p}(I_m/I_{m+1})$. By Nakayama's lemma, we conclude $I_m = I_{m+1}$ as claimed.

Now $(S^{-1}\mathfrak{q})^m = S^{-1}\mathfrak{q}^m = S^{-1}I_m$ (both equalities are easy to check) and the same is true for $m + 1$. But since $I_m = I_{m+1}$, this implies $(S^{-1}\mathfrak{q})^m = (S^{-1}\mathfrak{q})^{m+1}$.

Now $(S^{-1}\mathfrak{q})^m$ is an $S^{-1}R$ -module, but $S^{-1}R = R_{\mathfrak{q}}$ is local with maximal ideal $S^{-1}\mathfrak{q}$. Hence, the statement $(S^{-1}\mathfrak{q})^m = (S^{-1}\mathfrak{q})^{m+1}$ can be interpreted as an equality $J(S^{-1}R)(S^{-1}\mathfrak{q})^m = (S^{-1}\mathfrak{q})^m$ of $S^{-1}R$ -modules, and Nakayama tells us that $(S^{-1}\mathfrak{q})^m = 0$.

Now by the correspondence, we have a prime ideal $S^{-1}\mathfrak{q}' \subsetneq S^{-1}\mathfrak{q}$. Now $(S^{-1}\mathfrak{q})^m = 0 \subseteq S^{-1}\mathfrak{q}'$, so by primality we have $S^{-1}\mathfrak{q} \subseteq S^{-1}\mathfrak{q}'$. This is a contradiction, completing the proof. \square

THEOREM 4.30 (Generalised Hauptidealsatz). Let R be a noetherian ring, I a proper ideal generated by n elements and \mathfrak{p} a minimal prime over I . Then $\text{ht}(\mathfrak{p}) \leq n$.

PROOF. We perform induction on n . The case $n = 0$ is trivial, and the case $n = 1$ is just the Hauptidealsatz. Hence, suppose $n > 1$.

As in the proof of the Hauptidealsatz, by passing to $R_{\mathfrak{p}}$, we may assume that R is local and that \mathfrak{p} is the unique maximal ideal \mathfrak{p} .

Pick any prime such that \mathfrak{q} is maximal and satisfies $\mathfrak{q} \subsetneq \mathfrak{p}$ (this is possible since R is noetherian). In particular, \mathfrak{p} is the only prime strictly containing \mathfrak{q} . We will show that $\text{ht}(\mathfrak{q}) \leq n - 1$. Then, if we have any maximal chain of prime ideals ending in \mathfrak{p} , its second-to-last term will be such a \mathfrak{q} (otherwise it would be possible to extend the chain), so it follows that $\text{ht}(\mathfrak{p}) \leq n$ as required.

Since \mathfrak{p} is a minimal prime over I , we must have $I \not\subseteq \mathfrak{q}$. By assumption, we find generators a_1, \dots, a_n , and at least one of these is not contained in \mathfrak{q} . Reorder them such that $a_n \notin \mathfrak{q}$.

Now $\mathfrak{q} + (a_n)$ is strictly larger than \mathfrak{q} , so if $\mathfrak{q} + (a_n)$ is contained in any prime, this prime must be \mathfrak{p} by how we chose \mathfrak{q} . In particular, the image of \mathfrak{p} is the only prime ideal in $R/(\mathfrak{q} + (a_n))$. Replaying a part of the proof of the Hauptidealsatz with $\mathfrak{q} + (a_n)$ in place of (a) , this means that $R/(\mathfrak{q} + (a_n))$ is artinian, hence noetherian. Now 1.21 tells us that the image of \mathfrak{p} is nilpotent, i.e., $\mathfrak{p}^m \subseteq \mathfrak{q} + (a_n)$ for some m .

In particular, since $I \subseteq \mathfrak{p}$, for all $1 \leq i \leq n - 1$, we have $a_i^m \in \mathfrak{q} + (a_n)$, i.e., we may choose $x_i \in \mathfrak{q}$ and $r_i \in R$ such that $a_i^m = x_i + r_i a_n$. Note that this means that any prime ideal in R that contains x_1, \dots, x_{n-1} and a_n must contain a_1, \dots, a_n , so it must be equal to \mathfrak{p} . Also, since $x_i \in \mathfrak{q}$, we have $J := \sum_{i=1}^{n-1} R x_i \subseteq \mathfrak{q}$. Now if we can show that \mathfrak{q} is minimal over J , we are done, since J is generated by $n - 1$ elements, so $\text{ht}(\mathfrak{q}) \leq n - 1$ by the inductive hypothesis.

Indeed, let $\pi: R \rightarrow R/J$ be the projection. The ring R/J is local with unique maximal ideal $\pi(\mathfrak{p})$. Now any prime over the ideal $\pi((a_n))$ lifts to a prime ideal of R containing x_1, \dots, x_{n-1} and a_n so it is equal to \mathfrak{p} . Thus, $\pi(\mathfrak{p})$ is a minimal prime over $\pi((a_n))$. The Hauptidealsatz now tells us $\text{ht}(\pi(\mathfrak{p})) \leq 1$, but since $\pi(\mathfrak{q}) \subsetneq \pi(\mathfrak{p})$, this means that $\text{ht}(\pi(\mathfrak{q})) = 0$, i.e., $\pi(\mathfrak{q})$ is a minimal prime in R/J , i.e., \mathfrak{q} is a minimal prime over J as required, and we are done. \square

COROLLARY 4.31. Let R be a noetherian ring.

- (a) Each prime \mathfrak{p} of R has finite height.
- (b) If R is local with maximal ideal \mathfrak{m} and n is the minimal number of generators of \mathfrak{m} , then $\dim R \leq n$. Furthermore, $n = \dim_{R/\mathfrak{m}} \mathfrak{m}^2/\mathfrak{m}$.

PROOF. Part (a) is immediate from the generalised Hauptidealsatz, since every prime is minimal over itself.

Clearly, $\dim R = \text{ht}(\mathfrak{m})$, so the first part of (b) follows. For the second part, it will suffice to show that x_1, \dots, x_n generate \mathfrak{m} as an R -module if and only if $x_1 + \mathfrak{m}^2, \dots, x_n + \mathfrak{m}^2$ generate $\mathfrak{m}/\mathfrak{m}^2$ as a R/\mathfrak{m} -vector space.

The “only if” claim is immediate. Conversely, if $x_1 + \mathfrak{m}^2, \dots, x_n + \mathfrak{m}^2$ generate $\mathfrak{m}/\mathfrak{m}^2$, consider the submodule $I := (x_1, \dots, x_n) \subseteq \mathfrak{m}$. By assumption, we have $I + \mathfrak{m}^2 = \mathfrak{m}$. Let $x \in \mathfrak{m}$. Then this means that we find $m_i, n_i \in \mathfrak{m}$ such that $x - \sum_i m_i n_i \in I$. This means that as elements of the R -module \mathfrak{m}/I we have $x + I = \sum_i m_i (n_i + I)$, hence we have $\mathfrak{m}(\mathfrak{m}/I) = \mathfrak{m}/I$. Since R is local, $J(R) = \mathfrak{m}$, so by Nakayama’s lemma, we must have $\mathfrak{m}/I = 0$, and we are done. \square

COROLLARY 4.32. A noetherian ring satisfies the DCC on prime ideals.

PROOF. If we have a strictly descending chain of prime ideals, then the chain can have length at most $\text{ht}(\mathfrak{p})$. But this is finite by what we just saw. \square

DEFINITION 4.33. A regular local ring is a local ring with maximal ideal \mathfrak{m} such that $\dim R = \dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$.

It is possible to show that a regular local ring is an integral domain. In geometry, regular local rings correspond to localisation at non-singular points.

REMARK. In 4.31, we showed that the dimension of a noetherian local ring is at most the minimum number of generators of the maximal ideal \mathfrak{m} .

In fact, by 4.30, if I is any ideal such that $\sqrt{I} = \mathfrak{m}$, then $\dim R$ is bounded above by the minimal number of generators of I (are we using 1.24 here?). Even more, we can always find an I such that $\sqrt{I} = \mathfrak{m}$ and the minimal number of generators is exactly the dimension of R .

CHAPTER 5

I-adic topology

DEFINITION 5.1. Let M be an R -module. An infinite descending chain $M_0 \supseteq M_1 \supseteq \cdots$ of submodules of M is called a filtration. If I is an ideal of R , then $\{M_n\}$ is called an I -filtration if $IM_i \subseteq M_{i+1}$ for all i . It is called a stable I -filtration if there is some N such that for all $i \geq N$ we have $IM_i = M_{i+1}$. In particular, $\{I^n M\}$ is a stable I -filtration.

If $I \subseteq R$ is an ideal, the Rees ring is defined as $R^* := \bigoplus_{n \geq 0} I^n$. The Rees ring is isomorphic to the subring $R + IX + I^2 X^2 + \cdots$ of $R[X]$ via the obvious map. It is a graded ring.

DEFINITION 5.2. A graded ring T is a ring that, as an abelian group, is of the form $\bigoplus_{n \geq 0} T_n$, where the T_n are additive subgroups of T . Furthermore, we require $T_m T_n \subseteq T_{m+n}$ for all $m, n \geq 0$. In particular, T_0 is a subring of T and $T_+ := \bigoplus_{n \geq 1} T_n$ is an ideal of T . Furthermore, each T_n is a T_0 -module. We call T_n the n th homogeneous component of T .

If $\{M_n\}$ is an I -filtration of an R -module M , then $M^* := \bigoplus_{n \geq 0} M_n$ is a graded R^* -module (by a graded T -module N we mean a module of the form $\bigoplus_{i \geq 0} N_i$ such that $T_m N_i \subseteq N_{m+i}$ for all m and i . Observe that N_i is a T_0 -module). We use that $I^m M_n \subseteq M_{m+n}$ by the fact that we have an I -filtration.

A homogenous element is one lying in some compoent. A morphism of graded T -modules $\theta: N \rightarrow N' = \bigoplus N'_i$ is a T -linear map such that $\theta(N_i) \subseteq N'_i$ for all $i \geq 0$.

It is also possible to define gradings with different indexing sets (\mathbb{Z} is an example that sometimes comes up).

PROPOSITION 5.3. A graded ring T is noetherian if and only if T_0 is a noetherian ring and T is finitely generated as a T_0 -algebra.

PROOF. First suppose T is a noetherian ring. We have an isomorphism of T -modules $T_0 \cong T/T_+$. This means that T_0 is a noetherian T -module. Observe that elements from T_i for $i \neq 0$ act trivially on T_0 , so T_0 is actually a Noetherian T_0 -module. Hence, T_0 is a noetherian ring.

Since T is noetherian, T_+ is a finitely generated ideal. Splitting generators into components, we may assume that T_+ is generated by homogeneous elements x_1, \dots, x_s of degrees m_1, \dots, m_s , and $m_i > 0$ for all i . Define $T' := T_0[x_1, \dots, x_s]$. It will suffice to show that $T_i \subseteq T'$ for every $i \geq 0$. We will prove this by induction. The case $i = 0$ is trivial.

If $i > 0$, let $y \in T_i$. Then $y \in T_+$, so we may write $y = \sum_{j=1}^s t_j x_j$, where $t_j \in T_{i-m_j}$ (after possibly removing other summands which cancel each other out in different degrees). Then the inductive hypothesis says that $t_j \in T'$ for each j , and so $y \in T'$ as claimed.

Conversely, if T_0 is noetherian and T is a finitely generated T_0 -algebra, then T is a surjective image of a polynomial ring over T_0 in finitely many variables, so the claim follows from Hilbert's basis theorem. \square

REMARK. If R is a noetherian ring and I is an ideal, then I is finitely generated, say by x_1, \dots, x_s . Then the Rees ring R^* is generated as an R -algebra by x_1, \dots, x_s , so it is Noetherian by Hilbert's basis theorem.

LEMMA 5.4. Let R be a noetherian ring, M a finitely generated R -module and $\{M_n\}$ an I -filtration of M . Then M^* is a finitely generated R^* -module if and only if $\{M_n\}$ is I -stable.

PROOF. For $n \geq 0$, define

$$M_n^* := \bigoplus_{i=0}^n M_i \oplus \bigoplus_{j \geq 1} I^j M_n.$$

This is an R^* -submodule of M^* , and since each of the M_i is finitely generated as an R -module (since M is a noetherian R -module), we have that M_n^* is a finitely generated R^* -module. We have a chain $M_0^* \subseteq M_1^* \subseteq \dots$, and $M^* = \bigcup M_n^*$.

Now if M^* is finitely generated, then it is a noetherian R^* -module (since R^* is noetherian), so in particular this chain terminates. Conversely, if this chain terminates, then M^* is one of the M_n^* , so it is finitely generated.

But the chain terminates if and only if $M_{N+j} = I^j M_N$ for some N and all j (by a componentwise comparison of M^* and M_N^*), and this is just the definition of a stable filtration. \square

PROPOSITION 5.5 (Artin-Rees lemma (1956)). Let R be a noetherian ring, $I \subseteq R$ an ideal, M a finitely generated R -module, $\{M_n\}$ a stable I -filtration of M . If M' is a submodule of M , then $M' \cap M_n$ is a stable I -filtration of M' .

PROOF. It is immediate that $\{M' \cap M_n\}$ is an I -filtration of M' :

$$I(M' \cap M_n) \subseteq IM' \cap IM_n \subseteq M' \cap M_{n+1},$$

using the fact that $\{M_n\}$ is an I -filtration.

Now we get a graded R^* -submodule $N := \bigoplus_{n \geq 0} M' \cap M_n$ of M^* . Since $\{M_n\}$ is stable, 5.4 yields that M^* is finitely generated as an R^* -module, so it is noetherian, so N is finitely generated, so applying 5.4 again gives the claim. \square

COROLLARY 5.6 (Artin-Rees lemma). Let R be a noetherian ring, $I \subseteq R$, M a finitely generated R -module, and M' a submodule of M . Then there is some s such that for all $n \geq s$ we have

$$(I^n M) \cap M' = I^{n-s}((I^s M) \cap M').$$

PROOF. Take $M_n = I^n M$ in the previous lemma. \square

PROPOSITION 5.7 (Krull's intersection theorem). Let R be a noetherian ring, $I \subsetneq R$ a proper ideal, and M a finitely generated R -module. Define $N := \bigcap_{n \geq 0} I^n M$. Then

- (i) there is some $r \in 1 + I$ such that $rN = 0$,
- (ii) if $I \subseteq J(R)$, then $N = 0$,
- (iii) if R is integral then $\bigcap_{n \geq 0} I^n = 0$,
- (iv) if R is local then $N = 0$.

PROOF. The Artin-Rees lemma tells us that there is some s such that for all $n \geq s$ we have $N = (I^n M) \cap N = I^{n-s}((I^s M) \cap N) = I^{n-s}N$. In particular, we have $N = IN$.

Now (ii) follows from Nakayama (as seen on example sheet 1), and (i) follows from some variant of Nakayama (TODO). Furthermore, if R is an integral domain and we take $M = R$, then if $N \neq 0$, then $rN = 0$ implies that R has zero divisors, a contradiction. Finally, if R is local, then all ideals are contained in $J(R)$, so by (ii) we are done. \square

1. Topology and completion

REMARK. Let $\{M_n\}$ be a filtration of an R -module M with $M_0 = M$. We will define a topology on M , by declaring the open sets to be unions of sets of the form $m + M_n$ for some $m \in M$ and $n \in \mathbb{N} \setminus \{0\}$.

Clearly, any union of these is open. The intersection of two open sets is of the form

$$\bigcup_i m_i + M_{n_i} \cap \bigcup_i m'_i + M_{n'_i} = \bigcup_{i,j} m_i + M_{n_i} \cap m'_j + M_{n'_j}.$$

But if $n' > n$, then clearly $m + M_n = \bigcup_{\ell \in M_n} m + \ell + M_{n'}$, hence we may assume that $n_i = n'_i$ for all i . But if $x \in m + M_n \cap m' + M_n$, then actually $m + M_n = m' + M_n$, so the terms of the union over i and j are either $m_i + M_{n_i}$ or empty, so we have shown that the intersection of two closed sets is closed.

If $\cap M_n = 0$, then we can put a metric on M by declaring $d(m_1, m_2) = p^{-k}$, where k is the maximal natural number such that $m_1 - m_2 \in M_k$ and $p \in \mathbb{Z}$ is a prime number. This metric yields the same topology as above (in both cases, “balls” consist of things that all differ by the elements in some M_k).

The choice of p is important in the case $M = \mathbb{Z}$, $M_n = p^n \mathbb{Z}$. If we are only interested in the topology (which is the case most of the time), then the choice of p does not matter.

If $\{M_n\}$ and $\{M'_n\}$ are two filtrations such that there exists sequences s and t such that for each n we have

$$M'_{s(n)} \subseteq M_n, \quad M_{t(n)} \subseteq M'_n,$$

then the two filtrations determine the same topology.

Now, if I is an ideal, then the I -adic topology on M is the topology induced by the filtration $\{I^n M\}$. In particular, we get a topology on R from the filtration $\{I^n\}$.

All stable I -filtrations yield the same topology. Indeed, if $\{M_n\}$ is a stable I -filtration, then we have $I^n M \subseteq M_n$, because $IM_n \subseteq M_{n+1}$. On the other hand, there is some N such that for all $n \geq N$ we have $IM_n = M_{n+1}$, which means that $M_{n+N} = I^n M_N \subseteq I^n M$. Hence, by our previous consideration, the topology induced by $\{M_n\}$ is the same as the topology induced by $\{I^n M\}$.

EXAMPLE. • If we choose $I = (p) \subseteq \mathbb{Z}$ we get the usual p -adic topology. Two integers are “close together” if their difference is divisible by a large power of p .

• Another interesting example is $I = (f) \subseteq k[X]$, where f is irreducible.

Let $\{M_n\}$ be a stable I -filtration of any finitely generated module M over a noetherian ring R . If $N \subseteq M$ is a submodule, then Artin-Rees tells us that $N \cap M_n$ is a stable I -filtration on N . Since all stable I -filtrations induce the same topology, this means that the subspace topology on N induced from the I -adic topology on M is the same as the I -adic topology on N .

DEFINITION 5.8. A Cauchy sequence (x_m) in M is a sequence such that for any open set U containing 0 there is a natural number $a(U)$ such that for all $r, s \geq a(U)$ we have $x_r - x_s \in U$.

Since sets of the form $m + M_n$ form a basis of the topology and $0 \in m + M_n \iff m + M_n = M_n$, it is sufficient to consider open sets U of the form M_n . Hence, a Cauchy sequence is one such that for all $r, s \geq a(M_n)$, $x_r \equiv x_s \pmod{M_n}$.

Two Cauchy sequences $(x_n), (y_n)$ are called equivalent if $x_m - y_m \rightarrow 0$, i.e., that for any open U containing 0 we find $b(U)$ such that for all $m \geq b(U)$ we have $x_m - y_m \in U$.

DEFINITION 5.9. The I -adic completion \hat{M} of M is the set of equivalence classes of Cauchy sequences. If $(x_n), (y_n)$ are Cauchy sequences, so is $(x_n + y_n)$ and its class only depends on the classes of (x_n) and (y_n) . The I -adic completion \hat{R} of R is the set of equivalence classes of Cauchy sequences with the I -adic topology. We get a well-defined product via $[r_n][s_n] = [r_n s_n]$ and addition as above.

Hence (after checking a whole bunch of stuff), we have made \hat{R} into a ring and we make \hat{M} into an R -module in the obvious way. We get a homomorphism of rings $R \rightarrow \hat{R}$ by sending r to the constant sequence $[r]$. The kernel of this map is easily seen to be $\bigcap_{n \in \mathbb{N}} I^n$. Similarly, we have a homomorphism of abelian groups (and also of R -modules?) $M \rightarrow \hat{M}$ sending $x \mapsto [x]$. The kernel is $\bigcap I^n M$.

Krull's intersection theorem can be interpreted as giving sufficient conditions for these maps to be injective. For example, $R \rightarrow \hat{R}$ is injective if R is an integral domain, and $M \rightarrow \hat{M}$ is injective if $I \subseteq J(R)$.

DEFINITION 5.10. We call the ring R complete if the map $R \rightarrow \hat{R}$ is an isomorphism.

REMARK. Another way of defining these concepts is via the inverse limits $\varprojlim (M/M_n)$ and $\varprojlim (R/I^n)$, where $\{M_n\}$ is a stable I -filtration. Now $\varprojlim (M/M_n)$ is a subobject of $\prod (M/M_n)$, and this Cartesian product allows infinitely many entries that differ from 0. The elements are precisely the tuples with entries $y_n + M_n$ such that for $r > s$ the canonical projection $M/M_r \rightarrow M/M_s$ maps $y_r + M_r \mapsto y_s + M_s$. Addition (and, in the case of $\varprojlim (R/I^n)$, multiplication) are componentwise. We have a canonical projection $\varprojlim M/M_n \rightarrow M/M_r$ (and similar for R/I^r for each r).

Furthermore, we may declare a map $\varphi: \hat{M} \rightarrow \varprojlim (M/M_n)$ in the following way: if $[x_n] \in \hat{M}$ is a Cauchy sequence, then for each n there is $a(M_n)$ such that $x_{a(M_n)} - x_m \in M_n$ for all $m \geq a(M_n)$. Define the n -th component of $\varphi([x_n])$ to be $x_{a(M_n)} + M_n$. This is easily seen to be a morphism of abelian groups. Furthermore, it is injective, since every component of $\varphi([x_n])$ is the same information as the sequence being equivalent to the zero sequence. Also, any element $(\dots, y_n + M_n, \dots) \mapsto \varprojlim (M/M_n)$ has preimage $[y_n]$, and the fact that we have an element of the inverse limit ensures that this is a Cauchy sequence (set $a(M_n) := n$). Hence, we have an isomorphism $\hat{M} \cong \varprojlim (M/M_n)$ and we will freely transport along this isomorphism.

We define a filtration on $\hat{M} = \varprojlim (M/M_n)$: \hat{M}_n is the set of elements of $\varprojlim (M/M_n)$ whose first $n+1$ components are 0 (recall that $M_0 = M$, so the first component is always 0).

All of the above also applies to $\hat{R} = \varprojlim (R/I^n)$. In particular, the \hat{R}_n are ideals if we define $\hat{I} := \hat{R}_1$, then $R/I \cong \hat{R}/\hat{I}$, since in the right hand side we ignore everything except for the first two components, but the first component is trivial and the second component is R/I . More generally, we have $R/I^n \cong \hat{R}/\hat{I}^n$.

EXAMPLE. • If $R = \mathbb{Z}$, $I = (p)$ where p is a prime number, then \hat{R} is the ring of p -adic integers:

$$\varprojlim \mathbb{Z}/p^n \mathbb{Z} = \left\{ \sum_{i \geq 0} a_i p^i \mid 0 \leq a_i \leq p-1 \right\}.$$

- If $R = k[X]$, k is a field and $I = (X)$, then \hat{R} is the ring of formal power series $k[[X]]$.
- If $R = k[[X_1, \dots, X_n]]$, $I = (X_1, \dots, X_n)$, then R is complete with respect to I . For example, for $n = 1$, the power series $a + bX + cX^2 + \dots$ corresponds to the element $(0, a + (X), a + bX + (X^2), \dots)$.

REMARK 5.11. If $\hat{r} \in \hat{I}$, then $\hat{1} - \hat{r}$ has the multiplicative inverse $\hat{1} + \hat{r} + \hat{r}^2$ (indeed, the partial sums are a Cauchy sequence in the I -adic completion), and so $\hat{1} - \hat{r}$ is a unit. This means that $\hat{I} \subseteq J(\hat{R})$ (for example by Sheet 1, Exercise 10).

In particular, if I is maximal in R , then $\hat{R}/\hat{I} \cong R/I$ is a field, so \hat{I} is maximal. Hence, $\hat{I} = J(\hat{R})$, so \hat{R} is local with maximal ideal \hat{I} .

PROPOSITION 5.12. If R is noetherian and I is an ideal and if we have a short exact sequence of finitely generated R -modules

$$0 \longrightarrow M_1 \xrightarrow{\iota} M \xrightarrow{\varphi} M_2 \longrightarrow 0,$$

then we obtain an exact sequence of I -adic completions

$$0 \longrightarrow \hat{M}_1 \longrightarrow \hat{M} \longrightarrow \hat{M}_2 \longrightarrow 0.$$

PROOF. If $f: M \rightarrow N$ is any morphism of R -modules, then we have a map $f_n: M/I^n M \rightarrow N/I^n N$. These maps fit into a commutative diagram

$$\begin{array}{ccccccc} M/M & \longleftarrow & M/IM & \longleftarrow & M/I^2M & \longleftarrow & M/I^3M & \longleftarrow & \dots \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ N/N & \longleftarrow & N/IN & \longleftarrow & N/I^2N & \longleftarrow & N/I^3N & \longleftarrow & \dots \end{array}$$

By the universal property of the direct limit \hat{N} , we get a unique induced morphism $\hat{f}: \hat{M} \rightarrow \hat{N}$ such that $\pi_n(\hat{f}(x)) = f_n(\pi_n(x))$. This gives immediately that $\hat{\cdot}$ is functorial and if $f = 0$, then $\hat{f} = 0$.

Furthermore, we claim that if f is injective, then \hat{f} is injective. Indeed, by Artin-Rees, we find s such that for all $n \geq s$ we have

$$(I^n N) \cap f(M) = I^{n-s}((I^s N) \cap f(M)).$$

Now let $x \in \hat{M}$ such that $\hat{f}(x) = 0$. First, let $n \in \mathbb{N}_0$. If $\pi_{n+s}(x) = m + I^{n+s}M$, then $0 = \pi_{n+s}(\hat{f}(x)) = f_{n+s}(\pi_{n+s}(x)) = f(m) + I^{n+s}M$. Hence,

$$f(m) \in (I^{n+s}N) \cap f(M) = I^n((I^s N) \cap f(M)),$$

i.e., we find $i_k \in I^n$, $m'_k \in M$ such that $f(m) = \sum_k i_k f(m'_k) = f(\sum_k i_k m'_k)$. But f is injective, hence we conclude $m = \sum_k i_k m'_k$. The fact that \hat{M} is an inverse limit (so the projections form a cone over the inverse system) tells us that $\pi_n(x) = m + I^n M = \sum_k i_k m'_k + I^n M = 0$. Doing this for all n , we find that $x = 0$ as required.

Hence, we get our induced morphisms $\hat{\iota}$ and $\hat{\varphi}$ and we have already shown that $\hat{\iota}$ is injective and that $\text{im } \hat{\iota} \subseteq \ker \hat{\varphi}$.

In what follows, let s be the maximum of the Artin-Rees constants of the submodules $\iota(M_1) \subseteq M$ and $\varphi(M) \subseteq M_2$.

Next, we will show that $\ker \hat{\varphi} \subseteq \text{im } \hat{\iota}$. Indeed, let $x \in \hat{M}'$ such that $\hat{\varphi}(x) = 0$. Write $\pi_n(x) = x_n + I^n M$, then we have $\varphi(x_n) \in I^n M_2$.

Let $n \in \mathbb{N}$. Then using Artin-Rees we have $\varphi(x_{n+s}) \in I^n(I^s M_2 \cap \varphi(M))$, so we find $x'_{n+s,k} \in M_2$ and $i_{n+s,k} \in I^n$ such that $\varphi(x_{n+s}) = \sum_k i_{n+s,k} \varphi(x'_{n+s,k})$. Then $x_{n+s} - \sum_k i_{n+s,k} x'_{n+s,k} \in \ker \varphi$, so we find $y_{n+s} \in M_1$ such that $\iota(y_{n+s}) = x_{n+s} - \sum_k i_{n+s,k} x'_{n+s,k}$. But then

$$\iota_n(y_{n+s} + I^n M_1) = x_{n+s} - \sum_k i_{n+s,k} x'_{n+s,k} + I^n M = x_{n+s} + I^n M = x_n + I^n M.$$

Hence, we are done as long as we can show that $(y_{n+s} + I^n M_1)_{n \in \mathbb{N}}$ assemble into an element of \hat{M}_1 , i.e., that for $n \leq m$ we have $y_{m+s} + I^n M_1 = y_{n+s} + I^n M_1$. Indeed,

we have

$$\iota(y_{m+s} - y_{n+s}) = x_{m+s} - i_{m+s}x'_{m+s} - x_{n+s} + i_{n+s}x'_{n+s} \in I^{n+s}M,$$

so Artin-Rees tells us that we find $i_{n,m,k} \in I^n M$ and $y_{n,m,k} \in M_1$ such that $\iota(y_{m+s} - y_{n+s}) = \iota(\sum_k i_{n,m,k} y_{n,m,k})$. But ι is injective, so $y_{m+s} - y_{n+s} \in I^n M$ as required, completing the proof that $\ker \hat{\varphi} \subseteq \text{im } \hat{\iota}$.

It remains to show that $\hat{\varphi}$ is surjective. Indeed, let $z = (z_n + I^n M_2) \in \hat{M}_2$. We will construct a preimage $y = (y_n + I^n M) \in \hat{M}$ by induction. In fact, we will do something slightly stronger: we will construct a sequence (y_n) of elements of M such that $y_{n+1} + I^n M = y_n + I^n M$ and $\varphi(y_n) = z_n$ for every n .

We set y_0 to be a preimage of z_0 under φ . Now let $n > 0$ and suppose that we have already defined $y_n \in M$ such that $\varphi(y_n) = z_n$. We need to find $y_{n+1} \in M$ such that $\varphi(y_{n+1}) = z_{n+1}$ and $y_n + I^n M = y_{n+1} + I^n M$.

We have $z_n + I^n M = z_{n+1} + I^n M$, so $z_{n+1} - z_n \in I^n M$, i.e., $z_{n+1} - z_n = \sum r_i w_i$ for $r_i \in I^n$, $w_i \in M_2$. By surjectivity of φ , we find $t_i \in M$ such that $s := \sum r_i t_i \in I^n M$ satisfies $\varphi(s) = z_{n+1} - z_n$. Define $y_{n+1} := y_n + s$. Then $y_{n+1} + I^n M = y_n + I^n M$ since $s \in I^n M$, and $\varphi(y_{n+1}) = \varphi(y_n) + \varphi(s) = z_n + z_{n+1} - z_n = z_{n+1}$. \square

PROPOSITION 5.13. Let r_1, \dots, r_n be generators of I . Define

$$\varphi: R[X_1, \dots, X_n] \rightarrow R, \quad X_i \mapsto r_i,$$

Then we have an induced ring isomorphism $\tilde{\varphi}: R[X_1, \dots, X_n]/\ker \varphi \xrightarrow{\cong} R$, and the I -adic topology on R is the same as the $\varphi^{-1}(I)$ -adic topology on $R[X_1, \dots, X_n]/\ker \varphi$. But $\varphi^{-1}(I) = (J + \ker \varphi)/\ker \varphi$, where $J = (X_1, \dots, X_n)$, and so completing $R[X_1, \dots, X_n]/\ker \varphi$ as a ring with respect to the ideal $\varphi^{-1}(I)$ is the same as completing it as an $R[X_1, \dots, X_n]$ -module with respect to the ideal J of $R[X_1, \dots, X_n]$.

But then we can use the previous proposition to find that

$$(R[X_1, \dots, X_n]/\ker \varphi)^\vee \cong (R[X_1, \dots, X_n])^\vee / \ker \hat{\varphi}.$$

as $R[X_1, \dots, X_n]$ -modules. It is not hard to see that this is actually an isomorphism of rings. As previously remarked, the completion of $R[X_1, \dots, X_n]$ with regard to J is $\hat{R}[[X_1, \dots, X_n]]$, so \hat{R} is isomorphic as a ring to a quotient of $\hat{R}[[X_1, \dots, X_n]]$, which is noetherian.

PROPOSITION 5.14. For a finitely generated R -module M , the composite of R -linear maps

$$\hat{R} \otimes_R M \rightarrow \hat{R} \otimes_R \hat{M} \rightarrow \hat{R} \otimes_R \hat{M} \cong M$$

is surjective. If R is noetherian, it is an isomorphism.

PROOF. Since M is finitely generated, it fits into a short exact sequence

$$0 \longrightarrow N \longrightarrow F \longrightarrow M \longrightarrow 0,$$

where F is free of finite rank. But we have a chain of isomorphisms

$$\hat{R} \otimes_R F = \hat{R} \otimes_R R^n \cong (\hat{R} \otimes_R R)^n \cong \hat{R}^n = \widehat{R^n} = \hat{F},$$

and it is readily checked on generators that this agrees with the map $\hat{R} \otimes_R F \rightarrow \hat{F}$ described above. Hence, we have a commutative square

$$\begin{array}{ccc} \hat{R} \otimes_R F & \longrightarrow & \hat{R} \otimes_R M \\ \downarrow & & \downarrow \\ \hat{F} & \longrightarrow & \hat{M}, \end{array}$$

where the left map is an isomorphism as we just saw. Furthermore, in the proof of the exactness of completion, we did not use that R is noetherian to show surjectivity.

Hence, the bottom map is surjective, and by commutativity, the right map is surjective as claimed.

Now if R is noetherian, using right exactness of the tensor product and exactness of completion we get a commutative diagram

$$\begin{array}{ccccccc} \hat{R} \otimes_R N & \longrightarrow & \hat{R} \otimes_R F & \longrightarrow & \otimes_R M & \longrightarrow & 0 \\ \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \downarrow 0 \\ \hat{N} & \longrightarrow & \hat{F} & \longrightarrow & \hat{M} & \longrightarrow & 0 \end{array}$$

with exact rows. We already know that β is an isomorphism and γ is surjective, and since N is also finitely generated (Sheet 2, Exercise 9), α is surjective. Of course, the zero map is injective, and thus the four lemma tells us that γ is also injective, completing the proof. \square

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

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

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, \dots, r_n and so is I_2 , say by s_1, \dots, s_m . Then if $(r, s) \in I_1 \times I_2$, we have

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

so $I_1 \times I_2$ is finitely generated by $(r_1, 0), \dots, (r_n, 0), (0, s_1), \dots, (0, s_m)$. \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 $S := \bigcap_{P \in \mathcal{S}'} P$. S is obviously an ideal, and we will show that it is prime. Assume that $x, y \in A$ such that $xy \in S$. Since every $P \in \mathcal{S}'$ is prime, we may write $\mathcal{S}' = \mathcal{S}_x \cup \mathcal{S}_y$, where $\mathcal{S}_x := \{P \in \mathcal{S}' \mid x \in P\}$ and $\mathcal{S}_y := \{P \in \mathcal{S}' \mid y \in P\}$. We claim that it is true that

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

Indeed, the negation of this statement is

$$(\exists P \in \mathcal{S}' \forall P' \in \mathcal{S}_x: P' \not\subseteq P) \wedge (\exists Q \in \mathcal{S}' \forall Q' \in \mathcal{S}_y: Q' \not\subseteq Q),$$

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 $\text{coker } \theta^n$.]

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 $x \notin \text{im } \theta$. Let $n \in \mathbb{N}$. Then we have $\theta^n(x) \in \text{im } \theta^n$. Suppose that $\theta^n(x) \in \text{im } \theta^{n+1}$. 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, $\theta^n(x) \in \text{im } \theta^n \setminus \text{im } \theta^{n+1}$ and we have an infinite strictly decreasing chain

$$\text{im } \theta \supsetneq \text{im } \theta^2 \supsetneq \text{im } \theta^3 \supsetneq \cdots. \quad \square$$

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 $g := \sum_{i=0}^n a_i X^i$ 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. \square

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, \dots, M_k is a finitely generated submodule of M , say M_j is generated by $m_{j1}, \dots, m_{j\ell_j}$. There are polynomials $f_{j1}, \dots, f_{j\ell_j} \in N$ 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 expressible 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 combination of the f_{ij} , so f is expressible as a linear combination as well. \square

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 $r \in J(R)$. \square

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 \mathbb{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. \square

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 $\theta: M \rightarrow N$ be a homomorphism of A -modules. If the induced map $M/IM \rightarrow N/IN$ 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. \square

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-divisors 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. \square

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 proceed by induction on n . The claim is obviously true for $n = 1$. Suppose that

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

and q_{n+1} is a maximal ideal distinct from the q_i . We have $Q \not\subseteq q_{n+1}$, 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. \square

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 $Q_n := \bigcap_{i=1}^n q_i$. 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. \square

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, we 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

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

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 $\varphi: R \rightarrow S$ 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 $A[X] \rightarrow A$ and $A[[X]] \rightarrow A$ 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

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

and

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

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

$$\frac{\varphi^{-1}(M'_i)}{\varphi^{-1}(M'_{i+1})} \rightarrow \frac{M'_i}{M'_{i+1}}.$$

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

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, \dots, v_n , then defining $V_i := \langle v_1, \dots, v_{n-i} \rangle$ 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 $v_1, v_2, \dots \in B$ pairwise distinct. Then

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

is an infinite strictly ascending chain and

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

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

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 $A_i := P_1 \cdots P_i / P_1 \cdots P_{i+1}$ 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. \square

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 particular, if M is generated by m_1, \dots, m_n , we find s_i such that $s_i m_i = 0$. Define $s := \prod s_i$, 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. \square

Exercise 2.

EXERCISE. Let I be an ideal of R , and define $S := 1 + I$. 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

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

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 $s_1 s_2 \in S \cap I = \emptyset$, 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 the 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 $p_i \cap S = \emptyset$, 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 subsets 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.

$$\begin{array}{ccccc} R & \xrightarrow{\alpha} & S^{-1}R & \xrightarrow{\delta} & U^{-1}S^{-1}R \\ & \searrow \beta & \downarrow \gamma & \nearrow \Phi & \uparrow \Psi \\ & & (ST)^{-1}R & & \end{array}$$

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 $\gamma: S^{-1}R \rightarrow (ST)^{-1}R$ 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 $\Phi: U^{-1}S^{-1}R \rightarrow (ST)^{-1}R$ 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 $\Psi: (ST)^{-1}R \rightarrow U^{-1}S^{-1}R$ 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. \square

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 $\text{ann}(x) = \{r \in R \mid rx = 0\}$. If $\text{ann}(x) \neq R$, then $\text{ann}(x) \subseteq \mathfrak{m}$ for some maximal ideal \mathfrak{m} . Then \mathfrak{m} is prime. Let $\varphi: R \rightarrow R_{\mathfrak{m}}$. 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 $s \in \text{ann}(x)$, which is a contradiction. Hence we must have $\text{ann}(x) = R$, in particular $x = 1 \cdot x = 0$. \square

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 $R := \mathbb{Z}/6\mathbb{Z}$. 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. \square

Exercise 7.

EXERCISE. Suppose $R \neq 0$ and let Σ be the set of all 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 $I := R \setminus S$ is a prime ideal. If $r, s \in I$, then SM_r and SM_s , where $M_r := \{1, r, r^2, \dots\}$, 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 $r^n xt^n = 0$, 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 $R \setminus S'$. \square

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. \square

- EXERCISE.** (i) S_0 is the largest multiplicatively closed subset of R for which the homomorphism $R \rightarrow S_0^{-1}R$ 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 $R \rightarrow S_0^{-1}R$ is bijective.

SOLUTION. For (i), let S be any multiplicatively closed set. We claim that $\varphi: R \rightarrow S^{-1}R$ 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

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S_0^{-1}R \\ & \searrow \text{id} & \downarrow \theta \\ & & R \end{array}$$

commute. It remains to verify that $\varphi \circ \theta = \text{id}_{S_0^{-1}R}$. 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. \square

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

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

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

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

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. \square

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. \square

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 $rs m = srm = s0 = 0$.

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 $rs(m+n) = srm + rs n = 0$. \square

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 $sr m = 0$. 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. \square

EXERCISE. If $f: M \rightarrow N$ 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 $f(m) \in T(N)$. \square

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 $\text{im } f|_{T(M')}$ 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 $m \in \text{im } f|_{T(M')}$. \square

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. \square

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 $\text{ann}(m) = \{r \in R \mid rm = 0\}$. Suppose $\text{ann}(m)$ is a proper ideal. Then $\text{ann}(m) \subseteq \mathfrak{m}$ for some maximal ideal \mathfrak{m} . By Exercise 14(ii) and our assumption, m is in the kernel of the map $M \rightarrow M_{\mathfrak{m}}$, so we find $s \in R \setminus \mathfrak{m}$ such that $sm = 0$. But then $s \in \text{ann}(m) \cap R \setminus \mathfrak{m} = \emptyset$, a contradiction. We conclude $\text{ann}(m) = R$, so in particular $m = 1 \cdot m = 0$, i.e., M is torsion-free. \square

Example Sheet 4**Exercise 1.**

EXERCISE. Let M be an R -module and I an ideal of R . Suppose that $M_P = 0$ for all maximal ideals P containing I . Then $M = IM$.

PROOF. Since being trivial is a local property, it will suffice that $(M/IM)_P = 0$ for all maximal ideals P . Let P be a maximal ideal. We distinguish two cases.

First, if $I \subseteq P$, then $M_P = 0$. By exactness of localization, we have an exact sequence

$$0 \longrightarrow (IM)_P \longrightarrow M_P \longrightarrow (M/IM)_P \longrightarrow 0,$$

so the map $M_P \rightarrow (M/IM)_P$ is surjective, so $(M/IM)_P = 0$ as required.

Second, if $I \not\subseteq P$, then we find $i \in I \setminus P$. Now if $\frac{m+IM}{r}$ is any element of $(M/IM)_P$, then $i(m+IM) = 0$, so $\frac{m+IM}{r} = \frac{0}{1}$ as elements of $(M/IM)_P$, so $(M/IM)_P = 0$ as required. \square